Asigra Cloud Backup v14.2

DS-Client User Guide

June 2025

asigra

Disclaimer
Information in this document is subject to change without notice and does not represent a commitment on the part of Asigra Inc.

Asigra Inc. makes no representation or warranty, express, implied, or statutory, with respect to, and assumes no responsibility for the accuracy, completeness, sufficiency or usefulness of the information contained herein.

This document may contain sample screen shots, used to demonstrate Asigra Cloud Backup™ procedures. All information appearing in this document is used for illustration purposes only, and should be considered fictitious

The software described in this document is furnished under a license agreement. It is against the law to copy the software on any medium except as specifically allowed in the license agreement.

“Asigra”, the Asigra logo, “Asigra Cloud Backup”, “Recovery is Everything”, and “Recovery License Model” are trademarks of Asigra Inc. All other brand and product names are, or may be, trademarks of their respective owners.

4711 Yonge St, Suite 10098, North York, Ontario, Canada M2N 6K8

Release Date: June 2025

Contents

Document history **11**

1 Getting started **15**
1.1 Connecting to a DS-Client 16
1.2 Performing the initial DS-Client configuration 17
1.3 Working in the DS-User main window 19
1.4 Starting or stopping the DS-Client service or daemon 20
1.5 Viewing DS-Client information 21
1.6 Disconnecting from a DS-Client 21
1.7 Exiting the DS-User application 21

2 Configuring the DS-Client **23**
2.1 Configuring the DS-Client settings 23
2.1.1 Configuring the setup information 23
2.1.2 Configuring the default settings 24
2.1.3 Configuring the notification settings 27
2.1.4 Configuring the SNMP settings 29
2.1.5 Configuring the parameter settings 30
2.1.6 Configuring the DS-System connection settings 33
2.1.7 Configuring the user and group settings 35
2.1.8 Configuring the advanced settings 37
2.2 Configuring the initialization settings 60
2.2.1 Configuring the connection settings 60
2.2.2 Configuring the regional settings 63
2.2.3 Configuring the plug-in settings 63
2.2.4 Configuring the keep alive settings 64
2.3 Configuring users and groups 64
2.4 Configuring the LDAP user settings 65
2.5 Configuring the two-factor authentication settings 66
2.6 Configuring the Local DS-VDR Tool 68
2.7 Configuring the bandwidth throttle settings 69
2.8 Configuring the filter for the Event Log 70
2.9 Configuring the printer settings 71
2.10 Configuring the appearance of the main window 71
2.11 Managing DS-Client activities 72
2.11.1 Viewing the system status 73
2.11.2 Enabling or disabling DS-Client activities 74
2.11.3 Managing administrative processes 74
2.11.4 Recovering the DS-Client database 78
2.11.5 Shutting down the DS-Client computer 81
2.12 Managing passwords (Windows) 81
2.13 Exporting the DS-Client configuration to an XML file 83
2.14 Sending upgrade information to the DS-System 85
2.15 Viewing storage quotas 85
2.16 Viewing the DS-NOC settings 87
2.17 Viewing the memory allocation 87
2.18 Updating the DS-Client configuration file parameters 88

3 Working with schedules **89**
3.1 Configuring a schedule 90

3.2 Assigning a schedule to a backup . . . 93
3.3 Viewing scheduled backups . . . 94
3.4 Setting the priority of a scheduled backup . . . 95
3.5 Activating or suspending a schedule . . . 96

4 Working with retention rules . . . 97
4.1 Configuring a retention rule . . . 98
4.2 Assigning a retention rule to a backup . . . 103
4.3 Enforcing a retention rule . . . 104

5 Working with backups . . . 105
5.1 Backup types . . . 106
5.1.1 Online backups . . . 106
5.1.2 Self-contained backups . . . 106
5.1.3 Local-only backups . . . 106
5.1.4 Instant recovery backups . . . 107
5.1.5 Statistical backups . . . 107
5.2 Backup considerations . . . 108
5.2.1 Changed block tracking (CBT) . . . 108
5.2.2 Continuous data protection (CDP) . . . 108
5.2.3 DS-Client buffer . . . 110
5.2.4 Block-level resume . . . 111
5.2.5 Database backup policies . . . 112
5.2.6 Pre/Post backup processes . . . 113
5.2.7 Performance . . . 113
5.2.8 Backup wizard . . . 114
5.3 Restore considerations . . . 129
5.3.1 Restoring a specific generation of a file . . . 129
5.3.2 Pre/Post restore processes . . . 129
5.3.3 Restoring data to an alternate location . . . 130
5.3.4 Restoring system state and services database . . . 130
5.3.5 Restoring transaction logs only (Microsoft SQL) . . . 131
5.3.6 File-Level Restore (FLR) . . . 132
5.3.7 Restoring VSS-aware backup components . . . 133
5.3.8 Transmitted amount discrepancies . . . 134
5.3.9 Restore Wizard . . . 134
5.4 File system backups (Windows) . . . 142
5.4.1 Creating a File system backup . . . 142
5.4.2 Restoring a File system backup . . . 155
5.5 File system (NAS, NFS, UNIX-SSH) backups (Linux or Mac) . . . 162
5.5.1 Hard link requirements . . . 162
5.5.2 Creating a local file system backup . . . 163
5.5.3 Creating a NAS file system backup . . . 171
5.5.4 Creating an NFS file system backup . . . 179
5.5.5 Creating a UNIX-SSH file system backup . . . 186
5.5.6 Restoring a NAS, NFS, UNIX-SSH file system backup . . . 195
5.6 Email backups (Windows) . . . 200
5.6.1 Microsoft Exchange Server (ESW) requirements . . . 200
5.6.2 Microsoft Outlook (DS-MLR) requirements . . . 203
5.6.3 Creating a Microsoft Exchange Server (EWS) backup . . . 204
5.6.4 Restoring a Microsoft Exchange Server (EWS) backup . . . 211
5.6.5 Creating a Microsoft Outlook (DS-MLR) backup . . . 214
5.6.6 Restoring a Microsoft Outlook (DS-MLR) backup . . . 221
5.7 Google Workspace backups (Windows) . . . 225
5.7.1 Google Workspace requirements . . . 226

5.7.2 Creating a Google Workspace backup . . . 229
5.7.3 Restoring a Google Workspace backup . . . 236
5.8 IBM DB2 database backups (Linux) . . . 241
5.8.1 General requirements . . . 241
5.8.2 DS-Client computer requirements . . . 241
5.8.3 IBM DB2 requirements . . . 241
5.8.4 Backup requirements . . . 242
5.8.5 Restore requirements . . . 242
5.8.6 Creating an IBM DB2 database backup . . . 242
5.8.7 Restoring an IBM DB2 database backup . . . 250
5.9 MariaDB database backups (Windows, Linux, or Mac) . . . 253
5.9.1 General requirements . . . 253
5.9.2 Backup requirements . . . 253
5.9.3 Restore requirements . . . 254
5.9.4 Creating a MariaDB database backup (Windows) . . . 254
5.9.5 Creating a MariaDB database backup (Linux or Mac) . . . 261
5.9.6 Restoring a MariaDB database backup . . . 268
5.10 Microsoft 365 backups (Windows) . . . 272
5.10.1 General requirements . . . 273
5.10.2 Network requirements . . . 274
5.10.3 DS-Client computer requirements . . . 274
5.10.4 Microsoft 365 requirements . . . 274
5.10.5 Exchange Online requirements . . . 274
5.10.6 SharePoint Online and OneDrive requirements . . . 277
5.10.7 Creating a Microsoft 365 backup . . . 277
5.10.8 Restoring a Microsoft 365 backup . . . 284
5.11 Microsoft 365 Groups backups (Windows) . . . 288
5.11.1 Configuring Microsoft Azure Active Directory . . . 288
5.11.2 General limitations . . . 291
5.11.3 Backup limitations . . . 291
5.11.4 Restore limitations . . . 291
5.11.5 Creating a Microsoft 365 Groups backup . . . 292
5.11.6 Restoring a Microsoft 365 Groups backup . . . 296
5.12 Microsoft Exchange Server (VSS-aware) backups (Windows) . . . 298
5.12.1 Creating a Microsoft Exchange Server (VSS-aware) backup . . . 299
5.12.2 Performing a VSS restore . . . 309
5.12.3 Performing a file restore . . . 314
5.12.4 Performing a granular restore . . . 318
5.12.5 Performing a file restore to recovery database (RDB) . . . 327
5.13 Microsoft Hyper-V Server (VSS-aware) backups (Windows) . . . 328
5.13.1 General requirements . . . 328
5.13.2 Backup requirements . . . 329
5.13.3 Creating a Microsoft Hyper-V Server (VSS-aware) backup . . . 329
5.13.4 Performing a VSS restore . . . 338
5.13.5 Performing a file restore . . . 342
5.13.6 Performing a file-level restore . . . 346
5.14 Microsoft SharePoint Server (Classic) backups (Windows) . . . 348
5.14.1 Creating a Microsoft SharePoint Server (Classic) backup . . . 349
5.14.2 Restoring a Microsoft SharePoint Server (Classic) backup . . . 355
5.15 Microsoft SharePoint Server (VSS-aware) backups (Windows) . . . 357
5.15.1 General requirements . . . 357
5.15.2 DS-Client requirements . . . 357
5.15.3 Backup requirements . . . 358
5.15.4 Restore requirements . . . 358

5.15.5 Creating a Microsoft SharePoint Server (VSS-aware) backup . . . 359
5.15.6 Performing a VSS restore . . . 366
5.15.7 Performing a file restore . . . 370
5.15.8 Performing a granular restore . . . 375
5.16 Microsoft SQL Server (Classic) backups (Windows) . . . 382
5.16.1 Creating a Microsoft SQL Server (Classic) backup . . . 382
5.16.2 Restoring a Microsoft SQL Server (Classic) backup . . . 393
5.17 Microsoft SQL Server (VSS-aware) backups (Windows) . . . 397
5.17.1 Integrating with Nimble Storage . . . 398
5.17.2 Creating a Microsoft SQL Server (VSS-aware) backup . . . 400
5.17.3 Performing a database restore . . . 409
5.17.4 Performing a file restore . . . 414
5.18 Oracle database backups (Windows or Linux) . . . 419
5.18.1 General requirements . . . 420
5.18.2 DS-Client computer requirements . . . 420
5.18.3 Oracle database requirements . . . 421
5.18.4 Backup requirements . . . 421
5.18.5 Restore requirements . . . 422
5.18.6 Creating an Oracle database backup (Windows) . . . 423
5.18.7 Creating an Oracle database backup (Linux) . . . 430
5.18.8 Restoring an Oracle database backup . . . 437
5.19 Oracle MySQL database backups (Windows, Linux, or Mac) . . . 442
5.19.1 General requirements . . . 442
5.19.2 Backup requirements . . . 442
5.19.3 Restore requirements . . . 442
5.19.4 Creating an Oracle MySQL database backup (Windows) . . . 443
5.19.5 Creating an Oracle MySQL database backup (Linux or Mac) . . . 450
5.19.6 Restoring an Oracle MySQL database backup . . . 457
5.20 Oracle SBT database backups (Linux) . . . 461
5.20.1 Backup requirements . . . 461
5.20.2 Restore requirements . . . 462
5.20.3 Creating an Oracle SBT database backup . . . 462
5.21 Permissions Only backups (Windows, Linux, or Mac) . . . 467
5.21.1 Creating a Permissions Only backup . . . 467
5.21.2 Restoring a Permissions Only backup . . . 477
5.22 PostgreSQL database backups (Linux or Mac) . . . 480
5.22.1 General requirements . . . 480
5.22.2 DS-Client requirements . . . 480
5.22.3 PostgreSQL server requirements . . . 480
5.22.4 Restore requirements . . . 481
5.22.5 Creating a PostgreSQL database backup . . . 481
5.22.6 Restoring a PostgreSQL database backup . . . 487
5.23 Salesforce backups (Windows) . . . 490
5.23.1 General requirements . . . 490
5.23.2 DS-Client computer requirements . . . 490
5.23.3 Creating a Salesforce backup . . . 491
5.23.4 Performing a table level restore . . . 497
5.23.5 Performing a granular restore . . . 503
5.23.6 Performing an item restore . . . 505
5.23.7 Resuming a Salesforce data restore process . . . 508
5.24 VMware vCenter Server backups (Windows or Linux) . . . 509
5.24.1 Backing up virtual machines in a cluster . . . 511
5.24.2 Performing an incremental restore . . . 511
5.24.3 Using VMware transport libraries . . . 512

5.24.4 Creating a VMware vCenter Server backup . . . 513
5.24.5 Restoring a VMware vCenter Server backup . . . 520
5.25 Configuring Pre/Post processes (Windows) . . . 525
5.26 Configuring Pre/Post processes (Linux) . . . 528
5.27 Disabling CDP for a backup . . . 529

6 Managing backups . . . 531
6.1 Performing an on-demand backup . . . 531
6.1.1 Excluding files that failed to be backed up . . . 533
6.2 Working with instant recovery backups . . . 534
6.2.1 Creating an instant recovery backup . . . 535
6.2.2 Performing instant recovery (File system) . . . 536
6.2.3 Performing instant recovery (Exchange Server) . . . 537
6.2.4 Performing instant recovery (Hyper-V Server) . . . 538
6.2.5 Performing instant recovery (SharePoint Server) . . . 539
6.2.6 Performing instant recovery (SQL Server) . . . 540
6.2.7 Performing instant recovery (VMware vCenter) . . . 541
6.2.8 Performing a session-level delete . . . 542
6.2.9 Performing a machine-level delete . . . 542
6.3 Renaming a backup . . . 543
6.4 Activating or suspending a backup . . . 543
6.5 Synchronizing a backup . . . 544
6.6 Migrating a backup . . . 545
6.7 Cloning a backup . . . 546
6.8 Converting a backup . . . 547
6.9 Validating a backup . . . 547
6.10 Recovering an orphaned backup . . . 549
6.11 Changing the ownership of a backup . . . 551
6.12 Changing the permissions of a backup . . . 551
6.13 Configuring the properties of a backup . . . 552
6.13.1 Modifying share access properties . . . 553
6.13.2 Modifying connection information (Exchange Server) . . . 553
6.13.3 Modifying connection information (Email) . . . 554
6.13.4 Modifying connection options (Linux DS-Client) . . . 554
6.13.5 Modifying a backup name . . . 554
6.14 Deleting backups and backup data . . . 555
6.14.1 Performing a selective delete . . . 557
6.14.2 Performing an assisted delete . . . 558
6.14.3 Deleting a backup . . . 562
6.14.4 Deleting local-only backup data . . . 563
6.15 Cleaning local-only trash . . . 564
6.15.1 Modifying database information (SQL Server - Classic) . . . 564

7 Working with VM replication sets (Windows) . . . 565
7.1 Licensing considerations . . . 565
7.2 Credential considerations . . . 566
7.3 Configuration considerations . . . 566
7.4 Creating a VMware vCenter Server replication set . . . 567
7.4.1 Selecting the kind of VM replication set . . . 567
7.4.2 Selecting the VM replication type . . . 567
7.4.3 Specifying the source server . . . 568
7.4.4 Selecting the items to replicate . . . 568
7.4.5 Specifying replication item options . . . 568
7.4.6 Specifying the destination for the replication set . . . 568
7.4.7 Specifying destination for VM replication . . . 569

7.4.8 Specifying the replication set options . . . 570
7.4.9 Specifying notification options . . . 570
7.4.10 Assigning a schedule . . . 572
7.4.11 Naming the VM replication set . . . 572
7.5 Performing on-demand replication . . . 572
7.6 Performing offline replication . . . 573
7.6.1 Copying the initial replication data . . . 573
7.6.2 Importing the Initial VMR set . . . 573
7.7 Performing a failover . . . 574
7.8 Performing a failback . . . 575

8 Viewing logs . . . 577
8.1 Viewing the Activity Log . . . 578
8.2 Viewing the Event Log . . . 580
8.3 Viewing the Audit Trail . . . 582

9 Working with reports . . . 583
9.1 Configuring the font for reports . . . 583
9.2 Generating a global report for multiple DS-Clients . . . 583
9.3 Generating a Backup Groups Report . . . 585
9.4 Generating a Backup Items Report . . . 587
9.5 Generating a Backup / Restore Report . . . 589
9.6 Generating a Backup Sets Report . . . 591
9.7 Generating a Backup Trends Report . . . 593
9.8 Generating a Backup Users Report . . . 595
9.9 Generating a Restorable Volume Report . . . 596
9.10 Generating a Restore Activities Report . . . 598
9.11 Generating a Statistical Summary Report . . . 599
9.12 Viewing a Load Summary Report . . . 601
9.13 Viewing an Online File Summary Report . . . 602
9.14 Viewing a Storage Summary Report . . . 605
9.15 Exporting information about backups . . . 607
9.16 Creating a custom report . . . 608
9.16.1 Exporting a data set file for a custom report . . . 608
9.16.2 Creating a custom report using exported data . . . 610

10 Working with a Grid DS-Client (Windows) . . . 613
10.1 Managing a Grid DS-Client . . . 614
10.2 Viewing the Grid DS-Client Log . . . 615

11 Using premium backup and recovery services . . . 617
11.1 Initial backups . . . 617
11.1.1 Configuring the initial backup path . . . 618
11.1.2 Creating an initial backup . . . 619
11.1.3 Monitoring the status of an initial backup . . . 620
11.2 Disc/tape backups . . . 621
11.2.1 Requesting a disc/tape backup . . . 622
11.2.2 Viewing the status of a disc/tape request . . . 623
11.2.3 Restoring from a disc/tape backup . . . 624
11.3 Backup Lifecycle Management (BLM) . . . 624
11.3.1 Configuring a backup for BLM . . . 625
11.3.2 Performing an on-demand BLM request . . . 625
11.3.3 Configuring a BLM schedule . . . 626
11.3.4 Restoring from the BLM Archiver . . . 627
11.3.5 Converting from tape to BLM . . . 627
11.4 Local Storage Tool . . . 629

11.4.1 Local storage vs local storage cache . . . 630
11.4.2 Setting the default local storage path . . . 632
11.4.3 Configuring a backup with local storage . . . 632
11.4.4 Configuring a backup to use the local storage cache . . . 633
11.5 Multitenant DS-Clients . . . 634
11.5.1 Activating the multitenant feature . . . 634
11.5.2 Configuring a multitenant DS-Client . . . 635
11.6 Snapshot Manager (Linux) . . . 636
11.6.1 Configuring a storage device . . . 637
11.6.2 Configuring a snapshot retention policy . . . 638
11.6.3 Configuring a snapshot schedule . . . 639
11.6.4 Configuring a snapshot transfer . . . 640
11.6.5 Restoring a snapshot transfer . . . 641
11.6.6 Deactivating a snapshot transfer . . . 642
11.6.7 Reactivating a snapshot transfer . . . 642

12 Using LAN Storage Discovery Tool . . . 643
12.1 LAN Storage Discovery best practices . . . 643
12.2 Scanning for shares on the LAN . . . 644
12.3 Configuring scanned shares . . . 647
12.4 Monitoring scanned shares . . . 648
12.5 Generating a LAN File Summary Report . . . 649
12.6 Generating an Access Report . . . 650
12.7 Generating an Extensions Report . . . 651
12.8 Generating a File Size Report . . . 652
12.9 Generating a Growth Report . . . 652
12.10 Generating a Share Usage Report . . . 653
12.11 Generating a Virtual Machines Summary Report . . . 653
12.12 Exporting reports . . . 654

13 Using Unprotected LAN Resource Discovery Tool . . . 657
13.1 Scanning for unprotected LAN resources . . . 657
13.2 Viewing the list of unprotected LAN resources . . . 659

Document history

Version	Date	Summary
1.0	August 31, 2020	• Released for General Availability.
1.1	October 2, 2020	• Management Console users can now scan their Microsoft 365 (Exchange Online) files for malware during the backup and restore process. Requires Windows DS-Client (14.2.0.1) and Management Console (14.2.0.1) or later.
1.2	January 20, 2021	• Management Console users can now scan their Microsoft 365 (Groups and Teams) files for malware during the backup and restore process. Requires Windows DS-Client v14.2.0.2) and Management Console v14.2.0.2 or later. • Management Console users can now remotely manage DS-Clients without opening a port in the firewall on the DS-Client machine. Requires DS-Client v14.2.0.2, DS-System v14.2.0.2, and Management Console v14.2.0.2 or later. • Management Console users can now configure a process to run before and/or after a File system backup to perform actions when a condition is met. Requires Windows DS-Client v14.2.0.2 and Management Console v14.2.0.2 or later.
1.3	February 1, 2022	• The version of the log4j component used by the Asigra software has been updated to the latest version to ensure our software is not flagged by any scanning tools. Requires Windows DS-Client v14.2.0.5, DS-NOC v14.2.0.4, and Management Console v14.2.0.5 or later. • When configuring a Microsoft 365 backup in DS-User, users can now perform folder-level backups of SharePoint and OneDrive Document libraries. Requires Windows DS-Client v14.2.0.5 and Windows DS-User v14.2.0.4 or later. • When configuring a Salesforce backup in DS-User, users can now sort the list of database tables. Requires Windows DS-User v14.2.0.4 or later. • When performing a backup of a virtual machine on a VMware vCenter Server, a warning message is now displayed in the Event Log if a backup snapshot cannot be removed at the end of the backup activity. Requires Windows DS-Client v14.2.0.5 or Linux DS-Client v14.2.0.4 or later.
1.4	August 29, 2022	• Management Console users can now scan File System backups for potentially malicious or unauthorized content based on predefined policies. Requires Windows DS-License Server RLM v14.2.0.5, Windows DS-System v14.2.0.5, Windows DS-Client v14.2.0.6, and Management Console v14.2.0.6 or later. • Management Console users can now backup and restore Microsoft 365 SharePoint and OneDrive data using Modern Authentication credentials. Requires Windows DS-Client v14.2.0.6 and Management Console v14.2.0.6 or later. • Management Console users can now backup and restore individual Microsoft 365 SharePoint and OneDrive files that are up to 250 GB in size. Requires Windows DS-Client v14.2.0.6 or later. • When configuring a Microsoft 365 backup, users can now perform folder-level backups of SharePoint and OneDrive Document libraries. Requires Windows DS-Client v14.2.0.5, Windows DS-User v14.2.0.4 or Windows Management Console v14.2.0.6 or later.

1.4	August 29, 2022	• SharePoint and OneDrive performance has been improved when backing up and restoring multiple large files. DS-Client memory usage has been reduced when backing up and restoring SharePoint and OneDrive data. Requires Windows DS-Client v14.2.0.6 or later. • When configuring a VMware vCenter Server backup, users can now configure the days of the week on which they want to validate the disk signature of a protected virtual machine. Requires DS-User v14.2.0.5 or Management Console v14.2.0.6 and Windows DS-Client v14.2.0.5 or Linux DS-Client v14.2.0.4 or later. • When configuring the SMTP server notification settings in DS-User, users can now enter a password for the SMTP Server that contains up to 128 characters. Requires DS-User v14.2.0.5, Windows DS-Client v14.2.0.6 or Linux DS-Client v14.2.0.5 or later. • The embedded version of PostgreSQL installed with the DS-Client (Windows, Linux, Mac) software has been upgraded to the latest version of PostgreSQL 11 to address any security vulnerabilities. Requires Windows DS-Client v14.2.0.6, Linux DS-Client v14.2.0.5 or Mac DS-Client v14.2.0.5 or later.
1.5	April 10, 2023	• Management Console Global Administrators can now configure Multiperson Approval (MPA) for accounts so users require multiple people to approve a potentially destructive action that can result in the loss of data. Administrators must configure a threshold to determine how many approvals are required and select the approvers from a list of users. When a user attempts to perform a task that requires approval, the approvers receive an email with the name of the user and a description of the task and must approve or deny the request. The approval link expires after 30 minutes. A task must meet the configured approval threshold with no denials to be approved. Requires Management Console 14.2.0.8, Windows DS-Client 14.2.0.8 or Linux or Mac DS-Client 14.2.0.6, DS-System 14.2.0.6, and DS-Operator 14.2.0.6 or later. • Management Console users can now scan their File System backups for malware during the backup and restore process when connected to a Linux or Mac DS-Client. Requires Management Console 14.2.0.8 and Linux or Mac DS-Client 14.2.0.6 or later. • When scanning File System backups for malware during the restore process, Management Console users can now either quarantine the infected files in a password-protected zip file or attempt to clean the infected files and restore them when the remediation is successful. Requires Management Console 14.2.0.8 and Windows DS-Client 14.2.0.8 or Linux or Mac DS-Client 14.2.0.6 or later. • When scanning File System backups for malware during the backup process, files detected with malware are no longer quarantined. The files are backed up to the DS-System in an encrypted format so they cannot infect the data repository. Infected files can be quarantined or cleaned during the restore process. Requires Windows DS-Client 14.2.0.8 or later. • Improved performance when restoring Microsoft 365 (Exchange Online) data. Requires Windows DS-Client v14.2.0.8 or later. • Improved data processing and performance when backing up Microsoft 365 (SharePoint Online) data. Requires Windows DS-Client v14.2.0.8 or later • Windows DS-Client now supports the Transport Layer Security (TLS) 1.3 encryption protocol. Requires Windows DS-Client 14.2.0.8 or later.

1.5	April 10, 2023	• When performing a restore of a File system backup, users now have the option to restore data deduplication links as links, skip data deduplication links, or restore the last non-link. Requires Windows DS-Client 14.2.0.8 and DS-User 14.2.0.6 or later. • When performing a Bare Metal Restore (BMR) of a computer with active retention rules, users can now select a backup session suitable for BMR. Requires Windows DS-Client 14.2.0.8 and DS-User 14.2.0.6 or later. • When attempting to perform a backup of a Microsoft Hyper-V Server backup that is being replicated, a warning message is now displayed to indicate when a virtual machine is offline. Requires Windows DS-Client 14.2.0.8 or later. • Updated the Google Drive, Gmail, Calendar, and Contacts APIs to support the latest Google Workspace features and implemented dynamic thread pool management so the GAppsMaxJavaPluginThreads advanced configuration parameter is no longer required or available. Requires Windows DS-Client 14.2.0.8 or later. • Updated third-party components used by the Asigra software to address potential security vulnerabilities. Requires Windows DS-Client 14.2.0.8 and DS-User 14.2.0.6 or later.
1.6	December 4, 2023	• The maximum length of a Microsoft 365 backup name autogenerated by the autodiscover or multiple backup set creation process in Management Console has been extended from 80 to 255 characters. Backup names exceeding 255 characters are appended with a unique identifier. Requires Windows DS-Client 14.2.0.10 and Management Console 14.2.0.9 or later. • Management Console users can now configure a whitelist at the DS-Client and File system backup set level to exclude specific folders and files from the antimalware scan during the backup or restore process. Requires Windows DS-Client 14.2.0.10, Linux or Mac DS-Client 14.2.0.7, and Management Console 14.2.0.9 or later. • Users can configure the ExchangeOnlineBackupBatchResponseSizeLimit advanced configuration parameter in DS-User to specify the maximum response content size limit (in MB) for a single batch backup request for EWS or Exchange Online backups when the ExchangeOnlineBackupBatchSize parameter is enabled and set to greater than 1. Requires Windows DS-Client 14.2.0.10 or later. • Improved performance when using a Windows DS-Client to synchronize backups that contain many folders and files. Requires Windows DS-Client 14.2.0.10 and DS-System 14.2.0.7 or later. • The “Deletion of files removed from source” retention rule can now be applied to MariaDB, Microsoft SQL Server (Classic), Oracle MySQL, and VMware vCenter Server backup sets. Users can now specify in DS-User if they want to delete backed-up data that was removed from the source for this backup set type when performing a selective delete. Requires Windows DS-Client 14.2.0.10, Linux or Mac DS-Client 14.2.0.7, and DS-User 14.2.0.7 or later. • Users can now use DS-User to backup and restore MariaDB databases using a Windows or Linux DS-Client. Requires Windows DS-Client 14.2.0.10 or Linux DS-Client 14.2.0.7, DS-User 14.2.0.7, DS-System 14.2.0.7, DS-Operator 14.2.0.7, DS-NOC 14.2.0.7, BLM Archiver 14.2.0.6, DS-Billing 14.2.0.4 or later.

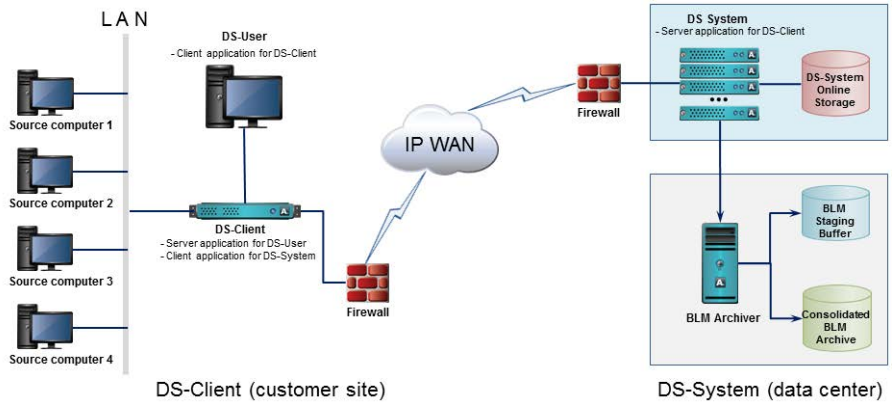
1.6	December 4, 2023	• When restoring a Microsoft Exchange Server (EWS) backup in DS-User, users can now select the “Latest generation of all data (except deleted data)” option to restore files that were deleted from the source but not removed from the online storage as of the last backup session. Requires DS-User 14.2.0.7 or later. • After performing an initial backup in DS-User, the Set Status column in the Initial Status window now indicates if the backup completed with errors. Requires DS-User 14.2.0.7 or later. • Eclipse Temurin OpenJDK 17 (LTS) runtime is now bundled and installed with the DS-Client software. Requires DS-Client 14.2.0.10 or later. • Updated third-party components used by DS-Client to address potential security vulnerabilities. Requires Windows DS-Client 14.2.0.10 and DS-User 14.2.0.7 or later.
1.7	June 2, 2025	• Improved performance when loading catalog files for large disk/tape media on DS-Clients with a PostgreSQL database. Users can now configure the PostgreSQLMediaLoadBatchSize advanced configuration parameter in DS-User to further tune the batch loading for restore operations from Disk/Tape. Requires Windows DS-Client 14.2.0.14 or later. • Improved performance when restoring a File system backup set using a Windows DS-Client, especially for Bare Metal Restore (BMR) scenarios. Requires Windows DS-Client 14.2.0.14 or later. • Improved performance when restoring a File System (Local, NAS, NFS, UNIX-SSH) backup with many folders and files using a Linux or Mac DS-Client. Requires Linux or Mac DS-Client 14.2.0.9 or later. • Improved the reporting of Microsoft 365 user counts to address discrepancies with Microsoft Entra. Requires Windows DS-Client 14.2.0.14 or later. • When performing a VMware vCenter Server backup using a Windows DS-Client, users can now select and restore individual disk (vmdk) files in DS-User. Requires Windows DS-Client 14.2.0.14 and DS-User 14.2.0.9 or later. • When performing Microsoft 365 backups, users are now deduplicated across multiple DS-Clients under the same customer account if the Exchange Online and SharePoint Online data associated with the same user is backed up using different DS-Clients. Requires Windows DS-Client 14.20.14 and DS-System 14.2.0.9 or later. • Updated the version of OpenSSL used by the DS-Client to address potential security vulnerabilities. Requires Windows DS-Client 14.20.14 or later. • Updated third-party components used by the DS-Client to address potential security vulnerabilities.Requires Windows DS-Client 14.20.14 or later.

1 Getting started

The DS-Client is responsible for defining the backups that determine what data is to be backed up from the source computers and for sending the backed up data to the DS-System for storage.

During the backup process, the DS-Client extracts, compresses, and encrypts the data. Only new or modified data is backed up, which accelerates the backup transmission time. Backup data is sent to a secure off-site data center that hosts the DS-System vault. Restore is performed on demand via the same DS-Client.

Ease of use comes from the agentless architecture, which allows you to install a DS-Client on only one LAN computer. As long as the DS-Client is on the same network as the source computers, you can back up and restore data as required.



NOTE: For information on how to install the DS-Client software, see the *Client Software Installation Guide*.

1.1 Connecting to a DS-Client

The DS-Client allows multiple simultaneous connections using the same or different authentication credentials. By default, access to the DS-Client is restricted to administrators or backup operators (Windows DS-Clients) and root users (Linux or Mac DS-Clients).

NOTE: An administrator can configure different roles to access a DS-Client. For more information, see Section 2.1.7, “Configuring the user and group settings”, on page 35.

To connect to a DS-Client:

1. Start the DS-User application.
2. From the list of DS-Clients on the left side of the main window, select the DS-Client to which you want to connect.
   - To switch between the computer name and IP address, right-click the list, and click **Sort by Name** or **Sort by IP**.
   - To rescan the network for available DS-Clients, click **Refresh**.

   Each DS-Client in the list is color coded as follows:

Color	Description
Blue	DS-Client running on the local machine with DS-User.
Black	Full-featured DS-Client (Windows, Linux, or Mac)
Green	Uninitialized DS-Client.
Light Blue	DS-Mobile Client (Windows)
Aqua	DS-Notebook Client (Mac)
Red	DS-Client service is not running.

Table 1 DS-Client color coding information

NOTE: If the DS-Client you want does not appear in the list, you can add it to the initialization settings. For more information, see Section 2.2.1, “Configuring the connection settings”, on page 60.

3. Under **Connection properties**, in the **Protocol** box, select the protocol you want to use for communication between the DS-User and the DS-Client service. The options are as follows:
   - **Encrypted** – All data between the DS-User and the DS-Client service will be encrypted with a random encryption key at every connection.
   - **Standard** – This option is only offered for backwards compatibility with old service/daemon versions that do not have this feature.

4. Under **Credentials**, type your user name and password. This must be a valid user account on the DS-Client computer.
5. In the **From** box, select the domain or server on which the credentials will be verified.
6. To save the credentials for the duration of the DS-User session, select the **Remember Credentials** check box.

NOTE: Exiting the DS-User application will clear these credentials.

---

7. To use your current credentials to automatically connect to the DS-Client, select the **Use current security context** check box.

NOTE: This option is only available when connecting to a Windows DS-Client.

---

8. Click **Connect**.

NOTE: If the DS-Client is unregistered, you must perform the initial configuration. See Section 1.2, “Performing the initial DS-Client configuration”, on page 17.

1.2 Performing the initial DS-Client configuration

The first time you connect to a DS-Client, you must perform the initial configuration required to connect to a DS-System.

To perform the initial DS-Client configuration:

1. Under **Customer Registration Info**, do the following:
   a) In the **Customer Name** box, type a descriptive name for the DS-Client. This is the name that appears in parentheses after the computer name in the list of available DS-Clients.
   b) In the **Account #** box, type the account number assigned by your service provider.
   c) In the **DS-Client #** box, type the client number assigned by your service provider.

NOTE: If you already registered the DS-Client with a service provider, you should have received a Customer Registration Information (CRI) file containing the required information. To select the file, click **Browse**.

---

2. Under **DS-System Info**, do the following:

a) In the **Address** box, type the IP address or DNS name of the DS-System to which the client will be connecting. Separate multiple IP addresses with a semi-colon.

b) To add an IP address, click **Add**.

c) To remove an IP address, select the IP address, and then click **Remove**.

3. Under **Private Key**, do the following:

   a) In the **Type** box, select the type of encryption you want to use. Stronger encryption requires longer keys.

   b) In the **Key** box, type the private encryption key that is to be used for all data that comes from your client.

   c) In the **Confirm** box, retype the private encryption key. You cannot change this key once it is set.

4. Under **Account Key**, do the following:

   a) In the **Type** box, select the type of encryption you want to use. Stronger encryption requires longer keys.

   b) In the **Key** box, type the account encryption key assigned by your service provider. Common backup data from all your clients will be encrypted with this same account key.

   c) In the **Confirm** box, retype the account encryption key. You cannot change this key once it is set.

   The account encryption key must be the same type and string for all the DS-Clients under the same customer account on the DS-System.

NOTE: Encryption keys are case sensitive and the character length depends on the type and level of encryption selected. DES requires 8 characters, AES-128 requires 16 characters, AES-192 requires 24 characters, and AES-256 requires 32 characters. If you type a shorter string, an auto-complete feature repeats the string until all the required characters are filled. For example, “123” becomes “1231231231231231”.

---

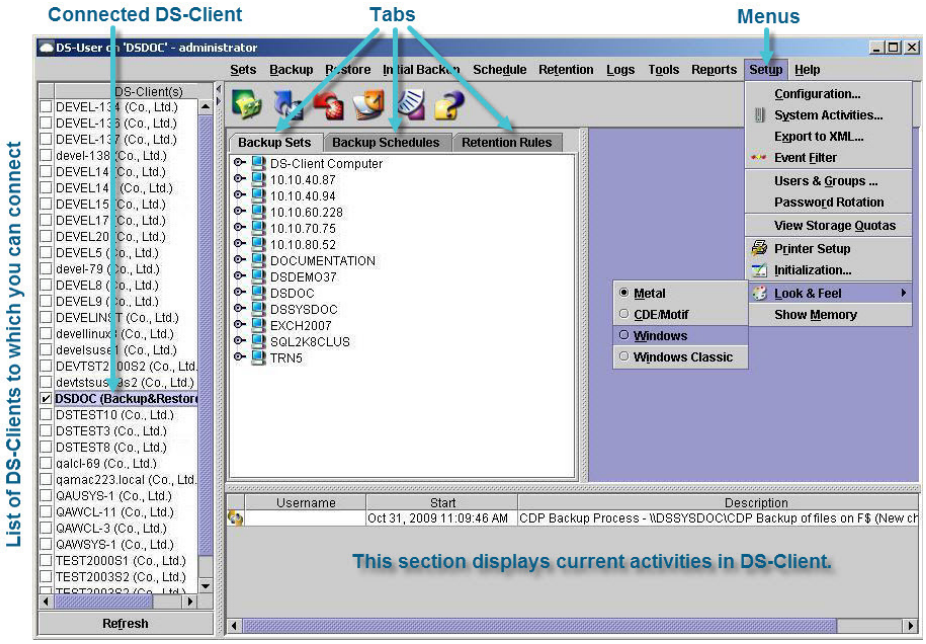
5. To forward the encryption keys to the DS-System the first time the client connects to the DS-System, select the **Allow encryption key forwarding to DS-System** check box. This allows your service provider to create a valid CRI file with the encrypted keys so they can recreate a working version of the client.

6. Under **User Info**, type the requested information about your organization.

7. Click **Save**. The DS-System verifies the encryption keys on every connection to ensure the integrity of both the private and account keys.

1.3 Working in the DS-User main window

After you have successfully connected to a DS-Client, the DS-User main window appears. From the main window, you can access all the functions required to manage a DS-Client.



- **Title bar –** Displays the name of the DS-Client to which you are connected.
- **Menu bar –** Allows you to perform various backup and restore tasks. Some items only appear if the corresponding tool is enabled.
- **Toolbar icons –** Provides quick access to the most commonly used features.

Icon	Function
	Creates a new backup.
	Performs an on-demand backup.
	Restores files.
	Opens the Schedule Calendar.
	Opens the Activity Log.
	Opens the online Help

Table 2 Toolbar icons

- **DS-Clients –** Displays a list of the available DS-Clients that you can connect to on the LAN. You can only connect to one DS-Client at a time.
- **Backup Set tab** – Displays a tree view of all the backups defined on the selected DS-Client. You can browse to select the required backup and right-click to display the options menu. The color of a backup indicates its status.
  - **Black** = Active
  - **Blue** = Local-only
  - **Gray** = Suspended
  - **Red** = Requires Synchronization
- **Backup Schedules tab** – Displays a tree view of all the backup schedules defined on the selected DS-Client. You can browse the tree to select the required schedule and right-click to display the options menu. You can reassign schedules to backups using the drag-and-drop functionality.
- **Retention Rules tab** – Displays a tree view of all the retention rules defined on the selected DS-Client. You can browse the tree to select the required retention rule and right-click to open the options menu. You can reassign retention rules to backups using the drag-and-drop functionality.
- **Monitor window –** Displays the active processes running on the DS-Client.

1.4 Starting or stopping the DS-Client service or daemon

You can start or stop the DS-Client service or daemon.

To start or stop a DS-Client service or daemon:

1. On the **Start** menu (Windows) or **Applications** menu (Linux), click **DS-Client Service Manager**.
2. In the **DS-Client Service Manager window**, click **Start** or **Stop**.

1.5 Viewing DS-Client information

You can view information about the DS-Client, including its version information, port configuration, and Java Runtime Environment (JRE) properties.

To view DS-Client information:

1. On the **Help** menu, click **About DS-User**.
2. To view detailed information about the DS-Client, including its version information, click **DS-Client Info**.
3. To view the ports used by the DS-Client to communicate with other components, click **Ports**.
4. To view information about the Java Runtime Environment (JRE) properties, click **JRE Properties**.
5. Click **Close**.

1.6 Disconnecting from a DS-Client

You can disconnect from a DS-Client at any time. This does not close the DS-User application and does not affect other DS-Client connections.

To disconnect from a DS-Client:

- In the list of DS-Clients, clear the check box beside the DS-Client from which you want to disconnect.

1.7 Exiting the DS-User application

You can exit the DS-User application at any time. This closes all connections to DS-Clients.

To exit DS-User application:

- On the **Sets** menu, click **Exit**.

2 Configuring the DS-Client

You can configure the DS-Client settings to meet your requirements.

2.1 Configuring the DS-Client settings

Most default configuration settings are defined during the initial configuration. However, you might want to edit some default configurations and settings.

2.1.1 Configuring the setup information

You can update some of the settings that you configured during the initial DS-Client configuration, re-register the DS-Client with the DS-System, enable the forwarding of encryption keys to the DS-System, forward encryption keys to the DS-System immediately, and request the deletion of forwarded encryption keys.

To configure the setup information:

1. On the **Setup** menu, click **Configuration**.
2. Click the **Setup** tab.
3. To modify a DS-Client configuration, click **Modify**. For more information, see Section 1.2, “Performing the initial DS-Client configuration”, on page 17.
4. To re-register the DS-Client with the DS-System, click **Register Now**. In the confirmation dialog box, click **Yes**. A confirmation message indicates if the registration was successful.

   NOTE: You must contact your service provider and ask the DS-System administrator to permit DS-Client registration. You only need to register again if you change the hardware or operating system of the DS-Client or if the DS-Client hardware registration is reset on the DS-System side.

5. To forward the encryption keys to the DS-System, select the **Enable Encryption keys forwarding to DS-System** check box. This allows your service provider to create a valid CRI file with the encrypted keys so they can recreate a working version of the client.

   NOTE: If your service provider enforces mandatory safeguarding, DS-Client is not be able to connect to DS-System until you enable this feature.

6. To forward the encryption keys immediately to the DS-System, click **Forward Now**.

7. To instruct the DS-System to delete the forwarded encryption keys from its database, click **Request Deletion**.
8. Click **OK**.

2.1.2 Configuring the default settings

You can configure the default settings that will apply to all new backups. You can still change the settings individually for each backup if required.

To configure the default settings:

1. On the **Setup** menu, click **Configuration**.
2. Click the **Defaults** tab.
3. Under **Generations setup**, do the following:
   a) In the **Maximum online generations** box, enter the maximum number of online generations of a backup that should be retained.
   b) In the **Default Retention Rule** box, select the default retention rule for new backups.

NOTE: For information on how to configure a retention rule, see Section 4.1, “Configuring a retention rule”, on page 98.

---

4. To back up the file permissions, under **Backup options**, select the **Backup permissions** check box.
5. Under **Open files**, do the following:
   a) In the **Default operation** box, specify how a backup should handle an open file during backup. The options are as follows:
      - **Try deny write** – Attempts to open the file in Deny write mode. If this fails because the file is already open, the file is placed in Allow write mode.
      - **Deny write** – Prevents any other process from writing to the file while the DS-Client has it open. The DS-Client does not back up the file if another process has already opened it for write. However, you can instruct the DS-Client to retry backing up the open file.
      - **Prevent write** – Attempts to open the file in Deny write mode. If this fails because the file is already open, the file is opened in Allow write mode and locked to prevent any other process from writing to the file. This ensures that the most recent version of the file is backed up.

- **Allow write** – Allows another process to read or write to the file without restrictions. Since other applications can write to the file while it is being backed up, this can affect file consistency.

NOTE: If the file is opened in another application, it will not be backed up unless the backup is using VSS. The Activity Log will display an error. To back up an open file, enable the VSS option for that particular backup.

b) In the **Retry times** box, enter the number of times that you want the DS-Client to attempt to back up the file.

c) In the **Retry interval** box, enter the interval, in seconds, between retries.

6. Under **Backup schedule**, select the default schedule for new backups. To create a new schedule, click **New**.

NOTE: For information on how to configure a schedule, see Section 3.1, “Configuring a schedule”, on page 90.

7. To configure the default notification settings for new backups, do the following:

a) Under **Notification**, click **Add/Modify**, and then do the following:

b) To send an email notification, select **E-Mail**. and then do the following:

1. To send the email notification to the DS-Client administrator, select **Administrator**.
2. To send an email to another recipient, select **Other**, and then specify the recipients email address.
3. To send detailed backup information, select the **Detailed notification** check box.
4. To include a detailed file-level backup log as an attachment, select the **Attach detail log** check box.
5. To send the email notification in HTML format, select the **Send E-Mail using HTML format** check box.

c) To send a pager notification, select **Pager**. The notification will be sent to the pager account configured for the DS-Client.

d) To send a broadcast notification, select **Broadcast**. Select the server containing the messenger service to which you want to send the message.

NOTE: Broadcast notifications to domains or workgroups are limited to 128 characters.

e) To send an event notification, elect **Event**. Select the server on which you want the notification to be recorded in the Event Log.

f) In the **Completion** box, specify under what conditions a notification will be sent, and click **OK**. The options are as follows:

- **All** – Notification will be sent under all conditions.
- **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
- **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.
- **Completed with errors** – Notification will be sent if an activity is completed with at least one error event.
- **Incomplete** – Notification will be sent if an activity is not completed successfully.

8. Click **Next**.

NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

---

9. Under **Data Compression**, select the default compression type that will be applied to new backups. The options are as follows:

- **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good option when the network is not the bottleneck.
- **ZLIB** – Produces better compression than LZOP, but will take more time. This is a good option when the bottleneck is the network.

10. Click **OK**.

2.1.3 Configuring the notification settings

DS-Client notifications are email reports or pager alerts that can be sent to the Administrator at the end of a backup session or on a regular basis during Admin processes.

If you are using MAPI with a Windows DS-Client, Microsoft Outlook is required and you must select a profile. If no profile is configured, email options will be hidden when creating new backups or reviewing backup properties. If you change the profile, you must restart the DS-Client service for the changes to take effect.

NOTE: Before configuring DS-Client to send notifications, you must create a mail profile. For more information, see your email server's documentation.

To configure the notification settings:

1. On the **Setup** menu, click **Configuration**.
2. Click the **Notification** tab.
3. Under **Outgoing E-mail Settings**, select **SMTP**.
4. Under **SMTP server settings**, do the following:
   a) Beside the **SNMP Server** box, click **[...]**, and then do the following:
      1. In the **SNMP Server** box, type the DNS name or IP address of the SMTP server the DS-Client will use.
      2. In the **Port** box, enter the port number. The default is 25.
      3. If the server requires authentication, select the **Server requires authentication** check box. Specify if you are using the SSL (Secure Sockets Layer) or TLS (Transport Level Security) protocol for communication, and then configure the settings accordingly.
      4. Click **OK**.

      NOTE: The DS-Client uses its existing network connection when sending SMTP notifications.

      ---

   b) In the **From (E-Mail Address)** box, type the email address that you want to appear in the From field of the email notification.
   c) In the **From (Display Name)** box, type the name that you want to appear in the From field of the email notification.
5. Under **E-Mail notification subject**, do the following:

a) In the **Backup activity** box, type the text that you want to appear in the subject line of email notifications for backup activities.

You can enter text and combine it with a backup activity placeholder. When a notification is sent, the placeholder text is replaced with corresponding data from the DS-Client database. Placeholders are case-sensitive and must be entered between the {} brace characters. For example:

- {DSC_NAME}
- {DSC_NUMBER}
- {BACKUP_SET_NAME}
- {BACKUP_SET_OWNER}
- {BACKUP_SOURCE}
- {BACKUP_RUN_RESULT}
- {USER_NAME}
- {BACKUP_STATUS}

b) In the **Admin activity** box, type the text that you want to appear in the subject line of email notifications for daily and weekly admin activities.

You can enter text and combine it with a admin activity placeholder. When a notification is sent, the placeholder text is replaced with corresponding data from the DS-Client database. Placeholders are case-sensitive and must be entered between the {} brace characters. For example:

- {DSC_NAME}
- {DSC_NUMBER}
- {USER_NAME}
- {ADMIN_TYPE}

6. Under **Administrator setup**, do the following:

a) In the **Admin E-Mail** box, type the email address of the DS-Client administrator. To test the notification, click **Test**.

b) In the **Pager E-Mail** box, type the pager email address of the DS-Client administrator. To test the notification, click **Test**.

NOTE: Separate multiple email addresses with a comma (,) or semicolon (;).

---

7. Under **Daily / Weekly Admin setup**, do the following:

a) To send an email to the Admin email account containing a summary of the Admin and backup processes, select the **Send summary** check box.

b) To include the backup details with the summary, select the **Send backup details** check box.

c) To send the summary in HTML format, select the **Send E-Mail using HTML Format** check box.

8. Click **OK**.

2.1.4 Configuring the SNMP settings

You can configure DS-Client to send SNMP traps when a backup has completed successfully, completed with warnings, completed with errors, or is incomplete.

An SNMP trap will be sent once, immediately after each backup activity finishes. The DS-Client can also be configured to send a special trap as a heartbeat signal to determine if the monitored service is running normally.

NOTE: To receive SNMP traps sent by the DS-Client, you must load the MIB (Management Information Base) file called **asigra.mib** file with your SNMP software. This file describes how the objects are organized and can be found in the DS-Client installation directory. The **IANA** Private Enterprise Number is **15538**. For more information, see http://www.iana.org/assignments/enterprise-numbers.

To configure the SNMP settings:

1. On the **Setup** menu, click **Configuration**.
2. Click the **SNMP** tab.
3. In the **Community** box, type a community name, and then click **Add to list**.

NOTE: Communities are groups of hosts to which a server running the SNMP service belongs. The community name is placed in the SNMP packet when the trap is sent.

4. Under **Destination host list**, do one of the following:
   - To add a destination host to the community, click **Add**.
   - To modify a destination host, select the destination host, and then click **Edit**.

NOTE: To delete a destination host, select the destination host, and then click **Remove**.

5. Type a host name or IP address from your network, and then click **OK**.
6. Continue to add the required destination hosts to the community as required.
7. To send SNMP traps as heartbeats, select the **Send traps as heartbeats every** check box, and then specify the frequency at which traps should be sent.
8. Click **OK**.

2.1.5 Configuring the parameter settings

You can configure administrative processes and options for your DS-Client.

To configure the parameter settings:

1. On the **Setup** menu, click **Configuration**.
2. Click the **Parameters** tab.
3. Under **Admin Process,** do the following:
   a) To schedule the Daily Admin process, select the **Daily start** check box, and then enter the time of the day when you want the process to start.
   b) To schedule the Weekly Admin process, select the **Weekly start** check box, and then enter the time of the day when you want the process to start.

   NOTE: If you want the admin processes to be performed on demand only, clear the check boxes.

   c) If you have scheduled the Weekly Admin process, in the **Every** box, select the day of the week on which you want the Weekly Admin process to run.
   d) To reboot the DS-Client computer after an Admin process has completed, select the **Reboot after admin** check box.
   e) In the **CDP Strategy** box, specify how the DS-Client should handle backups with Continuous Data Protection (CDP) enabled when the Daily or Weekly Admin process is scheduled to run. The options are as follows:
      - **Skip** – Backup sets with CDP enabled will continue to run while the Admin process is in progress. However, DS-Client does not perform the System Admin process on these backups.
      - **Suspend** – Backup sets with CDP enabled will be suspended while the Admin process is in progress. However, DS-Client performs the System Admin process on these backups. The backups will restart after the Admin process is finished.
4. Under **Database options**, do the following:

a) In the **DS-Client database backup** box, select when you want to save the DS-Client database to the DS-System. The options are as follows:

- **with Daily Admin** – DS-Client database backup is performed as part of the Daily Admin process.
- **with Weekly Admin** – DS-Client database backup is performed as part of the Weekly Admin process.
- **None** – DS-Client database backup is not performed.

IMPORTANT: We recommend that you back up the DS-Client database on a regular basis.

---

b) In the **Keep DS-Client database dump file** box, select how you want to handle the DS-Client database dump file. The option are as follows:

- **Do not delete** – Dump file remains in the DS-Client buffer until it is overwritten.
- **Delete after successful backup** – Dump file is deleted after it has been successfully backed up to the DS-System.
- **Always delete** – Dump file is always deleted after the Daily Admin or Weekly Admin process.

c) In the **Keep DS-Client logs** box, select how long you want to retain the DS-Client logs on the DS-Client.

5. Under **Backup/Restore options**, do the following:

a) In the **Attempt to reconnect [...]** box, enter how many times the DS-Client automatically attempts to reconnect to the DS-System if the connection is lost during a backup or restore process.

b) In the **at [...] minute intervals** box, enter the interval, in minutes, between reconnection attempts. The default is 5.

c) To skip running a pre-scan on all scheduled backups to speed up the backup process, select the **Skip pre-scan for scheduled backups** check box.

6. In the **DS-Client Buffer** box, specify the local disk location that the DS-Client uses to save buffer dumps for backups configured with the **Use Buffer** option. Windows DS-Client also saves its own database dumps from the Daily Admin and Weekly Admin processes in this location.

IMPORTANT: The DS-Client database server must be able to dump to this location. This is an important consideration if you are using a remote database. For more information, see Section 5.2.5, “Database backup policies”, on page 112.

---

7. In the **Local Storage Path** box, specify the path that will be used for backups configured to use the following features that require a local storage path.

   - **Self-contained backups –** If you enter a path, you will be able to select this type of backup. For more information, see Section 5.1.2, “Self-contained backups”, on page 106.
   - **Local-only backups –** Your service provider must enable the Local Storage tool and Local-only Capacity tool and assign a maximum storage amount for the DS-Client. For more information, see Section 5.1.4, “Instant recovery backups”, on page 107.
   - **Instant recovery backups –** Your service provider must enable the Local Storage Tool and the Local-only Capacity Tool, and assign a maximum Local-only capacity for the DS-Client. If you enter a path, you will be able to select this type of backup. (See Section 5.1.4, “Instant recovery backups”, on page 107.)

   IMPORTANT: Ensure there is sufficient disk space available to manage the additional data stored in the DS-Client database and that the DS-Client service account can access the local storage path. If you specify a network location, the DS-Client service account must have network access privileges. By default, the Local System Account cannot access a network location.

8. If you are using a Linux DS-Client, under **Instant Recovery Storage Options**, specify the location where the instant recovery backup data will be saved.

   NOTE: You must configure a ZFS storage volume located on a remote FreeBSD device that is accessible by the DS-Client. Each DS-Client must be able to mount to a unique ZFS storage volume via NFS. You must install an NFS client on the DS-Client machine.

   a) In the **ZFS mount path** box, specify the path on the remote machine where the ZFS storage volume is mounted.

   b) In the **IP/DNS** box, type the IP address or DNS name of the ZFS storage volume. Do not use the local loopback (127.0.0.1).

   c) In the **User name** box, type the user name for the DS-Client to access the ZFS storage volume.

   d) In the **Password** box, type the password for the user credentials.

   e) Beside the **ZFS volume name** box, click **[...]** to choose the ZFS storage volume. This is the location where instant recovery backup data will be stored.

   NOTE: You must update the `/etc/rc.conf` file on the remote FreeBSD device with the following line: `mountd_flags="-rS"`

9. Click **OK**.

2.1.6 Configuring the DS-System connection settings

You can configure the DS-System connection settings. Your service provider will supply you with the information you must use.

To configure the DS-System connection settings:

1. On the **Setup** menu, click **Configuration**.
2. Click the **Connections** tab.
3. To configure a DS-System connection, do one of the following:
   - To add a connection, click **Add**.
   - To modify a connection, select the connection, and then click **Modify**.

   NOTE: To delete a connection, select the connection, and then click **Delete**.

4. Under **DS-System connection entry**, do the following:
   a) To add or modify a DS-System connection entry, click **Add** or **Modify**, and then specify the host or IP address of the DS-System.
   b) To assign a DS-System as the primary connection, select the **Primary** check box.

      NOTE: There can only be one primary connection. All other connection entries are considered alternate connection to be used only if the primary connection fails. The DS-Client returns to the primary connection based on the **RetryPrimary** advanced configuration parameter.

   c) To enter a command to run on the DS-Client computer before it connects to the DS-System, select the **Pre-Command** check box, and then enter the command. To test the command, click **Test**.
   d) To enter a command to run on the DS-Client computer after it disconnects from the DS-System, select the **Post-Command** check box, and then enter the command. To test the command, click **Test**.
   e) To consider a connection failed if an exit code is returned from the pre-command, select the **Consider connection failed if pre-exitcode** check box, and then enter the exit code.
   f) To run the specified pre or post commands for each activity that requires a connection to the DS-System, select the **Consider Pre/Post individually for each connection** check box.

g) In the **Delay after executing pre-command** box, enter the amount of time, in seconds, that you want to delay after executing the pre-command before the DS-Client connects to the DS-System.

h) In the **Delay after executing post-command** box, enter the amount of time, in seconds, that you want to delay after executing the post-command activities will run on the DS-Client.

i) Click **OK**.

5. To test a connection, select the connection, and then click **Test Connection**.

6. To configure the DS-Client to use a proxy server to access the Internet when connecting to Management Console, DS-NOC or a cloud site, do the following:

   a) Under **Internet Connection Setup**, click **Proxy Server**.

   b) Under **Proxy Server Settings**, select one of the following options:

   - **No proxy** – DS-Client automatically selects the protocol (HTTP or HTTPS) based on the address provided by the DS-System. IMAP is used for email server backups.
   - **Auto-detect proxy settings for this network** – DS-Client automatically detects the proxy server.
   - **Manual proxy configuration** – Manually enter the proxy server address for the HTTP, HTTPS, and IMAP protocols. To use a single proxy server for all protocols, select the **Use the same proxy server for all protocols** check box. The standard ports used are 80 for HTTP, 443 for HTTPS, and 143 for IMAP.
   - **Automatic proxy configuration URL** – Type a URL to a PAC (Proxy Auto Configure) file that is accessible to the DS-Client. The DS-Client obtains the proxy server address and port number from this file. Type the full URL starting with "`http://`".

   NOTE: With the exception of the No proxy option, if the DS-Client fails to find the correct proxy server, it will try to connect directly. The HTTP or HTTPS protocol will be automatically selected based on the address provided by the DS-System. For cloud site connections, the protocol (HTTP/HTTPS/IMAP) will be selected automatically as required.

   c) If the proxy server requires authentication, select the **Server requires authentication** check box, and then type the user name and password.

   d) Click **OK**.

7. Click **OK**.

2.1.7 Configuring the user and group settings

Each user you configure must share an identical name with the equivalent user account created on the DS-Client machine. You do not need to create user groups because groups are automatically generated based on existing user groups on the DS-Client machine. Each time a user attempts to log on to the DS-Client, the account will be checked against the roles. When more than one role applies, the role with the greater rights will apply.

NOTE: Standalone users should connect to their DS-Client as local administrators or as a user with administrator privileges.

The right to perform a task is different from the permission to access a particular backup. For users with the Regular User Role, even if you have the right to perform a task, you must also have permission to the backup in question. By default, only the creator or owner and administrators have permissions to a backup. For more information on individual backup permissions, see Section 6.12, “Changing the permissions of a backup”, on page 551.

The following table describes the DS-Client roles that can be assigned to users and groups. Each type of user has rights to perform particular tasks.

Role	Description
Regular User	Regular users can perform the following tasks: • Create File System backups • Create special backups • View the list of backups (for which they have permission) • Modify backups • Backup a set on demand • Restore backups • Restore from a Disc/Tape • Request BLM and Restore from a BLM Restorable Image • Remove backups • Selective Delete of backed up files from Online storage • Enforce Retention on a backup • Suspend/Activate backups • Synchronize backups • Clone backups • Migrate backups • View and print reports • View Quotas • View Activity Log • View Event Log (from Activity Log or Current Activity Monitor only) • Convert Local-only backups to online backups • View the DS-Client Info (Help Menu)

Table 1 DS-Client roles

Role	Description
Backup Operator	In addition to Regular User tasks, Backup Operators can: • View the list of all backups • Perform a Demand Backup on all backups • Specify Notification options • Synchronize all backups • Create Initial backups • Perform a BLM Request for all backups • Create and modify Backup Schedules • View the Backup Groups Report • View the Load Summary • View the Storage Summary • Recover orphaned backups • Use the System Status utility • Send messages to connected users • Disconnect users from the DS-Client • Initiate Daily or Weekly Admin. Process runs on demand • Disable/Enable Scheduled Activities • Disable/Enable Demand Activities • View the Audit Trail • View the Event Log • View the DS-Client Configuration • Clean Local-only Trash • View DS-NOC Settings & set DS-NOC Proxy Server Settings **Note**: For Windows DS-Clients, the local Windows Backup Operators group is assigned to this role by default.
Administrator	In addition to Backup Operator tasks, Administrators can: • Get full access to all DS-User tools and features. • View information on all activities recorded in DS-Client logs. • Get full access to all backups • Request a Disc/Tape • Set and change user and group access rights to backups: • Set Maximum Online Amount for Users and/or Groups • View Users belonging to a Group and/or Groups • Change backup owner • Re-register the DS-Client with the DS-System • Repair the DS-Client Database (disaster recovery) • Shut Down the DS-Client computer • Change DS-Client default configurations • Add / remove permissions for a backup for users and groups • Perform Validation • Migrate the backup share/path to a different share/path • Use LAN Discovery • Use LAN Unprotected Resource Discovery • Perform DS-Client and encryption setup • Perform notification setup • Configure connections to the DS-System • Assign roles • Configure bandwidth throttle • Perform system activities administration • Export to XML • Use event filter **Note**: For Windows DS-Clients, the local Windows Administrators group is assigned to this role by default. For Linux/Mac DS-Clients, this role includes the local root user. You cannot remove this user from the Administrator role.

Table 1 DS-Client roles

To configure the user and group settings:

1. On the **Setup** menu, click **Configuration**.
2. Click the **Roles** tab.
3. To configure a new user or group, do one of the following:
   - To add a user or group, click **Add**.
   - To modify a user or group, select the user or group, and then click **Modify**.

   NOTE: To delete a user or group, select the user or group, and then click **Delete**.

4. In the **New User/Group Role** dialog box, do the following:
   a) In the **User Name** or **Group Name** box, type a name for the user or group.
   b) In the **From** box, select the computer or domain from which the user or group will be authenticated.
   c) In the **DS-Client Role** box, select the role for the user or group.
   d) Click **OK**.
5. Click **OK**.

NOTE: A user is not displayed until the user has logged on to the DS-Client at least once. A user group is not displayed until at least one user in the group has logged on to the DS-Client at least once.

2.1.8 Configuring the advanced settings

By default, the DS-Client is optimized for maximum performance. However, for users who have expert knowledge in managing their backup data, advanced parameters are available for further performance improvement. The parameters available depend on the type of DS-Client (Windows, Linux, or Mac).

When using a Windows Grid DS-Client, some parameters can be applied to an individual leaf node or globally to all the leaf nodes in the Grid DS-Client. All Windows DS-Client parameters are applied globally unless otherwise specified.

IMPORTANT: The default settings are sufficient to run any DS-Client. If you change a parameter, the DS-Client's performance will be affected. Do not attempt to change these settings unless you have a specific requirement and have confirmed this with your service provider. Depending on the parameter modified, you might need to restart the DS-Client service for the changes to take effect.

To configure the advanced settings:

1. On the **Setup** menu, click **Configuration**.
2. Click the **Advanced** tab.
3. In the **Category** box, select the category containing the advanced parameter you want to configure.
4. In the **Parameter** box, select the advanced parameter you want to configure.
5. In the **Value** box, enter a value for the parameter, and then click **OK**.

2.1.8.1 Admin parameters (Windows)

Parameter	Description
AdminNoSyncInterval	Interval (in weeks) the Weekly Admin process should not synchronize backups with only internal inconsistencies. • Default: 0 • Range: 0-12
AdminSkipSync	Skips the synchronization of backups during the Weekly Admin process if no database inconsistencies are detected. • Yes = On (Default) • No = Off
AdminSyncOrder	Order in which the backups will be synchronized during the Weekly Admin process. • Smaller sets first • Bigger sets first (Default) • No specific order enforced
AdminThreads	Maximum number of synchronization threads during the Weekly Admin process. • Default: 1 • Range: 1 to 8
DSCDBDumpPath	Dump path for the DS-Client database during administrative activities (Daily Admin / Weekly Admin). This path can be local or a UNC path. UNC is recommended for Grid DS-Clients.

2.1.8.2 Admin parameters (Linux or Mac)

Parameter	Description
AutoSync Order	Order in which backups will be synchronized during the Weekly Admin process based on estimated synchronization time. • small backups first • synchronize according to backup ID • big backups first - DEFAULT (Default)
Max AutoSync Number	Maximum number of synchronization activities that can run simultaneously during a scheduled Weekly Admin process. • Default: 1 • Range: 1-8
Skip WeeklyAdmin Sync	Skips the synchronization of backups during the scheduled Weekly Admin process if no database inconsistencies are detected: • Yes = On (Default) • No = Off
System Port	TCP/IP port the DS-Client uses to connect to DS-System. You can configure multiple ports by separating entries with a space, comma, semi-colon or pipe (|). • Default: 4401 • Range: 1-65535 Note: You should not change this setting unless instructed to by your service provider.

2.1.8.3 API connectivity parameters (Linux or Mac)

Parameter	Description
API Key File	SSL certificate/key file used for the API server. This should be in PEM format. • Default: /opt/CloudBackup/DS-Client/etc/api.pem
API Key Password	Password for the SSL certificate/key file specified in the **API Key File** parameter.
API Listen IP	IP address the DS-Client uses to listen for API connections. Use `0.0.0.0` to listen on all interfaces.
API Log File	File where the API server writes log messages and events. You can use any valid file name.
API Log Level	Level of logging to write to the API server log file. • warning (Default) • debug • info • error • fatal
API Port	Port on which DS-Client listens for API connections. • Default: 4411

2.1.8.4 Communication parameters (Windows)

Parameter	Description
CommunicationMethodDSS	Low-level communication method between DS-Client and DS-System. • 2 = Network packets encrypted on top of existing data encryption. Slowest method. (Default) • 1 = Same as method 0 with a different implementation for troubleshooting purposes only. • 0 = Network packets not encrypted. Fastest method.
CommunicationMethodMLR	Low-level communication method between DS-Client and DS-MLR / DS-Recovery Tools. • 2 = Network packets encrypted on top of existing data encryption. Slowest method. (Default) • 1 = Same as method 0 with a different implementation for troubleshooting purposes only. • 0 = Network packets not encrypted. Fastest method.
DSSystemAlternatePort	Alternate port to connect to DS-System if the DS-Client fails to connect on the default port (4401). • Default: 0 Note: A value of 0 means there is no alternate port.
HessianAPIListenIP	IP address the DS-Client uses to listen for Hessian API connections. Use `0.0.0.0` to listen on all interfaces. **Note:** This parameter requires the DS-Client to restart before taking effect.
HessianAPIListenPort	Port on which DS-Client listens for Hessian API connections. • Default: 4411 **Note:** This parameter requires the DS-Client to restart before taking effect.
HessianAPILogFile	File where the Hessian API server writes log messages and events. You can use any valid file name. **Note:** This parameter requires the DS-Client to restart before taking effect.
HessianApiLogLevel	Level of logging to write to the Hessian API server log file. • warning (Default) • debug • info • error • fatal **Note:** This parameter requires the DS-Client to restart before taking effect.
HessianApiSSLFile	SSL certificate/key file to use for the Hessian API server. This should be in PEM format. • Default: C:\Program Files\CloudBackup\DS-Client\api.pem **Note:** This parameter requires the DS-Client to restart before taking effect.
HessianApiSSLPassword	Password for the SSL certificate/key file.specified in the **HessianApiSSLFile** parameter. **Note:** This parameter requires the DS-Client to restart before taking effect.
LaptopCheckInterval	Interval at which DS-Client checks the network connection for schedules configured with the **DS-Client on portable computer (verify network connection)** option.
MaxQueuedMessages	Maximum number of queued messages during communication with DS-System. • Default: 128 • Range: 1-2048

Parameter	Description
MaxSendSize	Maximum TCP/IP socket block size to send at one time. Larger values can be used when communication over a fast connection is not performing as expected. • Default: 1500 • Range: 0-104,857,600 **Note**: Do not specify a value smaller than the default of 1500 unless for specific investigations as this can significantly affect performance.
MinApiMsgTimeout	Minimum (in minutes) timeout period for API messages. Increase this parameter if you encounter a large amount of “Timeout on receive message” errors. • Default: 10 • Range: 10-14400
RetryPrimary	Number of hours that must pass before retrying the primary DS-System connection after switching to a secondary connection. A value of -1 means “never retry”, and a value of 0 means “retry immediately”. • Default: 24 • Range: -1 to 240
TcpSocketBuffer	Internal socket buffer size (in bytes). This value is used if it is larger than the default. • Default: 34752 **Note:** Parameter can be applied globally or to individual nodes for Grid DS-Clients.
VSSKeepAliveTimeout	Timeout period (in seconds) for DS-Client to receive a response for a VSS (Volume Shadow Copy) operation. The VSS operation fails after the timeout period. • Default: 300 • Range: 60 to 3600

2.1.8.5 Installation parameters (Windows)

Parameter	Description
DS-UserAutoUpgrade	Specifies the DS-User auto-upgrade package the DS-Client downloads from DS-System (if they are available). • Disabled: DS-User auto-upgrade packages are not automatically downloaded from the DS-System. • Cross-PlatformDS-UserAutoUpgrade: DS-Client downloads all DS-User auto-upgrade packages that exist on the DS-System during Daily Admin or Weekly Admin. • CompatibleDS-User AutoUpgrade: DS-Client downloads only the DS-User upgrade packages that are compatible with the DS-Client operating system.

SystemFiles	A list of file names that Windows DS-Client skips from backup. It is an alphanumeric text string of file names, each separated by **\;**. The end of the string is indicated by a second **\;** as in the following example of the default list:
	`system.da0\;user.da0\;pagefile.sys\;win386.swp\;backout.tts\;btrieve.trn\;net$obj.sys\;net$val.sys\;net$prop.sys\;\;`
	
	Note: Each computer can have additional files configured to be skipped in the local registry key
	`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup`
	DS-Client skips these files when encountered during backup of regular shares or drives, but not for System State or Services Database items.

2.1.8.6 Miscellaneous parameters (Windows)

Parameter	Description
AllowAutoConfig	Allows DS-Client to apply auto-configuration from the `config-update.xml`. • Yes = On (Default) • No = Off
AllowAutoUpgrade	Allows auto-upgrade of DS-Client from DS-System when versions do not match. • Yes = On (Default) • No = Off **Note**: The automatic upgrade must be approved by the administrator using the DS-Operator.
AllowLocal	If set to **Yes**, allows execution of local commands during Pre/Post activities. You must be an administrator and have this option enabled to enable the Pre/Post activities. If this parameter is changed, it takes effect next time the DS-User connects to DS-Client Service. • No = Off (Default) • Yes = On
AllowScheduledBackupCheckSignature	Configures scheduled backups to use the **Verify signature for unchanged files** feature. By default, this option is turned off. If this parameter is set to **Yes**, scheduled backups will verify the signatures of unchanged files on the backup source. • No = Off (Default) • Yes = On **Note:** Turning this option on can have a significant impact on performance.
BrowseCheckSQLInstances	Detects Microsoft SQL Server instances when browsing domains and workgroups. • No = Off (Default) • Yes = On
DBQueryDefaultTimeout	Sets the default database query timeout (in seconds). A value of 0 means unlimited timeout. • Default: 500 • Range: 0 to 65535
DBQueryTimeout	Sets the longest database query timeout period (in hours). This only applies to time consuming database queries known by the DS-Client. If the database query takes longer than this value, it is aborted A value of 0 means unlimited timeout. • Default: 18 • Range: 0 to 19
DebugMessage	Sets the detail level of error messages reported in the DS-Client Event Log. • 0 = Standard level of error-message reporting. (Default) • 1 = Additional detailed log information is reported, such as database errors that are appended with the SQL statement. • 2 (or any higher number) = Same behavior as “1”, with additional debug information in a DS-Client debug log file (`dsclient.exe.dbg.log` located in the DS-Client installation directory). This option is meant for debug situations only. **Note:** For Grid DS-Clients, the parameter can be applied globally or to individual leaf nodes.

Parameter	Description
DefaultLocalTrashKeepDays	Default period (in days) to keep data in the Local-only trash. This applies to all the local-only paths. • Default: 7 • Range: 1-999
ExchangeOnlineBackupBatchResponseSizeLimit	Maximum response content size limit (in MB) for a single batch backup request for EWS or Microsoft Exchange Online backups when the ExchangeOnlineBackupBatchSize parameter is enabled and set to greater than 1. A value of 0 means there is no limit. • Default: 512 • Range: 2048
ExchangeOnlineBackupBatchSize	Maximum number of items that a batch should contain during backup of Microsoft 365 (Exchange Online) and Microsoft Exchange Server EWS backups. When set to 1, DS-Client downloads data from the source one item at a time. When set to 2 or greater, batch downloading is enabled and DS-Client downloads data one batch at a time from the source if DS-Client fills up a batch to the number of items specified by this parameter or DS-Client reaches time out duration specified in the parameter ExchangeOnlineBackupBatchTimeout. This can occur if there are not enough items remaining on the source to back up. • Default: 32 • Range: 1-40
ExchangeOnlineBackupBatchThreads	Number of batch backup request threads that are used when the ExchangeOnlineBackupBatchSize parameter is enabled and set to greater than 1. • Default: 2 • Range: 1-3
ExchangeOnlineBackupBatchTimeout	Wait time (in seconds) before DS-Client must download a batch from a source during the backup of Microsoft 365 (Exchange Online) and Microsoft Exchange Server EWS backups. • Default: 60 • Range: 0-3600
ExchangeOnlineBackupDataOptimization	Performs a one-time optimization task during the backup or retention process (whichever comes first) to clean up Microsoft Exchange Online backups. • No = Off (Default) • Yes = On
ExchangeOnlineBackupExtendedMetadata	Microsoft 365 (Exchange Online) backups will include the extended metadata (“To”, “From”, “Cc”, “Bcc”) to be able to search the item list on restore, delete, etc. If this is on, it will slow down the browse listing and the backup process. • No = Off (Default) • Yes = On
ExchangeOnlineEnableLogs	Activates logging for the Microsoft 365 (Exchange Online) backup. • No = Off (Default) • Yes = On
ExchangeOnlineExcludeGroupMailboxes	DS-Client verifies each mailbox on listing to prevent the display of Microsoft 365 (Exchange Online) group mailboxes. Group mailboxes are invalid backup items that will cause errors during backup if included in a Microsoft 365 (Exchange Online) backup. If on, the listing can be considerably slower because DS-Client must verify each mailbox before displaying filtered result. • No = Off (Default) • Yes = On

Parameter	Description
ExchangeOnlineFilterListingBySet	When on, improves the performance of incremental backups for Microsoft 365 (Exchange Online) and Microsoft Exchange Server EWS backups by using the last successful backup date and time as the backup filter instead of the last modified date and time of individual item. To back up items that have been created or modified before the last successful backup, turn this parameter off. • No = Off (Default) • Yes = On
ExchangeOnlineListingPageSize	Number of items per listing page for Microsoft 365 (Exchange Online) and Microsoft Exchange Server EWS backups. • Default: 1000 • Range: 100-1000
ExchangeOnlineOutlookConnectionTimeout	Timeout (in seconds) for the DS-Client connection attempt to Microsoft Outlook. This applies during a restore activity that archives Microsoft Exchange data to a PST file on the DS-Client local disk. It applies only to Microsoft 365 (Exchange Online) and Microsoft Exchange Server EWS backups. • Default: 120 • Range: 1-600
ForceBackupCheckSignature	Forces all applicable backups to check signature for unchanged files. The check will be performed once during the next backup of each backup. This setting applies only once. As soon as you select **Yes**, it will immediately take effect and the value is changed to **No** again. • No = Off (Default) • Yes = On
GAppsBackupExtendedMetadata	Backs up Google Workspace extended metadata for item list filtering. If yes, this can increase backup time significantly. • No = Off (Default) • Yes = On
GAppsBackupReadTimeout	Minimum timeout (in seconds) for backup read requests. • Default: 1 • Range: 0-4
GAppsPartialDownload	Downloads large Google Workspace drive files in smaller 1MB blocks to reduce memory usage on DS-Client. If On, the trade-off is 2-3 times slower performance than if this parameter off. • No = Off (Default) • Yes = On
GAppsRequestRetry	Number of times to retry if a Google Workspace item fails to backup or restore. • Default: 7 • Range: 0-9
GAppsRestoreCompleteTimeout	Minimum timeout for restore of any Google Workspace item. Increases automatically for files over 100MB. • Default: 300 (seconds) • Range: 0-3600

Parameter	Description
InstantRecoverySyncCheckingInterval	Amount of time (in minutes) DS-Client waits after performing an instant recovery before performing internal synchronization of data in the instant recovery folder. This is also the delay time before retrying if the instant recovery synchronization process fails or is interrupted. • Default: 30 • Range: 1-1440
InstantRecoverySyncRetryTimes	Number of times DS-Client attempts an instant recovery synchronization based on the InstantRecoverySyncCheckingInterval parameter. • Default: 10 • Range: 0-1000
LocalDriveAllowed	Configures the Local Drive Filter Flag for backup, which controls the drives available for backup (applicable only to File system & Permissions only). The decimal value is converted to binary to determine if a drive is allowed (1 means allowed, 0 means disabled). For example, to allow selection of only drives 'C' and 'E', use the value '20'. `. . . . . 2 0` [decimal value] `. . . 1 0 1 0 0` [binary] `. . . F E D C B A` [drive letter map] The binary representation of 20 matches bit0 for 'A:' disabled, bit1 for 'B:' disabled, bit2 on - 'C:' allowed, etc. • Default: -1 (allows all available local drives) **Note:** For Grid DS-Client, this parameter has no effect.
LogArchivePath	Path where detailed logs of DS-Client activities are stored as text files. Each backup has its own numbered sub-folder. Any path where the DS-Client can write data is valid. • Default: `<DS-Client installation folder>\asigra_archivlog` **Note:** For Grid DS-Clients, enter a UNC path that is accessible from all nodes of the Grid to ensure all detailed logs are located in a common accessible location.
MaxErrors	Sets the default "Stop on errors" value that appears when you create a new backup. • Default: 0 (no limit) • Range: 0 to 9999
MaxNonFullDumps	Maximum number of times a full dump of the database can be skipped in favor of a differential or incremental dump. Once this number is reached, the next backup forces a full dump of the database. • Default: 120 • Range: 2 to 1000
MCRemoteManagement	Allows the DS-Client to be remotely managed from the Management Console without opening a port in the firewall on the DS-Client machine. • Enabled (Default) • Disabled
Multi-Tenant	Enables the multitenant feature. • No = Off (Default) • Yes = On

Parameter	Description
Office365RequestRetry	Maximum number of retries when backing up or restoring Microsoft 365 data. • Default: 9 • Range: 0-20
Office365RequestTimeout	API request timeout duration (in seconds) for Microsoft 365 backups. • Default: 600 • Range: 0-3,600
PluginLogKeepDays	Number of days to keep the log files for Google Workspace, Microsoft 365, and Salesforce backups. • Default: 7 • Range: 1-9999
ReadOnlyUpgradeInterval	Interval (in minutes) at which DS-Client checks for an upgrade package from DS-System if it is running in Read-Only mode (no backup or restore allowed). • Default: 5 • Range: 1-60
RemoteExecutionTimeout	Timeout period (in minutes) for Remote Command Execution during Pre/Post activities. • Default: 60 • Range: 1 to 1440
ResetInvalidLSRootPath	Specifies if the configured local storage path should be reset (Yes) or retained (No) if DS-Client detects the configured local storage path is invalid or is temporarily unavailable. • Yes = Reset (Default) • No = Retained
RestoreTargetProvision	Path where the DS-Client can access the integration DLL file for automatic restore target provisioning. • Default: None **Note:** This parameter requires the DS-Client to restart before taking effect.
ScheduleMiss	Number of hours after the start time of a missed schedule that DS-Client continues to attempt to trigger it. For example, if set to 6 and a schedule from 12:00 PM to 20:00 PM is missed, the schedule will be triggered as long as it is within 6 hours of the scheduled start time and end time. • Default: 6 • Range: 1 to 16
SecurityDll	Path to a third-party security DLL to secure the communication. • Default: None **Note:** For Grid DS-Clients, this parameter can be applied globally or to individual leaf nodes.
SharePointOnlineBackupBatchSize	Maximum number of items a batch should contain during backup of Microsoft 365 (SharePoint Online) backups. When set to 1, DS-Client downloads data from the source one item at a time. When set to 2 or greater, DS-Client downloads data one batch at a time from the source if DS-Client fills up a batch to the number of items specified or DS-Client times out of the duration specified in the parameter **SharePointOnlineBackupBatchTimeout**. This can occur when the remaining number of items to be backed up on the source does not exceed the number specified in this parameter. • Default: 1 • Range: 1 to 10

Parameter	Description
SharePointOnlineBackupBatchTimeout	Timeout (in minutes) when batch downloading from a source during Microsoft 365 (SharePoint Online) backup. • Default: 720 • Range: 1 to 1440
SharePointOnlineLargeFileRestoreThreshold	Configures the chunk size (in MB) for Microsoft 365 (SharePoint Online) backups. Files smaller than this value are uploaded whole. • Default: 8 • Range: 1-2000
ShowAdvancedDataDedupOptions	Displays advanced options that can be used to restore data deduplication links as links, skip data deduplication links, or restore the last non-link when performing a restore of a File system backup. • No = Off (Default) • Yes = On
ShowPOSIX	Displays the **Backup as POSIX** check box for File System & Permissions Only backups. You can only select this option when creating a backup. • No = Off (Default) • Yes = On
SQLKeepDumpFile	Retains Microsoft SQL Server backup database dumps in the dump location after backup. This only applies to the classic Microsoft SQL Server backup. • No = Off (Default) — Dump is deleted after backup has finished. • Yes = On — Dump is kept in the dump location and is overwritten during the next backup. Note the storage implications, since this affects all Microsoft SQL Server backups created on the DS-Client.
SQLServerVDITimeout	Specifies the maximum wait time (in seconds) for a request to complete when backing up or restoring a Microsoft SQL Server backup using a Virtual Device Interface (VDI). • Default: 600 • Range: 60-86400
StopOnRetrieveLSNFailed	For Microsoft SQL Server (VSS-aware) backups. Stops a differential backup if it failed to retrieve the LSN (Log Sequence Number) information of the previous full backup. • Yes = On (Default) • No = Off
VMReplicationOpenListingTimeOut	Timeout (in seconds) for listing the VMware vCenter Server destination folders when creating a VM replication set. • Default: 300 • Range: 0-3600
VMRExternalIP	Specifies an external IP address to use to communicate with replication services on machines outside the network domain. • Default: None — Uses the internal IP address to communicate with replication services on machines on the same network domain.
VMRServiceStart	Start the VM Replication Service when DS-Client starts. • Yes = On (Default) — Allows you to create VM replication sets and run replication as long as DS-Client has sufficient VM Replication Capacity. • No = Off — The category DS-Client replication sets is hidden in the New Backup Set Wizard, and existing replication sets are inaccessible.

Parameter	Description
VMRSourcePort	Allows you to specify the port used by a DS-Client for VM replication processes. Ensure this value matches the network configuration for the DS-Client. This is equivalent to the source DS-Client port number in DS-Operator. Changes made to this value through either DS-User or DS-Operator are synchronized and will be shown in both interfaces. • Default: 8090 **Note:** This parameter requires the DS-Client to restart before taking effect.
VMwareVADPBackupValidateSignature	Forces all VMware vCenter Server backups that have Changed Block Tracking (CBT) enabled to validate the disk signature of a protected virtual machine after a specified number of backups. The interval count starts from the first backup after the setting is enabled. If a disk signature mismatch is detected, a master generation is sent to the DS-System for the affected virtual disk (vmdk). Verification consumes more system resources and increases the backup time, especially if the signature verification fails and requires backup of a new master. • -1 = Disables disk signature validation for all affected backups. • 0 (Default) = Uses the disk signature validation setting configured for each backup. • 1 = Validates the disk signature after every backup for all affected backups. • 2 to 100 = Validates the disk signature after the specified number of backups for all affected backups. **Note:** The disk signature validation setting will be reset to 0 each time the setting is applied to all affected backups.
VMwareVADPBackupValidateSignatureTime	Forces all VMware vCenter Server backups that have Changed Block Tracking (CBT) enabled to validate the disk signature of a protected virtual machine on specified days. If a disk signature mismatch is detected, a master generation is sent to the DS-System for the affected virtual disk (vmdk). Verification consumes more system resources and increases the backup time, especially if the signature verification fails and requires backup of a new master. • 0 (Default) = Disk signature validation is not performed on weekday. • 1 = Validates the disk signature on a Sunday. • 2 = Validates the disk signature on a Monday. • 4 = Validates the disk signature on a Tuesday. • 8 = Validates the disk signature on a Wednesday. • 16 = Validates the disk signature on a Thursday. • 32 = Validates the disk signature on a Friday. • 64 = Validates the disk signature on a Saturday. **Note:** To perform disk signature validation on multiple days, add the values together. For example, to validate the disk signature on Sunday (1), Tuesday (4), and Friday (32), specify 37.
VMwareVADPTransportMode	Applies only to VMware vCenter Server backups. Transport mode that DS-Client requests from the VMware libraries when initializing a connection for data transfer to or from a data center. • Empty (Default) — Library automatically chooses the transport mode based on VMware priorities among the available transport modes. • nbd — Network block device transport mode. • nbdssl — Network block device SSL transport mode. • san — SAN transport mode. • hotadd — HotAdd transport mode. For more information about the transport modes, see Section 5.24, “VMware vCenter Server backups (Windows or Linux)”, on page 509.

Parameter	Description
VSSContinueIfSnapshotCreatedWithWriterErrors	Continues a VSS-aware backup even if there are VSS writer errors, as long as the snapshot is successful. This only occurs after attempting all configured retries (VSSSnapshotRetries). • Yes = On (Default) • No = Off
VSSFreeDiskSpace	Performs a VSS validation check to ensure there is enough free disk space prior to performing a File system or VSS-aware backup using the Volume Shadow Copy Service (VSS). If the free disk space is less than the configured percentage value, VSS validation will fail. • Default: 0 • Range: 0-100 **Note**: A value of 0 means the free disk space check is skipped.
VSSSnapshotRetries	Number of times DS-Client attempts to create an 'error-free' snapshot during a VSS-aware backup. • Default: 3 • Range: 0-999, (0 means backup fails if snapshot encounters VSS writer errors)
VSSSnapshotRetryInterval	The retry interval (in minutes) for VSS snapshot retries (VSSSnapshotRetries). • Default: 5 • Range: 1-99
VSSValidationCheck	Performs a VSS validation check prior to performing a File system or VSS-aware backup using the Volume Shadow Copy Service (VSS). • Yes = On • No = Off (Default)
VSSWaitSnapshotTimeout	Timeout (in seconds) to wait for VSS snapshot creation. A longer period can prevent backup failures if different backups need to perform VSS backups of a common volume at nearly the same time. Only one VSS snapshot can be performed on a volume at a time. Since snapshots are fairly fast, a timeout of 5-15 minutes should ensure two different backups of the same volume can be successfully completed, even if they overlap. • Default: 60 • Range: 1-3600
WaitConfirmation	Time (in seconds) that DS-Client waits for confirmation from DS-System if stopping a backup. • Default: 60 • Range: 0 to 3600

2.1.8.7 Miscellaneous parameters (Linux or Mac)

Parameter	Description
AllowAutoConfig	Allows DS-Client to apply auto-configuration from the file `config-update.xml`. • Yes = On (Default) • No = Off
Auto Upgrade	Allows auto-upgrade of DS-Client from DS-System when the versions do not match. • Yes = On (Default) • No = Off **Note**: The automatic upgrade must be approved by the administrator using the DS-Operator.
Config Keep Days	Number of days to retain old copies of the DS-Client configuration file. • Default: 30 • Range: 1-99
DB2 Client Library Directory	Specifies the DB2 client library directory on the DS-Client machine. Ensure that the dynamic library <`libdb2.so.1`> resides in this directory. **Note:** This parameter requires the DS-Client to restart before taking effect.
DefaultLocalTrashKeepDays	Number of days to keep data in the Local-only trash. This applies to all Local-only paths defined for the DS-Client. • Default: 7 • Range: 1-999
DS-UserAutoUpgrade	Specifies which DS-User auto-upgrade package DS-Client downloads from DS-System if are available. • Default: **Compatible-Platform DS-User Auto-Upgrade**: DS-Client only downloads the DS-User upgrade packages which are compatible with the operating system of the DS-Client. • **Disabled**: DS-User auto-upgrade packages will not be automatically downloaded from the DS-System. • **Cross-Platform DS-User Auto-Upgrade**: DS-Client downloads all DS-User auto-upgrade packages that exist on the DS-System to the DS-Client directory during Daily Admin or Weekly Admin.
LogArchivePath	Path where detailed logs of DS-Client activities are stored as text files. Each backup has its own numbered sub-folder. Any path where the DS-Client can write data is valid. • Default: `<DS-Client installation folder>/asigra_archivelog`
MCRemoteManagement	Allows the DS-Client to be remotely managed from the Management Console without opening a port in the firewall on the DS-Client machine. • Enabled (Default) • Disabled
Multi-Tenant	Enables the multitenant feature. • No = Off (Default) • Yes = On
ReadOnlyUpgradeInterval	Interval (in minutes) at which DS-Client checks for an upgrade package from DS-System if it is running in Read-Only mode (no backup or restore allowed). • Default: 5 • Range: 1-32000
ScheduleMiss	Number of hours after the schedule start time that a missed schedule will still be triggered by the DS-Client. For example, if the value of this parameter is set to 6 and a schedule from 12:00 PM to 20:00 PM is missed, the schedule will still be triggered as long as it is within 6 hours of the scheduled start time and end time. • Default: 6 • Range: 1 to 16

Parameter	Description
Skip Compress	Skips compression on the following types of compressed files: lzop, zip, standard linux compression, gzip, bzip2, scocompress, bzip, jpeg, jfif, png, and gif. • Yes = On (Default) • No = Off **Note:** This parameter requires the DS-Client to restart before taking effect.
VMware Log Filter	Specifies a filter in Perl regular expression format. A regex search operation is performed and only matching lines are printed to the `dsclient.out` log file. This filter does not apply to the `vmlibexe.out` file. Each regex is a search 'for' that string, with all occurrences printed to the log file. • Default: . (dot, meaning log all)
VMware Log Level	Varies the amount and type of logging information inside the following log files: • `dsclient.out` — Contains the VMware related log messages generated from the DS-Client. • `vmlibexec.out` — Contains the log messages DS-Client receives from the VMware libraries. From the lowest to the highest level of logging: • **none** (Default) = No logging • **error** = Log errors • **debug** = Debug logging • **warning** = Log warnings • **info** = Log information messages • **trace** = Trace (log everything)
VMware Path Escape	Specifies how DS-Client handles VMware data paths. Since HTTP is used, URL paths can require 'path escaping' for special characters (meaning the use of '%26' instead of '&' in a URL path). • **auto** (Default) — DS-Client tries to determine what path format is required. • **no** — Never use 'escape characters' in paths. • **yes** — Always use 'escape characters' in paths. **Note:** This parameter requires the DS-Client to restart before taking effect.
VMware SOAP Debug	Writes trace logs of any SOAP requests to the `/tmp` folder on the DS-Client. • No = Off (Default) • Yes = On **Note:** This parameter requires the DS-Client to restart before taking effect.
VMware VADP TransportMode	Transport mode that DS-Client requests from the VMware libraries when initializing a connection for data transfer to or from a data center. • Empty (Default) — The library automatically chooses the transport mode based on the VMware priorities among the available transport modes. • **nbd** — Network block device transport mode. • **nbdssl** — Network block device SSL transport mode. • **san** — SAN transport mode. • **hotadd** — HotAdd transport mode. For more information about the transport modes, see Section 5.24, "VMware vCenter Server backups (Windows or Linux)", on page 509.

Parameter	Description
VMware VADP Verify Disk Signature	Forces all VMware vCenter Server backups that have Changed Block Tracking (CBT) enabled to validate the disk signature of a protected virtual machine after a specified number of backups. The interval count starts from the first backup after the setting is enabled. If a disk signature mismatch is detected, a master generation is sent to the DS-System for the affected virtual disk (vmdk). Verification consumes more system resources and increases the backup time, especially if the signature verification fails and requires backup of a new master. • -1 = Disables disk signature validation for all affected backups. • 0 (Default) = Uses the disk signature validation setting configured for each backup. • 1 = Validates the disk signature after every backup for all affected backups. • 2 to 100 = Validates the disk signature after the specified number of backups for all affected backups. **Note:** The disk signature validation setting will be reset to 0 each time the setting is applied to all affected backups.
VMware VADP Verify Disk Signature Time	Forces all VMware vCenter Server backups that have Changed Block Tracking (CBT) enabled to validate the disk signature of a protected virtual machine on specified days. If a disk signature mismatch is detected, a master generation is sent to the DS-System for the affected virtual disk (vmdk). Verification consumes more system resources and increases the backup time, especially if the signature verification fails and requires backup of a new master. • 0 (Default) = Disk signature validation is not performed on weekday. • 1 = Validates the disk signature on a Sunday. • 2 = Validates the disk signature on a Monday. • 4 = Validates the disk signature on a Tuesday. • 8 = Validates the disk signature on a Wednesday. • 16 = Validates the disk signature on a Thursday. • 32 = Validates the disk signature on a Friday. • 64 = Validates the disk signature on a Saturday. **Note:** To perform disk signature validation on multiple days, add the values together. For example, to validate the disk signature on Sunday (1), Tuesday (4), and Friday (32), specify 37.
VMware VixDiskLib Configfile Path	Path to the VMware Virtual Disk Library configuration file for VMware-VIX backup type only. Configuring this parameter is necessary only if you want to define your own configuration file and specify different settings. Any valid file name is a valid value. Refer to the VMware documentation for more information. • Default: blank — The default VMware Virtual Disk Library settings will be used. **Note:** This parameter requires the DS-Client to restart before taking effect.

2.1.8.8 Notification parameters (Windows)

Parameter	Description
DBEmergencyLevel	Emergency warning level for the available space on the disks where the DS-Client database resides. • Default: 500 (5%) • Range: 0-10000 Note: Only applies if DS-Client database is local.
DBReserveSpace	Configures the minimum amount of free space (in MB) reserved in the DS-Client database. Low space checking will not count this reserved space as free space. • Default: 100 • Range: 10 to 500 Note: Only applies if the DS-Client database is local.
DBStopServiceLevel	Stop service level for the available space on the disks where the DS-Client database resides. • Default: 100 (1%) • Range: 0-10000 Note: Only applies if the DS-Client database is local.
DBWarningLevel	Warning level for the available space on the disks where the DS-Client database resides. • Default: 1000 (10%) • Range: 0-10000 Note: This only applies if the DS-Client database is local. It is ignored if the database is remote.
EmergencyFrequency	Configures the interval (in hours) at which regular **Low Local Storage Emergency Warning Notifications** will be issued by DS-Client. • Default: 1 • Range: 1 to 6
MemEmergencyFreq	Configures the interval (in hours) at which regular **Low Memory Emergency Warning Notifications** will be issued by DS-Client. • Default: 1 • Range: 1 to 6
MemEmergencyLevel	Configures the **Free Memory Emergency Level**. If the DS-Client free memory falls to a level equal to or below this level, DS-Client will issue **Low Memory Emergency Warning Notifications**. • Default: 20 (20%) • Range: 5 to 100
MemWarningFreq	Configures the interval (in hours) at which regular **Low Memory Warning Notifications** will be issued by DS-Client. • Default: 4 • Range: 1 to 24
MemWarningLevel	Configures the **Free Memory Warning Level**. If the DS-Client free memory falls to equal or below this level, DS-Client issues **Low Memory Warning Notifications**. • Default: 30 (30%) • Range: 10 to 100
OLEmergencyLevel	Configures the **Emergency Warning Level** for DS-Client Local Storage root. If the DS-Client Local Storage free space falls to equal or below this level DS-Client issues **Emergency Warning Notifications**. • Default: 30 (0.3%) • Range: 1 to 10,000

Parameter	Description
OLWarningLevel	Configures the **Warning Level** for DS-Client Local Storage root. If the DS-Client Local Storage free space falls equal or below this level DS-Client issues warning notifications. • Default: 300 (3%) • Range: 1 to 10,000
WarningFrequency	Configures the interval (in hours) at which regular **Low Local Storage Warning Notifications** will be issued by DS-Client. • Default: 4 • Range: 1 to 24

2.1.8.9 Notification parameters (Linux or Mac)

Parameter	Description
Database Emergency Level	Emergency warning level for the available space on the disks where the DS-Client database resides. • Default: 500 (5%) • Range: 0-10000
Database Stop Level	Stop service level for the available space on the disks where the DS-Client database resides. • Default: 100 (1%) • Range: 0-10000
Database Warning Level	Warning level for the available space on the disks where the DS-Client database resides. • Default: 1000 (10%) • Range: 0-10000
Local Storage Emergency Level	Available space emergency warning level for local storage root. • Default: 30 (0.3%) • Range: 1-10000
Local Storage Warning Level	Available space warning level for local storage root. • Default: 300 (3%) • Range: 1-10000
Memory Emergency Level	Free memory emergency warning level. • Default: 20 (%) • Range: 5-100
Memory Warning Level	Free memory warning level. • Default: 30 (%) • Range: 10-100
PM Emergency Frequency	Emergency warning notification interval (in hours) when space is low (DS-Client database / Local Storage / Use Buffer / Memory). • Default: 1 • Range: 1-10
PM Warning Frequency	Warning notification interval (in hours) when space is low (DS-Client database / Local Storage / Use Buffer / Memory). • Default: 4 • Range: 4-10
Use Buffer Emergency Level	Available space emergency warning level for Use Buffer root. • Default: 30 (0.3%) • Range: 1-10000

Parameter	Description
Use Buffer Warning Level	Available space warning level for Use Buffer root. • Default: 300 (3%) • Range: 1-10000

2.1.8.10 Performance parameters (Windows)

Parameter	Description
BigMasterSize	During backup, DS-Client maintains additional meta-data for files larger than this size (in MB), until the new generation backs up to DS-System successfully. This overhead is balanced by the benefit of reducing the chance of re-sending the next generation as a master in case the backup experiences unexpected failures. • Default: 100 • Range: 1 to 102400
CacheSQLiteFile	Caches the SQLite database file to improve speed. • No = Off (Default) • Yes = On
DBBulkOptions	Configures one of the following database bulk insert options: • **Bulk inserts from files and memory allowed** (Default, recommended) • **Bulk inserts disabled** • **Bulk inserts from files allowed** • **Bulk inserts from memory allowed** The selection takes effect immediately.
DBConnections	How many database connections to create when the DS-Client service starts. • Default: 3 • Range: 1 to 16 **Notes:** • This parameter requires the DS-Client to restart before taking effect. • For Grid DS-Clients, this parameter can be applied globally or to individual leaf nodes.
DBSerializableRepeats	Number of times the DS-Client retries a PostgreSQL serializable transaction if it fails. • Default: 10 • Range: 0 to 20
DefaultCompression	Configures ZLIB compression level: • Default: 6 • Range: 0-9 0 = no compression (faster) 9 = maximum compression (slower)
DeltaThreads	Number of delta threads per backup thread. • Default: 1 • Range: 0 to 16 0 = Delta backup is singled threaded. 1 = A single thread does compression / encryption, but it is separated from I/O thread. > 1 = Delta process is multi-threaded. **Note:** For Grid DS-Clients, this parameter can be applied globally or to individual leaf nodes.

Parameter	Description
DeltaThreadsFS	Number of delta threads for file system backups. If you only back up big files, increasing this can improve speed. For backup of small files, the default is usually sufficient. • Default: 1 • Range: 0 to 16 **Note:** For Grid DS-Clients, this parameter can be applied globally or to individual leaf nodes.
DSClientPerformCopyFromSnapshot	For Microsoft SQL Server (VSS-aware) backups with Nimble Storage integration. How the data copy from the snapshot is triggered. • Yes (Default) — The copying of the data is triggered remotely by DS-Client. • No — The copying of the data is triggered locally by the VSS requester.
EncryptedLocalData	Encrypt the data saved in the Local Storage for Local Storage backups and Local-only backups using the DS-Client's Private Key. • No = Off (Default) • Yes = On
ExchangeOnlineRestoreBatchSize	Configure buffering when DS-Client restores Microsoft 365 (Exchange Online) or Microsoft Exchange Server EWS backups. • Default: 100 • Range: 1 to 1000 To specify the maximum number of items that can be cached to buffer, enter a value between 1 and 1000. When this parameter is set to 1, DS-Client uploads data one item at a time to the Cloud destination.When this parameter is set to 2 or greater, buffering is enabled. DS-Client will cache the data to buffer up to the number of items specified in this parameter and then upload the data to the Cloud destination.
FileReadBufferSize	The internal buffer size (in KB) allocated for reading a file during the backup process. • Default: 64 • Range: 16 to 65,536
MasterGenerations	Generates a full master file on DS-System after this number of generations. Used with the **SendFullMaster** parameter. • Default: 10 • Range: 1 to 25
MaxCacheCopySessions	Maximum concurrent activities supported by DS-Client. Increase if hardware can support additional processing. • Default: 12 • Range: 1 to 99 **Note:** For Grid DS-Clients, this parameter can be applied globally or to individual leaf nodes.
MaxDeltaSize	Maximum file size (in GB) for delta algorithm to apply. The bigger the size, the more memory that is needed for delta processing. • Default: 1048576 • Range: 1 to 1048576

Parameter	Description
MaxPendingIOPerFile	Maximum pending I/O requests for backup or restore of a single file. Increasing this value can improve backup / restore speed if the target storage has very good parallelism (ability to perform simultaneous I/O requests). This option is for high performance environments where you can test the disk I/O. • Default: 2 • Range: 1 to 16 **Important**: Increasing this value too much can cause performance to slow.
MaxRestoreReadThreads	Maximum number of read threads on DS-System side for a restore process. • Default: 1 • Range: 1-16 When restoring backups with many large files, such as VMware vCenter Server backups, we recommend you use the same value for the MaxRestoreReadThreads and MaxRestoreThreads parameters. **Note:** For Grid DS-Clients, this parameter can be applied globally or to individual leaf nodes.
MaxRestoreThreads	Maximum number of threads for a restore process. • Default: 4 • Range: 1 to 16 When restoring backups with many large files, such as VMware vCenter Server backups, we recommend you use the same value for the MaxRestoreReadThreads and MaxRestoreThreads parameters. **Note:** For Grid DS-Clients, this parameter can be applied globally or to individual leaf nodes.
MaxSessionCheck	Determines when the **MaxSessions** parameter applies. • **Scheduled Activities Only** (Default) = The number of scheduled activities that are concurrently running cannot exceed the limit configured in **MaxSessions**. Users can perform on-demand activities beyond the limit. • **Scheduled and On-Demand Activities** = The number of scheduled and on-demand activities that are concurrently running cannot exceed the limit configured in **MaxSessions**.
MaxSessions	Maximum concurrent activities supported by DS-Client. Increase only if your hardware can support additional processing. For Grid DS-Clients, this parameter also refers to the Task Limit (On the Grid menu, point to Grid Status, and then click the List tab for each node). • Default: 12 • Range: 1 to 99 **Note:** For Grid DS-Clients, this parameter can be applied globally or to individual leaf nodes.
MaxSharePointOnlinePowerShellSessions	Specifies the maximum number of PowerShell sessions that can run concurrently when checking the SharePoint Online user count. • Default: 3 • Range: 1 to 32
MaxThreads	Maximum number of threads for each backup activity. Increase only if your hardware can support additional processing. • Default: 4 • Range: 1 to 16 **Note:** For Grid DS-Clients, this parameter can be applied globally or to individual leaf nodes.

Parameter	Description
MaxThreadsMLR	Maximum number of threads for each DS-MLR backup activity. Increase only if your hardware can support additional processing. • Default: 4 • Range: 1 to 16 **Note:** For Grid DS-Clients, this parameter can be applied globally or to individual leaf nodes.
MinDeltaGen	The minimum number of online generations required to process files as deltas. • Default: 3 • Range: 2 or 3
MinDeltaSize	Minimum file size (in KB) for delta algorithm to apply. • Default: 64 • Range: 32 to 1048576
PostgreSQLMediaLoadBatchSize	Specifies the batch size when loading media catalog files. Only applicable to DS-Clients using a PostgreSQL database. • Default: 500 • Range: 0 to 10000
RestoreCacheBufferSize	Internal buffer size (in MB) for caching restore data. Increasing this value can improve the restore performance. • Default: 2 • Range: 1 to 1024
SalesforceExtractThreads	Number of threads to use when extracting data from Salesforce. • Default: 4 • Range: 1-16
SalesforceRestoreSysTables	Attempt to recover Salesforce system tables when performing restore. • No = Off (Default) • Yes = On
SalesforceUseBulkApi	Use the Salesforce “BULK API” protocol to retrieve data. If off, records are read row-by-row, which can significantly increase the number of API calls used. • Yes = On (Default) • No = Off
SendFullMaster	Backups always send a full master (instead of an incremental delta). • No = Off (Default) • Yes = On
SkipCompressionOnCompressedFiles	Skips compression on the following types of compressed files: pk, zip, gif, png, Microsoft Cabinet Files, gzip, win, jpeg & jfif. • Yes = On (Default) • No = Off
SortMethod	Sort algorithm used to sort internal list. • Merge Sort (Default) • Quick Sort
SQLQueriesUseIndexHints	Applicable for SQL Server databases only. Use index hints in SQL queries to the DS-Client database. • No = Off (Default) • Yes = On
StatisticalCpuUsage	Limits the DS-Client's consumption of the computer's CPU during statistical backups to this percentage. • Default: 70 • Range: 0 to 100

Parameter	Description
SyncUseLargeMessage	Uses fewer, larger messages during the file synchronization process, which is more efficient over higher latency networks. • Yes = On (Default) • No = Off

2.1.8.11 Performance parameters (Linux or Mac)

Parameter	Description
Compression Level	Configures ZLIB compression level: • Default: 6 • Range: 0-9 0 = no compression (faster) 9 = maximum compression (slower)
EncryptedLocalData	Encrypt the data saved in the Local Storage for Local Storage backups and Local-only backups using the DS-Client's Private Key. • No = Off (Default) • Yes = On
Max DeltaSize	Maximum file size (in GB) for delta algorithm to apply. The bigger the size, the more memory that is needed for delta processing. • Default: 1048576 • Range: 1 to 1048576
MaxSession Check	Determines when the **MaxSessions** parameter applies. • **Scheduled Activities Only** (Default) = The number of scheduled activities that are concurrently running cannot exceed the limit configured in **MaxSessions**. Users can perform on-demand activities beyond the limit. • **Scheduled and On-Demand Activities** = The number of scheduled and on-demand activities that are concurrently running cannot exceed the limit configured in **MaxSessions**.
MaxSession Number	Maximum concurrent activities supported by DS-Client. Increase only if your hardware can support additional processing. • Default: 12 • Range: 1 to 99
MaxThread Number	Maximum number of threads for each backup activity. Increase only if your hardware can support additional processing. • Default: 2 • Range: 1 to 99 **Note:** This parameter requires the DS-Client to restart before taking effect.
Min DeltaSize	Minimum file size (in KB) for delta algorithm to apply. • Default: 64 • Range: 32 to 1048576
MinDeltaGen	The minimum number of online generations required to process files as deltas. • Default: 3 • Range: 2 or 3 **Note:** This parameter requires the DS-Client to restart before taking effect.
Restore Threads Count	Maximum number of threads for a restore process (VMware and File system backups only, not including NAS). • Default: 1 per CPU (core) up to 4 • Range: 1 to 16

Parameter	Description
RetryPrimary	How often (in hours) to retry the primary DS-System connection after switching to a secondary connection. • Default: 24 • Range: -1 to 24 -1 = never retry 0 = retry immediately
Scan Shares Vacuum Frequency	Interval (in minutes) before the Scan Shares activity will perform a database vacuum on the `dslanfiles` database. This only removes unnecessary data to make the database more compact. It does not affect the information gathered from the scan. • Default: 30 • Range: 1 to 240

2.1.8.12 Local Setting parameters (Windows)

Grid DS-Client Only - Local Setting (Windows DS-Client)	
Parameter	**Description / Values**
DSCBuffer	This parameter only appears when a Grid DS-Client is used and **Local Setting** is selected among the **Type** options. It allows you configure the DS-Client buffer path for an individual leaf node of the Grid DS-Client. Enter a local path on the selected leaf node. The DS-Client service account must have full privileges for the location. The global value for the DS-Client buffer is set in the DS-Client Configuration. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

2.2 Configuring the initialization settings

The initialization settings can be configured without logging on to a DS-Client. The settings apply only to the DS-User on which the changes were made.

2.2.1 Configuring the connection settings

You can specify the host name or IP address where the DS-User will search for the DS-Client service. This will speed up your logon process in large network environments. You can also configure DS-User to scan entire subnets.

NOTE: If you do not specify an IP or DNS address, DS-User scans the local computer and the local computer’s subnet.

To configure the connection settings:

1. On the **Setup** menu, click **Initialization**.
2. Click the **Connection** tab.
3. In the **LAN search time** box, enter the amount of time, in seconds, that the DS-User should spend scanning the LAN for DS-Clients.
4. Under **Additional DS-Clients**, do the following:
   - To add a connection, click **New**.
   - To modify a connection, select the connection, and then click **Modify**.

   NOTE: To delete a connection, select the connection, and then click **Remove**.

5. In the **Add / Edit a DS-Client** dialog box, do the following:
   a) To specify the host name or IP address of a single DS-Client, select **Single DS-Client**, and then type the host name or IP address of the DS-Client.
   b) To specify the host name or IP address of each node in a Grid DS-Client, select **Grid DS-Client**, and then click **Add** or **Modify**. To load a text file containing a list of host names or IP addresses, click **Load.**
   c) In the **Port** box, enter the port number. The default is 4403. Do not change the port number unless you have a specific requirement to do so.
   d) To use the UDP protocol to display the list of DS-Clients faster, select the **Use UDP protocol to discover DS-Client** check box.
   e) Click **OK**.

   NOTE: DS-User scans the LAN for all active DS-Clients. DS-Clients that are not detected appear in Red. DS-Clients on the local computer appear in Blue.

6. Under **Additional Subnets**, do the following:
   - To add a subnet, click **New**.
   - To modify a subnet, select it, and then click **Modify**.

   NOTE: To delete a subnet, select it, and then click **Remove**.

7. In the **Add / Edit a subnet** dialog box, do the following:
   a) In the **Address** box, type the IP address of the subnet.
   b) In the **Port** box, enter the port number of the subnet.
   c) Click **OK**.

8. If you are using a Windows DS-Client and connecting to a DS-Client in an Active Directory domain using the security context of the current logged on user domain, under **Logon using security context**, do the following:

   a) In the **Target Name** box, type a target name. The default is CloudBakSvc.

   IMPORTANT: Your network administrator must create and register the target name with an Active Directory using the Microsoft Networking Tool (setspn.exe) to give it authentication to log on to the required DS-Clients. Once registered, the DS-User supplies the target name for the DS-Client to verify and allow the authenticated user from the DS-User to connect. Ensure any changes conform to your network security policies.

   b) In the **Auto-connect** box, configure how the DS-User behaves when it is launched. The options are as follows:

   - **Last DS-Client –** Searches for the last connected DS-Client. If the DS-Client is not available, the DS-User prompts the user to select a DS-Client.
   - **Local DS-Client –** Searches for the local DS-Client. If the DS-Client is not available, the DS-User prompts the user to select a DS-Client.
   - **Last or Local DS-Client –** Searches for the last connected DS-Client. If the last connected DS-Client is found, the DS-User attempts to connect with it using the credentials of the user already logged on from the current session provided the same user name and password is provided. If the last connected DS-Client is not available, the DS-User connects to the local DS-Client using the current security context.
   - **Local or Last DS-Client** (Default) – Searches for the local DS-Client and connects using the current security context. If the local DS-Client is not available, the DS-User attempts to connect to the last connected DS-Client using the current security context provided the same user network credentials are used, the local user exists on the remote DS-Client, and the appropriate user permissions are present on the remote DS-Client.
   - **Disabled –** Turns off the auto-connect functionality. Users must type a valid user name and password to connect to the selected DS-Client.

9. Click **OK**.

2.2.2 Configuring the regional settings

You can configure the DS-User language settings and other regional formatting.

NOTE: You must restart the DS-User for the changes to take effect

To configure the regional settings:

1. On the **Setup** menu, click **Initialization**.
2. Click the **Regional** tab.
3. In the **GUI Language** box, select a language for the DS-User interface.
4. Under **Date/Time display format**, do the following:
   - To use the standard formatting conventions of a particular language, click **Format using**, and then select a language.
   - To customize the formatting, click **Use custom formatting**, and then type the format that you want to use.
5. Under **Date Format Strings**, specify the format you want to use for dates.
6. Under **Number Format Strings**, specify the format you want to use for numbers.

   NOTE: You can edit the number format strings only if you have selected **Use custom formatting**.

7. Click **OK**.

2.2.3 Configuring the plug-in settings

Depending on the DS-Client configuration, some plug-ins are automatically applied. However, other plug-ins must be manually configured.

To configure the plug-in settings:

1. On the **Setup** menu, click **Initialization**.
2. Click the **Plugins** tab.
3. Enable or disable the plug-in as required.
4. To configure a plug-in, select it, and then click **Configure**.
5. Configure the available plug-in options, and then click **OK**.
6. Click **OK**.

2.2.4 Configuring the keep alive settings

The keep alive settings limit the amount of idle time on DS-User, after which the connection with the DS-Client is terminated.

To configure the keep-alive settings:

1. On the **Setup** menu, click **Initialization**.
2. Click the **Keep Alive** tab.
3. In the **Send "Keep alive" probes when a connection is idle for** box, enter the amount of time, in seconds, that the connection must be idle before the DS-User starts sending keep alive probes to detect the status of the DS-Client.
4. In the **Send "Keep alive" probes every** box, enter the interval, in seconds, at which the DS-User sends keep alive probes until it receives a response or the maximum number of probes have been sent.
5. In the **Terminate Connection after trying** box, enter the maximum number of retries before the DS-User terminates the connection with the DS-Client.
6. Click **OK**.

2.3 Configuring users and groups

You can configure the maximum online limits for specific users or an entire group of users. The lowest group limit applies to individual users.

NOTE: Backups will stop when the online limit has been reached. If more than one limit applies, the lower limit will be enforced.

To configure users and groups:

1. On the **Setup** menu, click **Users & Groups**.
2. To view information about a user or group, select the user or group, and then click **Show Users** or **Show Groups**.
3. To set a maximum online amount for a user or group, select the user or group, and then do the following:
   a) Click **Max Online**.
   b) Clear the **No Limit** check box. If this check box is enabled, the user or group will have unlimited online storage capacity.
   c) In the **Online storage limit** box, enter the maximum amount you want to assign to the user or group.

d) Click **OK**.

NOTE: The online limit is tracked during backups by taking the current online amount and adding new backups. When the online limit is reached, the backup stops even if it is not completed. If two backups are scheduled concurrently, DS-Client allows both backups to use the remaining online amount, which means it is possible for the online storage to exceed the maximum online limit.

4. To delete a user or group, select the user of group, and then click **Delete**.

NOTE: You cannot delete a user or group who has active backups. If a deleted user logs back on to the DS-Client, they will be added back to the list.

5. Click **Close**.

2.4 Configuring the LDAP user settings

If your service provider has configured the DS-Client to use LDAP user validation, you must configure and validate the user credentials before the DS-System permits DS-Client activities.

Each DS-Client is required to configure LDAP user validation by supplying their LDAP server user account credentials. If validation is successful, the DS-System saves the LDAP user settings. On each subsequent DS-Client connection, the DS-System verifies the LDAP user settings with the LDAP server. If the user account exists and is not disabled, the DS-System permits the DS-Client activity.

The LDAP server is a separate location where the DS-System validates that the supplied user account exists. This allows administrators an extra level of validation so they can disable or delete the account on the LDAP server to prevent further DS-Client activities.

To configure LDAP user validation:

1. On the **Setup** menu, click **LDAP User Validation**.
2. In the **User name** box, type the user name on the LDAP server the DS-Client will use for authentication.
3. In the **Password** box, type the password for the LDAP user.
4. In the **Confirm password** box, re-type the password.
5. In the **Domain** box, type the domain of the LDAP user account.

6. To validate the credentials immediately, click **Validate Now**. The DS-Client sends the credentials to the DS-System to validate with the LDAP server.

NOTE: If the validation is successful, the status changes to **Validation passed** and the boxes are cleared.

7. To save the credentials, click **Save**. The credentials are saved until the first validation instance is required by the DS-System.

2.5 Configuring the two-factor authentication settings

Two-factor authentication prevents accidental or unauthorized deletion of backups and backup data. When this feature is enabled, only authorized users can delete a backup or backup data or assign a retention rule to an existing backup while logged on to the DS-Client. Before performing these tasks, an authorized user is required to type an authentication code the DS-System generates.

If your service provider has already configured the DS-Client to use two-factor authentication, you must configure the two-factor authentication settings for the DS-Client. This includes the list of authorized users and their email addresses for receiving authentication codes from the DS-System. You can manually add the users or import a list of users.

NOTE: You must be a DS-Client administrator to configure the two-factor authentication settings for the DS-Client.

To configure the two-factor authentication settings:

1. On the **Setup** menu, click **Two-factor Authentication**.
2. Do one of the following:
   - To add a user, click **Add**.
   - To modify the details of a user, select the user, and then click **Modify**.

NOTE: To delete a user, select the user, and then click **Remove**.

3. In the **Add / Edit User** dialog box, do the following:
   a) In the **User name** box, type the name of the user you want to authorize.

NOTE: For successful authorization, the name must represent a valid existing user account on the DS-Client computer.

b) In the **Domain** box, select the domain to which the user belongs.

c) In the **Email address** box, type the email address associated with the user. This is the email address where an authorization code will be sent when the user attempts to delete a backup or backup data or assign a retention rule to an existing backup.

d) Click **OK**.

4. To import a list of users, do the following:

   a) Create a text file that lists each new user on a separate line. For each user, include the user name, domain, and email address, separating each item with a comma, and then save the text file. For example:

   ```
   user_example,example.com,user_example@example.com
   ```

   b) Click **Import**.

   c) Browse for and select the text file containing the list of users, and then click **Open**.

   d) Verify that the user name, domain, and email address of each user that has been imported to the list is correct.

5. Click **Forward to DS-System**.

6. In the **Two-factor Authentication Validation** dialog box, do the following:

   - In the **Authentication Code** box, type the authentication code that you received from the DS-System, and then click **Validate**.

   NOTE: The authentication code is sent to the email address where you usually receive notifications from the DS-System. The code is valid for two hours. To request an authentication code be resent to you, click **Resend**.

7. To export the list of users to a text file, click **Export**, and then save the file.

8. Click **Close**.

2.6 Configuring the Local DS-VDR Tool

The Local DS-VDR Tool is required to create VMware vCenter Server backups with the Local DS-VDR option enabled. This type of backup does not back up data to the DS-System, but instead protects VMware virtual machines by exporting the latest virtual machine through the VMware vCenter Server to another host or datastore that contains a standby virtual machine that is always available for failover within the same VMware vCenter Server.

NOTE: If connected to a VMware vCenter Server that is connected to two or more VMware ESXi standalone hosts, the Local DS-VDR Tool is able to clone virtual machines from one standalone host to another even if there is no shared storage available between the two hosts.

Before you can configure the Local DS-VDR Tool for the DS-Client, the following requirements must be met:

- The Local DS-VDR Tool must already be installed on a network computer that can connect both to the DS-Client and the target VMware vCenter Server. For more information, see the *Client Software Installation Guide*.
- The DS-Client must have at least one Local DS-VDR license count available. This is allocated by your service provider from the DS-System. For more information, see Section 2.15, “Viewing storage quotas”, on page 85.

NOTE: If the hardware of the machine where the Local DS-VDR Tool is installed has been modified or if you want the DS-Client to use another installation of the Local DS-VDR Tool, you must reconfigure the Local DS-VDR Tool.

To configure the Local DS-VDR Tool:

1. On the **Local DS-VDR** menu, click **Configure Local DS-VDR Tool**.
2. In the **Local DS-VDR Tool IP** box, type the IP address of the Local DS-VDR Tool. It must be accessible by the DS-Client via TCP port 4407 (default).

   NOTE: Each Local DS-VDR Tool can be used with only one DS-Client.

3. To reset the hardware cookie for the Local DS-VDR Tool, click **Reset**.

   NOTE: You need to reset the cookie only if you install the Local DS-VDR Tool on another machine or alter the hardware on the existing machine.

4. To test the DS-Client’s connection with the Local DS-VDR Tool, click **Connect**. The result is displayed as a message at the bottom of the dialog box.

5. To update the Local DS-VDR Tool database with the current Local DS-VDR backup configuration, click **Sync**.

NOTE: This process is performed automatically by the Daily Admin or Weekly Admin process.

6. Click **OK**.

2.7 Configuring the bandwidth throttle settings

The bandwidth throttle settings allow you to manage the outgoing and incoming bandwidth used by the DS-Client over a defined period. Separate throttles can be defined for backups to the DS-System and restores from the DS-System. By default, if these throttles are not configured, the DS-Client uses as much bandwidth as it requires to perform operations as fast as possible.

NOTE: When connected to a Grid DS-Client, the bandwidth throttle settings are enforced at the node-level. This means the actual bandwidth usage will be the bandwidth throttle value multiplied by the number of nodes running backups or restores simultaneously. For example, a bandwidth throttle of 64 KB/sec on a 3-node Grid DS-Client would be limited to 192 KB/sec.

To configure the bandwidth throttle settings:

1. On the **Setup** menu, click **Bandwidth Throttle**, and then do one of the following:
   - To use the maximum bandwidth to perform operations as fast as possible, select **Unlimited.**
   - To define the bandwidth usage, select **Limited to**, and then specify the bandwidth in KB/sec. This refers to the rate the source data is processed.
2. To configure a bandwidth throttle schedule, do one of the following:
   - To add a bandwidth throttle schedule, click **Add**.
   - To modify a bandwidth throttle schedule, select the schedule, and then click **Modify**.

   NOTE: To delete a bandwidth throttle schedule, select the schedule, and then click **Remove**.
3. In the **New / Edit Bandwidth Throttle Schedule Detail** dialog box, do the following:

a) Under **Days**, select the days of the week for the schedule detail.

b) Under **Starting at**, enter the start time of the schedule detail.

c) Under **Ending at**, enter the end time of the schedule detail.

d) Under **Bandwidth throttle**, select whether you want the bandwidth to be unlimited or limited to a specific amount.

e) Click **OK**.

NOTE: The schedule detail will be an exception to the default setting.

4. To select a group of bandwidth throttles, click **Select Group**.
5. Click **OK**.

2.8 Configuring the filter for the Event Log

An event filter allows you to configure the default severity for an entry in the Event Log by overriding the default severity with a custom setting.

To configure the filter for the Event Log:

1. On the **Setup** menu, click **Event Filter**.
2. Do one of the following
   - To add an event filter, click **New**.
   - To modify an event filter, select the event filter, and then click **Edit**.

NOTE: To delete an event filter, select the event filter, and then click **Remove**.

3. In the **Add / Edit Event Filter** dialog box, do the following:

   a) In the **Event #** box, type the event number as it appears in the Event Log Viewer.

   b) In the **Category** box, select the category associated with the event number as it appears in the Event Log Viewer.

   c) In the **Type** box, select the severity you want to assign to the event. This overrides the default setting and can affect the notifications that are sent.

   d) Click **OK**.

4. Click **OK**.

2.9 Configuring the printer settings

DS-User can interface with existing printers that are configured on the computer where it is installed.

To configure the printer settings:

1. On the **Setup** menu, click **Printer Setup**.
2. In the **Print** dialog box, use the **General**, **Page Setup**, and **Appearance** tabs to configure the printer as required.

2.10 Configuring the appearance of the main window

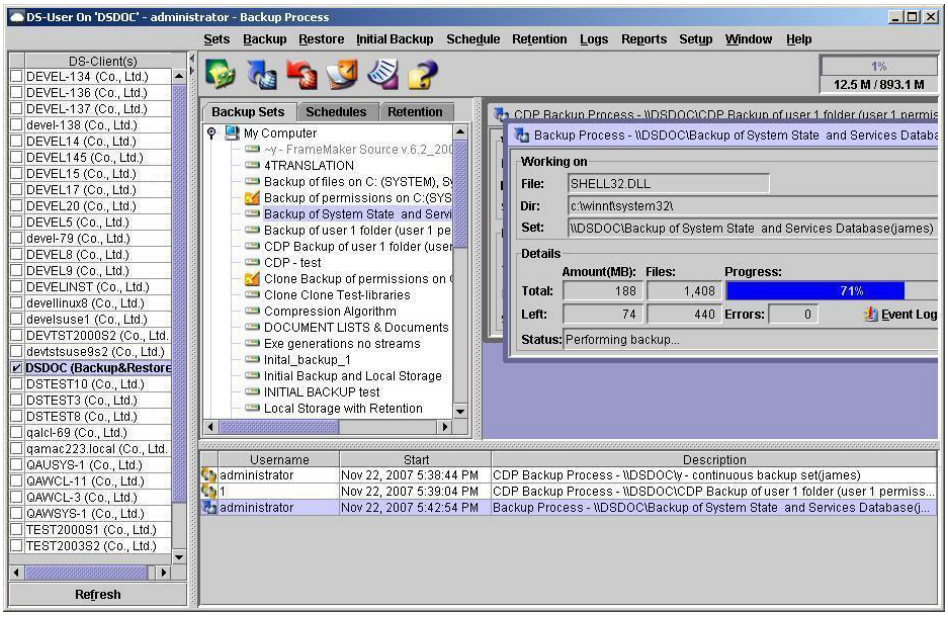
You can configure the appearance of the DS-User main window.

To configure the appearance of the main window:

1. On the **Setup** menu, point to **Look & Feel**, and then select one of the available themes.
2. If you selected the **Metal** theme, you can further configure the look and feel as follows:
   a) On the **Setup** menu, click **Initialization**.
   b) Click the **Look & Feel** tab. This tab will not appear for other themes.
   c) Under **Metal Theme**, select a default theme or under **Custom Colors**, select your colors.
   d) Click **OK**.

2.11 Managing DS-Client activities

The DS-Client provides tools that allow an administrator or backup operator to perform various administrative tasks, including monitoring activities in real time.



- **Real-time activity monitor** – This window is located in the lower section of the DS-User main window and cannot be hidden. It lists activities that are currently in progress and displays the user who authorized the activity, the time at which the activity started, the type of activity, and the name of the backup on which the activity is being performed.
- **Process window** – This window displays the type of process and the name of the backup for which the process is being performed. If you have started an activity on demand, the process window automatically appears.

NOTE: The process window allows you to access the Event Log to view events related to the current process. Most processes are multi-threaded and might finish before the process window can refresh.

To open the process window of an activity listed in the real-time activity monitor, double-click the activity or right-click the activity, and then click **Monitor**.

While an activity is in progress, you can stop the activity in one of two ways:

- In the real-time activity monitor, right-click the activity, and click **Stop Activity**.
- In the process window of the activity, click **Stop**.

2.11.1 Viewing the system status

You can view DS-Client system status information when checking performance or troubleshooting. System status information includes current network connections and processes as well as details of message queues and database connections.

To view the system status:

1. On the **Setup** menu, click **System Activities**.
2. Click **System**.
3. To view the network connections, click the **Network Connections** tab, and then do one of the following:
   a) To send a message to a user who is currently connected to the DS-Client, select the user, and then click **Send Message**. In the **Send Message** box, type the message, and then click **Send**.
   b) To remove a connection from the DS-Client, select the connection, and then click **Disconnect**.

   NOTE: You can send a message to inform the user before you remove the connection.

4. To view the database connections, click the **Database Connections** tab.
5. To view the message queues, click the **Message Queues** tab.
6. To view the threads, click the **Threads** tab.
7. To update the data, click **Refresh**.
8. Click **Close**.

2.11.2 Enabling or disabling DS-Client activities

You can enable or disable scheduled and on-demand activities on the DS-Client.

NOTE: By default, scheduled and on-demand activities are enabled.

To enable or disable DS-Client activities:

1. On the **Setup** menu, click **System Activities**.
2. Under **DS-Client Activities**, do one of the following:
   - To activate or suspend the operation of all scheduled activities on the DS-Client, beside **Scheduled activities**, click **Enable** or **Disable**.
   - To allow or prevent users from performing on-demand activities, beside **Demand activities**, click **Enable** or **Disable**.

NOTE: Disabled activities are automatically enabled the next time the DS-Client service restarts.

2.11.3 Managing administrative processes

The DS-Client is designed for unattended operation, which requires regular administrative processes to back up the DS-Client database, create statistical data, and verify backups with the DS-System online storage.

You can schedule the daily and weekly administrative processes or run them on demand. You can also update statistical data on demand.

The types of administrative processes are as follows:

- **Local Admin** – Performs activities that do not require a connection to the DS-System. The Local Admin process runs every time the DS-Client service starts, once every 12 hours from the previous Admin, or every 24 hours. This process cannot be disabled.
- **Daily Admin** – Performs all Local Admin activities, verifies backups, and transfers the DS-Client database dump to the DS-System. The Daily Admin process can be disabled or configured to run at a specific time.
- **Weekly Admin** – Performs all Daily Admin activities and a low-level synchronization of backups. The Weekly Admin process can be disabled or configured to run at a specific date and time.

The following table describes the administrative process activities in the order they are performed. The DS-System column indicates whether a connection to the DS-System is required for that activity.

Administrative process activity	Local	Daily	Weekly	DS-System
1. Prepare database dump For Microsoft SQL Server databases, this activity depends on the **Keep DS-Client database dump file** setting: • **Do not delete –** Saves the previous dump, dumps the DS-Client database and dsdelta database, and runs database consistency checks (DBCC). If an error occurs, it restores the previous dump. Otherwise, it deletes the previous dump and only keeps the current dump in the DS-Client buffer. • **Delete after successful backup –** Saves the previous dump (if it exists), dumps the DS-Client database and dsdelta database, and runs database consistency checks (DBCC). If no errors occur, it removes the previous database dump (if it exists) from the DS-Client buffer before connecting to the DS-System. If activity 6 (Transfer Database Dump) is successful, it removes the current database dump from the DS-Client buffer. • **Always delete –** Dumps the DS-Client database and dsdelta database and runs database consistency checks (DBCC). After the Daily Admin or Weekly Admin finishes, it deletes the database dump. **Note**: This step is not performed for PostgreSQL databases.	X	X	X	
2. Clean database Deletes old history logs (activities, events and statistics), drops unused tables, and deletes unused records.	X	X	X	
3. Update statistical data Updates statistical information for each backup (number of files and online amount).	X	X	X	
4. Expand database (if necessary) Updates statistical information for each backup (number of files and online amount).	X	X	X	
5. Verify backups Sends a list of all backups to the DS-System. DS-System sends back a list of backups that do not exist on the DS-System storage or exist on the DS-System storage but are not in the DS-Client's list.		X	X	X
6. Transfer database dump For PostgreSQL databases, performs backup of the database to DS-System via pipe. For Microsoft SQL Server databases, transfers database dumps to DS-System if activity 1 was performed successfully. Deletes database dumps if activity 1 is configured for **Delete after successful backup** or **Always delete**.		X	X	X
7. Synchronization (normal) Performs synchronization check for all backups that either do not exist on the DS-System storage or exist on the DS-System storage but are not in the DS-Client's list. This is the same as a Normal synchronization, but any synchronized files retain an active backup status.			X	X
8. Send daily email notification If the DS-Client is configured for email notifications, sends a summary of backup activities to the administrator showing what occurred since the last admin process.	X	X	X	

2.11.3.1 Running administrative processes on demand

You can run administrative processes on demand.

To run Daily Admin on demand:

1. On the **Setup** menu, click **System Activities**.
2. Under **Administrative Processes**, beside the **Last Daily Admin run on** box, click **Run Now**.

To run Weekly Admin on demand:

1. On the **Setup** menu, click **System Activities**.
2. Under **Administrative Processes**, beside the **Last Weekly Admin run on** box, click **Run Now**.
3. To force a synchronization of all backups, select the **Synchronize all sets** check box.

NOTE: Forcing the synchronization of all backups will increase the amount of time it takes to complete the Weekly Admin process. If this check box is not selected, the Weekly Admin process skips synchronizing backups as long as no database inconsistencies are detected. Applies to Windows DS-Clients.

---

4. In the **Number of simultaneous synchronizations** box, enter the maximum number of simultaneous synchronizations that will run.

NOTE: This number is limited by the maximum concurrent activities supported by the DS-Client as configured in the **MaxSessions** (Windows) and **MaxSession Number** (Linux) advanced configuration parameter.

---

5. Click **OK**.

NOTE: If you run the Weekly Admin process to obtain a DS-Client database backup for recovery purposes and you see synchronization for any backups, you should run the Weekly Admin process again to obtain the latest backup of the DS-Client database. This avoids repeating the synchronization process after the database is recovered.

2.11.3.2 Scheduling administrative processes

The default configuration for administrative processes is as follows:

- The Daily Admin process is scheduled to run once every day between 20:00 and 06:00.
- The Weekly Admin process is scheduled to run once a week between 20:00 Friday and 06:00 Monday.

NOTE: To distribute the administrative process load across many DS-Clients, the default start time is randomly determined by an algorithm based on the DS-Client number, which results in a time with an interval of 15 minutes.

No other activities are allowed to be performed while an administrative process is running. If an activity is running at the time the administrative process is scheduled, it waits for all activities to finish. Therefore it is possible that the scheduled administrative process never gets the opportunity to run (for example, if you have scheduled backups that run 24 hours a day, 7 days a week). If it is not possible to schedule an administrative process, you should occasionally run one manually.

NOTE: We recommend that you schedule administrative processes at times that do not conflict with scheduled backup activities.

To schedule Daily Admin:

1. On the **Setup** menu, click **Configuration** and then click the **Parameters** tab.
2. Ensure that the **Daily start** check box is selected.
3. Type the time of the day when you want the Daily Admin process to start.
4. Click **OK**.

To schedule Weekly Admin:

1. On the **Setup** menu, click **Configuration** and then click the **Parameters** tab.
2. Ensure that the **Weekly start** check box is selected.
3. Select the time of the day and a day of the week when you want the Weekly Admin process to start.
4. Click **OK**.

NOTE: The DS-Client can be configured to reboot after performing an admin process. By default, this option is disabled. To enable this option, select the Reboot after Admin check box. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

2.11.3.3 Updating statistical data on demand

The DS-Client accumulates statistical information that can help you analyze load, utilization, and storage trends.

For new target backup servers, the DS-Client can perform statistical backups for a few days or weeks to generate this information. These are similar to online backups except no data is sent to the DS-System. The data source is scanned and files are processed for compression and encryption to obtain statistics. You can analyze these statistics before performing actual backups.

Statistical data is updated automatically during a Daily Admin or Weekly Admin process. If no administrative processes are scheduled, the DS-Client automatically updates statistical data daily. You can also update statistical data on demand to ensure that it is available immediately before generating reports.

In production environments, the statistical information accumulates for all backup types (online, statistical, self-contained, local-only, and instant recovery). These details are presented in the reports that the DS-Client generates.

To update statistical data on demand:

1. On the **Setup** menu, click **System Activities**.
2. Under **Administrative Processes**, beside the **Statistics updated on** box, click **Update Now**.

2.11.4 Recovering the DS-Client database

By default, the DS-Client database is backed up by the Daily and Weekly Admin processes. There are several scenarios that might require you to recover the DS-Client database, including:

- Replacing the DS-Client machine
- Recovering a corrupted DS-Client database
- Migrating the DS-Client to another machine
- Reinstalling the DS-Client software after an operating system or hard disk failure

---

IMPORTANT: Before upgrading to a newer version of the DS-Client, you must install the same DS-Client software version and hotfix level that was installed on the original DS-Client, and then recover the DS-Client database.

When you perform a DS-Client database recovery, the recovered database contains the data up to the time of its last backup. On startup, the DS-Client checks if the database number is compatible with the executable. If it is not, the DS-Client

service stops or runs in a suspended mode that prevents connection or activity. If this occurs, check the operating system event log for details. Apply the missing patches up to the database build number you require.

For Grid DS-Clients, any node that has a lower software version than what is compatible with the current database build is auto-upgraded immediately after the DS-Client service starts.

NOTE: If you do not have a DS-Client database backup, you must recover each backup that is on the DS-System individually to recreate the database. You will not be able to recover the backup schedules or any of the logs. Do not create any new backups until you finish reconstructing the DS-Client database to the point it can synchronize successfully with the DS-System. For more information, see Section 6.5, “Synchronizing a backup”, on page 544.

To recover the DS-Client database:

1. Install an operating system supported by the DS-Client and recreate the user accounts, including the DS-Client service account.
2. Install the same DS-Client software version that was installed on the original DS-Client computer and apply the latest hotfixes for that version.
3. Start the DS-Client service and connect with the DS-User.
4. Verify the DS-Client database patch level as follows:
   a) On the **Help** menu, click **About DS-User**, and then click **DS-Client Info**.
   b) In the **DS-Client Version Info** dialog box, check the **Database Build** value. You need to compare this value with the one that appears after recovering the database.
5. On the **Setup** menu, click **System Activities**.
6. Beside **Repair DS-Client Database**, click **Repair**.
7. In the **Repair DS-Client** dialog box, do one of the following:
   - To recover the last backed up version of the dsclient and dsdelta databases, select **DS-Client & delta databases**, and then click **OK**.

     NOTE: The delta database contains delta information for all files and can only be recovered on Windows DS-Clients. If the database cannot be recovered, the DS-Client sends a new master on the next backup, which can significantly increase the time of the backup process.

- To recover the last backed up version of the dsclient database, select **DS-Client database**, and then click **OK**.

IMPORTANT: You existing database will be replaced. This operation cannot be undone.

8. To activate the recovered database, stop and restart the DS-Client service.
9. Run a Weekly Admin process. For more information, see Section 2.11.3.1, “Running administrative processes on demand”, on page 76.
10. Check the Event Log to ensure that no data exists on the DS-System that is not in the DS-Client database. If more data exists, you must synchronize the affected backups before any further backup or restore activities can be performed. For more information, see Section 6.5, “Synchronizing a backup”, on page 544.

NOTE: If the recovered DS-Client database data is missing backups, you must recover the orphaned backups. For more information, see Section 6.10, “Recovering an orphaned backup”, on page 549.

11. Change the ownership of the backups. For more information, see Section 6.11, “Changing the ownership of a backup”, on page 551.

NOTE: If you see two users with the same name it is because the DS-Client searches by Security ID (SID). Select the lower one because the current user is closest to the bottom of the list.

12. On the **Help** menu, click **About DS-User**, and then click **DS-Client Info**. Verify the DS-Client’s database patch levels again.

IMPORTANT: When you recover a DS-Client database, any configuration changes made after the last database backup must be manually reapplied.

2.11.5 Shutting down the DS-Client computer

If required, you can force a shutdown of the DS-Client computer at any time.

To shut down the DS-Client computer:

1. On the **Setup** menu, click **System Activities**.
2. Beside **Shutdown DS-Client computer,** click **Initiate**.
3. In the **Shutdown in** box. enter the time (in seconds) after which the system should shutdown.
4. To reboot the DS-Client computer after the shutdown, select the **Reboot** check box.
5. In the **Send message** box, type the message that you want to send to any users currently connected to the system.
6. Click **Shutdown**.

2.12 Managing passwords (Windows)

You can manage the network security of backups in two ways:

- Associate specific backups to designated users.
- Rotate the password of the designated users on demand or automatically.

You can manage the list of users that have their passwords randomized. Once a password is rotated, no one will know what it is. This means the only way you can use this user name is by applying it to a backup through this feature.

IMPORTANT: When password rotation is applied to a user account, the account cannot be used to log on or as credentials on your network until an administrator manually resets the password in the computer management console of Windows.

When prompted, the DS-Client service changes the Windows password of the specified network user or computer user. When automatic password rotation is enabled, the DS-Client randomly selects a new password for the specified user at a frequency and within the constraints that you define in a rotation rule.

When password management is used, you must manage backups in the Password Management dialog box. You cannot use the Backup Set Properties dialog box because the password has changed.

NOTE: This procedure describes the pages in the Create User Wizard, which correspond to the tabs in the Modify User dialog box.

To manage passwords:

1. On the **Setup** menu, click **Password Rotation**.
2. In the **Password Management** dialog box, do one of the following:
   - To add a user to the password management list, click **Add**.
   - To modify a user in the password management list, select the user, and then click **Edit**.

NOTE: To delete a user from the password management list, select the user, and then click **Remove**. You cannot remove a user who is associated with a backup. You must remove the backup associations first.

---

3. On the **Enter User Information** page, do the following:
   a) In the **User Name** box, type the user account from a computer or domain.
   b) In the **User From** box, type the corresponding computer or domain where the user account is located.
   c) In the **Password** box, type the current password for the user.

   NOTE: The current password is required when adding a user account for the first time to enable the randomization.

   ---

   d) In the **Notes** box, type any information about the user account.
   e) Click **Next**.
4. On the **Select Password Rotation Rule** page, do the following:
   a) To enable automatic password rotation, select the **Enable Automatic Password Rotation** check box.

   NOTE: If you do not enable automatic password rotation, you must manually rotate the password for the user.

   ---

   b) In the **Available Password Rotation Rules** dialog box, do the following:
      - To add or modify a password rotation rule, click **New or Edit**. Type a name for the rule and define the length constraints for the password. To define a complexity rule, click **Add**. Select the minimum number of characters and the character set that must be included, and then click **OK**. To remove a rule, select the rule, and then click **Remove**.
      - To apply an existing password rotation rule, select the rule, and then click **Select**.

c) In the **Rotation Rule** box, select the password rotation rule you want to apply to the user account.

d) In the **Rotation Frequency** box, enter the frequency at which the corresponding user account password is randomized.

e) Click **Next**.

5. On the **Select Associated Backup Sets** page, do the following:

a) Click **Select**.

b) Select the backups that you want to associate with the user, and then click **OK**.

NOTE: This will overwrite the Connect As setting in the Backup Set Properties for all selected backups.

---

c) Click **Finish**.

6. To rotate the selected user's password immediately, click **Rotate Now**.
7. To update the list of passwords, click **Refresh**.
8. Click **Close**.

2.13 Exporting the DS-Client configuration to an XML file

You can export the DS-Client configuration to an XML file (config-update.xml), which you can use to manually update the configurations of existing DS-Clients or to deploy a large number of DS-Clients. For more information, see the *DS-Client Mass Deployment Guide*.

NOTE: This feature is not supported for backups that have been configured with the Local DS-VDR option.

The DS-Client reads any XML file named config-update.xml and verifies the structure is correct. If the file has not previously been applied, the DS-Client applies its settings. You can use an exported config-update.xml file as is, edit the file, or create your own. The XML file must conform to the structure defined in the file asigra_conf.dtd.

- For Windows DS-Clients, place the file config-update.xml in the program folder containing the DS-Client service.

- For Linux / Mac DS-Clients, place the file config-update.xml in the `/etc` sub-folder of the program folder containing the DS-Client service.

NOTE: The config-update.xml is meant to update a properly functioning DS-Client and is not intended to be used to recover an existing DS-Client. If you need to recover a DS-Client that has its database backed up to the DS-System, it is better to use the repair function.

If the **AllowAutoConfig** parameter is enabled, the DS-Client checks for a file named config-update.xml at startup and every 10 seconds afterwards. The DS-Client reads the configuration file and then applies any updates it finds to its database. The DS-Client only applies the config-update.xml file if the file signature is different from the file signature of the previous file that was applied. Any existing configurations, backups, schedules, or retention rules are overwritten if the replace-existing attribute is set to Yes. After the XML file is applied, the DS-Client renames the file to **config-update-nnn.xml**, where nnn is an incremental number.

NOTE: The <account-name>, <account-number>, <client-number>, and <encryption-keys> elements are updated only when the DS-Client restarts.

To export the DS-Client configuration to an XML file:

1. On the **Setup** menu, click **Export to XML**.
2. Under **Export Items**, select the items you want to export. The choices are as follows:
   - **DS-Client Configuration** – Exports all DS-Client settings.
   - **Backup Schedules** – Exports all or selected backup schedules.
   - **Retention Rules** – Exports all or selected retention rules.
   - **Backup Sets** – Exports all or selected backups.

   NOTE: Recovered orphaned backups that have not been migrated or had their backup information reconfigured cannot be exported.

   ---

3. To include encrypted DS-Client and account keys in the XML file, select the **Include Encryption Keys** check box.
4. To use a meta symbol where required in the config-update.xml file, select the **Meta Symbol** check box (Windows DS-Client only). This allows the XML file to be used interchangeably on different localized operating systems.
5. To expand or collapse the list of items, click **Expand All** or **Collapse All**.
6. To save the XML file, click **Save As**.
7. Click **Close**.

2.14 Sending upgrade information to the DS-System

To enable DS-System administrators to manage the DS-Client automatic upgrade process using the DS-Operator, the DS-Client sends information to the DS-System every 24 hours. However, you can also send this information on demand.

NOTE: Automatic upgrades of the DS-Client must be approved by a DS-System administrator using the DS-Operator.

To send upgrade information to the DS-System:

- On the **Setup** menu, click **Send upgrade info**.

If successful, a message appears confirming the DS-Client upgrade information has been successfully sent to the DS-System.

2.15 Viewing storage quotas

You can view the storage quotas for your customer account and DS-Client account. This information is read-only and is configured by your service provider on the DS-System. Storage quotas are calculated based on the following:

- **Protected Size –** The size of the files that were backed up. This counts the original file size of each generation of a backed up file.
- **Stored Size** – The size of the files on the DS-System.
- **Native Size** – The restorable size of the backed up files, including files deleted from source. This only counts the original size of the latest generation of all backed up files.

To view the storage quotas:

1. On the **Setup** menu, click **View Quotas**. The following information is displayed:

Customer Storage Quota	
Quota	Total storage quota amount, in MB or GB, for all DS-Clients associated with the customer account.
Stop Backup level	Storage amount at which the DS-System stops all backups for the customer.
Send E-Mail when the following are reached	Specifies if an email will be sent when each event occurs. You must provide your service provider with an email address.
Used Quota	Quota used (number and percentage)
DS-Client Storage Quota	
Quota	Total storage quota, in MB or GB, for all backups on the DS-Client.

Stop Backup level	Storage amount at which the DS-System stops all backups for the DS-Client.
Send E-Mail when the following are reached	Specifies if an email will be sent when each event occurs. You must provide your service provider with an email address.
Used Quota	Quota used (number and percentage)
DS-Client Local-only Storage Quota	
Quota	The total storage quota, in GB, for all Local-only backups on the DS-Client.
Used Quota	Quota used (number and percentage)
DS-Client Local DS-VDR License	
Local DS-VDR Count	Total number of licenses that have been allocated to the DS-Client. If the used amount reaches or exceeds this number, you must ask your service provider to increase the amount for the DS-Client.
Used	Total number of virtual machines using Local DS-VDR. This a counter increases each time a Local DS-VDR backup is used to export a virtual machine. Each virtual machine counts as one license against the allocated pool for the DS-Client.
VM Replication Storage Quota	
VM Replication Capacity	Total size of the virtual machines that have been allocated to the DS-Client for replication. If this value is 0 and the VM Replication Count is greater than 0, you are allowed unlimited native capacity.
Used VM Replication Capacity	Total native capacity of virtual machines that have been replicated by the DS-Client.
VM Replication Count	Total number of virtual machines that have been allocated to the DS-Client for replication. If this value is 0 and the VM Replication Capacity is greater than 0, you are allowed an unlimited VM replication count.
Used VM Replication Count	Total number of virtual machines that have been replicated by the DS-Client.

2. To view the DS-Tools enabled for the DS-Client, click **DS-Tools**.
3. Click **Close**.

2.16 Viewing the DS-NOC settings

To view the DS-NOC settings, the DS-NOC must be enabled by you or your service provider. If enabled, the DS-Client sends event information to the DS-NOC for monitoring purposes.

1. On the **Setup** menu, click **DS-NOC Settings**.
2. To use the proxy configuration whenever DS-Client connects to the DS-NOC, select the **Use Proxy** check box. For more information see Section 2.1.6, “Configuring the DS-System connection settings”, on page 33.

NOTE: The rest of the information displayed is obtained from the DS-System and is read-only.

---

3. To connect the DS-Client immediately to the DS-System to obtain the latest settings, click **Check New Settings**. The DS-Client automatically updates the settings each time it connects to the DS-System.
4. To connect the DS-Client immediately to the DS-NOC server to send monitoring information, click **Connect to DS-NOC**.
5. Click **Close**.

2.17 Viewing the memory allocation

You can view the memory information that applies to the DS-User.

To view the memory allocation:

- On the **Setup** menu, click **Show Memory**. A memory usage bar appears in the top right corner of the DS-User window. When you hover the cursor over the bar, the following details are displayed:
  - **Maximum Memory** – Maximum amount of memory the DS-User can use.
  - **Total Memory** – Total amount of memory allocated to the DS-User.
  - **Free Memory** – Amount of allocated memory that is free to use.
  - **Used Memory** – Amount of memory that is currently being used.

2.18 Updating the DS-Client configuration file parameters

The DS-Client configuration file (dsclient.cfg) is a text file that stores basic configuration information about the DS-Client, such as the account number and account key of the DS-Client and the IP address of the DS-System, as well as any DS-Client advanced parameter values that differ from the default value.

NOTE: The DS-Client configuration file is created during the installation process and is available only for the Linux or Mac DS-Client. For the Windows DS-Client, the equivalent information resides in the registry and the database.

In the DS-Client configuration file, information is listed as key-value pairs, in which a colon (":") separates the key from the value. The name of the key can be followed by any number of spaces before the colon (":"). Depending on the key, the value may or may not be case sensitive.

IMPORTANT: We recommend that you do not access or modify the DS-Client configuration file except when performing database migration or troubleshooting database issues. If the dsclient.cfg file is improperly configured, damaged, or missing, the DS-Client might not start.

To update the DS-Client configuration file parameters:

1. Access the DS-Client configuration file in the following location:

   `/<DS-Client HOME>/etc/dsclient.cfg`

2. Find the key-value pair that represents the parameter that you want to modify and make the required changes.

   NOTE: When modifying the value of a parameter, always assume that the value is case sensitive.

3. Save the DS-Client configuration file.

To update passwords in the DS-Client configuration file:

Passwords in the DS-Client configuration file must be in an encrypted format.

NOTE: To generate an encrypted version of your password, use the Asigra Encryption Tool (asigraenc). For information, see the *Tools User Guide*.

3 Working with schedules

A schedule allows you to perform automatic unattended activities on a backup. You can create a schedule and assign backups to that schedule. A schedule is composed of details that define when unattended backups will be performed.

NOTE: The Backup Schedules tab allows Administrators and Backup Operators to monitor and adjust the scheduled backup load on the DS-Client.

The DS-Client checks for scheduled operations that are to be triggered 24 hours a day. If a scheduled activity is started but cannot finish because the connection to the DS-System cannot be established or is lost, the DS-Client retries thee times at five-minute intervals (by default) to resume or initiate the connection.

NOTE: You can configure the number of attempts and the interval between retries using the Attempt to reconnect setting. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

If the scheduled operation is missed for this reason, an attempt will be made to perform it at the next scheduled time. For example, a backup scheduled to take place every day at 14:00 will retry the next day at 14:00. If communication between the DS-Client and the customer's LAN fails for any reason, no attempts will be made to reconnect.

If an activity is running at the same time as a scheduled operation and the activity prevents other operations from running, the scheduled operation will start as soon as the activity ends. By default, the DS-Client attempts to start a scheduled operation every minute for 6 hours from the scheduled start time. You can configure the interval using the ScheduleMiss advanced configuration parameter. For more information, see Section 2.1.8, “Configuring the advanced settings”, on page 37.

You can limit the number of scheduled activities that can run concurrently by configuring the MaxSessions (Windows) or MaxSessions Number (Linux) advanced configuration parameter. For Grid DS-Clients, the limit will be the sum of all the MaxSessions parameters from all running nodes. This is useful if you are running simultaneous backups and some data is being backed up using a slower connection. Similarly, if there are too many backups using the same schedule, this will decrease the efficiency of the DS-Client. For more information, see Section 2.1.8, “Configuring the advanced settings”, on page 37.

3.1 Configuring a schedule

A schedule consists of a set of details that represent a specific set of tasks that will run at the defined frequency for the schedule. Each schedule must have at least one detail. You can add as many details to a schedule as required.

To configure a schedule:

1. Click the **Backup Schedules** tab, and then do one of the following:
   - To create a schedule, on the **Schedule** menu, click **New Schedule**.
   - To modify a schedule, select the schedule, on the **Schedule** menu, click **Edit Schedule**.

   NOTE: To delete a schedule, select the schedule, on the **Schedule** menu, click **Delete Schedule**.

2. Under **Schedule**, do the following:
   a) In the **Name** box, type a name for the schedule.
   b) To specify that only administrators can use the schedule, select the **Administrator only** check box (Windows DS-Clients only).
   c) If the schedule will be used by DS-Clients on laptops, select the **DS-Client on portable computer (verify network connection)** check box. In the **Limit CPU usage to (%)** box, enter the CPU limit for the DS-Client service.

   NOTE: The schedule checks for a network connection to the DS-System. If it does not exist, the schedule will not start. The DS-Client will display a message if the laptop schedule misses more than two scheduled backups.

3. Beside **Details**, do one of the following:
   - To create a schedule detail, click **New**. New schedule details appear as <Detail_Type>:<new> until they are saved.
   - To edit a schedule detail, select the detail. Each schedule detail has a unique number assigned to it (e.g. Daily:3).
   - To copy a schedule detail from an existing schedule, click **Copy**.
   - To create a negative schedule detail, select the **Excluded** check box. This specifically does not run a backup or any other tasks at the time and date of the schedule detail and overrides any other details that are scheduled to run at that time.
   - To delete a schedule detail, select the detail, and then click **Delete**.
4. Under **Occurs**, select the frequency at which the schedule runs. The options are as follows:

- **One Time** – Runs the schedule once on the date specified.
- **Daily** – Runs the schedule daily based on the frequency specified. For example, if you enter 3, the schedule will run every third day. The intervals are based on the start date.
- **Weekly**– Runs the schedule weekly based on the frequency specified. For example, if you enter 2, the schedule will run every second week on the days you specify. The intervals are based on the start date.
- **Monthly** – Runs the schedule monthly based on the frequency specified. You can enter a specific day each month (e.g. day 1 of every 1 month) or the day and weekday of each month (e.g. 1st Sunday or every 1 month) that you want to run the schedule.

5. Under **Detail Frequency**, do the following:

   a) To specify that the schedule occur only once, select **Occurs once**.

   b) To specify that the schedule occur every specific number of hours, select **Occurs every**, and then enter the number of hours.

   c) In the **Starting at** box, enter the start time for the schedule detail.

   d) To specify an end time for the schedule detail, select the **Ending at** check box, and then enter an end time for the schedule detail and time period.

   NOTE: If you select the **Occurs every** option, you must specify an end time. Scheduled backup or start LAN scan shares tasks will terminate when the end time is reached. All other tasks will run until they complete if they start before the end time.

6. Under **Detail Period**, do the following:

   a) In the **Start date** box, specify a start date for the schedule detail.

   b) To specify an end date for the schedule detail, select the **End date** check box, and then specify an end date for the schedule detail.

   NOTE: The detail will no longer apply to the schedule after the end date

7. Under **Tasks**, select the tasks that you want to run for the schedule detail. You can run one or multiple tasks in a single detail. The options are as follows:

   - **1. Perform Backup** — Starts a scheduled backup session.

     NOTE: If the schedule applies to a CDP backup, a full scan and backup of the items is performed once.

- **2. Enforce Retention** — Enforces the retention rules assigned to the backups.

NOTE: If the schedule applies to a CDP backup, the CDP process is suspended, retention is enforced, and a new CDP process is started.

- **3. Perform Validation** — Performs a scheduled validation of the backup data. Type the private and account encryption keys, and then click **OK**. To configure the validation options to be used for all backups using the backup schedule, click **>>**, and then do the following:
  - To validate only the latest generation of backup data for the selected backup, select the **Validate last generation only** check box.
  - To skip the validation of files that have been deleted from the source computer, select the **Exclude files deleted from source** check box.
  - To configure the schedule to resume validation from the point of interruption if the last scheduled validation did not finish, select the **Resume from previously interrupted location** check box.

NOTE: If the schedule applies to a CDP backup and validation is competed without errors, the CDP process is suspended and then resumed. If the validation process completes with errors, the CDP process is suspended and then restarted.

- **4. Perform BLM** — Requests the DS-System to copy a backup snapshot to the BLM Archiver. The default is for each BLM request to be added to the current archive package on the BLM Archiver. To configure the BLM options, click **>>**, and then do the following:
  - To use a new archive package, select the **Close archive package** check box, and then specify when the archive package will be closed. Once an archive package is closed, no new data will be added. Subsequent archiving requests will create a new archive package.
  - To allow the archive package to contain references to older archive packages, select the **Reference previous archive package(s)** check box. This can save space by removing data redundancy.
  - Under **Generations to include**, specify if you want the archive package to contain the latest generation or all generations.

NOTE: If the schedule applies to a CDP backup, the CDP process is suspended, BLM is performed, and then the CDP process is resumed.

- **Start LAN Scan Shares** — Starts scanning the LAN shares for statistical data. Since this can take a significant amount of time, this task is run last.

- **Clean Local-only Trash** — Starts a Clean Local-only Trash process on all local-only storage locations for the DS-Client.
- **Perform Replication** — Starts a replication process for any VM replication sets to which this schedule is assigned.

NOTE: Tasks 1-4 will run in that order on a backup. Other tasks will start immediately. If the schedule applies to a CDP backup, the DS-Client forces a full scan of all the items in the backup the next time the scheduled starts.

8. Click **Save**. Each new detail is automatically assigned a name, based on the frequency selected, and a number (e.g. daily:1, weekly:2).
9. Click **Close**.

3.2 Assigning a schedule to a backup

You can assign a schedule to a backup or remove a schedule that is assigned to an existing backup. Even though a backup schedule has a specific start time, the start time depends on the backup priority in the schedule.

NOTE: Only one backup schedule can be assigned to a backup at a time.

To assign a schedule to a backup:

1. On the **Backup Sets** tab, select the backup to which you want to assign a schedule.
2. On the **Sets** menu, point to **Backup Sets**, and then click **Properties**.
3. Click the **Schedule** tab.
4. Select **Scheduled**.

NOTE: To remove a schedule from a backup, select **Not scheduled**.

5. In the **Available schedules** box, select the schedule that you want to assign to the backup.

NOTE: If you are an administrator of backup operator you can create or edit a schedule by clicking **New** or **Edit**.

6. Click **OK**.

3.3 Viewing scheduled backups

You can view a calendar that displays the backups that are scheduled or performed. You can also view any schedules that overlap or errors that have occurred during the backup sessions. The numbers that appear in each cell represent the number of backup activities scheduled or performed in that period.

- **Bold (Scheduled only)** - The number of activities in the period exceeds the configured maximum concurrent activities set. The number in bold is the actual maximum concurrent amount allowed.
- **Light Green (Scheduled / Performed)** - A backup in the period overlaps with an Admin process.
- **Gray (Performed only)** - A backup in the period did not complete before the stop limit time.

The calendar changes depending on the selection. If you select all schedules, every active schedule layered on top of each other is displayed. If you select an individual schedule, only that schedule and any Admin processes is displayed. The color of a time cell represents the type of schedule that will run in that period:

- **Admin (Dark Blue)** - Schedule is a Daily or Weekly Admin.
- **Regular (Yellow)** - Schedule will run once during a fixed start and end period.
- **Recurring (Dark Green)** - Schedule is configured with a detail frequency that will run more than once during the scheduled period.
- **No End (Light Blue)** - Schedule is configured with no fixed end time.
- **Overlapped (Red)** - More than one schedule will run in the period.
- **Discontinued (White - Performed only)** - Schedule no longer applies.

To view schedule backups:

1. Click the **Backup Schedules** tab.
2. On the **Schedule** menu, click **Schedule Calendar**.
3. In the **Schedule(s)** box, select the schedule you want to view.
4. In the **Week starting** box, specify the week you want to view.
5. In the **Display interval** box, select the interval you want to view.
6. To display the schedule for a particular period, click the cell that contains the time. The **Description** section displays the details of the selected schedule.
7. To display processes that have run, under **Show**, click **Performed**. The numbers in the calendar reflect the actual number of backups at that time.
8. To display the backups that were backed up, click a time cell with a number. In the **Cell Details** section, you can browse all backups that ran.
9. Click **Close**.

3.4 Setting the priority of a scheduled backup

You can set the priority of a scheduled backup and limit the number of simultaneous backups the schedule will perform.

To set the priority of a schedule:

1. Click the **Backup Schedules** tab.
2. Right-click the schedule for which you want to set a priority, and then select **Set Priority**.
3. From the list of backups assigned to the schedule, select the backup you want to prioritize.
4. In the **Backup set priority** box, enter the priority of the selected backup. The number in the **#** column changes with the number field. The set will sort automatically by priority (lower number = higher priority).
5. To limit the number of backups that are run simultaneously by the schedule, select the **Schedule** check box, and then enter the number.

NOTE: The DS-Client database has an advanced configuration parameter called **MaxSessions** (Windows) and **MaxSession Number** (Linux) for maximum concurrent activities that affects the number of backups that can be scheduled at one time. For Grid DS-Clients, the limit is the sum of all the MaxSessions parameters from all running nodes.

---

6. Click **Save**.
7. Click **Close**.

3.5 Activating or suspending a schedule

By default, a schedule is active and the DS-Client performs the scheduled tasks based on the schedule details for all the backups that are currently assigned to the schedule. Active schedules appear in black on the Backup Schedules tab.

When a schedule is suspended, the DS-Client stops performing the scheduled tasks of a schedule for all the backups that are currently assigned to the schedule. Suspended schedules appear in gray on the Backup Schedules tab.

To activate a schedule:

1. Click the **Backup Schedules** tab.
2. Select the schedule that you want to activate.
3. On the **Schedule** menu, click **Activate**.

To suspend a schedule:

1. Click the **Backup Schedules** tab.
2. Select the schedule that you want to suspend.
3. On the **Schedule** menu, click **Suspend**.

4 Working with retention rules

A retention rule is an optional feature that allows you to implement granularity for backed up generations. For example, you might want to retain all generations from the previous day, one generation each day for a week, one generation each week for a month, one generation each month for a year, and one generation each year for 7 years. When using retention rules, you must know the nature of the backup data such as the number of generations and frequency of changes.

If you do not use a retention rule, your backup data remains online based on the maximum generation settings. This means the oldest generation of a file will be overwritten only when the configured maximum number of generations is reached. Generations are created in the DS-System online storage when the backup detects that a file has changed. Files that never change have only one generation.

After assigning a retention rule to a backup, you can enforce the retention rule on-demand or based on a schedule. When a retention rule is enforced, any data that does not qualify for retention is deleted.

When configuring a retention rule, consider the following:

- Ensure the retention rule works with the maximum number of generations for the backup. If the maximum number of generations is set to a low number (e.g. 7), the retention rule might not produce the intended result. because the oldest generations are likely to b overwritten by the backup process before any of the generations quality for deletion by the retention rule.
- Retention rules work best if the maximum generations parameter is configured to the maximum setting (9999) or a high number (e.g. 300). The retention rules help by deleting what you define to unnecessary and retaining online what you define to be critical.
- Due to the number of possible retention rule configurations, you should treat retention as if you are performing a manual deletion of data.

By default, enforcing a retention rule deletes all obsolete data from the DS-System online storage. However, a copy of the data can be sent to the BLM Archiver before it is removed completely from the DS-System online storage so you can effectively save a copy of every backup generation forever..

IMPORTANT: The system does not automatically delete backup data. This process must be performed by an authorized user. Apply caution when performing this process because data cannot be recovered after it has been deleted.

4.1 Configuring a retention rule

After a retention rule is configured, it can be assigned to a backup. When you enforce a retention rule on a backup, the DS-Client determines what data to retain in the DS-System online storage. If data qualifies for at least one of the keep-data options, it is retained even if it qualifies for deletion in another option. If data does not qualify for any keep-data options, it is considered obsolete data.

NOTE: The **Archive old data to BLM** and **Move obsolete data to BLM** options require configuration of the BLM Archiver. For more information, see Section 11.3, “Backup Lifecycle Management (BLM)”, on page 624.

To configure a retention rule:

1. Click the **Retention Rules** tab, and do one of the following:
   - To create a retention rule, on the **Retention** menu, click **New Retention Rule**.
   - To modify a retention rule, select the retention rule, on the **Retention** menu, click **Edit Retention Rule**.

   NOTE: To delete a retention rule, select the retention rule, on the **Retention** menu, click **Delete Retention Rule**.

2. Do the following:
   a) Under **Online and Local-Only retention**, select the type of retention rule you want to configure for data that is stored online in DS-System and data that is stored locally for Local-only backups. The options are as follows:
      - **Deletion of files removed from source / HSMed data** – Applies only to files that have been deleted from the source and data that has been moved by a third-party HSM/ILM solution to a remote location. This is the first rule that is applied when a retention rule is enforced.
      - **Time-based retention** – Applies time-based rules to determine what data to keep online. All other data is considered obsolete. For Online backups, this deletes data from the DS-System online storage. For Local-only backups, this deletes data from local storage.
      - **Archive old data to BLM (ignored for local-only backups**) – Sends a copy of the generations that are about to be deleted to the BLM Archiver. If this option is used with other retention rule types, it is applied last and only to the files that remain online after the other options have been applied.

b) To store the same number of generations of a backup file in the local storage directory that are stored in the DS-System online storage, under **Local Storage retention**, select the **Enable Local Storage retention (multiple generations)** check box.

NOTE: This option applies only to Online backups configured with the Use Local Storage option. When disabled, only the latest generation of a backup file is kept in the local storage directory.

---

c) If you are using component-based VSS-aware backups on a Windows DS-Client, under **Component data integration options for VSS-aware backup sets**, do the following:

- To delete files that are not referenced by any component, select the **Delete unreferenced files** check box.
- To delete incomplete components that are missing referenced files, select the **Delete incomplete components** check box.

NOTE: Unreferenced files and incomplete components are typically useless and should be removed. However, individual files can still be restored as pure files for troubleshooting purposes.

---

d) Click **Next**.

3. If you selected the **Deletion of files removed from source / HSMed data** option, do the following:

   a) To delete files from the backup source, select the **If files are removed from source** check box. In the **After** box, enter the amount of time that must pass before the file is deleted. In the **Keep generations** box, enter the number of generations of the file that you want to retain online.

   b) If you are using a third-party storage management (HSM) solution that migrates infrequently used files from the backup source and leaves a small placeholder or stub in its place, select the **If a placeholder/stub is detected on the source** check box, and the do one of the following:

   - To delete all file generations backed up prior to the placeholder or stub, select **Delete generations prior to the stub**. The latest placeholder or stub will be retained on the DS-System.

- To delete all generations that were backed up in an earlier session and are not a placeholder or stub, select **Delete non-stub generations prior to the stub**. This retains all generations that are placeholders or stubs.

NOTE: If the DS-Client detects that a placeholder or stub is created on the source, it assumes the file is already protected by the third-party solution and does not need to be stored online. Only the backup of the placeholder or stub will remain online.

c) Click **Next**.

4. If you selected the **Time-based retention** option, do the following:

a) In the **Keep most recent generations** box, enter the number of generations that you want to retain in the DS-System online storage. Any generations over this number will be deleted unless they qualify for another retention option.

NOTE: For Microsoft SQL Server database backups based on the Transaction Log Only database backup policy, you must specify a value of 0. For all other backup types, you can specify a value of 1 or higher.

b) To retain all generations that fall within a specific time period, select the **Keep all generation for the last** check box, and then enter the time period. Any generations outside the specified time period will be deleted unless they qualify for another retention option.

NOTE: For Microsoft SQL Server database backups based on the Transaction Log Only database backup policy, you must specify a time period.

c) To configure time-based retention options, click **Add**, and then do the following:

1. Under **Keep one generation**, select the interval for which you want to retain a generation. When this rule is enforced, the most recent generation from the interval is kept for as many intervals that can fit into the retention period. If you can specify the start date for a retention option, it will count backwards from that date by the specified interval.
2. In the **Retention option valid for last** box, enter the length of the retention period. At least one generation interval must fit into this retention period. If you select a retention option that spans a longer period, you should extend this value to at least match that period.
3. Click **OK**.

d) Click **Next**.

5. If you selected the **Archive old data to BLM (ignored for local-only backups)** option, do the following:

   a) To add an archive option, click **Add**, and then do the following:

      1. In the **Archive files older than** box, enter the time period after which you want to archive files. Online files older than the specified number of days will be pushed to the BLM Archiver.
      2. To archive all files, select **All Files**.
      3. To archive specific files, select **Specific files defined by the filtering rule**. To configure the file filtering rule, click **Add**.
      4. Click **OK**.

   b) To use only the backup time of a file to determine if it qualifies as old data, select the **Compare backup time only** check box. This means files that have not been modified for a long time will remain online until their last backup time qualifies them as old data.

   c) To archive special files, such as System State or the Services Databases, select the **Archive special files (i.e. System State files)** check box.

   d) To retain the latest generation of all special files (e.g. System State) online, select the **Do not archive latest generation of special files** check box. Select this option if the retention rule is being applied to any backup that is used for a Bare Metal Restore (BMR).

   e) Click **Next**.

NOTE: When files are archived they cannot be restored from the DS-System. The files are moved to the BLM Archiver and can only be written to a BLM restorable image if they need to be restored. If the last generation of a file is pushed, an archive stub (a small file containing only metadata) will be left in the DS-System online storage. This prevents the file from being backed up again by the DS-Client unless the source file is changed.

---

6. If you selected the **Enable Local Storage retention (multiple generations)** option, do the following:

a) In the **Keep all generations for** box, enter the time period for which you want to retain all generations in local storage.

b) To delete files removed from the source, select the **If files removed from source** check box. In the **After** box, enter the time period after which files that have been removed from the source will be deleted. In the **Keep generations** box, enter the number of generations you want to retain.

NOTE: Generations of a file that meet the criteria are kept in local storage. Everything else will be deleted from local storage.

---

c) Click **Next**.

7. Do the following:

a) In the **Name** box, type a name for the retention rule.

b) Under **Retention Option**, do one of the following:

- To delete all obsolete data when enforcing the retention rule, select **Delete obsolete data**.
- To move obsolete data to the BLM Archiver, select **Move obsolete data to BLM**.

NOTE: If the **Move obsolete data to BLM** option is not selected, obsolete data is permanently deleted and cannot be recovered.

---

c) To have the BLM Archiver create a new archive package every time data is sent, under **BLM Option**, select the **New Archive Package** check box.

NOTE: If you don't select this option, the archive request is added to the current archive package on the BLM Archiver. Archive packages are specific to a particular backup. Each BLM request is added to an archive package until it reaches a specified limit.

---

d) The **Summary** section displays the configured retention rule settings. To make corrections, click **Back**.

e) Click **Finish**.

4.2 Assigning a retention rule to a backup

You can assign a retention rule to a backup or remove a retention rule that is assigned to an existing backup. Retention rules apply only when they are enforced either on demand or via a schedule.

NOTE: If two-factor authentication is enabled on the DS-Client, you can assign a retention rule to an existing backup only if you are an authorized user listed in the two-factor authentication settings for the DS-Client. For more information on two-factor authentication, see Section 2.5, “Configuring the two-factor authentication settings”, on page 66.

To assign a retention rule to a backup:

1. On the **Backup Sets** tab, select the backup to which you want to assign a retention rule.
2. On the **Sets** menu, point to **Backup Sets**, and then click **Properties**.
3. Click the **Retention** tab.

   NOTE: If you are a DS-Client administrator, you can also click the **Retention Rules** tab, right-click the backup to which you want to assign the retention rule, and then click **Assign to Retention**.

4. Select **Use a specific Retention Rule**.

   NOTE: To remove a retention rule from a backup, select **No Retention Rule**.

5. Select the retention rule that you want to assign to the backup, and then click **OK**.
6. If two-factor authentication is enabled, in the **Authentication Code** box, type the authentication code that you have received from the DS-System, and then click **Validate**.

   NOTE: The authentication code is sent to the email address associated with the user account in the two-factor authentication settings for the DS-Client. The code is valid for two hours. To request an authentication code be resent, click **Resend**.

4.3 Enforcing a retention rule

The frequency at which a retention rule is applied should be always be considered. If you define a granular retention rule, such as time-based retention with rules for the daily, weekly, monthly, and yearly retention of online data from a long period of time, this type of retention works best when applied only once.

If you apply the retention again the next day, even if changes have been made in the past 24 hours and backed up, the other retention rules (weekly, monthly, yearly) will likely not capture data meeting the policy. By applying the rule only once, you can make it as granular as you want based on your knowledge of the online data.

Regular retention, such as weekly scheduled enforcement, is more effective with retention rules that do not contain rule intervals longer than the frequency of enforcement. This means if you enforce retention weekly, it is best not to have rules for intervals longer than a week. You must consider the frequency of data changes.

To enforce a retention rule:

1. Click the **Backup Sets** tab.
2. Select the backup on which you want to enforce retention.
3. On the **Retention** menu, click **Enforce Retention**.
4. When prompted to confirm that you want to enforce the retention rule, click **Yes**.

5 Working with backups

A backup consists of a list of items that need to be backed up and the settings that define how to perform the backup. The following backups are supported:

File System Backups	Windows	Linux	Mac
File System	✓		
File System (NAS, NFS, UNIX-SSH)		✓	
File System (NFS, UNIX-SSH)			✓
Permissions Only	✓	✓	✓
Cloud Backups	**Windows**	**Linux**	**Mac**
Google Workspace	✓		
Microsoft 365	✓		
Microsoft 365 Groups	✓		
Salesforce	✓		
Database Backups	**Windows**	**Linux**	**Mac**
IBM DB2		✓	
MariaDB	✓	✓	✓
Microsoft SQL Server (Classic or VSS-aware)	✓		
Oracle Database	✓	✓	
Oracle MySQL	✓	✓	✓
Oracle SBT		✓	
PostgreSQL		✓	✓
Email Backups	**Windows**	**Linux**	**Mac**
Microsoft Exchange Server (EWS)	✓		
Microsoft Outlook	✓		
Server Backups	**Windows**	**Linux**	**Mac**
Microsoft Exchange Server (VSS-aware)	✓		
Microsoft SharePoint Server (Classic or VSS-aware)	✓		
Virtual Machine Backups	**Windows**	**Linux**	**Mac**
Microsoft Hyper-V Server (Standalone or Cluster)	✓		
VMware vCenter Server	✓	✓	
VM Replication Sets	**Windows**	**Linux**	**Mac**
VMware vCenter Server Snapshot Replication	✓		

Table 1 Supported backup types

5.1 Backup types

You can create several types of backups for different purposes.

5.1.1 Online backups

Online backups allow you to perform backup and restore activities using the DS-System online storage. You must have a connection to a DS-System.

5.1.2 Self-contained backups

Self-contained backups allow you to perform backup and restore activities using only local storage. Data is stored locally on a local disk or UNC path. You can create up to five Self-contained backups with up to 10 GB of protected data. The stored data is compressed and only the latest generation of a file is protected.

Before creating a Self-contained backup, you must configure the local storage path. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

NOTE: You cannot convert a Self-contained backup to an Online backup. However, you can use the clone feature to duplicate it as a new Online backup. For more information, see Section 6.7, “Cloning a backup”, on page 546.

5.1.3 Local-only backups

Local-only backups are the same as Self-contained backups but do not have restrictions on the number of sets or capacity. Your service provider must enable the Local-only Capacity tool and assign a maximum storage amount for the DS-Client. Local-only backup data is protected from accidental or inadvertent deletion by a Safe Delete mechanism.

Data is stored locally on a local disk or UNC path. Stored data is compressed, but no master or delta processing is applied. The total amount of Local-only storage is allocated from the DS-System. There must be enough capacity available in the local storage path to accommodate the total amount of Local-only capacity licensed.

Before creating a Local-only backup, you must configure the local storage path. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

NOTE: You can convert a Local-only backup to an Online backup. For more information, see Section 6.8, “Converting a backup”, on page 547.

5.1.4 Instant recovery backups

Instant recovery backups allow you to save uncompressed and unencrypted backup data in its native format to a configured storage location called the instant recovery vault. Your service provider must enable the Local Storage and Local-only Capacity tools and assign a maximum storage amount for the DS-Client.

There are two instant recovery backup configurations.

- **Instant recovery backup type** — With this configuration, each time a backup is run, a new generation is stored in the instant recovery vault up to the maximum number of generations configured for the backup item.
- **Online backup type** with the **Save in instant recovery vault** option — With this configuration, data is backed up to both online storage and the instant recovery vault.

The following backup types support instant recovery:

- File System
- Microsoft Exchange Server (VSS-aware)
- Microsoft Hyper-V Server (VSS-aware)
- Microsoft SharePoint Server (VSS-aware)
- Microsoft SQL Server (VSS-aware)
- VMware vCenter Server

5.1.5 Statistical backups

Statistical backups allow you to generate statistical data on backup usage and trends before you perform actual backups. This allows you to estimate the initial backup size and the amount of data changes between backups to determine the duration of the initial backup of baseline data and subsequent backup sessions.

To perform a statistical backup, you do not need a customer account with a service provider because no backup data is transmitted. Only statistical data is gathered and stored in the DS-Client database during a Statistical backup session.

For best results, allow the backup to run on schedule or on demand to generate the statistical data. As a guideline, run the Statistical backup in your data environment for at least two weeks. The longer the period for which you run a Statistical backup, the more accurately the trend will be represented. You can use the DS-Client Load Summary, Storage Summary, and Report features to view the statistics generated.

NOTE: You cannot convert a Statistical backup to an Online backup.

5.2 Backup considerations

5.2.1 Changed block tracking (CBT)

Changed block tracking (CBT) is a feature that is supported for VMware vCenter Server backups. When CBT is enabled, the DS-Client attempts to reconfigure virtual machines to allow tracking of changed blocks of data. This can improve the speed of incremental backup activities, but can also slow down the virtual machine since it consumes additional resources.

When CBT is enabled, the first backup activity scans the virtual machine as follows:

- For thick disks, it scans the entire virtual machine disk.
- For thin disks, it scans only the space occupied by the disk.

Subsequent backup activities track the changes for the virtual machine files and only retrieve the blocks of data that have changed. These blocks are processed for master/delta generations and then sent to DS-System and/or local storage. If CBT fails or is not enabled, the DS-Client continues the incremental backup by reading all the data from the virtual machine disk.

5.2.2 Continuous data protection (CDP)

Continuous data protection (CDP) is a feature that continuously monitors the changes on a target server and backs up ongoing changes as soon as the changes are detected. It retains intermediate changes so you can recover data from a specific time.

CDP differs from a “point-in-time” backup and from replication or mirroring, which only keeps a snapshot of the latest image. You can enable CDP when creating or editing a backup. When CDP is enabled, the backup is triggered based on the detection of a change to a file on the backup source.

NOTE: Do not use CDP when performing an assisted delete, deleting a backup, or for disc/tape request operations.

CDP is available for the following backups:

- **File system (Windows or Linux)** – When configuring a File system backup with CDP, it is not necessary to select an entire server. You can select specific parts of a server, including any combination of share level, folder level, and file level filters. Extended regular expressions can be used to define complex selections.

  NOTE: CDP supports pure file system backup items only. System Status and Services Database are not supported.

- **Microsoft Exchange Server using EWS (Windows)** – When configuring a Microsoft Exchange Server backup (EWS) with CDP, you can select user accounts or individuals folders within the user accounts. Selecting individual emails with CDP enabled is not recommended. When an individually selected email is removed from its original location, it is not backed up.

NOTE: When using CDP, the Use Buffer, Pre-Scan, and Follow Junction Point options are not supported.

Before using the CDP option, do the following:

- Know your data environment. Statistical backups and LAN Storage Discovery can help you to assess your data environment. See Section 5.1.5, “Statistical backups”, on page 107 and Chapter 12, “Using LAN Storage Discovery Tool”.
- Consider the number of generations you want to maintain online. Normally, each change counts as a generation. The file change detection method depends on the operating system and backup kind. Backup frequency depends on the interval selected, which can be wide (up to many hours) or precise (down to the second-level).
- Ensure the system clocks on the DS-Client computer and the backup source computer are synchronized. CDP is a time-sensitive operation.
- For Microsoft Exchange Server (EWS) backups, ensure:
  - Autodiscover has been enabled on the Microsoft Exchange Server and the address Autodiscover provides is resolvable.
  - The internal network has a DNS server / hosts file configuration. This ensures the IP address of the Microsoft Exchange Server can be returned when the DS-Client attempts to connect to the Microsoft Exchange Server via the FQDN provided by the Autodiscover service.

After a CDP backup begins (on demand or scheduled), the session will continue to run unless explicitly stopped, for example, by the scheduled end time or by the user. The DS-Client continuously monitors the ongoing changes on the target backup server throughout the entire backup session.

As soon as the DS-Client detects a change, it immediately backs up the changes to the DS-System. On-demand and scheduled CDP backups use the reconnection settings from the DS-Client. CDP stops when one of the following events occurs:

- An on-demand stop is triggered.
- The scheduled time limit is reached.
- CDP is suspended by conflicting activities like, scheduled retention, validation, and BLM.
- CDP reaches the limit of retry connection attempts to the DS-System.
- Other unexpected stop conditions (exceptions, failed to connect to target, etc.)

5.2.3 DS-Client buffer

DS-Client buffer is a temporary storage location on the DS-Client computer that can be used to speed up backup and restore operations.

When using the DS-Client buffer, backup files are transferred to the buffer location at LAN speed and then transferred to the DS-System at DS-System connection speed. This minimizes the time the LAN must support the additional backup or restore traffic. This is useful if the DS-Client connection to the DS-System is much slower than its connection to the LAN.

The DS-Client deletes all files from the DS-Client buffer after each activity regardless of whether the operation was performed successfully.

DS-Client buffer can also provide temporary storage as the database dump location, which avoids the need for extra disk capacity on network servers.

NOTE: For information on how to change the DS-Client buffer location, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

For best results when using the DS-Client buffer, do the following:

- Ensure the buffer storage location is configured to use a folder other than a system temp folder. For example, C:\DS-Client\Buffer.
- Ensure sufficient disk capacity is available on the drive containing the DS-Client buffer folder. For example, to support the backup activities for SharePoint Online data, the DS-Client buffer must provide the storage capacity calculated based on the SharePointOnlineBackupBatchSize (Miscellaneous) and MaxSessions (Performance) advanced configuration parameters, and the size of files that are larger than 500 MB in SharePoint Online:

  ```
  SharePointOnlineBackupBatchSize x MaxSessions x Largest file size x Number of threads
  ```

  For example:

  - SharePointOnlineBackupBatchSize value = 1

- MaxSessions value = 1
- Largest files greater than 500 MB on your SharePoint Online Server = 15 GB
- Number of threads = 4 (MaxThreads for backup or MaxRestoreThreads for restore)

In this example, the DS-Client buffer capacity required for SharePoint Online backup activities is 1 item per batch x 1 session x 15 GB x 4 threads = 60 GB.

- Ensure the buffer storage location supports the same structure as the source. For example, if DS-Client buffer is on a Linux DS-Client, the maximum number of subfolders allowed within a single folder is 32767.
- Do not select the Use Buffer option for backups that have data on the DS-Client computer. The Use Buffer option copies files to the DS-Client buffer. From there, the files are processed for backup by the DS-Client. If the DS-Client buffer folder is part of a backup, issues can occur because the backup might catch a loop that reads the same directories being copied for backup.
- To maximize speed, provide credentials for all backups to access the DS-Client buffer folder. DS-Client buffer is also used by activities that access the DS-Client database to create temporary files for bulk insert. If a backup is not assigned credentials to create, delete, read, and write files in the DS-Client buffer folder, bulk insert operations will fail and a regular insert is used instead.

5.2.4 Block-level resume

Backups that use the DS-Client buffer can benefit from the block-level resume feature, which allows a backup to continue from the last successful file block backed up if the DS-System has received at least 100 MB of compressed data.

The benefit increases with the size of the file being backed up. If the backup process is interrupted, DS-Client attempts to reconnect a specified number of times to resume the backup. Without the block-level resume feature, a backup of a large file that is interrupted restarts from the beginning of the file.

The following backups support the block-level resume feature:

- File system (Windows, Linux, Mac)
- Permissions only (Windows, Linux, Mac)
- Email (Windows)
- IBM DB2 (Linux)
- Microsoft Exchange Server (Windows)
- Microsoft SQL Server (Windows)
- Oracle Database (Windows, Linux)
- Oracle MySQL (Windows, Linux, Mac)
- PostgreSQL database (Linux, Mac)

5.2.5 Database backup policies

Choosing a database backup policy method depends primarily on the size of the database and the frequency of the backups. For example, a user who needs to back up a 1 TB database might not be able to perform a backup every hour using the **Full dump always** policy. However, the backup might be able to accommodate an incremental or differential dump every hour.

- **Full dump: Always** – Performs a full dump (VSS snapshot) of the database. There are no restrictions on the number of backups. However, a dump time is required for each backup.
- **Full dump: Plus differential** – Performs a full dump (VSS snapshot) of the database on first backup followed by differential backups until another full backup is required. Differential backups contain all changes to the database since the last full dump, which means less data is transmitted from the source to the DS-Client over the LAN. This could result in possible storage savings on the DS-System because of the size of the differential generations. Even when a Full dump is required, the DS-Client still processes “incremental forever” and sends only the delta changes to the DS-System. Only one backup can back up the target database to maintain a record of differential backups.
- **Full dump: Plus incremental** – Performs a full dump (VSS snapshot) of the database on first backup followed by incremental backups until another full backup is required. Incremental backups contain all changes to the database since the last full dump, which means less data is transmitted from the source to the DS-Client over the LAN. This could result in possible storage savings on the DS-System because of the size of the incremental generations. Even when a Full dump is required, the DS-Client still processes “incremental forever” and sends only the delta changes to the DS-System. Only one backup can back up the target database to maintain a record of incremental backups. For Microsoft SQL Server backups, the database must be configured with the full or bulk_logged recovery model, which means that more processing will occur and more data and logs will be stored.
- **Transaction Log Only (Microsoft SQL Server)** – Only transaction logs are backed up. This offers more granular control by allowing you to restore the target database to a specific point in time. Shorter backup times are required because the backup of transaction logs require less data transfer. Requires two steps in the restore process: (1) restore a full database using a Microsoft SQL Server (Classic or VSS-aware) backup, and (2) restore transaction logs from a Microsoft SQL Server (Classic) backup.
- **Backup using VSS (Separate VSS-aware backup)** – Data is backed up using the Microsoft VSS (Volume Shadow Copy Service), which avoids the dump time for the data. This means more data is transmitted between the source and the DS-Client.

5.2.6 Pre/Post backup processes

Pre/Post processes allow you to specify a command to run before (Pre) and/or after the execution (Post) of a backup.

Services normally lock associated files while the Windows computer is running (i.e. these files will not be backed up). Examples of services are DHCP and WINS. You can back up Windows services using the Pre/Post processes.

The steps that apply to Windows service backups are identical to file system backups. However, you must know the specific file path of the service files.

5.2.7 Performance

DS-Client is designed to perform unattended scheduled backups of a single computer or an entire LAN. To maximize performance, consider the following:

- **Operating system** – Running the DS-Client on the latest supported operating system will boost backup speed.
- **CPU and memory** – Since the DS-Client performs compression and encryption during the backup process, it is CPU-intensive. Use the Load Summary Report to determine CPU and memory use during backups. If it is very high, consider a more powerful CPU and more memory for the DS-Client.
- **Multiprocessors** – The DS-Client is designed to scale on SMP systems, when installed on Windows. Running the DS-Client on such a system provides large performance boosts when compared with a single CPU configuration.
- **Dedicated database** – The DS-Client uses a database to store backup logs. When using the DS-Client in a LAN configuration that can exceed a few hundred thousand backup files, the database update and retrieval speed can affect backup performance significantly. Use a dedicated computer for the DS-Client database to provide faster performance.
- **LAN connections** – When running the DS-Client on a powerful system, LAN connections can become a bottleneck. Provide a faster LAN connection to significantly improve the backup speed.
- **Scheduled backups** – Scheduling too many backups simultaneously can increase backup time due to over utilization of CPU and memory resources. Use the Load Summary Report to optimize CPU and memory utilization.

5.2.8 Backup wizard

The Backup Wizard walks you through the process of creating a backup. Many pages in the Backup Wizard are shared by different backup types and correspond to a tab in the Backup Properties dialog box (see Table 2).

Page in the Backup Wizard	Tab in Backup Properties
Choose the kind of backup	**N/A**
Select the computer Select the backup source (Linux)	**N/A**
Select share & path for the database / data dump	**N/A**
Specify the protocol for dumping the database (Linux DS-Client)	**N/A**
Select directories/files for backup	**Items**
Specify backup item options	**Items**
Specify backup options	**Options**
Specify advanced options (Windows DS-Client)	**Advanced Options**
Specify backup performance options	**Performance**
Specify notification options	**Notification**
Choose a retention rule for the backup	**Retention**
Choose a schedule for the backup	**Schedule**
Choose the name for the backup	**Set Info**

Table 2 Corresponding tabs in the Set Properties dialog box

The following sections list the pages in the Backup Wizard and provide links to the relevant topics for each backup type.

5.2.8.1 Selecting the type of backup

Select the type of backup you want to create.

Backup	Sections
File System	Section 5.4.1.1, “Selecting the type of backup”, on page 142
Local file system	Section 5.5.2.1, “Selecting the type of backup”, on page 163
NAS file system	Section 5.5.3.1, “Selecting the type of backup”, on page 172
NFS file system	Section 5.5.4.1, “Selecting the type of backup”, on page 179
UNIX-SSH file system	Section 5.5.5.1, “Selecting the type of backup”, on page 186
E-mail - Microsoft Exchange Server (EWS)	Section 5.6.3.1, “Selecting the type of backup”, on page 204

Table 3 Selecting the type of backup

Backup	Sections
Email - Microsoft Outlook	Section 5.6.5.1, “Selecting the type of backup”, on page 214
Google Workspace	Section 5.7.2.1, “Selecting the type of backup”, on page 229
IBM DB2	Section 5.8.6.1, “Selecting the type of backup”, on page 242
Microsoft 365	Section 5.10.7.1, “Selecting the type of backup”, on page 278
Microsoft 365 Groups	Section 5.11.5.1, “Selecting the type of backup”, on page 292
Microsoft Exchange Server (VSS-aware)	Section 5.12.1.1, “Selecting the type of backup”, on page 299
Microsoft Hyper-V Server (VSS-aware)	Section 5.13.3.1, “Selecting the type of backup”, on page 330
Microsoft SharePoint Server (Classic)	Section 5.14.1.1, “Selecting the type of backup”, on page 349
Microsoft SharePoint Server (VSS-aware)	Section 5.15.5.1, “Selecting the type of backup”, on page 359
Microsoft SQL Server (Classic)	Section 5.16.1.1, “Selecting the type of backup”, on page 382
Microsoft SQL Server (VSS-aware)	Section 5.17.2.1, “Selecting the type of backup”, on page 400
Oracle database	Section 5.18.6.1, “Selecting the type of backup”, on page 423
Oracle MySQL database	Section 5.19.4.1, “Selecting the type of backup”, on page 443
Oracle SBT database	Section 5.20.3.1, “Selecting the type of backup”, on page 462
Permissions only	Section 5.21.1.1, “Selecting the type of backup”, on page 467
PostgreSQL database	Section 5.22.5.1, “Selecting the type of backup”, on page 481
Salesforce	Section 5.23.3.1, “Selecting the type of backup”, on page 491
VMware vCenter Server	Section 5.24.4.1, “Selecting the type of backup”, on page 513
VM replication	Section 7.4.1, “Selecting the kind of VM replication set”, on page 567

Table 3 Selecting the type of backup

5.2.8.2 Selecting the email server type

Select the type of email server you want to back up.

Topics	Sections
Selecting the Email server type - Microsoft Exchange Server (EWS)	Section 5.6.3.2, “Selecting the E-mail Server type”, on page 204
Selecting the Email server type - Microsoft Outlook (DS-MLR)	Section 5.6.5.2, “Selecting the E-mail server type”, on page 214

Table 4 Selecting the email server type

5.2.8.3 Selecting the cloud service type

Select the type of cloud service you want to back up.

Topics	Sections
Selecting the cloud service type - Google Workspace backup	Section 5.7.2.2, “Selecting the cloud service type”, on page 229
Selecting the cloud service type - Microsoft 365 backup	Section 5.10.7.2, “Selecting the type of cloud service”, on page 278
Selecting the cloud service type - Salesforce backup	Section 5.23.3.2, “Selecting the type of cloud service”, on page 491

Table 5 Selecting the cloud service type

5.2.8.4 Selecting the VSS-aware backup type

Select the type of VSS-aware backup you want to create.

Backup sets	Sections
Microsoft Exchange Server (VSS-aware)	Section 5.12.1.2, “Selecting the VSS-aware backup type”, on page 299
Microsoft Hyper-V Server (VSS-aware)	Section 5.13.3.2, “Selecting the VSS-aware backup type”, on page 330
Microsoft SharePoint Server (VSS-aware)	Section 5.15.5.1, “Selecting the type of backup”, on page 359
Microsoft SQL Server (VSS-aware)	Section 5.17.2.1, “Selecting the type of backup”, on page 400

Table 6 Selecting the VSS-aware backup type

5.2.8.5 Selecting the backup source

Select the backup source containing the databases you want to back up.

Backup sets	Sections
File system	Section 5.4.1.2, “Selecting the backup source”, on page 143
Local file system	Section 5.5.2.2, “Selecting the backup source”, on page 163
NAS file system	Section 5.5.3.2, “Selecting the backup source”, on page 172
NFS file system	Section 5.5.4.2, “Selecting the backup source”, on page 180
UNIX-SSH file system	Section 5.5.5.2, “Selecting the backup source”, on page 186
Email - Microsoft Exchange Server (EWS)	Section 5.6.3.3, “Selecting the backup source”, on page 204
Email - Microsoft Outlook	Section 5.6.5.3, “Selecting the backup source”, on page 214
Google Workspace	Section 5.7.2.3, “Selecting a logon mode”, on page 230
IBM DB2	Section 5.8.6.2, “Selecting the backup source”, on page 243
Microsoft 365	Section 5.10.7.3, “Selecting the server”, on page 278
Microsoft Exchange Server (VSS-aware)	Section 5.12.1.3, “Selecting the backup source”, on page 299
Microsoft Hyper-V Server (VSS-aware)	Section 5.13.3.3, “Selecting the backup source”, on page 330
Microsoft SharePoint Server (Classic)	Section 5.14.1.2, “Selecting the backup source”, on page 349
Microsoft SharePoint Server (VSS-aware)	Section 5.15.5.2, “Selecting the backup source”, on page 359
Microsoft SQL Server (Classic)	Section 5.16.1.2, “Selecting the backup source”, on page 382
Microsoft SQL Server (VSS-aware)	Section 5.17.2.2, “Selecting the backup source”, on page 400
Oracle database	Section 5.18.6.2, “Selecting the Oracle server”, on page 423
Oracle MySQL database (Windows)	Section 5.19.4.2, “Selecting the MySQL server”, on page 443
Oracle MySQL database (Linux or Mac)	Section 5.19.5.2, “Selecting the backup source”, on page 451
Oracle SBT database	Section 5.20.3.2, “Selecting the backup source”, on page 462
Permissions only	Section 5.21.1.2, “Selecting the backup source”, on page 468

Table 7 Selecting the backup source

Backup sets	Sections
PostgreSQL database	Section 5.22.5.2, “Selecting the backup source”, on page 481
Salesforce	Section 5.23.3.3, “Selecting the server”, on page 491
VMware vCenter Server	Section 5.24.4.2, “Selecting the backup source”, on page 513
VM replication	Section 7.4.3, “Specifying the source server”, on page 568

Table 7 Selecting the backup source

5.2.8.6 Selecting the protocol for dumping the database

Select a protocol to make a copy or dump of the database.

Backup sets	Sections
IBM DB2	Section 5.8.6.3, “Selecting the protocol for dumping the database”, on page 243
Oracle database	Section 5.18.7.3, “Selecting the protocol for the database dump”, on page 431

Table 8 Selecting the protocol for dumping database file

5.2.8.7 Selecting the share and path for the database dump

Select the location where you want to save the database dump.

Backup sets	Sections
Microsoft SharePoint Server (VSS-aware)	Section 5.14.1.3, “Selecting the share and path for the database dump”, on page 349
Microsoft SQL Server (Classic)	Section 5.16.1.3, “Selecting the share & path for the database dump”, on page 383
Oracle database	Section 5.18.6.3, “Selecting the database dump options”, on page 424
Oracle MySQL database	Section 5.19.4.3, “Selecting the database dump options”, on page 444

Table 9 Selecting the share and path for the database dump

5.2.8.8 Selecting the backup items

Select the items on the selected backup source you want to back up.

Backup sets	Sections
File system	Section 5.4.1.3, “Selecting the backup items”, on page 144
Local file system	Section 5.5.2.3, “Selecting the backup items”, on page 163
NAS	Section 5.5.3.3, “Selecting the backup items”, on page 173
NFS	Section 5.5.4.3, “Selecting the backup items”, on page 180
UNIX-SSH	Section 5.5.5.3, “Selecting the backup items”, on page 188
Email - Microsoft Exchange Server (EWS)	Section 5.6.3.4, “Selecting the backup items”, on page 205
Email - Microsoft Outlook	Section 5.6.3.4, “Selecting the backup items”, on page 205
Google Workspace	Section 5.7.2.4, “Selecting the backup items”, on page 231
IBM DB2 database	Section 5.11.5.4, “Selecting the backup items”, on page 294
Microsoft 365	Section 5.10.7.4, “Selecting the backup items”, on page 279
Microsoft 365 Groups	Section 5.11.5.4, “Selecting the backup items”, on page 294
Microsoft Exchange Server (VSS-aware)	Section 5.12.1.5, “Selecting the components to back up”, on page 300
Microsoft Hyper-V Server (VSS-aware)	Section 5.13.3.4, “Selecting the backup items”, on page 331
Microsoft SharePoint Server (Classic)	Section 5.14.1.4, “Selecting the backup items”, on page 349
Microsoft SharePoint Server (VSS-aware)	Section 5.15.5.3, “Selecting the backup items”, on page 359
Microsoft SQL Server (Classic)	Section 5.16.1.4, “Selecting the backup items”, on page 384
Microsoft SQL Server (VSS-aware)	Section 5.17.2.3, “Selecting the components to back up”, on page 401
Oracle database	Section 5.18.6.4, “Selecting the database(s) for backup”, on page 424
Oracle MySQL database	Section 5.19.4.4, “Selecting the database(s) to back up”, on page 444
Oracle SBT database	Section 5.20.3.3, “Selecting the backup items”, on page 462
Permissions only	Section 5.21.1.3, “Selecting the backup items”, on page 469

Table 10 Selecting the backup items

Backup sets	Sections
PostgreSQL database	Section 5.22.5.3, “Selecting the backup items”, on page 482
Salesforce	Section 5.23.3.4, “Selecting the backup items”, on page 492
VMware vCenter Server	Section 5.24.4.3, “Selecting the backup items”, on page 513
VM replication	Section 7.4.4, “Selecting the items to replicate”, on page 568

Table 10 Selecting the backup items

5.2.8.9 Selecting the backup item options

Select the options for the items you want to back up.

Backup sets	Sections
File system	Section 5.4.1.4, “Selecting the backup item options”, on page 145
Local file system	Section 5.5.2.4, “Selecting the backup item options”, on page 164
NAS	Section 5.5.3.4, “Selecting the backup item options”, on page 173
NFS	Section 5.5.4.4, “Selecting the backup item options”, on page 181
UNIX-SSH	Section 5.5.5.4, “Selecting the backup item options”, on page 189
Email - Microsoft Exchange Server (EWS)	Section 5.6.3.5, “Selecting the backup item options”, on page 205
Email - Microsoft Outlook	Section 5.6.5.5, “Selecting the backup item options”, on page 215
Google Workspace	Section 5.7.2.5, “Selecting the backup item options”, on page 232
IBM DB2 database	Section 5.8.6.6, “Selecting the backup item options”, on page 244
Microsoft 365	Section 5.10.7.5, “Selecting the backup item options”, on page 280
Microsoft 365 Groups	Section 5.11.5.5, “Selecting the backup item options”, on page 295
Microsoft Exchange Server (VSS-aware)	Section 5.12.1.6, “Selecting the backup item options”, on page 301
Microsoft Hyper-V Server (VSS-aware)	Section 5.13.3.5, “Selecting the backup item options”, on page 331
Microsoft SharePoint Server (Classic)	Section 5.14.1.5, “Selecting the backup item options”, on page 350

Table 11 Selecting the backup item options

Backup sets	Sections
Microsoft SharePoint Server (VSS-aware)	Section 5.15.5.4, “Selecting the backup item options”, on page 360
Microsoft SQL Server (Classic)	Section 5.16.1.5, “Selecting the backup item options”, on page 385
Microsoft SQL Server (VSS-aware)	Section 5.17.2.4, “Selecting the backup item options”, on page 401
Oracle database	Section 5.18.6.5, “Selecting the backup item options”, on page 424
Oracle MySQL database	Section 5.19.4.5, “Selecting the backup item options”, on page 444
Oracle SBT database	Section 5.20.3.4, “Selecting the backup item options”, on page 463
Permissions only	Section 5.21.1.4, “Selecting the backup item options”, on page 470
PostgreSQL database	Section 5.22.5.3, “Selecting the backup items”, on page 482
Salesforce	Section 5.23.3.5, “Selecting the backup item options”, on page 492
VMware vCenter Server	Section 5.24.4.4, “Selecting the backup item options”, on page 514
VM replication	Section 7.4.5, “Specifying replication item options”, on page 568

Table 11 Selecting the backup item options

5.2.8.10 Selecting the backup options

Select the options for the backup.

Backup sets	Sections
File system	Section 5.4.1.5, “Selecting the backup options”, on page 145
Local file system	Section 5.5.2.5, “Selecting the backup options”, on page 165
NAS	Section 5.5.3.5, “Selecting the backup options”, on page 174
NFS	Section 5.5.4.5, “Selecting the backup options”, on page 181
UNIX-SSH	Section 5.5.5.5, “Selecting the backup options”, on page 189
Email - Microsoft Exchange Server (EWS)	Section 5.6.3.6, “Selecting the backup options”, on page 206
Email - Microsoft Outlook	Section 5.6.3.6, “Selecting the backup options”, on page 206

Table 12 Selecting the backup options

Backup sets	Sections
Google Workspace	Section 5.7.2.6, “Selecting the backup options”, on page 232
IBM DB2 database	Section 5.8.6.7, “Selecting the backup options”, on page 245
Microsoft 365	Section 5.10.7.6, “Selecting the backup options”, on page 280
Microsoft 365 Groups	Section 5.11.5.6, “Selecting the backup options”, on page 295
Microsoft Exchange Server (VSS-aware)	Section 5.12.1.7, “Selecting the backup options”, on page 302
Microsoft Hyper-V Server (VSS-aware)	Section 5.13.3.6, “Selecting the backup options”, on page 331
Microsoft SharePoint Server (Classic)	Section 5.14.1.6, “Selecting the backup options”, on page 350
Microsoft SharePoint Server (VSS-aware)	Section 5.15.5.5, “Selecting the backup options”, on page 360
Microsoft SQL Server (Classic)	Section 5.16.1.6, “Selecting the backup options”, on page 386
Microsoft SQL Server (VSS-aware)	Section 5.17.2.5, “Selecting the backup options”, on page 402
Oracle database	Section 5.18.6.6, “Selecting the backup options”, on page 425
Oracle MySQL database	Section 5.19.4.6, “Selecting the backup options”, on page 444
Oracle SBT database	Section 5.20.3.5, “Selecting the backup options”, on page 463
Permissions only	Section 5.21.1.5, “Selecting the backup options”, on page 470
PostgreSQL database	Section 5.22.5.5, “Selecting the backup options”, on page 482
Salesforce	Section 5.23.3.6, “Selecting the backup options”, on page 492
VMware vCenter Server	Section 5.24.4.5, “Selecting the backup options”, on page 514
VM replication	Section 7.4.8, “Specifying the replication set options”, on page 570

Table 12 Selecting the backup options

5.2.8.11 Selecting the advanced options

Configure the advanced options for the backup.

Backup sets	Sections
File system	Section 5.4.1.6, “Selecting the advanced options”, on page 148
Permissions Only	Section 5.21.1.6, “Selecting the advanced options”, on page 472

Table 13 Selecting the advanced options

5.2.8.12 Selecting the backup performance options

Select the performance options for the backup.

Backup sets	Sections
File system	Section 5.4.1.7, “Specifying backup performance options”, on page 150
Microsoft Exchange Server (VSS-aware)	Section 5.12.1.8, “Specifying backup performance options”, on page 304
Microsoft Hyper-V Server (VSS-aware)	Section 5.13.3.7, “Specifying backup performance options”, on page 333
Microsoft SharePoint Server (VSS-aware)	Section 5.15.5.6, “Specifying backup performance options”, on page 362
Microsoft SQL Server (Classic)	Section 5.16.1.7, “Specifying backup performance options”, on page 388
Microsoft SQL Server (VSS-aware)	Section 5.17.2.6, “Specifying backup performance options”, on page 404
Oracle database	Section 5.18.6.7, “Specifying backup performance options”, on page 426

Table 14 Selecting the backup performance options

5.2.8.13 Selecting the notification options

Select the notification options for the backup.

Backup sets	Sections
File system	Section 5.4.1.8, “Selecting the notification options”, on page 151
Local file system	Section 5.5.2.6, “Selecting the notification options”, on page 167
NAS	Section 5.5.3.6, “Selecting the notification options”, on page 176
NFS	Section 5.5.4.6, “Selecting the notification options”, on page 183

Table 15 Selecting the notification options

Backup sets	Sections
UNIX-SSH	Section 5.5.5.6, “Selecting the notification options”, on page 192
Email - Microsoft Exchange Server (EWS)	Section 5.6.3.7, “Selecting the notification options”, on page 207
Email - Microsoft Outlook	Section 5.6.3.7, “Selecting the notification options”, on page 207
Google Workspace	Section 5.7.2.7, “Specifying notification options”, on page 233
IBM DB2 database	Section 5.8.6.9, “Specifying notification options”, on page 246
Microsoft 365	Section 5.10.7.7, “Specifying notification options”, on page 281
Microsoft Exchange Server (VSS-aware)	Section 5.12.1.9, “Selecting the notification options”, on page 305
Microsoft Hyper-V Server (VSS-aware)	Section 5.13.3.8, “Selecting the notification options”, on page 334
Microsoft SharePoint Server (Classic)	Section 5.14.1.7, “Selecting the notification options”, on page 351
Microsoft SharePoint Server (VSS-aware)	Section 5.15.5.7, “Selecting the notification options”, on page 363
Microsoft SQL Server (Classic)	Section 5.16.1.8, “Selecting the notification options”, on page 389
Microsoft SQL Server (VSS-aware)	Section 5.17.2.7, “Selecting the notification options”, on page 405
Oracle database	Section 5.18.6.8, “Selecting the notification options”, on page 427
Oracle MySQL database	Section 5.19.4.7, “Selecting the notification options”, on page 446
Oracle SBT database	Section 5.20.3.6, “Specifying notification options”, on page 464
Permissions only	Section 5.21.1.7, “Selecting the notification options”, on page 473
PostgreSQL database	Section 5.22.5.6, “Specifying notification options”, on page 484
Salesforce	Section 5.23.3.8, “Specifying notification options”, on page 494
VMware vCenter Server	Section 5.24.4.6, “Selecting the notification options”, on page 516
VM replication	Section 7.4.9, “Specifying notification options”, on page 570

Table 15 Selecting the notification options

5.2.8.14 Selecting a retention rule

Assign a retention rule to the backup.

Backup sets	Sections
File system	Section 5.4.1.9, “Assigning a retention rule”, on page 152
Local file system	Section 5.5.2.7, “Assigning a retention rule”, on page 168
NAS	Section 5.5.3.7, “Assigning a retention rule”, on page 177
NFS	Section 5.5.4.7, “Assigning a retention rule”, on page 184
UNIX-SSH	Section 5.5.5.7, “Assigning a retention rule”, on page 193
Email - Microsoft Exchange Server (EWS)	Section 5.6.3.8, “Assigning a retention rule”, on page 209
Email - Microsoft Outlook	Section 5.6.5.8, “Assigning a retention rule”, on page 219
Google Workspace	Section 5.7.2.8, “Assigning a retention rule”, on page 234
IBM DB2 database	Section 5.8.6.10, “Assigning a retention rule”, on page 248
Microsoft 365	Section 5.10.7.8, “Assigning a retention rule”, on page 282
Microsoft Exchange Server (VSS-aware)	Section 5.12.1.10, “Assigning a retention rule”, on page 306
Microsoft Hyper-V Server (VSS-aware)	Section 5.13.3.9, “Assigning a retention rule”, on page 336
Microsoft SharePoint Server (Classic)	Section 5.14.1.8, “Assigning a retention rule”, on page 352
Microsoft SharePoint Server (VSS-aware)	Section 5.15.5.8, “Assigning a retention rule”, on page 364
Microsoft SQL Server (Classic)	Section 5.16.1.9, “Assigning a retention rule”, on page 390
Microsoft SQL Server (VSS-aware)	Section 5.17.2.8, “Assigning a retention rule”, on page 407
Oracle database	Section 5.18.7.8, “Assigning a retention rule”, on page 435
Oracle MySQL database	Section 5.19.5.7, “Assigning a retention rule”, on page 455
Oracle SBT database	Section 5.20.3.7, “Assigning a retention rule”, on page 465
Permissions only	Section 5.21.1.8, “Assigning a retention rule”, on page 475
PostgreSQL database	Section 5.22.5.7, “Assigning a retention rule”, on page 485

Table 16 Selecting a retention rule

Backup sets	Sections
Salesforce	Section 5.23.3.9, “Assigning a retention rule”, on page 495
VMware vCenter Server	Section 5.24.4.7, “Assigning a retention rule”, on page 518

Table 16 Selecting a retention rule

5.2.8.15 Selecting a schedule

Assign a schedule to the backup.

Backup sets	Sections
File system	Section 5.4.1.10, “Assigning a schedule”, on page 153
Local file system	Section 5.5.2.8, “Assigning a schedule”, on page 168
NAS	Section 5.5.3.8, “Assigning a schedule”, on page 177
NFS	Section 5.5.4.8, “Assigning a schedule”, on page 185
UNIX-SSH	Section 5.5.5.8, “Assigning a schedule”, on page 193
Email - Microsoft Exchange Server (EWS)	Section 5.6.3.9, “Assigning a schedule”, on page 209
Email - Microsoft Outlook	Section 5.6.5.9, “Assigning a schedule”, on page 219
Google Workspace	Section 5.7.2.9, “Assigning a schedule”, on page 234
IBM DB2 database	Section 5.8.6.11, “Assigning a schedule”, on page 248
Microsoft 365	Section 5.10.7.9, “Assigning a schedule”, on page 282
Microsoft 365 Groups	Section 5.11.5.7, “Assigning a schedule”, on page 295
Microsoft Exchange Server (VSS-aware)	Section 5.12.1.11, “Assigning a schedule”, on page 307
Microsoft Hyper-V Server (VSS-aware)	Section 5.13.3.10, “Assigning a schedule”, on page 336
Microsoft SharePoint Server (Classic)	Section 5.14.1.9, “Assigning a schedule”, on page 353
Microsoft SharePoint Server (VSS-aware)	Section 5.15.5.9, “Assigning a schedule”, on page 364
Microsoft SQL Server (Classic)	Section 5.16.1.10, “Assigning a schedule”, on page 390
Microsoft SQL Server (VSS-aware)	Section 5.17.2.9, “Assigning a schedule”, on page 407

Table 17 Selecting a schedule

Backup sets	Sections
Oracle database	Section 5.18.7.9, “Assigning a schedule”, on page 435
Oracle MySQL database	Section 5.19.5.8, “Assigning a schedule”, on page 456
Oracle SBT database	Section 5.20.3.8, “Assigning a schedule”, on page 465
Permissions only	Section 5.21.1.9, “Assigning a schedule”, on page 475
PostgreSQL database	Section 5.22.5.8, “Assigning a schedule”, on page 485
Salesforce	Section 5.23.3.10, “Assigning a schedule”, on page 495
VMware vCenter Server	Section 5.24.4.8, “Assigning a schedule”, on page 518
VM replication	Section 7.4.10, “Assigning a schedule”, on page 572

Table 17 Selecting a schedule

5.2.8.16 Naming the backup

Specify a name for the backup and configure the backup type.

Backup sets	Sections
File system	Section 5.4.1.11, “Naming the backup”, on page 153
Local file system	Section 5.5.2.9, “Naming the backup”, on page 169
NAS	Section 5.5.3.9, “Naming the backup”, on page 178
NFS	Section 5.5.4.9, “Naming the backup”, on page 185
UNIX-SSH	Section 5.5.5.9, “Naming the backup”, on page 194
Email - Microsoft Exchange Server (EWS)	Section 5.6.3.10, “Naming the backup”, on page 209
Email - Microsoft Outlook	Section 5.6.3.10, “Naming the backup”, on page 209
Google Workspace	Section 5.7.2.10, “Naming the backup”, on page 235
IBM DB2 database	Section 5.8.6.12, “Naming the backup”, on page 248
Microsoft 365	Section 5.10.7.10, “Naming the backup”, on page 283
Microsoft 365 Groups	Section 5.11.5.8, “Naming the backup”, on page 296

Table 18 Naming the backup

Backup sets	Sections
Microsoft Exchange Server (VSS-aware)	Section 5.12.1.12, “Naming the backup”, on page 307
Microsoft Hyper-V Server (VSS-aware)	Section 5.13.3.11, “Naming the backup”, on page 336
Microsoft SharePoint Server (Classic)	Section 5.14.1.10, “Naming the backup”, on page 353
Microsoft SharePoint Server (VSS-aware)	Section 5.15.5.10, “Naming the backup”, on page 364
Microsoft SQL Server (Classic)	Section 5.16.1.11, “Naming the backup”, on page 391
Microsoft SQL Server (VSS-aware)	Section 5.17.2.10, “Naming the backup”, on page 407
Oracle database	Section 5.18.6.11, “Naming the backup”, on page 428
Oracle MySQL database	Section 5.19.4.10, “Naming the backup”, on page 448
Oracle SBT database	Section 5.20.3.9, “Naming the backup”, on page 466
Permissions only	Section 5.21.1.10, “Naming the backup”, on page 475
PostgreSQL database	Section 5.22.5.9, “Naming the backup”, on page 486
Salesforce	Section 5.23.3.11, “Naming the backup”, on page 496
VMware vCenter Server	Section 5.24.4.9, “Naming the backup”, on page 518

Table 18 Naming the backup

5.2.8.17 Selecting the Oracle server

Select the Oracle server you want to back up.

Topics	Sections
Oracle database (Windows)	Section 5.18.6.2, “Selecting the Oracle server”, on page 423
Oracle database (Linux)	Section 5.18.7.2, “Selecting the backup source”, on page 430

Table 19 Selecting the Oracle server

5.3 Restore considerations

5.3.1 Restoring a specific generation of a file

In some instances, you might want to restore an older version of a backed up file. For example, if you discover that files after a certain date are corrupted or you want to restore files from a specific backup session. The number of generations stored in the DS-System online storage is determined by the maximum generations setting configured for the backup and by the retention rule (if assigned) that is enforced on the backup. When it reaches the limit, the oldest generation is overwritten during the next backup.

If Continuous Data Protection (CDP) is enabled for a backup, each item is backed up when a change is detected. Multiple generations of the item are created and stored online within a backup session. Each generation is identified by its backup time, not by the backup session. The best uses for maximum generations are:

- When there are no retention rules, but online storage size is a concern.
- For CDP backups, where files are constantly changing and backed up and you want to control the number of generation in the DS-System online storage.

All cumulative backups (on-demand and scheduled) retain up to the configured maximum generations. If a low number of maximum generations is configured for a scheduled backup, the number of generation that is retained online might not be what you expect if you run an on-demand backup.

For example, you create a backup with maximum generations set to 7, and schedule the backup to run daily. Assuming all backup files change daily, you expect one generation for each day. However, if you run an on-demand backup, it might disrupt the pattern, giving you 2 generations from the same day, and restorable generations going back 6 days instead of 7.

NOTE: Maximum generations allow passive delete, which means the oldest generation is overwritten if necessary in the DS-System online storage. If you have BLM Archiver configured, you can archive the oldest generation before it is deleted.

5.3.2 Pre/Post restore processes

The DS-Client can perform a specific activity on the DS-Client computer or on the restore destination computer before and/or after a restore operation. For example, you might want to stop the Windows service before the restore and to restart it after the restore.

Similar to the Pre/Post process for backups, the Pre/Post options are automatically applied before and after each subsequent restore of the backup.

5.3.3 Restoring data to an alternate location

You can restore backup data to an alternate location other than the original source location. When you restore data to an alternate location, you must specify the path of the new location. An alternate location can be another disk drive on the same computer, another share on a different computer, or another server on a different network (with some restrictions).

You can select multiple items that are from the same drive and share a common path on the source to restore them to an alternate location. When you do that, the common path will be displayed as part of the restore destination path, which you can shorten using the **Truncate** option.

When restoring to an alternate location, the security of restored items at the destination location might not resemble the security of those items during backup. This can occur when users and/or groups that were included in the security descriptor of an item during backup cannot be resolved in the restore destination environment. For example, when users or groups have been deleted or when data is restored to a different domain. Users and groups are stored as security identifiers (SIDs) and remain in the security descriptor of the restored items. If the host cannot match the SIDs against valid names, it will not display them as valid names but only as SIDs, which look like this: S-1-5-21-1614895754-299502267-682003330-1139.

When restoring to an alternate location while truncating the destination path to the maximum: If you select the dot file (.) under the last directory that is being eliminated from the path, DS-Client will restore the security of that last directory to the destination directory in the alternate location.

5.3.4 Restoring system state and services database

When restoring Windows backups, you can select the following items:

- System State
- Services Database

You might want to recover the System State if a user account was accidentally deleted from a Windows computer. Since user accounts are generated with a unique Security ID, the only way to recover the user account is to restore a backed up System State containing the deleted user account.

For this type of restore, ensure the **Use Buffer** option is not selected as a restore method. Issues can result from restoring the Windows System State and Service Database via the DS-Client buffer.

NOTE: The System State contains information that is critical to your computer and applications. Use caution when using this feature.

5.3.5 Restoring transaction logs only (Microsoft SQL)

The Transaction Log Only database backup policy for a Microsoft SQL Server (Classic) backup allows you to restore a target database to a specific point in time, which offers granular control of the restore process and requires less transfer time.

This solution requires the collaboration of two backups:

- A Microsoft SQL Server (Classic or VSS-aware) backup based on the *Full dump: Always* database backup policy.
- A Microsoft SQL Server (Classic) backup based on the *Transaction Log Only* database backup policy.

When using a Microsoft SQL Server backup based on the Transaction Log Only database backup policy, you must do the following:

- Ensure the integrity of the sequence of the transaction logs in relation to the Full database backups performed by the other Microsoft SQL Server backup. Transaction logs can only be restored to the target database after the database has first been restored in full.
- Select the **Keep all generations for the last [specific period] retention** option and specify the period.
- Set the **Keep most recent generations time-based retention** setting to 0. The backup of transaction logs updates the same files over time and does not result in multiple generations. The files become obsolete after every full dump.

To restore transaction logs to a target database, you must do the following:

1. Restore the full database using the Microsoft SQL Server backup configured with the *Full dump: Always* database backup policy and leave the target database in RESTORING mode.
2. Restore the transaction logs to the target database using the Microsoft SQL Server (Classic) backup configured with the *Transaction Log Only* database backup policy.

NOTE: When performing the backup and restore, you must specify the source Microsoft SQL Server in the same format (computer name or IP address).

5.3.6 File-Level Restore (FLR)

File-level restore (FLR) is supported for Microsoft Hyper-V Server (VSS-aware) and VMware vCenter Server backups. FLR is supported on Windows NTFS and Linux Ext4 file systems installed on one of the following partition IDs for the target virtual machine:.
:

Partition ID	Description
00h	Empty partition.
05h	Extended partition.
07h	Installable file system.
83h	Native Linux file system.
8Eh	Single disk Linux LVM

Table 20 Supported partition types

For the single disk Linux LVM partition type, FLR only supports the Linear or Mirror logical volumes. You can verify the type of the LVM volume with the "`lvdisplay -m`" command. FLR does not support any type of mixed mapping. For example, if you have a logical volume using both Linear and Stripe mapping.

FLR can fail on corrupted partitions. To view the configuration of the disk partitions on the target backup virtual machine, use an application that provides disk configuration information, such as the Windows Disk Management tool or the Red Hat Disk Utility tool, to verify the following:

- Partition name, type, and size
- File system type
- Bootable and primary partitions

NOTE: For an unsupported partition type, FLR shows an empty partition with the name starting with "Unsupported ... partition ...".

FLR is not supported for the following:

- BLM or disc/tape restores.
- Instant recovery backups.
- Local-only Microsoft Hyper-V Server (VSS-aware) backups.
- Self-contained backups on Windows DS-Clients.
- System DLL files. In some cases, the size of files might be displayed as zero.
- Remote locations through NAS, UNIX-SSH, or NFS on Linux DS-Clients. FLR only restores to the local machine on which the DS-Client is running.

5.3.7 Restoring VSS-aware backup components

Each VSS-aware component (database or virtual machine) is represented by the component metadata, which is a file that includes the component and an entry for each file that belongs to the component. The metadata contains the following:

- File ID
- Generation ID
- Backup time
- Full path (folder and file name)

Metadata information is used by the applications and processes in different ways:

- DS-Client and DS-System use a combination of the File ID and Generation ID to identify the backed up component generation. The DS-Client saves this metadata in its database for use during activities like restore, delete, and retention. Synchronization is responsible for synchronizing them with the corresponding online file.
- BLM Archiver uses the full path and backup time to identify the backed up component generation. If a component generation is included on a BLM restorable image, the image must include all the component generation's referenced files.
- Retention, delete, BLM requests, and disc/tape requests work at the component level.
- Validation works at the individual backup file level.
- Restore works at both the component level and individual file level.

NOTE: A component generation is considered complete if all its referenced contents exist. Otherwise it is considered an incomplete component and its files are unreferenced files.

The component data integration metadata is backed up in separate files with the VSS-aware backup in the same way as the data file, except it is not encrypted because the DS-System and BLM Archiver must parse the metadata without knowing the encryption keys.

Incomplete component generations can exist to allow individual file restores from the incomplete component. They are not visible in the restore tree for VSS Restore, only for File Restore.

Files backed up in an incomplete component generation can be referenced by later generations of the same component to avoid backing up unchanged files again.

You can configure the backup to clean these types of files with the **Delete unreferenced files** and **Delete incomplete components** retention rule options. For more information, see Chapter 4, "Working with retention rules".

5.3.8 Transmitted amount discrepancies

During a restore, the amount of data received can differ from the transmitted amount recorded in the backup log. This can occur for two reasons:

- During an incremental, differential, or CBT backup, the amount of data transmitted is usually smaller than the actual size of the item. A reduction of transmitted data is also noticeable when a file is saved as a common file during backup. In these cases, the amount of data received during restore can be greater than the transmitted amount recorded in the backup log.
- DS-Client sends information such as file name and size along with a file to be stored on the DS-System during backup. This additional information is not sent during a restore, decreasing the data transfer amount by about 50 bytes for each file.

5.3.9 Restore Wizard

The Restore Wizard walks you through the process of restoring a backup. Many of the pages in the Restore Wizard are shared by the different backup types.

The following sections list the pages in the Restore Wizard and provide links to the relevant topics for each backup type.

5.3.9.1 Selecting the restore method

Select a method to restore the backup.

Backups	Sections
Microsoft Exchange Server (VSS-aware) - VSS restore	Section 5.12.2.1, “Selecting the restore method”, on page 310
Microsoft Exchange Server (VSS-aware) - File restore	Section 5.12.3.1, “Selecting the restore method”, on page 314
Microsoft Exchange Server (VSS-aware) - Granular restore	Section 5.12.4.1, “Selecting a restore method”, on page 319
Microsoft Hyper-V Server (VSS-aware) - VSS restore	Section 5.13.4.1, “Selecting a restore method”, on page 338
Microsoft Hyper-V Server (VSS-aware) - File restore	Section 5.13.5.1, “Selecting the restore method”, on page 342
Microsoft Hyper-V Server (VSS-aware) - File level restore	Section 5.13.6.1, “Selecting the restore method”, on page 346
Microsoft SharePoint Server (VSS-aware) - VSS restore	Section 5.15.6.1, “Selecting the restore method”, on page 367
Microsoft SharePoint Server (VSS-aware) - File restore	Section 5.15.7.1, “Selecting the restore method”, on page 371
Microsoft SharePoint Server (VSS-aware) - Granular restore	Section 5.15.8.1, “Selecting a restore method”, on page 376

Table 21 Selecting the restore method

Backups	Sections
Microsoft SQL Server (VSS-aware) - Database restore	Section 5.17.3.1, “Selecting the restore method”, on page 410
Microsoft SQL Server (VSS-aware) - File restore	Section 5.17.4.1, “Selecting the restore method”, on page 414
Salesforce - Table level restore	Section 5.23.4.1, “Selecting the restore method”, on page 497
Salesforce - Granular restore	Section 5.23.5.1, “Selecting a restore method”, on page 503

Table 21 Selecting the restore method

5.3.9.2 Selecting the items to restore

Select the items you want to restore.

Backups	Sections
File system	Section 5.4.2.1, “Selecting the restore items”, on page 155
Local file system	Section 5.5.6.1, “Selecting the restore items”, on page 195
NAS	Section 5.5.6.1, “Selecting the restore items”, on page 195
NFS	Section 5.5.6.1, “Selecting the restore items”, on page 195
UNIX-SSH	Section 5.5.6.1, “Selecting the restore items”, on page 195
Email - Microsoft Exchange Server (EWS)	Section 5.6.4.1, “Selecting the restore items”, on page 211
Email - Microsoft Outlook	Section 5.6.4.1, “Selecting the restore items”, on page 211
Google Workspace	Section 5.7.3.1, “Selecting the restore items”, on page 237
IBM DB2 database	Section 5.8.7.1, “Selecting the restore items”, on page 250
Microsoft 365	Section 5.10.8.1, “Selecting the restore items”, on page 284
Microsoft 365 Groups	Section 5.11.6.1, “Selecting the restore items”, on page 297
Microsoft Exchange Server (VSS-aware) - VSS restore	Section 5.12.2.2, “Selecting the restore items”, on page 310
Microsoft Exchange Server (VSS-aware) - File restore	Section 5.12.3.2, “Selecting the restore items”, on page 315
Microsoft Exchange Server (VSS-aware) - Granular restore	Section 5.12.4.2, “Selecting the restore items”, on page 319
Microsoft Hyper-V Server (VSS-aware) - VSS restore	Section 5.13.4.2, “Selecting the restore items”, on page 338

Table 22 Selecting the items to restore

Backups	Sections
Microsoft Hyper-V Server (VSS-aware) - File restore	Section 5.13.5.2, “Selecting the restore items”, on page 343
Microsoft Hyper-V Server (VSS-aware) - File level restore	Section 5.13.6.2, “Selecting the restore items”, on page 346
Microsoft SharePoint Server (Classic)	Section 5.14.2.1, “Selecting the restore items”, on page 355
Microsoft SharePoint Server (VSS-aware) - VSS restore	Section 5.15.6.2, “Selecting the restore items”, on page 367
Microsoft SharePoint Server (VSS-aware) - File restore	Section 5.15.7.2, “Selecting the restore items”, on page 371
Microsoft SharePoint Server (VSS-aware) - Granular restore	Section 5.15.8.2, “Selecting the restore items”, on page 376
Microsoft SQL Server (Classic)	Section 5.16.2.1, “Selecting the restore items”, on page 393
Microsoft SQL Server (VSS-aware) - Database restore	Section 5.17.3.2, “Selecting the restore items”, on page 410
Microsoft SQL Server (VSS-aware) - File restore	Section 5.17.4.2, “Selecting the restore items”, on page 415
Oracle database	Section 5.18.8.3, “Selecting the restore items”, on page 438
Oracle MySQL database	Section 5.19.6.1, “Selecting the restore items”, on page 458
Permissions only	Section 5.21.2.1, “Selecting the restore items”, on page 477
PostgreSQL database	Section 5.22.6.1, “Selecting the restore items”, on page 488
Salesforce	Section 5.23.4.2, “Selecting the restore items”, on page 498
Salesforce - Table level restore	Section 5.23.4.3, “Selecting the table(s) to restore”, on page 499
Salesforce - Items restore	Section 5.23.6.2, “Selecting the database to restore”, on page 506
VMware vCenter Server	Section 5.24.5.1, “Selecting the restore items”, on page 520

Table 22 Selecting the items to restore

5.3.9.3 Selecting the restore destination

Select the destination location where to restore the data.

Backups	Sections
File system	Section 5.4.2.2, “Selecting the restore location”, on page 158
Local file system, NAS, NFS, UNIX-SSH	Section 5.5.6.2, “Selecting the restore location”, on page 197
Email - Microsoft Exchange Server (EWS)	Section 5.6.4.2, “Selecting the restore location”, on page 212
Email - Microsoft Outlook	Section 5.6.6.2, “Selecting the restore location”, on page 223
Google Workspace	Section 5.7.3.2, “Selecting the restore location”, on page 238
IBM DB2 database	Section 5.8.7.2, “Selecting the restore location”, on page 251
Microsoft 365	Section 5.10.8.2, “Selecting the restore location”, on page 286
Microsoft 365 Groups	Section 5.11.6.2, “Selecting the restore location”, on page 298
Microsoft Exchange Server (VSS-aware) - VSS restore	Section 5.12.2.3, “Selecting the restore location”, on page 311
Microsoft Exchange Server (VSS-aware) - File restore	Section 5.12.3.3, “Selecting the restore location”, on page 316
Microsoft Exchange Server (VSS-aware) - Granular restore	Section 5.12.4.3, “Selecting the restore location”, on page 320
Microsoft Hyper-V Server (VSS-aware) - VSS restore	Section 5.13.4.3, “Selecting the restore location”, on page 339
Microsoft Hyper-V Server (VSS-aware) - File restore	Section 5.13.5.3, “Selecting the restore location”, on page 344
Microsoft Hyper-V Server (VSS-aware) - File-level restore	Section 5.13.6.3, “Selecting the restore location”, on page 347
Microsoft SharePoint Server (Classic)	Section 5.14.2.2, “Selecting the restore location”, on page 356
Microsoft SharePoint Server (VSS-aware) - VSS restore	Section 5.15.6.3, “Selecting the restore location”, on page 368
Microsoft SharePoint Server (VSS-aware) - File restore	Section 5.15.7.3, “Selecting the restore location”, on page 372
Microsoft SharePoint Server (VSS-aware) - Granular restore	Section 5.15.8.3, “Selecting the restore location”, on page 377
Microsoft SQL Server (Classic)	Section 5.16.2.2, “Selecting the restore location”, on page 395
Microsoft SQL Server (VSS-aware) - Database restore	Section 5.17.3.3, “Selecting the restore location”, on page 411
Microsoft SQL Server (VSS-aware) - File restore	Section 5.17.4.3, “Selecting the restore location”, on page 416

Table 23 Selecting the restore destination

Backups	Sections
Oracle database	Section 5.18.8.4, “Selecting the database restore location”, on page 439
Oracle MySQL database	Section 5.19.6.2, “Selecting the restore location”, on page 459
Permissions only	Section 5.21.2.2, “Selecting the restore location”, on page 478
PostgreSQL database	Section 5.22.6.2, “Selecting the restore location”, on page 489
Salesforce - Table level restore	Section 5.23.4.4, “Selecting the restore location”, on page 500
Salesforce - Granular restore	Section 5.23.5.3, “Selecting the restore location”, on page 504
VMware vCenter Server	Section 5.24.5.4, “Selecting the restore location”, on page 523

Table 23 Selecting the restore destination

5.3.9.4 Selecting the performance options

Select the performance options for the restore.

Backups	Sections
File system	Section 5.4.2.3, “Selecting the performance options (Windows)”, on page 159
Microsoft Exchange Server (VSS-aware) - VSS restore	Section 5.12.2.4, “Selecting the performance options”, on page 312
Microsoft Exchange Server (VSS-aware) - File restore	Section 5.12.3.4, “Selecting the performance options”, on page 316
Microsoft Exchange Server (VSS-aware) - Granular restore	Section 5.12.4.4, “Selecting the performance options”, on page 321
Microsoft Hyper-V Server (VSS-aware) - VSS restore	Section 5.13.4.4, “Selecting the performance options”, on page 340
Microsoft Hyper-V Server (VSS-aware) - File restore	Section 5.13.5.4, “Selecting the performance options”, on page 345
Microsoft SharePoint Server (VSS-aware) - VSS restore	Section 5.15.6.4, “Selecting the performance options”, on page 369
Microsoft SharePoint Server (VSS-aware) - File restore	Section 5.15.7.4, “Selecting the performance options”, on page 373
Microsoft SharePoint Server (VSS-aware) - Granular restore	Section 5.15.8.4, “Selecting the performance options”, on page 377
Microsoft SQL Server (Classic)	Section 5.16.2.3, “Selecting the performance options”, on page 396
Microsoft SQL Server (VSS-aware) - Database restore	Section 5.17.3.4, “Selecting the performance options”, on page 412

Table 24 Selecting the performance options

Backups	Sections
Microsoft SQL Server (VSS-aware) - File restore	Section 5.17.4.4, “Selecting the performance options”, on page 417
Oracle database	Section 5.18.8.5, “Selecting the performance options”, on page 440

Table 24 Selecting the performance options

5.3.9.5 Selecting the restore options

Select the restore options.

Backups	Sections
File system	Section 5.4.2.4, “Selecting the restore options”, on page 159
Local file system, NAS, NFS, UNIX-SSH	Section 5.5.6.3, “Selecting the restore options”, on page 199
Email - Microsoft Exchange Server (EWS)	Section 5.6.4.3, “Selecting the restore options”, on page 213
Email - Microsoft Outlook	Section 5.6.6.4, “Selecting the restore options”, on page 224
Google Workspace	Section 5.7.3.3, “Selecting the restore options”, on page 240
IBM DB2 database	Section 5.8.7.3, “Selecting the restore options”, on page 252
Microsoft 365	Section 5.10.8.3, “Selecting the restore options”, on page 287
Microsoft 365 Groups	Section 5.11.6.3, “Selecting the restore options”, on page 298
Microsoft Exchange Server (VSS-aware) - VSS restore	Section 5.12.2.5, “Selecting the restore options”, on page 313
Microsoft Exchange Server (VSS-aware) - File restore	Section 5.12.3.5, “Selecting the restore options”, on page 317
Microsoft Exchange Server (VSS-aware) - Granular restore	Section 5.12.4.12, “Selecting the emails to restore”, on page 325
Microsoft Hyper-V Server (VSS-aware) - VSS restore	Section 5.13.4.5, “Selecting the restore options”, on page 341
Microsoft SharePoint Server (Classic)	Section 5.14.2.3, “Selecting the restore options”, on page 356
Microsoft SharePoint Server (VSS-aware) - VSS restore	Section 5.15.6.5, “Selecting the restore options”, on page 370
Microsoft SharePoint Server (VSS-aware) - File restore	Section 5.15.7.5, “Selecting the restore options”, on page 374
Microsoft SharePoint Server (VSS-aware) - Granular restore	Section 5.15.8.5, “Selecting the restore options”, on page 378
Microsoft SQL Server (Classic)	Section 5.16.2.4, “Selecting the restore options”, on page 396

Table 25 Selecting the restore options

Backups	Sections
Microsoft SQL Server (VSS-aware) - Database restore	Section 5.17.3.5, “Selecting the restore options”, on page 413
Microsoft SQL Server (VSS-aware) - File restore	Section 5.17.4.5, “Selecting the restore options”, on page 418
Oracle database	Section 5.18.8.6, “Selecting the restore options”, on page 441
Oracle MySQL database	Section 5.19.6.3, “Selecting the restore options”, on page 460
Permissions only	Section 5.21.2.3, “Selecting the restore options”, on page 479
PostgreSQL database	Section 5.22.6.3, “Selecting the restore options”, on page 489
Salesforce - Table level restore	Section 5.23.4.5, “Selecting the restore options”, on page 501
Salesforce - Granular restore	Section 5.23.5.4, “Selecting the restore options”, on page 505
VMware vCenter Server	Section 5.24.5.5, “Selecting the restore options”, on page 524

Table 25 Selecting the restore options

5.3.9.6 Selecting the reason for the restore

Select the reason for this restore.

Backups	Sections
File system	Section 5.4.2.5, “Selecting the reason for the restore”, on page 161
Local file system, NAS, NFS, UNIX-SSH	Section 5.5.6.4, “Selecting the reason for the restore”, on page 200
Email - Microsoft Exchange Server (EWS)	Section 5.6.4.4, “Selecting the reason for the restore”, on page 213
Email - Microsoft Outlook	Section 5.6.6.5, “Selecting the reason for the restore”, on page 225
Google Workspace	Section 5.7.3.4, “Selecting the reason for the restore”, on page 240
IBM DB2 database	Section 5.8.7.4, “Selecting the reason for the restore”, on page 253
Microsoft 365	Section 5.10.8.4, “Selecting the reason for the restore”, on page 287
Microsoft 365 Groups	Section 5.11.6.4, “Selecting the reason for the restore”, on page 298
Microsoft Exchange Server (VSS-aware) - VSS restore	Section 5.12.2.6, “Selecting the reason for the restore”, on page 314
Microsoft Exchange Server (VSS-aware) - File restore	Section 5.12.3.6, “Selecting the reason for the restore”, on page 318

Table 26 Selecting the reason for the restore

Backups	Sections
Microsoft Exchange Server (VSS-aware) - Granular restore	Section 5.12.4.6, “Selecting the reason for the restore”, on page 322
Microsoft Hyper-V Server (VSS-aware) - VSS restore	Section 5.13.4.6, “Selecting the reason for the restore”, on page 341
Microsoft Hyper-V Server (VSS-aware) - File restore	Section 5.13.5.5, “Selecting the reason for the restore”, on page 345
Microsoft Hyper-V Server (VSS-aware) - File-level restore	Section 5.13.6.4, “Selecting the reason for the restore”, on page 348
Microsoft SharePoint Server (Classic)	Section 5.14.2.4, “Selecting the reason for the restore”, on page 356
Microsoft SharePoint Server (VSS-aware) - VSS restore	Section 5.15.6.6, “Selecting the reason for the restore”, on page 370
Microsoft SharePoint Server (VSS-aware) - File restore	Section 5.15.7.6, “Selecting the reason for the restore”, on page 375
Microsoft SharePoint Server (VSS-aware) - Granular restore	Section 5.15.8.6, “Selecting the reason for the restore”, on page 378
Microsoft SQL Server (Classic)	Section 5.16.2.5, “Selecting the reason for the restore”, on page 397
Microsoft SQL Server (VSS-aware) - Database restore	Section 5.17.3.6, “Selecting the reason for the restore”, on page 413
Microsoft SQL Server (VSS-aware) - File restore	Section 5.17.4.6, “Selecting the reason for the restore”, on page 419
Oracle database	Section 5.18.8.7, “Selecting the reason for the restore”, on page 441
Oracle MySQL database	Section 5.19.6.4, “Selecting the reason for the restore”, on page 461
Permissions only	Section 5.21.2.4, “Selecting the reason for the restore”, on page 480
PostgreSQL database	Section 5.22.6.4, “Selecting the reason for the restore”, on page 490
Salesforce - Table level restore	Section 5.23.4.6, “Selecting the reason for the restore”, on page 502
Salesforce - Granular restore	Section 5.23.5.5, “Selecting the reason for the restore”, on page 505
VMware vCenter Server	Section 5.24.5.6, “Selecting the reason for the restore”, on page 525

Table 26 Selecting the reason for the restore

5.4 File system backups (Windows)

You can back up and restore individual files, folders, or drives at various levels of the tree structure in a local file system on a Windows computer.

You can also perform a backup of NAS (Network Attached Storage) devices via snapshots. DS-Client backs up data from a snapshot it creates using a dedicated API from the NAS vendor. When the backup is finished, the snapshot is deleted.

NOTE: Only CIFS shares of volumes with the NTFS security type are currently supported by the Windows DS-Client.

Before creating a File system backup, consider the following:

- For NAS volumes, ensure the volume configuration option that enables accessing the snapshot file for CIFS when browsing the NetApp volume is enabled. Otherwise, the DS-Client will not be able to access the snapshot.
- The Windows DS-Client supports backing up file shares for SMB protocols that are supported and enabled by the host Windows operating system. Enabling SMB 1.0 is not advised for security reasons.
- To back up files encrypted with Encrypting File System (EFS) when the DS-Client and source machine are not in the same domain, the DS-Client must be running under an account with matching name and password with a full administrator account on the source machine

NOTE: If the DS-Client and source machine are in the same domain and the DS-Client is running under a domain account or a local administrator account under the same conditions as a non-domain configuration, the backup works.

5.4.1 Creating a File system backup

This section describes how to create a File system backup on Windows.

5.4.1.1 Selecting the type of backup

1. On the **Sets** menu, click **New Backup Set**.
2. Select **File System**, and then click **Next**.

5.4.1.2 Selecting the backup source

1. Select the computer containing the files you want to back up.The **Path** box displays the network path of the item selected in the tree.

   NOTE: DS-Client Computer represents the local DS-Client computer. For NAS devices, type the IP address or host name in the Path box.

2. To provide the credentials for the selected computer, select the **Ask for Network Credentials** check box. You will be prompted to enter a valid user name and password for the selected computer.

   NOTE: You must connect to the computer using an Administrator or equivalent account.

3. To use the DS-Client service account credentials to connect to the local DS-Client computer, select the **Use DS-Client Account** check box.

   NOTE: This option is available only when you select DS-Client Computer. You must be logged in using an Administrator or equivalent account.

4. To perform a backup of a NAS device, select the **Ask for NAS API credentials** check box and do the following:

   a) In the **NAS Type** box, select the NAS device type. Only NetApp is currently supported.

   b) In the **API Protocol** box, select the protocol for accessing the API. The protocol must be enabled on the NAS device.

   c) In the **Port Number** box, enter the port number for accessing the API. The port must be open on the NAS device.

   d) In the **User Name** and **Password** boxes, type the user name and password of a user who has permission to execute API commands on the NAS device. This is typically a member of the Administrators group.

      NOTE: To browse for an encrypted key file containing the user credentials, click **[...]**. If the file is valid, you must enter the correct key to unlock the credentials stored in the file.

   e) Click **OK**.

5. Click **Next**.

5.4.1.3 Selecting the backup items

1. To add an item, select the item, and then click **Add**. For NAS devices, select the CIFS share.

   NOTE: You can add only one item at a time. Subdirectories are included by default. To exclude subdirectories, clear the Include SubDirs check box.

2. To exclude an item when its parent folder is selected for backup, select the item, and then click **Exclude**.
3. To exclude an item using regular expressions, select the item, and then click **RegEx**.

   NOTE: Regular expressions provide more specific filtering than the exclude function. For example, you can use regular expressions to exclude individual file names or patterns. Use this option only if you are familiar with the syntax.

4. To add specific files from a folder, select the folder from which you want to add the files, and then click **Files**. Select the file(s) that you want to add, and then click **Add**.
5. To search for files that match a certain criteria, in the **Filter** box, type the file pattern you want to search for in the selected folder. For example, *.doc will search for all the files with the doc file extension.

   NOTE: For a Windows file system, you can add special backup items such as System State (including Registry) and Services Database.

6. To modify a regular expression, select the regular expression, and then click **Modify**.
7. To remove an item from the list, select the item, and then click **Remove**.

   NOTE: Removing an item will not remove previous backups of that item. To remove previously backed-up data, you must use the Delete function.

8. Click **Next**.

5.4.1.4 Selecting the backup item options

1. To configure the maximum generations for a backup item that will be stored online, double click the **Max Gen** cell, and then enter the value.
2. To back up the file permissions for an item, select the item, and then select the **Backup permissions** check box.
3. To back up the streams of data associated with an item, select the item, and then select the **Backup streams** check box.

NOTE: The configured options for the backup item appear as follows: P = Backup permissions, S = Backup streams.

---

4. Click **Next**.

5.4.1.5 Selecting the backup options

1. Configure the options for the backup. The options are as follows:
   - **Use buffer** – Copies files to the DS-Client buffer to free up the backup source as fast as possible. The DS-Client then sends the files from the DS-Client buffer to the DS-System. This option cannot be configured if CDP is enabled. For more information, see Section 5.2.7, “Performance”, on page 113.
   - **Detailed log** – Records all files that are backed up in the Activity Log. For more information, see Section 8.1, “Viewing the Activity Log”, on page 578.
   - **Initial backup** – Uses the Initial Backup feature for the first backup. To configure the initial backup path, click **[>>]**. For more information, see Section 11.1.1, “Configuring the initial backup path”, on page 618.
   - **Disable common files** – Excludes the backup files from common file storage reduction. This means duplicate files will be encrypted and backed up individually, thereby potentially increasing the stored size.

     NOTE: This feature must be activated for your DS-Client by your service provider. You can only enable this option when creating the backup. This option cannot be changed afterwards.

   - **Continuous data protection** – Enables continuous data protection (CDP) for the backup. To configure the CDP settings, click **[>>]**, and then do the following:

a) In the **File Change Detection** box, **Windows Built-in File Monitoring** is automatically selected and cannot be changed.

b) To specify the minimum interval the DS-Client must wait before backing up a changed item or file, select **Do not back up more often than**, and then enter the interval and unit of measurement. You can set a longer interval if you do not want to back up changes frequently or a shorter interval if you want the backup of changes to be more granular.

c) To specify the minimum interval the DS-Client must wait before backing up a changed item or file after detecting that it has not changed, select **Backup if file stops changing for**, and then enter the interval and unit of measurement. This option is intended for data that you know changes frequently.

d) Select the scheduled activities that will suspend the CDP backup process. The options are **Retention**, **BLM**, and **Validation**.

e) Click **OK**. For more information, see Section 5.2.2, “Continuous data protection (CDP)”, on page 108.

- **Stop on errors** – Stops a backup process when the number of errors reaches the specified value. A value of 0 means the DS-Client does not stop a backup process regardless of the number of errors.

NOTE: You can configure the default setting using the **MaxErrors** advanced configuration parameter. For more information, see Section 2.1.8.6, “Miscellaneous parameters (Windows)”, on page 42.

- **PreScan** – Scans all files in the backup prior to performing the backup to display an estimated completion time for the backup.
- **Compression type** – Specifies the type of compression that will be applied to the backup. The options are as follows:
  - **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good default compression when the network is not the bottleneck.
  - **ZLIB (Global, Low, Medium, and High)** – Normally produces better compression than LZOP, but will take more time to compress. This is a good default compression when the bottleneck is the network. ZLIB Low corresponds to a value of 3, ZLIB Medium = 6, and ZLIB High = 9.
  - **None** – Disables compression for the backup.

2. In the **Default operation** box, specify how the backup should handle an open file during backup. The options are as follows:
   - **Try deny write** – Attempts to open the file in Deny write mode. If this fails because the file is already open, the file is placed in Allow write mode.

- **Deny write** – Prevents any other process from writing to the file while the DS-Client has it open. The DS-Client will not back up the file if another process has already opened it for write. However, you can instruct the DS-Client to retry backing up the open file.
- **Prevent write** – Attempts to open the file in Deny write mode. If this fails because the file is already open, the file is opened in Allow write mode and locked to prevent any other process from writing to the file. This ensures that the most recent version of the file is backed up.
- **Allow write** – Allows another process to read or write to the file without restrictions. Since other applications can write to the file while it is being backed up, this can affect file consistency.

3. In the **Retry times** box, enter the number of times you want the DS-Client to attempt to back up the file.
4. In the **Retry interval (sec)** box, enter the interval between retries.
5. To specify a command to run before (Pre) and/or after (Post) the execution of the backup, click **Pre/Post**. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525 and Section 5.26, “Configuring Pre/Post processes (Linux)”, on page 528.
6. To exclude old files from being backed up, click **Exclude old files**, and then do the following:
   a) To include all old files, select **No exclusion**.
   b) To exclude files older than a specified period, select **Exclude files older than**, and then enter the period in days, weeks, months, or years.

   NOTE: If the backup fails, the exclude period will be extended to reflect the conditions of the failed backup until a successful backup is completed.

   c) To exclude files older than a specified date, select **Exclude files older than**, and enter the date.
   d) Click **OK**.

   NOTE: The age of a file is determined by its last modified date. This option is not available if the Windows System State or Services Database is selected.

7. Click **Next**.

5.4.1.6 Selecting the advanced options

IMPORTANT: These options are disabled by default. If you select any of these options, the size of the data that is backed up will increase.

1. To back up all data on remote media, select the **Backup data in Remote Storage** check box.

   NOTE: Some operating systems can migrate infrequently accessed data from the local hard drive to directly attached tape libraries. The local disk usage is reduced by replacing the file with a link. If disabled, only the link is backed up.

2. To back up each instance of a file separately, select the **Backup Single Instance Store / Data Deduplication file data** check box.

   NOTE: Some operating systems have an optional Single Instance Store to handle multiple copies of the same file on the computer. Local disk usage is reduced by placing one copy of the file in the Single Instance Store with links in all associated directories. If disabled, only the link is backed up. If you have activated Single Instance Store, select this option.

3. To back up all data in the directory referenced by the junction point, select the **Follow junction point** check box.

   NOTE: Junction points are links to other folders. If disabled, only links to the folder are backed up. Junction points mounted as FAT or FAT32 volumes are not supported.

4. If the target computer supports the Volume Shadow Copy Service (VSS) feature, do the following:

   a) To initiate a Volume Shadow Copy Service (VSS) snapshot of any local volumes and perform the backup from the VSS snapshot, select the **Backup through volume shadow copies** check box.

      NOTE: When configured, the DS-Client uses the VSS feature to copy the volumes selected for backup and then performs the backup from the VSS snapshot. If the VSS snapshot fails, the DS-Client attempts to perform the backup like a normal File system backup.

   b) To specify whether VSS validation is run prior to performing the backup, select one of the following options:

      - **Disable** – VSS validation is not performed.

- **Enable** – VSS validation is performed.
- **Use DS-Client's settings** – VSS validation is performed using the DS-Client settings.

c) To specify that the DS-Client does not notify VSS-aware applications when a backup is performed so the resulting backup is only crash-consistent (e.g. it will contain whatever was on the hard disk during the backup), select the **Do not involve writers** check box.

d) To specify that the VSS snapshot is performed without processing components, select the **Do not process components** check box.

NOTE: Processing components means verifying if the files are included in the volumes selected for the snapshot. This option is useful if you have selected only a portion of a component for backup and do not want to encounter errors because the VSS verification would otherwise detect missing files or dependencies.

e) To manually exclude specific VSS writers or components, select the **Exclude some writers / components** check box, and then click **[>>]**.

NOTE: This has the same effect as choosing the Do not involve writers option, but only applies to the writers or components you choose.

5. To control the automatic file filtering performed by the DS-Client during a backup, select the **Non-filtered share data backup** check box. By default, the DS-Client excludes some files automatically from the share-based backup of files even if such files are readable. Excluded files can include temporary files, files being backed up as part of System State backups, registry hive files, or other files that can interfere with a successful Bare Metal Restore (BMR).

NOTE: Use this option only if excluded data needs to be included in the share-based backup. Selecting this option affects the ability to perform BMR without manual file filtering. However, it can be used in conjunction with the VSS option to allow bootable-disk BMR. Unless BMR provisioning is supported by your DS-Client, it is recommended that you do not select this option.

6. To force the backup of files that are already backed up, select the **Force backup even if the modified time and size did not change** check box.

NOTE: By default, the DS-Client skips files that have already been backed up by comparing the last modified time and size with the latest generation in the database. Normally this is the required behavior for backups.

7. Click **Next**.

5.4.1.7 Specifying backup performance options

IMPORTANT: These options are intended for high performance environments where the DS-Client can take advantage of the speed of the storage where the source data resides. Test different settings to determine the optimal value. Slower storage can result in performance issues if the values are not properly configured.

1. Configure the maximum I/O operations the DS-Client will use for each file in the backup.
   - To use the default **MaxPendingIOPerFile** advanced configuration parameter, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value**, and then enter the value.

   IMPORTANT: This setting is for storage devices that support better parallel disk I/O, such as NAS devices. The optimal setting for this value depends on the storage device and network speed. Increasing this value can significantly increase the backup speed. If your storage device does not support better parallel disk I/O, use the default value, otherwise the performance can be significantly degraded.

2. Configure the internal buffer size (in KB) for reading a file during the backup process.
   - To use the default **FileReadBufferSize** advanced configuration parameter, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific buffer size (KB)**, and then enter the value.

   IMPORTANT: To achieve optimum backup performance, the DS-Client read buffer size might need to be different, depending on the combination of the target storage device, target operating system, and any mid-ware involved between the storage and the operating system.

3. Click **Next**.

5.4.1.8 Selecting the notification options

1. To configure a notification, do one of the following:
   - To add a notification, click **Add.**
   - To modify a notification, select the notification, and then click **Modify.**

   NOTE: To delete a notification, select the notification, and then click **Delete**.

2. To send an email notification, select **E-Mail**. and then do the following:
   a) To send the email notification to the DS-Client administrator, select **Administrator**.
   b) To send an email to another recipient, select **Other**, and then specify the recipients email address.
   c) To send detailed backup information, select the **Detailed notification** check box.
   d) To include a detailed file-level backup log as an attachment, select the **Attach detail log** check box.
   e) To send the email notification in HTML format, select the **Send E-Mail using HTML format** check box.

   NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

   f) Click **OK**.
3. To send a pager notification, select **Pager**. The notification will be sent to the pager account configured for the DS-Client.

   NOTE: The pager option is available only if the DS-Client has been configured for pager notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

4. To send a broadcast notification, select **Broadcast**. Select the server containing the service to which you want to send the message and click **OK**.

   NOTE: Broadcast notifications to domains/workgroups are limited to 128 characters.

5. To send an event notification, elect **Event**. Select the server on which you want the notification to be recorded in the Event Log and click **OK**.
6. In the **Completion** box, specify under what conditions a notification will be sent, and then click **OK**. The options are as follows:
   - **All** – Notification will be sent under all conditions.
   - **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
   - **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.
   - **Completed with errors** – Notification will be sent if an activity is completed with at least one error event.
   - **Incomplete** – Notification will be sent if an activity is not completed successfully.
7. Configure the DS-Client to send SNMP traps when the backup has completed successfully, completed with warnings, completed with errors, or is incomplete.
8. Click **Next**.

5.4.1.9 Assigning a retention rule

1. To assign a retention rule to the backup, do one of the following:
   - If you don't want to assign a retention rule, select **No retention rule**.
   - To assign a retention rule, select **Use a specific retention rule**, and then select the retention rule.

NOTE: To create or edit a retention rule, click **[...]**. For more information, see Section 4.1, "Configuring a retention rule", on page 98.

---

2. Click **Next**.

5.4.1.10 Assigning a schedule

1. To assign a schedule to the backup, do one of the following:
   - If you don't want to assign a schedule to the backup, select **Not scheduled**.
   - To assign a schedule to the backup, select **Scheduled.** In the **Available schedules** box, select an existing schedule.

NOTE: To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, "Configuring a schedule", on page 90.

---

2. Click **Next**.

5.4.1.11 Naming the backup

1. In the **Set name** box, type a name for the backup.
2. In the **Set type** box, select the type of backup you want to create. The list of available backup types depends on the configuration of your DS-Client.
   - Online
   - Self-contained
   - Local-only
   - Instant recovery
   - Statistical

NOTE: For more information, see Section 5.1, "Backup types", on page 106.

---

3. If you selected **Online**, do the following:
   a) To send a copy of the oldest generation of the file that is about to be overwritten from the DS-System to the BLM Archiver, select the **BLM (Infinite Generations)** check box.

NOTE: The Backup Lifecycle Management tool must be enabled for the DS-Client.

---

b) To save a copy of the backup data to a local storage location on the DS-Client computer, select the **Save on Local Storage** check box.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Self-contained and Local Only backups.

c) To use the local storage as a cache if the DS-Client loses connection with the DS-System, select the **Transmission cache on Local Storage** check box. The cached backup data will be sent to the DS-System on the next connection after synchronization.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path.

d) To save a copy of the backup data to the instant recovery vault, select the **Save in instant recovery vault** check box.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Instant Recovery backups.

e) Beside the **Local Storage Path** box, click **>>**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

4. If you selected **Self-Contained**, beside the **Local Storage Path** box, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

5. If you selected **Local Only**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

6. If you selected **Instant Recovery**, the **Save in instant recovery vault** option is selected by default.

IMPORTANT: Each DS-Client must have a unique ZFS volume name.

---

7. If you selected **Statistical** and want to emulate an actual backup transfer process, select the **Calculate transmit amount** check box. During the backup, specified backup files will be read from their source and processed for compression and encryption.
8. If the multitenant feature is enabled and configured, in the **Customer** list, select the customer to which you want to assign the backup. For more information, see Section 11.5, “Multitenant DS-Clients”, on page 634.
9. Click **Finish**.

5.4.2 Restoring a File system backup

You can restore a Windows File system backup.

IMPORTANT: If any of your selected files have already been archived to BLM Archiver, you can only restore the archived generations by requesting a BLM restorable image of that data. You can request a BLM restorable image from your service provider or backup administrator. If you have already installed the DS-NOC, you can access your BLM data via DS-NOC. For more information, see Section 11.3.4, “Restoring from the BLM Archiver”, on page 627.

5.4.2.1 Selecting the restore items

1. Browse the backups tree and select the backup you want to restore.
2. On the **Restore** menu, click **Restore Now**.
3. To restore an entire backup or folder, browse the tree and select the check box beside the backup or folder you want to restore.
4. To restore individual files, select the folder containing the required files, click **Show Files**, and then do one of the following:

- To view details about the backed up file, select the file, and then click **File Info**.
- To view modified files, click **Show Modified**.
- To view archived files, click **Show Archived**.

5. To view the number of files and calculate the total amount of files selected, select the **Calculate amount** check box.
6. To exclude subdirectories, clear the **Include SubDirs** check box. The default setting is to include sub-directories.
7. To search for files that match a certain criteria, in the **Filter** box, type the file pattern that you want to search for in the selected folder. For example, *.doc will search for all files with the doc file extension.
8. To search for a specific backed up file, click **Find File**. In the **Find Backed Up File** dialog box, do the following:
   a) Select the search criteria to search for a backed up file either by **File name** or by **File ID**.
   b) Click **Find**.
   c) Select the required backed up file, and then click **Select**.
9. To view the details of the items you selected, click **Selection**.
10. To refine your selection of items to restore, click **Advanced**, and then select which generation you want to display. The options are as follows:
    - To restore the latest generation of all the files, select **Latest generation of all data**.
    - To restore files that were deleted from the source, but not removed from the online storage as of the last backup session, select **Latest generation of all data (except deleted data)**.
    - To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:
      a) Beside **From**, click **[>>]**, and select a start date and time. No backup sessions before this date will be displayed.
      b) Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.

      NOTE: If you are performing a Bare Metal Restore (BMR) of a computer with active retention rules you can display only the backup sessions that are suitable for BMR by selecting the **Show only backup sessions suitable for BMR** check box.

      c) Click **OK**.

11. Select the type of filter you want to apply to the backups. The options are as follows:
    - **Show all data** – No filter is applied.
    - **Hide data (dirs/files) deleted from source on/before** – Hides backed up data (folders and files) that was intentionally deleted from the source computer.
    - **Show only data (dirs/files) deleted from source on/before** – Displays only backed up data (folders and files) that was intentionally deleted from the source computer.

    NOTE: These options are available only if the DS-Client database can be used to filter the backups. It does not appear for BLM Image Restore or Disc/Tape Restore, since they have been written to media and are no longer synchronized with the DS-Client database.

12. Select how files are restored. The options are as follows:
    - **Restore all** – All selected files are restored to the destination folder. Files with the same name are overwritten.
    - **Restore newer** – Only files newer than those in the destination folder are restored.
    - **Restore older** – Only files older than those in the destination folder are restored.
    - **Restore different** – Only files with different dates/sizes than those in the destination directory are restored.
    - **Skip existing** – Existing files with the same name in the destination folder are not restored.
13. Select how you want to restore Microsoft data deduplication links. The options are as follows:
    - **Restore as links** – Restores data deduplication links as links.
    - **Skip links** – Restores only the files that have the last generation as full and skips the files with the last generation as a link.
    - **Restore last non-link** – Searches for a previous generation of the file that is not a link. If a non-link generation is not found, such a file will be skipped.
14. Click **OK**.
15. Click **Next**.

5.4.2.2 Selecting the restore location

1. Select the location to which you want to restore the backup. The options are as follows:

   - **Original location** – Data is restored to the original backup source location and existing files with the same name are overwritten. This is the default option.
   - **Alternate location** – Data is restored to a location other than the original backup source.

   NOTE: When restoring to an alternate location, the security of restored items in the destination location might not resemble the security of those items during backup.

2. If you selected **Alternate location**, do the following:

   a) Beside the **Alternate location** box, click **[>>]**.

   b) In the **Select Alternate Server** dialog box, select the computer where you want to restore the data.

   c) To provide the credentials for the selected computer, select the **Ask for Network Credentials** checkbox, and then click **Select**.

   d) In the **Enter Network Credentials** dialog box, enter the credentials to connect to the destination computer, and then click **OK**.

   e) In the **Destination** cell, select a share location.

   f) In the **Restore to** cell, type the name of the folder you want to restore to or click **[>>]** and select a folder.

   NOTE: For more information, see Section 5.3.3, “Restoring data to an alternate location”, on page 130.

3. Click **Next**.

5.4.2.3 Selecting the performance options (Windows)

IMPORTANT: These options are intended for large backups in high performance environments where the DS-Client can take advantage of the speed of the storage where the source data resides. Test different settings to determine the optimal value. Slower storage can result in performance issues if these values are not configured correctly.

1. Configure the maximum number of I/O operations the DS-Client will use for each file during the restore process.
   - To use the default MaxPendingIOPerFile advanced configuration parameter setting, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value** and then enter the value.
2. Configure the number of files the DS-System can read simultaneously for the restore process.
   - To use the default MaxRestoreReadThreads advanced configuration parameter setting, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value** and then enter the value.
3. Click **Next**.

5.4.2.4 Selecting the restore options

1. Select a restore option for permissions. The options are as follows:
   - **Yes** – Restores the permissions for all the backed up files.
   - **Skip** – Skips the file security information of the backed up files. Newly created files and folders inherit the security settings of the parent folder.
   - **Only** – Restores the permissions for only the selected files and folders.

NOTE: If you have been assigned ownership of a user's backup and want to restore files with ACL, the DS-Client checks if you have access rights. If you do not have access rights, you will not be able to restore the ACL. You must choose Skip to restore the file. If you have access rights, but the file ownership is not yours, the file will be restored without ownership, and an error message will appear in the Event Log.

2. Select a method for the DS-Client to perform the restore. The options are as follows:

   - **Save** – Restores files to a temporary location first to prevent partially restored files from overwriting an existing file. If the file is restored successfully, the original file is overwritten with the temporary file.
   - **Use buffer** – Restores files to the DS-Client buffer first and then transfers the files to the restore destination. This method minimizes the duration for which the restore process occupies the destination server.
   - **Fast** – Uses a direct restore method by writing data as it is received.

   NOTE: If you select the Fast method, files in the destination location are overwritten upon receipt of the first byte of data.

3. Select a restore method for locked files. The options are as follows:

   - **Rename** – Renames locked files while still in use. The renamed files are registered with the operating system for deletion on reboot. This is useful when restoring system files that are opened before the operating system has had a chance to replace the locked file.
   - **Don't rename** – Restores locked files as temporary files. The temporary files are registered with the operating system for deletion on reboot.
   - **Skip** – Skips locked files. An error is reported in the Activity Log.

4. To skip the restore of an online file if it is a stub, select the **Skip offline files (stubs)** check box.
5. To replace any junction points (special folders that link to another location) of the same name, select the **Overwrite junction point** check box.
6. To record all restored files in the Activity Log, select the **Detailed log** check box.
7. To skip the pre and post restore processes, select the **Skip Pre/Post** check box. If this check box is cleared, the DS-Client runs a specified activity before and/or after a restore operation. For more information, see Section 5.25, "Configuring Pre/Post processes (Windows)", on page 525.
8. If the backup source and the restore destination support file level compression, select a compression setting. The options are as follows:

   - **Default Compression** – Restored files take on the compression attribute of the parent folder where they were restored.
   - **Preserve Compression** – Restored files retain their original compression setting.
   - **Force Compress** – Restored files are compressed using the compression of the destination file system.

- **Force Expand** – Restored files are not compressed.

9. Select a restore setting for files backed up with Encrypting File System (EFS). The options are as follows:
   - **Include Encrypted Files** – Restores files encrypted with EFS.
   - **Skip Encrypted Files** – Skips files encrypted with EFS.
   - **Restore Encrypted Files Only** – Restores only files encrypted with EFS.
10. Click **Next**.

5.4.2.5 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, select the type of restore. The options are as follows:
   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.
3. Click **Finish**.

5.5 File system (NAS, NFS, UNIX-SSH) backups (Linux or Mac)

You can back up and restore the local file system on a Linux or Mac computer visible on the LAN using the NFS or UNIX-SSH protocol. Only Linux DS-Clients can back up NAS (Networked Attached Storage) devices.

5.5.1 Hard link requirements

Hard links are created in Linux-based file systems with the `ln` function. If you want to back up and restore hard links, you must create a backup that includes all files that are linked through hard links.

If even one linked file from a hard link group is not included in the backup, the backup will not be able to record all the hard link information. Note the following:

- By default, the **Backup hard links** option is selected for new backups. The backup records file and hard link information so the hard links can be restored.
- If the **Backup hard links** option is not selected for a backup, any backed up hard link will be backed up and restored as a separate individual file. The backup will not contain any hard link information.
- Even with the **Backup hard links** option selected, you must create a backup that includes all the hard linked files. Otherwise a warning will appear in the Event Log for the backup activity and your existing hard links will be broken when you restore from that backup. This is also applicable if you perform a partial restore of hard linked files.

Restoring hard links assumes the backup contains all hard linked files and file information. For example, if the source computer has 5 files that are hard linked, your backup must contain those same 5 files and have the **Backup hard links** option selected. The restore behavior depends on the restore method selected:

- **Save / Use Buffer** — This is the default restore method, which will restore the selected hard linked files and recreate the hard links for the restored files.
- **Fast** — This method allows you to selectively restore the hard link data (inode information) from a single file while preserving the existing hard link information on the restore target. This effectively changes the data of the other linked files that were not restored.

If only some of the hard-linked files are selected for restore, the restore will only link the hard linked files that are restored. If you want to restore only one file and preserve any existing hard links, use the **Fast** restore option. This also changes the data of other linked files that are not restored.

5.5.2 Creating a local file system backup

You can create a local file system backup on Linux or Mac.

NOTE: Ensure the backup items exclude the postgres data folder as this can cause errors during the backup process. This might occur if you select "/" as the backup item (e.g. the entire "/" drive).

5.5.2.1 Selecting the type of backup

1. On the **Sets** menu, click **New Backup Set**.
2. Select **NAS, UNIX-SSH, NFS, Local File System**, and then click **Next**.

5.5.2.2 Selecting the backup source

1. Select **Local File System** and browse to **My Computer**.
2. To use the log in credentials of the selected source computer, select **Ask for local machine credentials**, and then click **Next**.
3. Type the user name and password or click **[...]** to select a user.
4. Click **OK**.
5. Click **Next**.

5.5.2.3 Selecting the backup items

1. Select the shares or directories you want to back up.
2. To add an entire directory, select the directory, and then click **Add**. Sub-directories are included by default.
   - To exclude sub-directories, clear the **Include SubDirs** check box.
3. To exclude an item when its parent folder is selected for backup, select the item, and then click **Exclude.**
4. To exclude an item using regular expressions, select the item, and then click **RegEx**.

NOTE: Regular expressions provide more specific filtering than the exclude function. For example, you can use regular expressions to exclude individual file names or patterns. Use this option only if you are familiar with the syntax.

5. To search for files that match a certain criteria, in the **Filter** box, type the file pattern you want to search for in the selected folder. For example, *.doc will search for all the files with the doc file extension.
6. To modify a regular expression, select the regular expression, and then click **Modify**.
7. To remove an item from the list, select the item, and then click **Remove**.

NOTE: Removing an item will not remove previous backups of that item. To remove previously backed-up data, you must use the Delete function.

---

8. Click **Next**.

5.5.2.4 Selecting the backup item options

1. To configure the maximum generations for a backup item that will be stored online, double click the **Max Gen** cell, and then enter the value.
2. To back up the access control list (file permissions), select the **Back up ACL** check box.
3. To back up the local file system with the extended ACL, select the **Back up POSIXACL** check box.
4. To back up the security enhanced Linux attribute of files or folders for local file system and SSH backups, select the **Back up SElinux** check box.
5. Click **Next.**

To select the backup item options (Macintosh DS-Client):

1. To back up the resource fork of a file, select the **Back up Resource** check box.
2. To back up the file attributes for files, select the **Back up File Attributes** check box.
3. Click **Next**.

5.5.2.5 Selecting the backup options

1. Configure the options for the backup. The options are as follows:

   - **Use buffer** –Copies files to the DS-Client buffer to free up the backup source as fast as possible. The DS-Client then sends the files from the DS-Client buffer to the DS-System. This option cannot be configured if CDP is enabled. For more information, see Section 5.2.7, “Performance”, on page 113.
   - **Detailed log** – Records all files that backed up in the Activity Log. For more information, see Section 8.1, “Viewing the Activity Log”, on page 578.
   - **Initial backup** – Uses the Initial Backup feature for the first backup. To configure the initial backup path, click **[>>]**. For more information, see Section 11.1.1, “Configuring the initial backup path”, on page 618.
   - **PreScan** – Flags the backup to scan all files in the backup prior to backup to display an estimated completion time for the backup.
   - **Disable common files** – Excludes the backup files from common file storage reduction. This means duplicate files will be encrypted and backed up individually, thereby potentially increasing the stored size.

     NOTE: This feature must be activated for your DS-Client by your service provider. You can enable this option when creating the backup. This option cannot be changed afterwards.

   - **Continuous data protection** – Enables continuous data protection (CDP) for the backup. To configure the CDP settings, click **[>>]**, and beside **File Change Detection**, select a method for file change detection. The options are as follows:

     - **Generic Scanner** – Loops the scanning function from online File system backups.
     - **File Alteration Monitor (Only Linux)** – You must install FAM on the target machine and the FAM daemon must be running,. It interfaces with the Linux operating system functionality of notifications for file changes. If FAM is not installed, DS-Client will try to copy and execute a FAM instance on the target Linux machine.

     a) To specify the minimum interval the DS-Client must wait before backing up a changed item or file, select **Do not back up more often than**, and then enter the interval and unit of measurement. You can set a longer interval if you do not want to back up changes frequently or a shorter interval if you want backup of changes to be more granular.

     b) To specify the minimum interval the DS-Client must wait before backing up a changed item or file after detecting that it has not changed, select **Backup if file stops changing for**, and then enter the interval and unit of measurement. This option is intended for data that you know changes frequently.

c) Select the scheduled activities that will suspend the CDP backup process. The options are **Retention**, **BLM**, and **Validation**.

d) Click **OK**. For more information, see Section 5.2.2, “Continuous data protection (CDP)”, on page 108.

- **Stop on errors** – Stops a backup process when the number of errors reaches the specified value. A value of 0 means the DS-Client does not stop a backup process regardless of the number of errors.

NOTE: You can configure the default setting using the **MaxErrors** advanced configuration parameter. For more information, see Section 2.1.8.6, “Miscellaneous parameters (Windows)”, on page 42.

- **Compression type** – Specifies the type of compression that will be applied to the backup. The options are as follows:
  - **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good default compression when the network is not the bottleneck.
  - **ZLIB** (**Global**, **Low**, **Medium**, and **High**) – Normally produces better compression than LZOP, but will take more time to compress. This is a good default compression when the network is the bottleneck. ZLIB High corresponds to a value of 9, ZLIB Medium=6, and ZLIB Low=3.
  - **None** – Disables compression for the backup.

2. To configure additional backup options, do the following:

   a) To force the backup of a file, even if it’s last modified time and size have not changed since the last backup, select the **Force backup even if the modified time or size did not change** check box.

   b) To backup the file with hard link information, select the **Backup hard links** check box. Even if you select this option, you must create a backup that includes all the hard linked files.

3. To specify a command to run before (Pre) and/or after (Post) the execution of the backup, click **Pre/Post**. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525 and Section 5.26, “Configuring Pre/Post processes (Linux)”, on page 528.

4. To exclude old files from being backed up, click **Exclude old files**, and then do one of the following:

a) To include all old files, select **No exclusion**.

b) To exclude files older than a specified time period, select **Exclude files older than**, and then enter the time period.

NOTE: If the backup fails, the exclude period will be extended to reflect the conditions of the failed backup until a successful backup is completed.

c) To exclude files older than a specified date, select **Exclude files older than**, and enter the date.

d) Click **OK**

5. Click **Next.**

5.5.2.6 Selecting the notification options

1. To configure a notification, do one of the following:
   - To add a notification, click **Add**.
   - To modify a notification, select the notification, and then click **Modify**.

NOTE: To delete a notification, select the notification, and then click **Delete**.

2. To send an email notification, select **E-Mail**, and then do the following:

   a) To send the email notification to the DS-Client administrator, select **Administrator**.

   b) To send an email to another recipient, select **Other**, and then specify the recipient's email address.

   c) To send detailed backup information, select the **Detailed notification** check box.

   d) To include a detailed file-level backup log as an attachment, select the **Attach detailed log** check box.

   e) To send the email notification in HTML format, select the **Send E-Mail using HTML format** check box.

NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, "Configuring the notification settings", on page 27.

   f) Click **OK**.

g) In the **Completion** box, specify under what conditions a notification will be sent, and click **OK**. The options are as follows:

- **All** – Notification will be sent under all conditions.
- **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
- **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.
- **Complete with errors** – Notification will be sent if an activity is completed with at least one error event.
- **Incomplete** – Notification will be sent if an activity is not completed successfully.

3. Configure the DS-Client to send SNMP traps when the backup has completed successfully, completed with warnings, completed with errors, or is incomplete.
4. Click **Next**.

5.5.2.7 Assigning a retention rule

1. To assign a retention rule to the backup, do one of the following:
   - If you don't want to assign a retention rule, select **No retention rule**.
   - To assign a retention rule, select **Use a specific retention rule**, and then select the retention rule.

NOTE: To create or edit a retention rule, click **[...]**. For more information, see Section 4.1, "Configuring a retention rule", on page 98.

---

2. Click **Next**.

5.5.2.8 Assigning a schedule

1. To assign a schedule to the backup, do one of the following:
   - To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, "Configuring a schedule", on page 90.
   - To assign a schedule, select **Scheduled**. In the **Available schedules** box, select an existing schedule.
   - If you don't want to assign a schedule, select **Not scheduled**.
2. Click **Next**.

5.5.2.9 Naming the backup

1. In the **Set Name** box, type a name for the backup.
2. In the **Set Type** box, select the type of backup you want to create. The list of available backup types depends on the configuration of your DS-Client.
   - Online
   - Self-contained
   - Local-only
   - Instant recovery
   - Statistical

   NOTE: For more information, see Section 5.1, “Backup types”, on page 106.

3. If you selected **Online**, do the following:
   a) To save a copy of the backup data to a local storage location on the DS-Client computer, select the **Save on Local Storage** check box.

      NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Self-contained and Local Only backups.

   b) To use the local storage as a cache if the DS-Client loses connection with the DS-System, select the **Transmission cache on Local Storage** check box. The cached backup data will be sent to the DS-System on the next connection after synchronization.

      NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path.

   c) To save a copy of the backup data to the instant recovery vault, select the **Save in instant recovery vault** check box.

      NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Instant Recovery backups.

d) Beside the **Local Storage Path** box, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

4. If you selected **Self-Contained**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

5. If you selected **Local-Only**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**..

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

6. If you selected **Instant Recovery**, the **Save in instant recovery vault** option is selected by default.

IMPORTANT: Each Linux DS-Client must have a unique ZFS file name.

---

7. If you selected **Statistical**, and want to emulate an actual backup transfer process, select the **Calculate transmit amount** check box. During the backup, specified backup files will be read from their source and processed for compression and encryption.
8. If the multitenant feature is enabled and configured, in the **Customer** list, you can select the customer to which you want to assign the backup. For more information, see Section 11.5, “Multitenant DS-Clients”, on page 634.
9. Click **Finish**.

5.5.3 Creating a NAS file system backup

You can create a backup of a NAS (Networked Attached Storage) device using a dedicated API from the NAS vendor. The DS-Client uses the API to create a volume-based snapshot on the NAS device for the data selected in the backup. After creating a snapshot, the DS-Client temporarily mounts a NAS share and backs up the data from the snapshot. When the backup is finished, DS-Client unmounts the NAS share and deletes the snapshot.

IMPORTANT: NAS backups are not supported on Mac DS-Clients. CIFS shares or volumes with NTFS / Mixed security type are not supported.

When creating a NAS backup, consider the following:

- For NetApp NAS volumes, you must select the volume configuration option which enables access to the snapshot file for NFS when browsing the NetApp volumes. Otherwise the DS-Client cannot access the snapshot.
- If you are backing up a NetApp cluster, select **NAS type** in the **Ask for NAS API credentials** dialog box. This allows the DS-Client to interact with the NAS API correctly.
- If the DS-System is using a NetApp storage and is configured to support the NetApp Snapdiff, the **Use Snapdiff API** option will appear in the DS-Client. If selected, the DS-Client attempts to use the NetApp Snapdiff API to avoid rescanning the entire NAS volume during an incremental backup. Snapdiff compares the current snapshot with the last snapshot of the target NAS volume and generates the list of new and changed files. This can provide significant improvements to the backup process, especially on large volumes.

  NOTE: A previous snapshot should exist so the Snapdiff API can function. In the event Snapdiff fails, the DS-Client will attempt to perform a full scan of the NAS volume.

The following limitations apply when using the Snapdiff API:

- Snapdiff does not work on the first (baseline) backup.
- Snapdiff does not work if the current snapshot fails.
- Snapdiff does not work if any backup item has changed, since the last backup.

5.5.3.1 Selecting the type of backup

1. On the **Sets** menu, click **New Backup Set**.
2. Select **NAS, UNIX-SSH, NFS, Local File System**, and then click **Next**.

5.5.3.2 Selecting the backup source

1. Select **NAS** and in the **Path** box, type the NAS IP address or DNS name in the format NAS\10.10.20.33.
2. To use the log in credentials of the selected source computer, select **Ask for local machine credentials**, and then click **Next**.
3. Type the user name and password or click **[...]** to select a user.
4. Click **OK**.
5. By default, **Ask for NAS API credentials** check box is selected. Type the NAS API connection credentials.
   a) In the **NAS Type** box, select the NAS type.
   b) In the **API Protocol** box, select the API access protocol.
   c) In the **Port Number** box, type the port for the API connection.
   d) In the **User Name** box, type the user name to access the API protocol.
   e) In the **Password** box, type the password to access the API protocol.
   f) In the **Mount-point** box, type the mount point to be used for mounting the NAS share during the backup. Use an existing mount point or create a new one for the backup purpose.
   g) Click **OK**.

NOTE: The user must be a member of the Administrators group and must rights to execute the API commands on the NAS device.

5.5.3.3 Selecting the backup items

1. Select the shares/directories you want to back up.
2. To add an entire directory, select the directory, and then click **Add**. Sub-directories are included by default.
   - To exclude sub-directories, clear the **Include SubDirs** check box.
3. To exclude an item when its parent directory is selected for backup, select the item, and then click **Exclude**.
4. To exclude an item using regular expressions, select the item, and then click **RegEx**.

NOTE: Regular expressions provide more specific filtering than the exclude function. For example, you can use regular expressions to exclude individual file names or patterns. Use this option only if you are familiar with the syntax.

---

5. To search for files that match a certain criteria, in the **Filter** box, type the file pattern you want to search for in the selected folder. For example, *.doc will search for all the files with the doc file extension.
6. To modify a regular expression, select the regular expression, and then click **Modify**.
7. To remove an item from the list, select the item, and then click **Remove**.

NOTE: Removing an item will not remove previous backups of that item. To remove previously backed-up data, you must use the Delete function.

---

8. Click **Next**.

5.5.3.4 Selecting the backup item options

1. To configure the number of maximum generations of the selected backup item that will be stored online, double click in the **Max gen** cell, and then enter the new value.
2. To backup the access control list (file permissions), select the **Back up ACL** check box.
3. Click **Next**.

5.5.3.5 Selecting the backup options

1. Configure the options for the backup. The options are as follows:

   - **Use buffer** –Copies files to the DS-Client buffer to free up the backup source as fast as possible. The DS-Client then sends the files from the DS-Client buffer to the DS-System. For more information, see Section 5.2.7, “Performance”, on page 113.
   - **Detailed log** – Records all files that backed up in the Activity Log. For more information, see Section 8.1, “Viewing the Activity Log”, on page 578.
   - **Disable common files** – Excludes the backup files from common file storage reduction. This means duplicate files will be encrypted and backed up individually, thereby potentially increasing the stored size.

     NOTE: This feature must be activated for your DS-Client by your service provider. You can enable this option when creating the backup. This option cannot be changed afterwards.

   - **Initial backup** – Uses the Initial Backup feature for the first backup. To configure the initial backup path, click **[>>]**. For more information, see Section 11.1.1, “Configuring the initial backup path”, on page 618.
   - **PreScan** – Flags the backup to scan all files in the backup prior to backup to display an estimated completion time for the backup.
   - **Stop on errors** – Stops a backup process when the number of errors reaches the specified value. A value of 0 means the DS-Client does not stop a backup process regardless of the number of errors.

     NOTE: You can configure the default setting using the **MaxErrors** advanced configuration parameter. For more information, see Section 2.1.8.6, “Miscellaneous parameters (Windows)”, on page 42.

   - **Compression type** – Specifies the type of compression that will be applied to the backup. The options are as follows:
     - **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good default compression when the network is not the bottleneck.
     - **ZLIB** (**Global**, **Low**, **Medium**, and **High**) – Normally produces better compression than LZOP, but will take more time to compress. This is a good default compression when the network is the bottleneck. ZLIB High corresponds to a value of 9, ZLIB Medium=6, and ZLIB Low=3.
     - **None** – Disables compression for the backup.

2. To configure additional backup options, do the following:

a) To force the backup of a file, even if it's last modified time and size have not changed since the last backup, select the **Force backup even if the modified time or size did not change** check box.

b) To enable the handling of backup of the file and hard link information for the hard links to be restored, select the **Backup hard links** check box. Even if you select this option, you must create a backup that includes all the hard linked files.

c) To continue the backup if the snapshot fails, select the **Continue backup on snapshot failure** check box.DS-Client will try to access the data selected in the backup directly by skipping the snapshot functionality.

3. To specify a command to run before (Pre) and/or after (Post) the execution of the backup, click **Pre/Post**. For more information, see Section 5.25, "Configuring Pre/Post processes (Windows)", on page 525 and Section 5.26, "Configuring Pre/Post processes (Linux)", on page 528.

4. To exclude old files from being backed up, click **Exclude old files**, and then do one of the following:

   a) To include all old files, select **No exclusion**.

   b) To exclude files older than a specified period, select **Exclude files older than**, and then enter the period in days, weeks, months, or years.

   NOTE: If the backup fails, the exclude period will be extended to reflect the conditions of the failed backup until a successful backup is completed.

   c) To exclude files older than a specified date, select **Exclude files older than**, and enter the date.

   d) Click **OK**.

5. Click **Next.**

5.5.3.6 Selecting the notification options

IMPORTANT: The email and pager options are available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

1. To configure a notification, do one of the following:
   - To add a notification, click **Add**.
   - To modify a notification, select the notification, and then click **Modify**.

   NOTE: To delete a notification, select the notification, and then click **Delete**.

2. To send an email notification, select **E-Mail**, and then do the following:
   a) To send the email notification to the DS-Client administrator, select **Administrator**.
   b) To send an email to another recipient, select **Other**, and then specify the recipient’s email address.
   c) To send detailed backup information, select the **Detailed notification** check box.
   d) To include a detailed file-level backup log as an attachment, select the **Attach detailed log** check box.
   e) To send the email notification in HTML format, select the **Send E-Mail using HTML format** check box.

   NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

   f) Click **OK**.
   g) In the **Completion** box, specify under what conditions a notification will be sent, and click **OK**. The options are as follows:
      - **All** – Notification will be sent under all conditions.
      - **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
      - **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.
      - **Complete with errors** – Notification will be sent if an activity is completed with at least one error event.

- **Incomplete** – Notification will be sent if an activity is not completed successfully.

3. Configure the DS-Client to send SNMP traps when the backup has completed successfully, completed with warnings, completed with errors, or is incomplete.
4. Click **Next**.

5.5.3.7 Assigning a retention rule

1. To assign a retention rule to the backup, do one of the following:
   - If you don't want to assign a retention rule, select **No retention rule**.
   - To assign a retention rule, select **Use a specific retention rule**, and then select the retention rule.

NOTE: To create or edit a retention rule, click **[...]**. For more information, see Section 4.1, "Configuring a retention rule", on page 98.

---

2. Click **Next**.

5.5.3.8 Assigning a schedule

1. To assign a schedule to the backup, do one of the following:
   - If you don't want to assign a schedule to the backup, select **Not scheduled**.
   - To assign a schedule to the backup, select **Scheduled.** In the **Available schedules** box, select an existing schedule.

NOTE: To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, "Configuring a schedule", on page 90.

---

2. Click **Next**.

5.5.3.9 Naming the backup

1. In the **Set Name** box, type a name for the backup.
2. In the **Set Type** box, select the type of backup you want to create. The list of available backup types depends on the configuration of your DS-Client.
   - Online
   - Statistical

   NOTE: For more information, see Section 5.1, “Backup types”, on page 106.
3. If you selected **Online**, do the following:
   - To configure the backup for BLM Archiver, select the **BLM (Infinite Generations)** check box. DS-Client will instruct DS-System to send a copy of the oldest generation (which is about to be overwritten) to the BLM Archiver.

     NOTE: The BLM module must be enabled.
4. If you selected **Statistical**, and want to emulate an actual backup transfer process, select the **Calculate transmit amount** check box. During the backup, specified backup files will be read from their source and processed for compression and encryption.
5. If the multitenant feature is enabled and configured, in the **Customer** list, you can select the customer to which you want to assign the backup. For more information, see Section 11.5, “Multitenant DS-Clients”, on page 634.
6. Click **Finish**.

5.5.4 Creating an NFS file system backup

You can create an NFS backup using the NFS protocol. When creating an NFS backup, consider the following:

- The DS-Client and backup source machine must be configured to use the same protocol (TCP or UDP) to perform the initial RPC-based communication and establish the NFS connection. The DS-Client uses UDP by default. You can change this setting by adding the line [*NFS Connection : tcp]* in the DS-Client configuration file (dsclient.cfg). This change will be applied to all existing and new NFS backups. To change the protocol on the Linux backup source machine, update the /etc/nfs.conf file.
- The NFS source server must be configured to export the NFS share to back up a source machine that supports NFS,
- To verify if the source server is exporting the NFS share, run the following command on DS-Client:

  `rpcinfo –p NFS_server_address`

  If it is working, nfs should be listed in the output, and you must be able to connect to the NFS share with the Linux or Mac DS-Client.
- Edit the `/etc/exports` file to get NFS to work with DS-Client. This file is on the source machine, and contains a list of entries. Each entry indicates a volume that is shared and how it is shared. An entry in /etc/exports typically looks like this:

  `directory machine1(option11,option12)`
- Save the file and restart the NFS daemon using the following command:

  `/etc/init.d/nfs restart`

NOTE: These recommendations do not consider network security requirements. Consult your network administrator and NFS documentation for full details.

5.5.4.1 Selecting the type of backup

1. On the **Sets** menu, click **New Backup Set**.
2. Select **NAS, UNIX-SSH, NFS, Local File System**, and then click **Next**.

5.5.4.2 Selecting the backup source

1. Select **NFS** and then select the source DS-Client.
2. To use the log in credentials of the selected source computer, select **Ask for local machine credentials**, and then click **Next**.
3. Type the user name and password or click **[...]** to select a user.
4. Click **OK**.
5. Click **Next**.

5.5.4.3 Selecting the backup items

1. Select the shares or directories and add them to the **Selected Items for Backup** list.
2. To add an entire directory, select the directory, and then click **Add**. Sub-directories are included by default.
   - To exclude sub-directories, clear the **Include SubDirs** check box.
3. To exclude an item when its parent directory is selected for backup, select the item, and then click **Exclude**.
4. To exclude an item using regular expressions, select the item, and then click **RegEx**.

NOTE: Regular expressions provide more specific filtering than the exclude function. For example, you can use regular expressions to exclude individual file names or patterns. Use this option only if you are familiar with the syntax.

---

5. To add files matching a filter, type the file pattern that you would like to search for in the **Filter** box.
6. To add specific files, do the following:
   a) Select the directory with the required files, and then click **Files**.
   b) Select the file you want to back up, and then click **Select**.
   - To exclude an item when its parent folder is selected for backup, select the item, and then click **Exclude.**
7. To remove an item from the list of selected items for backup, select the item, and then click **Remove**.
8. To modify an existing regular expression, select the regular expression, and then click **Modify**.
9. Click **Next**.

5.5.4.4 Selecting the backup item options

1. To configure the maximum generations for a backup item that will be stored online, double click the **Max Gen** cell, and then enter the value.
2. To back up the access control list (file permissions), select the **Back up ACL** check box.
3. Click **Next**.

5.5.4.5 Selecting the backup options

1. Configure the options you want to apply to the backup. The options are as follows:
   - **Use buffer** – Copies files to the DS-Client buffer to free up the backup source as fast as possible. The DS-Client then sends the files from the DS-Client buffer to the DS-System. This option cannot be configured if CDP is enabled. For more information, see Section 5.2.7, “Performance”, on page 113.
   - **Detailed log** – Records all files that backed up in the Activity Log. For more information, see Section 8.1, “Viewing the Activity Log”, on page 578.
   - **Initial backup** – Uses the Initial Backup feature for the first backup. To configure the initial backup path, click **[>>]**. For more information, see Section 11.1.1, “Configuring the initial backup path”, on page 618.
   - **Disable common files** – Excludes the backup files from common file storage reduction. This means duplicate files will be encrypted and backed up individually, thereby potentially increasing the stored size.

     NOTE: This feature must be activated for your DS-Client by your service provider. You can enable this option when creating the backup. This option cannot be changed afterwards.

   - **PreScan** – Flags the backup to scan all files in the backup prior to backup to display an estimated completion time for the backup.
   - **Continuous data protection** – Enables continuous data protection (CDP) for the backup. To configure the CDP settings, click **[>>]**, and beside **File Change Detection**, select a method for file change detection. The options are as follows:
     - **Generic Scanner** – Loops the scanning function from online File system backups.

- **File Alteration Monitor (Only Linux)** – You must install FAM on the target machine and the FAM daemon must be running,. It interfaces with the Linux operating system functionality of notifications for file changes. If FAM is not installed, DS-Client will try to copy and execute a FAM instance on the target Linux machine.

  a) To specify the minimum interval the DS-Client must wait before backing up a changed item or file, select **Do not back up more often than**, and then enter the interval and unit of measurement. You can set a longer interval if you do not want to back up changes frequently or a shorter interval if you want backup of changes to be more granular.

  b) To specify the minimum interval the DS-Client must wait before backing up a changed item or file after detecting that it has not changed, select **Backup if file stops changing for**, and then enter the interval and unit of measurement. This option is intended for data that you know changes frequently.

  c) Select the scheduled activities that will suspend the CDP backup process. The options are **Retention**, **BLM**, and **Validation**.

  d) Click **OK**. For more information, see Section 5.2.2, “Continuous data protection (CDP)”, on page 108.

- **Compression type** – Specifies the type of compression that will be applied to the backup. The options are as follows:

  - **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good default compression when the network is not the bottleneck.

  - **ZLIB** (**Global**, **Low**, **Medium**, and **High**) – Normally produces better compression than LZOP, but will take more time to compress. This is a good default compression when the network is the bottleneck. ZLIB High corresponds to a value of 9, ZLIB Medium=6, and ZLIB Low=3.

  - **None** – Disables compression for the backup.

2. To configure additional backup options, do the following:

   a) To force the backup of a file, even if it’s last modified time and size have not changed since the last backup, select the **Force backup even if the modified time or size did not change** check box.

   b) To enable the handling of backup of the file and hard link information for the hard links to be restored, select the **Backup hard links** check box. Even if you select this option, you must create a backup that includes all the hard linked files.

3. To specify a command to run before (Pre) and/or after (Post) the execution of the backup, click **Pre/Post**. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525 and Section 5.26, “Configuring Pre/Post processes (Linux)”, on page 528.

4. To exclude old files from being backed up, click **Exclude old files**, and then do one of the following:

   a) To include all old files, select **No exclusion**.

   b) To exclude files older than a specified period, select **Exclude files older than**, and then enter the period in days, weeks, months, or years.

   NOTE: If the backup fails, the exclude period will be extended to reflect the conditions of the failed backup until a successful backup is completed.

   c) To exclude files older than a specified date, select **Exclude files older than**, and enter the date.

   d) Click **OK**.

5. Click **Next.**

5.5.4.6 Selecting the notification options

IMPORTANT: The email and pager options are available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

1. To configure a notification, do one of the following:

   - To add a notification, click **Add**.
   - To modify a notification, select the notification, and then click **Modify**.

   NOTE: To delete a notification, select the notification, and then click **Delete**.

2. To send an email notification, select **E-Mail**, and then do the following:

   a) To send the email notification to the DS-Client administrator, select **Administrator**.

   b) To send an email to another recipient, select **Other**, and then specify the recipient’s email address.

   c) To send detailed backup information, select the **Detailed notification** check box.

   d) To include a detailed file-level backup log as an attachment, select the **Attach detailed log** check box.

      - To compress the detailed log, select the **Compress** check box.

e) To send the email notification in HTML format, select the **Send E-Mail using HTML format** check box.

NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

---

f) Click **OK**.

g) In the **Completion** box, specify under what conditions a notification will be sent, and click **OK**. The options are as follows:

- **All** – Notification will be sent under all conditions.
- **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
- **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.
- **Complete with errors** – Notification will be sent if an activity is completed with at least one error event.
- **Incomplete** – Notification will be sent if an activity is not completed successfully.

3. Under **Send SNMP traps when**, configure the DS-Client to send SNMP traps when the backup has completed successfully, completed with warnings, completed with errors, or is incomplete.
4. Click **Next**.

5.5.4.7 Assigning a retention rule

1. To assign a retention rule to the backup, do one of the following:
   - If you don’t want to assign a retention rule, select **No retention rule**.
   - To assign a retention rule, select **Use a specific retention rule**, and then select the retention rule.

NOTE: To create or edit a retention rule, click **[...]**. For more information, see Section 4.1, “Configuring a retention rule”, on page 98.

---

2. Click **Next**.

5.5.4.8 Assigning a schedule

1. To assign a schedule to the backup, do one of the following:
   - If you don't want to assign a schedule to the backup, select **Not scheduled**.
   - To assign a schedule to the backup, select **Scheduled.** In the **Available schedules** box, select an existing schedule.

   NOTE: To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, "Configuring a schedule", on page 90.

2. Click **Next**.

5.5.4.9 Naming the backup

1. In the **Set Name** box, type a name for the backup.
2. In the **Set Type** box, select the type of backup you want to create. The list of available backup types depends on the configuration of your DS-Client.
   - Online
   - Statistical

   NOTE: For more information, see Section 5.1, "Backup types", on page 106.

3. If you selected **Online**, do the following:
   - To configure the backup for BLM Archiver, select the **BLM (Infinite Generations)** check box. DS-Client will instruct DS-System to send a copy of the oldest generation (which is about to be overwritten) to the BLM Archiver.

     NOTE: The BLM module must be enabled.

4. If you selected **Statistical**, and want to emulate an actual backup transfer process, select the **Calculate transmit amount** check box. During the backup, specified backup files will be read from their source and processed for compression and encryption.
5. If the multitenant feature is enabled and configured, in the **Customer** list, you can select the customer to which you want to assign the backup. For more information, see Section 11.5, "Multitenant DS-Clients", on page 634.
6. Click **Finish**.

5.5.5 Creating a UNIX-SSH file system backup

You can create a UNIX-SSH backup using the UNIX-SSH protocol. When creating a UNIX-SSH backup, consider the following:

- The backup source machine must be a Unix file system.
- The source machine must have an OpenSSH compatible server installed and running.
- The source machine must have either Perl5 or Python installed. Alternatively, you can use the **DIRECT** option to run a specific script or binary located on the source machine.
- UNIX-SSH cannot scan the LAN to obtain an initial machine list. Therefore you must specify the IP address of the source machine or add the initial machine list to the `hostlist_ssh` file located in the installation path.
- If Perl or Python are not installed in the default path on the source machine, you must type the path in the **Advanced connection options** dialog box.

IMPORTANT: If you are logged on to a Mac DS-Client as a root user and want to connect to the source machine using an SSH connection, you must configure the **RemoteRootLogin** setting in the OpenSSH SSH daemon configuration file (./etc/ssh/sshd_config file) to **Yes**. If you want to use the computer name instead of the IP address and the source machine is not the client machine, you must add the entry for the machine in the **/etc/hosts** file of the machine where the DS-Client is running.

5.5.5.1 Selecting the type of backup

1. On the **Sets** menu, click **New Backup Set**.
2. Select **NAS, UNIX-SSH, NFS, Local File System**, and then click **Next**.

5.5.5.2 Selecting the backup source

1. Select **UNIX-SSH** and then select the source DS-Client.
2. By default, **Ask for local machine credentials** check box is selected.
3. Click **Next**.
4. In the **Ask for local machine credentials** dialog box, type a valid user name and password, and then click **OK.**

5. If for security reasons, you do not want to use a super user for remote logon to the source machine, select the **"sudo" as an alternate user** check box, and then do the following:

NOTE: The regular user must have privileges to connect to the SSH server on the source machine. Both regular and alternate users must be listed in the 'sudoers' file on the source machine. A regular user must have privileges to run the `/usr/bin/perl` or `/usr/bin/python` command on the source machine as the alternate user. If you have Perl or Python installed in a different path, each 'sudoers' user must be able to run Perl or Python from that installed path. For more information, see *'sudo'* documentation.

---

   a) In the **User Name** box, enter a valid user name.

   b) In the **Password** box, type the corresponding password or passphrase which is applicable only for UNIX-SSH.

   c) In the **Private Key File** box, click **[>>]**, and select the private key file. Using this key, you can back up and restore using SSH public key authentication.

      - If no private key is specified, and a default private key is found on the DS-Client machine, you must first try the public key authentication. If that fails, try password authentication.
      - If no default key is found, try password authentication only.
      - If a private key file is specified for the backup, the SSH connection will use the public key authentication only.

   d) Click **OK**.

6. To view or edit connection options for the selected backup, select the **Advanced connection options** check box, and then do the following:

   a) In the **Access interface** box, select the script language to run on the backup source computer from PERL, PYTHON or DIRECT.

NOTE: Use the script language DIRECT only if you have a specific binary on the target computer that will perform the backup and restore.

---

   b) In the **Interpreter/Program path**, enter the path to the PERL/PYTHON/DIRECT binary on the target computer.

   c) Click **OK**.

7. Click **Next**.

5.5.5.3 Selecting the backup items

1. Under **Shares & Directories List**, select the shares/directories and add them to the **Selected Items for Backup** list.
2. To add an entire directory, select the directory, and then click **Add**. Sub-directories are included by default.
   - To exclude sub-directories, clear the **Include SubDirs** check box.
   - To exclude an item when its parent folder is selected for backup, select the item, and then click **Exclude.**
3. To exclude an item using regular expressions, select the item, and then click **RegEx**.

NOTE: Regular expressions provide more specific filtering than the exclude function. For example, you can use regular expressions to exclude individual file names or patterns. Use this option only if you are familiar with the syntax.

---

4. To search for files that match a certain criteria, in the **Filter** box, type the file pattern you want to search for in the selected folder. For example, *.doc will search for all the files with the doc file extension.
5. To modify a regular expression, select the regular expression, and then click **Modify**.
6. To remove an item from the list, select the item, and then click **Remove**.

NOTE: Removing an item will not remove previous backups of that item. To remove previously backed-up data, you must use the Delete function.

---

7. Click **Next**.

5.5.5.4 Selecting the backup item options

1. To configure the maximum generations for a backup item that will be stored online, double click the **Max Gen** cell, and then enter the value.
2. To back up the access control list (file permissions), select the **Back up ACL** check box.
3. To back up the Security Enhanced Linux attribute of files or folders for Local File System and SSH backups, select the **Backup SElinux** check box.

NOTE: For SSH backups with Perl (default), the target Linux machine must have the *Linux-UserXAttr* package installed and for SSH backups with Python, the target Linux machine must have the *pyxattr* package installed for this option to appear.

---

4. Click **Next**.

5.5.5.5 Selecting the backup options

1. Under **Backup options**, configure the options you want to apply to the backup. The options are as follows:
   - **Use buffer** –Copies files to the DS-Client buffer to free up the backup source as fast as possible. The DS-Client then sends the files from the DS-Client buffer to the DS-System. This option cannot be configured if CDP is enabled. For more information, see Section 5.2.7, “Performance”, on page 113.
   - **Detailed log** – Records all files that backed up in the Activity Log. For more information, see Section 8.1, “Viewing the Activity Log”, on page 578.
   - **Disable common files** – Excludes the backup files from common file storage reduction. This means duplicate files will be encrypted and backed up individually, thereby potentially increasing the stored size.

     NOTE: This feature must be activated for your DS-Client by your service provider. You can enable this option when creating the backup. This option cannot be changed afterwards.

   - **Initial backup** – Uses the Initial Backup feature for the first backup. To configure the initial backup path, click **[>>]**. For more information, see Section 11.1.1, “Configuring the initial backup path”, on page 618.
   - **PreScan** – Flags the backup to scan all files in the backup prior to backup to display an estimated completion time for the backup.

- **Continuous data protection** – Enables continuous data protection (CDP) for the backup. To configure the CDP settings, click **[>>]**, and beside **File Change Detection**, select a method for file change detection. The options are as follows:
  - **Generic Scanner** – Loops the scanning function from online File system backups.
  - **File Alteration Monitor (Only Linux)** – You must install FAM on the target machine and the FAM daemon must be running,. It interfaces with the Linux operating system functionality of notifications for file changes. If FAM is not installed, DS-Client will try to copy and execute a FAM instance on the target Linux machine.

  a) To specify the minimum interval the DS-Client must wait before backing up a changed item or file, select **Do not back up more often than**, and then enter the interval and unit of measurement. You can set a longer interval if you do not want to back up changes frequently or a shorter interval if you want backup of changes to be more granular.

  b) To specify the minimum interval the DS-Client must wait before backing up a changed item or file after detecting that it has not changed, select **Backup if file stops changing for**, and then enter the interval and unit of measurement. This option is intended for data that you know changes frequently.

  c) Under **Suspend Backup for Scheduled**, select the scheduled activities that will suspend the CDP backup process. The options are **Retention**, **BLM**, and **Validation**.

  d) Click **OK**. For more information, see Section 5.2.2, “Continuous data protection (CDP)”, on page 108.
- **Stop on errors** – Enter the maximum number of errors at which a backup will be stopped.
- **Compression type** – Specifies the type of compression that will be applied to the backup. The options are as follows:
  - **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good default compression when the network is not the bottleneck.
  - **ZLIB** (**Global**, **Low**, **Medium**, and **High**) – Normally produces better compression than LZOP, but will take more time to compress. This is a good default compression when the network is the bottleneck. ZLIB High corresponds to a value of 9, ZLIB Medium=6, and ZLIB Low=3.
  - **None** – Disables compression for the backup.

2. To configure additional backup options, do the following:

a) To back up only the mount point, select the **Do not follow the mount point** check box.

b) To force the backup of a file, even if it's last modified time and size have not changed since the last backup, select the **Force backup even if the modified time or size did not change** check box.

c) To enable the handling of backup of the file and hard link information for the hard links to be restored, select the **Backup hard links** check box. Even if you select this option, you must create a backup that includes all the hard linked files.

3. To specify a command to run before (Pre) and/or after (Post) the execution of the backup, click **Pre/Post**. For more information, see Section 5.26, "Configuring Pre/Post processes (Linux)", on page 528.

4. To exclude old files from being backed up, click **Exclude old files**, and then do one of the following:

   a) To include all old files, select **No exclusion**.

   b) To exclude files older than a specified period, select **Exclude files older than**, and then enter the period in days, weeks, months, or years.

   NOTE: If the backup fails, the exclude period will be extended to reflect the conditions of the failed backup until a successful backup is completed.

   c) To exclude files older than a specified date, select **Exclude files older than**, and enter the date.

   d) Click **OK**.

5. Click **Next.**

5.5.5.6 Selecting the notification options

IMPORTANT: The email and pager options are available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

1. To configure a notification, do one of the following:
   - To add a notification, click **Add**.
   - To modify a notification, select the notification, and then click **Modify**.

   NOTE: To delete a notification, select the notification, and then click **Delete**.

2. To send an email notification, select **E-Mail**, and then do the following:
   a) To send the email notification to the DS-Client administrator, select **Administrator**.
   b) To send an email to another recipient, select **Other**, and then specify the recipient’s email address.
   c) To send detailed backup information, select the **Detailed notification** check box.
   d) To include a detailed file-level backup log as an attachment, select the **Attach detailed log** check box.
   e) To compress the detailed log, select the **Compress** check box.
   f) To send the email notification in HTML format, select the **Send E-Mail using HTML format** check box.

   NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

   g) Click **OK**.
   h) In the **Completion** box, specify under what conditions a notification will be sent, and click **OK**. The options are as follows:
      - **All** – Notification will be sent under all conditions.
      - **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
      - **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.

- **Complete with errors** – Notification will be sent if an activity is completed with at least one error event.
- **Incomplete** – Notification will be sent if an activity is not completed successfully.

3. Configure the DS-Client to send SNMP traps when the backup has completed successfully, completed with warnings, completed with errors, or is incomplete.
4. Click **Next**.

5.5.5.7 Assigning a retention rule

1. To assign a retention rule to the backup, do one of the following:
   - If you don't want to assign a retention rule, select **No retention rule**.
   - To assign a retention rule, select **Use a specific retention rule**, and then select the retention rule.

NOTE: To create or edit a retention rule, click **[...]**. For more information, see Section 4.1, "Configuring a retention rule", on page 98.

---

2. Click **Next**.

5.5.5.8 Assigning a schedule

1. To assign a schedule to the backup, do one of the following:
   - If you don't want to assign a schedule to the backup, select **Not scheduled**.
   - To assign a schedule to the backup, select **Scheduled.** In the **Available schedules** box, select an existing schedule.

NOTE: To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, "Configuring a schedule", on page 90.

---

2. Click **Next**.

5.5.5.9 Naming the backup

1. In the **Set Name** box, type a name for the backup.
2. In the **Set Type** box, select the type of backup you want to create. The list of available backup types depends on the configuration of your DS-Client.
   - Online
   - Statistical

   NOTE: For more information, see Section 5.1, “Backup types”, on page 106.
3. If you selected **Online**, do the following:
   - To configure the backup for BLM Archiver, select the **BLM (Infinite Generations)** check box. DS-Client will instruct DS-System to send a copy of the oldest generation (which is about to be overwritten) to the BLM Archiver. The BLM module must be enabled.
4. If you selected **Statistical**, and want to emulate an actual backup transfer process, select the **Calculate transmit amount** check box. During the backup, specified backup files will be read from their source and processed for compression and encryption.
5. If the multitenant feature is enabled and configured, in the **Customer** list, you can select the customer to which you want to assign the backup. For more information, see Section 11.5, “Multitenant DS-Clients”, on page 634.
6. Click **Finish**.

5.5.6 Restoring a NAS, NFS, UNIX-SSH file system backup

You can restore a NAS, NFS, or UNIX-SSH File system backup.

5.5.6.1 Selecting the restore items

1. Browse the backups tree and select the backup you want to restore.
2. On the **Restore** menu click **Restore Now**.
3. To restore an entire backup or folder, browse the tree and select the check box beside the backup or folder you want to restore.
4. To restore individual files, select the older containing the required files, click **Show Files**, and then do one of the following:
   - To view details about the backed up file, select the file, and then click **File Info**.
   - To view modified files, click **Show Modified**.
   - To view archived files, click **Show Archived**.
5. To view the number of files selected and calculate the total amount of files selected, select the **Calculate amount** check box.
6. To exclude subdirectories, clear the **Include SubDirs** check box, as the default setting is to include sub-directories.
7. To search for files that match a certain criteria, in the **Filter** box, type the file pattern that you want to search for in the selected folder. For example, *.doc will search for all files with the doc file extension.
8. To search for a specific backed up file, click **Find File**. In the **Find Backed Up File** dialog box, do the following:
   a) Under **Search for**, select the search criteria to search for a backed up file either by **File name** or by **File ID**.
   b) Click **Find**.
   c) Select the required backed up file, and then click **Select**.
9. To view the details of the items you selected, click **Selection**.
10. To refine your selection of items to restore, click **Advanced**. Under **Show**, select which generation you want to display. The options are as follows:
    - To restore the latest generation of all the files, select **Latest generation of all data**.

- To restore files that were deleted from the source, but not removed from the online storage as of the last backup session, select **Latest generation of all data (except deleted data)**.
- To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:

  a) Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.

  b) Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.

  c) Click **OK**.

11. Under **Filter**, select the type of filter you want to apply to the backups. The options are as follows:
    - **Show all data** – No filter is applied.
    - **Hide data (dirs/files) deleted from source on/before** – You can hide backed up data (directories and files) that was intentionally deleted from the source computer.
    - **Show only data (dirs/files) deleted from source on/before** – You can view and restore backed up data (directories and files) that was intentionally deleted from the source computer.

    NOTE: This options are available only if the restore or request wizard can use the DS-Client database to filter the backups. It does not appear for BLM Image Restore or Disc/Tape Restore, since they have been written to media and are no longer synchronized with the DS-Client database.

    ---

12. Under **File overwrite**, select how files are restored. The options are as follows:
    - **Restore all** – All selected files are restored to the destination folder. Files with the same name are overwritten.
    - **Restore newer** – Only files newer than those in the destination folder are restored.
    - **Restore older** – Only files with older than those in the destination folder are restored.
    - **Restore different** – Only files with different dates/sizes than those in the destination folder are restored.
    - **Skip existing** – Existing files with the same name in the destination folder are not restored.
13. Click **OK**.
14. Click **Next**.

5.5.6.2 Selecting the restore location

1. Select the location to which you want to restore the backup. The options are as follows:
   - **Original location** – Data is restored to the original backup source location and existing files with the same name are overwritten. This is the default option.
   - **Alternate location** – Data is restored to a location other than the original backup source.

   NOTE: When restoring to an alternate location, the security of restored items in the destination location might not resemble the security of those items during backup.

2. If you selected **Alternate location**, then do the following:
   a) Beside the **Alternate location** box, click **[>>]**.
   b) In the **Select Alternate location** dialog box, select the server to which you want to restore.
   c) If you selected directory under **Local File System** as the destination location, then do the following:
      1. To enter the credentials for the source or database server that initiates the connection, select the **Ask for local machine credentials** check box, and then click **Select**.
      2. In the **Ask for local machine credentials** dialog box, enter the required credentials, and then click **OK**.
   d) If you selected a **NAS** component as the destination location, then do the following:
      1. To enter the credentials for the source or database server that initiates the connection, select the **Ask for local machine credentials** check box, and then click **Select**.
      2. In the **Ask for local machine credentials** dialog box, enter the required credentials, and then click **OK**.

   NOTE: The Ask for NAS API credentials check box is selected by default.

   e) If you selected a DS-Client belonging to a **NFS** as the destination location, then do the following:

1. To enter the credentials for the source or database server that initiates the connection, select the **Ask for local machine credentials** check box, and then click **Select**.
2. In the **Ask for local machine credentials** dialog box, enter the required credentials, and then click **OK**.

f) If you selected a **UNIX SSH** component as the destination location, then do the following:

1. To enter the credentials for the source or database server that initiates the connection, select the **Ask for local machine credentials** check box, click **Select**, enter the required credentials, and then click **OK**.
2. If for security reasons, you do not want to use a super user for remote logon to the source machine, select the **"sudo" as an alternate user** check box, click **Select,** enter the required credentials, and then click **OK**.

g) To view or edit connection options for the selected backup, select the **Advanced connection options** check box, and then do the following:

1. In the **Access interface** box, select the script language to run on the backup source computer from PERL, PYTHON or DIRECT.

NOTE: Use the script language DIRECT only if you have a specific binary on the target computer that will perform the backup and restore.

---

2. In the **Interpreter/Program path**, enter the path to the PERL/PYTHON/DIRECT binary on the target computer.
3. Click **OK**.

NOTE: After you select a computer as the alternate location, you must specify a share location

---

h) In the **Destination** cell, select a share location.

i) Click in the **Restore to** cell and type the name of the directory or click **[>>]** and select a directory.

j) In the **Truncate** box, you can increase the truncate level to shorten the common portion of the restore path, if the selected restore items contain a common path.

NOTE: If the entire path is truncated, the alternate location directory will inherit the security of the truncated parent directory.

---

3. Click **Next**.

NOTE: For more information, see Section 5.3.3, “Restoring data to an alternate location”, on page 130.

5.5.6.3 Selecting the restore options

1. Beside **Restore permissions**, select a restore option for permissions. The options are as follows:
   - **Yes** – Restores the permissions for all the backed up files.
   - **Only** – Restores permissions for the selected files and directories only. This will apply permissions only to existing files on the destination volume.
   - **Skip** – Skips the file security information of the backed up files. Newly created files and folders inherit the security settings of the parent folder.
2. Beside **Restore Method**, select a method for DS-Client to complete the restore. The options are as follows:
   - **Save** – Restores files to a temporary location first to prevent restored files from overwriting an existing file. If the file is restored successfully, the original file is overwritten with the temporary file.
   - **Use buffer** – Restores files to the DS-Client buffer first and then transfers the files to the restore destination. This method minimizes the duration for which the restore process occupies the destination server.
   - **Fast** – Uses a direct restore method by writing data as it is received.

     NOTE: If you selected the fast method, files in the destination location are overwritten upon receipt of the first byte of data.
3. To skip the pre and post restore processes, select the **Skip Pre/Post** check box. If this check box is cleared, the DS-Client runs a specified activity before and/or after a restore operation. For more information, see Section 5.26, “Configuring Pre/Post processes (Linux)”, on page 528.
4. To record all restored files in the Activity Log, select the **Detailed log** check box.
5. Click **Next**.

5.5.6.4 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. Click **Finish**.

5.6 Email backups (Windows)

You can back up and restore email at the individual message level. Restoring a message or mailbox is faster than rolling back an entire database to the last backup. Depending on the email server type, DS-Client uses two different methods to support the backup and restore of email at the individual message level.

5.6.1 Microsoft Exchange Server (ESW) requirements

You can back up and restore the following data from an on-premises Microsoft Exchange Server using Exchange Web Services (EWS).

- Emails
- Calendars and appointments
- Contacts (including Contact Lists, but not Contact Groups)
- Tasks

NOTE: Exchange Online data must be in a user mailbox, shared mailbox, or resource mailbox and can be restored to the same mailbox or a different mailbox on the original domain or a different domain.

Before performing a backup or restore of data from an on-premises Microsoft Exchange Server using EWS, do the following:

- Configure the settings in the Local Group Policy Editor as follows:
  1. Click **Start** and then **Run**.
  2. Type gpedit.msc.
  3. In the Group Policy Object Editor, browse to Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Client.
  4. Set up the authentication as follows:

```
Allow Basic Authentication : Enabled
Allow CredSSPauthentication : Not configured
Allow unencrypted traffic : Enabled
Disallow Digest authentication : Not configured
```

```
Disallow Kerberos authentication : Not configured
Disallow Negotiate authentication : Enabled
Trusted Hosts : Enabled
```

NOTE: When you enable Trusted Hosts, you must add the computer name of the on-premises Microsoft Exchange Server or add * to the TrustedHostsList.

- Enable Windows Authentication for the virtual directory in IIS as follows:
  1. On the on-premises Microsoft Exchange Server, open Internet Information Services Manager (IIS).
  2. Browse to the default web site/EWS folder.
  3. For the Windows Authentication folder, set the status to **Enabled**. The authentication settings should appear as follows:

     ```
     Anonymous Authentication : Disabled
     ASP .NET Impersonation : Disabled
     Basic Authentication : Enabled
     Digest Authentication : Disabled
     Forms Authentication : Disabled
     Windows Authentication : Enabled
     ```
  4. Enable Basic Authentication for EWS as follows:
     a) Go to the administrative settings for your on-premises Microsoft Exchange Server (https://<server>/ecp), where <server> is the IP address, host name, or FQDN at which the Microsoft Exchange Server can be accessed.
     b) In the Exchange Admin Center, click **Servers** to go to your on-premises Exchange Server.
     c) Click **Virtual directories** and double-click **EWS**.
     d) Under Authentication, select **Basic authentication**.
- Configure the credentials that will be used for backing up the Microsoft Exchange data. Each user account must be associated with a user mailbox. Configure each user as follows:
  1. Go to the administrative settings for your on-premises Microsoft Exchange Server (https://<server>/ecp), where <server> is the IP address, host name, or FQDN at which the Microsoft Exchange Server can be accessed.
  2. Add users to Discovery Management as follows:
     a) Go to **permissions** > **admin roles**.
     b) In the list, select **Discovery Management**, and then click the Edit button.

c) In the pop-up window, under Members, click **+**.

d) In a new pop-up window, select the user you need to add, click **add**, and then click **OK**.

e) In the first pop-up window, click **Save**.

f) In the admin roles pane, verify that the user you need to add is listed under Members of the Discovery Management group.

3. Add users to Organization Management as follows:

a) Go to the administrative settings for Exchange.

b) Go to **permissions** > **admin roles**.

c) In the list, select **Organization Management**, and then click the Edit button.

d) In the pop-up window, under Members, click **+**.

e) In a new pop-up window, select the user you need to add, click **add**, and then click **OK**.

f) In the first pop-up window, click **Save**.

g) In the admin roles pane, verify that the user you need to add is listed under Members of the Organization Management group.

4. Add application impersonation as an assigned role in Organization Management as follows:

a) Go to **permissions** > **admin roles**.

b) In the list, select **Organization Management**, and then click the Edit button.

c) In the pop-up window, under Role, click **+**.

d) In a new pop-up window, select **ApplicationImpersonation**, click **add**, and then click **OK**.

e) In the first pop-up window, click **Save**.

f) In the admin roles pane, verify that **ApplicationImpersonation** is listed under Assigned Roles of the Organization Management group.

NOTE: Backups can fail if the DS-Client does not have access to multiple credentials or if concurrent backup activities use the same credentials.

The minimum number of credentials required is proportional to the maximum number of concurrent activities, which is configured using the MaxSessions advanced configuration parameter.

- When the MaxSessions parameter value is 4 or less, you must provide at least one credential per DS-Client.

- When the MaxSessions parameter value is between 5 and 8, you must provide at least two credentials per DS-Client.
- When the MaxSessions parameter value is between 9 and 12, you must provide at least three credentials per DS-Client.

IMPORTANT: Each credential you provide can support no more than four concurrent activities.

- To exclude SMTP addresses not associated with a mailbox, set the **ExchangeOnlineExcludeGroupMailboxes** value to **Yes**. This automatically makes distribution groups, deleted users, and other email addresses that do not have a mailbox unavailable for selection.

NOTE: If this parameter is not enabled, you must ensure distribution groups are not selected alongside mailboxes that you have manually selected for backup in a Microsoft 365 backup.

5.6.2 Microsoft Outlook (DS-MLR) requirements

You can back up and restore data at the individual message level from Microsoft Outlook using DS-MLR (Message Level Restore). DS-MLR is a Windows service that searches for email based on a user-defined filter, then transforms each email into a data stream that is passed to the DS-Client for processing and then backed up to the DS-System.

The DS-Client scans all email data and backs up only the new or changed items to the DS-System. You can perform message-level backups and restore email data at the message level to the original or an alternate location.

Before backing up Microsoft Outlook data using DS-MLR, consider the following:

- Ensure Microsoft Outlook is closed during backup activities. Backup is successful only when Microsoft Outlook is closed.
- If you have configured Microsoft Outlook to use a .PST file on a remote machine, the DS-MLR service must be installed on the computer with Outlook.
- If Microsoft Outlook is configured for Microsoft Exchange profiles, the emails are located on the Microsoft Exchange Server. To access those emails, the DS-MLR service account must have the Receive-As privilege on that Microsoft Exchange Server. The DS-MLR service account must be recognized on the Microsoft Exchange Server.
- The DS-MLR service must be installed and running on the same machine where the emails are stored and DS-Recovery Tools must be enabled on the DS-System by your service provider. For more information, see the *Client Software Installation Guide* and *DS-System User Guide*.

5.6.3 Creating a Microsoft Exchange Server (EWS) backup

You can back up emails from a Microsoft Exchange Server using EWS.

5.6.3.1 Selecting the type of backup

1. On the **Sets** menu, click **New Backup Set**.
2. Select **E-Mail Messages**, and then click **Next**.

5.6.3.2 Selecting the E-mail Server type

1. Select **Microsoft Exchange Server (using EWS)**.
2. Click **Next**.

5.6.3.3 Selecting the backup source

1. In the **Path** box, type the IP address of the Exchange server from which you want to back up data.
2. To provide the credentials for the selected computer, select the **Ask for Network Credentials** check box. You will be prompted to enter a valid user name and password for the selected computer.

NOTE: By default, your credentials for DS-Client will be used to connect to the selected computer.

---

3. In the **Enter Network Credentials** dialog box, do the following:
   a) In the **Connect as** box, type an existing user name that has the required permissions and license.
   b) In the **Password** box, type the corresponding password.
   c) In the **From** box, type the domain name (case sensitive) of the backup source.
   d) Click **OK**.
4. Click **Next**.

5.6.3.4 Selecting the backup items

1. To add an item, select the item, and then click **Add**.

NOTE: You can add only one item at a time. Subdirectories are included by default. To exclude subdirectories, clear the Include SubDirs check box.

---

2. To exclude an item when its parent folder is selected for backup, select the item, and then click **Exclude.**
3. To exclude an item using regular expressions, select the item, and then click **RegEx**.

NOTE: Regular expressions provide more specific filtering than the exclude function. For example, you can use regular expressions to exclude individual file names or patterns. Use this option only if you are familiar with the syntax.

---

4. To add individual items inside a folder, do the following:
   a) Expand the mailbox, select the folder, and then click **Items**.
   b) Select the individual emails or entries that you want to specify, and then click **Add**.
      - To prevent an item from being backed up, select the individual item, and then click **Exclude**.
   c) Click **Finish**.
5. To remove an item from the list of selected items for backup, select the item, and then click **Remove**.
6. To modify an existing regular expression, select the regular expression, and then click **Modify**.
7. Click **Next**.

5.6.3.5 Selecting the backup item options

1. To configure the maximum generations for a backup item that will be stored online, double click the **Max Gen** cell, and then enter the value.
2. Click **Next**.

5.6.3.6 Selecting the backup options

1. Under **Backup options**, configure the options you want to apply to the backup. The options are as follows:

   - **Use buffer** – Copies files to the DS-Client buffer to free up the backup source as fast as possible. The DS-Client then sends the files from the DS-Client buffer to the DS-System. This option cannot be configured if CDP is enabled. For more information, see Section 5.2.7, “Performance”, on page 113.
   - **Detailed log** – Records all files that are backed up in the Activity Log. For more information, see Section 8.1, “Viewing the Activity Log”, on page 578.
   - **Initial backup** – Uses the Initial Backup feature for the first backup. To configure the initial backup path, click **[>>]**. For more information, see Section 11.1.1, “Configuring the initial backup path”, on page 618.
   - **Continuous data protection** – Enables continuous data protection (CDP) for the backup. To configure the CDP settings, click **[>>]**, and then do the following:

     a) In the **File Change Detection** box, **Windows Built-in File Monitoring** is automatically selected and cannot be changed.

     b) To specify the minimum interval the DS-Client must wait before backing up a changed item or file, select **Do not back up more often than**, and then enter the interval and unit of measurement. You can set a longer interval if you do not want to back up changes frequently or a shorter interval if you want the backup of changes to be more granular.

     c) To specify the minimum interval the DS-Client must wait before backing up a changed item or file after detecting that it has not changed, select **Backup if file stops changing for**, and then enter the interval and unit of measurement. This option is intended for data that you know changes frequently.

     d) Under **Suspend Backup for Scheduled**, select the scheduled activities that will suspend the CDP backup process. The options are **Retention**, **BLM**, and **Validation**.

     e) Click **OK**. For more information, see Section 5.2.2, “Continuous data protection (CDP)”, on page 108.

   - **Stop on errors** – Stops a backup process when the number of errors reaches the specified value. A value of 0 means the DS-Client does not stop a backup process regardless of the number of errors.

   NOTE: You can configure the default setting using the **MaxErrors** advanced configuration parameter. For more information, see Section 2.1.8.6, “Miscellaneous parameters (Windows)”, on page 42.

- **Compression type** – Specifies the type of compression that will be applied to the backup. The options are as follows:
  - **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good default compression when the network is not the bottleneck.
  - **ZLIB (Global, Low, Medium, and High)** – Normally produces better compression than LZOP, but will take more time to compress. This is a good default compression when the bottleneck is the network. ZLIB Low corresponds to a value of 3, ZLIB Medium = 6, and ZLIB High = 9.
  - **None** – Disables compression for the backup.

2. To specify a command to run before (Pre) and/or after (Post) the execution of the backup, click **Pre/Post**. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525 and Section 5.26, “Configuring Pre/Post processes (Linux)”, on page 528.

5.6.3.7 Selecting the notification options

1. To configure a notification, do one of the following:
   - To add a notification, click **Add.**
   - To modify a notification, select the notification, and then click **Modify.**

NOTE: To delete a notification, select the notification, and then click **Delete**.

---

2. To send an email notification, select **E-Mail**. and then do the following:
   a) To send the email notification to the DS-Client administrator, select **Administrator**.
   b) To send an email to another recipient, select **Other**, and then specify the recipients email address.
   c) To send detailed backup information, select the **Detailed notification** check box.
   d) To include a detailed file-level backup log as an attachment, select the **Attach detail log** check box.
   e) To send the email notification in HTML format, select the **Send E-Mail using HTML format** check box.

NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

---

f) Click **OK**.

3. To send a pager notification, select **Pager**. The notification will be sent to the pager account configured for the DS-Client.

NOTE: The pager option is available only if the DS-Client has been configured for pager notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

---

4. To send a broadcast notification, select **Broadcast**. Select the server containing the messenger service to which you want to send the message and click **OK**.

NOTE: Broadcast notifications to domains or workgroups are limited to 128 characters.

---

5. To send an event notification, select **Event**. Select the server on which you want the notification to be recorded in the Event Log and click **OK**.
6. In the **Completion** box, specify under what conditions a notification will be sent, and click **OK**. The options are as follows:
   - **All** – Notification will be sent under all conditions.
   - **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
   - **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.
   - **Completed with errors** – Notification will be sent if an activity is completed with at least one error event.
   - **Incomplete** – Notification will be sent if an activity is not completed successfully.
7. Under **Send SNMP Traps when**, configure the DS-Client to send SNMP traps when the backup has completed successfully, completed with warnings, completed with errors, or is incomplete.
8. Click **Next**.

5.6.3.8 Assigning a retention rule

1. To assign a retention rule to the backup, do one of the following:
   - If you don't want to assign a retention rule, select **No retention rule**.
   - To assign a retention rule, select **Use a specific retention rule**, and then select the retention rule.

NOTE: To create or edit a retention rule, click **[...]**. For more information, see Section 4.1, "Configuring a retention rule", on page 98.

---

2. Click **Next**.

5.6.3.9 Assigning a schedule

1. To assign a schedule to the backup, do one of the following:
   - If you don't want to assign a schedule to the backup, select **Not scheduled**.
   - To assign a schedule to the backup, select **Scheduled.** In the **Available schedules** box, select an existing schedule.

NOTE: To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, "Configuring a schedule", on page 90.

---

2. Click **Next**.

5.6.3.10 Naming the backup

1. In the **Set name** box, type a name for the backup.
2. In the **Set type** box, select the type of backup you want to create. The list of available backup types depends on the configuration of your DS-Client.
   - Online
   - Statistical

NOTE: For more information, see Section 5.1, "Backup types", on page 106.

---

3. If you selected **Online**, do the following:

a) To send a copy of the oldest generation of the file that is about to be overwritten from the DS-System to the BLM Archiver, select the **BLM (Infinite Generations)** check box.

NOTE: The Backup Lifecycle Management tool must be enabled for the DS-Client.

---

b) To save a copy of the backup data to a local storage location on the DS-Client computer, select the **Save on Local Storage** check box.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Self-contained and Local Only backups.

---

c) To use the local storage as a cache if the DS-Client loses connection with the DS-System, select the **Transmission cache on Local Storage** check box. The cached backup data will be sent to the DS-System on the next connection after synchronization.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path.

---

d) To save a copy of the backup data to the instant recovery vault, select the **Save in instant recovery vault** check box.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Instant Recovery backups.

---

e) Beside the **Local Storage Path** box, click **>>**. Enter a local storage path for the backup, and then click **OK**

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

4. If you selected **Statistical**, and want to emulate an actual backup transfer process, select the **Calculate transmit amount** check box. During the backup, specified backup files will be read from their source and processed for compression and encryption.
5. If the multitenant feature is enabled and configured, in the **Customer** list, you can select the customer to which you want to assign the backup. For more information, see Section 11.5, “Multitenant DS-Clients”, on page 634.

6. Click **Finish**.

5.6.4 Restoring a Microsoft Exchange Server (EWS) backup

You can restore a Microsoft Exchange Server (EWS) backup.

5.6.4.1 Selecting the restore items

1. Browse the backups tree and select the backup items you want to restore.
2. On the **Restore** menu, click **Restore Now**.
3. To restore an entire backup or folder, browse the tree and select the check box beside the backup or folder you want to restore.
4. To restore individual files, select the folder containing the required files, click **Show Files**, and then do the following:
   - To view details about the backed up file, select the file, and then click **File Info**.
   - To view modified files, click **Show Modified**.
   - To view archived files, click **Show Archived**.
5. To view the number of files selected and calculate the total amount of files selected, select the **Calculate amount** check box.
6. To exclude subdirectories, clear the **Include SubDirs** check box, as the default setting is to include sub-directories.
7. To search for files that match a certain criteria, in the **Filter** box, type the file pattern that you want to search for in the selected folder. For example, *.doc will search for all files with the doc file extension.
8. To search for a specific backed up file, click **Find File**. In the **Find Backed Up File** dialog box, do the following:
   a) Under **Search for**, select the search criteria to search for a backed up file either by **File name** or by **File ID**.
   b) Click **Find**.
   c) Select the required backed up file, and then click **Select**.
9. To refine your selection of items to restore, click **Advanced**. Under **Show**, select which generation you want to display. The options are as follows:
   - To restore the latest generation of all the files, select **Latest generation of all data**.

- To restore files that were deleted from the source, but not removed from the online storage as of the last backup session, select **Latest generation of all data (except deleted data)**.
- To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:
  1. Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.
  2. Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.
  3. Click **OK**.

10. Click **Next**.

5.6.4.2 Selecting the restore location

1. Select the location to which you want to restore the backup. The options are as follows:
   - **Original location** – Data is restored to the original backup source location and existing files with the same name are overwritten. This is the default option.
   - **Alternate location** – Data is restored to a location other than the original backup source.

   NOTE: When restoring to an alternate location, the security of restored items in the destination location might not resemble the security of those items during backup.

2. If you selected **Alternate location**, then do the following:
   a) Beside the **Alternate location** box, click **[>>]**.
   b) In the **Select Alternate Server** dialog box, select the computer where you want to restore the data.
   c) To provide the credentials for the selected computer, select the **Ask for Network Credentials** checkbox, and then click **Select**.
   d) In the **Enter Network Credentials** dialog box, enter the credentials to connect to the destination computer, and then click **OK**.
   e) In the **Restore to** cell, type the name of the folder or click **[>>]** and select a folder.
3. To restore data to a location on the DS-Client computer, select the **Restore to local disk** check box, and then click **[>>]** to specify the location.

4. To archive Microsoft Exchange data to a PST file, select the **Archive restored files to PST** check box. This option is available if you have selected restore to local disk.
5. In the **Truncate** box, you can increase the truncate level to shorten the common portion of the restore path, if the selected restore items contain a common path.

NOTE: For more information, see Section 5.3.3, “Restoring data to an alternate location”, on page 130.

---

6. Click **Next**.

5.6.4.3 Selecting the restore options

The restore options are selected by default and cannot be changed. Click **Next**.

5.6.4.4 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, under **Restore classification**, select the type of restore. The options are as follows:
   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.
3. Click **Finish**.

5.6.5 Creating a Microsoft Outlook (DS-MLR) backup

You can create a backup for the purpose of backing up email data at the individual message level from Microsoft Outlook using DS-MLR.

5.6.5.1 Selecting the type of backup

1. On the **Sets** menu, click **New Backup Set**.
2. Select **E-Mail Messages**, and then click **Next**.

5.6.5.2 Selecting the E-mail server type

1. Select **Microsoft Outlook**.
2. Click **Next**.

5.6.5.3 Selecting the backup source

1. In the **Path** box, type the IP address or computer name of the server.
2. To provide the credentials for the selected computer, select the **Ask for Network Credentials** check box.
3. In the **Enter Network Credentials** dialog box, do the following:
   a) In the **Connect as** box, type an existing user name that has the required permissions and license.
   b) In the **Password** box, type the corresponding password.
   c) In the **From** box, type the domain name (case sensitive) of the backup source.
   d) Click **OK**.
4. Click **Next**.

5.6.5.4 Selecting the backup items

1. To add an item, select the item, and then click **Add**.

NOTE: You can add only one item at a time. Subdirectories are included by default. To exclude subdirectories, clear the Include SubDirs check box.

---

2. To exclude an item when its parent folder is selected for backup, select the item, and then click **Exclude.**
3. To exclude an item using regular expressions, select the item, and then click **RegEx**.

NOTE: Regular expressions provide more specific filtering than the exclude function. For example, you can use regular expressions to exclude individual file names or patterns. Use this option only if you are familiar with the syntax.

---

4. To add individual items inside a folder, do the following:
   a) Expand the mailbox, select the folder, and then click **E-Mails**.
   b) Select the individual emails or entries that you want to back up, and then click **Add**.
      - To prevent an item from being backed up, select the individual item, and then click **Exclude**.
   c) Click **Finish**.
5. To remove an item from the list of selected items for backup, select the item, and then click **Remove**.
6. To modify an existing regular expression, select the regular expression, and then click **Modify**.
7. Click **Next**.

5.6.5.5 Selecting the backup item options

1. To configure the maximum generations for a backup item that will be stored online, double click the **Max Gen** cell, and then enter the value.
2. Click **Next**.

5.6.5.6 Selecting the backup options

1. Under **Backup options**, configure the options you want to apply to the backup. The options are as follows:

   - **Use buffer** – Copies files to the DS-Client buffer to free up the backup source as fast as possible. The DS-Client then sends the files from the DS-Client buffer to the DS-System. This option cannot be configured if CDP is enabled. For more information, see Section 5.2.7, “Performance”, on page 113.
   - **Detailed log** – Records all files that are backed up in the Activity Log. For more information, see Section 8.1, “Viewing the Activity Log”, on page 578.
   - **Initial backup** – Uses the Initial Backup feature for the first backup. To configure the initial backup path, click **[>>]**. For more information, see Section 11.1.1, “Configuring the initial backup path”, on page 618.
   - **Continuous data protection** – Enables continuous data protection (CDP) for the backup. To configure the CDP settings, click **[>>]**, and then do the following:

     a) In the **File Change Detection** box, **Windows Built-in File Monitoring** is automatically selected and cannot be changed.

     b) To specify the minimum interval the DS-Client must wait before backing up a changed item or file, select **Do not back up more often than**, and then enter the interval and unit of measurement. You can set a longer interval if you do not want to back up changes frequently or a shorter interval if you want the backup of changes to be more granular.

     c) To specify the minimum interval the DS-Client must wait before backing up a changed item or file after detecting that it has not changed, select **Backup if file stops changing for**, and then enter the interval and unit of measurement. This option is intended for data that you know changes frequently.

     d) Under **Suspend Backup for Scheduled**, select the scheduled activities that will suspend the CDP backup process. The options are **Retention**, **BLM**, and **Validation**.

     e) Click **OK**. For more information, see Section 5.2.2, “Continuous data protection (CDP)”, on page 108.

   - **Stop on errors** – Stops a backup process when the number of errors reaches the specified value. A value of 0 means the DS-Client does not stop a backup process regardless of the number of errors.

   NOTE: You can configure the default setting using the **MaxErrors** advanced configuration parameter. For more information, see Section 2.1.8.6, “Miscellaneous parameters (Windows)”, on page 42.

- **Compression type** – Specifies the type of compression that will be applied to the backup. The options are as follows:
  - **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good default compression when the network is not the bottleneck.
  - **ZLIB (Global, Low, Medium, and High)** – Normally produces better compression than LZOP, but will take more time to compress. This is a good default compression when the bottleneck is the network. ZLIB Low corresponds to a value of 3, ZLIB Medium = 6, and ZLIB High = 9.
  - **None** – Disables compression for the backup.

2. To specify a command to run before (Pre) and/or after (Post) the execution of the backup, click **Pre/Post**. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525 and Section 5.26, “Configuring Pre/Post processes (Linux)”, on page 528.
3. To apply a filter, click **Filter**, and then select an existing filter or click **Add** to create a new filter.
4. Click **Next**.

5.6.5.7 Specifying notification options

1. To configure a notification, do one of the following:
   - To add a notification, click **Add.**
   - To modify a notification, select the notification, and then click **Modify.**

   NOTE: To delete a notification, select the notification, and then click **Delete**.

2. To send an email notification, select **E-Mail**. and then do the following:
   a) To send the email notification to the DS-Client administrator, select **Administrator**.
   b) To send an email to another recipient, select **Other**, and then specify the recipients email address.
   c) To send detailed backup information, select the **Detailed notification** check box.
   d) To include a detailed file-level backup log as an attachment, select the **Attach detail log** check box.

e) To send the email notification in HTML format, select the **Send E-Mail using HTML format** check box.

NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

f) Click **OK**.

3. To send a pager notification, select **Pager**. The notification will be sent to the pager account configured for the DS-Client.

NOTE: The pager option is available only if the DS-Client has been configured for pager notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

g) To send a broadcast notification, select **Broadcast**. Select the server containing the messenger service to which you want to send the message and click **OK**.

NOTE: Broadcast notifications to domains or workgroups are limited to 128 characters.

4. To send an event notification, select **Event**. Select the server on which you want the notification to be recorded in the Event Log and click **OK**.
5. In the **Completion** box, specify under what conditions a notification will be sent, and click **OK**. The options are as follows:
   - **All** – Notification will be sent under all conditions.
   - **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
   - **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.
   - **Completed with errors** – Notification will be sent if an activity is completed with at least one error event.
   - **Incomplete** – Notification will be sent if an activity is not completed successfully.
6. Under **Send SNMP Traps when**, configure the DS-Client to send SNMP traps when the backup has completed successfully, completed with warnings, completed with errors, or is incomplete.
7. Click **Next**.

5.6.5.8 Assigning a retention rule

1. To assign a retention rule to the backup, do one of the following:
   - If you don't want to assign a retention rule, select **No retention rule**.
   - To assign a retention rule, select **Use a specific retention rule**, and then select the retention rule.

NOTE: To create or edit a retention rule, click **[...]**. For more information, see Section 4.1, "Configuring a retention rule", on page 98.

---

2. Click **Next**.

5.6.5.9 Assigning a schedule

1. To assign a schedule to the backup, do one of the following:
   - If you don't want to assign a schedule to the backup, select **Not scheduled**.
   - To assign a schedule to the backup, select **Scheduled.** In the **Available schedules** box, select an existing schedule.

NOTE: To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, "Configuring a schedule", on page 90.

---

2. Click **Next**.

5.6.5.10 Naming the backup

1. In the **Set name** box, type a name for the backup.
2. In the **Set type** box, select the type of backup you want to create. The list of available backup types depends on the configuration of your DS-Client.
   - Online
   - Statistical

NOTE: For more information, see Section 5.1, "Backup types", on page 106.

---

3. If you selected **Online**, do the following:

a) To send a copy of the oldest generation of the file that is about to be overwritten from the DS-System to the BLM Archiver, select the **BLM (Infinite Generations)** check box.

NOTE: The Backup Lifecycle Management tool must be enabled for the DS-Client.

---

b) To save a copy of the backup data to a local storage location on the DS-Client computer, select the **Save on Local Storage** check box.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Self-contained and Local Only backups.

---

c) To use the local storage as a cache if the DS-Client loses connection with the DS-System, select the **Transmission cache on Local Storage** check box. The cached backup data will be sent to the DS-System on the next connection after synchronization.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path.

---

d) To save a copy of the backup data to the instant recovery vault, select the **Save in instant recovery vault** check box.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Instant Recovery backups.

---

e) Beside the **Local Storage Path** box, click **>>**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

4. If you selected **Statistical**, and want to emulate an actual backup transfer process, select the **Calculate transmit amount** check box. During the backup, specified backup files will be read from their source and processed for compression and encryption.
5. If the multitenant feature is enabled and configured, in the **Customer** list, you can select the customer to which you want to assign the backup. For more information, see Section 11.5, “Multitenant DS-Clients”, on page 634.

6. Click **Finish**.

5.6.6 Restoring a Microsoft Outlook (DS-MLR) backup

You can restore email data that has been backed up at the individual message level from Microsoft Outlook using DS-MLR.

IMPORTANT: Before restoring email data to an alternate location, ensure the DS-MLR service is installed and running on the destination email server.

If you encounter a restore issue when using DS-MLR, it is likely related to the DS-MLR service account configuration. For details on the requirements for the DS-MLR service account, see the *Client Software Installation Guide*.

5.6.6.1 Selecting the restore items

1. Browse the backups tree and select the backup you want to restore.
2. On the **Restore** menu, click **Restore Now**.
3. To restore an entire backup or folder, browse the tree and select the check box beside the backup or folder you want to restore.
4. To restore individual files, select the folder containing the required files, click **Show Files**, and then do the following:
   - To view details about the backed up file, select the file, and then click **File Info**.
   - To view the details of the items you selected, click **Selection**.
   - To view archived files, click **Show Archived**.
   - To view modified files, click **Show Modified**.
   - To include the modified files for restore, click **Add Modified**.
5. To view the number of files selected and calculate the total amount of files selected, select the **Calculate amount** check box.
6. To exclude subdirectories, clear the **Include SubDirs** check box, as the default setting is to include sub-directories.
7. To filter for specific emails, click **Filter**.
8. In the **Modify Filter** dialog box, do the following:
   a) In the **Filter Name** box, type a name for the filter.
   b) In the **Field** box, select the field to search. The available selections depend on the email server type, and if this filter is for backup or restore.

c) In the **Criteria** box, select the criteria you want to apply to the search field.

- To make the criteria ineffective, select the **Not** check box.

d) In the **Value** box, type a value or select a value from the available options which depends on the selection you made for the **Field**.

e) Beside **Logical**, select the boolean operator that you want to apply for each filter condition.

f) Use the left and right brackets to define complex filters.

g) Click **Add** to save the filter condition.

h) Click **OK**. The **Description** box displays the details of the filter.

9. To refine your selection of items to restore, click **Advanced**. Under **Show**, select which generation you want to display. The options are as follows:

- To restore the latest generation of all the files, select **Latest generation of all data**.
- To restore files that were deleted from the source, but not removed from the online storage as of the last backup session, select **Latest generation of all data (except deleted data)**.
- To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:

a) Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.

b) Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.

c) Click **OK**.

10. Under **Filter**, select the type of filter you want to apply to the backups. The options are as follows:

- **Show all data** – No filter is applied.
- **Hide data (dirs/files) deleted from source on/before** – You can hide backed up data (directories and files) that was intentionally deleted from the source computer.
- **Show only data (dirs/files) deleted from source on/before** – You can view and restore backed up data (directories and files) that was intentionally deleted from the source computer.

NOTE: These options are available only if the DS-Client database can be used to filter the backups. It does not appear for BLM Image Restore or Disc/Tape Restore, since they have been written to media and are no longer synchronized with the DS-Client database.

---

11. Under **File overwrite**, select how files are restored. The options are as follows:
    - **Restore all** – All selected files are restored to the destination directory.Files with the same name are overwritten.
    - **Restore newer** – Only files newer than those in the destination folder are restored.
    - **Restore older** – Only files with older than those in the destination folder are restored.
    - **Restore different** – Only files with different dates/sizes than those in the destination folder are restored.
    - **Skip existing** – Existing files with the same name in the destination folder are not restored.
12. Click **OK** and then click **Next**.

5.6.6.2 Selecting the restore location

1. Select the location to which you want to restore the backup. The options are as follows:
    - **Original location** – Data is restored to the original backup source location and existing files with the same name are overwritten. This is the default option.
    - **Alternate location** – Data is restored to a location other than the original backup source.

    NOTE: When restoring to an alternate location, the security of restored items in the destination location might not resemble the security of those items during backup.

2. If you selected **Alternate location**, then do the following:
    a) Beside the **Alternate location** box, click **[>>]**.
    b) In the **Select Alternate Server** dialog box, select the computer to which you want to restore, and then map the Source Mailbox to the Destination Mailbox.
    c) To specify alternate network credentials, select the **Ask for Network Credentials** checkbox, and then click **Select**.
    d) In the **Enter Network Credentials** dialog box, enter the credentials to connect to the destination computer, and then click **OK**.
    e) In the **Destination** cell, select a share location.
    f) Click in the **Restore to** cell and type the name of the folder you want to restore to or click **[>>]** and select a folder.

3. In the **Truncate** box, you can increase the truncate level to shorten the common portion of the restore path, if the selected restore items contain a common path.
4. Click **Next**.

5.6.6.3 Selecting the performance options

IMPORTANT: These options are intended for large backups in high performance environments where the DS-Client can take advantage of the speed of the storage where the source data resides. Test different settings to determine the optimal value. Slower storage can result in performance issues if these values are not configured correctly.

1. To specify the number of files the DS-System can read simultaneously for the restore process, select one of the following options:
2. Under **DS-System side read threads**, configure the number of files the DS-System can read simultaneously for the restore process.
   - To use the default MaxRestoreReadThreads advanced configuration parameter setting, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting and configure a custom value that only applies for this backup, click **Use specific value** and then enter the value.
3. Click **Next**.

5.6.6.4 Selecting the restore options

1. Under **Method**, select a method for the DS-Client to perform the restore. The options are as follows:
   - **Use buffer** – Restores files to the DS-Client buffer first and then transfers the files to the restore destination. This method minimizes the duration for which the restore process occupies the destination server.
   - **Fast** – Uses a direct restore method by writing data as it is received.

     NOTE: If you select the Fast method, files in the destination location are overwritten upon receipt of the first byte of data.
2. To record all restored files in the Activity Log, select the **Detailed log** check box.

3. To skip the pre and post restore processes, select the **Skip Pre/Post** check box. If this check box is cleared, the DS-Client runs a specified activity before and/or after a restore operation. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525.

5.6.6.5 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, under **Restore classification**, select the type of restore. The options are as follows:
   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.
3. Click **Finish**.

5.7 Google Workspace backups (Windows)

You can back up and restore the following data from Google Workspace:

- Calendars
- Contacts
- Documents
- Email
- Sites

For best results, we recommend using the Windows DS-NOC to create Google Workspace backups. After the backups have been created, you can use DS-User to initiate on-demand backups or restore the data as required.

IMPORTANT: Do not use the DS-User to modify the properties of a Google Workspace backup that was created in the DS-NOC. Changing the backup name or schedule in DS-User can adversely affect the operation of the system.

5.7.1 Google Workspace requirements

Before backing up Google Workspace data, consider the following:

- The DS-User must be able to connect to the Google Workspace domain.
- The DS-Client computer must have an Internet connection and be able to connect to the Google Workspace domain.
- You must have an existing Google Workspace domain on which there are active Workspace user accounts that need to be backed up.
- You must have a Google administrative account that has the permission to access all user accounts to be backed up from the domain.
- If you are using the DS-NOC, ensure that the web server hosting the DS-NOC is able to connect to the Google Workspace domain where the data that needs to be backed up resides.
- If the DS-NOC service, DS-Client service, or DS-User application is behind a proxy server, ensure the respective proxy server settings are configured.

Before performing a Google Workspace backup, do the following.

1. Sign in to Gmail using the super admin user account.
2. On the **Settings** menu, click **Manage** this domain.
3. Enable API access as follows:
    a) Sign in to the Google Admin console for your Workspace domain.
    b) On the **Security** menu, click **Access and data control**.
    c) Click **API Controls**.
    d) Ensure the **Trust internal apps** check box is selected.
4. Create a project and enable the required Workspace APIs for the project.
    a) Sign in to the Google Cloud Platform console for your Google Workspace domain.
    b) Create a project.
    c) Select the project.
    d) On the **APIs and Services** menu, click **Enable APIs and Services**.
    e) Search for and enable the following Google APIs:
        - Admin SDK API
        - CalDAV API
        - Contacts API
        - Gmail API

- Google Calendar API
- Google Drive API
- Google People API

5. Create credentials for the service account as follows:
   a) Sign in to the Google Cloud Platform console for your Google Workspace domain.
   b) On the **IAM & admin** menu, click **Service accounts**.
   c) On the **Service accounts** page, click **Create Service Account**.
   d) Under the **Project** category, add the **Owner** and **Editor** roles.
   e) Create a service account. Ensure the project role is set to **Owner** and the **Enable Google Workspace Domain-wide Delegation** option is enabled. An OAuth 2.0 client ID is automatically generated for the service account.

NOTE: You must generate the credentials that are required based on the logon mode that will be used during backup configuration and backup and restore activities. The credentials will be used to access the backup source and restore destination. The Service account logon mode allows access to one or multiple user accounts on your Google Workspace domain. This mode is available in DS-User and is the only logon mode in DS-NOC. The Client ID for native application logon mode allows access to one Google Workspace user account only, which is available only in DS-User.

---

6. Create encryption keys for the service account as follows:
   a) Sign in to the Google Cloud Platform console for your Google Workspace domain.
   b) On the **IAM & admin** menu, click **Service accounts**.
   c) On the **Service accounts** page, select the service account you created, and then click **Create key** on the **Actions** menu.
   d) Create a private key in JSON format for the service account, download the key, and store it in a secure location.
   e) Create a private key in P12 format for the service account, download the key, and store it in a secure location.

NOTE: The encryption keys are used for the credentials when logging on to the DS-Client and DS-NOC.

---

7. Locate and record the Client ID as follows:

a) Sign in to the Google Cloud Platform console for your Google Workspace domain.

b) On the **APIs and Services** menu, click **Credentials**.

c) On the **Credentials** page, locate the project you created and copy the Client ID.

8. Configure the OAuth 2.0 client ID of the service account to use the required API scopes as follows:

   a) Sign in to the Google Admin console for your Google Workspace domain.

   b) On the **Security** menu, click **API Controls**.

   c) Click **Manage API client access**, and then click **New**.

   d) In the **Client Name** box, paste the Client ID.

   e) In the **One or More API Scopes** box, add the following API scopes separated by a comma, and then click **Authorize**.

      - https://mail.google.com/,
      - https://sites.google.com/feeds/,
      - https://www.google.com/calendar/feeds/,
      - https://www.google.com/m8/feeds/,
      - https://www.googleapis.com/auth/admin.directory.user,
      - https://www.googleapis.com/auth/calendar,
      - https://www.googleapis.com/auth/drive,
      - https://www.googleapis.com/auth/contacts,
      - https://www.googleapis.com/auth/contacts.other.readonly,
      - https://www.googleapis.com/auth/directory.readonly

9. Create Client mode Credentials as follows:

   a) Select the project.

   b) On the **APIs and Services** menu, click **Oauth Consent Screen**.

   c) Select **User Type: External**, and then click **Create**.

   d) Enter the app information, and then click **Save and Continue**.

   e) Click **Add and Remove Scopes** and update the scope as follows:

      - Admin SDK API
      - CalDAV API
      - Contacts API

- Gmail API
- Google Calendar API
- Google Drive API
- Google People API

f) Click **Save and Continue**, and then click **Add Test User.**

g) Click **Save and Continue**.

10. Review the Summary Page, and then click **Back to Dashboard**.
11. On the **APIs and Services** menu, click **Credentials**.
    a) Create the credentials, and then click **Oauth Client**.
    b) Select **Application Type : Desktop Client**, and then click **Create**.
12. Download the OAuth Client Json file.

5.7.2 Creating a Google Workspace backup

You can create a Google Workspace backup.

5.7.2.1 Selecting the type of backup

You must select the type of backup you want to create.

1. On the **Sets** menu, click **New Backup Set**.
2. Select **Backup from the cloud**, and then click **Next**.

5.7.2.2 Selecting the cloud service type

You must select the type of cloud service you want to back up.

1. Select **Google Workspace**.
2. Click **Next**.

5.7.2.3 Selecting a logon mode

Select the type of logon method you want to use to access the backup source.

1. Select a logon method. The options are as follows:
   - **Client ID for native application** – The DS-Client uses the client ID to access the Google account for which it was generated. The DS-Client can access only one Google account at a time.
   - **Service account logon** – The DS-Client uses the service account credentials to access one or multiple accounts in the Google Workspace domain.
2. If you selected **Service account logon**, do the following:
   a) In the **www.** box, type the name of the Google Workspace cloud domain for which you want to back up data, and then click **Next**.
   b) In the **Google account** box, type the user name of the Google administrative account that you have used to create the service account which you will use for API access.
   c) Beside **Email address**, click **[...]**, and then select the JSON file that contains the client email address of the same service account. You can also type the service account client email address.
   d) Beside **Private key**, click **[...]**, and then select the PKCS12-format (or P12) private key generated for the same service account. This private key is a binary file with a .p12 extension.
   e) Click **OK**.
3. If you selected **Client ID for native application**, click **Next**, and then do the following:
   a) Beside **Client ID**, click **[...]**, and then select the JSON file that contains the OAuth 2.0 client ID and the client secret for the Workspace account for which you want to back up data. The name of the file begins with `client_secret`. You can also type the client ID.
   b) If you selected a JSON file for the **Client ID**, the **Client secret** box is automatically filled. If you have typed the client ID, then type the client secret that corresponds with the client ID.
   c) Click **OK**. On successful sign-in, a permission request is displayed in the **Request for Permission** dialog box.

NOTE: The Google account must be the same account for which you generated the credentials and have permission to access the data.

---

d) Grant the application the permission to access data on the Google account. An access permission and a verification code are displayed on the Google account page shown in the **Request for Permission** dialog box.

e) Copy and paste the entire string of the verification code into the **Code** box, and then click **OK**.

4. Click **Next**.

5.7.2.4 Selecting the backup items

1. To add an item, select the item, and then click **Add**.

NOTE: You can add only one item at a time. Subdirectories are included by default. To exclude subdirectories, clear the Include SubDirs check box.

---

2. To exclude an item when its parent folder is selected for backup, select the item, and then click **Exclude.**
3. To exclude an item using regular expressions, select the item, and then click **RegEx**.

NOTE: Regular expressions provide more specific filtering than the exclude function. For example, you can use regular expressions to exclude individual file names or patterns. Use this option only if you are familiar with the syntax.

---

4. To add individual items inside a folder, do the following:
   a) Select the folder, and then click **Items**.
   b) Select the items or entries that you want to back up, and then click **Add**.
      - To prevent an item from being backed up, select the individual item, and then click **Exclude**.
   c) Click **Finish**.
5. To modify an existing regular expression, select the regular expression, and then click **Modify**.
6. To remove an item from the list of selected items for backup, select the item, and then click **Remove**.
7. Click **Next**.

5.7.2.5 Selecting the backup item options

1. To configure the maximum generations for a backup item that will be stored online, double click the **Max Gen** cell, and then enter the value.
2. Click **Next**.

5.7.2.6 Selecting the backup options

1. Configure the options for the backup. The options are as follows:
   - **Detailed log** – Records all files that are backed up in the Activity Log. For more information, see Section 8.1, “Viewing the Activity Log”, on page 578.
   - **Initial backup** – Uses the Initial Backup feature for the first backup. To configure the initial backup path, click **[>>]**. For more information, see Section 11.1.1, “Configuring the initial backup path”, on page 618.
   - **Stop on errors** – Stops a backup process when the number of errors reaches the specified value. A value of 0 means the DS-Client does not stop a backup process regardless of the number of errors.

     NOTE: You can configure the default setting using the **MaxErrors** advanced configuration parameter. For more information, see Section 2.1.8.6, “Miscellaneous parameters (Windows)”, on page 42.

   - **Compression type** – Specifies the type of compression that will be applied to the backup. The options are as follows:
     - **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good default compression when the network is not the bottleneck.
     - **ZLIB (Global, Low, Medium, and High)** – Normally produces better compression than LZOP, but will take more time to compress. This is a good default compression when the bottleneck is the network. ZLIB Low corresponds to a value of 3, ZLIB Medium = 6, and ZLIB High = 9.
     - **None** – Disables compression for the backup.
2. Click **Next**.

5.7.2.7 Specifying notification options

1. To configure a notification, do one of the following:
   - To add a notification, click **Add.**
   - To modify a notification, select the notification, and then click **Modify.**

   NOTE: To delete a notification, select the notification, and then click **Delete**.

2. To send an email notification, select **E-Mail**, and then do the following:
   a) To send the email notification to the DS-Client administrator, select **Administrator**.
   b) To send an email to another recipient, select **Other**, and then specify the recipients email address.
   c) To send detailed backup information, select the **Detailed notification** check box.
   d) To include a detailed file-level backup log as an attachment, select the **Attach detail log** check box.

   NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

   e) To send the email notification in HTML format, select the **Send E-Mail using HTML format** check box.
   f) Click **OK**.
3. To send a pager notification, select **Pager**. The notification will be sent to the pager account configured for the DS-Client.

   NOTE: The pager option is available only if the DS-Client has been configured for pager notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

4. To send a broadcast notification, select **Broadcast**. Select the server containing the messenger service to which you want to send the message and click **OK**.

   NOTE: Broadcast notifications to domains or workgroups are limited to 128 characters.

5. To send an event notification, select **Event**. Select the server on which you want the notification to be recorded in the Event Log and click **OK**.
6. In the **Completion** box, specify under what conditions a notification will be sent, and click **OK**. The options are as follows:
   - **All** – Notification will be sent under all conditions.
   - **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
   - **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.
   - **Completed with errors** – Notification will be sent if an activity is completed with at least one error event.
   - **Incomplete** – Notification will be sent if an activity is not completed successfully.
7. Click **Next**.

5.7.2.8 Assigning a retention rule

1. To assign a retention rule to the backup, do one of the following:
   - If you don't want to assign a retention rule, select **No retention rule**.
   - To assign a retention rule, select **Use a specific retention rule**, and then select the retention rule.

NOTE: To create or edit a retention rule, click **[...]**. For more information, see Section 4.1, "Configuring a retention rule", on page 98.

---

2. Click **Next**.

5.7.2.9 Assigning a schedule

1. To assign a schedule to the backup, do one of the following:
   - If you don't want to assign a schedule to the backup, select **Not scheduled**.
   - To assign a schedule to the backup, select **Scheduled.** In the **Available schedules** box, select an existing schedule.

NOTE: To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, "Configuring a schedule", on page 90.

---

2. Click **Next**.

5.7.2.10 Naming the backup

1. In the **Set name** box, type a name for the backup.
2. In the **Set type** box, select the type of backup you want to create. The list of available backup types depends on the configuration of your DS-Client.
   - Online
   - Self-contained
   - Local-only
   - Statistical

NOTE: For more information, see Section 5.1, “Backup types”, on page 106.

---

3. If you selected **Online**, do the following:
   a) To send a copy of the oldest generation of the file that is about to be overwritten from the DS-System to the BLM Archiver, select the **BLM (Infinite Generations)** check box.

   NOTE: The Backup Lifecycle Management tool must be enabled for the DS-Client.

   ---

   b) To save a copy of the backup data to a local storage location on the DS-Client computer, select the **Save on Local Storage** check box.

   NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Self-contained and Local Only backups.

   ---

   c) To use the local storage as a cache if the DS-Client loses connection with the DS-System, select the **Transmission cache on Local Storage** check box. The cached backup data will be sent to the DS-System on the next connection after synchronization.

   NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path.

   ---

d) Beside the **Local Storage Path** box, click **>>**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

4. If you selected **Self-Contained**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

5. If you selected **Local-Only**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

6. If you selected **Statistical**, and want to emulate an actual backup transfer process, select the **Calculate transmit amount** check box. During the backup, specified backup files will be read from their source and processed for compression and encryption.
7. If the multitenant feature is enabled and configured, in the **Customer** list, you can select the customer to which you want to assign the backup. For more information, see Section 11.5, “Multitenant DS-Clients”, on page 634.
8. Click **Finish**.

5.7.3 Restoring a Google Workspace backup

You can restore a Google Workspace backup.

NOTE: Before selecting an alternate location, if the user account that was backed up does not exist in the restore destination, DS-Client will attempt to create the user account in that location before restoring data (this might incur additional costs).

5.7.3.1 Selecting the restore items

1. Browse the backups tree and select the backup you want to restore.
2. On the **Restore** menu, click **Restore Now**.
3. To restore an entire backup or folder, browse the tree and select the check box beside the backup or folder you want to restore.
4. To restore individual files, select the folder containing the required files, click **Show Files**, and then do the following:
   - To view details about the backed up file, select the file, and then click **File Info**.
   - To view archived files, click **Show Archived**.
5. To view the number of files selected and calculate the total amount of files selected, select the **Calculate amount** check box.
6. To exclude subdirectories, clear the **Include SubDirs** check box, as the default setting is to include sub-directories.
7. To filter the list of files, in the **Filter box**, enter a filter using * as a wildcard, and then click **Show Files** to update the list of files.
8. To search for a specific backed up file, click **Find File**. In the **Find Backed Up File** dialog box, do the following:
   a) Under **Search for**, select the search criteria to search for a backed up file either by **File name** or by **File ID**.
   b) Click **Find**.
   c) Select the required backed up file, and then click **Select**.
9. To view the details of the items you selected, click **Selection**.
10. To refine your selection of items to restore, click **Advanced**. Under **Show**, select which generation you want to display. The options are as follows:
    - To restore the latest generation of all the files, select **Latest generation of all data**.
    - To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:
      a) Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.
      b) Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.
      c) Click **OK**.
11. Click **Next**.

5.7.3.2 Selecting the restore location

1. Select the location to which you want to restore the backup. The options are as follows:

   - **Original location** – Data is restored to the original backup source location and existing files with the same name are overwritten. This is the default option.
   - **Alternate location** – Data is restored to a location other than the original backup source.

   NOTE: When restoring to an alternate location, the security of restored items in the destination location might not resemble the security of those items during backup.

2. If you selected **Alternate location**, then beside the **Alternate location** box, click **[>>]**.

   a) In the **Select Alternate Server** dialog box, select a logon method. The options are as follows:

      - **Client ID for native application** – DS-Client will use this client ID to access the Google account for which the client ID was generated. DS-Client can access only one Google account.
      - **Service account logon** – DS-Client will use the service account credentials to access one or multiple accounts on your Google Workspace domain. In the **www.** box, type the name of the Google Workspace cloud domain for which you want to back up data.

   b) Click **Select**.

3. If you selected **Client ID for native application**, then in the **Enter API Access Credentials** dialog box, do the following:

   NOTE: When you select an alternate location as the restore destination, DS-Client will verify if the user account that was backed up exists in that location. If the user account exists, DS-Client will restore data to that destination. If the user account does not exist, DS-Client will first attempt to create the user account and then restore data to that destination (this might incur additional costs). The user account will also have a randomly generated password that the Administrator must reset so that the user can log on.

a) Beside **Client ID**, click **[...]**, and then select the JSON file that contains the OAuth 2.0 client ID and the client secret for the Workspace account for which you want to back up data. The name of the file begins with `client_secret`. You can also type the client ID.

b) If you have selected a JSON file for the **Client ID**, the **Client secret** box is automatically filled. If you have typed the client ID, then type the client secret that corresponds with the client ID.

c) Click **OK**.

d) In the **Request for Permission** dialog box, on the Google account page, sign in to the Google account for which you want to back up data. The application needs permission to access this data.

NOTE: This Google account must be the same account with which you generated the credentials that you have provided in the **Enter API Access Credentials** dialog box.

On successful sign-in, a permission request is displayed in the **Request for Permission** dialog box.

NOTE: The service account must have the required privilege to access the restore destination.

---

e) Grant the application the permission to access data on the Google account. An access permission and a verification code are displayed on the Google account page shown in the **Request for Permission** dialog box.

f) In the **Request for Permission** dialog box, copy and paste the entire string of the verification code into the **Code** box.

g) Click **OK**.

4. If you have selected **Service account logon**, then in the **Enter API Access Credentials** dialog box, do the following:

a) In the **Google account** box, type the user name of the Google administrative account that you have used to create the service account which you will use for API access.

b) Beside **Email address**, click **[...]**, and then select the JSON file that contains the client email address of the same service account. You can also type the service account client email address.

c) Beside **Private key**, click **[...]**, and then select the PKCS12-format (or P12) private key generated for the same service account. This private key is a binary file with a .p12 extension.

d) Click **OK**.

5. To restore data to a location on the DS-Client computer, select the **Restore to local disk** check box, and then click **[>>]** to specify the location. UNC paths are not supported.
6. If you are restoring an email backup, in the **Custom Mail Label(s)** box, type the name of the folder that will be created on the Workspace site. The selected emails are restored to this folder.
7. Click **Next**.

5.7.3.3 Selecting the restore options

The applicable options are selected by default. Click **Next**.

5.7.3.4 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, under **Restore classification**, select the type of restore. The options are as follows:
   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.
3. Click **Finish**.

5.8 IBM DB2 database backups (Linux)

You can back up and restore data from an IBM DB2 database.

5.8.1 General requirements

- You must have knowledge of the IBM DB2 database file structure and instance management.
- You must record the remote node and database name before creating or restoring a IBM DB2 database backup. You cannot browse the databases for names, therefore you must know the exact name beforehand.
- The account used to connect to the IBM DB2 client instance must exist on the DS-Client computer.
- The credentials used for the backup and restore of the IBM DB2 database must have the SYSADM, SYSCTRL, or SYSMAINT authority.

5.8.2 DS-Client computer requirements

- You must install the IBM DB2 client on the same computer as the DS-Client.
- The IBM DB2 client must be the same version as the IBM DB2 servers being backed up.
- You must configure the IBM DB2 client library directory on the DS-Client using the DB2 Client Library Directory advanced configuration parameter. For more information, see Section 2.1.8, “Configuring the advanced settings”, on page 37).

5.8.3 IBM DB2 requirements

- The IBM DB2 server should be a certified product.
- Edit the IBM DB2 instance configuration file and ensure the TCP/IP service name is properly configured and the SVCENAME parameter is set to the appropriate service name and corresponds to the correct port number.

5.8.4 Backup requirements

- The IBM DB2 database must not be in use when you perform an offline backup, otherwise an error will be reported.
- Ensure the DS-Client has read and write privileges to access the transaction log directory on the IBM DB2 database computer.
- Online backups are available only for databases configured with the logarchmeth1 value set to either logretain or userexit.
- The backup must specify if the backup is online or offline, as determined by the IBM DB2 database configuration settings.

IMPORTANT: If you need to change this setting in the IBM DB2 configuration, make a new backup with the new option setting.

- Do not change the online option setting for an on-demand backup. If it is changed, you must make a record of the change and the date so the information is available if a restore is performed.

5.8.5 Restore requirements

- The IBM DB2 database must not be in use when you perform the restore. This requirement applies to all IBM DB2 backups (online or offline).
- The IBM DB2 database must be configured for online or offline restore. This setting must match the setting that was used for the backup.

5.8.6 Creating an IBM DB2 database backup

This section describes how to create an IBM DB2 database backup.

5.8.6.1 Selecting the type of backup

1. On the **Sets** menu, click **New Backup Set**.
2. Select **DB2 Server**, and then click **Next**.

5.8.6.2 Selecting the backup source

1. Select the DB2 server.

   NOTE: The host name or IP address is displayed in the Path box and must be the same as the one used in the DB2 catalog command, but can be on a different subnet.

   By default, the **Ask for database credentials** check box is selected and you must supply the credentials to the DB2 database.

2. Click **Next**.
3. In the **Ask for database credentials** dialog box, do the following:
   a) In the **User Name** box, type a valid database user name on the IBM DB2 database server you want to back up.
   b) In the **Password** box, type the corresponding password.
   c) In the **Node Name** box, type the local alias of the target DB2 server node. This is the name on the DS-Client computer that is used to identify that node.
   d) In the **Port Number** box, type the TCP/IP port number of the DB2 Server Database Manager instance.
   e) In the **DB2 Client Instance** box, type the local IBM DB2 instance name installed on the DS-Client computer.
   f) Click **OK**.
4. Click **Next**.

5.8.6.3 Selecting the protocol for dumping the database

Select a protocol to make a copy or “dump” of the database, if you want to back up an active database.

To select the protocol for dumping the database:

1. In the **Select the protocol for dumping database file** dialog box, select the method to handle the database dump. The options are as follows:
   - **Local File System** – For DB2 Server on the DS-Client computer.
   - **NFS** – For remote DB2 Server.
   - **UNIX-SSH** – For remote DB2 Server.
2. To provide the credentials for the selected computer, select the **Ask for network credentials** check box.

a) In the **User Name** box, enter a valid user name.

b) In the **Password** box, type the corresponding password or passphrase applicable only for UNIX-SSH.

c) In the **Private Key File** box, click **[>>]**, and select the private key file. With this key, you can back up and restore using SSH public key authentication.

- If no private key is specified, and a default private key is found on the DS-Client machine, you must first try the public key authentication. If that fails, try password authentication.
- If no default key is found, try password authentication only.
- If a private key file is specified for the backup, the SSH connection will use the public key authentication only.

d) Click **OK**.

3. Click **Next**.

5.8.6.4 Selecting the path for the database dump file

1. Select the dump device path.

IMPORTANT: Ensure the DB2 Server username has “read and “write” privileges to this dump path.

2. Click **Next**.

5.8.6.5 Selecting the backup items

1. Select the required databases, and then click **Add**.
2. To exclude a database using regular expressions, select the database, and then click **RegEx**.
3. To remove a database from the list of selected databases for backup, select the database, and then click **Remove**.
4. Click **Next**.

5.8.6.6 Selecting the backup item options

1. To configure the maximum generations for a backup item that will be stored online, double click the **Max Gen** cell, and then enter the value.
2. Click **Next**.

5.8.6.7 Selecting the backup options

1. Under **Backup options**, configure the options you want to apply to the backup. The options are as follows:

   - **Use buffer** –Copies files to the DS-Client buffer to free up the backup source as fast as possible. The DS-Client then sends the files from the DS-Client buffer to the DS-System. For more information, see Section 5.2.7, “Performance”, on page 113.
   - **Detailed log** – Records all files that are backed up in the Activity Log. For more information, see Section 8.1, “Viewing the Activity Log”, on page 578.
   - **Initial backup** – Uses the Initial Backup feature for the first backup. To configure the initial backup path, click **[>>]**. For more information, see Section 11.1.1, “Configuring the initial backup path”, on page 618.
   - **Stop on errors** – Stops a backup process when the number of errors reaches the specified value. A value of 0 means the DS-Client does not stop a backup process regardless of the number of errors.

     NOTE: You can configure the default setting using the **MaxErrors** advanced configuration parameter. For more information, see Section 2.1.8.6, “Miscellaneous parameters (Windows)”, on page 42.

   - **Compression type** – Specifies the type of compression that will be applied to the backup. The options are as follows:
     - **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good default compression when the network is not the bottleneck.
     - **ZLIB (Global, Low, Medium, and High)** – Normally produces better compression than LZOP, but will take more time to compress. This is a good default compression when the bottleneck is the network. ZLIB Low corresponds to a value of 3, ZLIB Medium = 6, and ZLIB High = 9.
     - **None** – Disables compression for the backup.
2. Under **Additional Backup Options**, you can configure the following DB2 database options:
   - If you selected the **Prune History / Logfile** check box, this will delete entries from the history file or log files from the active log path.
   - To perform Online DB2 backup, select the **Online Backup** check box. An online backup allows applications to connect to the database and read and write to tables during database backup. Log retain or userexit must be enabled for an online backup.
   - To perform Offline DB2 backup, clear the **Online Backup** check box. During an offline backup, applications cannot connect to the database.

3. To specify a command to run before (Pre) and/or after (Post) the execution of the backup, click Pre/Post. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525 and Section 5.26, “Configuring Pre/Post processes (Linux)”, on page 528.
4. Click **Next**.

5.8.6.8 Selecting the DB2 ‘userexit’ log path

NOTE: This page appears only if you have selected the online backup option.

1. If **User Exit** is OFF on the DB2 database server, leave this field empty.
2. If **User Exit** is ON on the DB2 database server, type the path where the DB2 Archive files are written by the user exit program.
   a) To specify the path, beside the **Archive Log backup path box,** click **[>>]**.
   b) In the **Select Directory** dialog box, specify the path where the User Exit program writes the DB2 Archive Log files.
3. Click **Next**.

5.8.6.9 Specifying notification options

1. To configure a notification, do one of the following:
   - To add a notification, click **Add.**
   - To modify a notification, select the notification, and then click **Modify.**

   NOTE: To delete a notification, select the notification, and then click **Delete**.
2. To send an email notification, select **E-Mail**. and then do the following:
   a) To send the email notification to the DS-Client administrator, select **Administrator**.
   b) To send an email to another recipient, select **Other**, and then specify the recipients email address.
   c) To send detailed backup information, select the **Detailed notification** check box.
   d) To include a detailed file-level backup log as an attachment, select the **Attach detail log** check box.

e) To send the email notification in HTML format, select the **Send E-Mail using HTML format** check box.

NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

---

f) Click **OK**.

3. To send a pager notification, select **Pager**. The notification will be sent to the pager account configured for the DS-Client.

NOTE: The pager option is available only if the DS-Client has been configured for pager notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

---

4. To send a broadcast notification, select **Broadcast**. Select the server containing the messenger service to which you want to send the message and click **OK**.

NOTE: Broadcast notifications to domains or workgroups are limited to 128 characters.

---

5. To send an event notification, elect **Event**. Select the server on which you want the notification to be recorded in the Event Log.
6. In the **Completion** box, specify under what conditions a notification will be sent, and click **OK**.The options are as follows:

- **All** – Notification will be sent under all conditions.
- **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
- **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.
- **Completed with errors** – Notification will be sent if an activity is completed with at least one error event.
- **Incomplete** – Notification will be sent if an activity is not completed successfully.

5. Under **Send SNMP Traps when**, configure the DS-Client to send SNMP traps when the backup has completed successfully, completed with warnings, completed with errors, or is incomplete.
6. Click **Next**.

5.8.6.10 Assigning a retention rule

1. To assign a retention rule to the backup, do one of the following:
   - If you don't want to assign a retention rule, select **No retention rule**.
   - To assign a retention rule, select **Use a specific retention rule**, and then select the retention rule.

NOTE: To create or edit a retention rule, click **[...]**. For more information, see Section 4.1, "Configuring a retention rule", on page 98.

---

2. Click **Next**.

5.8.6.11 Assigning a schedule

1. To assign a schedule to the backup, do one of the following:
   - If you don't want to assign a schedule to the backup, select **Not scheduled**.
   - To assign a schedule to the backup, select **Scheduled.** In the **Available schedules** box, select an existing schedule.

NOTE: To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, "Configuring a schedule", on page 90.

---

2. Click **Next**.

5.8.6.12 Naming the backup

1. In the **Set name** box, type a name for the backup.
2. In the **Set type** box, select the type of backup you want to create. The list of available backup types depends on the configuration of your DS-Client.
   - Online
   - Self-contained
   - Local-only
   - Statistical

NOTE: For more information, see Section 5.1, "Backup types", on page 106.

---

3. If you selected **Online**, do the following:

a) To send a copy of the oldest generation of the file that is about to be overwritten from the DS-System to the BLM Archiver, select the **BLM (Infinite Generations)** check box.

NOTE: The Backup Lifecycle Management tool must be enabled for the DS-Client.

---

b) To save a copy of the backup data to a local storage location on the DS-Client computer, select the **Save on Local Storage** check box.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Self-contained and Local Only backups.

---

c) To use the local storage as a cache if the DS-Client loses connection with the DS-System, select the **Transmission cache on Local Storage** check box. The cached backup data will be sent to the DS-System on the next connection after synchronization.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path.

---

d) Beside the **Local Storage Path** box, click **>>**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

4. If you selected **Self-Contained**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

5. If you selected **Local-Only**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

6. If you selected **Statistical**, and want to emulate an actual backup transfer process, select the **Calculate transmit amount** check box. During the backup, specified backup files will be read from their source and processed for compression and encryption.
7. If the multitenant feature is enabled and configured, in the **Customer** list, you can select the customer to which you want to assign the backup. For more information, see Section 11.5, “Multitenant DS-Clients”, on page 634.
8. Click **Finish**.

5.8.7 Restoring an IBM DB2 database backup

You can restore an IBM DB2 database backup.

5.8.7.1 Selecting the restore items

1. Browse the backups tree, select the backup you want to restore.
2. On the **Restore** menu, click **Restore Now**.
3. To restore an entire backup or folder, browse the tree and select the check box beside the backup or folder you want to restore.
4. To restore individual files, select the folder containing the required files, click **Show Files**, and then do the following:
   - To view details about the backed up file, select the file, and then click **File Info**.
   - To view archived files, click **Show Archived**.
5. To view the number of files selected and calculate the total amount of files selected, under **Options**, select the **Calculate amount** check box.
6. To search for a specific backed up file, click **Find File**. In the **Find Backed Up File** dialog box, do the following:
   a) Under **Search for**, select the search criteria to search for a backed up file either by **File name** or by **File ID**.
   b) Click **Find**.

c) Select the required backed up file, and then click **Select**.

7. To refine your selection of items to restore, click **Advanced**. Under **Show**, select which generation you want to display. The options are as follows:

   a) To restore the latest generation of all the files, select **Latest generation of all data**.

   b) To restore files that were deleted from the source, but not removed from the online storage as of the last backup session, select **Latest generation of all data (except deleted data)**.

   c) To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:

      1. Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.

      2. Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.

      3. Click **OK**.

8. Click **Next**.

5.8.7.2 Selecting the restore location

1. Select the location to which you want to restore the backup. The options are as follows:

   - **Original location** – Data is restored to the original backup source location and existing files with the same name are overwritten. This is the default option.
   - **Alternate location** – Data is restored to a location other than the original backup source.

   NOTE: When restoring to an alternate location, the security of restored items in the destination location might not resemble the security of those items during backup.

2. If you selected **Alternate location**, do the following:

   a) Beside the **Alternate location** box, click **[>>]**.

   b) In the **Select Alternate location** dialog box, select the server to which you want to restore.The **Ask for database credentials** checkbox is selected by default.

   c) Click **Select**.

   d) In the **Ask for database credentials** dialog box, do the following:

1. In the **User Name** box, type a valid database user name on the DB2 database server that you want to back up.
2. In the **Password** box, type the corresponding password.
3. In the **Node Name** box, type the local alias of the target DB2 server node. This is the name on the DS-Client computer that is used to identify that node.
4. In the **Port Number** box, type the TCP/IP port number of the DB2 Server Database Manager instance.
5. In the **DB2 Client Instance** box, type name of the local DB2 instance installed on the DS-Client computer.
6. Click **OK**.

e) To change the location for the database dump, click **[>>]** beside the **Dump to** box.

1. In the **Select Directory** dialog box, select a path for the database dump.
2. Click **Select**.

f) In the **Destination** cell, select a share location.

3. To restore the dump file to the specified location, select the **Restore as Pure Files** check box.

NOTE: For more information, see Section 5.3.3, “Restoring data to an alternate location”, on page 130.

---

4. Click **Next**.

5.8.7.3 Selecting the restore options

1. To record all restored files in the Activity Log, select the **Detailed log** check box.
2. To skip the pre and post restore processes, select the **Skip Pre/Post** check box. If this check box is cleared, the DS-Client runs a specified activity before and/or after a restore operation. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525.

5.8.7.4 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, under **Restore classification**, select the type of restore. The options are as follows:
   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.
3. Click **Finish**.

5.9 MariaDB database backups (Windows, Linux, or Mac)

You can back up and restore a MariaDB database in a standalone or cluster configuration.

5.9.1 General requirements

You must install the MariaDB client software on the DS-Client computer and have knowledge of the MariaDB database file structure and instance management.

5.9.2 Backup requirements

The DS-Client **mariadb-dump** and **mariadb** utilities that are used to back up the MariaDB database must be compatible with the MariaDB version running on the source machine. The following requirements depend on the type of DS-Client:

- **Windows DS-Client** — Ensure the mariadb-dump and mariadb utilities are listed in the PATH environment variable of the DS-Client computer. To verify if the path is included, open the command prompt and type the following command:

  ```
  path
  ```

  NOTE: If you edit this variable, you must stop and restart the DS-Client service after making the change.

- **Linux DS-Client** — Ensure the mariadb-dump and mariadb utilities are listed in the PATH environment variable of the root user on the DS-Client computer. To verify, edit the following file and ensure that the folder is listed in the PATH:

  `/etc/init.d/dsclient`

- **Mac DS-Client** — Ensure the folder that contains the mariadb-dump and mariadb utilities is in the search PATH of the DS-Client by adding it to the following file on the DS-Client computer:

  `/etc/rc.common`

5.9.3 Restore requirements

To restore backed up stored routines, you must have the following privileges for the MariaDB database:

- Grant
- Create_Routines
- Alter_Routines

5.9.4 Creating a MariaDB database backup (Windows)

You can create a MariaDB database backup using a Windows DS-Client.

5.9.4.1 Selecting the type of backup

1. On the **Sets** menu, click **New Backup Set**.
2. Select **MariaDB Server**, and then click **Next**.

5.9.4.2 Selecting the MariaDB server

1. Browse and select the MariaDB server you want to back up. You can also type the IP address of the server in the **Path** box. To use non-standard port numbers, type the IP address and port number in the following format:

   `\\IP_address:Port_Number`

   NOTE: If you do not specify a port number, Windows DS-Client uses port 3306 by default.

2. By default, DS-Client uses the current user's logon credentials to connect to the selected computer. To provide credentials for the selected computer, select the **Ask for Network Credentials** check box. You will be prompted to enter a valid user name and password for the selected computer.
3. The **Ask for database credentials** check box is selected by default. Click **Next**.
4. In the **Enter database credentials** dialog box, do the following:
   a) In the **User name** and **Password** boxes, type the credentials required to connect to the selected database server.
   b) Click **OK**.
5. Click **Next**.

5.9.4.3 Selecting the database dump options

1. Select a path or method to handle the database dump. The options are as follows:
   - **DS-Client Buffer** – Save the dump file to the local storage on the DS-Client computer.
   - **DS-Client Pipe** – During backup, the DS-Client reads from the pipe on the source database. This method is useful if the database is too large to be dumped to a file on either the database server or the DS-Client buffer.
2. Click **Next**.

5.9.4.4 Selecting the database(s) to back up

1. Select the items you want to back up:
   - To add an instance, select the instance, and then click **Add**.
   - To remove an instance, select the instance from the **Backup Items Selected** list, and then click **Remove**.
2. Click **Next**.

5.9.4.5 Selecting the backup item options

1. To configure the maximum generations for a backup item that will be stored online, double click the **Max Gen** cell, and then enter the value.
2. Click **Next**.

5.9.4.6 Selecting the backup options

1. Configure the options for the backup. The options are as follows:

   - **Detailed log** – Records all files that are backed up in the Activity Log. For more information, see Section 8.1, “Viewing the Activity Log”, on page 578.
   - **Initial backup** – Uses the Initial Backup feature for the first backup. To configure the initial backup path, click **[>>]**. For more information, see Section 11.1.1, “Configuring the initial backup path”, on page 618.
   - **Stop on errors** – Stops a backup process when the number of errors reaches the specified value. A value of 0 means the DS-Client does not stop a backup process regardless of the number of errors.

     NOTE: You can configure the default setting using the **MaxErrors** advanced configuration parameter. For more information, see Section 2.1.8.6, “Miscellaneous parameters (Windows)”, on page 42.

   - **Compression type** – Specifies the type of compression that will be applied to the backup. The options are as follows:
     - **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good default compression when the network is not the bottleneck.
     - **ZLIB (Global, Low, Medium, and High)** – Normally produces better compression than LZOP, but will take more time to compress. This is a good default compression when the bottleneck is the network. ZLIB Low corresponds to a value of 3, ZLIB Medium = 6, and ZLIB High = 9.
     - **None** – Disables compression for the backup.
2. Configure additional options for the backup as follows:
   - To lock the tables before inserting data on restore, select the **Add locks around insert statements** check box. For more information, see *MySQL* documentation.
   - To add MySQL specific extensions to the backed up database dump, select the **Add MariaDB specific table create options** check box.
   - To specify how table rows are inserted into the database, beside **Insert statements type**, select an insertion type. For more information, see *MySQL* documentation. The options are as follows:
     - **Extended** – Table rows are inserted to the database dump very quickly. This method is not useful for manual loading into non MySQL databases.
     - **Normal** – Table rows are inserted using a standard method which is slower but is portable to other databases.

- **Complete** – Table rows are inserted using complete INSERT statements that include column names.

- To specify how tables are dumped, beside **Table dumping option**, select a table dump method. The options are as follows:
  - **Lock all tables** – Sets the tables to ready only mode and prevents changes to data during the backup process.
  - **Single transaction** – Prevents changes to the backup data, but does not set the tables to read-only mode during the backup process.This option works only with transactional tables.
  - **Do not lock tables** – You can change the table during the creation of the dump file.This could impact the consistency of the backup.
  - **None** – Database dump is performed using the mysqldump function with no special conditions.

3. To specify a command to run before (Pre) and/or after (Post) the execution of the backup, click **Pre/Post**. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525 and Section 5.26, “Configuring Pre/Post processes (Linux)”, on page 528.
4. Click **Next**.

5.9.4.7 Selecting the notification options

1. To configure a notification, do one of the following:
   - To add a notification, click **Add.**
   - To modify a notification, select the notification, and then click **Modify.**

   NOTE: To delete a notification, select the notification, and then click **Delete**.

2. To send an email notification, select **E-Mail**. and then do the following:
   a) To send the email notification to the DS-Client administrator, select **Administrator**.
   b) To send an email to another recipient, select **Other**, and then specify the recipients email address.
   c) To send detailed backup information, select the **Detailed notification** check box.
   d) To include a detailed file-level backup log as an attachment, select the **Attach detail log** check box.

e) To send the email notification in HTML format, select the **Send E-Mail using HTML format** check box.

NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

---

3. To send a pager notification, select **Pager**. The notification will be sent to the pager account configured for the DS-Client.

NOTE: The pager option is available only if the DS-Client has been configured for pager notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

---

4. To send a broadcast notification, select **Broadcast**. Select the server containing the messenger service to which you want to send the message and click **OK**.

NOTE: Broadcast notifications to domains or workgroups are limited to 128 characters.

---

5. To send an event notification, elect **Event**. Select the server on which you want the notification to be recorded in the Event Log.
6. In the **Completion** box, specify under what conditions a notification will be sent, and click **OK**. The options are as follows:
    - **All** – Notification will be sent under all conditions.
    - **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
    - **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.
    - **Completed with errors** – Notification will be sent if an activity is completed with at least one error event.
    - **Incomplete** – Notification will be sent if an activity is not completed successfully.
7. Click **Next**.

5.9.4.8 Assigning a retention rule

1. To assign a retention rule to the backup, do one of the following:
   - If you don't want to assign a retention rule, select **No retention rule**.
   - To assign a retention rule, select **Use a specific retention rule**, and then select the retention rule.

   NOTE: To create or edit a retention rule, click **[...]**. For more information, see Section 4.1, "Configuring a retention rule", on page 98.

2. Click **Next**.

5.9.4.9 Assigning a schedule

1. To assign a schedule to the backup, do one of the following:
   - If you don't want to assign a schedule, select **Not scheduled**.
   - To assign a schedule, select **Scheduled.** In the **Available schedules** box, select an existing schedule.

   NOTE: To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, "Configuring a schedule", on page 90.

2. Click **Next**.

5.9.4.10 Naming the backup

1. In the **Set name** box, type a name for the backup.
2. In the **Set type** box, select the type of backup you want to create. The list of available backup types depends on the configuration of your DS-Client.
   - Online
   - Self-contained
   - Local-only
   - Statistical

   NOTE: For more information, see Section 5.1, "Backup types", on page 106.

3. If you selected **Online**, do the following:

a) To send a copy of the oldest generation of the file that is about to be overwritten from the DS-System to the BLM Archiver, select the **BLM (Infinite Generations)** check box.

NOTE: The Backup Lifecycle Management tool must be enabled for the DS-Client.

---

b) To save a copy of the backup data to a local storage location on the DS-Client computer, select the **Save on Local Storage** check box.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Self-contained and Local Only backups.

---

c) To use the local storage as a cache if the DS-Client loses connection with the DS-System, select the **Transmission cache on Local Storage** check box. The cached backup data will be sent to the DS-System on the next connection after synchronization.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path.

---

d) To save a copy of the backup data to the instant recovery vault, select the **Save in instant recovery vault** check box.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Instant Recovery backups.

---

e) If you selected **Save in instant recovery vault**, beside the **Local Storage Path** box, click **>>**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

4. If you selected **Self-Contained**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

5. If you selected **Local-Only**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

6. If you selected **Statistical**, and want to emulate an actual backup transfer process, select the **Calculate transmit amount** check box. During the backup, specified backup files will be read from their source and processed for compression and encryption.
7. Click **Finish**.

5.9.5 Creating a MariaDB database backup (Linux or Mac)

You can create a MariaDB database backup using a Linux or Mac DS-Client. You can use the MariaDB Configuration Utility (**mariadb_config_editor**) to define all the logon paths that you need. For each logon path, you must define the following:

- Name of the logon path
- Host name
- User name
- Password

The logon path information is stored in the encrypted .mylogin.cnf file. Copy the .mylogin.cnf file to the DS-Client installation folder. The default location is:

```
/opt/CloudBackup/DS-Client
```

After you have defined the logon path, ensure the .mylogin.cnf file is in the DS-Client installation folder and contains the logon paths that are required by your MariaDB database backups.

IMPORTANT: Updates to the **.mylogin.cnf** file are not accessible to DS-Client unless the updated file is in the DS-Client installation folder.

5.9.5.1 Selecting the type of backup

1. On the **Sets** menu, click **New Backup Set**.
2. Select **MariaDb Server**, and then click **Next**.

5.9.5.2 Selecting the backup source

1. Browse and select the MariaDB server you want to backup. You can also type the IP address of the server in the **Path** box.
2. The **Ask for database credentials** check box is selected by default.
3. To specify the database dump application to use for the MariaDB database backup, select the **Database Dump Configuration** check box.
4. Click **Next**.
5. In the **Ask for database credentials** dialog box, do the following:
   a) In th **User name** and **Password** boxes, type the credentials required to connect to the selected database server.

      To refer to a logon path, type the following text in the **User Name** box:

      `--login-path=<login path name>`

      where `<login path name>` is the name that is specified for the logon path.

   b) In the **Port** box, enter the port number DS-Client will use to communicate with the database. By default, Linux DS-Client uses port 3306.

   IMPORTANT: Do not change the port number unless you have a specific requirement to do so. For more information, refer to the *MariaDB* documentation.

   c) Click **OK**.
6. In the **Dump utility directory** box, type the installation path of a specific MariaDB database dump application that will be used for this backup. If you do not specify the path, DS-Client will select one automatically.

5.9.5.3 Selecting the database(s) to back up

1. Browse the database list and select the items to back up.
   - To add an instance, select the instance, and then click **Add**.
   - To view details about the backup item selected, click **Items**.
   - To remove an instance, select the instance from the **Backup Items Selected**, and then click **Remove**.
2. Click **Next**.

5.9.5.4 Selecting the backup item options

1. To configure the maximum generations for a backup item that will be stored online, double click the **Max Gen** cell, and then enter the value.
2. Click **Next**.

5.9.5.5 Selecting the backup options

1. Configure the options for the backup. The options are as follows:
   - **Use buffer** – Copies files to the DS-Client buffer to free up the backup source as fast as possible. The DS-Client then sends the files from the DS-Client buffer to the DS-System. This option is selected by default. **For more information, see Section 5.2.7, "Performance", on page 113.**
   - **Detailed log** – Records all files that are backed up in the Activity Log. For more information, see Section 8.1, "Viewing the Activity Log", on page 578.
   - **Initial backup** – Uses the Initial Backup feature for the first backup. To configure the initial backup path, click **[>>]**. For more information, see Section 11.1.1, "Configuring the initial backup path", on page 618.
   - **Stop on errors** – Stops a backup process when the number of errors reaches the specified value. A value of 0 means the DS-Client does not stop a backup process regardless of the number of errors.

     NOTE: You can configure the default setting using the **MaxErrors** advanced configuration parameter. For more information, see Section 2.1.8.6, "Miscellaneous parameters (Windows)", on page 42.

   - **Compression type** – Specifies the type of compression that will be applied to the backup. The options are as follows:
     - **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good default compression when the network is not the bottleneck.

- **ZLIB (Global, Low, Medium, and High)** – Normally produces better compression than LZOP, but will take more time to compress. This is a good default compression when the bottleneck is the network. ZLIB Low corresponds to a value of 3, ZLIB Medium = 6, and ZLIB High = 9.
- **None** – Disables compression for the backup.

2. Configure additional options for the backup as follows:
   - To lock the tables before inserting data on restore, select the **Add locks around insert statements** check box. For more information, see *MySQL* documentation.
   - To add MySQL specific extensions to the backed up database dump, select the **Add MariaDB specific table create options** check box.
   - To specify how table rows are inserted into the database, beside **Insert statements type**, select an insertion type. For more information, see *MySQL* documentation. The options are as follows:
     - **Extended** – Table rows are inserted to the database dump very quickly. This method is not useful for manual loading into non MySQL databases.
     - **Normal** – Table rows are inserted using a standard method which is slower but is portable to other databases.
     - **Complete** – Table rows are inserted using complete INSERT statements that include column names.
   - To specify how tables are dumped, beside **Table dumping option**, select a table dump method. The options are as follows:
     - **Lock all tables** – Sets the tables to ready only mode and prevents changes to data during the backup process.
     - **Single transaction** – Prevents changes to the backup data, but does not set the tables to read-only mode during the backup process.This option works only with transactional tables.
     - **Do not lock tables** – You can change the table during the creation of the dump file.This could impact the consistency of the backup.
     - **None** – Database dump is performed using the mysqldump function with no special conditions.
3. To specify a command to run before (Pre) and/or after (Post) the execution of the backup, click **Pre/Post**. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525 and Section 5.26, “Configuring Pre/Post processes (Linux)”, on page 528.
4. Click **Next**.

5.9.5.6 Specifying notification options

IMPORTANT: The email and pager options are available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

1. To configure a notification, do one of the following:
   - To add a notification, click **Add**.
   - To modify a notification, select the notification, and then click **Modify**.

   NOTE: To delete a notification, select the notification, and then click **Delete**.

2. To send an email notification, select **E-Mail**, and then do the following:
   a) To send the email notification to the DS-Client administrator, select **Administrator**.
   b) To send an email to another recipient, select **Other**, and then specify the recipient’s email address.
   c) To send detailed backup information, select the **Detailed notification** check box.
   d) To include a detailed file-level backup log as an attachment, select the **Attach detailed log** check box.
   e) To compress the detailed log, select the **Compress** check box.
   f) To send detailed backup information, select the **Detailed notification** check box.
   g) To include a detailed file-level backup log as an attachment, select the **Attach detail log** check box.
   h) To send the email notification in HTML format, select the **Send E-Mail using HTML format** check box.

      NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

   i) Click **OK**.

3. To send a pager notification, select **Pager**. The notification will be sent to the pager account configured for the DS-Client.

NOTE: The pager option is available only if the DS-Client has been configured for pager notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

---

4. In the **Completion** box, specify under what conditions a notification will be sent, and click **OK**. The options are as follows:
   - **All** – Notification will be sent under all conditions.
   - **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
   - **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.
   - **Complete with errors** – Notification will be sent if an activity is completed with at least one error event.
   - **Incomplete** – Notification will be sent if an activity is not completed successfully.
5. Under **Send SNMP traps when**, configure the DS-Client to send SNMP traps when the backup has completed successfully, completed with warnings, completed with errors, or is incomplete.
6. Click **Next**.

5.9.5.7 Assigning a retention rule

1. To assign a retention rule to the backup, do one of the following:
   - If you don’t want to assign a retention rule, select **No retention rule**.
   - To assign a retention rule, select **Use a specific retention rule**, and then select the retention rule.

NOTE: To create or edit a retention rule, click **[...]**. For more information, see Section 4.1, “Configuring a retention rule”, on page 98.

---

2. Click **Next**.

5.9.5.8 Assigning a schedule

1. To assign a schedule to the backup, do one of the following:
   - If you don't want to assign a schedule, select **Not scheduled**.
   - To assign a schedule, select **Scheduled.** In the **Available schedules** box, select an existing schedule.

   NOTE: To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, "Configuring a schedule", on page 90.

2. Click **Next**.

5.9.5.9 Specifying a backup name

1. In the **Set name** box, type a name for the backup.
2. In the **Set type** box, select the type of backup you want to create. The list of available backup types depends on the configuration of your DS-Client.
   - Online
   - Self-contained
   - Local-only
   - Statistical

   NOTE: For more information, see Section 5.1, "Backup types", on page 106.

3. If you selected **Online**, do the following:
   a) To send a copy of the oldest generation of the file that is about to be overwritten from the DS-System to the BLM Archiver, select the **BLM (Infinite Generations)** check box.

   NOTE: The Backup Lifecycle Management tool must be enabled.

   b) To save a copy of the backup data to a local storage location on the DS-Client computer, select the **Save on Local Storage** check box.

   NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Self-contained and Local Only backups.

c) To use the local storage as a cache if the DS-Client loses connection with the DS-System, select the **Transmission cache on Local Storage** check box. The cached backup data will be sent to the DS-System on the next connection after synchronization.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

4. If you selected **Self-Contained**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

5. If you selected **Local-Only**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

6. If you selected **Statistical**, and want to emulate an actual backup transfer process, select the **Calculate transmit amount** check box. During the backup, specified backup files will be read from their source and processed for compression and encryption.
7. Click **Finish**.

5.9.6 Restoring a MariaDB database backup

You can restore data from a MariaDB database backup.

NOTE: Only users with the required permissions can restore a MariaDB database backup.

5.9.6.1 Selecting the restore items

1. Browse the backups tree and select the backup you want to restore.
2. On the **Restore** menu click **Restore Now**.
3. To restore an entire backup or an entire database, browse the database tree, and select the check box beside the backup or folder you want to restore.
4. To restore individual files, select the folder containing the required files, and then click **Show Files**. Under **File List**, do the following:
5. To view the number of files selected and calculate the total amount of files selected, select the **Calculate amount** check box under **Options**.
6. In the **Files List** section, do one of the following:
   - To view details about the backed up file, select the file, and then click **File Info**.
   - To view the details of the items you selected, click **Selection**.
   - To view a list of archived generations for a folder, do the following:
     a) In the **Database Tree**, select the folder, and then click **Show Files**.
     b) Under **Files**, click **Show Archived**.
7. To refine your selection of items to restore, click **Advanced**, and then in the **Advanced Options** dialog box, do the following:
   a) To restore the latest generation of all the files, select **Latest generation of all data**.
   b) To restore files that were deleted from the source, but not removed from the online storage as of the last backup session, select **Latest generation of all data (except deleted data)**.
   c) To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:
      1. Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.
      2. Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.
   d) Click **OK**.
8. Click **Next**.

5.9.6.2 Selecting the restore location

1. Select the location to which you want to restore the backup. The options are as follows:
   - **Original location** – Data is restored to the original backup source location and existing files with the same name are overwritten. This is the default option.
   - **Alternate location** – Select to restore data to a location other than the original backup source.
2. If you selected **Alternate location**, then do one of the following:
   - To restore to a different server on the network, do the following:
     a) Beside the **Alternate location** box, click **[>>]**.
     b) In the **Select alternate location** dialog box, select the server where you want to restore the backed up database. You can also type the name or the IP address in the **Path** box.

     NOTE: By default, DS-Client uses your current user credentials to connect to the selected computer and database.

     c) The **Ask for database credentials** check box is selected by default. You will be prompted to enter a valid user name and password for the selected database.
     d) To specify the database dump application to use for the MySQL database backup, select the **Database Dump Configuration** check box.
     e) Click **Select**.
     f) In th **User name** and **Password** boxes, type the credentials required to connect to the selected database server.
     g) In the **Port** box, enter the port number DS-Client will use to communicate with the database. By default, DS-Client uses port 3306.
   - To use a different dump path during restore, beside the **Dump to** box, click **[>>]**, and select a dump path (for Windows only). The options are as follows:
     - **Dump path** – Save the dump file to a path on the Oracle server. The **Restore only the dump file(s)** check box is selected by default.
     - **DS-Client Buffer** – Save the dump file to the local storage on the DS-Client computer.

h) **DS-Client Pipe** – During restore, the DS-Client reads from the pipe on the source database. This method is useful if the database is too large to be dumped to a file on either the database server or the DS-Client buffer.

IMPORTANT: Do not change the port number unless you have a specific requirement to do so. For more information, refer to the *Oracle MySQL* documentation.

---

i) Click **OK**.

j) In the **Dump utility directory** box, type the installation path of a specific MySQL database dump application that will be used for this backup. If you do not specify the path, DS-Client will select one automatically.

k) Click **OK**.

3. To restore the dump file to the specified location, select the **Restore as Pure Files** check box.
4. Click **Next**.

5.9.6.3 Selecting the restore options

1. To skip the pre and post restore processes, select the **Skip Pre/Post** check box. If this check box is clear, click **Pre/Post**. DS-Client will run a specified activity before and/or after a restore operation. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525.
2. To record all restored files in the Activity Log, select the **Detailed log** check box.
3. If the database selected for restore already exists and you want DS-Client to restore to the existing database, select the **Do not drop existing DB before restore** check box.
4. Click **Next**.

5.9.6.4 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, select the type of restore. The options are as follows:
   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.
3. Click **Finish**.

5.10 Microsoft 365 backups (Windows)

You can back up and restore data from the following Microsoft 365 services:

- **Exchange Online** – You can back up and restore the following data:
  - Emails
  - Calendars and appointments
  - Contacts (including Contact Lists, but not Contact Groups)
  - Tasks

  NOTE: The Exchange Online data must be in a user mailbox, shared mailbox, or resource mailbox and can be restored to the same mailbox or a different mailbox on the original domain or a different domain.

- **SharePoint Online** – You can back up and restore the following data:
  - Sites
  - Subsites
  - Lists
  - List items
  - Settings

- Permissions

NOTE: You can back up data at the site and list levels. You cannot select list items individually as backup items, but the individual list items within selected lists will be backed up. You can select individual list items for restore.

- **OneDrive** – You can back up and restore OneDrive data under personal sites.

NOTE: The OneDrive data is backed up as the Documents List of personal sites for each user.

We recommend using the Management Console or DS-NOC rather than the DS-User to configure and schedule Microsoft 365 backups. After the backups have been created and scheduled, you can use the Management Console or DS-User to perform on-demand backups or restore the data.

IMPORTANT: Do not use the DS-User to modify the properties of a Microsoft 365 backup that was created in the Management Console or DS-NOC. In particular, changing the backup name or the schedule in this manner can adversely affect the operation of the system.

5.10.1 General requirements

To optimize the speed of Microsoft 365 backups, we recommend you set up the DS-Client and DS-System to communicate within the same local area network (LAN) at the same site location. This setup keeps communication localized between the DS-Client and DS-System. After obtaining data from the source, the DS-Client can send the backup data to the DS-System over the LAN, which is more efficient than transferring over a wide area network (WAN).

NOTE: This setup differs from the typical recommendation of installing the DS-Client on the same LAN with the backup source.

5.10.2 Network requirements

Ensure that the following network requirements are met:

- The DS-Client computer is able to access *.office365.com.
- Ports 80, 8080, and 443 are open on the DS-Client computer.
- Proxy server settings are configured if the DS-Client service is behind a proxy.

5.10.3 DS-Client computer requirements

Ensure that the DS-Client service uses a Windows administrator account to log on when it starts. If the DS-Client service uses a local system account, logon failure errors might occur due to a limitation of the authentication method used by Microsoft when you attempt to create a Microsoft 365 backup.

5.10.4 Microsoft 365 requirements

A Microsoft 365 license is required for each user who has Microsoft 365 data that will be backed up and restored and for each user who will manage the backup and restore process or whose credentials will be used by the DS-Client to access the backup source. For example, to back up and restore a Microsoft 365 mailbox or SharePoint site, a corresponding Exchange Online license or SharePoint Online license is required.

5.10.5 Exchange Online requirements

Before performing a backup or restore of data from Exchange Online:

- Configure the settings in the Local Group Policy Editor as follows:

  1. Click **Start** and then **Run**.
  2. Type gpedit.msc. The Group Policy Object Editor appears.
  3. Browse to **Local Computer Policy** > **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Windows Remote Management (WinRM)** > **WinRM Client**.
  4. Set up authentication as follows:

```
Allow Basic Authentication        : Enabled
Allow CredSSPauthentication       : Not configured
Allow unencrypted traffic         : Enabled
Disallow Digest authentication    : Not configured
Disallow Kerberos authentication  : Not configured
Disallow Negotiate authentication : Enabled
```

```
Trusted Hosts                       : Enabled
```

NOTE: When you enable Trusted Hosts, you must add the computer name of the on-premises Microsoft Exchange Server or add * to the TrustedHostsList.

- Configure the credentials that will be used for the backup of the Microsoft Exchange data. Each user account must be associated with a user mailbox. Configure each user as follows:

  1. Go to the administrative settings for Exchange:
     - For Exchange Online: In the Microsoft 365 account, on the ADMIN menu, select Exchange.
     - For Exchange Online in a Microsoft 365 Small Business domain, visit https://outlook.office365.com/ecp/.

1. Add users to Discovery Management as follows:
   a) Go to **permissions** > **admin roles**.
   b) In the list, select **Discovery Management**, and then click the Edit button.
   c) In the pop-up window, under Members, click **+**.
   d) In a new pop-up window, select the user you need to add, click **add**, and then click **OK**.
   e) In the first pop-up window, click **Save**.
   f) In the admin roles pane, verify that the user you need to add is listed under Members of the Discovery Management group.
2. Add users to Organization Management as follows:
   a) Go to **permissions** > **admin roles**.
   b) In the list, select **Organization Management**, and then click the Edit button.
   c) In the pop-up window, under Members, click **+**.
   d) In a new pop-up window, select the user you need to add, click **add**, and then click **OK**.
   e) In the first pop-up window, click **Save**.
   f) In the admin roles pane, verify that the user you need to add is listed under Members of the Organization Management group.
3. Add application impersonation as an assigned role in Organization Management as follows:

a) Go to **permissions** > **admin roles**.

b) In the list, select **Organization Management**, and then click the Edit button.

c) In the pop-up window, under Role, click **+**.

d) In a new pop-up window, select **ApplicationImpersonation**, click **add**, and then click **OK**.

e) In the first pop-up window, click **Save**.

f) In the admin roles pane, verify that **ApplicationImpersonation** is listed under Assigned Roles of the Organization Management group.

NOTE: Backups can fail if the DS-Client does not have access to multiple credentials or if concurrent backup activities use the same credentials.

The minimum number of credentials required is proportional to the maximum number of concurrent activities, which is configured using the MaxSessions advanced configuration parameter.

- When the MaxSessions parameter value is 4 or less, you must provide at least one credential per DS-Client.
- When the MaxSessions parameter value is between 5 and 8, you must provide at least two credentials per DS-Client.
- When the MaxSessions parameter value is between 9 and 12, you must provide at least three credentials per DS-Client.

IMPORTANT: Each credential you provide can support no more than four concurrent activities.

- To exclude SMTP addresses not associated with a mailbox, set the **ExchangeOnlineExcludeGroupMailboxes** value to **Yes**. This automatically makes distribution groups, deleted users, and other email addresses that do not have a mailbox unavailable for selection.

NOTE: If this parameter is not enabled, you must ensure distribution groups are not selected alongside mailboxes that you have manually selected for backup in a Microsoft 365 backup.

5.10.6 SharePoint Online and OneDrive requirements

Before performing a backup or restore of SharePoint Online or OneDrive data:

- Create at least one dedicated SharePoint account for each DS-Client for the purpose of accessing the backup source and restore destination. The dedicated SharePoint account requires the following permissions:
  - **Global Admin** – Must be configured as a Global administrator.
  - **Site Admin** – The same Global Administrator must be configured as a Site Administrator for each site. The DS-Client applies the Site Administrator role automatically for personal sites.
- Ensure the DS-Client buffer location provides sufficient space because it is used to temporarily store files larger than 500 MB. The DS-Client buffer must be able to data based on a combination of the batch size and the largest possible size of files to be backed up simultaneously.

NOTE: For more information, see Section 5.2.7, “Performance”, on page 113.

5.10.7 Creating a Microsoft 365 backup

You can create a Microsoft 365 backup.

- To back up Microsoft Exchange mailboxes, the user must have the Microsoft 365 Exchange Online license or a Microsoft 365 license that includes equivalent permissions.
- To back up Microsoft SharePoint sites, users must have a Microsoft 365 SharePoint Online license or a Microsoft 365 license that includes equivalent permissions. The user performing the backup must be a Global admin or SharePoint admin as well as a Site admin.

NOTE: In Microsoft 365 Small Business domains, only the backup and restore of Exchange Online data is supported by DS-Client.

5.10.7.1 Selecting the type of backup

1. On the **Sets** menu, click **New Backup Set**.
2. Select **Backup from the cloud**, and then click **Next**.

NOTE: An Exchange backup that contains distribution groups as backup items or as part of backup items can result in errors during backup.

5.10.7.2 Selecting the type of cloud service

1. Select **Microsoft 365**.
2. Click **Next**.

IMPORTANT: When you configure Microsoft 365 backups for a domain in Cloud Management System, ensure that distribution groups are not selected alongside mailboxes that you have manually selected for backup.

5.10.7.3 Selecting the server

3. In the **Enter Network Credentials** dialog box, do the following:
   a) In the **Connect as** box, type the user name for the Microsoft 365 server.
   b) In the **Password** box, type the associated password.
   c) In the **From** box, type the domain name of the backup source, i.e., your Microsoft 365 server domain, as configured on your network.
4. Click **OK**.

NOTE: The list of items displayed depends on the credentials entered. For more information, see Section 5.11, “Microsoft 365 Groups backups (Windows)”, on page 288.

5.10.7.4 Selecting the backup items

IMPORTANT: You can select multiple user accounts or site, but we recommend limiting each backup to one user account or one site for performance reasons. When you create Microsoft 365 backups using Cloud Management System in Windows DS-NOC, this limitation is enforced automatically.

1. Select a user, folder, or site to back up, and then click **Add**.

   NOTE: Do not select items from both Exchange and SharePoint to back up in the same Microsoft 365 backup. Use a separate Microsoft 365 backup for each backup source.

   - To exclude an item when its parent directory is selected for backup, select the item, and then click **Exclude.**
   - To remove a selected item, select the item under **Backup Items Selected**, and then click **Remove**.
   - To exclude an item using regular expressions, select the item, and then click **RegEx**.

   NOTE: Regular expressions provide more specific filtering than the exclude function. For example, you can use regular expressions to exclude individual file names or patterns. Use this option only if you are familiar with the syntax.

   - To add or exclude individual items inside a folder (Exchange Online only), do the following:

     a) Expand the user, select the folder, and then click **Items**.

     NOTE: The value displayed in the size column reflects the size of the item on the source server in MIME format. This might differ from the size of the item in storage with full fidelity after it has been backed up.

     b) Select the individual emails or entries you want to add or exclude to or from the backup.

     c) Click **Add** or **Exclude**.

     d) Click **Finish**.

2. Click **Next**.

5.10.7.5 Selecting the backup item options

1. To configure the maximum generations for a backup item that will be stored online, double click the **Max Gen** cell, and then enter the value.
2. To back up the file permissions for an item, select the item, and then select the **Backup permissions** check box.
3. Click Next.

5.10.7.6 Selecting the backup options

1. Under **Backup options**, configure the options you want to apply to the backup. The options are as follows:
   - **Detailed log** – Records all files that are backed up in the Activity Log. For more information, see Section 8.1, “Viewing the Activity Log”, on page 578.
   - **Initial backup** – Uses the Initial Backup feature for the first backup. To configure the initial backup path, click **[>>]**. For more information, see Section 11.1.1, “Configuring the initial backup path”, on page 618.
   - **Stop on errors** – Enter the number of errors that must occur before a back up is stopped.
   - **Compression type** – Specifies the type of compression that will be applied to the backup. The options are as follows:
     - **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good default compression when the network is not the bottleneck.
     - **ZLIB (Global, Low, Medium, and High)** – Normally produces better compression than LZOP, but will take more time to compress. This is a good default compression when the bottleneck is the network. ZLIB Low corresponds to a value of 3, ZLIB Medium = 6, and ZLIB High = 9.
     - **None** – Disables compression for the backup.
2. Click **Next**.

5.10.7.7 Specifying notification options

1. To configure a notification, do one of the following:
   - To add a notification, click **Add.**
   - To modify a notification, select the notification, and then click **Modify.**

   NOTE: To delete a notification, select the notification, and then click **Delete**.

2. To send an email notification, select **E-Mail**. and then do the following:
   a) To send the email notification to the DS-Client administrator, select **Administrator**.
   b) To send an email to another recipient, select **Other**, and then specify the recipients email address.
   c) To send detailed backup information, select the **Detailed notification** check box.
   d) To include a detailed file-level backup log as an attachment, select the **Attach detail log** check box.
   e) To send the email notification in HTML format, select the **Send E-Mail using HTML format** check box.
   f) Click OK.

   NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

3. To send a pager notification, select **Pager**. The notification will be sent to the pager account configured for the DS-Client.

   NOTE: The pager option is available only if the DS-Client has been configured for pager notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

4. To send a broadcast notification, select **Broadcast**. Select the server containing the messenger service to which you want to send the message and click **OK**.

   NOTE: Broadcast notifications to domains or workgroups are limited to 128 characters.

5. To send an event notification, select **Event**. Select the server on which you want the notification to be recorded in the Event Log and click **OK**.
6. In the **Completion** box, specify under what conditions a notification will be sent, and click **OK**. The options are as follows:
   - **All** – Notification will be sent under all conditions.
   - **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
   - **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.
   - **Completed with errors** – Notification will be sent if an activity is completed with at least one error event.
   - **Incomplete** – Notification will be sent if an activity is not completed successfully.
7. Click **Next**.

5.10.7.8 Assigning a retention rule

1. To assign a retention rule to the backup, do one of the following:
   - If you don't want to assign a retention rule, select **No retention rule**.
   - To assign a retention rule, select **Use a specific retention rule**, and then select the retention rule.

NOTE: To create or edit a retention rule, click **[...]**. For more information, see Section 4.1, "Configuring a retention rule", on page 98.

---

2. Click **Next**.

5.10.7.9 Assigning a schedule

1. To assign a schedule to the backup, do one of the following:
   - If you don't want to assign a schedule to the backup, select **Not scheduled**.
   - To assign a schedule to the backup, select **Scheduled.** In the **Available schedules** box, select an existing schedule.

NOTE: To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, "Configuring a schedule", on page 90.

---

2. Click **Next**.

5.10.7.10 Naming the backup

1. In the **Set name** box, type a name for the backup.
2. In the **Set type** box, select the type of backup you want to create. The list of available backup types depends on the configuration of your DS-Client.
   - Online
   - Statistical

   NOTE: For more information, see Section 5.1, “Backup types”, on page 106.
3. If you selected **Online**, do the following:
   - To send a copy of the oldest generation of the file that is about to be overwritten from the DS-System to the BLM Archiver, select the **BLM (Infinite Generations)** check box.

     NOTE: The Backup Lifecycle Management tool must be enabled for the DS-Client.
4. If you selected **Statistical**, and want to emulate an actual backup transfer process, select the **Calculate transmit amount** check box. During the backup, specified backup files will be read from their source and processed for compression and encryption.
5. If the multitenant feature is enabled and configured, in the **Customer** list, you can select the customer to which you want to assign the backup. For more information, see Section 11.5, “Multitenant DS-Clients”, on page 634.
6. Click **Finish**.

5.10.8 Restoring a Microsoft 365 backup

You can restore data from a Microsoft 365 backup. If you restore Microsoft Exchange data to the local disk, you can archive the restored files to a PST file. Before archiving Microsoft Exchange data to a PST file, consider the following:

- Ensure Microsoft Outlook is installed on the same machine as the DS-Client. During the restore process, the DS-Client will access Microsoft Outlook in the background.
- Ensure the security settings in the Microsoft Outlook Trust Center (Options > Trust Center > Trust Center Settings > Programmatic Access) are configured to never warn you about suspicious activity. For detailed instructions, see the Microsoft documentation.
- Ensure all the stores, such as mailboxes, that have been added to the current Microsoft Outlook profile are accessible (that is, with a legitimate license and not deleted or corrupted). Remove all other stores that are not added to the current profile.
- Ensure all foreground instances of Microsoft Outlook are closed on the DS-Client machine. If multiple restore activities will be running sequentially or simultaneously, ensure that all Microsoft Outlook instances are closed in the foreground before the first restore activity in the series.

NOTE: Microsoft Exchange data restored to a PST file does not retain the original time stamp and therefore should not be used for auditing purposes.

5.10.8.1 Selecting the restore items

IMPORTANT: Before restoring Microsoft Exchange data, ensure that the required mailbox already exists and is active in the domain at the destination (original or alternate). If the mailbox does not exist and is not active, not, the restore will fail.

---

1. Browse the backups tree and select the backup you want to restore.
2. On the **Restore** menu click **Restore Now**.
3. To restore an entire backup or folder, browse the tree and select the check box beside the backup or folder you want to restore.
4. To restore individual files, select the folder containing the required files, and then click **Show Files**. Under **File List**, do the following:
   - To view the details of the items you selected, click **Selection**.
   - To view archived files, click **Show Archived**.

5. To view the number of files selected and calculate the total amount of files selected, select the **Calculate amount** check box.
6. To exclude subdirectories, clear the **Include SubDirs** check box, as the default setting is to include sub-directories.
7. To search for files that match a certain criteria, in the **Filter** box, type the file pattern that you want to search for in the selected folder. For example, *.doc will search for all files with the doc file extension.
8. To search for a specific backed up file, click **Find File**. In the **Find Backed Up File** dialog box, do the following:
    a) Under **Search for**, select the search criteria to search for a backed up file either by **File name** or by **File ID**.
    b) Click **Find**.
    c) Select the required backed up file, and then click **Select**.
9. To refine your selection of items to restore, click **Advanced**. Under **Show**, select which generation you want to display. The options are as follows:
    a) To restore the latest generation of all the files, select **Latest generation of all data**.
    b) To restore files that were deleted from the source, but not removed from the online storage as of the last backup session, select **Latest generation of all data (except deleted data)**.
    c) To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:
        1. Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.
        2. Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.
    d) Click **OK**
10. Click **Next**.

5.10.8.2 Selecting the restore location

1. Select the location to which you want to restore the backup. The options are as follows:
   - **Original location** – This is the default option. Data is restored to the original backup source location, that is, the original Microsoft 365 account.
   - **Alternate location** – This option is available for Microsoft Exchange Online only.
2. If you have selected **Alternate location**, do the following:
   a) Beside the **Alternate location** box, click [>>].
   b) In the **Select Alternate Server** dialog box, do one of the following:
      - To proceed with the existing restore location, click **Select**, and in the **Enter Network Credentials** dialog box, enter the credentials to connect to the destination computer, and then click **OK**.

      IMPORTANT: The domain name that you provide in the network credentials must be identical to the domain name of the restore destination location, for both original and alternate restore locations.

      - Click **[...]** beside the **User Name** box to browse for an encrypted key file containing the user credentials. If it is a valid file, you must enter the correct key to unlock the file.
      - To restore to an on premises Microsoft Exchange Server, select the **Alternate Server** check box, type the complete address of the Microsoft Exchange Server to which you want to restore, and then click **Select**.

   c) In the **Restore to** cell, type the name of the folder or click **[>>]**, and select a folder.
   d) In the **Truncate** box, you can increase the truncate level to shorten the common path portion of the restore path, if the selected restore items contain a common path.
3. To restore the selected items to a disk location on the DS-Client computer, select the **Restore to local disk** check box, click **[>>]**, and then select the DS-Client computer.
4. To archive Microsoft Exchange data to a PST file at the specified restore location, select the **Archive restored files to PST** check box. This option is available when you select local disk as the restore location.

   IMPORTANT: If a PST file of the same name already exists in the folder, the restore process will not overwrite the existing PST file but append to the existing file. Ensure all foreground instances of Microsoft Outlook are closed.

DS-Client accesses Microsoft Outlook in the background during the restore process. You must not manually stop Microsoft Outlook when running as a background process during restore activities. Microsoft Outlook will close after all restore activities that require archiving to a PST file are completed.

5. Click **Next**.

5.10.8.3 Selecting the restore options

The required restore options are selected by default and you cannot make any changes. Click **Next**.

5.10.8.4 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, under **Restore classification**, select the type of restore. The options are as follows:
   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.
3. Click **Finish**.

NOTE: If you selected the restore option Archive restored files to PST and DS-Client cannot successfully connect to Microsoft Outlook to start the restore activity, increase the value of the *ExchangeOnlineOutlookConnectionTimeout* advanced parameter. For more information, see Section 2.1.8, “Configuring the advanced settings”, on page 37.

5.11 Microsoft 365 Groups backups (Windows)

You can back up and restore the following objects in Microsoft 365 Groups:

- **Groups** — Microsoft 365 Groups (or Unified Groups).
- **Conversations** — Conversations, threads, and posts, including attachments.
- **Drive** — SharePoint team site documents (or OneDrive documents), including drive folders.
- **Events** — Calendar events.
- **Members** — List of members.
- **Notes** — Notebooks in OneNote Online, including section groups, sections, and page contents.
- **Owners** — List of owners.
- **Photo** — Photo contents.
- **Plans** — Plans, plan details, buckets, tasks, and task details.

NOTE: Backup of reference attachments is not supported.

5.11.1 Configuring Microsoft Azure Active Directory

NOTE: Each set of OAuth 2.0 client credentials includes a value for the Directory, Client ID, Redirect URI, and Client secret used by DS-Client to access the Azure Active Directory. For more information, see the Microsoft Azure documentation

1. Sign in to the Microsoft Azure Active Directory admin center.
2. Configure the Azure Active Directory properties as follows:
   a) Click the **Azure Active Directory** service.
   b) Under **Manage**, click **Properties**.
   c) Under **Global admin can manage Azure Subscriptions and Management Groups**, click **No**.

   NOTE: Record the **Directory ID** or domain name. This is the **Directory** you must enter when creating a Microsoft 365 backup.

3. Configure the directory role for the active user who will create the OAuth 2.0 client credentials for the DS-Client to access Azure AD as follows:

a) Click the **Azure Active Directory** service.

b) Under **Manage**, click **Users**, and then select the active user you want to configure.

c) Under **Manage**, click **Assigned roles**, and then set the directory role for the active user as **Global Administrator**.

4. Register a new Microsoft Azure Active Directory web application and prepare a set of OAuth 2.0 client credentials for each new Microsoft 365 Groups backup as follows:

a) Click the **Azure Active Directory** service.

b) Under **Manage**, click **App registrations**.

c) Click **New application registration**.

d) In the **Name** box, type a name for the application.

e) In the **Application type** box, select **Web**.

f) Under **Supported account types**, click **Accounts in any organization directory (Any Azure AD directory - Multitenant)**.

g) In the **Redirect URL** box, type http://localhost:4413/. This is the **Redirect URI** you must enter when creating a Microsoft 365 backup.

h) Click **Register**.

NOTE: Record the **Application ID**. This is the **Client ID** you must enter when creating a Microsoft 365 backup.

---

5. Configure the settings for the Microsoft Azure Active Directory web application as follows:

a) Click **Certificates and Secrets**.

b) Click **New Client Secret**, provide a description, and then click **Add**.

NOTE: Record the key value. This is the **Client Secret** you must enter when creating a Microsoft 365 backup.

---

c) Click **API permissions**.

d) Click **Add a permission**.

e) Click **Microsoft APIs**, and then click **Microsoft Graph**.

f) Click **Delegated permissions**, and select the following permissions:

- Have full access to user calendars
- Read and write all groups

- Read and write all users' full profiles
- Read and write all OneNote notebooks that user can access

g) Click **Add permissions**

h) Click **Grant admin consent**.

5.11.1.1 Creating OAuth 2.0 client credential configuration file

To create an OAuth 2.0 client credential configuration file that can be imported when creating a Microsoft 365 Groups backup to automate the process., do one of the following:

- To use the directory ID in the properties of the Azure Active Directory, use this format:

```
directory:xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
client_id:xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
client_secret:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

- To use the domain name of the Microsoft 365 Group, use this format:

```
directory:example.onmicrosoft.com
client_id:xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
client_secret:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

NOTE: OAuth credentials that are saved as part of the backup might expire if the backup is not used for an extended period. If this occurs, the credentials can be reauthorized by typing them again on the **Share** tab of the **Properties** dialog box.

5.11.1.2 Configuring permissions and credentials

- Ensure that the user who will sign in to Microsoft 365 is both an owner and a member of the group that you want to back up and restore.

5.11.1.3 Configuring network settings

- On the machine on which the DS-User application runs, ensure that the specific inbound TCP port that is specified in the sign-on URL is open.

5.11.2 General limitations

The following functionality is not supported with Microsoft 365 Groups backups:

- Receiving notifications
- Assigning retention rules
- Migrating a backup
- Converting a backup
- Validating a backup
- Changing the ownership of a backup
- Performing an initial backup
- Restoring from disc/tape
- Copying to and restoring from a BLM Archiver

5.11.3 Backup limitations

The following limitations apply when backing up a Microsoft 365 Groups backups:

- Each group can contain a maximum of 5000 drive items, including folders.
- If you rename a section in OneNote Online, the section will still be recognized by the previous name during subsequent requests.
- The contents of an Microsoft 365 Group on the Files panel in the Outlook Web App are only backed up if they belong to a supported object type.
- Some lower-level directory tree items and folders cannot be added or excluded as backup items. During the backup process, these items and folders will be added or excluded accordingly with their parent folders.

5.11.4 Restore limitations

The following limitations apply when restoring a Microsoft 365 Groups backups:

- The reported size of items might differ from the actual size of items.
- Posts and events that are larger than 4 MB (including attachments) cannot be restored.
- When restoring calendar events that contain attachments, the attachments are not restored.
- Some object properties might retain their existing values even after a successful restore activity.

- You can browse through a folder structure for a specific backed up file, but cannot search for the file.
- Referenced contents (such as images) in restored objects (such as posts and pages) might not appear as the original.
- During the restore process, there might be a delay of up to 72 hours before some items appear in their respective web interfaces.
- On occasion, restored notebooks appear in the Notebooks folder of the Documents tab of the SharePoint portal rather than the OneNote Online portal.
- When restoring note pages, some HTML content and formatting might be lost. For example, page attachments, drawings, table borders, text highlighting, etc.
- When restoring conversation posts, the From field always displays the name of the user who performed the restore activity. In addition, the restored conversation posts might contain collapsed older posts.
- If you delete user accounts from an owner or member list, the associated users cannot be restored. Other entries in the owner or member list are unaffected. We recommend that you perform an on-demand backup of the affected backups after deleting user accounts associated with an owner or member list.

5.11.5 Creating a Microsoft 365 Groups backup

You can create a Microsoft 365 Groups backup.

5.11.5.1 Selecting the type of backup

1. On the **Sets** menu, click **New Backup Set**.
2. Select **Backup from the cloud**, and then click **Next**.

5.11.5.2 Selecting the type of cloud service

1. Select **Microsoft 365 Groups**.
2. Click **Next**.

5.11.5.3 Entering the Azure AD application credentials

1. On the **Enter Credentials** page, click **Next**.
2. In the **Azure AD OAuth 2.0 Client Credentials Grant** dialog box, do the following:
   a) In the **Directory** box, type the directory ID of the Azure Active Directory or the domain name of the Microsoft 365 Group that you want to back up.
   b) In the **Client ID** box, type the application ID.
   c) In the **Client secret** box, type the value that is generated on creating the API access key. To enter the required information, you can import a text file that contains the required OAuth 2.0 client credentials. To open the text file, click **Browse**. For more information, see Section 5.11.1, “Configuring Microsoft Azure Active Directory”, on page 288.

NOTE: Using a new set of OAuth 2.0 client credentials for each new Microsoft 365 Groups backup helps prevent throttling. For more information, see the *Microsoft documentation* on *Microsoft Graph throttling*.

---

3. If the **Authorize Azure AD Application** dialog box appears, do the following:
   a) Sign in to Azure AD using the credentials of a user who is both an owner and a member of the Microsoft 365 Group that you want to back up. Otherwise, the group must be public for the backup and restore processes to be successful.

NOTE: If prompted to stay signed in, click **No**. Otherwise, you will not be able to sign in as a different user when creating other new Microsoft 365 Groups backups.

---

   b) When prompted, indicate that you agree to grant the application the delegated permissions to the resources that belong to the signed-in user.
   c) Click **OK**.

5.11.5.4 Selecting the backup items

IMPORTANT: To back up the properties of a thread, ensure that you have also added the parent conversation item to be backed up. Adding the thread backs up only the posts that belong to the thread.

1. Expand the tree in the **Users and Services List**, and select the item you want to back up.
2. Click **Add**.
   - To exclude an item when its parent directory is selected for backup, select the item, and then click **Exclude.**
   - To remove a selected item, select the item under **Backup Items Selected**, and then click **Remove**.
   - To exclude an item using regular expressions, select the item, and then click **RegEx**.

     NOTE: Regular expressions provide more specific filtering than the exclude function. For example, you can use regular expressions to exclude individual file names or patterns. Use this option only if you are familiar with the syntax.

   - To view the items in a folder, select the folder, and then click **Items**.
   - To exclude subdirectories, clear the Include SubDirs check box, as the default setting is to include sub-directories.
3. Click **Next**.

IMPORTANT: Each item that you add to a Microsoft 365 Groups backup is identified by a unique path. If an item that is listed in the backup is deleted from the source server after the backup is created, the unique path of the deleted item becomes unusable. A newly created object with an identical name in the same location is identified by a new unique path and will not be backed up by the backup.

5.11.5.5 Selecting the backup item options

1. To configure the number of maximum generations of the selected backup item that will be stored online, double click in the **Max gen** cell, and then enter the new value.
2. Click **Next**.

5.11.5.6 Selecting the backup options

1. Under **Backup options**, configure the options you want to apply to the backup. The options are as follows:
   - **Detailed log** – Records all files that are backed up in the Activity Log.
   - **Stop on errors** – Enter the number of errors that must occur before a back up is stopped.
2. Click **Next**.

5.11.5.7 Assigning a schedule

1. To assign a schedule to the backup, do one of the following:
   - If you don't want to assign a schedule to the backup, select **Not scheduled**.
   - To assign a schedule to the backup, select **Scheduled.** In the **Available schedules** box, select an existing schedule.

NOTE: To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, "Configuring a schedule", on page 90.

---

2. Click **Next**.

5.11.5.8 Naming the backup

1. In the **Set name** box, type a name for the backup.
2. Click **Finish**.

NOTE: If an error occurs when validating credentials, you must reauthoriz. To reauthorize, close the wizard and create the Microsoft 365 Groups backup again. When prompted, enter the required credentials. To reauthorize after seeing the error in the Event Log of an existing Microsoft 365 Groups backup, on the **Share** tab of the **Set Properties** dialog box, verify and ensure the credentials that are entered for the backup are valid. For information on the required credentials, see Section 5.11.1, “Configuring Microsoft Azure Active Directory”, on page 288.

5.11.6 Restoring a Microsoft 365 Groups backup

You can restore data from a Microsoft 365 Groups backup. Existing objects at the restore destination are updated during the restore process. To restore backed up data as new objects, delete the existing objects from the restore destination location before you start the restore process.

To restore the properties of a thread, ensure you have also selected the parent conversation item to be restored. Selecting the thread restores only the posts that belong to the thread. Some properties of a restored task will not return to their original value. For example, the task completion date will display the time at which the task was restored rather than the time the task was completed.

NOTE: If you have deleted an entire Microsoft 365 Group from the restore destination, allow at least 24 hours for Microsoft to permanently delete the group and its data before you start the restore process. Otherwise, the group and its data might be incompletely restored.

5.11.6.1 Selecting the restore items

1. Browse the backups tree and select the backup you want to restore.
2. On the **Restore** menu click **Restore Now**.
3. To restore an entire backup or folder, browse the tree and select the check box beside the backup or folder you want to restore.
4. To restore individual files, select the folder containing the required files, and then click **Show Files**. Under **File List**, do the following:

NOTE: When you restore the list of members or owners, the restore process replaces the existing list with the restored list. Items in the existing list that are not in the restored list are removed from the restore destination after the restore process.

---

5. To view the number of files selected and calculate the total amount of files selected, select the **Calculate amount** check box.
6. To exclude subdirectories, clear the **Include SubDirs** check box, as the default setting is to include sub-directories.
7. To filter the list of files, in the **Filter box**, enter a filter using * as a wildcard, and then click **Show Files** to update the list of files.
8. To review a list of the items that you have selected, click **Selection**.
9. To see details about an item, highlight the item and then click **Show Files**. To locate and select older generations of a file, highlight the file and then click **File Info**. For more information, see Section 5.3.1, “Restoring a specific generation of a file”, on page 129.
10. To refine your selection of items to restore, click **Advanced**. Under **Show**, select which generation you want to display. The options are as follows:
    a) To restore the latest generation of all the files, select **Latest generation of all data**.
    b) To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:
        1. Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.
        2. Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.
    c) Click **OK**.
11. Click **Next**.

5.11.6.2 Selecting the restore location

1. The default restore location is **Original location**.
2. Click **Next**.

5.11.6.3 Selecting the restore options

The required restore options are selected by default and you cannot make any changes. Click **Next**.

5.11.6.4 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, under **Restore classification**, select the type of restore. The options are as follows:
   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.
3. Click **Finish**.

5.12 Microsoft Exchange Server (VSS-aware) backups (Windows)

You can back up and restore data on a Microsoft Exchange Server by performing an online backup using the Microsoft VSS (Volume Shadow Copy Service) component on the destination computer.

Each Microsoft Exchange database is presented as a component by the Microsoft Exchange VSS writer. A component must be restored with all its contents, based on the rules specified in its metadata. For more information, see Section 5.3.7, “Restoring VSS-aware backup components”, on page 133.

IMPORTANT: When creating a VSS-aware backup, the source database cannot reside on an SMB remote share as this is currently not supported and can result in a VSS snapshot failure.

5.12.1 Creating a Microsoft Exchange Server (VSS-aware) backup

You can create a Microsoft Exchange Server (VSS-aware) backup in a standalone or database availability group (DAG) configuration.

IMPORTANT: To back up and restore a Microsoft Exchange Server in a DAG configuration, you must configure DNS on the DS-Client computer. Ensure the domain controller and all DAG nodes can be accessed through their fully qualified domain name (FDQN).

5.12.1.1 Selecting the type of backup

1. On the **Sets** menu, click **New Backup Set**.
2. Select **VSS-aware Backup Set**, and then click **Next**.

5.12.1.2 Selecting the VSS-aware backup type

1. Select **Microsoft Exchange Server**.
2. Click **Next**.

5.12.1.3 Selecting the backup source

IMPORTANT: Remote UAC is enabled by default for a VSS-aware backup. Local administrator account must have access to admin$ share on the source machine.

1. Do the following:
   a) In the **Path** box, type the IP address or DNS name of the source Microsoft Exchange server or select the computer containing the files you want to back up. For DAG, this can be any of the mail server nodes.

      NOTE: By default, DS-Client uses your current credentials to connect to the selected computer.

   b) To provide the logon credentials for the selected, select the **Ask for Network Credentials** check box. You will be prompted to enter a valid user name and password for the selected computer.
   c) Click **OK**.

2. Click **Next**.

5.12.1.4 Selecting the Database Availability Group options

1. Do one of the following:
   - To back up only the node at the IP address you have connected to, select the **Back up individual mail server node** option.
   - To back up the DAG configuration, select the **Back up entire Database Availability Group** option, and then do one of the following:
     - To back up the active databases in the DAG, select the **Back up active databases** option, and then click **Next**.
     - To back up the passive databases in the DAG, select the **Back up passive databases** option.

NOTE: If you are backing up a non-DAG Microsoft Exchange Server, the Back up individual mail server node option is selected by default.

---

2. To reorder the backup priority, select a mail server node from the list, and then click **Move Up** or **Move Down**
3. Click **Next**.

5.12.1.5 Selecting the components to back up

1. To add an item, select the item, and then click **Add**. You can add only one item at a time.
2. To exclude an item when its parent directory is selected for backup, select the item, and then click **Exclude.**
3. To back up the entire Microsoft Exchange Server, select **Microsoft Information Store**, and then click **Add**.
4. To remove an item from the list of selected items for backup, select the item, and then click **Remove**.
5. Click **Next**.

5.12.1.6 Selecting the backup item options

1. If you selected **Back up individual mail server node**, do one of the following:
   - To configure the maximum generations for a backup item that will be stored online, double click the **Max Gen** cell, and then enter the value.
   - To back up only active mailbox databases, select the **Back up active database** check box.
   - To backup only passive mailbox databases, select the **Back up passive database**

   NOTE: You must not select one of these options if you have selected one or multiple folders or individual mailbox databases as backup items.

2. If you selected **Back up entire Database Availability Group**, do one of the following:
   - To configure the maximum generations for a backup item that will be stored online, double click the **Max Gen** cell, and then enter the value.
   - To back up the file permissions for an item, select the item, and then select the **Backup permissions** check box.
   - To back up the streams of data associated with an item, select the item, and then select the **Backup streams** check box.
3. Click Next.

NOTE: The truncation of transaction log files with VSS-aware backups is controlled by Microsoft components and differs depending on the kind of backup being performed (non-DAG configuration or DAG replicated configuration). For more information, see the *Microsoft Developer Network* documentation.

5.12.1.7 Selecting the backup options

The differential backup policy works if the backup is the only process that backs up the database. If another backup is used to back up the database, or the internal Exchange commands are used to perform manual backups or dumps, then the next backup requires a full dump.

1. Under **Backup options**, configure the options you want to apply to the backup. The options are as follows:

   - **Detailed log** – Records all files that are backed up in the Activity Log. For more information, see Section 8.1, “Viewing the Activity Log”, on page 578.
   - **Initial backup** – Uses the Initial Backup feature for the first backup. To configure the initial backup path, click **[>>]**. For more information, see Section 11.1.1, “Configuring the initial backup path”, on page 618.
   - **Stop on errors** – Stops a backup process when the number of errors reaches the specified value. A value of 0 means the DS-Client does not stop a backup process regardless of the number of errors.

     NOTE: You can configure the default setting using the **MaxErrors** advanced configuration parameter. For more information, see Section 2.1.8.6, “Miscellaneous parameters (Windows)”, on page 42.

   - **VSS validation** – Specifies the type of VSS validation that will be applied prior to performing the backup. The options are as follows:
     - **Disable** – VSS validation is not performed.
     - **Enable** – VSS validation is performed.
     - **Use DS-Client’s settings** – VSS validation is performed using the DS-Client settings.
   - **Compression type** – Specifies the type of compression that will be applied to the backup. The options are as follows:
     - **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good default compression when the network is not the bottleneck.
     - **ZLIB (Global, Low, Medium, and High)** – Normally produces better compression than LZOP, but will take more time to compress. This is a good default compression when the bottleneck is the network. ZLIB Low corresponds to a value of 3, ZLIB Medium = 6, and ZLIB High = 9.
     - **None** – Disables compression for the backup.

2. Under **Database backup policy**, in the **Full dump** box, select a method for the full dump: The options are as follows:

- **Always** (Default) — Performs a full dump (VSS snapshot) of each database.
- **Plus Differential** — Performs a full dump (VSS snapshot) of the database on first backup followed by differential backups until another full backup is required. Differential backups contain all the changes to the database since the last full dump.
- **Plus Incremental** — Performs a full dump (VSS snapshot) of the database on first backup followed by incremental backups until another full backup is required.

Other than the first time, a full dump is required when:

- A database has been backed up by another backup or manually from the Exchange tools.
- A database has been restored either from another database or an earlier generation.
- The database properties have been modified. For example, if the recovery model has been switched to simple.

d) To prevent a full dump from being performed during the selected time period, select the **Do not start full dump on** check box, select the day, and then specify the time period.

NOTE: The **Do not start full dump** option uses the same number set in the **MasterGenerations** advanced parameter. For more information, see Section 2.1.8, “Configuring the advanced settings”, on page 37.

- To force a full backup to be performed at an interval, select the **Full every** check box, and then specify the values for the interval.
- To force a full backup to be performed on a specific day of the week, select the **Full every week on** check box, select the day, and then specify the time after which the full backup can be performed.
- To force full backup to be performed on a regular monthly interval, select the **Full every month on** check box, select the day, and then specify the time after which the full backup can be performed.

IMPORTANT: You must perform Full dumps at a regular frequency to protect the integrity of the database backup. By default, DS-Client allows a full backup to be skipped a maximum of 120 consecutive times. You can configure this value using the **MaxNonFullDumps** advanced parameter.

For more information about database backup policy options, see Section 5.2.5, “Database backup policies”, on page 112.

3. To specify a command to run before (Pre) and/or after (Post) the execution of the backup, click **Pre/Post**. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525 and Section 5.26, “Configuring Pre/Post processes (Linux)”, on page 528.
4. Click **Next**.

5.12.1.8 Specifying backup performance options

IMPORTANT: These options are intended for high performance environments where the DS-Client can take advantage of the speed of the storage where the source data resides. Test different settings to determine the optimal value. Slower storage can result in performance issues if the values are not properly configured.

1. Under **Maximum pending asynchronous I/O for a file**, configure the maximum I/O operations the DS-Client will use for each file from the backup.
   - To use the default MaxPendingIOPerFile advanced configuration parameter setting, click **Use DS-Client’s settings**. For more information, see Section 2.1.8.10, “Performance parameters (Windows)”, on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value** and then enter the value.

   NOTE: This setting is for storage devices that support better parallel disk I/O, such as NAS devices. The optimal setting for this value depends on the storage device and network speed. Increasing this value can significantly increase the backup speed. If your storage device does not support better parallel disk I/O, use the default value, otherwise the performance can be significantly degraded.

2. Under **Read buffer size for backup**, configure the internal buffer size (in KB) for reading a file during the backup process.
   - To use the default **FileReadBufferSize** advanced configuration parameter, click **Use DS-Client’s settings**. For more information, see Section 2.1.8.10, “Performance parameters (Windows)”, on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific buffer size (KB)**, and then enter the value.

   IMPORTANT: To achieve optimum backup performance, the DS-Client read buffer size might need to be different, depending on the combination of the target storage device, target operating system, and any mid-ware involved between the storage and the operating system.

3. Click **Next**.

5.12.1.9 Selecting the notification options

1. To configure a notification, do one of the following:
   - To add a notification, click **Add.**
   - To modify a notification, select the notification, and then click **Modify.**

   NOTE: To delete a notification, select the notification, and then click **Delete**.

2. To send an email notification, select **E-Mail**. and then do the following:
   a) To send the email notification to the DS-Client administrator, select **Administrator**.
   b) To send an email to another recipient, select **Other**, and then specify the recipients email address.
   c) To send detailed backup information, select the **Detailed notification** check box.
   d) To include a detailed file-level backup log as an attachment, select the **Attach detail log** check box.
   e) To send the email notification in HTML format, select the **Send E-Mail using HTML format** check box.
   f) Click **OK**.

   NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

3. To send a pager notification, select **Pager**. The notification will be sent to the pager account configured for the DS-Client.

   NOTE: The pager option is available only if the DS-Client has been configured for pager notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

4. To send a broadcast notification, select **Broadcast**. Select the server containing the messenger service to which you want to send the message and click **OK**.

NOTE: Broadcast notifications to domains or workgroups are limited to 128 characters.

---

5. To send an event notification, elect **Event**. Select the server on which you want the notification to be recorded in the Event Log.
6. In the **Completion** box, specify under what conditions a notification will be sent, and click **OK**. The options are as follows:
   - **All** – Notification will be sent under all conditions.
   - **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
   - **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.
   - **Completed with errors** – Notification will be sent if an activity is completed with at least one error event.
   - **Incomplete** – Notification will be sent if an activity is not completed successfully.
7. Click **Next**.

5.12.1.10 Assigning a retention rule

1. To assign a retention rule to the backup, do one of the following:
   - If you don't want to assign a retention rule, select **No retention rule**.
   - To assign a retention rule, select **Use a specific retention rule**, and then select the retention rule.

NOTE: To create or edit a retention rule, click **[...]**. For more information, see Section 4.1, "Configuring a retention rule", on page 98.

---

2. Click **Next**.

5.12.1.11 Assigning a schedule

1. To assign a schedule to the backup, do one of the following:
   - If you don't want to assign a schedule, select **Not scheduled**.
   - To assign a schedule, select **Scheduled.** In the **Available schedules** box, select an existing schedule.

NOTE: To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, "Configuring a schedule", on page 90.

---

2. Click **Next**.

5.12.1.12 Naming the backup

1. In the **Set name** box, type a name for the backup.
2. In the **Set type** box, select the type of backup you want to create. The list of available backup types depends on the configuration of your DS-Client.
   - Online
   - Self-contained
   - Local-only
   - Instant recovery
   - Statistical

NOTE: For more information, see Section 5.1, "Backup types", on page 106.

---

3. If you selected **Online**, do the following:
   a) To send a copy of the oldest generation of the file that is about to be overwritten from the DS-System to the BLM Archiver, select the **BLM (Infinite Generations)** check box.

NOTE: The Backup Lifecycle Management tool must be enabled for the DS-Client.

---

b) To save a copy of the backup data to a local storage location on the DS-Client computer, select the **Save on Local Storage** check box.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Self-contained and Local Only backups.

---

c) To use the local storage as a cache if the DS-Client loses connection with the DS-System, select the **Transmission cache on Local Storage** check box. The cached backup data will be sent to the DS-System on the next connection after synchronization.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path.

---

d) To save a copy of the backup data to the instant recovery vault, select the **Save in instant recovery vault** check box.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Instant Recovery backups.

---

e) Beside the **Local Storage Path** box, click **>>**. Enter a local storage path for the backup, and then click **OK**

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

4. If you selected **Self-Contained**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

5. If you selected **Local-Only**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

6. If you selected **Instant Recovery**, the **Save in instant recovery vault** option is selected by default.

IMPORTANT: Each Linux DS-Client must have a unique ZFS file name.

---

7. If you selected **Statistical**, and want to emulate an actual backup transfer process, select the **Calculate transmit amount** check box. During the backup, specified backup files will be read from their source and processed for compression and encryption.
8. If the multitenant feature is enabled and configured, in the **Customer** list, you can select the customer to which you want to assign the backup. For more information, see Section 11.5, “Multitenant DS-Clients”, on page 634.
9. Click **Finish**.

5.12.2 Performing a VSS restore

You can perform a VSS restore of the selected backup session to the original backup source or alternate location using the Microsoft VSS tools on the destination computer.

- If you are restoring to the original location or an alternate location, you must prepare the restore destination before performing the restore activity
- If you are restoring to the original location, the DS-Client replaces the database files in the physical location.
- Whether you are restoring to original location or an alternate location, the domain name of the network credentials used for the restore activity must be identical to the domain name of the restore destination.
- If the domain name or the network credentials is different from that of the original source, then you must select alternate location when specifying the restore destination. Alternate location allows you to select an alternative restore destination location that is not the original source and to provide the necessary network credentials for the restore activity.

- If you are restoring to an alternate location, the DS-Client restores the log files to a restoredlogs folder, and then restores the database files to the physical location. VSS writers apply the logs from the restoredlogs folder and then remove the folder.
- The DS-client verifies if the destination database to be restored is in a mounted state.You can restore a Microsoft Exchange database only if the destination database for the restore is in a mounted state.
- The DS-Client retrieves information from the mounted database, including the physical path and database GUID.
- The DS-Client unmounts and mounts the Microsoft Exchange database.

5.12.2.1 Selecting the restore method

1. Browse the backups tree and select the backup you want to restore.
2. On the **Restore** menu, click **Restore Now**.
3. Select **VSS Restore**
4. Click **Next**.

5.12.2.2 Selecting the restore items

1. To restore an entire backup or folder, browse the tree and select the check box beside the backup or folder you want to restore.
2. To restore individual files, select the folder containing the required files, click **Show Files**, and then do the following:
   - To view details about the backed up file, select the file, and then click **File Info**.
   - To view archived files, click **Show Archived**.
3. To view the number of files selected and calculate the total amount of files selected, under **Options**, select the **Calculate amount** check box.
4. To search for files that match a certain criteria, in the **Filter** box, type the file pattern that you want to search for in the selected folder. For example, *.doc will search for all files with the doc file extension.
5. To view the details of the items you selected, click **Selection**.
6. To view the files that are part of the selected VSS component, click **VSS Component**.
7. To refine your selection of items to restore, click **Advanced**. Under **Show**, select which generation you want to display. The options are as follows:

- To restore the latest generation of all the files, select **Latest generation of all data**.
- To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:

  a) Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.

  b) Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.

  c) Click **OK**.

8. Click **Next**.

5.12.2.3 Selecting the restore location

1. Select the location to which you want to restore the backup. The options are as follows:
   - **Original location** – Data is restored to the original backup source location and existing files with the same name are overwritten. This is the default option.
   - **Alternate location** – Data is restored to a location other than the original backup source.

   NOTE: When restoring to an alternate location, the security of restored items in the destination location might not resemble the security of those items during backup.

2. If you selected **Alternate location**, then do the following:

   a) Beside the **Alternate location** box, click **[>>]**.

   b) In the **Select Alternate Server** dialog box, select the computer where you want to restore the data.

   c) To specify alternate network credentials, select the **Ask for Network Credentials** checkbox, and then click **Select**.

   d) In the **Enter Network Credentials** dialog box, enter the credentials to connect to the destination computer, and then click **OK**.

   e) To rename the individual components being restored, click **Rename component**.

   f) In the **Rename Component** dialog box, do the following:

1. Double click in the **Target Component** column and edit the name or path for the component.
2. To load mapping contents from a saved XML file, click **Load XML**.

NOTE: A mapping is loaded only if the logical path and the source component columns from the XML file exactly match with those displayed in the list.

---

3. To save the contents from the current source target mapping list to an XML file, click **Save XML**.
4. Click **OK**.

3. Click **Next**.

NOTE: For more information, see Section 5.3.3, “Restoring data to an alternate location”, on page 130.

5.12.2.4 Selecting the performance options

IMPORTANT: These options are intended for large backups in high performance environments where the DS-Client can take advantage of the speed of the storage where the source data resides. Test different settings to determine the optimal value. Slower storage can result in performance issues if these values are not configured correctly.

---

1. Under **Maximum pending asynchronous I/O for a file**, configure the maximum number of I/O operations the DS-Client will use for each file during the restore process.
   - To use the default MaxPendingIOPerFile advanced configuration parameter setting, click **Use DS-Client’s settings**. For more information, see Section 2.1.8.10, “Performance parameters (Windows)”, on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value** and then enter the value.
2. Under **DS-System side read threads**, configure the number of files the DS-System can read simultaneously for the restore process.
   - To use the default MaxRestoreReadThreads advanced configuration parameter setting, click **Use DS-Client’s settings**. For more information, see Section 2.1.8.10, “Performance parameters (Windows)”, on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value** and then enter the value.

3. Click **Next**.

5.12.2.5 Selecting the restore options

1. Under **Restore options,** do the following:

   a) To record all restored files in the Activity Log, select the **Detailed log** check box.

   b) To skip the pre and post restore processes, select the **Skip Pre/Post** check box. If this check box is clear, click **Pre/Post**. DS-Client will run a specified activity before and/or after a restore operation. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525.

2. Under **Microsoft Exchange database restore options**, do one of the following:

   - To automatically mount the database after the restore, select the **Mount database after restore** check box.
   - To automatically set the Microsoft Exchange Server’s allow restore to overwrite database parameter before restoring the database, select the **Force allow overwrite database** check box.

3. Under **Existing file options**, do one of the following:

   - To delete all the existing files in the restore directory, select **Delete**.
   - To retain all the existing files in the restore directory, select **Keep**.
   - To rename existing files till all restore items are successfully restored, select **Rename**.

4. Depending on the DAG configuration selected when performing the backup, under **DAG restore options**, select the restore option. The options are as follows:

   a) **Restore from active node backup** – If the backup is configured to back up active databases.

   b) **Restore from passive node backup** – If the backup is configured to back up passive databases.

5. Click **Next**.

5.12.2.6 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, under **Restore classification**, select the type of restore. The options are as follows:
   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.
3. Click **Finish**.

5.12.3 Performing a file restore

You can selectively restore individual files from a backup session. This is also known as a pure file restore and does not recreate the working database.

5.12.3.1 Selecting the restore method

1. Browse the backups tree and select the backup you want to restore.
2. On the **Restore** menu, click **Restore Now**.
3. Select **File Restore**.
4. Click **Next**.

5.12.3.2 Selecting the restore items

1. To restore an entire backup or folder, browse the tree and select the check box beside the backup or folder you want to restore.
2. To restore individual files, select the folder containing the required files, click **Show Files**, and then do the following:
   - To view details about the backed up file, select the file, and then click **File Info**.
   - To view archived files, click **Show Archived**.
3. To view the number of files selected and calculate the total amount of files selected, select the **Calculate amount** check box.
4. To exclude subdirectories, clear the **Include SubDirs** check box, as the default setting is to include sub-directories.
5. To search for files that match a certain criteria, in the **Filter** box, type the file pattern that you want to search for in the selected folder. For example, *.doc will search for all files with the doc file extension.
6. To narrow down your selection of items to restore, click **Advanced**, and then under **Show**, select which generation of the data you want to display. The options are as follows:
   - To restore the latest generation of all the files, select **Latest generation of all data**.
   - To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:
     a) Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.
     b) Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.
     c) Click **OK**.
7. Click **Next**.

5.12.3.3 Selecting the restore location

1. Beside the **Alternate location** box, click **[>>]**.
   a) In the **Select Alternate Server** dialog box, select the computer where you want to restore the data.
   b) To specify alternate network credentials, select the **Ask for Network Credentials** checkbox, and then click **Select**.
   c) In the **Enter Network Credentials** dialog box, enter the credentials to connect to the destination computer, and then click **OK**.
2. In the **Destination** cell, and select a destination folder for each item you want to restore.
3. In the **Truncate** box, you can increase the truncate level to shorten the common portion of the restore path, if the selected restore items contain a common path.
4. Click **Next**.

5.12.3.4 Selecting the performance options

IMPORTANT: These options are intended for large backups in high performance environments where the DS-Client can take advantage of the speed of the storage where the source data resides. Test different settings to determine the optimal value. Slower storage can result in performance issues if these values are not configured correctly.

---

1. Under **Maximum pending asynchronous I/O for a file**, configure the maximum number of I/O operations the DS-Client will use for each file during the restore process.
   - To use the default MaxPendingIOPerFile advanced configuration parameter setting, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value** and then enter the value.
2. Under **DS-System side read threads**, configure the number of files the DS-System can read simultaneously for the restore process.
   - To use the default MaxRestoreReadThreads advanced configuration parameter setting, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value** and then enter the value.

3. Click **Next**.

5.12.3.5 Selecting the restore options

1. Under **Permissions**, select a restore option for permissions. The options are as follows:
   - **Yes** – Restores the permissions for all the backed up files.
   - **Skip** – Skips the file security information of the backed up files. Newly created files and folders inherit the security settings of the parent folder.
   - **Only** – Restores the permissions for only the selected files and folders.
2. Under **Method**, select a method for the DS-Client to perform the restore. The options are as follows:
   - **Save** – Restores files to a temporary location first to prevent restored files from overwriting an existing file. If the file is restored successfully, the original file is overwritten with the temporary file.
   - **Use buffer** – Restores files to the DS-Client buffer first and then transfers the files to the restore destination. This method minimizes the duration for which the restore process occupies the destination server.
   - **Fast** – Uses a direct restore method by writing data as it is received.

   NOTE: If you select the Fast method, files in the destination location are overwritten upon receipt of the first byte of data.
3. To record all restored files in the Activity Log, select the **Detailed log** check box.
4. To skip the pre and post restore processes, select the **Skip Pre/Post** check box. If this check box is clear, click **Pre/Post**. DS-Client will run a specified activity before and/or after a restore operation. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525.
5. Click **Next**.

5.12.3.6 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, under **Restore classification**, select the type of restore. The options are as follows:
   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.
3. Click **Finish**.

5.12.4 Performing a granular restore

You can perform a granular restore at the individual item-level from a backed up Microsoft Exchange database. Before performing a granular restore, consider the following:

- Ensure the target Microsoft Exchange Server where you want to perform the granular restore has the DS-Recovery Tools installed and running. For more information, see the *Client Software Installation Guide*.
- Ensure the DS-Recovery Tools service account has access to the Microsoft Exchange Server where the items are going to be restored.

There are two steps to performing an item-level restore:

1. Restore the Microsoft Exchange database to the point-in-time that contains the items you want to restore.
2. Connect to the Microsoft Exchange database and select the individual items you want to restore.

NOTE: If you are restoring from a BLM Restorable Image or Disc/Tape media, you can perform only step 1 which will restore the database from the media. You must perform step 2 on the database restored in step 1.

5.12.4.1 Selecting a restore method

1. Browse the backups tree, select the backup, and then on the **Restore** menu, click **Restore Now**.
2. Select **Granular Restore**, and then select **Step 1. Database restore**.
3. Click **Next**.

5.12.4.2 Selecting the restore items

1. To restore an entire backup or folder, browse the tree and select the check box beside the backup or folder you want to restore.
2. To restore individual files, select the folder containing the required files, and then click **Show Files**. Under **File List**, do the following:
3. To view the number of files selected and calculate the total amount of files selected, under Options, select the Calculate amount check box.
4. To filter the list of files, in the **Filter box**, enter a filter using * as a wildcard, and then click **Show Files** to update the list of files.
5. To find a backed up file, click **Show Files**, and then do one of the following:
   - To view details about the backed up file, select the file, and then click **File Info**.
   - To view the details of the items you selected, click **Selection**.
   - To view a list of archived generations for a folder, do the following:
     a) In the **Database Tree**, select the folder, and then click **Show Files**.
     b) Under **Files**, click **Show Archived**.
   - To view the files that are part of the selected VSS component, click **VSS Component**.
6. To refine your selection of items to restore, click **Advanced**. Under **Show**, select which generation you want to display. The options are as follows:
   a) To restore the latest generation of all the files, select **Latest generation of all data**.
   b) To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:
      1. Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.
      2. Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.
   c) Click **OK**.

7. Click **Next**.

5.12.4.3 Selecting the restore location

1. Select the location to which you want to restore the backup. The options are as follows:
   - **Original location** – Data is restored to the original backup source location and existing files with the same name are overwritten. This is the default option.
   - **Alternate location** – Data is restored to a location other than the original backup source.

   NOTE: When restoring to an alternate location, the security of restored items in the destination location might not resemble the security of those items during backup.

2. If you selected **Original location**, then do the following:
   a) In the **Restore To** cell, click **[>>]**, and then select the folder to which you want to restore.
   b) In the **Restore Logs to** cell, click **[>>]**, and then select the folder to which you want to restore the logs.
3. If you selected **Alternate location**, then do the following:
   a) Beside the **Alternate location** box, click **[>>]**.
   b) In the **Select Alternate Server** dialog box, select the computer where you want to restore the data.
   c) To specify alternate network credentials, select the **Ask for Network Credentials** checkbox, and then click **Select**.
   d) In the **Enter Network Credentials** dialog box, enter the credentials to connect to the destination computer, and then click **OK**.
4. Click **Next**.

5.12.4.4 Selecting the performance options

IMPORTANT: These options are intended for large backups in high performance environments where the DS-Client can take advantage of the speed of the storage where the source data resides. Test different settings to determine the optimal value. Slower storage can result in performance issues if these values are not configured correctly.

1. Under **Maximum pending asynchronous I/O for a file**, configure the maximum number of I/O operations the DS-Client will use for each file during the restore process.
   - To use the default MaxPendingIOPerFile advanced configuration parameter setting, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value** and then enter the value.
2. Under **DS-System side read threads**, configure the number of files the DS-System can read simultaneously for the restore process.
   - To use the default MaxRestoreReadThreads advanced configuration parameter setting, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value** and then enter the value.
3. Click **Next**.

5.12.4.5 Selecting the restore options

1. To record all restored files in the Activity Log, select the **Detailed log** check box.
2. To skip the pre and post restore processes, select the **Skip Pre/Post** check box. If this check box is clear, click **Pre/Post**. DS-Client will run a specified activity before and/or after a restore operation. For more information, see Section 5.25, "Configuring Pre/Post processes (Windows)", on page 525.
3. To send a notification when the database restore is complete, select the **Send E-Mail notification when database restore finishes** check box, and in the **E-Mail Address** field, type the email address to which you want to send the notification.
4. Click **Next**.

5.12.4.6 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, under **Restore classification**, select the type of restore. The options are as follows:
   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.
3. Click **Finish**.

NOTE: After the database has been restored to a Microsoft Exchange Server, you can proceed to step 2 - restoring at Item-Level.

5.12.4.7 Performing an items restore

1. Browse the backups tree, select the same backup, and then on the **Restore** menu, click **Restore Now**.
2. Select **Granular Restore**, and then select **Step 2. Items Restore**.
3. Click **Next**.

5.12.4.8 Selecting the database restore location

1. Select the location where you want to restoreSelect the location to which you want to restore the backup. The options are as follows:
   - **Original location** – Data is restored to the original backup source location and existing files with the same name are overwritten. This is the default.
   - **Alternate location** – Data is restored to a location other than the original backup source.
2. If you selected **Alternate location**, then do the following:

a) Beside the **Alternate location** box, click **[>>]**.

b) In the **Mailbox Server** dialog box, select the server to which you want to restore.

c) To specify alternate network credentials, select the **Ask for Network Credentials** checkbox, and then click **Select**.

d) In the **Enter Network Credentials** dialog box, enter the credentials to connect to the destination computer, and then click **OK**.

3. Under **Client Access Server** do one of the following:

   - Select the **Client Access Server and Mailbox Server are the same** check box, if the Mailbox Server has the role of the Client Access Server.

     DS-Recovery Tools must be running on the Client Access Server you select. If it is not running on the same machine as the Microsoft Exchange Mailbox Server, specify an alternate Client Access Server on which DS-Recovery Tools (DS-MLR) service is running. for more information, see the *Client Software Installation Guide*.

   - If the Client Access Server is on a different machine, then do the following:

     1. Under **Client Access Server**, click **[>>]**.
     2. In the **Client Access Server** dialog box, select the required server.
     3. To specify alternate network credentials, select the **Ask for Network Credentials** checkbox, and then click **Select**.
     4. In the **Enter Network Credentials** dialog box, enter the credentials to connect to the destination computer.
     5. Click **OK**.

4. Click **Next**.

5.12.4.9 Verifying the prerequisites

Wait until DS-Client completes the compatibility check for the selected restore location. You can only continue when all prerequisite checks have passed.

- To repeat the verification of the prerequisites, click **Rerun**.
- To view the details of a rule that has not passed the verification, select the rule, and then click **Details**.
- Click **Next**.

5.12.4.10 Selecting the EDB file path and log folder path

The **Mailbox Server Name** displays the selected target Microsoft Exchange Mailbox Server to which the items will be restored.

1. In the **EDB File** box, select the location of the Exchange Database File you restored in step 1 of granular restore.
2. In the **Log Folder** box, click **[>>]**, and select a log folder under the parent directory that has the same path as the EDB file.

NOTE: This field is automatically filled in if there is a corresponding log folder under the same parent directory as the path to the EDB file.

---

3. To use a previously generated recovery database, select the **Reuse existing recovery database** check box. Otherwise, in the next stage, DS-Client will prepare the EDB file into a recovery database.
4. To validate and repair the Microsoft Exchange database, select the **Validate and repair the Exchange database and log files against corruption** check box.
5. Click **Next**.

5.12.4.11 Mounting the recovery database

DS-Client prepares the selected Microsoft Exchange database file for Item-Level restore. You can proceed to the next stage only when all checks have passed.

- To repeat the verification of the prerequisites, click **Rerun**.
- To view the details of a rule that has not passed the verification, select the rule, and then click **Details**.
- Click **Next**.

IMPORTANT: Ensure that the required databases are mounted.

5.12.4.12 Selecting the emails to restore

1. To restore an entire mailbox, click **Mailbox**, and then do the following:
   a) Under **Source mailbox**, select the mailbox you want to restore.

   NOTE: You can select only one mailbox per pass of the wizard.

   b) Under **Source Folder**, select the folders in the selected mailbox you want to restore.
   c) Click **Next**.
2. Select the target mailbox. The options are as follows:
   - To restore the mailbox to the original mailbox location, select **Original mailbox**.
   - To restore the mailbox to different location, select **Alternate mailbox**.
3. If you selected **Alternate mailbox**, click **[>>]**, and then select the mailbox.
4. To select the target email folder, do one of the following:
   - To restore emails to the original email folder location, select **Original folder**.
   - To restore emails to a different older, select **Alternate folder**.
5. If you selected **Alternate folder**, do the following:
   a) In the **Top folder** box, select a folder to which you want to restore the emails.
   b) In the **Sub-folder** box, type the name of a new target folder that will be created under the selected top folder.
   c) Click **Finish**.
6. To restore specific emails, click **E-Mails**.
7. Do the following:
   a) In the **Subject** box, type the search text string that is in the subject line of the email.
   b) Beside **Attachment**, select an option for the attachment. The options are as follows:
      - **Yes** – Search for emails with an attachment.
      - **No** – Search for emails without an attachment.
      - **Both** – Ignore the search and show either.

c) In the **Recipient(s)** box, type the email addresses of the recipients by which you want to search.

d) In the **Sender(s)** box, type the email addresses of the senders by which you want to search.

e) In the **Body** box, type the text string in the body of the email by which you want to search.

f) In the **From Time** box, specify the date and time from which you want to search emails. No emails before this date and time will be displayed.

g) In the **To Time** box, specify the date and time till which you want to search emails. No emails after this date and time will be displayed.

h) Click **Next**.

8. Select the mailboxes that you want to search for the emails based on the criteria specified.

   a) Under **Available Mailboxes**, select a mailbox, and then click **Add**.

   b) Click **Next**.

9. Select the emails you want to restore, and then click **Add**. Repeat till you have added all the emails you want to restore.

   - To view the details of an email, select the email, and then click **Details**.
   - To remove an email from the list of selected emails for restore, select the email, and then click **Remove**.
   - Click **Next**.

10. Do the following:

    a) Under **Target Mailbox**, do one of the following:

       - To restore the selected mailbox to the original location, select **Original mailbox**.
       - To restore the selected mailbox to another location, select **Alternate mailbox**.

    b) If you selected **Alternate mailbox**, click **[>>]** beside **Alternate mailbox**, and then select the mailbox to which you want to restore.

    c) Under **Target E-Mail Folder**, do one of the following:

       - To restore the selected emails to the original location, select **Original folder**.
       - To restore the selected emails to another location, select **Alternate folder**.

11. If you selected **Alternate folder**, do the following:

a) In the **Top folder** box, select a folder to which you want to restore the emails.

b) In the **Sub-folder** box, type the name of a new target folder that will be created under the selected top folder.

c) Click **Finish**.

12. Select a restore option. The options are as follows:

- **Detailed log** – Records all files that are restored. You can view them in the activity log.
- **Remove recovery database after restore is finished successfully** – If the restore is completed successfully, the recovery database used for the granular restore is deleted.
- **Delete database file and logs after restore is finished successfully** – If the restore is completed successfully, the database and log files used for the granular restore are deleted.

13. Click **Finish**.

5.12.5 Performing a file restore to recovery database (RDB)

A direct VSS restore to a recovery database (RDB) is not supported. However, you can use the File Restore method to restore the backup files and then manually load those files to the recovery database. Only one recovery database can be mounted at a time.

1. Perform a file restore of the Exchange database files. For each database you want to restore, select the entire backup folder (including all log files) and restore to the original or alternate location, as required.
2. Create the recovery database and specify the restored database name.
3. Before mounting the database, run the Eseutil tool in the database folder, which will reset the database to a clean shutdown state. For example:

```
eseutil  /r e00 /i /d
```

4. Mount the recovery database.

5.13 Microsoft Hyper-V Server (VSS-aware) backups (Windows)

You can back up and restore data on a Microsoft Hyper-V Server using the Microsoft VSS (Volume Shadow Copy Service) component.

Each Microsoft Hyper-V virtual machine is presented as a component by the VSS writer. A component must be restored with all its contents, based on the rules specified in its metadata. For more information, see Section 5.3.7, “Restoring VSS-aware backup components”, on page 133.

NOTE: You can back up a Microsoft Hyper-V Server in standalone or cluster configuration, but you must specify the type when you create the backup.

When performing a backup of a Microsoft Hyper-V Server (VSS-aware) backup, consider the following:

- The backup unit is the Microsoft Hyper-V Server virtual machine (not individual files within the virtual machine). A Microsoft Hyper-V Server virtual machine is a group of files governed with strong data integration.
- The backup mechanism is called the Saved State method, where the virtual machine is put into a saved state during the snapshot process. Snapshots are taken of the appropriate volumes, and the virtual machine is returned to the previous state after the snapshot process is done.
- The GUID of the Microsoft Hyper-V Server virtual machine is the identifier for the virtual machine and is considered the name of the virtual machine. The virtual machine name might not be unique for all virtual machines in a host.
- Microsoft Hyper-V Server WMI APIs allow you to search for the virtual machines on a host server you want to back up. You can also select all virtual machines to be backed up.
- VSS provides a consistent interface that allows for an online backup of a Microsoft Hyper-V Server virtual machine.
- VSS-related metadata is saved with the backup data to provide the rules for data integration in each backed up virtual machine.
- Master, delta, and library files are supported for this type of backup.

5.13.1 General requirements

- The Hyper-V Virtual Machine Management service must be running on the target server.

- For application consistent checkpoints, ensure the Hyper-V Integration Services is installed on the guest operating system of the virtual machine.

IMPORTANT: When restoring virtual machines, ensure that the same virtual machine (based on GUID) does not exist on any other node that is part of the same Microsoft Hyper-V Server cluster.

5.13.2 Backup requirements

When performing a backup of a Microsoft Hyper-V Server in a cluster configuration, consider the following:

- You must add the IP address and computer name of all the nodes in the Microsoft Hyper-V server cluster configuration to the hosts file on the DS-Client computer, which is located in C:\Windows\system32\drivers\etc\hosts.
- You must create the backup by selecting Microsoft Cluster Hyper-V.
- You must specify the computer using the IP address of the cluster virtual node. This is configured on the Microsoft Hyper-V Server cluster. If you can connect to the computer, there is an additional folder level named <HAVMs> that contains the high availability virtual machines you can select for backup.

When performing an incremental backup of a Microsoft Hyper-V Server, consider the following:

- You must apply the latest Microsoft hotfixes to each target Microsoft Hyper-V Server.
- You must configure Microsoft incremental backups on the Microsoft Hyper-V Server host. This is normally done using PowerShell. The Microsoft incremental backup setting must be applied as a property to each virtual machine selected for backup. If any virtual machine in the backup is not configured with this setting, the entire session will be backed up with the Full dump: Always method.

5.13.3 Creating a Microsoft Hyper-V Server (VSS-aware) backup

You can create a Microsoft Hyper-V Server (VSS-aware) backup in a standalone or cluster configuration.

NOTE: You must know the type of Microsoft Hyper-V Server configuration before creating the backup. You cannot change the setting after the backup has been created.

5.13.3.1 Selecting the type of backup

1. On the **Sets** menu, click **New Backup Set**.
2. Select **VSS-aware Backup Set** and then click **Next**.

5.13.3.2 Selecting the VSS-aware backup type

1. Select one of the following backup type depending on the configuration of the target backup server:
   - **Microsoft Hyper-V** — Performs an online backup of a Microsoft Hyper-V Server virtual machine using the VSS component of the target computer.
   - **Microsoft Cluster Hyper-V** — Performs an online backup of a Microsoft Hyper-V Server cluster using the VSS component of the target virtual node.
2. Click **Next**.

5.13.3.3 Selecting the backup source

IMPORTANT: A Microsoft Cluster Hyper-V Server backup requires you to select the Cluster Virtual Node by its IP address.

a) In the **Path** box, type the IP address or DNS name of the source computer with the VSS component.

b) To provide the logon credentials for the selected source computer, select the **Ask for Network Credentials** check box. You will be prompted to enter a valid user name and password for the selected computer.

c) Click **OK**.

IMPORTANT: For a VSS aware backup, remote UAC is enabled by default. The local administrator account must have access to the admin$ share on the source machine.

3. Click **Next**.

5.13.3.4 Selecting the backup items

1. Select the VSS component you want to back up, and then click **Add**.
   - To prevent an item from being backed up, select the item, and then click **Exclude**.

     NOTE: You can exclude a VSS component or an item only when the parent folder has already been added.

   - To remove a selected item, select the item under **Backup Items Selected**, and then click **Remove**.
2. Click **Next**.

5.13.3.5 Selecting the backup item options

1. To configure the number of maximum generations of the selected backup item that will be stored online, double click in the **Max gen** cell, and then enter the new value.
2. To back up the permissions, select the **Back up permissions** check box.
3. Click **Next**.

5.13.3.6 Selecting the backup options

1. Under **Backup options**, configure the options you want to apply to the backup. The options are as follows:
   - **Detailed log** – Records all files that are backed up in the Activity Log.

     NOTE: For more information, see Section 8.1, “Viewing the Activity Log”, on page 578.

   - **Initial backup** – Uses the Initial Backup feature for the first backup. To configure the initial backup path, click **[>>]**. For more information, see Section 11.1.1, “Configuring the initial backup path”, on page 618.
   - **Stop on errors** – Enter the number of errors that must occur before a back up is stopped.
   - **VSS validation** – Specifies the type of VSS validation that will be applied prior to performing the backup. The options are as follows:
     - **Disable** – VSS validation is not performed.
     - **Enable** – VSS validation is performed.

- **Use DS-Client's settings** – VSS validation is performed using the DS-Client settings.

- **Compression type** – Specifies the type of compression that will be applied to the backup. The options are as follows:
  - **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good default compression when the network is not the bottleneck.
  - **ZLIB (Global, Low, Medium, and High)** – Normally produces better compression than LZOP, but will take more time to compress. This is a good default compression when the bottleneck is the network. ZLIB Low corresponds to a value of 3, ZLIB Medium = 6, and ZLIB High = 9.
  - **None** – Disables compression for the backup.

2. Under **Additional backup options**, to enable a file-level restore, select the **Use FLR** check box.
3. Under **Hyper-V backup policy**, do the following:

   a) In the **Full dump** box, select a method for the full dump. A full dump is required (other than first time) when a virtual machine has been backed up by another backup or manually from the Hyper-V tools.The options are as follows:
   - **Always** (Default) — Performs a full dump (VSS snapshot) of each virtual machine.
   - **Plus Incremental** — Performs a full dump (VSS snapshot) of the virtual machine on first backup followed by incremental backups until another full backup is required.

   NOTE: For a Full dump Plus Incremental backup, ensure the required virtual machine is enabled for an incremental backup with the appropriate PowerShell script.

   ---

   b) To prevent a full dump from being performed during the selected time period, select the **Do not start full dump on** check box, select the day, and then specify the time period.

   IMPORTANT: You must perform Full dumps at a regular frequency to protect the integrity of the virtual machine backup. By default, DS-Client allows a full backup to be skipped a maximum of 120 consecutive times. This number is configurable using the **MaxNonFullDumps** advanced parameter.

   ---

   c) To force a full backup to be performed at an interval, select the **Full every** check box, and then specify the values for the interval.

d) To force a full backup to be performed on a specific day of the week, select the **Full every week on** check box, select the day, and then specify the time after which the full backup can be performed.

e) To force full backup to be performed on a regular monthly interval, select the **Full every month on** check box, select the day, and then specify the time after which the full backup can be performed.

NOTE: A set number of consecutive differential backups are performed, unless over-ruled with the Do not start full dump option. This uses the same value set for the MasterGenerations advanced parameter (this parameter is also used for another purpose). For more information, see Section 2.1.8, “Configuring the advanced settings”, on page 37.

4. To specify a command to run before (Pre) and/or after (Post) the execution of the backup, click **Pre/Post**. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525.

5. Click **Next**.

5.13.3.7 Specifying backup performance options

IMPORTANT: These options are intended for high performance environments where the DS-Client can take advantage of the speed of the storage where the source data resides. Test different settings to determine the optimal value. Slower storage can result in performance issues if the values are not properly configured.

1. Under **Maximum pending asynchronous I/O for a file**, configure the maximum I/O operations the DS-Client will use for each file from the backup.

   - To use the default **MaxPendingIOPerFile** advanced configuration parameter, click **Use DS-Client’s settings**. For more information, see Section 2.1.8.10, “Performance parameters (Windows)”, on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value**, and then enter the value.

   NOTE: This setting is for storage devices that support better parallel disk I/O, such as NAS devices. The optimal setting for this value depends on the storage device and network speed. Increasing this value can significantly increase the backup speed. If your storage device does not support higher parallel disk I/O, use the default value, otherwise the performance can be significantly degraded.

2. Under **Read buffer size for backup**, configure the internal buffer size for reading a file during the backup process.

- To use the default **FileReadBufferSize** advanced configuration parameter, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.

3. Under **DS-System side read threads**, configure the number of files the DS-System can read simultaneously for the restore process.

   - To use the default MaxRestoreReadThreads advanced configuration parameter setting, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value** and then enter the value.

   IMPORTANT: To achieve optimum backup performance, the DS-Client read buffer size might need to be different, depending on the combination of the target storage device, target operating system, and any mid-ware involved between the storage and the operating system.

4. Click **Next**.

5.13.3.8 Selecting the notification options

1. To configure a notification, do one of the following:

   - To add a notification, click **Add.**
   - To modify a notification, select the notification, and then click **Modify.**

   NOTE: To delete a notification, select the notification, and then click **Delete**.

2. To send an email notification, select **E-Mail**. and then do the following:

   a) To send the email notification to the DS-Client administrator, select **Administrator**.

   b) To send an email to another recipient, select **Other**, and then specify the recipients email address.

   c) To send detailed backup information, select the **Detailed notification** check box.

   d) To include a detailed file-level backup log as an attachment, select the **Attach detail log** check box.

e) To send the email notification in HTML format, select the **Send E-Mail using HTML format** check box.

NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

---

f) Click **OK**.

3. To send a pager notification, select **Pager**. The notification will be sent to the pager account configured for the DS-Client.

NOTE: The pager option is available only if the DS-Client has been configured for pager notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

---

4. To send a broadcast notification, select **Broadcast**. Select the server containing the messenger service to which you want to send the message and click **OK**.

NOTE: Broadcast notifications to domains or workgroups are limited to 128 characters.

---

5. To send an event notification, select **Event**. Select the server on which you want the notification to be recorded in the Event Log and click **OK**.
6. In the **Completion** box, specify under what conditions a notification will be sent, and click **OK**. The options are as follows:
   - **All** – Notification will be sent under all conditions.
   - **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
   - **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.
   - **Completed with errors** – Notification will be sent if an activity is completed with at least one error event.
   - **Incomplete** – Notification will be sent if an activity is not completed successfully.
7. Click **Next**.

5.13.3.9 Assigning a retention rule

1. To assign a retention rule to the backup, do one of the following:
   - If you don't want to assign a retention rule, select **No retention rule**.
   - To assign a retention rule, select **Use a specific retention rule**, and then select the retention rule.

NOTE: To create or edit a retention rule, click **[...]**. For more information, see Section 4.1, "Configuring a retention rule", on page 98.

---

2. Click **Next**.

5.13.3.10 Assigning a schedule

1. To assign a schedule to the backup, do one of the following:
   - If you don't want to assign a schedule, select **Not scheduled**.
   - To assign a schedule, select **Scheduled.** In the **Available schedules** box, select an existing schedule.

NOTE: To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, "Configuring a schedule", on page 90.

---

2. Click **Next**.

5.13.3.11 Naming the backup

1. In the **Set name** box, type a name for the backup.
2. In the **Set type** box, select the type of backup you want to create. The list of available backup types depends on the configuration of your DS-Client.
   - Online
   - Self-contained
   - Local-only
   - Instant recovery
   - Statistical

NOTE: For more information, see Section 5.1, "Backup types", on page 106.

---

3. If you selected **Online**, do the following:

   a) To send a copy of the oldest generation of the file that is about to be overwritten from the DS-System to the BLM Archiver, select the **BLM (Infinite Generations)** check box.

   NOTE: The Backup Lifecycle Management tool must be enabled for the DS-Client.

4. If you selected **Self-Contained**, beside the **Local Storage Path** box, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

   NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

5. If you selected **Local Only**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

   NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

6. If you selected **Instant Recovery**, the **Save in instant recovery vault** option is selected by default.
7. If you selected **Statistical**, and want to emulate an actual backup transfer process, select the **Calculate transmit amount** check box. During the backup, specified backup files will be read from their source and processed for compression and encryption.
8. If the multitenant feature is enabled and configured, in the **Customer** list, you can select the customer to which you want to assign the backup. For more information, see Section 11.5, “Multitenant DS-Clients”, on page 634.
9. Click **Finish**.

5.13.4 Performing a VSS restore

You can perform a VSS restore using the VSS writer to restore the entire virtual machine. All files on the virtual machine are provided based on the saved metadata.

5.13.4.1 Selecting a restore method

1. Browse the backups tree and select the backup you want to restore.
2. On the **Restore** menu, click **Restore Now**.
3. Select **VSS Restore.**
4. Click **Next**.

5.13.4.2 Selecting the restore items

1. To restore an entire backup or folder, browse the tree and select the backup or folder you want to restore.
2. To restore individual files, select the folder containing the required file, click **Show Files**, and then do the following:
   - To view details about the backed up file, select the file, and then click **File Info**.
   - To view archived files, click **Show Archived**.
3. To view the number of files selected and calculate the total amount of files selected, select the **Calculate amount** check box.
4. To exclude subdirectories, clear the **Include SubDirs** check box, as the default setting is to include sub-directories.
5. To search for files that match a certain criteria, in the **Filter** box, type the file pattern that you want to search for in the selected folder. For example, *.doc will search for all files with the doc file extension.
6. To view the files that are part of the selected VSS component, click **VSS Component**.
7. To refine your selection of items to restore, click **Advanced**. Under **Show**, select which generation you want to display. The options are as follows:
   a) To restore the latest generation of all the files, select **Latest generation of all data**.
   b) To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:

1. Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.
2. Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.
3. Click **OK**.

8. Click **Next**.

5.13.4.3 Selecting the restore location

1. Select the location to which you want to restore the backup. The options are as follows:
   - **Original location** – Data is restored to the original backup source location and existing files with the same name are overwritten. This is the default option.
   - **Alternate location** – Data is restored to a location other than the original backup source.

   NOTE: When restoring to an alternate location, the security of restored items in the destination location might not resemble the security of those items during backup.

2. If you selected **Alternate location**, then do the following:
   a) Beside the **Alternate location** box, click **[>>]**.
   b) In the **Select Alternate Server** dialog box, select the computer where you want to restore the data.
   c) To specify alternate network credentials, select the **Ask for Network Credentials** checkbox, and then click **Select**.
   d) In the **Enter Network Credentials** dialog box, enter the credentials to connect to the destination computer, and then click **OK**.
   e) To rename the individual components being restored, click **Rename component**.
   f) In the **Rename Component** dialog box, do the following:

1. Double click in the **Target Path** column and edit the name or path for the component.
2. To load mapping contents from a saved XML file, click **Load XML**.

NOTE: A mapping is loaded only if the logical path and the source component columns from the XML file exactly match with those displayed in the list.

---

3. To save the contents from the current source target mapping list to an XML file, click **Save XML**.
4. Click **OK**.

3. Click **Next**.

5.13.4.4 Selecting the performance options

IMPORTANT: These options are intended for large backups in high performance environments where the DS-Client can take advantage of the speed of the storage where the source data resides. Test different settings to determine the optimal value. Slower storage can result in performance issues if these values are not configured correctly.

---

1. Under **Maximum pending asynchronous I/O for a file**, configure the maximum number of I/O operations the DS-Client will use for each file during the restore process.
   - To use the default MaxPendingIOPerFile advanced configuration parameter setting, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value** and then enter the value.
2. Under **DS-System side read threads**, configure the number of files the DS-System can read simultaneously for the restore process.
   - To use the default MaxRestoreReadThreads advanced configuration parameter setting, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value** and then enter the value.
3. Click **Next**.

5.13.4.5 Selecting the restore options

1. Under **Restore options,** do the following:

   a) To record all restored files in the Activity Log, select the **Detailed log** check box.

   b) To skip the pre and post restore processes, select the **Skip Pre/Post** check box. If this check box is clear, click **Pre/Post**. DS-Client will run a specified activity before and/or after a restore operation. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525.

2. Click **Next**.

5.13.4.6 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, under **Restore classification**, select the type of restore. The options are as follows:

   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.

3. Click **Finish**.

5.13.5 Performing a file restore

NOTE: This option is useful when VM-level restore is not possible or the files are restored for other purposes other than as part of a virtual machine.+

If the ownership of a user's backup have been assigned to you and you want to restore files with ACL, consider the following:

- DS-User will check whether you have access rights to Take Ownership and Change Permissions of the restore file.
- If you do not have access rights, you will not be able to restore the ACL. You must choose Skip Permissions Restore to restore the file.
- If you have the access rights, but the file ownership is not yours, the file will be restored without ownership, and a corresponding error message will appear in the event log, describing the security error.

5.13.5.1 Selecting the restore method

1. Browse the backups tree and select the backup you want to restore.
2. On the **Restore** menu, click **Restore Now**.
3. Select **File Restore.**
4. Click **Next**.

5.13.5.2 Selecting the restore items

1. To restore an entire backup or folder, browse the tree and select the backup or folder you want to restore.
2. To restore individual files, select the folder containing the required files, click **Show Files**, and then do the following:
   - To view details about the backed up file, select the file, and then click **File Info**.
   - To view archived files, click **Show Archived**.
3. To view the number of files selected and calculate the total amount of files selected, select the **Calculate amount** check box.
4. To exclude subdirectories, clear the **Include SubDirs** check box, as the default setting is to include sub-directories.
5. To search for files that match a certain criteria, in the **Filter** box, type the file pattern that you want to search for in the selected folder. For example, *.doc will search for all files with the doc file extension.
6. To search for a specific backed up file, click **Find File**.
7. To refine your selection of items to restore, click **Advanced**. Under **Show**, select which generation you want to display. The options are as follows:
   a) To restore the latest generation of all the files, select **Latest generation of all data**.
   b) To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:
      1. Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.
      2. Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.
   c) Click **OK**.
8. Click **Next**.

5.13.5.3 Selecting the restore location

NOTE: Before restoring to an alternate location, ensure there is no virtual machine with the same GUID on the target machine. If there is a virtual machine with the same GUID, the existing virtual machine will be overwritten.

1. Select the location to which you want to restore the backup. The options are as follows:
   - **Original location** – Data is restored to the original backup source location and existing files with the same name are overwritten. This is the default option.
   - **Alternate location** – Data is restored to a location other than the original backup source.

     NOTE: When restoring to an alternate location, the security of restored items in the destination location might not resemble the security of those items during backup.

2. If you selected **Alternate location**, then do the following:
   a) Beside the **Alternate location** box, click **[>>]**.
   b) In the **Select Alternate Server** dialog box, select the computer where you want to restore the data.
   c) To specify alternate network credentials, select the **Ask for Network Credentials** checkbox, and then click **Select**.
   d) In the **Enter Network Credentials** dialog box, enter the credentials to connect to the destination computer, and then click **OK**.
3. For each item selected for restore, do the following:
   a) In the **Destination** cell, select the restore destination.
   b) In the **Restore To** cell, click **[>>]**, and select the folder to which you want to restore.
4. In the **Truncate** box, you can increase the truncate level to shorten the common portion of the restore path, if the selected restore items contain a common path.
5. Click **Next**.

5.13.5.4 Selecting the performance options

IMPORTANT: These options are intended for large backups in high performance environments where the DS-Client can take advantage of the speed of the storage where the source data resides. Test different settings to determine the optimal value. Slower storage can result in performance issues if these values are not configured correctly.

1. Under **Maximum pending asynchronous I/O for a file**, configure the maximum number of I/O operations the DS-Client will use for each file during the restore process.
   - To use the default MaxPendingIOPerFile advanced configuration parameter setting, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value** and then enter the value.
2. Under **DS-System side read threads**, configure the number of files the DS-System can read simultaneously for the restore process.
   - To use the default MaxRestoreReadThreads advanced configuration parameter setting, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value** and then enter the value.
3. Click **Next**.

5.13.5.5 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, under **Restore classification**, select the type of restore. The options are as follows:
   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.

3. Click **Finish**.

5.13.6 Performing a file-level restore

If the backup was configured with the Use FLR option, you can perform a file-level restore of the data from the Microsoft Hyper-V Server virtual disk.

5.13.6.1 Selecting the restore method

1. Browse the backups tree and select the backup you want to restore.
2. On the **Restore** menu, click **Restore Now**.
3. Select **File-Level Restore.**
4. Click **Next**.

5.13.6.2 Selecting the restore items

1. To restore an entire backup or folder, browse the tree and select the backup or folder you want to restore.
2. To restore individual files, select the folder containing the required files, click **Show Files**, and then do the following:
   - To view details about the backed up file, select the file, and then click **File Info**.
   - To view archived files, click **Show Archived**.
3. To view the number of files selected and calculate the total amount of files selected, select the **Calculate amount** check box.
4. To exclude subdirectories, clear the **Include SubDirs** check box, as the default setting is to include sub-directories.
5. To search for files that match a certain criteria, in the **Filter** box, type the file pattern that you want to search for in the selected folder. For example, *.doc will search for all files with the doc file extension.
6. To refine your selection of items to restore, click **Advanced**. Under **Show**, select which generation you want to display. The options are as follows:
   a) To restore the latest generation of all the files, select **Latest generation of all data**.
   b) To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:

1. Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.
2. Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.

c) Click **OK**.

7. Click **Next**.

5.13.6.3 Selecting the restore location

1. Select **Alternate location**, and then do the following:

NOTE: When restoring to an alternate location, the security of restored items in the destination location might not resemble the security of those items during backup.

---

a) Beside the **Alternate location** box, click **[>>]**.

b) In the **Select Alternate Server** dialog box, select the computer where you want to restore the data.

c) To specify alternate network credentials, select the **Ask for Network Credentials** checkbox, and then click **Select**.

d) In the **Enter Network Credentials** dialog box, enter the credentials to connect to the destination computer, and then click **OK**.

2. For each item selected for restore, do the following:

a) In the **Destination** cell, select the restore destination.

b) In the **Restore To** cell, click **[>>]**, and select the folder to which you want to restore.

3. In the **Truncate** box, you can increase the truncate level to shorten the common portion of the restore path, if the selected restore items contain a common path.

NOTE: If the entire path is truncated, the alternate location directory will inherit the security of the truncated parent directory.

---

4. Click **Next**.

5.13.6.4 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, under **Restore classification**, select the type of restore. The options are as follows:
   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.
3. Click **Finish**.

5.14 Microsoft SharePoint Server (Classic) backups (Windows)

You can back up and restore data at the item-level from a Microsoft SharePoint Server in a standalone or farm configuration.

Before working with Microsoft SharePoint Server (Classic) backups, ensure the following requirements are met.

- The DS-Recovery Tools feature must be enabled for the DS-Client in the DS-System.
- You must install the DS-Recovery Tools service on the Microsoft SharePoint Server computer. For more information, see the *Client Software Installation Guide*.

There are two configuration files in the DS-Recovery Tools installation directory:

- **dsrcvtools.cfg** — Main configuration file containing the path to the log configuration file and sharepoint.dll.
- **logconf.cfg** — Configuration file for logging. By default, debug logging is disabled.

NOTE: Configuring the DS-Recovery Tools service to dump a debug log will create a large text file that could impact performance.

5.14.1 Creating a Microsoft SharePoint Server (Classic) backup

You can create a Microsoft SharePoint Server (Classic) backup.

5.14.1.1 Selecting the type of backup

1. On the **Sets** menu, click **New Backup Set**.
2. Select **Microsoft SharePoint Server**, and then click **Next**.

5.14.1.2 Selecting the backup source

1. Select the server you want to back up or type the IP address of the server you want to back up in the **Path** box.
2. To provide alternate network credentials, select the **Ask for Network Credentials** check box. You will be prompted to enter a valid user name and password for the selected computer.

NOTE: By default, DS-Client uses the current user's logon credentials to connect to the selected computer.

---

3. Click **Next**.

5.14.1.3 Selecting the share and path for the database dump

1. Select a location to dump the database on the local computer (the backup target machine).
2. Click **Next**.

5.14.1.4 Selecting the backup items

1. To add an item, select the item, and then click **Add**.
2. To add specific files from a directory, select the directory from which you want to add the files, and then click **Files**. Select the file(s) that you want to add, and then click **Add**.
3. To remove an item from the **Backup Items Selected** list, select the item, and then click **Remove**.
4. Click **Next**.

5.14.1.5 Selecting the backup item options

1. To configure the maximum generations for a backup item that will be stored online, double click the **Max Gen** cell, and then enter the value.
2. Click **Next**.

5.14.1.6 Selecting the backup options

1. Configure the options for the backup. The options are as follows:

- **Use buffer** – Copies files to the DS-Client buffer to free up the backup source as fast as possible. The DS-Client then sends the files from the DS-Client buffer to the DS-System. For more information, see Section 5.2.7, “Performance”, on page 113.
  - **Detailed log** – Records all files that are backed up in the Activity Log. For more information, see Section 8.1, “Viewing the Activity Log”, on page 578.
  - **Initial backup** – Uses the Initial Backup feature for the first backup. To configure the initial backup path, click **[>>]**. For more information, see Section 11.1.1, “Configuring the initial backup path”, on page 618.
  - **Stop on errors** – Stops a backup process when the number of errors reaches the specified value. A value of 0 means the DS-Client does not stop a backup process regardless of the number of errors.

    NOTE: You can configure the default setting using the **MaxErrors** advanced configuration parameter. For more information, see Section 2.1.8.6, “Miscellaneous parameters (Windows)”, on page 42.

  - **PreScan** – Scans all files in the backup prior to performing the backup to display an estimated completion time for the backup.
  - **Compression type** – Specifies the type of compression that will be applied to the backup. The options are as follows:
    - **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good default compression when the network is not the bottleneck.
    - **ZLIB (Global, Low, Medium, and High)** – Normally produces better compression than LZOP, but will take more time to compress. This is a good default compression when the bottleneck is the network. ZLIB Low corresponds to a value of 3, ZLIB Medium = 6, and ZLIB High = 9.
    - **None** – Disables compression for the backup.

2. To specify a command to run before (Pre) and/or after (Post) the execution of the backup, click **Pre/Post**. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525.

3. Click **Next**.

5.14.1.7 Selecting the notification options

1. To configure a notification, do one of the following:
   - To add a notification, click **Add.**
   - To modify a notification, select the notification, and then click **Modify.**

   NOTE: To delete a notification, select the notification, and then click **Delete**.

2. To send an email notification, select **E-Mail**. and then do the following:
   a) To send the email notification to the DS-Client administrator, select **Administrator**.
   b) To send an email to another recipient, select **Other**, and then specify the recipients email address.
   c) To send detailed backup information, select the **Detailed notification** check box.
   d) To include a detailed file-level backup log as an attachment, select the **Attach detail log** check box.
   e) To send the email notification in HTML format, select the **Send E-Mail using HTML format** check box.

   NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

   f) Click **OK**.
3. To send a pager notification, select **Pager**. The notification will be sent to the pager account configured for the DS-Client.

   NOTE: The pager option is available only if the DS-Client has been configured for pager notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

4. To send a broadcast notification, select **Broadcast**. Select the server containing the messenger service to which you want to send the message and click **OK**.

NOTE: Broadcast notifications to domains or workgroups are limited to 128 characters.

---

5. To send an event notification, elect **Event**. Select the server on which you want the notification to be recorded in the Event Log.
6. In the **Completion** box, specify under what conditions a notification will be sent, and click **OK**. The options are as follows:
   - **All** – Notification will be sent under all conditions.
   - **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
   - **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.
   - **Completed with errors** – Notification will be sent if an activity is completed with at least one error event.
   - **Incomplete** – Notification will be sent if an activity is not completed successfully.
7. Under **Send SNMP Traps when**, configure the DS-Client to send SNMP traps when the backup has completed successfully, completed with warnings, completed with errors, or is incomplete.
8. Click **Next**.

5.14.1.8 Assigning a retention rule

1. To assign a retention rule to the backup, do one of the following:
   - If you don't want to assign a retention rule, select **No retention rule**.
   - To assign a retention rule, select **Use a specific retention rule**, and then select the retention rule.

NOTE: To create or edit a retention rule, click **[...]**. For more information, see Section 4.1, "Configuring a retention rule", on page 98.

---

2. Click **Next**.

5.14.1.9 Assigning a schedule

1. To assign a schedule to the backup, do one of the following:
   - If you don't want to assign a schedule, select **Not scheduled**.
   - To assign a schedule, select **Scheduled.** In the **Available schedules** box, select an existing schedule.

   NOTE: To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, "Configuring a schedule", on page 90.

2. Click **Next**.

5.14.1.10 Naming the backup

1. In the **Set name** box, type a name for the backup.
2. In the **Set type** box, select the type of backup you want to create. The list of available backup types depends on the configuration of your DS-Client.
   - Online
   - Self-contained
   - Local-only
   - Statistical

   NOTE: For more information, see Section 5.1, "Backup types", on page 106.

3. If you selected **Online**, do the following:
   a) To send a copy of the oldest generation of the file that is about to be overwritten from the DS-System to the BLM Archiver, select the **BLM (Infinite Generations)** check box.

   NOTE: The Backup Lifecycle Management tool must be enabled for the DS-Client.

   b) To save a copy of the backup data to a local storage location on the DS-Client computer, select the **Save on Local Storage** check box.

   NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Self-contained and Local Only backups.

c) To use the local storage as a cache if the DS-Client loses connection with the DS-System, select the **Transmission cache on Local Storage** check box. The cached backup data will be sent to the DS-System on the next connection after synchronization.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path.

d) To save a copy of the backup data to the instant recovery vault, select the **Save in instant recovery vault** check box.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Instant Recovery backups.

e) Beside the **Local Storage Path** box, click **>>**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

4. If you selected **Self-Contained**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

5. If you selected **Local-Only**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**..

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

6. If you selected **Statistical**, and want to emulate an actual backup transfer process, select the **Calculate transmit amount** check box. During the backup, specified backup files will be read from their source and processed for compression and encryption.
7. If the multitenant feature is enabled and configured, in the **Customer** list, you can select the customer to which you want to assign the backup. For more information, see Section 11.5, “Multitenant DS-Clients”, on page 634.

8. Click **Finish**.

5.14.2 Restoring a Microsoft SharePoint Server (Classic) backup

You can restore data from a Microsoft SharePoint Server (Classic) backup. The SharePoint data can only be restored to the same site in the same domain. When specifying the restore destination, you can only select the original location.

5.14.2.1 Selecting the restore items

1. Browse the backups tree and select the backup you want to restore.
2. On the **Restore** menu, click **Restore Now**.
3. To restore an entire backup or an entire Microsoft SharePoint site, browse the directories tree and select the check box beside the backup or folder you want to restore.
4. To restore individual files, select the site containing the required list, click **Show Files**, and then do the following:
   - To view details about the backed up file, select the file, and then click **File Info**.
   - To view modified files, click **Show Modified**.
   - To view archived files, click **Show Archived**.
5. To view the number of files selected and calculate the total amount of files selected, select the **Calculate amount** check box.
6. To exclude subdirectories, clear the **Include SubDirs** check box, as the default setting is to include sub-directories.
7. To search for files that match a certain criteria, in the **Filter** box, type the file pattern that you want to search for in the selected folder. For example, *.doc will search for all files with the doc file extension.
8. To search for a specific backed up file, click **Find File**. In the **Find Backed Up File** dialog box, do the following:
   a) Under **Search for**, select the search criteria to search for a backed up file either by **File name** or by **File ID**.
   b) Click **Find**.
   c) Select the required backed up file, and then click **Select**.
9. To view the details of the items you selected, click **selection**.
10. To refine your selection of items to restore, click **Advanced**. Under **Show**, select which generation you want to display. The options are as follows:

a) To restore the latest generation of all the files, select **Latest generation of all data**.

b) To restore files that were deleted from the source, but not removed from the online storage as of the last backup session, select **Latest generation of all data (except deleted data)**.

c) To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:

1. Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.
2. Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.
3. Click **OK**.

11. Click **Next**.

5.14.2.2 Selecting the restore location

Select the destination where you want to restore the backed up data. SharePoint data can be restored only to the same site in the same domain using the DS-Client, which is the original location.

- Click **Next**.

5.14.2.3 Selecting the restore options

The default option is **Detailed log**. Click **Next**.

5.14.2.4 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, under **Restore classification**, select the type of restore. The options are as follows:
   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.

3. Click **Finish**.

5.15 Microsoft SharePoint Server (VSS-aware) backups (Windows)

You can back up and restore data on a Microsoft SharePoint Server in a single server farm or multiple server farm configuration using the Microsoft VSS (Volume Shadow Copy Service) component.

Each Microsoft SharePoint Server is presented as a component by the VSS writer. A component must be restored with all its contents, based on the rules specified in its metadata. For more information, see Section 5.3.7, “Restoring VSS-aware backup components”, on page 133.

IMPORTANT: When creating a VSS-aware backup, the source database cannot reside on an SMB remote share as this is currently not supported and can result in VSS snapshot failure.

5.15.1 General requirements

- The account running the VSS writer must be a member of the Domain Administrators group and have permission to issue BACKUP DATABASE and RESTORE DATABASE commands to the target database servers.
- The account running the VSS writer must have permission to access the Microsoft SQL Server, which requires it to be a member of the SQL Server administrator group with db_creator and sysadmin roles.

5.15.2 DS-Client requirements

- The DS-Client must be able to resolve the computer name of the Microsoft SQL Server.
- The DS-Client must be able to access all the Microsoft SQL Server databases used by SharePoint.

5.15.3 Backup requirements

- You must register the VSS writer in the Windows registry by running the following command:

  ```
  STSADM –o registerwsswriter
  ```

- You must manually start the VSS writer service on every target Microsoft SharePoint computer you want to back up.

  NOTE: By default, the service must be started manually. However, you can configure it with the Automatic startup type.

- If you are backing up a SharePoint farm, the following additional requirements must be met:
  - The VSS writer service must be running on every Microsoft SQL Server machine in the SharePoint farm.
  - You must add the IP address and computer name for all the Microsoft SQL Servers and SharePoint web servers that are in the farm to the hosts file on the DS-Client computer, which is usually found in C:\Windows\system32\drivers\etc\hosts.

5.15.4 Restore requirements

There are two phases in the restore process. The first phase restores the Microsoft SQL full backup. The second phase restores the Microsoft SQL differential backups (if applicable).

Before restoring a web application to its original location, any existing web application with the same name and related shared service application must be deleted from SharePoint Central Admin.

5.15.5 Creating a Microsoft SharePoint Server (VSS-aware) backup

You can create a Microsoft SharePoint Server (VSS-aware) backup.

5.15.5.1 Selecting the type of backup

1. On the **Sets** menu, click **New Backup Set**.
2. Select **VSS-aware Backup Set**, and then click **Next**
3. Select **Microsoft SharePoint Server**, and then click **Next**.

5.15.5.2 Selecting the backup source

IMPORTANT: For a VSS aware backup, remote UAC is enabled by default. The local administrator account must have access to the admin$ share on the source machine.

To select the backup source:

1. Select the computer running the Microsoft SharePoint server.
2. By default, the **Ask for Network Credentials** check box is selected.
3. Click **Next**.
4. In the **Enter Network Credentials** dialog box, enter the required credentials to connect to the Microsoft SharePoint Server.
5. Click **OK**.

5.15.5.3 Selecting the backup items

1. To add an item, select the item, and then click **Add**.
2. To exclude an item when its parent directory is selected for backup, select the item, and then click **Exclude.**
3. To remove an item from the list of selected items for backup, select the item, and then click **Remove**.
4. Click **Next**.

5.15.5.4 Selecting the backup item options

1. To configure the number of maximum generations of the selected backup item that will be stored online, double click in the **Max gen** cell, and then enter the new value.
2. To back up the file permissions for an item, select the item, and then select the **Backup permissions** check box.
3. To back up the streams of data associated with an item, select the item, and then select the **Backup streams** check box.

NOTE: The configured options for the backup item appear under Options as follows: P = Backup permissions, S = Backup streams.

---

4. Click **Next**.

5.15.5.5 Selecting the backup options

1. Configure the options for the backup. The options are as follows:
   - **Detailed log** – Records all files that are backed up in the Activity Log. For more information, see Section 8.1, “Viewing the Activity Log”, on page 578.
   - **Initial backup** – Uses the Initial Backup feature for the first backup. To configure the initial backup path, click **[>>]**. For more information, see Section 11.1.1, “Configuring the initial backup path”, on page 618.
   - **Stop on errors** – Stops a backup process when the number of errors reaches the specified value. A value of 0 means the DS-Client does not stop a backup process regardless of the number of errors.

     NOTE: You can configure the default setting using the **MaxErrors** advanced configuration parameter. For more information, see Section 2.1.8.6, “Miscellaneous parameters (Windows)”, on page 42.

   - **VSS validation** – Specifies the type of VSS validation that will be applied prior to performing the backup. The options are as follows:
     - **Disable** – VSS validation is not performed.
     - **Enable** – VSS validation is performed.
     - **Use DS-Client’s settings** – VSS validation is performed using the DS-Client settings.
   - **Compression type** – Specifies the type of compression that will be applied to the backup. The options are as follows:

- **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good default compression when the network is not the bottleneck.
- **ZLIB (Global, Low, Medium, and High)** – Normally produces better compression than LZOP, but will take more time to compress. This is a good default compression when the bottleneck is the network. ZLIB Low corresponds to a value of 3, ZLIB Medium = 6, and ZLIB High = 9.
- **None** – Disables compression for the backup.

2. Under **Database backup policy**, in the **Full dump** box, select a method for the full dump: The options are as follows:
    - **Always** (Default) — Performs a full dump (VSS snapshot) of each database.
    - **Plus Differential** — Performs a full dump (VSS snapshot) of the database on first backup followed by differential backups until another full backup is required (*). Differential backups contain all the changes to the database since the last full dump. (*) A full dump is needed (other than first time) when:

- A database has been backed up by another backup or manually from the SharePoint tools.
- A database has been restored (either from another database or an earlier generation).
- The database properties have been modified (recovery model switched to ‘simple’).
- A set number of consecutive differential backups have been performed, unless over-ruled with the **Do not start full dump** option. This uses the same number set in the **MasterGenerations** advanced parameter (note this parameter is also used for another purpose). For more information, see Section 2.1.8, “Configuring the advanced settings”, on page 37.

For greater control of when the full dump occurs, you can delay or force a full dump. For more information see Section 5.2.5, “Database backup policies”, on page 112. The options are as follows:

- **Do not start full dump on** — Specifies days and time period.
- **Full every** — Specifies a regular interval.
- **Full every week on** — Specifies a regular interval.

- **Full every month on** — Specifies a regular interval.

IMPORTANT: You must perform Full dumps at a regular frequency to protect the integrity of the database backup. By default, DS-Client allows a full backup to be skipped a maximum of 120 consecutive times. This number is configurable using the **MaxNonFullDumps** advanced parameter.

d) To specify a command to run before (Pre) and/or after (Post) the execution of the backup, click **Pre/Post**. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525.

3. Click **Next**.

5.15.5.6 Specifying backup performance options

IMPORTANT: These options are intended for high performance environments where the DS-Client can take advantage of the speed of the storage where the source data resides. Test different settings to determine the optimal value. Slower storage can result in performance issues if the values are not properly configured.

1. Under Maximum pending asynchronous I/O for a file, configure the maximum I/O operations the DS-Client will use for each file from the backup.

NOTE: This setting is for storage devices that support better parallel disk I/O, such as NAS devices. The optimal setting for this value depends on the storage device and network speed. Increasing this value can significantly increase the backup speed. If your storage device does not support better parallel disk I/O, use the default value, otherwise the performance can be significantly degraded.

- To use the default **MaxPendingIOPerFile** advanced configuration parameter, click **Use DS-Client’s settings**. For more information, see Section 2.1.8.10, “Performance parameters (Windows)”, on page 55.
- To override the default setting with a custom value that only applies for the backup, click **Use specific value**, and then enter the value.

2. Under **Read buffer size for backup**, configure the internal buffer size (in KB) for reading a file during the backup process.

- To use the default **FileReadBufferSize** advanced configuration parameter, click **Use DS-Client’s settings**. For more information, see Section 2.1.8.10, “Performance parameters (Windows)”, on page 55.

- To override the default setting with a custom value that only applies for the backup, click **Use specific buffer size (KB)**, and then enter the value.

IMPORTANT: To achieve optimum backup performance, the DS-Client read buffer size might need to be different, depending on the combination of the target storage device, target operating system, and any mid-ware involved between the storage and the operating system.

3. Click **Next**.

5.15.5.7 Selecting the notification options

1. To configure a notification, do one of the following:
   - To add a notification, click **Add.**
   - To modify a notification, select the notification, and then click **Modify.**

NOTE: To delete a notification, select the notification, and then click **Delete**.

2. To send a broadcast notification, select **Broadcast**. Select the server containing the messenger service to which you want to send the message and click **OK**.

NOTE: Broadcast notifications to domains or workgroups are limited to 128 characters.

3. To send an event notification, elect **Event**. Select the server on which you want the notification to be recorded in the Event Log.
4. In the **Completion** box, specify under what conditions a notification will be sent, and click **OK**. The options are as follows:
   - **All** – Notification will be sent under all conditions.
   - **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
   - **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.
   - **Completed with errors** – Notification will be sent if an activity is completed with at least one error event.
   - **Incomplete** – Notification will be sent if an activity is not completed successfully.
5. Click **Next**.

5.15.5.8 Assigning a retention rule

1. To assign a retention rule to the backup, do one of the following:
   - If you don't want to assign a retention rule, select **No retention rule**.
   - To assign a retention rule, select **Use a specific retention rule**, and then select the retention rule.

NOTE: To create or edit a retention rule, click [...]. For more information, see Section 4.1, "Configuring a retention rule", on page 98.

---

2. Click **Next**.

5.15.5.9 Assigning a schedule

1. To assign a schedule to the backup, do one of the following:
   - If you don't want to assign a schedule, select **Not scheduled**.
   - To assign a schedule, select **Scheduled.** In the **Available schedules** box, select an existing schedule.

NOTE: To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, "Configuring a schedule", on page 90.

---

2. Click **Next**.

5.15.5.10 Naming the backup

1. In the **Set name** box, type a name for the backup.
2. In the **Set type** box, select the type of backup you want to create. The list of available backup types depends on the configuration of your DS-Client.
   - Online
   - Self-contained
   - Local-only
   - Instant recovery
   - Statistical

NOTE: For more information, see Section 5.1, "Backup types", on page 106.

---

3. If you selected **Online**, do the following:

   a) To send a copy of the oldest generation of the file that is about to be overwritten from the DS-System to the BLM Archiver, select the **BLM (Infinite Generations)** check box.

   NOTE: The Backup Lifecycle Management tool must be enabled for the DS-Client.

   b) To save a copy of the backup data to a local storage location on the DS-Client computer, select the **Save on Local Storage** check box.

   NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Self-contained and Local Only backups.

   c) To use the local storage as a cache if the DS-Client loses connection with the DS-System, select the **Transmission cache on Local Storage** check box. The cached backup data will be sent to the DS-System on the next connection after synchronization.

   NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path.

   d) To save a copy of the backup data to the instant recovery vault, select the **Save in instant recovery vault** check box.

   NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Instant Recovery backups.

   e) Beside the **Local Storage Path** box, click **>>**. Enter a local storage path for the backup, and then click **OK**.

   NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

4. If you selected **Self-Contained**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

   NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

5. If you selected **Local-Only**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

   NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

6. If you selected **Instant Recovery**, the **Save in instant recovery vault** option is selected by default.

   IMPORTANT: Each Linux DS-Client must have a unique ZFS file name.

7. If you selected **Statistical**, and want to emulate an actual backup transfer process, select the **Calculate transmit amount** check box. During the backup, specified backup files will be read from their source and processed for compression and encryption.
8. If the multitenant feature is enabled and configured, in the **Customer** list, you can select the customer to which you want to assign the backup. For more information, see Section 11.5, “Multitenant DS-Clients”, on page 634.
9. Click **Finish**.

5.15.6 Performing a VSS restore

You can perform a VSS restore of a Microsoft SharePoint Server (VSS-aware) backup using the Microsoft VSS tools.

NOTE: Only one generation (backup session) can be restored at a time.

5.15.6.1 Selecting the restore method

1. Browse the backups tree and select the backup you want to restore.
2. On the **Restore** menu, click **Restore Now**.
3. Select **VSS Restore**.
4. Click **Next**.

5.15.6.2 Selecting the restore items

1. To restore an entire backup or folder, browse the tree and select the check box beside the backup or folder you want to restore.
2. To restore individual files, select the folder containing the required files, click **Show Files**, and then do the following:
   - To view details about the backed up file, select the file, and then click **File Info**.
   - To view modified files, click **Show Modified**.
   - To view archived files, click **Show Archived**.
3. To view the number of lists selected and calculate the total amount of files selected, select the **Calculate amount** check box.
4. To exclude subdirectories, clear the **Include SubDirs** check box, as the default setting is to include sub-directories.
5. To search for files that match a certain criteria, in the **Filter** box, type the file pattern that you want to search for in the selected folder. For example, *.doc will search for all files with the doc file extension.
6. To search for a specific backed up file, click **Find File**. In the **Find Backed Up File** dialog box, do the following:
   a) Under **Search for**, select the search criteria to search for a backed up file either by **File name** or by **File ID**.
   b) Click **Find**.
   c) Select the required backed up file, and then click **Select**.
   d) To view the details of the items you selected, click **Selection**.
7. To view the files that are part of the selected VSS component, click **VSS Component**.
8. To refine your selection of items to restore, click **Advanced**. Under **Show**, select which generation you want to display. The options are as follows:

a) To restore the latest generation of all the files, select **Latest generation of all data**.

b) To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:

1. Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.

2. Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.

c) Click **OK**.

9. Click **Next**.

5.15.6.3 Selecting the restore location

1. Select the location to which you want to restore the backup. The options are as follows:

- **Original location** – Data is restored to the original backup source location and existing files with the same name are overwritten. This is the default option.
- **Alternate location** – Data is restored to a location other than the original backup source.

NOTE: When restoring to an alternate location, the security of restored items in the destination location might not resemble the security of those items during backup.

2. If you selected **Alternate location**, then do the following:

a) Beside the **Alternate location** box, click **[>>]**.

b) In the **Select Alternate Server** dialog box, select the server to which you want to restore, and then click **Next**.

c) In the **Enter Network Credentials** dialog box, enter the credentials to connect to the destination computer, and then click **OK**.

d) To rename the individual components being restored, click **Rename component**.

e) In the **Rename Component** dialog box, do the following:

1. Click in the **Target Path** cell and edit the name or path for the component.
2. To load mapping contents from a saved XML file, click **Load XML**.

NOTE: A mapping is loaded only if the logical path and the source component columns from the XML file exactly match with those displayed in the list.

---

3. To save the contents from the current source target mapping list to an XML file, click **Save XML**.
4. Click **OK**.

3. Click **Next**.

5.15.6.4 Selecting the performance options

IMPORTANT: These options are intended for large backups in high performance environments where the DS-Client can take advantage of the speed of the storage where the source data resides. Test different settings to determine the optimal value. Slower storage can result in performance issues if these values are not configured correctly.

---

1. Under **Maximum pending asynchronous I/O for a file**, configure the maximum number of I/O operations the DS-Client will use for each file during the restore process.
   - To use the default MaxPendingIOPerFile advanced configuration parameter setting, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value** and then enter the value.
2. Under **DS-System side read threads**, configure the number of files the DS-System can read simultaneously for the restore process.
   - To use the default MaxRestoreReadThreads advanced configuration parameter setting, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value** and then enter the value.
3. Click **Next**.

5.15.6.5 Selecting the restore options

1. Under **Restore options,** do the following:

   a) To record all restored files in the Activity Log, select the **Detailed log** check box.

   b) To skip the pre and post restore processes, select the **Skip Pre/Post** check box. If this check box is cleared, the DS-Client runs a specified activity before and/or after a restore operation. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525.

2. Click **Next**.

5.15.6.6 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, under **Restore classification**, select the type of restore. The options are as follows:

   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.

3. Click **Finish**.

5.15.7 Performing a file restore

You can perform a file restore to restore individual files. This restore method does not recreate the working database.

5.15.7.1 Selecting the restore method

1. Browse the backups tree and select the backup you want to restore.
2. On the **Restore** menu, click **Restore Now**.
3. Select **File Restore**.
4. Click **Next**.

5.15.7.2 Selecting the restore items

1. To restore an entire backup or folder, browse the tree and select the check box beside the backup or folder you want to restore.
2. To restore individual files, select the folder containing the required files, and then click **Show Files**. Under **File List**, do the following:
3. To view the number of files selected and calculate the total amount of files selected, select the **Calculate amount** check box.
4. To exclude sites and lists, clear the **Include SubDirs** check box, as the default setting is to include sites.
5. To search for files that match a certain criteria, in the **Filter** box, type the file pattern that you want to search for in the selected folder. For example, *.doc will search for all files with the doc file extension.
6. To restore individual files, select the folder containing the required files, click **Show Files**, and then do the following:
   - To view details about the backed up file, select the file, and then click **File Info**.
   - To view the details of the items you selected, click **Selection**.
   - To view archived files, click **Show Archived**.
7. To refine your selection of items to restore, click **Advanced**. Under **Show**, select which generation you want to display. The options are as follows:
   - To restore the latest generation of all the files, select **Latest generation of all data**.
   - To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:
     a) Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.
     b) Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.
   c) Click **OK**.

8. Click **Next**.

5.15.7.3 Selecting the restore location

1. Select the location to which you want to restore the backup. The options are as follows:
   - **Original location** – Data is restored to the original backup source location and existing files with the same name are overwritten. This is the default option.
   - **Alternate location** – Data is restored to a location other than the original backup source on the same server.

   NOTE: When restoring to an alternate location, the security of restored items in the destination location might not resemble the security of those items during backup.

2. If you selected **Alternate location**, then do the following:
   a) Beside the **Alternate location** box, click **[>>]**.
   b) In the **Select Alternate Server** dialog box, select the computer where you want to restore the data.
   c) In the **Enter Network Credentials** dialog box, enter the credentials to connect to the destination computer, and then click **OK**.
   d) In the **Destination** cell, select a share location.
   e) Click in the **Restore to** cell and type the name of the directory or click **[>>]** and select a directory.
   f) In the **Truncate** box, you can increase the truncate level to shorten the common portion of the restore path, if the selected restore items contain a common path.

   NOTE: If the entire path is truncated, the alternate location directory will inherit the security of the truncated parent directory.

3. Click **Next**.

5.15.7.4 Selecting the performance options

IMPORTANT: These options are intended for large backups in high performance environments where the DS-Client can take advantage of the speed of the storage where the source data resides. Test different settings to determine the optimal value. Slower storage can result in performance issues if these values are not configured correctly.

1. Under **Maximum pending asynchronous I/O for a file**, configure the maximum number of I/O operations the DS-Client will use for each file during the restore process.
   - To use the default MaxPendingIOPerFile advanced configuration parameter setting, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value** and then enter the value.
2. Under **DS-System side read threads**, configure the number of files the DS-System can read simultaneously for the restore process.
   - To use the default MaxRestoreReadThreads advanced configuration parameter setting, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value** and then enter the value.
3. Click **Next**.

5.15.7.5 Selecting the restore options

1. Under Permissions, select a restore option for permissions. The options are as follows:
   - **Yes** – Restores the permissions for all the backed up files.
   - **Skip** – Skips the file security information of the backed up files. Newly created files and folders inherit the security settings of the parent folder.
2. Under **Method**, select a method for the DS-Client to perform the restore. The options are as follows:
   - **Save** – Restores files to a temporary location first to prevent restored files from overwriting an existing file. If the file is restored successfully, the original file is overwritten with the temporary file.
   - **Use buffer** – Restores files to the DS-Client buffer first and then transfers the files to the restore destination. This method minimizes the duration for which the restore process occupies the destination server.
   - **Fast** – Uses a direct restore method by writing data as it is received.

   NOTE: If you select the **Fast** method, files in the destination location are overwritten upon receipt of the first byte of data.
3. To record all restored files in the Activity Log, select the **Detailed log** check box.
4. To skip the pre and post restore processes, select the **Skip Pre/Post** check box. If this check box is clear, click **Pre/Post**. DS-Client will run a specified activity before and/or after a restore operation. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525.
5. Click **Next**.

5.15.7.6 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, under **Restore classification**, select the type of restore. The options are as follows:
   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.
3. Click **Finish**.

5.15.8 Performing a granular restore

You can perform a granular restore to restore at the individual item-level. Before performing a granular restore, consider the following:

- The backup must be created using the VSS-aware backup type.
- The target Microsoft SharePoint server where you want to perform the granular restore must have the DS-Recovery Tools installed and running. This is a separate installation. For detailed instructions, see the *Client Software Installation Guide*.
- The DS-Recovery Tools service account must have access to the Microsoft SQL Server instance and the Microsoft SharePoint Server where the items are going to be restored.

There are two steps to performing a granular restore:

1. Restore the Microsoft SharePoint Server (VSS aware) database to the point-in- time that contains the items you want to restore.
2. Connect to the restored Microsoft SharePoint Server (VSS aware) database and select the individual items you want to restore.

NOTE: If you are restoring from a BLM Restorable Image or Disc/Tape media, you can only perform step 1 which will restore the database from the media. You must perform step 2 on the database restored in step 1

5.15.8.1 Selecting a restore method

1. Browse the backups tree and select the backup you want to restore.
2. On the **Restore** menu, click **Restore Now**.
3. Select **Granular Restore**, and then select **Step 1. Database Restore**.
4. Click **Next**.

5.15.8.2 Selecting the restore items

1. To restore an entire backup or folder, browse the tree and select the check box beside the backup or folder you want to restore.
2. To restore individual files, select the folder containing the required files, and then click **Show Files**. Under **File List**, do the following:
3. To view the number of files selected and calculate the total amount of files selected, select the **Calculate amount** check box.
4. To exclude subdirectories, clear the **Include SubDirs** check box, as the default setting is to include sub-directories.
5. To filter the list of files, in the **Filter box**, enter a filter using * as a wildcard, and then click **Show Files** to update the list of files.
6. To find a backed up file, click **Show Files**, and then do the following:
   - To view details about the backed up file, select the file, and then click **File Info**.
   - To view the details of the items you selected, click **Selection**.
   - To view a list of archived generations for a folder, do the following:
     a) In the **Database Tree**, select the folder, and then click **Show Files**.
     b) Under **Files**, click **Show Archived**.
7. To refine your selection of items to restore, click **Advanced**. Under **Show**, select which generation you want to display. The options are as follows:
   a) To restore the latest generation of all the files, select **Latest generation of all data**.
   b) To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:
      1. Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.
      2. Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.
   c) Click **OK**.

8. Click **Next**.

5.15.8.3 Selecting the restore location

1. Beside the **Select computer** box, click **[>>]**, and then select a computer with the Microsoft SQL database server.
2. In the **Instance Name** box, select the Microsoft SQL server instance to which you want to restore.
3. Beside the **Physical File Location** box, click **[>>]**, and then select a folder on the selected computer where the data will be restored.
4. Click **Next**.

5.15.8.4 Selecting the performance options

IMPORTANT: These options are intended for large backups in high performance environments where the DS-Client can take advantage of the speed of the storage where the source data resides. Test different settings to determine the optimal value. Slower storage can result in performance issues if these values are not configured correctly.

---

1. Under **Maximum pending asynchronous I/O for a file**, configure the maximum number of I/O operations the DS-Client will use for each file during the restore process.
   - To use the default MaxPendingIOPerFile advanced configuration parameter setting, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value** and then enter the value.
2. Under **DS-System side read threads**, configure the number of files the DS-System can read simultaneously for the restore process.
   - To use the default MaxRestoreReadThreads advanced configuration parameter setting, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value** and then enter the value.
3. Click **Next**.

5.15.8.5 Selecting the restore options

1. Do one of the following:

   a) To record all restored files in the Activity Log, select the **Detailed log** check box.

   b) To skip the pre and post restore processes, select the **Skip Pre/Post** check box. If this check box is clear, click **Pre/Post**. DS-Client will run a specified activity before and/or after a restore operation. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525.

   c) To send a notification when the database restore is complete, select the **Send E-Mail notification when database restore finishes** check box, and in the **E-Mail Address** field, type the email address to which you want to send the notification.

2. Click **Next**.

5.15.8.6 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, under **Restore classification**, select the type of restore. The options are as follows:

   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.

3. Click **Finish**.

NOTE: After the database has been restored to a Microsoft SQL server, you can proceed to step 2 - restoring at Item-Level.

5.15.8.7 Performing an items restore

1. Browse the backups tree and select the same backup you want to restore.
2. On the **Restore** menu, click **Restore Now**.
3. Select **Granular Restore**, and then select **Step 2. Items Restore**.
4. Click **Next**.

5.15.8.8 Selecting the database restore location

1. Browse and select the Microsoft SQL database server to which you want to restore the Microsoft SharePoint Server (VSS aware) backup.
2. By default, DS-Client uses your current user credentials to connect to the selected computer and database. To specify different credentials, select **Ask for Network Credentials** and/or **Ask for database credentials**.
3. Click **Next**
4. When prompted, type the valid credentials to connect to the selected computer and/or database, and then click **OK**.

5.15.8.9 Selecting the database to restore

1. From the databases list, select the database that you restored in step 1, and then click **Add**.
   - To remove a database, select the database under backup items selected, and then click **Remove**.
2. Click **Next**.

5.15.8.10 Selecting the restore location

NOTE: The restore destination must be running the DS-Recovery Tools. This requires a separate installation. See the *Client Software Installation Guide* for instructions.

1. Select the location to which you want to restore the backup. The options are as follows:
   - **Original location** – Data is restored to the original backup source location and existing files with the same name are overwritten. This is the default option.
   - **Alternate location** – Data is restored to a location other than the original backup source.

     NOTE: When restoring to an alternate location, the security of restored items in the destination location might not resemble the security of those items during backup.

2. If you selected **Alternate location**, then do the following:
   a) Beside the **Alternate location** box, click **[>>]**.
   b) In the **Select Alternate Server** dialog box, select the server to which you want to restore, and then click **Select**.
   c) By default, DS-Client uses the current user's logon credentials to connect to the selected computer. If you need to specify alternate network credentials, select the **Ask for Network Credentials** check box.
   d) In the **Enter Network Credentials** dialog box, type a valid user name and password for the selected computer, and then click **OK**.
3. Beside the **Dump to** field, click **[>>]**, and select a dump location on the restore target.
4. Click **Next**.

5.15.8.11 Selecting a Site/Sub-Site

1. Do one of the following:
   - To add an entire site (/) folder, or a specific sub-site, select the folder, and then click **Add**.
   - To restore a **Full List**, highlight the site folder (or sub-folder) containing the list you want, click **Add Lists**, and then do the following:
     1. Select the list, customer list, or document library you want to restore.
     2. Click **Finish**.
   - To restore a list-item, highlight the site folder (or sub-folder) containing the list you want, click **Add List Items**, and then do the following:
     1. Select the list or document library you want to restore, and then click **Next**.
     2. Select the list items you want to restore (use CTRL + click for multiple items).
     3. Click **Finish**.

   You can hover the mouse pointer over a folder to view the corresponding URL and source database name.
2. Click **Next**.

5.15.8.12 Selecting the restore options

1. To record all restored files in the Activity Log, select the **Detailed Log** check box.
2. To overwrite a restore item that already exists on the target restore, select the **Overwrite if exists** check box.
3. To delete the database you used for step 1 of the granular restore, select the **Remove database after restore is finished successfully** check box.
4. In the **Web Application URL** box, enter URL of the web-application you are restoring. This target URL exists in the Microsoft SharePoint Server central administration.
5. Click **Finish**.

5.16 Microsoft SQL Server (Classic) backups (Windows)

You can back up and restore a Microsoft SQL Server database.The first backup is always a full database dump and subsequent backups are incremental forever.

The value of separate transaction logs is that they can be restored as separate dump files to an alternate location. This method is better than restoring from a full back up only if there is a specific transaction point you want to restore between two full backup sessions.

5.16.1 Creating a Microsoft SQL Server (Classic) backup

You can create a Microsoft SQL Server backup.

5.16.1.1 Selecting the type of backup

1. On the **Sets** menu, click **New Backup Set**.
2. Select **Microsoft SQL Server**, and then click **Next**.

5.16.1.2 Selecting the backup source

1. Select the computer containing the files you want to back up. The **Path** box displays the network path of the item selected in the tree.
2. To provide the credentials for the selected computer, select the **Ask for Network Credentials** check box. You will be prompted too enter a valid user name and password for the selected computer.
3. To provide credentials for the database, select the **Ask for database credentials** check box. You will be prompted to enter a valid user name and password for the selected database.
4. Click **Next**.

NOTE: For Microsoft SQL Server Clusters, you can type the virtual node in the **Path** box. The DS-Client must be able to connect to all the nodes and resolve the virtual node (IP address), all individual nodes (names and IP addresses), and the Windows cluster's name (IP address).

5.16.1.3 Selecting the share & path for the database dump

To back up an active database, a full dump, incremental dump, or differential dump of the database must be made. Select a path where to save the dump file on the computer running the Microsoft SQL server.

1. Select how and where the DS-Client handles the database dump.
2. Select a method to handle the database dump. The options are as follows:
   - To dump the database directly to a disk file, select an available share/folder or type an accessible UNC path in the **Dump Path** box. The dump file will be in the format `database.y` (where y is an internal number). This file will be backed up like a regular file and then removed. A database that is backed up using this method can be restored only using the same method.

     NOTE: If you specify a UNC path, both the Microsoft SQL Server service account and the backup user credentials must have read-write permissions to access the UNC path.

   - To save the dump file to the local storage on the DS-Client computer, select **DS-Client Buffer**. Use this option if you do not have enough space on the Microsoft SQL Server computer
   - To dump the database through a pipe created on the Microsoft SQL Server computer, select **DS-Client Pipe**. Use this method if the database is too big to be dumped to a file and you have a fast and reliable connection to the DS-System.

     NOTE: Microsoft SQL Server requires a VDI Tool for backup and restore using DS-Client Buffer or DS-Client Pipe.

3. If you selected **DS-Client Buffer** or **DS-Client Pipe** as the database dump method, select **VDI Tool Directory** to specify the location on a remote computer where the DS-Client will run the VDI Tool.

   NOTE: If you do not select this option, the DS-Client will run the tool from a default directory on the “c:\” drive of the target computer.

4. Click **Next**.

5.16.1.4 Selecting the backup items

1. Add the items you want to back up:
   - To add all databases, select the entire instance, and then click **Add**.
   - To add a specific database to the backup, browse the Databases List and select the database you want to include, and then click **Add**.

   NOTE: Multiple instances on the same server are displayed; however, you can only add from one instance per backup.

2. To exclude an item when its parent directory is selected for backup, select the item, and then click **Exclude.**
3. To exclude an item using regular expressions, select the item, and then click **RegEx**.

   NOTE: Regular expressions provide more specific filtering than the exclude function. For example, you can use regular expressions to exclude individual file names or patterns. Use this option only if you are familiar with the syntax.

4. To remove an item from the list of selected items for backup, select the item, and then click **Remove**.
5. Click **Next**.

5.16.1.5 Selecting the backup item options

1. To configure the maximum generations for a backup item that will be stored online, double click the **Max Gen** cell, and then enter the value.
2. To verify database integrity and ensure backup of a valid database dump, select the **Run DBCC before backup** check box.
3. To have DS-Client dump the transaction log and send it to DS-System, along with the database, select the **Backup Transaction Log** check box. The timing of the truncation depends on the database backup policy.
   - **Full** — Transaction logs are truncated before the database dump.
   - **Differential** — Transaction logs are truncated before the database dump.
   - **Incremental** — Transaction logs are first backed up and then truncated.

   NOTE: The database must be configured with the full or bulk_logged recovery model.

   Truncation of Microsoft SQL Server database transaction logs is automatically handled by the SQL Server engine. Whenever log truncation occurs, it only frees up the space within the log files. It does not reduce the physical file size. Various factors can also delay transaction log truncation. For more information, see *Microsoft SQL Server* documentation.
   - For databases configured in **Simple** recovery mode, the transaction logs should be truncated whenever you perform a full backup.
   - For databases configured in **Full** or **Bulk-logged** recovery mode, the transaction logs should be truncated whenever you perform a transaction log backup, or if a checkpoint has occurred since the previous backup.
4. To prevent the backup of dump file(s) if DBCC errors are detected, select the **Stop on DBCC errors** check box.
5. Click **Next**.

5.16.1.6 Selecting the backup options

1. Configure the options for the backup. The options are as follows:

   - **Use buffer** – Copies files to the DS-Client buffer to free up the backup source as fast as possible. The DS-Client then sends the files from the DS-Client buffer to the DS-System. This option is selected by default. For more information, see Section 5.2.7, “Performance”, on page 113.
   - **Detailed log** – Records all files that are backed up in the Activity Log. For more information, see Section 8.1, “Viewing the Activity Log”, on page 578.
   - **Initial backup** – Uses the Initial Backup feature for the first backup. To configure the initial backup path, click **[>>]**. For more information, see Section 11.1.1, “Configuring the initial backup path”, on page 618.
   - **Stop on errors** – Stops a backup process when the number of errors reaches the specified value. A value of 0 means the DS-Client does not stop a backup process regardless of the number of errors.

     NOTE: You can configure the default setting using the **MaxErrors** advanced configuration parameter. For more information, see Section 2.1.8.6, “Miscellaneous parameters (Windows)”, on page 42.

   - **Compression type** – Specifies the type of compression that will be applied to the backup. The options are as follows:
     - **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good default compression when the network is not the bottleneck.
     - **ZLIB (Global, Low, Medium, and High)** – Normally produces better compression than LZOP, but will take more time to compress. This is a good default compression when the bottleneck is the network. ZLIB Low corresponds to a value of 3, ZLIB Medium = 6, and ZLIB High = 9.
     - **None** – Disables compression for the backup.
2. Under **Database backup policy**, in the **Full dump** box, select a method for the full dump. The options are as follows:

   - **Always** (Default) — Performs a full dump (VSS snapshot) of each database.
   - **Plus Differential** — Performs a full dump (VSS snapshot) of the database on first backup followed by differential backups until another full backup is required. Differential backups contain all the changes to the database since the last full dump.
   - **Plus Incremental** — Performs a full dump (VSS snapshot) of the database on first backup followed by incremental backups until another full backup is required.

- **Transaction Log Only backup** — Use this database backup policy in combination with a separate VSS-aware or Classic Microsoft SQL Server backup that performs full database backups of the database(s). When using this database backup policy, you must do the following:
  - Ensure the integrity of the sequence of the transaction logs in relation to the Full database backups performed by the other Microsoft SQL Server backup.
  - Select the option to keep all generations within a specific period and specify that period.
  - Set the retention settings to keep 0 generations.

  For more information, see Section 5.3.5, “Restoring transaction logs only (Microsoft SQL)”, on page 131.

  Other than the first time, a full dump is required when:
  - A database has been restored either from another database or an earlier generation.
  - The database properties have been modified. For example, if the recovery model has been switched to simple.

e) To prevent a full dump from being performed during the selected time period, select the **Do not start full dump on** check box, select the day, and then specify the time period.

NOTE: The **Do not start full dump** option uses the same number set in the **MasterGenerations** advanced parameter. For more information, see Section 2.1.8, “Configuring the advanced settings”, on page 37.

- To force a full backup to be performed at an interval, select the **Full every** check box, and then specify the values for the interval.
- To force a full backup to be performed on a specific day of the week, select the **Full every week on** check box, select the day, and then specify the time after which the full backup can be performed.
- To force full backup to be performed on a regular monthly interval, select the **Full every month on** check box, select the day, and then specify the time after which the full backup can be performed.

3. To specify a command to run before (Pre) and/or after (Post) the execution of the backup, click **Pre/Post**. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525.
4. Click **Next**.

5.16.1.7 Specifying backup performance options

IMPORTANT: These options are intended for high performance environments where the DS-Client can take advantage of the speed of the storage where the source data resides. Test different settings to determine the optimal value. Slower storage can result in performance issues if the values are not properly configured.

1. Under Maximum pending asynchronous I/O for a file, configure the maximum I/O operations the DS-Client will use for each file from the backup.

   NOTE: This setting is for storage devices that support better parallel disk I/O, such as NAS devices. The optimal setting for this value depends on the storage device and network speed. Increasing this value can significantly increase the backup speed. If your storage device does not support better parallel disk I/O, use the default value, otherwise the performance can be significantly degraded.

   - To use the default **MaxPendingIOPerFile** advanced configuration parameter, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value**, and then enter the value.

2. Under **Read buffer size for backup**, configure the internal buffer size (in KB) for reading a file during the backup process.

   - To use the default **FileReadBufferSize** advanced configuration parameter, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific buffer size (KB)**, and then enter the value.

   IMPORTANT: To achieve optimum backup performance, the DS-Client read buffer size might need to be different, depending on the combination of the target storage device, target operating system, and any mid-ware involved between the storage and the operating system.

3. Click **Next**.

5.16.1.8 Selecting the notification options

1. To configure a notification, do one of the following:
   - To add a notification, click **Add.**
   - To modify a notification, select the notification, and then click **Modify.**

   NOTE: To delete a notification, select the notification, and then click **Delete**.

2. To send an email notification, select **E-Mail**. and then do the following:
   a) To send the email notification to the DS-Client administrator, select **Administrator**.
   b) To send an email to another recipient, select **Other**, and then specify the recipients email address.
   c) To send detailed backup information, select the **Detailed notification** check box.
   d) To include a detailed file-level backup log as an attachment, select the **Attach detail log** check box.
   e) To send the email notification in HTML format, select the **Send E-Mail using HTML format** check box.

      NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

   f) Click **OK**.
3. To send a pager notification, select **Pager**. The notification will be sent to the pager account configured for the DS-Client.

   NOTE: The pager option is available only if the DS-Client has been configured for pager notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

4. To send a broadcast notification, select **Broadcast**. Select the server containing the messenger service to which you want to send the message and click **OK**.

   NOTE: Broadcast notifications to domains or workgroups are limited to 128 characters.

5. To send an event notification, elect **Event**. Select the server on which you want the notification to be recorded in the Event Log.
6. In the **Completion** box, specify under what conditions a notification will be sent, and click **OK**. The options are as follows:
   - **All** – Notification will be sent under all conditions.
   - **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
   - **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.
   - **Completed with errors** – Notification will be sent if an activity is completed with at least one error event.
   - **Incomplete** – Notification will be sent if an activity is not completed successfully.
7. Click **Next**.

5.16.1.9 Assigning a retention rule

1. To assign a retention rule to the backup, do one of the following:
   - If you don't want to assign a retention rule, select **No retention rule**.
   - To assign a retention rule, select **Use a specific retention rule**, and then select the retention rule.

NOTE: To create or edit a retention rule, click **[...]**. For more information, see Section 4.1, "Configuring a retention rule", on page 98.

---

2. Click **Next**.

5.16.1.10 Assigning a schedule

1. To assign a schedule to the backup, do one of the following:
   - If you don't want to assign a schedule, select **Not scheduled**.
   - To assign a schedule, select **Scheduled.** In the **Available schedules** box, select an existing schedule.

NOTE: To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, "Configuring a schedule", on page 90.

---

2. Click **Next**.

5.16.1.11 Naming the backup

1. In the **Set name** box, type a name for the backup.
2. In the **Set type** box, select the type of backup you want to create. The list of available backup types depends on the configuration of your DS-Client.
   - Online
   - Self-contained
   - Local-only
   - Statistical

   NOTE: For more information, see Section 5.1, “Backup types”, on page 106.
3. If you selected **Online**, do the following:
   a) To send a copy of the oldest generation of the file that is about to be overwritten from the DS-System to the BLM Archiver, select the **BLM (Infinite Generations)** check box.

   NOTE: The Backup Lifecycle Management tool must be enabled for the DS-Client.

   b) To save a copy of the backup data to a local storage location on the DS-Client computer, select the **Save on Local Storage** check box.

   NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Self-contained and Local Only backups.

   c) To use the local storage as a cache if the DS-Client loses connection with the DS-System, select the **Transmission cache on Local Storage** check box. The cached backup data will be sent to the DS-System on the next connection after synchronization.

   NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path.

d) To save a copy of the backup data to the instant recovery vault, select the **Save in instant recovery vault** check box.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Instant Recovery backups.

e) Beside the **Local Storage Path** box, click **>>**. Enter a local storage path for the backup, and then click **OK**

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

4. If you selected **Self-Contained**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

5. If you selected **Local-Only**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

6. If you selected **Statistical**, and want to emulate an actual backup transfer process, select the **Calculate transmit amount** check box. During the backup, specified backup files will be read from their source and processed for compression and encryption.
7. If the multitenant feature is enabled and configured, in the **Customer** list, you can select the customer to which you want to assign the backup. For more information, see Section 11.5, “Multitenant DS-Clients”, on page 634.
8. Click **Finish**.

5.16.2 Restoring a Microsoft SQL Server (Classic) backup

You can restore data from a Microsoft SQL Server (Classic) backup.

5.16.2.1 Selecting the restore items

1. Browse the backups tree and select the backup you want to restore.
2. On the **Restore** menu click **Restore Now**.
3. To restore an entire backup or folder, browse the tree and select the check box beside the backup or folder you want to restore.
4. To restore individual files, select the folder containing the required files, and then click **Show Files**. Under **File List**, do the following:
5. To view the number of files selected and calculate the total amount of files selected, select the **Calculate amount** check box.
6. To exclude subdirectories, clear the **Include SubDirs** check box, as the default setting is to include sub-directories.
7. To filter the list of files, in the **Filter box**, enter a filter using * as a wildcard, and then click **Show Files** to update the list of files.
8. To find a backed up file, click **Show Files**, click **Find File**, and then in the **Find Backed Up File** dialog box, do the following:
   a) Under **Search for**, select the search criteria to search for a backed up file either by **File name** or by **File ID**.
   b) Click **Find**.
   c) Select the required backed up file, and then click **Select**.
9. In the **Files List** section, do one of the following:
   - To view details about the backed up file, select the file, and then click **File Info**.
   - To view the details of the items you selected, click **Selection**.
   - To view a list of archived generations for a folder, do the following:
     a) In the **Directories Tree**, select the folder, and then click **Show Files**.
     b) Under **Files**, click **Show Archived**.
10. To add modified items to the list of selected items for restore, do the following:
    a) Select a directory, and then click **Show Files**.
    b) To locate modified files, under **Files**, click **Show Modified**. Modified files located by the DS-Client are highlighted.

c) To include the modified files for restore, click **Add Modified**.

11. To refine your selection of items to restore, click **Advanced**. Under **Show**, select which generation you want to display. The options are as follows:

    a) To restore the latest generation of all the files, select **Latest generation of all data**.

    b) To restore files that were deleted from the source, but not removed from the online storage as of the last backup session, select **Latest generation of all data (except deleted data)**.

    c) To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:

        1. Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.

        2. Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.

        3. Click **OK**.

12. In the **Filter** section, select the type of filter you want to apply to the backups. The options are as follows:

    - **Show all data** – No filter is applied.
    - **Hide data (dirs/files) deleted from source on/before** – You can hide backed up data (directories and files) that was intentionally deleted from the source computer.
    - **Show only data (dirs/files) deleted from source on/before** – You can view and restore backed up data (directories and files) that was intentionally deleted from the source computer.

    NOTE: This section is available only if the restore or request wizard can use the DS-Client database to filter the backups. It does not appear for BLM Image Restore or Disc/Tape Restore, since they have been written to media and are no longer synchronized with the DS-Client database.

13. Click **OK**.

14. Click **Next**.

5.16.2.2 Selecting the restore location

1. Select the location to which you want to restore the backup. The options are as follows:
   - **Original location** – Data is restored to the original backup source location and existing files with the same name are overwritten. This is the default option.
   - **Alternate location** – Data is restored to a location other than the original backup source.
2. To change the location for the database dump, click **[>>]** beside the **Dump to** box.
   a) In the **Select Directory** dialog box, select a path for the database dump.
   b) Click **Select**.
3. If you selected **Original location**, do the following:
   - To restore the files to their original paths, select the **Preserve original database file location** check box. If this check box is clear, the restored files will be placed on the default path(s) of the target instance.
4. If you selected **Alternate location**, then do one of the following:
   - To restore to a different directory on the same server, skip the remaining steps and move to selecting the performance options.
   - To restore to a different server on the network, do the following:
     a) Beside the **Alternate location** box, click **[>>]**.
     b) In the **Select Alternate Server** dialog box, select the server where you want to restore the backed up database.You can also type the name or the IP address in the **Path** box.

     NOTE: By default, DS-Client uses your current user credentials to connect to the selected computer and database.

     c) To provide credentials for the selected computer, select the **Ask for Network Credentials** check box. You will be prompted too enter a valid user name and password for the selected computer.
     d) To provide credentials for the database, select the **Ask for database credentials** check box. You will be prompted to enter a valid user name and password for the selected database.
5. Click **Next**.

5.16.2.3 Selecting the performance options

IMPORTANT: These options are intended for large backups in high performance environments where the DS-Client can take advantage of the speed of the storage where the source data resides. Test different settings to determine the optimal value. Slower storage can result in performance issues if these values are not configured correctly.

1. Under **Maximum pending asynchronous I/O for a file**, configure the maximum number of I/O operations the DS-Client will use for each file during the restore process.
   - To use the default MaxPendingIOPerFile advanced configuration parameter setting, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value** and then enter the value.
2. Click **Next**.

5.16.2.4 Selecting the restore options

1. Under **Restore options,** do the following:
   a) To record all restored files in the Activity Log, select the **Detailed log** check box.
   b) To skip the pre and post restore processes, select the **Skip Pre/Post** check box. If this check box is clear, click **Pre/Post**. DS-Client will run a specified activity before and/or after a restore operation. For more information, see Section 5.25, "Configuring Pre/Post processes (Windows)", on page 525.
   c) To retain the database in restoring mode after the restore is complete, select the **Leave Database(s) in 'RESTORING' state** check box. DS-Client will not bring the database online.

5.16.2.5 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, under **Restore classification**, select the type of restore. The options are as follows:
   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.
3. Click **Finish**.

5.17 Microsoft SQL Server (VSS-aware) backups (Windows)

You can back up and restore data on a Microsoft SQL Server using the Microsoft VSS (Volume Shadow Copy Service) components on the destination computer.

Each Microsoft SQL Server database is presented as a component by the Microsoft SQL VSS writer. A component must be restored with all its contents, based on the rules specified in its metadata. For more information, see Section 5.3.7, “Restoring VSS-aware backup components”, on page 133.

IMPORTANT: When creating a VSS-aware backup, the source database cannot reside on an SMB remote share as this is currently not supported and can result in VSS snapshot failure.

5.17.1 Integrating with Nimble Storage

You can create Microsoft SQL Server (VSS-aware) backups that can be integrated with Nimble Storage to create persistent hardware snapshots of the Nimble Storage volumes. You can store the databases on Nimble Storage volumes and then restore only the selected databases from the snapshot or revert the entire volume.

NOTE: To specify how the copying of data from the snapshot to the destination is triggered, you can configure the DSClientPerformCopyFromSnapshot advanced configuration parameter. For more information, see Section 2.1.8, “Configuring the advanced settings”, on page 37.

Before integrating a Microsoft SQL Server (VSS-aware) backup with Nimble Storage, you must do the following:

- Ensure the VSS Nimble Provider has been installed on the Microsoft SQL Server host. For more information, see the *Client Software Installation Guide*.
- Manually create one or more volume collections, depending on your environment and user requirements. Configure each volume that contains the database(s) you plan to create snapshots for with a volume collection, and create an externally triggered schedule for each collection.
- To enable replication, configure a Nimble Storage replication partner in the Nimble Storage Management Console. You must provide the name or IP address of the replication partner on which you want the hardware snapshots to be created.
- Determine the retention settings you need in the DS-System, production Nimble Storage location, and Nimble Storage replication partner (if required). You will be asked to specify the maximum snapshots to be kept at each of these locations.
- If you have configured CHAP on the volumes where the Nimble Storage resides, you must provide the CHAP credentials for the DS-Client to use. You can only provide one set of CHAP credentials for each Microsoft SQL Server (VSS-aware) backup. All volumes added to the backup must be configured with the same set of CHAP credentials.

5.17.1.1 Restoring a full database from Nimble Storage

When a Microsoft SQL Server (VSS-aware) backup has been integrated with Nimble Storage, you can restore a full database from the hardware snapshots on the Nimble Storage array.

If you are restoring a full database from a production Nimble Storage and want to automatically establish the connection between the Microsoft SQL Server host and the production Nimble Storage where the hardware snapshot is stored, select the **Use automount for restore** option in the Restore Now Wizard.

If you are restoring a full database from a Nimble Storage replication partner, you must do the following before starting the restore process:

- In the Nimble Storage Management Console, set the snapshot online. This refers to the snapshot from which you want to restore the full database.
- Connect the hardware snapshot from the Nimble Storage to the Microsoft SQL Server host via the iSCSI initiator.
- If the volume containing the hardware snapshot is configured with CHAP, you must provide the required credentials.
- In the Microsoft SQL Server host, mark the disk online and assign a drive letter to the disk. This refers to the disk that contains the target database in the Microsoft SQL Server host.

Like other Microsoft SQL Server backups, a Microsoft SQL Server (VSS-aware) backup that is integrated with Nimble Storage can be used in combination with another Microsoft SQL Server (Classic) backup configured with the Transaction Log Only database backup policy. For more information, see Section 5.3.5, “Restoring transaction logs only (Microsoft SQL)”, on page 131.

5.17.1.2 Nimble storage limitations

The following limitations apply to Nimble Storage integration with Microsoft SQL Server (VSS-aware) backups:

- Full dump always is the only database backup policy that supports integration with Nimble Storage for Microsoft SQL Server (VSS-aware) backups.
- The automount option for restoring from Nimble Storage snapshots is supported for restoring from the production Nimble Storage only.
- When the production Nimble Storage contains multiple partitions, the automount option for restoring a full database from Nimble Storage snapshots is not supported.

5.17.2 Creating a Microsoft SQL Server (VSS-aware) backup

You can create a Microsoft SQL Server (VSS-aware) backup.

- If the Microsoft SQL Server is running on a remote machine or the DS-Client is running in a Docker container, you might need to add the Microsoft SQL Server IP address and host name to the hosts file on the DS-Client. The default path is: `C:\Windows\System32\drivers\etc\hosts`
- To create a backup of a Microsoft SQL Server Always On Availability Group, type the name or IP address of the Availability Group Listener. DS-Client will automatically detect this type of configuration and display all databases that are currently in the Availability Group.
- For Microsoft SQL Server Clusters, type the virtual node in the **Path** box. The DS-Client must be able to connect to all the nodes and resolve the virtual node (IP address), all individual nodes (names and IP addresses), and the Windows cluster's name (IP address).

NOTE: If you plan to integrate a Microsoft SQL Server backup with Nimble Storage, see Section 5.17.1, "Integrating with Nimble Storage", on page 398.

5.17.2.1 Selecting the type of backup

1. On the **Sets** menu, click **New Backup Set**.
2. Select **VSS-aware Backup Set**, and then click **Next**.
3. Select **Microsoft SQL Server**, and then click **Next**.

5.17.2.2 Selecting the backup source

IMPORTANT: For a VSS aware backup, remote UAC is enabled by default. The local administrator account must have access to the admin$ share on the source machine.

---

1. Select the computer with the Microsoft SQL Server.
2. By default, the **Ask for Network Credentials** checkbox is selected.
3. In the **Enter Network Credentials** dialog box, type the credentials to the target computer, and then click **OK**.
4. Click **Next**.

5.17.2.3 Selecting the components to back up

1. Add the items you want to backup.
2. To exclude an item when its parent directory is selected for backup, select the item, and then click **Exclude**.
3. To remove an item from the list of selected items for backup, select the item, and then click **Remove**.
4. Click **Next**.

5.17.2.4 Selecting the backup item options

1. To configure the maximum generations for a backup item that will be stored online, double click the **Max Gen** cell, and then enter the value.
2. To back up file permissions for an item, select the item, and then select the **Back up permissions** check box.
3. To back up the streams of data associated with an item, select the item, and then select the **Back up streams** check box.
4. Click **Next**.

NOTE: Microsoft does not support VSS-aware transaction log backups. If you need a transaction log backup, use SQL Server Management Studio or the Microsoft SQL Server (Classic) backup. For more information, see Section 5.16, “Microsoft SQL Server (Classic) backups (Windows)”, on page 382.

5.17.2.5 Selecting the backup options

NOTE: A VSS-aware backup of a Microsoft SQL Server's master database does not support the Full dump: Plus differential database backup policy.

1. Configure the options for the backup. The options are as follows:

   - **Detailed log** – Records all files that are backed up in the Activity Log. For more information, see Section 8.1, "Viewing the Activity Log", on page 578.
   - **Initial backup** – Uses the Initial Backup feature for the first backup. To configure the initial backup path, click **[>>]**. For more information, see Section 11.1.1, "Configuring the initial backup path", on page 618.
   - **Stop on errors** – Stops a backup process when the number of errors reaches the specified value. A value of 0 means the DS-Client does not stop a backup process regardless of the number of errors.

     NOTE: You can configure the default setting using the **MaxErrors** advanced configuration parameter. For more information, see Section 2.1.8.6, "Miscellaneous parameters (Windows)", on page 42.

   - **Nimble Storage Integration Settings** – Select this check box to configure the Nimble Storage integration settings. For more information, see Section 5.17.1, "Integrating with Nimble Storage", on page 398. In the **Nimble Storage Integration Settings** dialog box, do the following:

     1. To back up data using the default system VSS provider that is available, select the **If Nimble snapshot fails, use default provider** check box, in case attempts to use the VSS Nimble provider fail.
     2. In the **IP address** box, type the management IP address of your Nimble Storage Array.
     3. In the **Port number** box, type the management port number of your Nimble Storage Array. The default is 5392.
     4. In the **User name** box, type a valid user name for DS-Client to access the Nimble Storage Array Management IP via REST API.
     5. In the **Password** box, type the associated password for DS-Client to access the Nimble Storage Array Management IP via REST API.
     6. In the **Retention ... snapshots to keep** box, enter the maximum number of snapshots to be retained by DS-Client on the production Nimble Storage for the backup.
     7. To enable hardware snapshots to be replicated to a Nimble Storage replication partner, select the **Enable Replication** check box.

8. If you have selected **Enable replication**, enter the maximum number of snapshots that you want the Nimble Storage replication partner to retain.
9. If you have selected **Enable replication**, type the name or IP address of the replication partner on which you want hardware snapshots to be replicated.
10. To enable the backup of a Nimble Storage configured with CHAP log on, select the **Enable CHAP log on** check box, and then type the required credentials.

- **VSS validation** – Specifies the type of VSS validation that will be applied prior to performing the backup. The options are as follows:
  - **Disable** – VSS validation is not performed.
  - **Enable** – VSS validation is performed.
  - **Use DS-Client's settings** – VSS validation is performed using the DS-Client settings.
- **Compression type** – Specifies the type of compression that will be applied to the backup. The options are as follows:
  - **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good default compression when the network is not the bottleneck.
  - **ZLIB (Global, Low, Medium, and High)** – Normally produces better compression than LZOP, but will take more time to compress. This is a good default compression when the bottleneck is the network. ZLIB Low corresponds to a value of 3, ZLIB Medium = 6, and ZLIB High = 9.
  - **None** – Disables compression for the backup.

2. Under **Database backup policy**, in the **Full dump** box, select a method for the full dump. The options are as follows:
   - **Always** (Default) — Performs a full dump (VSS snapshot) of each database.
   - **Plus Differential** — Performs a full dump (VSS snapshot) of the database on first backup, followed by differential backups until another full backup is required (*). Differential backups contain all the changes to the database since the last full dump.

   (*) A full dump is needed (other than first time) when:

   - A database has been backed up by another backup (or manually from the SQL tools).
   - A database has been restored (either from another database or an earlier generation).

- The database properties have been modified (recovery model switched to ‘simple’).
- A set number of consecutive differential backups have been performed, unless over-ruled with the **Do not start full dump** option. This uses the same number set in the **MasterGenerations** advanced parameter (note this parameter is also used for another purpose). For more information, see Section 2.1.8, “Configuring the advanced settings”, on page 37.

d) For greater control of when the full dump occurs (for example, outside of business hours) you can delay or force a full dump by configuring the frequency.

IMPORTANT: You must perform Full dumps at a regular frequency to protect the integrity of the database backup. By default, DS-Client allows a full backup to be skipped a maximum of 120 consecutive times. This number is configurable using the **MaxNonFullDumps** advanced parameter.

For more information about database backup policy options, see Section 5.1, “Backup types”, on page 106.

e) To specify a command to run before (Pre) and/or after (Post) the execution of the backup, click **Pre/Post**. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525.

3. Click **Next**.

5.17.2.6 Specifying backup performance options

IMPORTANT: These options are intended for high performance environments where the DS-Client can take advantage of the speed of the storage where the source data resides. Test different settings to determine the optimal value. Slower storage can result in performance issues if the values are not properly configured.

---

1. Under **Maximum pending asynchronous I/O for a file**, configure the maximum I/O operations the DS-Client will use for each file from the backup.

NOTE: This setting is for storage devices that support better parallel disk I/O, such as NAS devices. The optimal setting for this value depends on the storage device and network speed. Increasing this value can significantly increase the backup speed. If your storage device does not support better parallel disk I/O, use the default value, otherwise the performance can be significantly degraded.

- To use the default **MaxPendingIOPerFile** advanced configuration parameter, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
- To override the default setting with a custom value that only applies for the backup, click **Use specific value**, and then enter the value.

2. Under **Read buffer size for backup**, configure the internal buffer size (in KB) for reading a file during the backup process.
   - To use the default **FileReadBufferSize** advanced configuration parameter, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific buffer size (KB)**, and then enter the value.

IMPORTANT: To achieve optimum backup performance, the DS-Client read buffer size might need to be different, depending on the combination of the target storage device, target operating system, and any mid-ware involved between the storage and the operating system.

---

3. Click **Next**.

5.17.2.7 Selecting the notification options

1. To configure a notification, do one of the following:
   - To add a notification, click **Add.**
   - To modify a notification, select the notification, and then click **Modify.**

NOTE: To delete a notification, select the notification, and then click **Delete**.

---

2. To send an email notification, select **E-Mail**. and then do the following:
   a) To send the email notification to the DS-Client administrator, select **Administrator**.
   b) To send an email to another recipient, select **Other**, and then specify the recipients email address.
   c) To send detailed backup information, select the **Detailed notification** check box.
   d) To include a detailed file-level backup log as an attachment, select the **Attach detail log** check box.
   e) To send the email notification in HTML format, select the **Send E-Mail using HTML format** check box.

f) Click **OK**.

NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

---

3. To send a pager notification, select **Pager**. The notification will be sent to the pager account configured for the DS-Client.

NOTE: The pager option is available only if the DS-Client has been configured for pager notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

---

4. To send a broadcast notification, select **Broadcast**. Select the server containing the messenger service to which you want to send the message and click **OK**.

NOTE: Broadcast notifications to domains or workgroups are limited to 128 characters.

---

5. To send an event notification, elect **Event**. Select the server on which you want the notification to be recorded in the Event Log.
6. In the **Completion** box, specify under what conditions a notification will be sent, and click **OK**. The options are as follows:
   - **All** – Notification will be sent under all conditions.
   - **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
   - **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.
   - **Completed with errors** – Notification will be sent if an activity is completed with at least one error event.
   - **Incomplete** – Notification will be sent if an activity is not completed successfully.
7. Click **Next**.

5.17.2.8 Assigning a retention rule

1. To assign a retention rule to the backup, do one of the following:
   - If you don't want to assign a retention rule, select **No retention rule**.
   - To assign a retention rule, select **Use a specific retention rule**, and then select the retention rule.

NOTE: To create or edit a retention rule, click **[...]**. For more information, see Section 4.1, "Configuring a retention rule", on page 98.

---

2. Click **Next**.

5.17.2.9 Assigning a schedule

1. To assign a schedule to the backup, do one of the following:
   - If you don't want to assign a schedule, select **Not scheduled**.
   - To assign a schedule, select **Scheduled.** In the **Available schedules** box, select an existing schedule.

NOTE: To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, "Configuring a schedule", on page 90.

---

2. Click **Next**.

5.17.2.10 Naming the backup

1. In the **Set name** box, type a name for the backup.
2. In the **Set type** box, select the type of backup you want to create. The list of available backup types depends on the configuration of your DS-Client.
   - Online
   - Self-contained
   - Local-only
   - Instant Recovery
   - Statistical

NOTE: For more information, see Section 5.1, "Backup types", on page 106.

---

3. If you selected **Online**, do the following:

   a) To send a copy of the oldest generation of the file that is about to be overwritten from the DS-System to the BLM Archiver, select the **BLM (Infinite Generations)** check box.

   NOTE: The Backup Lifecycle Management tool must be enabled for the DS-Client.

   b) To save a copy of the backup data to a local storage location on the DS-Client computer, select the **Save on Local Storage** check box.

   NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Self-contained and Local Only backups.

   c) To use the local storage as a cache if the DS-Client loses connection with the DS-System, select the **Transmission cache on Local Storage** check box. The cached backup data will be sent to the DS-System on the next connection after synchronization.

   NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path.

   d) To save a copy of the backup data to the instant recovery vault, select the **Save in instant recovery vault** check box.

   NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Instant Recovery backups.

   e) If you selected **Save in instant recovery vault**, beside the **Local Storage Path** box, click **>>**. Enter a local storage path for the backup, and then click **OK**.

   NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

4. If you selected **Self-Contained**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

5. If you selected **Local-Only**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**..

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

6. If you selected **Instant Recovery**, the **Save in instant recovery vault** option is selected by default.

IMPORTANT: Each Linux DS-Client must have a unique ZFS file name.

---

7. If you selected **Statistical**, and want to emulate an actual backup transfer process, select the **Calculate transmit amount** check box. During the backup, specified backup files will be read from their source and processed for compression and encryption.
8. Click **Finish**.

5.17.3 Performing a database restore

You can perform a database restore to restore the selected backup session to the original backup source or an alternate location.

IMPORTANT: Before you restore a database of an Always On Availability Group, you must remove the target database from the Availability Group. After a successful restore, you can add the database back to the Availability Group. For more information, see the *Microsoft SQL Server* documentation.

5.17.3.1 Selecting the restore method

1. Browse the backups tree and select the backup you want to restore.
2. On the **Restore** menu, click **Restore Now**.
3. Select **Database Restore**.
4. Click **Next**.

5.17.3.2 Selecting the restore items

1. To restore an entire backup or folder, browse the tree and select the check box beside the backup or folder you want to restore.
2. To restore individual files, select the folder containing the required files, and then click **Show Files**. Under **File List**, do the following:
3. To view the number of files selected and calculate the total amount of files selected, select the **Calculate amount** check box.
4. To exclude subdirectories, clear the **Include SubDirs** check box, as the default setting is to include sub-directories.
5. To filter the list of files, in the **Filter box**, enter a filter using * as a wildcard, and then click **Show Files** to update the list of files.
6. To find a backed up file, click **Show Files**.
7. In the **Files List** section, do one of the following:
   - To view details about the backed up file, select the file, and then click **File Info**.
   - To view the details of the items you selected, click **Selection**.
   - To view a list of archived generations for a folder, do the following:
     a) In the **Database Tree**, select the folder, and then click **Show Files**.
     b) Under **Files**, click **Show Archived**.
   - To view the files that are part of the selected VSS component, click **VSS Component**.
8. To refine your selection of items to restore, click **Advanced**. Under **Show**, select which generation you want to display. The options are as follows:
   a) To restore the latest generation of all the files, select **Latest generation of all data**.
   b) To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:

1. Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.
2. Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.

c) Click **OK**.

9. Click **Next**.

5.17.3.3 Selecting the restore location

VSS-aware backups use the Microsoft VSS (Volume Shadow Copy Service) writers on the target restore computer to perform the restore.

NOTE: When restoring a Microsoft SQL Server (VSS-aware) backup to an alternate location, the destination must have the same instance name as the source.

---

1. Select the location to which you want to restore the backup. The options are as follows:
   - **Original location** – Data is restored to the original backup source location and existing files with the same name are overwritten. This is the default option.
   - **Alternate location** – Data is restored to a location other than the original backup source.

   NOTE: When restoring to an alternate location, the security of restored items in the destination location might not resemble the security of those items during backup.

   ---

2. If you selected **Alternate location**, then do the following:
   a) Beside the **Alternate location** box, click **[>>]**.
   b) In the **Select Alternate Server** dialog box, select the computer where you want to restore the data.
   c) To specify alternate network credentials, select the **Ask for Network Credentials** checkbox, and then click **Select**.
   d) In the **Enter Network Credentials** dialog box, enter the credentials to connect to the destination computer, and then click **OK**.
   e) To rename the individual components being restored, click **Rename component**, and then in the **Rename Component** dialog box, do the following:

1. Double click in the **Target Component** column and edit the name or path for the component.
2. To load mapping contents from a saved XML file, click **Load XML**.

NOTE: A mapping is loaded only if the logical path and the source component columns from the XML file exactly match with those displayed in the list.

---

3. To save the contents from the current source target mapping list to an XML file, click **Save XML**.
4. Click **OK**.

3. Click **Next**.

5.17.3.4 Selecting the performance options

IMPORTANT: These options are intended for large backups in high performance environments where the DS-Client can take advantage of the speed of the storage where the source data resides. Test different settings to determine the optimal value. Slower storage can result in performance issues if these values are not configured correctly.

---

1. Under **Maximum pending asynchronous I/O for a file**, configure the maximum number of I/O operations the DS-Client will use for each file during the restore process.
   - To use the default MaxPendingIOPerFile advanced configuration parameter setting, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value** and then enter the value.
2. Under **DS-System side read threads**, configure the number of files the DS-System can read simultaneously for the restore process.
   - To use the default MaxRestoreReadThreads advanced configuration parameter setting, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value** and then enter the value.
3. Click **Next**.

5.17.3.5 Selecting the restore options

1. Under **Restore options,** do the following:

   a) To record all restored files in the Activity Log, select the **Detailed log** check box.

   b) To skip the pre and post restore processes, select the **Skip Pre/Post** check box. If this check box is clear, click **Pre/Post**. DS-Client will run a specified activity before and/or after a restore operation. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525.

   c) To retain the database in restoring mode after the restore is complete, select the **Leave Database(s) in ‘RESTORING’ state** check box. DS-Client will not bring the database online.

2. Click **Next**.

5.17.3.6 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, under **Restore classification**, select the type of restore. The options are as follows:

   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.

3. Click **Finish**.

5.17.4 Performing a file restore

You can perform a file restore to selectively restore individual files from a backup session. This is a pure file restore, which can be used by the corresponding Microsoft management tools.

To restore a Microsoft SQL Server database to an alternate location, you must first restore the database files as pure files:

- Browse and select the folders and files you want to restore. You need the *.ldf and *.mdf files to restore a Microsoft SQL Server database from pure files.
- After the pure files have been restored, you can use Microsoft SQL Management Studio to attach the databases to the destination Microsoft SQL Server instance.For more information, see the Microsoft SQL Server documentation for further instructions.

If the backup uses the Full dump: Plus Differential database backup policy, there is an additional differential file (*.mdf.diff) that is saved in a format that only the DS-Client can use. You must do the following:

1. Restore the .mdf, .mdf.diff, and .ldf database files to the same folder.
2. As a Windows administrator, copy the VssDiffApply.exe file from the \Software\Tools\MS_SQL_Differential_Merge\ folder to the same folder.
3. Merge the .mdf and .mdf.diff files for the database using the following command:

   ```
   VssDiffApply.exe [/y] <.mdf file> <.mdf.diff file>
   ```

4. Attach the .mdf database file to the Microsoft SQL Server instance using SQL Management Studio.

5.17.4.1 Selecting the restore method

1. Browse the backups tree and select the backup you want to restore.
2. On the **Restore** menu, click **Restore Now**.
3. Select **File Restore**.
4. Click **Next**.

5.17.4.2 Selecting the restore items

1. To restore an entire backup or folder, browse the tree and select the check box beside the backup or folder you want to restore.
2. To restore individual files, select the folder containing the required files, and then click **Show Files**. Under **File List**, do the following:
3. To view the number of files selected and calculate the total amount of files selected, select the **Calculate amount** check box.
4. To exclude subdirectories, clear the **Include SubDirs** check box, as the default setting is to include sub-directories.
5. To filter the list of files, in the **Filter box**, enter a filter using * as a wildcard, and then click **Show Files** to update the list of files.
6. To find a backed up file, click **Show Files**, and then do one of the following:
   - To view details about the backed up file, select the file, and then click **File Info**.
   - To view the details of the items you selected, click **Selection**.
   - To view a list of archived generations for a folder, do the following:
     a) In the **Database Tree**, select the folder, and then click **Show Files**.
     b) Under **Files**, click **Show Archived**.
7. To refine your selection of items to restore, click **Advanced**. Under **Show**, select which generation you want to display. The options are as follows:
   a) To restore the latest generation of all the files, select **Latest generation of all data**.
   b) To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:
      1. Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.
      2. Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.
   c) Click **OK**.
8. Click **Next**.

5.17.4.3 Selecting the restore location

VSS-aware backups use the Microsoft VSS (Volume Shadow Copy Service) writers on the target restore computer to perform the restore.

NOTE: When restoring a Microsoft SQL Server (VSS-aware) backup to an alternate location, the destination must have the same instance name as the source.

Select the destination where you want to restore the backed up data.

To select the restore location:

1. Select the location to which you want to restore the backup. The options are as follows:
   - **Original location** – Data is restored to the original backup source location and existing files with the same name are overwritten. This is the default option.
   - **Alternate location** – Data is restored to a location other than the original backup source.

     NOTE: When restoring to an alternate location, the security of restored items in the destination location might not resemble the security of those items during backup.

2. If you selected **Alternate location**, then do the following:
   a) Beside the **Alternate location** box, click **[>>]**.
   b) In the **Select Alternate Server** dialog box, select the computer where you want to restore the data.
   c) To specify alternate network credentials, select the **Ask for Network Credentials** checkbox, and then click **Select**.
   d) In the **Enter Network Credentials** dialog box, enter the credentials to connect to the destination computer, and then click **OK**.

   NOTE: After you select a computer as the alternate location, you must specify a share location.

   e) In the **Destination** cell, select a share location.
   f) Click in the **Restore to** cell, and type the name of the directory or click **[>>]** and select a directory.

g) In the **Truncate** box, you can increase the truncate level to shorten the common portion of the restore path, if the selected restore items contain a common path.

NOTE: If the entire path is truncated, the alternate location directory will inherit the security of the truncated parent directory.

3. Click **Next**.

5.17.4.4 Selecting the performance options

IMPORTANT: These options are intended for large backups in high performance environments where the DS-Client can take advantage of the speed of the storage where the source data resides. Test different settings to determine the optimal value. Slower storage can result in performance issues if these values are not configured correctly.

1. Under **Maximum pending asynchronous I/O for a file**, configure the maximum number of I/O operations the DS-Client will use for each file during the restore process.
   - To use the default MaxPendingIOPerFile advanced configuration parameter setting, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value** and then enter the value.
2. Under **DS-System side read threads**, configure the number of files the DS-System can read simultaneously for the restore process.
   - To use the default MaxRestoreReadThreads advanced configuration parameter setting, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value** and then enter the value.
3. Click **Next**.

5.17.4.5 Selecting the restore options

1. Under Permissions, select a restore option for permissions. The options are as follows:
   - **Yes** – Restores the permissions for all the backed up files.
   - **Skip** – Skips the file security information of the backed up files. Newly created files and folders inherit the security settings of the parent folder.
2. Under **Method**, select a method for the DS-Client to perform the restore. The options are as follows:
   - **Save** – Restores files to a temporary location first to prevent restored files from overwriting an existing file. If the file is restored successfully, the original file is overwritten with the temporary file.
   - **Use buffer** – Restores files to the DS-Client buffer first and then transfers the files to the restore destination. This method minimizes the duration for which the restore process occupies the destination server.
   - **Fast** – DS-Client uses a direct restore method, writing data as it is received.

   NOTE: If you select the **Fast** method, files in the destination location are overwritten upon receipt of the first byte of data.
3. To record all restored files in the Activity Log, select the **Detailed log** check box.
4. To skip the pre and post restore processes, select the **Skip Pre/Post** check box. If this check box is clear, click **Pre/Post**. DS-Client will run a specified activity before and/or after a restore operation. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525.
5. Click **Next**.

5.17.4.6 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, under **Restore classification**, select the type of restore. The options are as follows:
   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.
3. Click **Finish**.

5.18 Oracle database backups (Windows or Linux)

You can back up and restore data from an Oracle database on a scheduled or on-demand basis.

When you perform a backup, the DS-Client instructs the Oracle's Recovery Manager (RMAN) to access the Oracle database and use the Oracle-supplied functions via Pipe or using dump files. The data is then compressed, encrypted and transmitted to the DS-System.

The first time the backup process is performed, the entire database is dumped and transmitted to create a master. During subsequent backups, only the changes are transmitted to create a delta. The DS-Client never accesses the Oracle database files directly, so there is never an issue with open and locked database files. The database does not have to be taken off-line to perform the backup.

During the Oracle database backup, the database credentials (sysdba username and password) are entered and stored in the DS-Client database using AES128 encryption. The backup data is secured with up to AES-256 strength encryption using a private key known only to you. Your service provider will never have access to this information. The DS-System uses a one-way hash to validate encryption keys, however the hash cannot be used to recover the encryption keys.

5.18.1 General requirements

- You must have knowledge of the Oracle database file structure and instance management to use Oracle database backups.
- When creating a new backup, you must know the exact name of the Oracle service because you cannot browse for the database.
- The credentials used for the backup and restore of the Oracle database must have the sysdba privilege.
- For offline database backup and restore, the operations and requirements are the same as a File system backup and restore. You can use the Pre/Post function to stop and start the Oracle database before and after backup and restore. If your database is in NOARCHIVE mode, you must perform an offline backup of the database. For more information, see Section 5.2.6, “Pre/Post backup processes”, on page 113.

5.18.2 DS-Client computer requirements

- You must install the Recovery Manager (RMAN) utility on the DS-Client computer.
- You must install a full Oracle client on the DS-Client computer that performs the backup and restore of the target Oracle database.
- The Oracle client must be the same version as the Oracle database you want to back up. If you want to back up different versions of the Oracle database, you must install each corresponding version of the Oracle client on the DS-Client computer.
- Configure the Net service Name for the Oracle client to connect to each Oracle database you want to back up or restore. If the Oracle instance is a shared server, set the Connection Type as Dedicated Server. This is the TNS alias that is specified in the tnsnames.ora file on your Oracle client.
- Configure a separate Net service Name to access the Oracle database at the CDB-level or PDB-level. The CDB-level provides access to the entire container database (Root and all pluggable databases). The PDB-level provides access only to the specified pluggable database.
- For Linux DS-Clients, configure the remote Oracle database server host name in the /etc/hosts file on the Linux DS-Client computer.

5.18.3 Oracle database requirements

- Ensure the Oracle database is a certified product.
- Ensure the Oracle instance is running in ARCHIVELOG MODE. This allows for an online backup of the database.
- Set the CONTROL_FILE_RECORD_KEEP_TIME parameter to slightly longer than the period between backups of the entire Oracle database.
- Increase the “redo log file” size to reduce the number of archived logs. RMAN has a limitation of how many archived logs can be backed up at a time.
- For Windows DS-Clients, do the following:
  - Copy the orasbt_x64.dll file to the target Oracle database computer. Rename the file to orasbt.dll and place it in the System Root path (\%SYSTEMROOT%\SYSTEM32). You can find this file in the DS-Client installation folder.
  - If you are using the DS-Client Buffer or pipe as the dump path for the backup, ensure both the OracleServiceXXXX and Oracle TNSListener services use the administrator account. The Oracle database user must be a member of the Administrators Group on the Windows operating system.
- For Linux DS-Clients, to use DS-PIPE for backup and restore, a library file must be copied to $ORACLE_HOME/lib on the Oracle server. This file must correspond to the Oracle platform and can be found in the /Misc/Oracle_Classic_Library subfolder of the DS-Client installation folder.
  - **libobk-64.so** — Copy this file to $ORACLE_HOME/lib on the Linux Oracle Server and make a soft link with the following command:

    ```
    ln -s libobk-64.so libobk.so.
    ```

5.18.4 Backup requirements

- When performing an online backup, the Oracle database must be in Open state.
- When performing backups, you do not need to place online tablespaces in backup mode.
- By default, threaded execution is disabled on the Oracle database. If enabled, a DS-Client using DS-PIPE will fail to back up the control file.
- For Linux DS-Clients, when performing an Oracle backup using the NFS protocol, you must enter the user account of root for the network credentials.

5.18.5 Restore requirements

- When performing a full or alternate restore of an Oracle database, the backup must be a full Oracle database backup and the password and init files should be backed up in a File system backup.
- To restore the control file, start the database in nomount (started) state.
- To restore tablespaces without the control file, start the database in mount state. Otherwise, change the tablespaces offline.
- The control file should only be restored when performing DBPITR (Database Point In Time Recovery). After restoring, the database will be opened with the RESETLOGS option. By doing this, you will not be able to restore any tablespaces backed up after that point in time unless you restore the control file.
- Tablespaces can be restored, but the logs will be applied to the present database (unless DBPITR is performed), which means they will not be the same as when they were backed up.
- When performing a DBPITR, all the files backed up in a particular session must be restored.
- For a full restore to the original location, the target computer is the original computer.
- Before performing a DBPITR, if the backup and flash_recovery_area have different reset log times, you must rename the flash_recovery_area folder. After performing the restore, shutdown and manually restart the Oracle database.
- When performing a restore to an alternate location, ensure the following:
  - The target restore computer must have an Oracle database service instance with the same name. This simplifies the process of recovery. If you use a different instance name, you must modify the initial file manually.
  - The target restore computer must have the same tablespace path as the original backup which can be created when setting up the database. All information about file structure is recorded in the control file and the Oracle database as a whole.
  - You must restore the File system backup of the password file and the init file to the alternate computer. This is a separate backup of the password file and the init file from the original backup computer.
- You must restore the full Oracle database backup. If you choose a different dump path, only dump files are restored to that path. You must use RMAN to manually restore the Oracle database.

5.18.6 Creating an Oracle database backup (Windows)

You can create an Oracle database backup using a Windows DS-Client.

5.18.6.1 Selecting the type of backup

1. On the **Sets** menu, click **New Backup Set**.
2. Select **Oracle Server**, and then click **Next**.

5.18.6.2 Selecting the Oracle server

1. Browse and select the server you want to back up. For Oracle on Windows, expand the Microsoft Windows network tree.
2. By default, DS-Client uses the current user's logon credentials to connect to the selected computer. To provide credentials for the selected computer, select the **Ask for Network Credentials** check box. You will be prompted to enter a valid user name and password for the selected computer.
3. The **Ask for database credentials** check box is selected by default. Click **Next**.
4. In the **Enter database credentials** dialog box, do the following:
   a) In the **User name** and **Password** boxes, type the credentials required to connect to the selected database server.
   b) In the **Service Name** box, type the name of the Oracle service you want to back up. The Service Name is the TNS alias that is specified in the tnsnames.ora file on your Oracle client.

   NOTE: If you supply the service name defined at CDB-level, you can browse the entire container database (Root and all pluggable databases). If you supply the service name defined at PDB-level, you can browse that specific pluggable database only.

   c) Click **OK**.
5. Click **Next**.

5.18.6.3 Selecting the database dump options

1. Select a path to save the database dump. The options are as follows:

   NOTE: Ensure that the Oracle Server has read and write privileges to this dump path.

   - **Dump path** – Save the dump file to a path on the Oracle server.
   - **DS-Client Buffer** – Save the dump file to the local storage on the DS-Client computer.
   - **DS-Client Pipe** – During backup, the DS-Client reads from the pipe on the source database. This method is useful if the database is too large to be dumped to a file on either the database server or the DS-Client buffer.

2. Click **Next**.

5.18.6.4 Selecting the database(s) for backup

1. Do one of the following:
   - To add an entire Oracle database, select the root folder from the databases list, and then click **Add**.
   - To select individual items, browse the database list, select the required items, and then click **Add**.
   - To remove a database, select the database under **Backup Items Selected**, and then click **Remove**.
2. Click **Next**.

5.18.6.5 Selecting the backup item options

1. To configure the maximum generations for a backup item that will be stored online, double click the **Max Gen** cell, and then enter the value.
2. To back up only the logs that are necessary for the database, select the **Backup Only Current Archived Logs** check box.
3. To clear the archive logs associated with the items after the backup, select the **Truncate Archived Logs** check box.
4. Click **Next**.

5.18.6.6 Selecting the backup options

1. Configure the options for the backup. The options are as follows:
   - **Detailed log** – Records all files that are backed up in the Activity Log. For more information, see Section 8.1, “Viewing the Activity Log”, on page 578.
   - **Initial backup** – Uses the Initial Backup feature for the first backup. To configure the initial backup path, click **[>>]**. For more information, see Section 11.1.1, “Configuring the initial backup path”, on page 618.
   - **Stop on errors** – Stops a backup process when the number of errors reaches the specified value. A value of 0 means the DS-Client does not stop a backup process regardless of the number of errors.

     NOTE: You can configure the default setting using the **MaxErrors** advanced configuration parameter. For more information, see Section 2.1.8.6, “Miscellaneous parameters (Windows)”, on page 42.

   - **Compression type** – Specifies the type of compression that will be applied to the backup. The options are as follows:
     - **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good default compression when the network is not the bottleneck.
     - **ZLIB (Global, Low, Medium, and High)** – Normally produces better compression than LZOP, but will take more time to compress. This is a good default compression when the bottleneck is the network. ZLIB Low corresponds to a value of 3, ZLIB Medium = 6, and ZLIB High = 9.
     - **None** – Disables compression for the backup.
2. To specify a command to run before (Pre) and/or after (Post) the execution of the backup, click **Pre/Post**. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525 and Section 5.26, “Configuring Pre/Post processes (Linux)”, on page 528.
3. Click **Next**.

5.18.6.7 Specifying backup performance options

IMPORTANT: These options are intended for high performance environments where the DS-Client can take advantage of the speed of the storage where the source data resides. Test different settings to determine the optimal value. Slower storage can result in performance issues if the values are not properly configured.

1. Under **Maximum pending asynchronous I/O for a file**, configure the maximum I/O operations the DS-Client will use for each file from the backup.

   NOTE: This setting is for storage devices that support better parallel disk I/O, such as NAS devices. The optimal setting for this value depends on the storage device and network speed. Increasing this value can significantly increase the backup speed. If your storage device does not support better parallel disk I/O, use the default value, otherwise the performance can be significantly degraded.

   - To use the default **MaxPendingIOPerFile** advanced configuration parameter, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value**, and then enter the value.

2. Under **Read buffer size for backup**, configure the internal buffer size (in KB) for reading a file during the backup process.

   - To use the default **FileReadBufferSize** advanced configuration parameter, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific buffer size (KB)**, and then enter the value.

   IMPORTANT: To achieve optimum backup performance, the DS-Client read buffer size might need to be different, depending on the combination of the target storage device, target operating system, and any mid-ware involved between the storage and the operating system.

3. Click **Next**.

5.18.6.8 Selecting the notification options

1. To configure a notification, do one of the following:
   - To add a notification, click **Add.**
   - To modify a notification, select the notification, and then click **Modify.**

   NOTE: To delete a notification, select the notification, and then click **Delete**.

2. To send a broadcast notification, select **Broadcast**. Select the server containing the messenger service to which you want to send the message and click **OK**.

   NOTE: Broadcast notifications to domains or workgroups are limited to 128 characters.

3. To send an event notification, select **Event**. Select the server on which you want the notification to be recorded in the Event Log.
4. In the **Completion** box, specify under what conditions a notification will be sent, and click **OK**. The options are as follows:
   - **All** – Notification will be sent under all conditions.
   - **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
   - **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.
   - **Completed with errors** – Notification will be sent if an activity is completed with at least one error event.
   - **Incomplete** – Notification will be sent if an activity is not completed successfully.
5. Click **Next**.

5.18.6.9 Assigning a retention rule

1. To assign a retention rule to the backup, do one of the following:
   - If you don't want to assign a retention rule, select **No retention rule**.
   - To assign a retention rule, select **Use a specific retention rule**, and then select the retention rule.

NOTE: To create or edit a retention rule, click **[...]**. For more information, see Section 4.1, "Configuring a retention rule", on page 98.

---

2. Click **Next**.

5.18.6.10 Assigning a schedule

1. To assign a schedule to the backup, do one of the following:
   - If you don't want to assign a schedule to the backup, select **Not scheduled**.
   - To assign a schedule to the backup, select **Scheduled.** In the **Available schedules** box, select an existing schedule.

NOTE: To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, "Configuring a schedule", on page 90.

---

2. Click **Next**.

5.18.6.11 Naming the backup

1. In the **Set name** box, type a name for the backup.
2. In the **Set type** box, select the type of backup you want to create. The list of available backup types depends on the configuration of your DS-Client.
   - Online
   - Self-contained
   - Local-only
   - Statistical

NOTE: For more information, see Section 5.1, "Backup types", on page 106.

---

3. If you selected **Online**, do the following:

a) To send a copy of the oldest generation of the file that is about to be overwritten from the DS-System to the BLM Archiver, select the **BLM (Infinite Generations)** check box.

NOTE: The Backup Lifecycle Management tool must be enabled for the DS-Client.

---

b) To save a copy of the backup data to a local storage location on the DS-Client computer, select the **Save on Local Storage** check box.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Self-contained and Local Only backups.

---

c) To use the local storage as a cache if the DS-Client loses connection with the DS-System, select the **Transmission cache on Local Storage** check box. The cached backup data will be sent to the DS-System on the next connection after synchronization.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

4. If you selected **Self-Contained**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

5. If you selected **Local-Only**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

6. If you selected **Statistical**, and want to emulate an actual backup transfer process, select the **Calculate transmit amount** check box. During the backup, specified backup files will be read from their source and processed for compression and encryption.

7. Click **Finish**.

5.18.7 Creating an Oracle database backup (Linux)

You can create an Oracle database backup using a Linux DS-Client.

5.18.7.1 Selecting the type of backup

1. On the **Sets** menu, click **New Backup Set**.
2. Select **Oracle Server**, and then click **Next**.

5.18.7.2 Selecting the backup source

1. In the **Path** box, type the IP address of the Oracle server in the following format:

   `Oracle Server\<IP Address>`
2. The **Ask for database credentials** check box is selected by default. Click **Next.**
3. In the **Enter Database Credentials** dialog box, do the following:

   a) In the **User name** and **Password** boxes, type the credentials required o connect to the selected database server.

   b) In the **Service Name** box, type the name of the Oracle service you want to back up. The Service Name is the TNS alias that is specified in the tnsnames.ora file on your Oracle client.

   NOTE: If you provide the service name defined at CDB-level, you can browse the entire container database (Root and all pluggable databases). If you provide the service name defined at PDB-level, you can browse that specific pluggable database only.

4. Click **OK**.

5.18.7.3 Selecting the protocol for the database dump

1. Select the protocol you want to use for this backup. The options displayed depend on your network configuration or the target Oracle server that is selected.
   - **DS-PIPE** – During backup, DS-Client reads from the pipe on the source database. This method is useful if the database is too big to be dumped to a file.
   - **Local File System** (for Oracle servers on the DS-Client computer) – The database dump is created on a specified path on the file system of the DS-Client computer. To provide credentials for the selected computer, select the **Ask for Network Credentials** check box. You will be prompted to enter a valid user name and password for the selected computer.
   - **NFS** (for remote Oracle servers) – DS-Client will read the database dump files from the database server using the NFS transmission protocol.
   - **UNIX-SSH** (for remote Oracle servers) – DS-Client will read the database dump files from the database server using the UNIX-SSH transmission protocol.
2. Click **Next**. Depending on the protocol you selected, you will be prompted to provide additional credentials.
3. If you selected **Local File System**, then select the folder where you want to save the database dump file, and then click **Next.**

NOTE: Ensure that the Oracle Server has read and write privileges to this dump path.

5.18.7.4 Selecting the backup items

1. To add an entire Oracle database, select the root folder from the databases list, and then click **Add**.
2. To remove a database, select the database under **Backup Items Selected**, and then click **Remove**.
3. To exclude an item when its parent directory is selected for backup, select the item, and then click **Exclude**.
4. To include an item using regular expressions, select the item, and then click **RegEx**.
5. Click **Next**.

5.18.7.5 Selecting the backup item options

1. To configure the maximum generations for a backup item that will be stored online, double click the **Max Gen** cell, and then enter the value.
2. Click **Next**.

5.18.7.6 Selecting the backup options

1. Configure the options for the backup. The options are as follows:
   - **Use buffer** – Copies files to the DS-Client buffer to free up the backup source as fast as possible. The DS-Client then sends the files from the DS-Client buffer to the DS-System. This option is selected by default. **For more information, see Section 5.2.7, "Performance", on page 113.**
   - **Detailed log** – Records all files that are backed up in the Activity Log. For more information, see Section 8.1, "Viewing the Activity Log", on page 578.
   - **Initial backup** – Uses the Initial Backup feature for the first backup. To configure the initial backup path, click **[>>]**. For more information, see Section 11.1.1, "Configuring the initial backup path", on page 618.
   - **Stop on errors** – Stops a backup process when the number of errors reaches the specified value. A value of 0 means the DS-Client does not stop a backup process regardless of the number of errors.

     NOTE: You can configure the default setting using the **MaxErrors** advanced configuration parameter. For more information, see Section 2.1.8.6, "Miscellaneous parameters (Windows)", on page 42.

   - **Compression type** – Specifies the type of compression that will be applied to the backup. The options are as follows:
     - **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good default compression when the network is not the bottleneck.
     - **ZLIB (Global, Low, Medium, and High)** – Normally produces better compression than LZOP, but will take more time to compress. This is a good default compression when the bottleneck is the network. ZLIB Low corresponds to a value of 3, ZLIB Medium = 6, and ZLIB High = 9.
     - **None** – Disables compression for the backup.
2. Configure additional options for the backup. The options are as follows:
   - **Logical Corruption check** – This is selected by default. Clear the check box if you don't want to perform a corruption check on the database prior to back up.

- **Back up only Current Archived Logs** – Select this check box if you want to back up only those logs that are required for the Oracle database.
- **Truncate Archived Logs** – Select this check box if you want to clear the Oracle database logs associated with the item selected for backup, after the back up is complete.

3. To back up the Oracle database as a compressed backup, select a compression method. The options are as follows:
   - **None** – RMAN compression is not applied to the backup.
   - **Archive Logs** – RMAN compression is applied only to Archive Logs.
   - **Archive Logs and Tablespaces** – RMAN compression is applied to both Archive Logs and Tablespaces.
4. In the **Force pipe library path** box, type the path of the Media Management Library libobk.so which is required by RAMN for backup and restore using a PIPE. If you do not specify a path, the default path "$ORACLE_HOME/lib/libobk.so is used.

NOTE: Ensure that the Oracle Server has full rights to read and execute in the library path. DS-Client does not validate the path before forwarding it to RMAN.

5. To specify a command to run before (Pre) and/or after (Post) the execution of the backup, click **Pre/Post**. For more information, see Section 5.25, "Configuring Pre/Post processes (Windows)", on page 525 and Section 5.26, "Configuring Pre/Post processes (Linux)", on page 528.

5.18.7.7 Specifying notification options

1. To configure a notification, do one of the following:
   - To add a notification, click **Add**.
   - To modify a notification, select the notification, and then click **Modify**.

NOTE: To delete a notification, select the notification, and then click **Delete**.

2. To send an email notification, select **E-Mail**, and then do the following:
   a) To send the email notification to the DS-Client administrator, select **Administrator**.
   b) To send an email to another recipient, select **Other**, and then specify the recipient's email address.
   c) To send detailed backup information, select the **Detailed notification** check box.

d) To include a detailed file-level backup log as an attachment, select the **Attach detailed log** check box.

NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

e) To compress the detailed log, select the **Compress** check box.

f) To send detailed backup information, select the **Detailed notification** check box.

g) To include a detailed file-level backup log as an attachment, select the **Attach detail log** check box.

h) To send the email notification in HTML format, select the **Send E-Mail using HTML format** check box.

3. To send a pager notification, select **Pager**. The notification will be sent to the pager account configured for the DS-Client.

NOTE: The pager option is available only if the DS-Client has been configured for pager notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

4. In the **Completion** box, specify under what conditions a notification will be sent, and click **OK**. The options are as follows:
   - **All** – Notification will be sent under all conditions.
   - **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
   - **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.
   - **Complete with errors** – Notification will be sent if an activity is completed with at least one error event.
   - **Incomplete** – Notification will be sent if an activity is not completed successfully.
5. Under **Send SNMP traps when**, configure the DS-Client to send SNMP traps when the backup has completed successfully, completed with warnings, completed with errors, or is incomplete.
6. Click **Next**.

5.18.7.8 Assigning a retention rule

1. To assign a retention rule to the backup, do one of the following:
   - If you don't want to assign a retention rule, select **No retention rule**.
   - To assign a retention rule, select **Use a specific retention rule**, and then select the retention rule.

NOTE: To create or edit a retention rule, click **[...]**. For more information, see Section 4.1, "Configuring a retention rule", on page 98.

---

2. Click **Next**.

5.18.7.9 Assigning a schedule

1. To assign a schedule to the backup, do one of the following:
   - If you don't want to assign a schedule, select **Not scheduled**.
   - To assign a schedule, select **Scheduled.** In the **Available schedules** box, select an existing schedule.

NOTE: To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, "Configuring a schedule", on page 90.

---

2. Click **Next**.

5.18.7.10 Naming the backup

1. In the **Set name** box, type a name for the backup.
2. In the **Set type** box, select the type of backup you want to create. The list of available backup types depends on the configuration of your DS-Client.
   - Online
   - Self-contained
   - Local-only
   - Statistical

NOTE: For more information, see Section 5.1, "Backup types", on page 106.

---

3. If you selected **Online**, do the following:

a) To send a copy of the oldest generation of the file that is about to be overwritten from the DS-System to the BLM Archiver, select the **BLM (Infinite Generations)** check box.

NOTE: The Backup Lifecycle Management tool must be enabled.

---

b) To save a copy of the backup data to a local storage location on the DS-Client computer, select the **Save on Local Storage** check box.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Self-contained and Local Only backups.

---

c) To use the local storage as a cache if the DS-Client loses connection with the DS-System, select the **Transmission cache on Local Storage** check box. The cached backup data will be sent to the DS-System on the next connection after synchronization.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

4. If you selected **Self-Contained**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

5. If you selected **Local-Only**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

6. If you selected **Statistical**, and want to emulate an actual backup transfer process, select the **Calculate transmit amount** check box. During the backup, specified backup files will be read from their source and processed for compression and encryption.
7. Click **Finish**.

5.18.8 Restoring an Oracle database backup

You can restore data from an Oracle database backup.

5.18.8.1 Restoring the entire container database (CDB)

Restoring the whole CDB is similar to restoring a non-CDB database.

Restore of CDB with controlfile:

- The database must be in **nomount** (Started) state.
- The Database Controlfile, the Root container (CDB$ROOT), and all the Pluggable Databases (PDBs) are selected for restore.

NOTE: When restoring the whole CDB with controlfile, you must remove all the autobackup controlfiles under the directory “autobackup”. (If the flash_recovery_area is configured, the “autobackup” directory is in the “flash_recovery_area”.) Remove any old controlfiles and old archived logs.

Restore of CDB without controlfile:

- The database is in **Mounted** state.
- The Root container and all the PDBs are selected for restore.

5.18.8.2 Restoring only part of the container database CDB

Restore of the Root container:

- The database is in **Mounted** state.
- The Root container is selected for restore.

IMPORTANT: Restore of only the Root container (CDB$ROOT) can leave the database in a state of inconsistency between the Root and PDBs. Oracle recommends that if the Root is restored, all the PDBs should be restored as well.

Restore of PDB(s):

- The target PDB(s) must be closed (in **Mounted** state).
- The target PDB(s) are selected for the restore.

Restore of Tablespace(s):

- The target tablespace must be taken offline. (Alternatively, the PDB where the tablespace resides must be closed.)
- The target tablespace is selected for the restore.

Restore of the special pluggable database PDB$SEED:

NOTE: By default, when a CDB is started and opened, the special pluggable database PDB$SEED is in **Read Only** state, and it will remain in this state for normal database operations. If you need to restore the PDB$SEED, you must close it on the target first, before you can restore.

1. To close the PDB$SEED, from the SQL*Plus command line, type the following commands:

```
alter session set "_oracle_script" = TRUE;
alter pluggable database PDB$SEED close immediate
instances=all;
```

2. Restore the PDB$SEED.
3. After you restore the PDB$SEED, open it in the **Read Only** mode again.
4. From the SQL*Plus command line, type the following command:

```
alter pluggable database PDB$SEED open read only
```

5.18.8.3 Selecting the restore items

1. Browse the backups tree and select the backup you want to restore.
2. On the **Restore** menu click **Restore Now**.
3. To restore an entire backup or an entire database, browse the database tree, and select the check box beside the backup or folder you want to restore.
4. To restore individual files, select the folder containing the required files, and then click **Show Files**. Under **File List**, do the following:
5. To view the number of files selected and calculate the total amount of files selected, select the **Calculate amount** check box under **Options**.
6. In the **Files List** section, do one of the following:
   - To view details about the backed up file, select the file, and then click **File Info**.
   - To view the details of the items you selected, click **Selection**.
   - To view a list of archived generations for a folder, do the following:
     a) In the **Database Tree**, select the folder, and then click **Show Files**.
     b) Under **Files**, click **Show Archived**.
7. To refine your selection of items to restore, click **Advanced**, and then in the **Advanced Options** dialog box, do the following:

a) To restore the latest generation of all the files, select **Latest generation of all data**.

b) To restore files that were deleted from the source, but not removed from the online storage as of the last backup session, select **Latest generation of all data (except deleted data)**.

c) To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:

1. Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.

2. Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.

d) Click **OK**.

8. Click **Next**.

5.18.8.4 Selecting the database restore location

1. Select the location to which you want to restore the backup. The options are as follows:

   - **Original Location –** Data is restored to the original backup source location and existing files with the same name are overwritten. This is the default option.

   - **Alternate location –** For more information, see Section 5.18.5, “Restore requirements”, on page 422.

2. If you selected **Alternate location**, then do one of the following:

   - To restore to a different server on the network, do the following:

     a) Beside the **Alternate location** box, click **[>>]**.

     b) In the **Select Alternate Server** dialog box, select the server where you want to restore the backed up database. You can also type the name or the IP address in the **Path** box.

NOTE: By default, DS-Client uses your current user credentials to connect to the selected computer and database.

---

     c) To provide credentials for the selected computer, select the **Ask for Network Credentials** check box. You will be prompted too enter a valid user name and password for the selected computer.

     d) The **Ask for database credentials** check box is selected by default. You will be prompted to enter a valid user name, password, and service name for the selected database.

e) Click **OK**.

- To use a different dump path during restore, beside the **Dump to** box, click **[>>]**, and select a dump path. The options are as follows:
  - **Dump path** – Save the dump file to a path on the Oracle server. The **Restore only the dump file(s)** check box is selected by default.
  - **DS-Client Buffer** – Save the dump file to the local storage on the DS-Client computer.
  - **DS-Client Pipe** – During restore, the DS-Client reads from the pipe on the source database. This method is useful if the database is too large to be dumped to a file on either the database server or the DS-Client buffer.

3. To have DS-Client automatically add a temp file in the default location for each tablespace, select the **Create temp files** check box.

NOTE: After restoring the Control File, all temporary tablespaces with local extent management will not have any temp file. For the Oracle database to function correctly after restore, you must manually add the temp files.

---

4. Click **Next**.

5.18.8.5 Selecting the performance options

IMPORTANT: These options are intended for large backups in high performance environments where the DS-Client can take advantage of the speed of the storage where the source data resides. Test different settings to determine the optimal value. Slower storage can result in performance issues if these values are not configured correctly.

---

1. Under **Maximum pending asynchronous I/O for a file**, configure the maximum number of I/O operations the DS-Client will use for each file during the restore process.
   - To use the default MaxPendingIOPerFile advanced configuration parameter setting, click **Use DS-Client's settings**. For more information, see Section 2.1.8.10, "Performance parameters (Windows)", on page 55.
   - To override the default setting with a custom value that only applies for the backup, click **Use specific value** and then enter the value.
2. Click **Next**.

5.18.8.6 Selecting the restore options

1. Under **Restore options,** do the following:

   a) To record all restored files in the Activity Log, select the **Detailed log** check box.

   b) To skip the pre and post restore processes, select the **Skip Pre/Post** check box. If this check box is clear, click **Pre/Post**. DS-Client will run a specified activity before and/or after a restore operation. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525.

5.18.8.7 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, under **Restore classification**, select the type of restore. The options are as follows:

   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.

3. Click **Finish**.

5.19 Oracle MySQL database backups (Windows, Linux, or Mac)

You can back up and restore an Oracle MySQL database in a standalone or cluster configuration.

5.19.1 General requirements

- You must install the Oracle MySQL client software on the DS-Client computer.
- You must have knowledge of the Oracle MySQL database file structure and instance management.

5.19.2 Backup requirements

The DS-Client **mysqldump** and **mysql** utilities that are used to back up the Oracle MySQL database must be compatible with the Oracle MySQL version running on the source machine. The following requirements depend on the type of DS-Client:

- **Windows DS-Client** — Ensure the mysqldump and mysql utilities are listed in the PATH environment variable of the DS-Client computer. To verify if the path is included, open the command prompt and type the following command:

  ```
  path
  ```

  NOTE: If you edit this variable, you must stop and restart the DS-Client service after making the change.

- **Linux DS-Client** — Ensure the mysqldump and mysql utilities are listed in the PATH environment variable of the root user on the DS-Client computer. To verify, edit the following file and ensure that the folder is listed in the PATH:

  ```
  /etc/init.d/dsclient
  ```

- **Mac DS-Client** — Ensure the folder that contains the mysqldump and mysql utilities is in the search PATH of the DS-Client by adding it to the following file on the DS-Client computer:

  ```
  /etc/rc.common
  ```

5.19.3 Restore requirements

To restore backed up stored routines, you must have the following privileges for the Oracle MySQL database:

- Grant
- Create_Routines
- Alter_Routines

5.19.4 Creating an Oracle MySQL database backup (Windows)

You can create an Oracle MySQL database backup using a Windows DS-Client.

5.19.4.1 Selecting the type of backup

1. On the **Sets** menu, click **New Backup Set**.
2. Select **MySQL Server**, and then click **Next**.

5.19.4.2 Selecting the MySQL server

1. Browse and select the computer you want to back up. You can also type the IP address of the computer in the **Path** box. To use non-standard port numbers, type the IP address and port number in the following format:

   ```
   \\IP_address:Port_Number
   ```

   NOTE: If you do not specify a port number, Windows DS-Client uses port 3306 by default.

2. By default, DS-Client uses the current user's logon credentials to connect to the selected computer. To provide credentials for the selected computer, select the **Ask for Network Credentials** check box. You will be prompted to enter a valid user name and password for the selected computer.
3. The **Ask for database credentials** check box is selected by default. Click **Next**.
4. In the **Enter database credentials** dialog box, do the following:
   a) In the **User name** and **Password** boxes, type the credentials required to connect to the selected database server.
   b) Click **OK**.
5. Click **Next**.

5.19.4.3 Selecting the database dump options

1. Select a path or method to handle the database dump. The options are as follows:
   - **DS-Client Buffer** – Save the dump file to the local storage on the DS-Client computer.
   - **DS-Client Pipe** – During backup, the DS-Client reads from the pipe on the source database. This method is useful if the database is too large to be dumped to a file on either the database server or the DS-Client buffer.
2. Click **Next**.

5.19.4.4 Selecting the database(s) to back up

1. Select the items you want to back up:
   - To add an instance, select the instance, and then click **Add**.
   - To remove an instance, select the instance from the **Backup Items Selected** list, and then click **Remove**.
2. Click **Next**.

5.19.4.5 Selecting the backup item options

1. To configure the maximum generations for a backup item that will be stored online, double click the **Max Gen** cell, and then enter the value.
2. Click **Next**.

5.19.4.6 Selecting the backup options

1. Configure the options for the backup. The options are as follows:
   - **Detailed log** – Records all files that are backed up in the Activity Log. For more information, see Section 8.1, “Viewing the Activity Log”, on page 578.
   - **Initial backup** – Uses the Initial Backup feature for the first backup. To configure the initial backup path, click **[>>]**. For more information, see Section 11.1.1, “Configuring the initial backup path”, on page 618.

- **Stop on errors** – Stops a backup process when the number of errors reaches the specified value. A value of 0 means the DS-Client does not stop a backup process regardless of the number of errors.

NOTE: You can configure the default setting using the **MaxErrors** advanced configuration parameter. For more information, see Section 2.1.8.6, “Miscellaneous parameters (Windows)”, on page 42.

- **Compression type** – Specifies the type of compression that will be applied to the backup. The options are as follows:
  - **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good default compression when the network is not the bottleneck.
  - **ZLIB (Global, Low, Medium, and High)** – Normally produces better compression than LZOP, but will take more time to compress. This is a good default compression when the bottleneck is the network. ZLIB Low corresponds to a value of 3, ZLIB Medium = 6, and ZLIB High = 9.
  - **None** – Disables compression for the backup.

2. Configure additional options for the backup as follows:
   - To lock the tables before inserting data on restore, select the **Add locks around insert statements** check box. For more information, see *MySQL* documentation.
   - To add MySQL specific extensions to the backed up database dump, select the **Add MySQL specific table create options** check box.
   - To specify how table rows are inserted into the database, beside **Insert statements type**, select an insertion type. For more information, see *MySQL* documentation. The options are as follows:
     - **Extended** – Table rows are inserted to the database dump very quickly. This method is not useful for manual loading into non MySQL databases.
     - **Complete** – Table rows are inserted using complete INSERT statements that include column names.
     - **Normal** – Table rows are inserted using a standard method which is slower but is portable to other databases.
   - To specify how tables are dumped, beside **Table dumping option**, select a table dump method. The options are as follows:
     - **Lock all tables** – Sets the tables to ready only mode and prevents changes to data during the backup process.

- **Single transaction** – Prevents changes to the backup data, but does not set the tables to read-only mode during the backup process.This option works only with transactional tables.
- **Do not lock tables** – You can change the table during the creation of the dump file.This could impact the consistency of the backup.
- **None** – Database dump is performed using the mysqldump function with no special conditions.

3. To specify a command to run before (Pre) and/or after (Post) the execution of the backup, click **Pre/Post**. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525 and Section 5.26, “Configuring Pre/Post processes (Linux)”, on page 528.
4. Click **Next**.

5.19.4.7 Selecting the notification options

1. To configure a notification, do one of the following:
   - To add a notification, click **Add.**
   - To modify a notification, select the notification, and then click **Modify.**

   NOTE: To delete a notification, select the notification, and then click **Delete**.

2. To send an email notification, select **E-Mail**. and then do the following:
   a) To send the email notification to the DS-Client administrator, select **Administrator**.
   b) To send an email to another recipient, select **Other**, and then specify the recipients email address.
   c) To send detailed backup information, select the **Detailed notification** check box.
   d) To include a detailed file-level backup log as an attachment, select the **Attach detail log** check box.
   e) To send the email notification in HTML format, select the **Send E-Mail using HTML format** check box.

   NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

3. To send a pager notification, select **Pager**. The notification will be sent to the pager account configured for the DS-Client.

NOTE: The pager option is available only if the DS-Client has been configured for pager notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

---

4. To send a broadcast notification, select **Broadcast**. Select the server containing the messenger service to which you want to send the message and click **OK**.

NOTE: Broadcast notifications to domains or workgroups are limited to 128 characters.

---

5. To send an event notification, elect **Event**. Select the server on which you want the notification to be recorded in the Event Log.
6. In the **Completion** box, specify under what conditions a notification will be sent, and click **OK**. The options are as follows:
    - **All** – Notification will be sent under all conditions.
    - **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
    - **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.
    - **Completed with errors** – Notification will be sent if an activity is completed with at least one error event.
    - **Incomplete** – Notification will be sent if an activity is not completed successfully.
7. Click **Next**.

5.19.4.8 Assigning a retention rule

1. To assign a retention rule to the backup, do one of the following:
   - If you don't want to assign a retention rule, select **No retention rule**.
   - To assign a retention rule, select **Use a specific retention rule**, and then select the retention rule.

   NOTE: To create or edit a retention rule, click **[...]**. For more information, see Section 4.1, "Configuring a retention rule", on page 98.

2. Click **Next**.

5.19.4.9 Assigning a schedule

1. To assign a schedule to the backup, do one of the following:
   - If you don't want to assign a schedule, select **Not scheduled**.
   - To assign a schedule, select **Scheduled.** In the **Available schedules** box, select an existing schedule.

   NOTE: To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, "Configuring a schedule", on page 90.

2. Click **Next**.

5.19.4.10 Naming the backup

1. In the **Set name** box, type a name for the backup.
2. In the **Set type** box, select the type of backup you want to create. The list of available backup types depends on the configuration of your DS-Client.
   - Online
   - Self-contained
   - Local-only
   - Statistical

   NOTE: For more information, see Section 5.1, "Backup types", on page 106.

3. If you selected **Online**, do the following:

a) To send a copy of the oldest generation of the file that is about to be overwritten from the DS-System to the BLM Archiver, select the **BLM (Infinite Generations)** check box.

NOTE: The Backup Lifecycle Management tool must be enabled for the DS-Client.

---

b) To save a copy of the backup data to a local storage location on the DS-Client computer, select the **Save on Local Storage** check box.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Self-contained and Local Only backups.

---

c) To use the local storage as a cache if the DS-Client loses connection with the DS-System, select the **Transmission cache on Local Storage** check box. The cached backup data will be sent to the DS-System on the next connection after synchronization.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path.

---

d) To save a copy of the backup data to the instant recovery vault, select the **Save in instant recovery vault** check box.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Instant Recovery backups.

---

e) If you selected **Save in instant recovery vault**, beside the **Local Storage Path** box, click **>>**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

4. If you selected **Self-Contained**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

5. If you selected **Local-Only**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

6. If you selected **Statistical**, and want to emulate an actual backup transfer process, select the **Calculate transmit amount** check box. During the backup, specified backup files will be read from their source and processed for compression and encryption.
7. Click **Finish**.

5.19.5 Creating an Oracle MySQL database backup (Linux or Mac)

You can create a MySQL database backup using a Linux or Mac DS-Client. You can use the MySQL Configuration Utility (**mysql_config_editor**) to define all the logon paths that you need. For each logon path, you must define the following:

- Name of the logon path
- Host name
- User name
- Password

The logon path information is stored in the encrypted .mylogin.cnf file. Copy the .mylogin.cnf file to the DS-Client installation folder. The default location is:

```
/opt/CloudBackup/DS-Client
```

After you have defined the logon path, ensure the .mylogin.cnf file is in the DS-Client installation folder and contains the logon paths that are required by your Oracle MySQL database backups.

IMPORTANT: Updates to the **.mylogin.cnf** file are not accessible to DS-Client unless the updated file is in the DS-Client installation folder.

5.19.5.1 Selecting the type of backup

1. On the **Sets** menu, click **New Backup Set**.
2. Select **MySQL Server**, and then click **Next**.

5.19.5.2 Selecting the backup source

1. rowse and select the computer you want to backup. You can also type the IP address of the computer in the **Path** box.
2. The **Ask for database credentials** check box is selected by default.
3. To specify the database dump application to use for the MySQL database backup, select the **Database Dump Configuration** check box.
4. Click **Next**.
5. In the **Ask for database credentials** dialog box, do the following:

   a) In th **User name** and **Password** boxes, type the credentials required to connect to the selected database server.

   To refer to a logon path, type the following text in the **User Name** box:

   `--login-path=<login path name>`

   where `<login path name>` is the name that is specified for the logon path.

   b) In the **Port** box, enter the port number DS-Client will use to communicate with the database. By default, Linux DS-Client uses port 3306.

   IMPORTANT: Do not change the port number unless you have a specific requirement to do so. For more information, refer to the *Oracle MySQL* documentation.

   c) Click **OK**.

6. In the **Dump utility directory** box, type the installation path of a specific MySQL database dump application that will be used for this backup. If you do not specify the path, DS-Client will select one automatically.

5.19.5.3 Selecting the database(s) to back up

1. Browse the database list and select the items to back up.
   - To add an instance, select the instance, and then click **Add**.
   - To view details about the backup item selected, click **Items**.
   - To remove an instance, select the instance from the **Backup Items Selected**, and then click **Remove**.
2. Click **Next**.

5.19.5.4 Selecting the backup item options

1. To configure the maximum generations for a backup item that will be stored online, double click the **Max Gen** cell, and then enter the value.
2. Click **Next**.

5.19.5.5 Selecting the backup options

1. Configure the options for the backup. The options are as follows:
   - **Use buffer** – Copies files to the DS-Client buffer to free up the backup source as fast as possible. The DS-Client then sends the files from the DS-Client buffer to the DS-System. This option is selected by default. **For more information, see Section 5.2.7, "Performance", on page 113.**
   - **Detailed log** – Records all files that are backed up in the Activity Log. For more information, see Section 8.1, "Viewing the Activity Log", on page 578.
   - **Initial backup** – Uses the Initial Backup feature for the first backup. To configure the initial backup path, click **[>>]**. For more information, see Section 11.1.1, "Configuring the initial backup path", on page 618.
   - **Stop on errors** – Stops a backup process when the number of errors reaches the specified value. A value of 0 means the DS-Client does not stop a backup process regardless of the number of errors.

     NOTE: You can configure the default setting using the **MaxErrors** advanced configuration parameter. For more information, see Section 2.1.8.6, "Miscellaneous parameters (Windows)", on page 42.

   - **Compression type** – Specifies the type of compression that will be applied to the backup. The options are as follows:
     - **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good default compression when the network is not the bottleneck.

- **ZLIB (Global, Low, Medium, and High)** – Normally produces better compression than LZOP, but will take more time to compress. This is a good default compression when the bottleneck is the network. ZLIB Low corresponds to a value of 3, ZLIB Medium = 6, and ZLIB High = 9.
- **None** – Disables compression for the backup.

2. Configure additional options for the backup as follows:
   - To lock the tables before inserting data on restore, select the **Add locks around insert statements** check box. For more information, see *MySQL* documentation.
   - To add MySQL specific extensions to the backed up database dump, select the **Add MySQL specific table create options** check box.
   - To specify how table rows are inserted into the database, beside **Insert statements type**, select an insertion type. For more information, see *MySQL* documentation. The options are as follows:
     - **Extended** – Table rows are inserted to the database dump very quickly. This method is not useful for manual loading into non MySQL databases.
     - **Complete** – Table rows are inserted using complete INSERT statements that include column names.
     - **Normal** – Table rows are inserted using a standard method which is slower but is portable to other databases.
   - To specify how tables are dumped, beside **Table dumping option**, select a table dump method. The options are as follows:
     - **Lock all tables** – Sets the tables to ready only mode and prevents changes to data during the backup process.
     - **Single transaction** – Prevents changes to the backup data, but does not set the tables to read-only mode during the backup process.This option works only with transactional tables.
     - **Do not lock tables** – You can change the table during the creation of the dump file.This could impact the consistency of the backup.
     - **None** – Database dump is performed using the mysqldump function with no special conditions.
3. To specify a command to run before (Pre) and/or after (Post) the execution of the backup, click **Pre/Post**. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525 and Section 5.26, “Configuring Pre/Post processes (Linux)”, on page 528.
4. Click **Next**.

5.19.5.6 Specifying notification options

IMPORTANT: The email and pager options are available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

1. To configure a notification, do one of the following:
   - To add a notification, click **Add**.
   - To modify a notification, select the notification, and then click **Modify**.

   NOTE: To delete a notification, select the notification, and then click **Delete**.

2. To send an email notification, select **E-Mail**, and then do the following:
   a) To send the email notification to the DS-Client administrator, select **Administrator**.
   b) To send an email to another recipient, select **Other**, and then specify the recipient’s email address.
   c) To send detailed backup information, select the **Detailed notification** check box.
   d) To include a detailed file-level backup log as an attachment, select the **Attach detailed log** check box.
   e) To compress the detailed log, select the **Compress** check box.
   f) To send detailed backup information, select the **Detailed notification** check box.
   g) To include a detailed file-level backup log as an attachment, select the **Attach detail log** check box.
   h) To send the email notification in HTML format, select the **Send E-Mail using HTML format** check box.

      NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

   i) Click **OK**.

3. To send a pager notification, select **Pager**. The notification will be sent to the pager account configured for the DS-Client.

NOTE: The pager option is available only if the DS-Client has been configured for pager notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

---

4. In the **Completion** box, specify under what conditions a notification will be sent, and click **OK**. The options are as follows:
   - **All** – Notification will be sent under all conditions.
   - **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
   - **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.
   - **Complete with errors** – Notification will be sent if an activity is completed with at least one error event.
   - **Incomplete** – Notification will be sent if an activity is not completed successfully.
5. Under **Send SNMP traps when**, configure the DS-Client to send SNMP traps when the backup has completed successfully, completed with warnings, completed with errors, or is incomplete.
6. Click **Next**.

5.19.5.7 Assigning a retention rule

1. To assign a retention rule to the backup, do one of the following:
   - If you don’t want to assign a retention rule, select **No retention rule**.
   - To assign a retention rule, select **Use a specific retention rule**, and then select the retention rule.

NOTE: To create or edit a retention rule, click **[...]**. For more information, see Section 4.1, “Configuring a retention rule”, on page 98.

---

2. Click **Next**.

5.19.5.8 Assigning a schedule

1. To assign a schedule to the backup, do one of the following:
   - If you don't want to assign a schedule, select **Not scheduled**.
   - To assign a schedule, select **Scheduled.** In the **Available schedules** box, select an existing schedule.

   NOTE: To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, "Configuring a schedule", on page 90.

2. Click **Next**.

5.19.5.9 Specifying a backup name

1. In the **Set name** box, type a name for the backup.
2. In the **Set type** box, select the type of backup you want to create. The list of available backup types depends on the configuration of your DS-Client.
   - Online
   - Self-contained
   - Local-only
   - Statistical

   NOTE: For more information, see Section 5.1, "Backup types", on page 106.

3. If you selected **Online**, do the following:
   a) To send a copy of the oldest generation of the file that is about to be overwritten from the DS-System to the BLM Archiver, select the **BLM (Infinite Generations)** check box.

   NOTE: The Backup Lifecycle Management tool must be enabled.

   b) To save a copy of the backup data to a local storage location on the DS-Client computer, select the **Save on Local Storage** check box.

   NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Self-contained and Local Only backups.

c) To use the local storage as a cache if the DS-Client loses connection with the DS-System, select the **Transmission cache on Local Storage** check box. The cached backup data will be sent to the DS-System on the next connection after synchronization.

NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

4. If you selected **Self-Contained**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

5. If you selected **Local-Only**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

6. If you selected **Statistical**, and want to emulate an actual backup transfer process, select the **Calculate transmit amount** check box. During the backup, specified backup files will be read from their source and processed for compression and encryption.
7. Click **Finish**.

5.19.6 Restoring an Oracle MySQL database backup

You can restore data from an Oracle MySQL database backup.

NOTE: Only users with the required permissions can restore an Oracle MySQL database backup.

5.19.6.1 Selecting the restore items

1. Browse the backups tree and select the backup you want to restore.
2. On the **Restore** menu click **Restore Now**.
3. To restore an entire backup or an entire database, browse the database tree, and select the check box beside the backup or folder you want to restore.
4. To restore individual files, select the folder containing the required files, and then click **Show Files**. Under **File List**, do the following:
5. To view the number of files selected and calculate the total amount of files selected, select the **Calculate amount** check box under **Options**.
6. In the **Files List** section, do one of the following:
   - To view details about the backed up file, select the file, and then click **File Info**.
   - To view the details of the items you selected, click **Selection**.
   - To view a list of archived generations for a folder, do the following:
     a) In the **Database Tree**, select the folder, and then click **Show Files**.
     b) Under **Files**, click **Show Archived**.
7. To refine your selection of items to restore, click **Advanced**, and then in the **Advanced Options** dialog box, do the following:
   a) To restore the latest generation of all the files, select **Latest generation of all data**.
   b) To restore files that were deleted from the source, but not removed from the online storage as of the last backup session, select **Latest generation of all data (except deleted data)**.
   c) To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:
      1. Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.
      2. Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.
   d) Click **OK**.
8. Click **Next**.

5.19.6.2 Selecting the restore location

1. Select the location to which you want to restore the backup. The options are as follows:
   - **Original location** – Data is restored to the original backup source location and existing files with the same name are overwritten. This is the default option.
   - **Alternate location** – Select to restore data to a location other than the original backup source.
2. If you selected **Alternate location**, then do one of the following:
   - To restore to a different server on the network, do the following:
     a) Beside the **Alternate location** box, click **[>>]**.
     b) In the **Select alternate location** dialog box, select the server where you want to restore the backed up database. You can also type the name or the IP address in the **Path** box.

     NOTE: By default, DS-Client uses your current user credentials to connect to the selected computer and database.

     c) The **Ask for database credentials** check box is selected by default. You will be prompted to enter a valid user name and password for the selected database.
     d) To specify the database dump application to use for the MySQL database backup, select the **Database Dump Configuration** check box.
     e) Click **Select**.
     f) In th **User name** and **Password** boxes, type the credentials required to connect to the selected database server.
     g) In the **Port** box, enter the port number DS-Client will use to communicate with the database. By default, DS-Client uses port 3306.
   - To use a different dump path during restore, beside the **Dump to** box, click **[>>]**, and select a dump path (for Windows only). The options are as follows:
     - **Dump path** – Save the dump file to a path on the Oracle server. The **Restore only the dump file(s)** check box is selected by default.
     - **DS-Client Buffer** – Save the dump file to the local storage on the DS-Client computer.

h) **DS-Client Pipe** – During restore, the DS-Client reads from the pipe on the source database. This method is useful if the database is too large to be dumped to a file on either the database server or the DS-Client buffer.

IMPORTANT: Do not change the port number unless you have a specific requirement to do so. For more information, refer to the *Oracle MySQL* documentation.

---

i) Click **OK**.

j) In the **Dump utility directory** box, type the installation path of a specific MySQL database dump application that will be used for this backup. If you do not specify the path, DS-Client will select one automatically.

k) Click **OK**.

3. To restore the dump file to the specified location, select the **Restore as Pure Files** check box.
4. Click **Next**.

5.19.6.3 Selecting the restore options

1. To skip the pre and post restore processes, select the **Skip Pre/Post** check box. If this check box is clear, click **Pre/Post**. DS-Client will run a specified activity before and/or after a restore operation. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525.
2. To record all restored files in the Activity Log, select the **Detailed log** check box.
3. If the database selected for restore already exists and you want DS-Client to restore to the existing database, select the **Do not drop existing DB before restore** check box.
4. Click **Next**.

5.19.6.4 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, select the type of restore. The options are as follows:
   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.
3. Click **Finish**.

5.20 Oracle SBT database backups (Linux)

You can back up data using the Oracle Recovery Manager (RMAN). RMAN interacts with the DS-Client through the Oracle SBT (System Backup to Tape) protocol, which allows the process to be redirected through the DS-Client to the DS-System instead of to tape. For more information, see the *DS-Client Oracle SBT (System Backup to Tape) User Guide*.

IMPORTANT: This backup type requires manual command input from the Oracle Server. All backup and restore commands must be initiated from the Oracle Server, either through the RMAN command-line or Oracle Enterprise Manager. Only Oracle database administrators should attempt to use this backup type.

5.20.1 Backup requirements

- If you are using the controlfile as the RMAN repository, you might need to increase the CONTROL_FILE_RECORD_KEEP_TIME parameter to keep the maximum Oracle backups records in the controlfile.
- To include a backup of the controlfile and spfile, set the CONFIGURE CONTROLFILE AUTOBACKUP parameter to ON. This allows you to restore the files and mount the database in case of disaster recovery. Otherwise, you must configure the Recovery Catalog to keep track of all the backup records.

5.20.2 Restore requirements

If you restore only a tablespace from an Oracle SBT database backup, RMAN will read the backup and restore the tablespace. After the tablespace is restored, the SBT channel is released and RMAN stops. However, the DS-Client still expects RMAN to send the entire database from the backup, which causes the following error in the DS-Client Event Log, which is safe to ignore:

```
SBT restore canceled: Remote side stopped the restore of this file
before all data was transmitted.
```

5.20.3 Creating an Oracle SBT database backup

You can create an Oracle SBT backup.

5.20.3.1 Selecting the type of backup

1. On the **Sets** menu, click **New Backup Set**.
2. Select **Oracle SBT**, and then click **Next**.

5.20.3.2 Selecting the backup source

1. Browse the Oracle SBT tree and select **RMAN-SBT-Data**.
2. The **Specify backup set access credentials** check box is selected by default.
3. Click **Next.** You will be prompted to enter the backup access credentials required by the Oracle RMAN client.

   These credentials are defined in the **DS-Client/Oracle SBT parameter file**. For more information, see the *DS-Client Oracle SBT (System Backup to Tape) User Guide*.
4. Click **OK**.

5.20.3.3 Selecting the backup items

1. Select **data_dumps**, and then click **Add**.
2. To view details about the selected item, select the item, and then click **Files**.
3. To remove an item, select the item, and then click **Remove**.
4. To include an item using regular expressions, select the item, and then click **RegEx**.
5. Click **Next**.

5.20.3.4 Selecting the backup item options

1. To configure the maximum generations for a backup item that will be stored online, double click the **Max Gen** cell, and then enter the value.
2. Click **Next**.

5.20.3.5 Selecting the backup options

1. Configure the options for the backup. The options are as follows:
   - **Detailed log** – Records all files that are backed up in the Activity Log. For more information, see Section 8.1, “Viewing the Activity Log”, on page 578.
   - **Initial backup** – Uses the Initial Backup feature for the first backup. To configure the initial backup path, click **[>>]**. For more information, see Section 11.1.1, “Configuring the initial backup path”, on page 618.
   - **Stop on errors** – Stops a backup process when the number of errors reaches the specified value. A value of 0 means the DS-Client does not stop a backup process regardless of the number of errors.

     NOTE: You can configure the default setting using the **MaxErrors** advanced configuration parameter. For more information, see Section 2.1.8.6, “Miscellaneous parameters (Windows)”, on page 42.

   - **Compression type** – Specifies the type of compression that will be applied to the backup. The options are as follows:
     - **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good default compression when the network is not the bottleneck.
     - **ZLIB (Global, Low, Medium, and High)** – Normally produces better compression than LZOP, but will take more time to compress. This is a good default compression when the bottleneck is the network. ZLIB Low corresponds to a value of 3, ZLIB Medium = 6, and ZLIB High = 9.
     - **None** – Disables compression for the backup.
2. To specify a command to run before (Pre) and/or after (Post) the execution of the backup, click **Pre/Post**. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525 and Section 5.26, “Configuring Pre/Post processes (Linux)”, on page 528.

5.20.3.6 Specifying notification options

IMPORTANT: The email and pager options are available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

1. To configure a notification, do one of the following:
   - To add a notification, click **Add**.
   - To modify a notification, select the notification, and then click **Modify**.

   NOTE: To delete a notification, select the notification, and then click **Delete**.

2. To send an email notification, select **E-Mail**, and then do the following:
   a) To send the email notification to the DS-Client administrator, select **Administrator**.
   b) To send an email to another recipient, select **Other**, and then specify the recipient’s email address.
   c) To send detailed backup information, select the **Detailed notification** check box.
   d) To include a detailed file-level backup log as an attachment, select the **Attach detailed log** check box.

      NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

   e) To compress the detailed log, select the **Compress** check box.
   f) To send detailed backup information, select the **Detailed notification** check box.
   g) To include a detailed file-level backup log as an attachment, select the **Attach detail log** check box.
   h) To send the email notification in HTML format, select the **Send E-Mail using HTML format** check box.
   i) Click **OK**.

3. To send a pager notification, select **Pager**. The notification will be sent to the pager account configured for the DS-Client.

NOTE: The pager option is available only if the DS-Client has been configured for pager notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

---

4. In the **Completion** box, specify under what conditions a notification will be sent, and click **OK**. The options are as follows:
   - **All** – Notification will be sent under all conditions.
   - **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
   - **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.
   - **Complete with errors** – Notification will be sent if an activity is completed with at least one error event.
   - **Incomplete** – Notification will be sent if an activity is not completed successfully.
5. Configure the DS-Client to send SNMP traps when the backup has completed successfully, completed with warnings, completed with errors, or is incomplete.
6. Click **Next**.

5.20.3.7 Assigning a retention rule

IMPORTANT: Retention should not be assigned via the DS-Client to an Oracle SBT backup. Retention rules should be managed by RMAN itself. Even if you enforce retention from DS-Client on an Oracle SBT backup, DS-Client will not delete any files because all files only have a single generation. Retention always keeps the latest generation of every file.

- Click **Next**.

5.20.3.8 Assigning a schedule

IMPORTANT: You cannot assign a schedule to an Oracle SBT backup. Oracle SBT backups are controlled by Oracle RMAN and not from DS-User. On-demand and scheduled backups do not apply to it.

- Click **Next**.

5.20.3.9 Naming the backup

1. In the **Set name** box, type a name for the backup.
2. In the **Set type** box, select the type of backup you want to create. The list of available backup types depends on the configuration of your DS-Client.
   - Online
   - Self-contained
   - Local-only
   - Statistical

   NOTE: For more information, see Section 5.1, “Backup types”, on page 106.

3. If you selected **Online**, do the following:
   a) To send a copy of the oldest generation of the file that is about to be overwritten from the DS-System to the BLM Archiver, select the **BLM (Infinite Generations)** check box.

      NOTE: The Backup Lifecycle Management tool must be enabled for the DS-Client.

   b) To save a copy of the backup data to a local storage location on the DS-Client computer, select the **Save on Local Storage** check box.
      - Beside **Local Storage Path**, click **[>>]**, and select the path for the local storage.

      NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Self-contained and Local Only backups.

4. If you selected **Self-Contained**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

   NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

5. If you selected **Local-Only**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**..

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

6. If you selected **Statistical**, and want to emulate an actual backup transfer process, select the **Calculate transmit amount** check box. During the backup, specified backup files will be read from their source and processed for compression and encryption.
7. Click **Finish**.

5.21 Permissions Only backups (Windows, Linux, or Mac)

You can back up and restore only the permissions of a selected item. This reduces the backup time because it does not back up the actual files. You can select more than one backup item and a separate dump file is saved for each backup item.

An Online File system backup saves its files with the current permissions and attributes. If the permissions or attributes are changed, but the content of the files remains the same, the DS-Client does not detect the changes at the next backup session. In this type of backup environment, modifications to attributes like Compress, Read-Only, Hidden, Archive, and Index can be detected and backed up with a Permissions Only backup.

NOTE: Modifications to the Encrypt attribute can be detected only by using an Online File system backup.

5.21.1 Creating a Permissions Only backup

You can create a Permissions Only backup.

5.21.1.1 Selecting the type of backup

1. On the **Sets** menu, click **New Backup Set**.
2. Select **Permissions Only** (Windows) or **Permissions** (Linux), and then click **Next**.

5.21.1.2 Selecting the backup source

1. Select the computer containing the files you want to back up.The **Path** box displays the network path of the item selected in the tree.

   NOTE: DS-Client Computer represents the local DS-Client computer. For NAS devices, type the IP address or host name in the Path box.

2. To provide the credentials for the selected computer, select the **Ask for Network Credentials** check box. You will be prompted to enter a valid user name and password for the selected computer.

   NOTE: You must connect to the computer using an Administrator or equivalent account.

3. To use the DS-Client service account credentials to connect to the local DS-Client computer, select the **Use DS-Client Account** check box.

   NOTE: This option is available only when you select DS-Client Computer. You must be logged in using an Administrator or equivalent account.

4. To perform a backup of a NAS device, select the **Ask for NAS API credentials** check box and do the following:

   a) In the **NAS Type** box, select the NAS device type. Only NetApp is currently supported.

   b) In the **API Protocol** box, select the protocol for accessing the API. The protocol must be enabled on the NAS device.

   c) In the **Port Number** box, enter the port number for accessing the API. The port must be open on the NAS device.

   d) In the **User Name** and **Password** boxes, type the user name and password of a user who has permission to execute API commands on the NAS device. This is typically a member of the Administrators group.

   NOTE: To browse for an encrypted key file containing the user credentials, click **[...]**. If the file is valid, you must enter the correct key to unlock the credentials stored in the file.

e) Click **OK**.

NOTE: The DS-Client backs up data from a snapshot that it creates using a dedicated API from the NAS vendor. When the backup is finished, the snapshot is deleted.

5. Click **Next**.

5.21.1.3 Selecting the backup items

1. To add an item, select the item, and then click **Add**. For NAS devices, select the CIFS share.

NOTE: You can add only one item at a time. Subdirectories are included by default. To exclude subdirectories, clear the Include SubDirs check box.

2. To exclude an item when its parent directory is selected for backup, select the item, and then click **Exclude**.
3. To exclude an item using regular expressions, select the item, and then click **RegEx**.

NOTE: Regular expressions provide more specific filtering than the exclude function. For example, you can use regular expressions to exclude individual file names or patterns. Use this option only if you are familiar with the syntax.

4. To add specific files from a directory, select the directory from which you want to add the files, and then click **Files**. Select the file(s) that you want to add, and then click **Add**.
5. To search for files that match a certain criteria, in the **Filter** box, type the file pattern that you want to search for in the selected directory. For example, *.doc will search for all the files with the doc file extension.

NOTE: In a Windows file system, you can also add special backup items like System State (including Registry) and Services Database.

6. To modify a regular expression, select the regular expression, and then click **Modify**.

7. To remove an item from the list, select the item, and then click **Remove**.

NOTE: Removing an item will not remove previous backups of that item. To remove previously backed-up data, you must use the Delete function.

8. Click **Next**.

5.21.1.4 Selecting the backup item options

1. To configure the maximum generations for a backup item that will be stored online, double click the **Max Gen** cell, and then enter the value.
2. Click **Next**.

5.21.1.5 Selecting the backup options

1. Configure the options for the backup. The options are as follows:
   - **Use buffer** – Copies files to the DS-Client buffer to free up the backup source as fast as possible. The DS-Client then sends the files from the DS-Client buffer to the DS-System. This option cannot be configured if the CDP is enabled. For more information, see Section 5.2.7, “Performance”, on page 113.
   - **Detailed log** – Records all files that are backed up in the Activity Log. For more information, see Section 8.1, “Viewing the Activity Log”, on page 578.
   - **Initial backup** – Uses the Initial Backup feature for the first backup. To configure the initial backup path, click **[>>]**. For more information, see Section 11.1.1, “Configuring the initial backup path”, on page 618.
   - **Stop on errors** – Stops a backup process when the number of errors reaches the specified value. A value of 0 means the DS-Client does not stop a backup process regardless of the number of errors.

     NOTE: You can configure the default setting using the **MaxErrors** advanced configuration parameter. For more information, see Section 2.1.8.6, “Miscellaneous parameters (Windows)”, on page 42.

   - **Compression type** – Specifies the type of compression that will be applied to the backup. The options are as follows:
     - **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good default compression when the network is not the bottleneck.

- **ZLIB (Global, Low, Medium, and High)** – Normally produces better compression than LZOP, but will take more time to compress. This is a good default compression when the bottleneck is the network. ZLIB Low corresponds to a value of 3, ZLIB Medium = 6, and ZLIB High = 9.
- **None** – Disables compression for the backup.

2. In the **Default operation** box, specify how the backup should handle an open file during backup. The options are as follows:
   - **Try deny write** – Attempts to open the file in Deny write mode. If this fails because the file is already open, the file is placed in Allow write mode.
   - **Deny write** – Prevents any other process from writing to the file while the DS-Client has it open. The DS-Client will not back up the file if another process has already opened it for write. However, you can instruct the DS-Client to retry backing up the open file.
   - **Prevent write** – Attempts to open the file in Deny write mode. If this fails because the file is already open, the file is opened in Allow write mode and locked to prevent any other process from writing to the file. This ensures that the most recent version of the file is backed up.
   - **Allow write** – Allows another process to read or write to the file without restrictions. Since other applications can write to the file while it is being backed up, this can affect file consistency.
3. In the **Retry times** box, enter the number of times you want the DS-Client to attempt to back up the file.
4. In the **Retry interval (sec)** box, enter the interval between retries.
5. To specify a command to run before (Pre) and/or after (Post) the execution of the backup, click **Pre/Post**. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525 and Section 5.26, “Configuring Pre/Post processes (Linux)”, on page 528.
6. Click **Next**.

5.21.1.6 Selecting the advanced options

NOTE: These options are disabled by default. If you select any of these options, the size of the data that is backed up will increase.

1. To back up all data on remote media, select the **Backup data in Remote Storage** check box.

   NOTE: Some operating systems can migrate infrequently accessed data from the local hard drive to directly attached tape libraries. The local disk usage is reduced by replacing the file with a link. If disabled, only the link is backed up.

2. To back up each instance of a file separately, select the **Backup Single Instance Store / Data Deduplication file data** check box.

   NOTE: Some operating systems have an optional Single Instance Store to handle multiple copies of the same file on the computer. Local disk usage is reduced by placing one copy of the file in the Single Instance Store with links in all associated directories. If disabled, only the link is backed up. If you have activated Single Instance Store, select this option.

3. To back up all data in the directory referenced by the junction point, select the **Follow junction point** check box.

   NOTE: Junction points are links to other folders. If disabled, only links to the folder are backed up. Junction points that are mounted FAT or FAT32 volumes are not supported.

4. If the target computer supports the Volume Shadow Copy Service (VSS) feature, under **Volume Shadow Copy**, do the following:

   a) To initiate a Volume Shadow Copy Service (VSS) snapshot of any local volumes and perform the backup from the VSS snapshot, select the **Backup through volume shadow copies** check box.

      NOTE: When configured, the DS-Client uses the VSS feature to copy the volumes selected for backup and then performs the backup from the VSS snapshot. If the VSS snapshot fails, the DS-Client attempts to perform the backup like a normal Permissions only backup.

   b) To specify whether VSS validation is run prior to performing the backup, select one of the following options:

- **Disable** – VSS validation is not performed.
- **Enable** – VSS validation is performed.
- **Use DS-Client's settings** – VSS validation is performed using the DS-Client settings.

c) To specify that the DS-Client does not notify VSS-aware applications when a backup is performed so the resulting backup is only crash-consistent (e.g. it will contain whatever was on the hard disk during the backup), select the **Do not involve writers** check box.

d) To specify that the VSS snapshot is performed without processing components, select the **Do not process components** check box.

NOTE: Processing components means verifying if the files are included in the volumes selected for the snapshot. This option is useful if you have selected only a portion of a component for backup and do not want to encounter errors because the VSS verification would otherwise detect missing files or dependencies.

e) To manually exclude specific VSS writers or components, select the **Exclude some writers / components** check box, and then click **[>>]**.

NOTE: This has the same effect as choosing the Do not involve writers option, but only applies to the writers or components you choose.

5. Click **Next**.

5.21.1.7 Selecting the notification options

1. To configure a notification, do one of the following:
   - To add a notification, click **Add.**
   - To modify a notification, select the notification, and then click **Modify.**

NOTE: To delete a notification, select the notification, and then click **Delete**.

2. To send an email notification, select **E-Mail**. and then do the following:

NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, "Configuring the notification settings", on page 27.

a) To send the email notification to the DS-Client administrator, select **Administrator**.

b) To send an email to another recipient, select **Other**, and then specify the recipients email address.

c) To send detailed backup information, select the **Detailed notification** check box.

d) To include a detailed file-level backup log as an attachment, select the **Attach detail log** check box.

e) To send the email notification in HTML format, select the **Send E-Mail using HTML format** check box.

NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

---

3. To send a pager notification, select **Pager**. The notification will be sent to the pager account configured for the DS-Client.

NOTE: The pager option is available only if the DS-Client has been configured for pager notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

---

4. To send a broadcast notification, select **Broadcast**. Select the server containing the messenger service to which you want to send the message and click **OK**.

NOTE: Broadcast notifications to domains or workgroups are limited to 128 characters.

---

5. To send an event notification, elect **Event**. Select the server on which you want the notification to be recorded in the Event Log.
6. In the **Completion** box, specify under what conditions a notification will be sent and then click **OK**. The options are as follows:

   - **All** – Notification will be sent under all conditions.
   - **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
   - **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.
   - **Completed with errors** – Notification will be sent if an activity is completed with at least one error event.

- **Incomplete** – Notification will be sent if an activity is not completed successfully.

7. Click **Next**.

5.21.1.8 Assigning a retention rule

1. To assign a retention rule to the backup, do one of the following:
   - If you don't want to assign a retention rule, select **No retention rule**.
   - To assign a retention rule, select **Use a specific retention rule**, and then select the retention rule.

NOTE: To create or edit a retention rule, click **[...]**. For more information, see Section 4.1, "Configuring a retention rule", on page 98.

---

2. Click **Next**.

5.21.1.9 Assigning a schedule

1. To assign a schedule to the backup, do one of the following:
   - If you don't want to assign a schedule, select **Not scheduled**.
   - To assign a schedule, select **Scheduled.** In the **Available schedules** box, select an existing schedule.

NOTE: To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, "Configuring a schedule", on page 90.

---

2. Click **Next**.

5.21.1.10 Naming the backup

1. In the **Set name** box, type a name for the backup.
2. In the **Set type** box, select the type of backup you want to create. The list of available backup types depends on the configuration of your DS-Client.
   - Online
   - Self-contained
   - Local-only

- Statistical

NOTE: For more information, see Section 5.1, “Backup types”, on page 106.

3. If you selected **Online**, do the following:

   a) To send a copy of the oldest generation of the file that is about to be overwritten from the DS-System to the BLM Archiver, select the **BLM (Infinite Generations)** check box.

   NOTE: The Backup Lifecycle Management tool must be enabled for the DS-Client.

   b) To save a copy of the backup data to a local storage location on the DS-Client computer, select the **Save on Local Storage** check box.

   NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Self-contained and Local Only backups.

   c) To use the local storage as a cache if the DS-Client loses connection with the DS-System, select the **Transmission cache on Local Storage** check box. The cached backup data will be sent to the DS-System on the next connection after synchronization.

   NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path.

   d) Beside the **Local Storage Path** box, click **>>**. Enter a local storage path for the backup, and then click **OK**.

   NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

4. If you selected **Self-Contained**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

5. If you selected **Local-Only**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

6. If you selected **Statistical**, and want to emulate an actual backup transfer process, select the **Calculate transmit amount** check box. During the backup, specified backup files will be read from their source and processed for compression and encryption.
7. If the multitenant feature is enabled and configured, in the **Customer** list, you can select the customer to which you want to assign the backup. For more information, see Section 11.5, “Multitenant DS-Clients”, on page 634.
8. Click **Finish**.

5.21.2 Restoring a Permissions Only backup

You can restore data from a Permissions only backup.

NOTE: When restoring a Permissions Only backup using a Windows DS-Client, you cannot perform a granular restore of an item.

5.21.2.1 Selecting the restore items

1. Browse the backups tree and select the backup you want to restore.
2. On the **Restore** menu, click **Restore Now**.
3. To restore an entire backup or folder, browse the tree and select the check box beside the backup or folder you want to restore.
4. To restore individual files, select the folder containing the required files, click **Show Files**, and then do the following:
   - To view details about the backed up file, select the file, and then click **File Info**.
   - To view modified files, click **Show Modified**.
   - To view archived files, click **Show Archived**.
5. To view the number of files selected and calculate the total amount of files selected, select the **Calculate amount** check box.

6. To search for files that match a certain criteria, in the **Filter** box, type the file pattern that you want to search for in the selected folder. For example, *.doc will search for all files with the .doc extension.
7. In the **Files List** section, do one of the following:
   - To view details about the backed up file, select the file, and then click **File Info**.
   - To view the details of the items you selected, click **Selection**.
   - To view a list of archived generations for a folder, do the following:
     a) In the **Directories Tree**, select the folder, and then click **Show Files**.
     b) Under **Files**, click **Show Archived**.
8. To refine your selection of items to restore, click **Advanced**. Under **Show**, select which generation you want to display. The options are as follows:
   a) To restore the latest generation of all the files, select **Latest generation of all data**.
   b) To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:
      1. Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.
      2. Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.
      3. Click **OK**.
9. Click **Next**.

5.21.2.2 Selecting the restore location

1. Select the location to which you want to restore the backup. The options are as follows:
   - **Original location** – Data is restored to the original backup source location and existing files with the same name are overwritten. This is the default option.
   - **Alternate location** – Data is restored to a location other than the original backup source.

   NOTE: When restoring to an alternate location, the security of restored items in the destination location might not resemble the security of those items during backup.

2. If you selected **Alternate location**, then do the following:

a) Beside the **Alternate location** box, click **[>>]**.

b) In the **Select Alternate Server** dialog box, select the computer where you want to restore the data.

c) To provide the credentials for the selected computer, select the **Ask for Network Credentials** checkbox, and then click **Select**.

d) In the **Enter Network Credentials** dialog box, enter the credentials to connect to the destination computer, and then click **OK**.

e) In the **Destination** cell, select a share location.

f) Click in the **Restore to** cell and type the name of the folder or click **[>>]** and select a folder.

g) In the **Truncate** box, you can increase the truncate level to shorten the common portion of the restore path, if the selected restore items contain a common path.

h) Click **Next**.

NOTE: For more information, see Section 5.3.3, “Restoring data to an alternate location”, on page 130.

5.21.2.3 Selecting the restore options

1. To record all restored files in the Activity Log, select the **Detailed log** check box.
2. To skip the pre and post restore processes, select the **Skip Pre/Post** check box. If this check box is cleared, the DS-Client runs a specified activity before and/or after a restore operation. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525.
3. To restore permissions for a specific path, type the path name in the **Restore permissions from** box. If you leave this box empty, all backed up permissions are restored.
4. Click **Next**.

5.21.2.4 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, select the type of restore. The options are as follows:
   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.
3. Click **Finish**.

5.22 PostgreSQL database backups (Linux or Mac)

You can back up and restore your PostgreSQL database.

5.22.1 General requirements

- You must have knowledge about the PostgreSQL database structure.
- You must configure the <pg_data_path>/postgresql.conf file for each PostgreSQL database to be able to connect to other PostgreSQL instances. For more information, see the PostgreSQL documentation.

5.22.2 DS-Client requirements

- Ensure the **psql** and **pg_dump** utilities are listed in the PATH environment variable of the root user on the DS-Client computer.
- The DS-Client **psql** and **pg_dump** utilities that are used to back up the PostgreSQL database must be compatible with the PostgreSQL version running on the source machine.

5.22.3 PostgreSQL server requirements

- The PostgreSQL server must be a certified product.

5.22.4 Restore requirements

- The PostgreSQL database must not be in use when you perform a restore to the original or alternate location.

5.22.5 Creating a PostgreSQL database backup

You can create a PostgreSQL database backup.

5.22.5.1 Selecting the type of backup

1. On the **Sets** menu, click **New Backup Set**.
2. Select **PgSQL** and then click **Next**.

5.22.5.2 Selecting the backup source

1. Browse and select the server you want to back up.
2. To provide credentials for the database, select the **Ask for database credentials** check box.
3. Click **Next**.
4. In the **Ask for database credentials** dialog box, enter a valid user name and password for the selected database, and then click **OK**.

NOTE: To back up a PostgreSQL Server that is using non-standard ports, you must specify the port number when you create the backup.

---

5. To specify the database dump application to use for the PostgreSQL database backup, select the **Database Dump Configuration** check box. If a path is not specified, DS-Client chooses one automatically.
6. Click **Next**.

5.22.5.3 Selecting the backup items

1. To add an item, browse the database list, select the required database(s), and then click **Add**.
2. To remove an item, select an item from the **Selected Items for backup** list, and then click **Remove**.
3. To view the details an item you selected, click **Items**.
4. To exclude an item using regular expressions, select the item, and then click **RegEx**.

NOTE: Regular expressions provide more specific filtering than the exclude function. For example, you can use regular expressions to exclude individual file names or patterns. Use this option only if you are familiar with the syntax.

---

5. Click **Next**.

5.22.5.4 Selecting the backup item options

1. To configure the maximum generations for a backup item that will be stored online, double click the **Max Gen** cell, and then enter the value.
2. Click **Next**.

5.22.5.5 Selecting the backup options

1. Configure the options for the backup. The options are as follows:
   - **Use buffer** – Copies files to the DS-Client buffer to free up the backup source as fast as possible. The DS-Client then sends the files from the DS-Client buffer to the DS-System. This option is selected by default.**For more information, see Section 5.2.7, “Performance”, on page 113.**
   - **Detailed log** – Records all files that are backed up in the Activity Log. For more information, see Section 8.1, “Viewing the Activity Log”, on page 578.
   - **Initial backup** – Uses the Initial Backup feature for the first backup. To configure the initial backup path, click **[>>]**. For more information, see Section 11.1.1, “Configuring the initial backup path”, on page 618.

- **Stop on errors** – Stops a backup process when the number of errors reaches the specified value. A value of 0 means the DS-Client does not stop a backup process regardless of the number of errors.

NOTE: You can configure the default setting using the **MaxErrors** advanced configuration parameter. For more information, see Section 2.1.8.6, “Miscellaneous parameters (Windows)”, on page 42.

- **Compression type** – Specifies the type of compression that will be applied to the backup. The options are as follows:
  - **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good default compression when the network is not the bottleneck.
  - **ZLIB (Global, Low, Medium, and High)** – Normally produces better compression than LZOP, but will take more time to compress. This is a good default compression when the bottleneck is the network. ZLIB Low corresponds to a value of 3, ZLIB Medium = 6, and ZLIB High = 9.
  - **None** – Disables compression for the backup.

2. Configure additional options for the backup as follows:
   - To dump only the schema (data definitions) without the data, select the **Back up only the schema, not the data** check box.
   - To back up only the data without the privileges of the database, select the **Do not back up privileges (grant/revoke)** check box.
   - To dump data as INSERT commands instead of copying, select the **Backup data as INSERT, rather than COPY** check box. This will slow down the restore but the backup is more portable to other SQL database packages.
   - To optimize the PostgreSQL database before performing the backup, select the **Vacuum database before backup** check box.
   - To back up the ownership of any objects within the database, select the **Back up ownership of database objects** check box.The ownership of the entire database is always backed up by DS-Client independent of this option.
3. To specify a command to run before (Pre) and/or after (Post) the execution of the backup, click **Pre/Post**. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525 and Section 5.26, “Configuring Pre/Post processes (Linux)”, on page 528.

5.22.5.6 Specifying notification options

1. To configure a notification, do one of the following:
   - To add a notification, click **Add.**
   - To modify a notification, select the notification, and then click **Modify.**

   NOTE: To delete a notification, select the notification, and then click **Delete**.

2. To send an email notification, select **E-Mail**. and then do the following:
   a) To send the email notification to the DS-Client administrator, select **Administrator**.
   b) To send an email to another recipient, select **Other**, and then specify the recipients email address.
   c) To send detailed backup information, select the **Detailed notification** check box.
   d) To include a detailed file-level backup log as an attachment, select the **Attach detail log** check box.
   e) To send the email notification in HTML format, select the **Send E-Mail using HTML format** check box.

      NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

   f) Click **OK**.
3. To send a pager notification, select **Pager**. The notification will be sent to the pager account configured for the DS-Client.

   NOTE: The pager option is available only if the DS-Client has been configured for pager notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

4. In the **Completion** box, specify under what conditions a notification will be sent and then click **OK**. The options are as follows:
   - **All** – Notification will be sent under all conditions.
   - **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
   - **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.

- **Completed with errors** – Notification will be sent if an activity is completed with at least one error event.
- **Incomplete** – Notification will be sent if an activity is not completed successfully.

5. Configure the DS-Client to send SNMP traps when the backup has completed successfully, completed with warnings, completed with errors, or is incomplete.
6. Click **Next**.

5.22.5.7 Assigning a retention rule

1. To assign a retention rule to the backup, do one of the following:
   - If you don't want to assign a retention rule, select **No retention rule**.
   - To assign a retention rule, select **Use a specific retention rule**, and then select the retention rule.

NOTE: To create or edit a retention rule, click **[...]**. For more information, see Section 4.1, "Configuring a retention rule", on page 98.

---

2. Click **Next**.

5.22.5.8 Assigning a schedule

1. To assign a schedule to the backup, do one of the following:
   - If you don't want to assign a schedule, select **Not scheduled**.
   - To assign a schedule, select **Scheduled.** In the **Available schedules** box, select an existing schedule.

NOTE: To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, "Configuring a schedule", on page 90.

---

2. Click **Next**.

5.22.5.9 Naming the backup

1. In the **Set name** box, type a name for the backup.
2. In the **Set type** box, select the type of backup you want to create. The list of available backup types depends on the configuration of your DS-Client.
   - Online
   - Self-contained
   - Local-only
   - Statistical

   NOTE: For more information, see Section 5.1, “Backup types”, on page 106.
3. If you selected **Online**, do the following:
   a) To send a copy of the oldest generation of the file that is about to be overwritten from the DS-System to the BLM Archiver, select the **BLM (Infinite Generations)** check box.

      NOTE: The Backup Lifecycle Management tool must be enabled for the DS-Client.

   b) To save a copy of the backup data to a local storage location on the DS-Client computer, select the **Save on Local Storage** check box.

      NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Self-contained and Local Only backups.

   c) To use the local storage as a cache if the DS-Client loses connection with the DS-System, select the **Transmission cache on Local Storage** check box. The cached backup data will be sent to the DS-System on the next connection after synchronization.

      NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path.

d) Beside the **Local Storage Path** box, click **>>**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

4. If you selected **Self-Contained**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

5. If you selected **Local-Only**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

6. If you selected **Statistical** and want to emulate an actual backup transfer process, select the Calculate transmit amount check box. During the backup, specified backup files will be read from their source and processed for compression and encryption.
7. If the multitenant feature is enabled and configured, in the **Customer** list, you can select the customer to which you want to assign the backup. For more information, see Section 11.5, “Multitenant DS-Clients”, on page 634.
8. Click **Finish**.

5.22.6 Restoring a PostgreSQL database backup

You can restore data from a PostgreSQL database backup.

NOTE: Only users with the required permissions can restore a PostgreSQL database backup.

5.22.6.1 Selecting the restore items

1. Browse the backups tree and select the backup you want to restore.
2. On the **Restore** menu, click **Restore Now**.
3. To restore an entire backup or folder, browse the tree and select the check box beside the backup or folder you want to restore.
4. To restore individual files, select the folder containing the required files, and then click **Show Files**.
5. To view the number of files selected and calculate the total amount of files selected, select the **Calculate amount** check box.
6. To filter the list of files, in the **Filter box**, enter a filter using * as a wildcard, and then click **Show Files** to update the list of files.
7. In the **Files List** section, do one of the following:
   - To view details about the backed up file, select the file, and then click **File Info**.
   - To view the details of the items you selected, click **Selection**.
   - To view a list of archived generations for a folder, do the following:
     a) In the **Directories Tree**, select the folder, and then click **Show Files**.
     b) Under **Files**, click **Show Archived**.
8. To refine your selection of items to restore, click **Advanced**, and then select which generation you want to display. The options are as follows:
   a) To restore the latest generation of all the files, select **Latest generation of all data**.
   b) To restore files that were deleted from the source, but not removed from the online storage as of the last backup session, select **Latest generation of all data (except deleted data)**.
   c) To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:
      1. Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.
      2. Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.
      3. Click **OK**.
9. Click **Next**.

5.22.6.2 Selecting the restore location

1. Select the location to which you want to restore the backup. The options are as follows:
   - **Original location** – Data is restored to the original backup source location and existing files with the same name are overwritten. This is the default option.
   - **Alternate location** – Select to restore data to a location other than the original backup source.
2. If you selected **Alternate location**, To restore to a different server on the network, do the following:
   a) Beside the **Alternate location** box, click **[>>]**.
   b) In the **Select alternate location** dialog box, select the server where you want to restore the backed up database. You can also type the name or the IP address in the **Path** box.
   c) Click **Select**.

   NOTE: By default, DS-Client uses your current user credentials to connect to the selected computer and database.

   d) To restore the dump file to the specified location, select the **Restore as Pure Files** check box.
3. Click **Next**.

5.22.6.3 Selecting the restore options

1. To skip the pre and post restore processes, select the **Skip Pre/Post** check box. If this check box is clear, click **Pre/Post**. DS-Client will run a specified activity before and/or after a restore operation. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525.
2. To record all restored files in the Activity Log, select the **Detailed log** check box.
3. If the database selected for restore already exists and you want DS-Client to restore to the existing database, select the **Do not drop existing DB before restore** check box.
4. Click **Next**.

5.22.6.4 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, select the type of restore. The options are as follows:
   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.
3. Click **Finish**.

5.23 Salesforce backups (Windows)

You can back up and restore your Salesforce data.

5.23.1 General requirements

- You must have a valid Salesforce account (username, password, and security token).
- Your Salesforce product must be an edition that allows API integration.

NOTE: If you need to change your Salesforce password, you must obtain a new security token from the Salesforce website. All existing Salesforce backups must be updated with the new credentials.

5.23.2 DS-Client computer requirements

- Ensure the local storage path is set. For more information, see Section 11.4, “Local Storage Tool”, on page 629.
- The DS-Client computer must connect to the Salesforce site. Optionally, you can configure the DS-Client to connect to Salesforce via a proxy server.

5.23.3 Creating a Salesforce backup

You can create a Salesforce backup.

5.23.3.1 Selecting the type of backup

1. On the **Sets** menu, click **New Backup Set**.
2. Select **Backup from the cloud**, and then click **Next**.

5.23.3.2 Selecting the type of cloud service

1. Select **Salesforce.com**.
2. Click **Next**.

5.23.3.3 Selecting the server

1. Select the Cloud Server to back up and then click **Next**.
2. In the **Enter Network Credentials** dialog box, do the following:
   a) In the **Connect as** box, type the Salesforce user name and password.
   b) In the **Password** box, type the associated password.

   NOTE: If you need to change the password, you must obtain a new security token from Salesforce and update your security token.

   c) In the **Target** box, select the database for backup. The options are as follows:
      - **Production** – This is the live, functioning version of the Salesforce database.
      - **Sandbox** – This is the developer/testing version of the Salesforce database.
   d) Click **OK**.

5.23.3.4 Selecting the backup items

1. To back up the entire Salesforce database and tables, select the database, and then click **Add**.
2. To remove an item from the **Backup items selected list**, select the item, and then click **Remove.**
3. To exclude specific database tables form the backup, click **Tables**.In the **Select Table** dialog box, select the database tables, and then click **Exclude**.
4. To configure the backup to automatically exclude Salesforce System tables, select the **Exclude all system tables which are not restorable** check box.
5. Click **Tables** to selectively include or exclude specific database tables from the backup.The number of tables displayed depends on the exclude/include system tables setting.
6. Click **Next**.

5.23.3.5 Selecting the backup item options

1. To configure the maximum generations for a backup item that will be stored online, double click the **Max Gen** cell, and then enter the value.
2. Click **Next**.

5.23.3.6 Selecting the backup options

1. Configure the options for the backup. The options are as follows:
   - **Detailed log** – Records all files that are backed up in the Activity Log. For more information, see Section 8.1, “Viewing the Activity Log”, on page 578.
   - **Initial backup** – Uses the Initial Backup feature for the first backup. To configure the initial backup path, click **[>>]**. For more information, see Section 11.1.1, “Configuring the initial backup path”, on page 618.
   - **Stop on errors** – Stops a backup process when the number of errors reaches the specified value. A value of 0 means the DS-Client does not stop a backup process regardless of the number of errors.

     NOTE: You can configure the default setting using the MaxErrors advanced configuration parameter. For more information, see Section 2.1.8.6, “Miscellaneous parameters (Windows)”, on page 42.

   - **Compression type** – Specifies the type of compression that will be applied to the backup. The options are as follows:

- **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good default compression when the network is not the bottleneck.
- **ZLIB (Global, Low, Medium, and High)** – Normally produces better compression than LZOP, but will take more time to compress. This is a good default compression when the bottleneck is the network. ZLIB Low corresponds to a value of 3, ZLIB Medium = 6, and ZLIB High = 9.
- **None** – Disables compression for the backup.

2. To specify a command to run before (Pre) and/or after (Post) the execution of the backup, click **Pre/Post**. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525.
3. Click **Next**.

5.23.3.7 Selecting the restore items parameters

1. To dump the database to the local storage path and be retained for subsequent backups to use for differential comparison, select the **Keep DB dump for differential backup** check box.

NOTE: The local storage path must be configured from the DS-Client Configuration - Parameters tab.

---

2. To include tables referenced by the table selected for backup, select the **Include referenced tables automatically** check box.
3. Beside **Timeout**, enter the duration in seconds the DS-Client will wait for a response from the Cloud Server before timing out. The default is 100 seconds.
4. Beside **Buffer Size (MB)**, enter the maximum size the DS-Client will buffer for each query requested to or from the Cloud Server. If the buffer reaches this limit before the “Query Batch Size” or “Destination Batch Size” is reached, the data will be immediately transferred to clear the buffer. The default is 20 MB.
5. Beside **Query Batch Size**, enter the number of rows the DS-Client will query from the Cloud Server each time. The default is 200.
6. Beside **Destination Batch Size**, enter the number of rows in a batch the DS-Client will write to the Cloud Server to update the database. The default is 5000.

5.23.3.8 Specifying notification options

1. To configure a notification, do one of the following:
   - To add a notification, click **Add.**
   - To modify a notification, select the notification, and then click **Modify.**

   NOTE: To delete a notification, select the notification, and then click **Delete**.

2. To send an email notification, select **E-Mail**. and then do the following:
   a) To send the email notification to the DS-Client administrator, select **Administrator**.
   b) To send an email to another recipient, select **Other**, and then specify the recipients email address.
   c) To send detailed backup information, select the **Detailed notification** check box.
   d) To include a detailed file-level backup log as an attachment, select the **Attach detail log** check box.
   e) To send the email notification in HTML format, select the **Send E-Mail using HTML format** check box.

      NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

   f) Click **OK**.
3. To send a pager notification, select **Pager**. The notification will be sent to the pager account configured for the DS-Client.

   NOTE: The pager option is available only if the DS-Client has been configured for pager notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

4. To send a broadcast notification, select **Broadcast**. Select the server containing the messenger service to which you want to send the message and click **OK**.

   NOTE: Broadcast notifications to domains or workgroups are limited to 128 characters.

5. To send an event notification, select **Event**. Select the server on which you want the notification to be recorded in the Event Log and click **OK**.
6. In the **Completion** box, specify under what conditions a notification will be sent and then click **OK**. The options are as follows:
   - **All** – Notification will be sent under all conditions.
   - **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
   - **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.
   - **Completed with errors** – Notification will be sent if an activity is completed with at least one error event.
   - **Incomplete** – Notification will be sent if an activity is not completed successfully.
7. Click **Next**.

5.23.3.9 Assigning a retention rule

1. To assign a retention rule to the backup, do one of the following:
   - If you don't want to assign a retention rule, select **No retention rule**.
   - To assign a retention rule, select **Use a specific retention rule**, and then select the retention rule.

NOTE: To create or edit a retention rule, click **[...]**. For more information, see Section 4.1, "Configuring a retention rule", on page 98.

---

2. Click **Next**.

5.23.3.10 Assigning a schedule

1. To assign a schedule to the backujp, do one of the following:
   - If you don't want to assign a schedule, select **Not scheduled**.
   - To assign a schedule, select **Scheduled.** In the **Available schedules** box, select an existing schedule.

NOTE: To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, "Configuring a schedule", on page 90.

---

2. Click **Next**.

5.23.3.11 Naming the backup

1. In the **Set name** box, type a name for the backup.
2. In the **Set type** box, select the type of backup you want to create. The list of available backup types depends on the configuration of your DS-Client.
   - Online
   - Self-contained
   - Local-only
   - Statistical

   NOTE: For more information, see Section 5.1, “Backup types”, on page 106.
3. If you selected **Online**, do the following:
   a) To send a copy of the oldest generation of the file that is about to be overwritten from the DS-System to the BLM Archiver, select the **BLM (Infinite Generations)** check box.

      NOTE: The Backup Lifecycle Management tool must be enabled for the DS-Client.

   b) To save a copy of the backup data to a local storage location on the DS-Client computer, select the **Save on Local Storage** check box.

      NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Self-contained and Local Only backups.

   c) To use the local storage as a cache if the DS-Client loses connection with the DS-System, select the **Transmission cache on Local Storage** check box. The cached backup data will be sent to the DS-System on the next connection after synchronization.

      NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path.

d) Beside the **Local Storage Path** box, click **>>**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

4. If you selected **Self-Contained**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

5. If you selected **Local-Only**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**..

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

6. If you selected **Statistical**, and want to emulate an actual backup transfer process, select the **Calculate transmit amount** check box. During the backup, specified backup files will be read from their source and processed for compression and encryption.
7. If the multitenant feature is enabled and configured, in the **Customer** list, you can select the customer to which you want to assign the backup. For more information, see Section 11.5, “Multitenant DS-Clients”, on page 634.
8. Click **Finish**.

5.23.4 Performing a table level restore

You can restore data from a Salesforce backup at the table level.

5.23.4.1 Selecting the restore method

1. Browse the backups tree and select the backup you want to restore.
2. On the **Restore** menu, click **Restore Now**.
3. Select **Table Restore**, and then click **Next**.

5.23.4.2 Selecting the restore items

1. To restore an entire backup or folder, browse the tree and select the check box beside the backup or folder you want to restore.
2. To restore individual files, select the folder containing the required files, and then click **Show Files**.

NOTE: For this kind of backup, there is only one backup item **Salesforce.fdb**.

---

3. Under **Database Tree**, select **Salesforce**.
4. Under **Options**, do the following:
   a) To view the number of files selected and calculate the total amount of files selected, select the **Calculate amount** check box.
   b) To exclude subdirectories, clear the **Include SubDirs** check box, as the default setting is to include sub-directories.
5. To filter the list of files, in the **Filter box**, enter a filter using * as a wildcard, and then click **Show Files** to update the list of files.
6. To find a backed up Salesforce database, click **Show Files**.
7. In the **Files List** section, do one of the following:
   - To view details about the backed up file, select the file, and then click **File Info**.
   - To view the details of the items you selected, click **Selection**.
   - To view a list of archived generations for a folder, do the following:
     a) In the **Database Tree**, select the folder, and then click **Show Files**.
     b) Under **Files**, click **Show Archived**.
8. To refine your selection of items to restore, click **Advanced**, and then select which generation you want to display. The options are as follows:
   a) To restore the latest generation of all the files, select **Latest generation of all data**.
   b) To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:
      1. Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.
      2. Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.
   c) Click **OK**.
9. Click **Next**.

5.23.4.3 Selecting the table(s) to restore

A list of all the tables in the **Salesforce.fdb** appears. By default, all tables are selected. The data from each selected table will be appended to the existing table on the Cloud application server (Salesforce).

During a table-level restore of a Salesforce backup, the restored records might be duplicated if the same tables are restored multiple times. To avoid this issue, do the following:

- To prevent duplicate records in all tables except the Case and Contract tables, select the **Detect duplicate records by name comparison** restore option.
- To prevent duplicate records in the Case or Contract tables, manually delete the entire contents of the table before performing the restore.

NOTE: Records in the Case and Contract tables are not identified by name but by unique IDs that are incremented automatically. Duplicate records in these tables cannot be detected by name comparison.

---

1. To select all the tables, click **Select All**.
2. To select specific tables, select the check box beside the required table(s).
3. To remove all the tables from the restore, click **Deselect All** or click **Deselect** for individual tables.
4. Click **Next**.

5.23.4.4 Selecting the restore location

NOTE: If you are restoring a Salesforce backup that has been written to a BLM restorable image or disc/tape media, the Original location option is not available. When restoring from these media, select Alternate location so that you can provide the credentials for accessing the restore.

1. Select the location to which you want to restore the backup. The options are as follows:
   - **Original location** – Data is restored to the original backup source location (the original Salesforce account) and existing files with the same name are overwritten. This is the default option.
   - **Alternate location** – Data is restored to a location other than the original backup source. For Salesforce backups, an alternate location can be another Salesforce account, the original location, or a different target on the same account (e.g. from Production to Sandbox or vice versa).

     NOTE: When restoring to an alternate location, the security of restored items in the destination location might not resemble the security of those items during backup.

2. If you selected **Alternate location**, then do the following:
   a) Beside the **Alternate location** box, click **[>>]**.
   b) In the **Modify Network Credentials** dialog box, enter the credentials to connect to the Salesforce account, and then click **OK**.
   c) To restore the dump file as an FDB file to a specific location on the DS-Client computer, select the **Restore to a local database file** check box.

      NOTE: UNC paths are not supported with this option.

      1. Type the path or click **[>>]** and in the **Select Directory** dialog box, select the folder.
      2. Click **Select**.

d) To restore the database in CSV format to a specific location, select the **Restore to multiple data files (CSV)** check box.

NOTE: Salesforce system tables are not restorable to the Salesforce online database. You can restore backed up Salesforce system tables. Each table will be a standalone CSV file in the destination folder.

---

1. Type the path or click **[>>]** and in the **Select Directory** dialog box, select the folder.
2. Click **Select**.

3. Click **Next**.

5.23.4.5 Selecting the restore options

Salesforce balances transaction loads by imposing two types of limits on API calls:

- Concurrent API Request Limits
- Total API Request Limits

If your Salesforce account exceeds the specified limits, errors can occur. To modify the API limits associated with your account, contact Salesforce.

IMPORTANT: DS-Client uses the Salesforce API for backup and restore processes. There are API call usage limits that are enforced by Salesforce.

---

1. To record all restored files in the Activity Log, select the **Detailed log** check box.
2. To skip the pre and post restore processes, select the **Skip Pre/Post** check box. If this check box is clear, click **Pre/Post**. DS-Client will run a specified activity before and/or after a restore operation. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525.
3. To use the backed up schema(s) to clear the tables and then rebuild them in the Salesforce database, select the **Restore Schema** check box.This option is useful if the structure of any tables have changed since the backup session you are restoring.
4. To minimize the number of API call counts made by the restore process, select the **Use Bulk API** check box. This option is selected by default. When files are uploaded via Bulk API, a file size limit of 10 MB is enforced by Salesforce.

NOTE: Ensure that you clear this check box if the data to be restored contains files that are larger than 10 MB.

---

5. To enforce DS-Client to trace the ID change and fill the foreign key with the new ID that was inserted, thereby maintaining the relationship between tables, select the **Restore with automatic relationship fix** check box. This is applicable if you are restoring multiple tables at the same time.
   - To include all backed up tables that are related to the table being restored, select the **Include all referenced tables automatically** check box.
   - To enforce DS-Client to find any missing referenced records based on a comparison of the name columns, select the **Additional relationship fix based on name comparison** check box.
6. To prevent existing data from being restored and duplicated, select the **Detect duplicate records by name comparison** check box.
7. To enable the restore process to resume in the event that it is stopped during the uploading stage, select the **Save temporary database file in local storage for resume** check box. For more information, see Section 5.23.7, “Resuming a Salesforce data restore process”, on page 508.
8. To remove the selected tables from the online Salesforce database, before performing the restore to re-populate those tables, select the **Delete all records before restoring** check box.
9. Click **Next**.

5.23.4.6 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, select the type of restore. The options are as follows:
   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.
3. Click **Finish**.

5.23.5 Performing a granular restore

You can restore data from a backed up Salesforce database at the item level.

NOTE: Each individual item in an item-level restore is a row from a table in a Salesforce database.

There are two steps to performing a granular restore:

1. Restore the Salesforce database to the point-in-time that contains the items you want to restore. It is recommended you restore to a local disk location on the DS-Client machine.
2. Connect to the restored Salesforce database and select the individual items you want to restore to the online Salesforce account.

NOTE: If you are restoring from a BLM restorable image or disc/tape media, you can only perform step 1. You must perform step 2 from the database restored in step 1.

5.23.5.1 Selecting a restore method

1. Browse the backups tree, select the backup, and then on the **Restore** menu, click **Restore Now**.
2. Select **Granular Restore**, and then select **Step 1. Database Restore**.
3. Click **Next**.

5.23.5.2 Selecting the restore items

1. To restore an entire backup or folder, browse the tree and select the check box beside the backup or folder you want to restore.
2. To restore individual files, select the folder containing the required files, and then click **Show Files**.
3. To view the number of files selected and calculate the total amount of files selected, select the **Calculate amount** check box.
4. To exclude subdirectories, clear the **Include SubDirs** check box, as the default setting is to include sub-directories.
5. To filter the list of files, in the **Filter box**, enter a filter using * as a wildcard, and then click **Show Files** to update the list of files.
6. To find a backed up file, click **Show Files**.

7. In the **Files List** section, do one of the following:
   - To view details about the backed up file, select the file, and then click **File Info**.
   - To view the details of the items you selected, click **Selection**.
   - To view a list of archived generations for a folder, do the following:
     a) In the **Database Tree**, select the folder, and then click **Show Files**.
     b) Under **Files**, click **Show Archived**.
   - To view the files that are part of the selected VSS component, click **VSS Component**.
8. To refine your selection of items to restore, click **Advanced**, and then select which generation you want to display. The options are as follows:
   a) To restore the latest generation of all the files, select **Latest generation of all data**.
   b) To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:
      1. Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.
      2. Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.
   c) Click **OK**.
9. Click **Next**.

5.23.5.3 Selecting the restore location

1. Beside the **Select the path to put the database file** box, click **[>>]**, and in the **Select Directory** dialog box, select the folder where you want to restore the Salesforce database.
2. Click **Next**.

NOTE: Ensure that the Salesceforce.com database file is located on a local drive for DS-Client to access. For expedience, select a local disk location in the DS-Client machine as the restore destination for the database file.

5.23.5.4 Selecting the restore options

1. To record all restored files in the Activity Log, select the **Detailed log** check box.
2. To skip the pre and post restore processes, select the **Skip Pre/Post** check box. If this check box is clear, click **Pre/Post**. DS-Client will run a specified activity before and/or after a restore operation. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525.
3. Click **Next**.

5.23.5.5 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, select the type of restore. The options are as follows:
   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.
3. Click **Finish**.

NOTE: After the database has been restored, you can proceed to step 2 for item-level restore.

5.23.6 Performing an item restore

This is the second step for performing a granular restore of a Salesforce backup. Ensure that the Salesforce database file from which you plan to restore at the item level is located on a local drive in the DS-Client machine. Otherwise, DS-Client will not be able to access it.

1. Browse the backups tree and select the backup you restored in step 1.
2. On the **Restore** menu, click **Restore Now**.
3. Select **Granular Restore**, and then **Step 2. Items Restore**.

4. Click **Next**.

5.23.6.1 Selecting the restore location

1. Beside **SalesForce DB Path**, click **[>>]**, and select the Salesforce database file that was restored in step 1. The file needs to be located on a local disk in the DS-Client machine for DS-Client to access it.
2. Select a location to restore the Salesforce database. The options are as follows:
   - To restore to a Salesforce site, select **Salesforce Account (online)**. Beside **Connect to Salesforce with**, click **[>>]**, and then enter the credentials for the Salesforce site to which you want to restore data.
   - To restore the Salesforce database in CSV format to a specific location, select **Multiple data files (CSV)**. Beside **Specify a directory**, click **[>>]**, select the folder to which you want to restore, and then click **Select**.
3. Click **Next**.

5.23.6.2 Selecting the database to restore

1. Select the tables or items to restore.
   - To select an entire table, select the corresponding check box.
   - To select specific items (or rows from a table), click **[...]** in the **Items** column for the corresponding table. In the **Select Table Items** dialog box select the backed up items from that table.
     a) In the **Filter box,** type a regular expression to find specific items or to narrow down the items displayed.
     b) Select the items to restore, and then click **OK**.
   - Using the filter, you can search for items. The two methods are as follows;
     a) Type a string, a word, or a multi-word phrase to find any cell that matches the exact spelling and arrangement.
     b) To search for strings or words that co-occur with variations, use a Regular Expression; for example, the regular expression `data.*inc` finds any individual cell that contains this combination: “data” and any string and “inc”. The filter searches all cells; therefore, you do not need to specify a column for the search.
2. Click **Next**.

5.23.6.3 Selecting the restore options

1. To record all restored files in the Activity Log, select the **Detailed log** check box.
2. To skip the pre and post restore processes, select the **Skip Pre/Post** check box. If this check box is clear, click **Pre/Post**. DS-Client will run a specified activity before and/or after a restore operation. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525.
3. To use the backed up schema(s) to clear the tables and then rebuild them in the Salesforce database, select the **Restore Schema** check box.This option is useful if the structure of any tables have changed since the backup session you are restoring.
4. To minimize the number of API call counts made by the restore process, select the **Use Bulk API** check box. This option is selected by default. When files are uploaded via Bulk API, a file size limit of 10 MB is enforced by Salesforce.

NOTE: Ensure that you clear this check box if the data to be restored contains files that are larger than 10 MB.

---

5. To enforce DS-Client to trace the ID change and fill the foreign key with the new ID that was inserted, thereby maintaining the relationship between tables, select the **Restore with automatic relationship fix** check box. This is applicable if you are restoring multiple tables at the same time.
   - To include all backed up tables that are related to the table being restored, select the **Include all referenced tables automatically** check box.
   - To enforce DS-Client to find any missing referenced records based on a comparison of the name columns, select the **Additional relationship fix based on name comparison** check box.
6. To prevent existing data from being restored and duplicated, select the **Detect duplicate records by name comparison** check box.
7. To enable the restore process to resume in the event that it is stopped during the uploading stage, select the **Save temporary database file in local storage for resume** check box. For more information, see Section 5.23.7, “Resuming a Salesforce data restore process”, on page 508.
8. To remove the selected tables from the online Salesforce database, before performing the restore to re-populate those tables, select the **Delete all records before restoring** check box.
9. Click **Next**.

5.23.6.4 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, select the type of restore. The options are as follows:
   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.
3. Click **Finish**.

5.23.7 Resuming a Salesforce data restore process

The uploading stage of a Salesforce restore can be time consuming as the DS-Client uploads the restored tables and/or items to an online Salesforce account. If the process stops for any reason during the uploading stage, you can resume the restore.

Before you start to restore a Salesforce backup, consider the following:

- Select the **Save temporary database file in local storage for resume** check box.
- Before stopping a Salesforce restore process, determine the current stage of the process by checking the Description in the real-time Activity Monitor.

NOTE: A Salesforce restore process can be resumed only if it is stopped during the uploading stage.

---

1. On the **Restore** menu, click **Resume restore**. A list appears with all restores of Salesforce backups for which the option **Save temporary database file in local storage for resume** was selected. A cache is created for each table in the local storage. you can view the parameters DS-Client is using for each restore in the list, including a summary of the options selected for the restore.
2. To view more information on a specific restore process, select a backup from the list, and then click **Shows status**.

3. Click **OK**.

NOTE: Before resuming the restore process of a backup, select the backup and verify the details . If you notice discrepancies, do not resume the restore. You can start a new restore with the correct settings.

4. Click **Resume**.

5.24 VMware vCenter Server backups (Windows or Linux)

You can back up and restore virtual machines using the native VMware vStorage API for Data Protection (VADP).

NOTE: The DS-Client automatically locks the target virtual machine during the VMware vCenter Server backup and restore process. This prevents any attempts to delete or migrate the target until the backup or restore process has completed.

Before working with VMware vCenter Server backups, ensure the following requirements are met.

- For application consistent backups, ensure VMware Tools is installed on the guest operating system of the virtual machine.
- Firewalls are configured correctly and allow the DS-Client to communicate with the VMware vCenter Server and each ESXi host of the cluster via port #902.
- If an ESXi host is added with the DNS name of the VMware vCenter Server, the DS-Client machine must have name resolution to the ESXi host to back up or restore the virtual machines.
- To restore to an alternate location, the DS-Client must have network access to the destination VMware vCenter Server and all involved ESXi hosts.
- To use the Local DS-VDR option, you must configure the Local DS-VDR Tool for the DS-Client and have a VMware vCenter Server account with administrator privileges. For more information, see Section 2.6, “Configuring the Local DS-VDR Tool”, on page 68.

To perform a backup or restore of a VMware vCenter Server backup, you must create a user role with the following permissions:

- Datastore: Allocate space
- Datastore: Browse datastore
- Datastore: Low level file operation
- Folder: Create folder
- Global: Disable methods

- Global: Enable methods
- Global: Licenses
- Network: Assign network
- Resource: Assign virtual machine to resource pool
- Resource: Create resource pool
- Virtual machine: Change Configuration (with all sub-options)
- Virtual machine: Edit Inventory: Create new
- Virtual machine: Edit Inventory: Register
- Virtual machine: Edit Inventory: Unregister
- Virtual machine: Interaction: Power off
- Virtual machine: Interaction: Power on
- Virtual machine: Provisioning: Allow disk access
- Virtual machine: Provisioning: Allow read-only disk access
- Virtual machine: Provisioning: Allow virtual machine download
- Virtual machine: Provisioning: Allow virtual machine files upload
- Virtual machine: Snapshot management (with all sub-options)

Each user assigned to this role requires access to the following levels of the VMware vCenter Server:

- vCenter
- Datacenter
- Cluster
- Host
- Datastore
- Network interface

NOTE: To prevent users from having access to all underlying levels, clear the “Propagate to children” option for each level.

Select the folder containing the virtual machines to be backed up, and then add the user and assign the Administrator role to allow Web GUI full control access to the folder. To be able to back up subfolders, select the "Propagate to children" option.

5.24.1 Backing up virtual machines in a cluster

Backing up virtual machines in a VMware cluster should be done through the VMware vCenter Server. Normally, the VMware DRS (Distributed Resource Scheduler) cluster automation level is configured to be Fully automated for High Availability. This means the individual virtual machines that make up the cluster will be dynamically assigned to the best suited host at startup.

A virtual machine can be automatically moved to another host when the VMware cluster or virtual machine is restarted. If the virtual machine moves to another host, it will not be found by the DS-Client on backup and errors will occur. If the virtual machine is selected using the VMware vCenter Server IP address, the location of the virtual machine is always known, even if it moves to another host.

If you must back up a specific virtual machine in a VMware cluster with a dedicated backup using a specific host machine's IP address, you must configure the cluster to not move that virtual machine to different hosts:

- In the Virtual Center, edit the VMware DRS cluster settings: “Enable individual virtual machine automation levels”.
- For the virtual machine that you want, change its **Automation Level** setting to **Disabled** to prevent the VMware vCenter Server from migrating it.

5.24.2 Performing an incremental restore

Before performing an incremental virtual machine restore, consider the following:

- Incremental restore is available only on a Linux DS-Client.
- The virtual machine must already exist in the target restore destination as a result of a previous virtual machine restore.
- To perform an incremental virtual machine restore, you must select the **Attempt incremental restore** check box. Otherwise, the DS-Client performs a full virtual machine restore by default.
- In the first restore session after a VMware vCenter Server backup has been configured for an incremental virtual machine restore, the DS-Client performs a full virtual machine restore and saves the backup information with the restored virtual machine. On subsequent restores, the DS-Client attempts an incremental virtual machine restore for that restore session until you clear the check box.
- When a restored virtual machine is powered on, the VM configuration parameters will likely change. As a result, the DS-Client disallows further incremental virtual machine restores and forces a full virtual machine restore in the next restore session.
- To test a restored virtual machine, clone the virtual machine using the VMware tools, and use the clone. Do not test the restored virtual machine directly.

- Do not power on a restored virtual machine in the VMware vCenter Server unless you are using the restored virtual machine as a production machine.
- During an incremental virtual machine restore, the DS-Client compares the backup generation to be restored and the virtual machine at the destination location. If the DS-Client detects any differences in the virtual machine configuration parameters, it forces a full virtual machine restore.

5.24.3 Using VMware transport libraries

VMware transport libraries are included with the DS-Client to allow VMware to take advantage of the different transport modes that are supported when accessing the VMware VMFS datastore using the Fibre Channel (FC), Fibre Channel over Ethernet (FCoE), or iSCSI protocols.

By default, the DS-Client uses VADP and VDDK APIs to interact with the VMWare ESXi environment for backup and restore. The DS-Client automatically uses the most efficient transport mode available and deduplicates, compresses, and encrypts the virtual machine before sending the data to the DS-System. For more information, see the VMware documentation.

The following VMware virtual disk transport methods are used:

- **NBD (Network Block Device)** and **NBDSSL (encrypted) transport mode** — Allows you to transfer data over the LAN when the DS-Client is running on a physical or virtual machine and does not have direct access to the VMware VMFS datastore. The DS-Client reads from the .vmdk virtual disks where the data is stored and transfers the data from the ESXi host to the DS-Client.
- **SAN (Storage Area Network) transport mode** — Allows you to transfer data over the SAN when the DS-Client is running on a physical machine and has direct access to the VMware VMFS datastore. The DS-Client reads the data directly from the SAN storage where the .vmdk virtual disks are stored. No data is transferred over the LAN from the ESXi host to the DS-Client. When using this method to perform a restore, the DS-Client automatically disables the CBT parameters in the virtual machine advanced settings.
- **HotAdd transport mode** — Allows you to transfer data over the SAN when the DS-Client is running on a virtual machine and has direct access to the VMware VMFS datastore where the source virtual machines are located. The DS-Client reads the data directly from the SAN storage where the .vmdk virtual disks are stored. No data is transferred over the LAN from the VMware ESXi host to the DS-Client. The HotAdd transport mode is supported only when the virtual machines being backed up are using SCSI virtual disks.

5.24.4 Creating a VMware vCenter Server backup

You can create a VMware vCenter Server backup.

5.24.4.1 Selecting the type of backup

1. On the **Sets** menu, click **New Backup Set**.
2. Select **VMware VADP**, and then click **Next**.

5.24.4.2 Selecting the backup source

1. In the **Path** box, type the IP address of the VMware ESXi server or VMware vCenter Server. For Linux DS-Clients, type the path in the following format:

   ```
   VMware vCenter Server\IP_Address
   ```

   NOTE: When an ESXi host is managed by a VMware vCenter Server, you must point to the IP address of the VMware vCenter Server. You can point to the IP of an ESXi host only if the host is a standalone ESXi host that is not managed by a VMware vCenter Server.

2. To specify credentials for the DS-Client to connect to the VMware ESXi server or VMware vCenter Server, select the **Ask for Network Credentials** Windows) or **Ask for VMware logon credentials** (Linux) check box. When prompted, provide the credentials for the DS-Client to connect to the VMware ESXi server or VMware vCenter Server.
3. Click **Next**.

5.24.4.3 Selecting the backup items

NOTE: For Windows DS-Clients, the VMware folder listings are cached when browsed for the first time in a DS-User session. To refresh the listing of the VMware vCenter Server, disconnect and reconnect to the DS-Client.

1. In the **Shares & Directories list**, browse and select the VM you want to back up, and click **Add**.
2. To exclude an item when its parent directory is selected for backup, select the item, and then click **RegEx**.
3. To view details about an item, select the item, and then click **Files**.
4. To remove an item, select an item, and then click **Remove**.

5. Click **Next**.

5.24.4.4 Selecting the backup item options

NOTE: If you plan to enable the Local DS-VDR option, the backup item generations (Max Gen) setting determines how many versions of a virtual machine will be exported to the VMware vCenter Server. When this limit has been reached, the oldest exported virtual machine is overwritten at the next backup.

1. To configure the maximum generations for a backup item that will be stored online, double click the **Max Gen** cell, and then enter the value.
2. Click **Next**.

5.24.4.5 Selecting the backup options

1. Configure the options for the backup. The options are as follows:
   - **Detailed log** – Records all files that are backed up in the Activity Log. For more information, see Section 8.1, “Viewing the Activity Log”, on page 578.
   - **Initial backup** – Uses the Initial Backup feature for the first backup. To configure the initial backup path, click **[>>]**. For more information, see Section 11.1.1, “Configuring the initial backup path”, on page 618.
   - **Stop on errors** – Stops a backup process when the number of errors reaches the specified value. A value of 0 means the DS-Client does not stop a backup process regardless of the number of errors.

     NOTE: You can configure the default setting using the **MaxErrors** advanced configuration parameter. For more information, see Section 2.1.8.6, “Miscellaneous parameters (Windows)”, on page 42.

   - **Compression type** – Specifies the type of compression that will be applied to the backup. The options are as follows:
     - **LZOP** – A faster compression than ZLIB, but comes at the expense of less compression. This is a good default compression when the network is not the bottleneck.
     - **ZLIB (Global, Low, Medium, and High)** – Normally produces better compression than LZOP, but will take more time to compress. This is a good default compression when the bottleneck is the network. ZLIB Low corresponds to a value of 3, ZLIB Medium = 6, and ZLIB High = 9.
     - **None** – Disables compression for the backup.

2. Configure additional options for the backup as follows.

   - To enable pausing of the applications to guarantee consistent and usable backup, select the **Attempt to quisce I/O before taking backup snapshot** check box.
   - To enable the DS-Client attempt to reconfigure virtual machines to use Changed Block Tracking (CBT), do one of the following:
     - For Windows, select the **Attempt to use CBT for backing up Virtual Machines** check box.
     - For Linux, select the **Attempt to use Change Block Tracking for backing up Virtual Machines** check box. For more information, see Section 5.2.1, “Changed block tracking (CBT)”, on page 108.
   - To configure the VMware vCenter Server backup to be able to perform a file-level restore, select the **Use FLR** check box.

     NOTE: To perform FLR from a local storage location on a Linux DS-Client, you must enable both the FLR and CBT options.

   - To use the Local DS-VDR tool, select the **Use Local DS-VDR** check box (only for Windows).

     NOTE: Each virtual machine you add uses one count from the Local DS-VDR license that has been allocated to the DS-Client.

   - To save the virtual machine state, including any running programs that are loaded in memory, select the **Backup Virtual Machine Memory** check box. This ensures the state of the target virtual machine matches the state of the source virtual machine.

     NOTE: The target virtual machine is automatically powered off (or placed in suspended mode if using Local DS-VDR) and functions as a standby virtual machine to avoid network conflicts.

   - To specify the number of generations after which the system should verify the disk signature, select the **Verify disks signature interval (generations)** check box, and then enter the number of generations.

- To specify on which days the system should verify the disk signature, clear the **Verify disks signature interval (generations)** check box, and then select the days on which you want the process to be performed.

NOTE: The **Verify disks signature** option is available only if you have enabled Changed Block Tracking (CBT).

3. To export the actual running virtual machine and all its snapshots, select the **Backup Virtual Machine's snapshots** check box. If this check box is not selected, DS-Client will only export the actual running virtual machine without snapshots.
4. In the **Export to host** list, select the destination ESXi host on the VMware vCenter Server to which you want to export the selected virtual machines. Then click **[>>]** to provide credentials for DS-Client to access the selected host.
5. In the **Export to datastore** list, select the datastore on the destination host to which you want to export the selected virtual machines.
6. Click **Next**.

5.24.4.6 Selecting the notification options

1. To configure a notification, do one of the following:
   - To add a notification, click **Add.**
   - To modify a notification, select the notification, and then click **Modify.**

NOTE: To delete a notification, select the notification, and then click **Delete**.

2. To send an email notification, select **E-Mail**. and then do the following:
   a) To send the email notification to the DS-Client administrator, select **Administrator**.
   b) To send an email to another recipient, select **Other**, and then specify the recipients email address.
   c) To send detailed backup information, select the **Detailed notification** check box.
   d) To include a detailed file-level backup log as an attachment, select the **Attach detail log** check box.

e) To send the email notification in HTML format, select the **Send E-Mail using HTML format** check box.

NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

---

f) Click **OK**.

3. To send a pager notification, select **Pager**. The notification will be sent to the pager account configured for the DS-Client.

NOTE: The pager option is available only if the DS-Client has been configured for pager notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

---

g) To send a broadcast notification, select **Broadcast** (only for Windows). Select the server containing the messenger service to which you want to send the message and click **OK**.

NOTE: Broadcast notifications to domains or workgroups are limited to 128 characters.

---

h) To send an event notification, select **Event** (only for Windows). Select the server on which you want the notification to be recorded in the Event Log.

i) In the **Completion** box, specify under what conditions a notification will be sent and then click **OK**. The options are as follows:

- **All** – Notification will be sent under all conditions.
- **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
- **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.
- **Completed with errors** – Notification will be sent if an activity is completed with at least one error event.
- **Incomplete** – Notification will be sent if an activity is not completed successfully.

4. Configure the DS-Client to send SNMP traps when the backup has completed successfully, completed with warnings, completed with errors, or is incomplete.
5. Click **Next**.

5.24.4.7 Assigning a retention rule

1. To assign a retention rule to the backup, do one of the following:
   - If you don't want to assign a retention rule, select **No retention rule**.
   - To assign a retention rule, select **Use a specific retention rule**, and then select the retention rule.

NOTE: To create or edit a retention rule, click **[...]**. For more information, see Section 4.1, "Configuring a retention rule", on page 98.

---

2. Click **Next**.

5.24.4.8 Assigning a schedule

1. To assign a schedule to the backup, do one of the following:
   - If you don't want to assign a schedule, select **Not scheduled**.
   - To assign a schedule, select **Scheduled.** In the **Available schedules** box, select an existing schedule.

NOTE: To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, "Configuring a schedule", on page 90.

---

2. Click **Next**.

5.24.4.9 Naming the backup

1. In the **Set name** box, type a name for the backup.
2. In the **Set type** box, select the type of backup you want to create. The list of available backup types depends on the configuration of your DS-Client.
   - Online
   - Self-contained
   - Local-only
   - Instant Recovery
   - Statistical

NOTE: For more information, see Section 5.1, "Backup types", on page 106.

---

3. If you selected **Online**, do the following:

   a) To send a copy of the oldest generation of the file that is about to be overwritten from the DS-System to the BLM Archiver, select the **BLM (Infinite Generations)** check box.

   NOTE: The Backup Lifecycle Management tool must be enabled for the DS-Client.

   b) To save a copy of the backup data to a local storage location on the DS-Client computer, select the **Save on Local Storage** check box.

   - Beside the **Local Storage Path** box, click **[>>]**, enter a specific local storage path for the backup, and then click **OK**.

   NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path. This option is automatically enabled for Self-contained and Local Only backups.

   c) To use the local storage as a cache if the DS-Client loses connection with the DS-System, select the **Transmission cache on Local Storage** check box. The cached backup data will be sent to the DS-System on the next connection after synchronization.

   - Beside the **Local Storage Path** box, click **[>>]**, enter a specific local storage path for the backup, and then click **OK**.

   NOTE: You must enable the Local Storage tool for the DS-Client and configure a local storage path.

   d) To save the online backup to an instant recovery vault, select the **Save in instant recovery vault** check box.

   - Beside the **Local Storage Path** box, click [>>], enter a specific local storage path for the backup, and then click **OK**.

   NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

4. If you selected **Self-Contained**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**.

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

5. If you selected **Local-Only**, beside **Local Storage Path**, click **[>>]**. Enter a local storage path for the backup, and then click **OK**..

NOTE: If you do not enter a specific local storage path for the backup, the default local storage path will be used. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

---

6. If you selected **Instant Recovery**, the **Save in instant recovery vault** option is selected by default.

IMPORTANT: Each Linux DS-Client must have a unique ZFS file name.

---

7. If you selected **Statistical**, and want to emulate an actual backup transfer process, select the **Calculate transmit amount** check box. During the backup, specified backup files will be read from their source and processed for compression and encryption.
8. If the multitenant feature is enabled and configured, in the **Customer** list, you can select the customer to which you want to assign the backup. For more information, see Section 11.5, “Multitenant DS-Clients”, on page 634.
9. Click **Finish**.

5.24.5 Restoring a VMware vCenter Server backup

You can restore data from a VMware vCenter Server backup.

NOTE: We recommend restoring only one backup at a time. Restoring multiple backups concurrently can affect performance.

5.24.5.1 Selecting the restore items

1. Browse the backups tree and select the backup you want to restore.
2. On the **Restore** menu, click **Restore Now**.

5.24.5.2 Selecting the restore level

1. To restore an entire virtual machine, select **VM-level Restore**.You can restore one or multiple virtual machines.

   NOTE: To perform an incremental restore of the selected virtual machines, select Attempt incremental restore. This option is available only for Linux DS-Clients.

2. To restore individual virtual disks for one or multiple virtual machines, select **VM Disk-level Restore**. This option is available only for Linux DS-Clients.
3. To restore individual files or directories for one or multiple virtual machines, select **File-level Restore**.

5.24.5.3 Selecting the restore items

1. If you selected **VM-level Restore**, select a virtual machine. The color in which each virtual machine is displayed indicates the status of the backup generation that will be used for the restore:
   - Green indicates that the backup generation contains the expected number of virtual disks.
   - Red indicates that the backup generation does not contain the expected number of virtual disks. It also indicates that the virtual machine was backed up partially.
2. If the entire virtual machine is not available to be restored from the backup period selected, the item is unavailable for you to select. To view the backup period that has been selected, click **Advanced**.

   NOTE: Unless you click **Advanced** and specify a different generation, the status is determined based on the most recent backup generation.

3. If you selected **VM Disk-level Restore**, browse the tree, select a virtual machine, click **Show Files** to view the *.vmdk files in each folder, and then select individual virtual disks from the list.
4. If you selected **File-level Restore**, browse the tree, select an individual directory, click **Show Files**, and select individual files from the list.
5. To view the number of files selected and calculate the total amount of files selected, select the **Calculate amount** check box.
6. To exclude subdirectories, clear the **Include SubDirs** check box, as the default setting is to include sub-directories.

7. To filter the list of files, in the **Filter box**, enter a filter using * as a wildcard, and then click **Show Files** to update the list of files.
8. To find a backed up file, click **Show Files**, click **Find File**, and then in the **Find Backed Up File** dialog box, do the following:
    a) Select the search criteria to search for a backed up file either by **File name** or by **File ID**.
    b) Click **Find**.
    c) Select the required backed up file, and then click **Select**.
9. In the **Files List** section, do one of the following:
    - To view details about the backed up file, select the file, and then click **File Info**.
    - To view the details of the items you selected, click **Selection**.
    - To view a list of archived generations for a folder, do the following:
        a) In the **Directories Tree**, select the folder, and then click **Show Files**.
        b) Under **Files**, click **Show Archived**.
10. To refine your selection of items to restore, click **Advanced**, and then select which generation you want to display. The options are as follows:
    a) To restore the latest generation of all the files, select **Latest generation of all data**.
    b) To restore files from a specific period, select **Selective data (from a certain period)**, and then do the following:
        1. Beside **From**, click **[>>]**, and then select a start date and time. No backup sessions before this date will be displayed.
        2. Beside **To**, click **[>>]**, and then select an end date and time. No backup sessions after this date and time will be displayed.
        3. Click **OK**.
11. Click **Next**.

5.24.5.4 Selecting the restore location

1. Select the location to which you want to restore the backup. The options are as follows:

   - **Original location** – Data is restored to the original backup source location and existing files with the same name are overwritten. This is the default option.
   - **Alternate location** – Data is restored to a location other than the original backup source. For more information, see Section 5.24.5, “Restoring a VMware vCenter Server backup”, on page 520.

   NOTE: When restoring to an alternate location, the security of restored items in the destination location might not resemble the security of those items during backup.

   - **Show Datastores/Hide Datastores** – Opens or hides the files list for the selected virtual machine only if you are restoring a full virtual machine.

2. If you selected **Original location**, the **Ask for Network Credentials** check box is selected by default.When prompted, type the required credentials to connect to the VMware vCenter Server.

3. If you selected **Alternate location**, then do the following:

   a) Beside the **Alternate location** box, click **[>>]**.

   b) In the **Select Alternate Server** dialog box, select the computer where you want to restore the data.

   c) To provide the credentials for the selected computer, select the **Ask for Network Credentials** checkbox, and then click **Select**.

   - For Linux DS-Client:

     a) Click the VMware vCenter Server icon to type the prefix for the path field.

     b) In the **Path** box, type the IP address of either a VMware vCenter Server or a VMware ESXi host in the following format – VMware vCenter Server\IP_Address, and then click **Select**:

     c) When prompted, type the VMware logon credentials, and then click **OK**.

   - For Windows DS-Client:

a) Type the IP address in the **Path** box.

b) When prompted, type the VMware logon credentials, and then click **OK**.

NOTE: After you select a computer as the alternate location, you must specify a share location

d) Do the following:

1. Click in the **Folder path** cell, type the destination folder location, or click **[>>]**, and then select the target Virtual machine or directory.
2. Double click in the **VM Name** cell, and type the name of the target virtual machine when it is restored.
3. Click in the **Host** cell, select the destination ESXi host to which the virtual machine will be restored.
4. Click in the **Datastore** cell, and select the datastore on the selected destination host to which you are restoring the individual disks.

4. Click **Next**.

5.24.5.5 Selecting the restore options

1. To skip the pre and post restore processes, select the **Skip Pre/Post** check box. If this check box is cleared, the DS-Client runs a specified activity before and/or after a restore operation. For more information, see Section 5.25, “Configuring Pre/Post processes (Windows)”, on page 525.
2. To record all restored files in the Activity Log, select the **Detailed log** check box.
3. Select the required restore options. Depending on your restore selection, the additional restore options can change.
   - To start the virtual machine if it is successfully restored, select the **Power on VM after restore** check box.
   - To unregister the VM from the VMware vCenter Server after the restore is complete, select the **Unregister VM after restore** check box.
   - To append the restore time to the name of the virtual machine, select the **Add time stamp to VM name** check box.
   - To enable DS-Client to restore the virtual machine using SAN transport mode, select the **Use SAN with all disk types** check box.
4. Click **Next**.

5.24.5.6 Selecting the reason for the restore

1. In the **Restore reason** box, select the reason for the restore.
2. If the backup is currently in a scheduled recovery drill period, select the type of restore. The options are as follows:
   - **Real production recovery, resulting from data loss** — Select this type to perform a normal restore for a real data loss.
   - **Stop DR Drill restore if DR Drill capacity is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to stop when your DR Drill capacity runs out.
   - **Augment with production recovery capacity if DR Drill is fully used** — Select this type if the restore is a Recovery Drill and you want the restore to continue when your DR Drill capacity runs out. When the DR Drill capacity is used up, the remaining balance of the restore is treated as a production recovery.
3. Click **Finish**.

5.25 Configuring Pre/Post processes (Windows)

You can use the Pre/Post option to specify a command to run before (Pre) and/or after execution (Post) of the backup.

1. Browse the backups tree and select the backup.
2. On the **Sets** menu, point to **Backups**, and then click **Properties**.
3. In the **Set Properties** dialog box, click the **Options** tab, and then click **Pre/Post**.
4. Under **Perform this activity before backup**, do one of the following:
   - To execute a Pre/Post command on a remote machine, where the files of the backup are located, select the **Execute on remote system** check box.

     NOTE: This option is disabled if the backup is on the local DS-Client computer.

   - To run a command, select **Run command**, and then type the command.

     NOTE: You must type “cmd /c” before the command if it is not the name of an executable file. This command must not run anything that requires user input.

  - On a local DS-Client machine, DS-Client will terminate the process if the command requires user input.
  - On a remote Windows machine, the connect as properties of the backup must have administrator privileges because the schedule service is used to run the command on the remote Windows machine.
  - On a remote Linux machine, ensure the rexec service is running on the remote machine.

- To stop a service before backup, select **Stop service**, click **[>>]**, and then select the service.
- To start a service before backup, select **Start service,** click **[>>]**, and then select the service.
- The following options are available only for Netware:
  - **Run NCF**– Runs the command batch file specified in the box on the remote NetWare server. All the rules for running NCF from the console are applied. If the NCF is not in the search path, you must provide the full path (sys:dir_name\name.ncf). The NCF file must be in 8.3 name format, since the console does not understand long file names. You must have Console Operator Rights.
  - **Unload NLM** – Unloads the NLM (NetWare Loadable Module) specified in the box. You must have Console Operator Rights.
  - **Load NLM**– Loads the NLM (NetWare Loadable Module) specified in the box. You must have Console Operator Rights.

5. Select the condition when you want the DS-Client to perform the activity before backup. The options are as follows:
   - **On exit code** – The condition is applied if the exit code (for local commands), is equal (=) or not equal (<>) to the exit code entered in the box. This is applicable if you know that the command will produce an exit code when finished.
   - **On file existence** – The condition is applied if a particular file exists or not. Enter the full path (include the drive on local machines; include the share but not the server on remote machines) in the box.
   - **On output string** – The condition is applied (Local commands & UNIX only) if the command output contains a particular string or not. Enter the string (case sensitive) in the box. For a large output string, only the first 16K is checked for occurrences of the string.
   - **On execution success** – The condition is applied if the command is executed successfully.
   - **On execution failure** – The condition is applied if the command fails to execute.

- **Or execution failure** – Select the **Or execution checkbox** to combine the condition of execution failure with the exit code, file existence or output string conditions.
- **Don't perform Post activity** – If a selected condition is fulfilled, the DS-Client will not perform the post activity.
- **Don't perform backup** – If a selected condition is fulfilled, the DS-Client will not perform the backup and restore.
- **Delay backup** – You can delay the backup/restore in situations where the command activates background processes responsible for creating data for backup. This also allows time for the pre activity to terminate properly.

NOTE: You must not use Test Pre with the delay option because a delay of more than 60 seconds results in a timeout.

---

6. Under **Perform this activity after backup**, do one of the following:
   - To stop a service after backup, select **Stop service**, click **[>>]**, and then select the service.
   - To start a service after backup, select **Start service,** click **[>>]**, and then select the service.
   - The following options are available only for Netware:
     - **Run NCF**– Runs the command batch file specified in the box on the remote NetWare server. All the rules for running NCF from the console are applied. If the NCF is not in the search path, you must provide the full path (sys:dir_name\name.ncf). The NCF file must be in 8.3 name format, since the console does not understand long file names. You must have Console Operator Rights.
     - **Unload NLM** – Unloads the NLM (NetWare Loadable Module) specified in the box. You must have Console Operator Rights.
     - **Load NLM**– Loads the NLM (NetWare Loadable Module) specified in the box. You must have Console Operator Rights.
7. Select the condition when you don't want the DS-client to perform the activity after backup. The options are as follows:
   - **Successful** – The DS-Client will not perform the activity if the backup or restore is successful.
   - **With errors** – The DS-Client will not perform the activity if the backup or restore is completed with errors.
   - **Incomplete** – The DS-Client will not perform the activity if the backup or restore is incomplete.

8. Click **Test Pre** or **Test Post** to test the command.

IMPORTANT: You must not use Test Pre and Test Post with a combination of Stop Service and Start Service commands, because this will only execute the Pre command, effectively stopping a service until you manually restart the service.

9. Click **OK**.

5.26 Configuring Pre/Post processes (Linux)

You can use the Pre/Post option to specify a command to run before (Pre) and/or after execution (Post) of the backup.

1. Browse the backups tree and select the backup.
2. On the **Sets** menu, point to **Backup Sets**, and then click **Properties**.
3. In the **Set Properties** dialog box, click the **Options** tab, and then click **Pre/Post**.
4. Under **Before backup**, do the following:
   a) Select the **Execute** check box, and type the command you want to run before backup. Click **Test** to verify the command.
   b) To apply a condition if the exit code is equal (=) or not equal (<>) to the exit code entered in the box, select the **On exit code** check box. This is required if you know the command will produce an exit code when finished.
   c) Select the **Do not perform backup** check box, if you do not want the DS-Client to perform the backup when the exit code condition is fulfilled.
   d) Select the **Do not perform backup post activity** check box, if you do not want the DS-Client to perform the post activity when the exit code condition is fulfilled.
5. Under **After backup**, do the following:
   a) Select the **Execute** check box, and type the command you want to run after backup.
   b) To execute the command after the backup data has been copied to the DS-Client buffer, select the **Execute after data has been copied to DS-Client buffer (if applicable)** check box.
   c) Click **Test** to verify the command.
6. Under **Before restore**, do the following:

a) Select the **Execute** check box, and type the command you want to run before backup.

b) To apply a condition if the exit code (for local commands), is equal (=) or not equal (<>) to the exit code entered in the box, select the **On exit code** check box. This is applicable if you know that the command will produce an exit code when finished.

c) Select the **Do not perform restore** check box, if you do not want the DS-Client to perform the restore when the exit code condition is fulfilled.

d) Select the **Do not perform restore post activity** check box, if you do not want the DS-Client to perform the post activity when the exit code condition is fulfilled.

e) Click **Test** to verify the command.

7. Under **After restore**, do the following:

   a) Select the **Execute** check box, and type the command you want to run after backup.

   b) Click **Test**.

8. Click **OK**.

5.27 Disabling CDP for a backup

1. If a backup session for a backup with CDP is in progress, stop the backup session.
2. In the backups tree, right-click on the backup for which you want to disable CDP, and then click **Properties**.
3. Click the **Options** tab, and then clear the **Continuous data protection** check box.
4. Click **OK**.

6 Managing backups

You can manage the backups you have created.

6.1 Performing an on-demand backup

The system is designed to perform unattended backups at scheduled intervals. However, you can perform on-demand backups at any time if required.

NOTE: Another type of backup that you can perform outside of a schedule is called initial backup. For more information, see Section 11.1, “Initial backups”, on page 617.

To perform an on-demand backup:

1. Click the **Backup Sets** tab.
2. Select the backup for which you want to perform an on-demand backup.
3. On the **Backup** menu, click **Backup Now.**
4. Select the items you wan to include in the backup.
5. Select the options for the selected items, and then click **Next**.
6. To copy files to the DS-Client buffer, select the **Use buffer** check box. This frees up the backup source as fast as possible. The DS-Client then sends the files from the DS-Client buffer to the DS-System.
7. To record all files that are backed up, select the **Detail log** check box.
8. To delay starting the backup, select the **Start at** check box, and then enter the time you want the backup to start. Leave this box blank to start the demand backup immediately.
9. To read the digital signature from the latest online generation of each unchanged file and compare it with the digital signature that was generated from the current source file, select the **Verify signature for unchanged files** check box. If the signatures do not match, DS-Client backs up the file again in the same backup session.

   This option is available only for File System backups and email backups that use DS-MLR. It applies only to the latest file generation and cannot be used with the Use Buffer option.

   IMPORTANT: Selecting this option slows down the backup performance because unchanged files that are normally skipped must be processed.

10. In the **Stop on errors** box, enter the number of errors that must occur before a backup is stopped.
11. To perform a scan of all the files in the backup to estimate a time for completion, select the **PreScan** check box.
12. In the **Default operation** box, specify how DS-Client should handle any open files during backup. The options are as follows:
    - **Try deny write** – Attempts to open a backup file in the Deny write mode. If the file is already open, DS-Client places the backup file in the Allow write mode.
    - **Deny write** – Prevents any other process from writing to the backup file, if it is open in the DS-Client.
    - **Prevent write** – Attempts to open the backup file in the Deny write mode. If the file is already open, DS-Client places the backup file in the Allow write mode and locks it.
    - **Allow write** – Allows another process to read/write to the backup file. This can affect file consistency.
13. In the **Retry times** box, enter the number of times you want the DS-Client to attempt to back up the file.
14. In the **Retry interval** box, enter the interval between the retry attempts.

NOTE: These options do not guarantee that an open file will be backed up. To back up locked files, you must use the VSS option or a VSS backup.

---

15. To back up data on remote media, select the **Back up data in Remote Storage** check box.
16. To back up each instance of a file separately, select the **Back up Single Instance Store/Data Deduplication file data** check box. This option is only available if the operating system supports the Single Instance Store service.
17. To back up all data in a folder referenced by a junction point, select the **Follow junction point** check box.

NOTE: Junction points are links to other folders. If disabled, only links to the folder are backed up. Junction points that are mounted FAT or FAT32 volumes are not supported.

---

18. Click **Finish**.

6.1.1 Excluding files that failed to be backed up

There can be specific files or files with specific extensions that cannot be backed up from the source. You can exclude these files from the backup.

1. Click the **Backup Sets** tab.
2. On the **Sets** menu, point to **Backup Sets**, and then click **Properties**. The **Backup Set Properties** dialog box appears.
3. Click the **Items** tab.
4. Click **Edit**.
5. Click **Failed Files**. The file list displays every file that failed to back up since this backup was created.
6. Select files to exclude in one of two ways:
   - Use the CTRL or SHIFT key to select multiple files.
   - Select a failed file and select **Custom Exclude** to exclude all files with the same file extension located in the selected path.
7. Click **Exclude**. The **Edit Items** dialog box appears with the selected files in the list of backup items selected.
8. In the **Edit Items** dialog box, click **Close**.
9. In the **Backup Set Properties** dialog box, click **OK** to save the changes.

6.2 Working with instant recovery backups

You can use instant recovery backups to save uncompressed and unencrypted backup data in its native format to a configured storage location called an instant recovery vault.

Two backup configurations can send backup data to the instant recovery vault:

- **Instant recovery backup type —** This is a dedicated backup type for instant recovery. Each time a backup is run, a new generation is stored in the instant recovery vault up to the maximum number of generations configured.
- **Online backup type** with the **Save in instant recovery vault option —** This backs up data to both online storage and the instant recovery vault.

The following types of backups can be configured for instant recovery:

- File System
- Microsoft Exchange Server (VSS-aware)
- Microsoft Hyper-V Server (VSS-aware)
- Microsoft SharePoint Server (VSS-aware)
- Microsoft SQL Server (VSS-aware)
- VMware vCenter Server

IMPORTANT: Instant recovery backups are not supported in the Management Console. You must use DS-User to back up, restore, configure, and delete instant recovery backups.

Before working with instant recovery backup:

- Ensure the DS-Client account on the DS-System is configured with the Local Storage DS-Tool.
- Ensure both the **Local Storage** and **Local-only** tools are enabled.
- If you are configuring an online backup type with the instant recovery vault option, ensure the **Local Storage** tool is enabled.

To verify these settings, on the **Setup** menu, click **View Quotas**, and then click **DS-Tools**. If they are not enabled, contact your service provider.

NOTE: To perform an instant recovery of a backup, you must have at least one generation of backup data in the instant recovery vault.

6.2.1 Creating an instant recovery backup

By default, instant recovery backup data will be saved to the local storage path configured for DS-Client. However, you can configure a different location for the instant recovery vault.

IMPORTANT: Ensure the instant recovery vault has sufficient capacity and is accessible by both the DS-Client service and the backup source server.

To create an instant recovery backup:

1. Configure the backup.
2. Do one of the following:
   a) To configure a backup that sends data only to the instant recovery vault, in the **Set Type** box, select **Instant Recovery**.
   b) To configure a backup that sends data to both the DS-System online storage and the instant recovery vault, in the **Set Type** box, select **Online**, and then select the **Save in instant recovery vault** check box.
3. To configure the location of the instant recovery vault:
   a) Beside the **Local Storage Path** box, click **>>**.
   b) In the **Path** box, specify the location of the instant recovery vault for this backup.
   c) Click **OK**.

   NOTE: If you are using a Linux DS-Client, you must configure the ZFS storage volume that serves as the instant recovery vault. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

   ---

4. Click **Finish**.

6.2.2 Performing instant recovery (File system)

Before performing instant recovery of a File system backup:

- The DS-Client service account must be run under a local administrator account and have write access to the instant recovery vault.
- You must provide simple access to a share that is immediately accessible on your network.
- For Windows DS-Clients, special file system items (System State and Services Database) are not supported for instant recovery.
- For Linux DS-Clients, hard links and soft (or symbolic) links are not supported for instant recovery.

NOTE: When performing an instant recovery of a Windows File system backup, symbolic links are restored as files.

To perform instant recovery of a File system backup:

1. Click the **Backup Sets** tab.
2. Select the backup you want to instantly recover.
3. On the **Restore** menu, click **Instant Recovery**.
4. Select a backup session, and then click **Next**.
5. If you are using a Windows DS-Client, type the share name used to connect to the instant recovery data. You must map to this computer and share to access the data.
6. If you are using a Linux DS-Client, type the name of the subfolder you want to create on the instant recovery vault. You must map to this computer and folder to access the data.
7. Click **Finish**.

6.2.3 Performing instant recovery (Exchange Server)

Before performing instant recovery of a Microsoft Exchange Server backup:

- The DS-Client service account must be run under a local administrator account and have write access to the instant recovery vault.
- The Microsoft Exchange Server must be running and configured with sufficient credentials to operate in the Windows domain of the database server so that it can accept the data from the instant recovery vault.
- The destination Microsoft Exchange Server must have the same domain name and Microsoft Exchange Server name as the backup source.
- The instant recovery vault can reside on the original Microsoft Exchange Server or a dedicated Microsoft Exchange Server. The path to the instant recovery vault must be unique to each DS-Client.

To perform instant recovery of an Exchange Server (VSS-aware) backup:

1. Click the **Backup Sets** tab.
2. Select the backup you want to instantly recover.
3. On the **Restore** menu, click **Instant Recovery**.
4. Select a backup session, and then click **Next**.
5. Select the components to restore, and then click **Next**.
6. In the **Share name** box, type the share name that is used to connect to the instant recovery data. Users must map to this computer and this share to access the data.
7. Click **Finish**.

NOTE: After an instant recovery share has been activated, you can use the files to recover the database and mount it to the Microsoft Exchange Server. For more information, see the Microsoft Exchange documentation.

6.2.4 Performing instant recovery (Hyper-V Server)

Before performing instant recovery of a Microsoft Hyper-V Server backup:

- The DS-Client service account must be run under a local administrator account and have write access to the instant recovery vault.
- Instant recovery is only supported for Microsoft Hyper-V Server (Standalone) configurations.
- If you want to recover to a different Microsoft Hyper-V Server, ensure that the server version is the same as the original.

To perform instant recovery of a Hyper-V Server (VSS-aware) backup:

1. Click the **Backup Sets** tab.
2. Select the backup you want to instantly recover.
3. On the **Restore** menu, click **Instant Recovery**.
4. Select a backup session, and then click **Next**.
5. Select the components to restore, and then click **Next**.
6. In the **Share name** box, type the share name that is used to connect to the instant recovery data, and then click **Next**.
7. Select the **Mount Virtual Machines to Hyper-V Server** option to configure the destination Hyper-V Server where the DS-Client will mount the restored virtual machines. To restore the virtual machines in the instant recovery vault and manually register the same Hyper-V Server, leave this option cleared.

   IMPORTANT: The instant recovery vault must be located in the Hyper-V Server or the host must be located in the same domain as the Hyper-V Server.

8. Click **Finish**.

6.2.5 Performing instant recovery (SharePoint Server)

Before performing instant recovery of a Microsoft SharePoint Server backup:

- The DS-Client service account must be run under a local administrator account and have write access to the instant recovery vault.
- The credentials used to access the Microsoft SQL Server database when performing an instant recovery must have sufficient rights to create the database.
- The Microsoft SharePoint Server must be running and configured with sufficient credentials to operate in the Windows domain of the database server so that it can accept the data from the instant recovery vault.
- If the Microsoft SQL Server and instant recovery vault reside on the same machine, the SQL Server service account must be able to access the local instant recovery folder.
- If the Microsoft SQL Server and instant recovery vault reside on different machines and the SQL Server service account is a domain account, the SQL Server and instant recovery host machine must be on the same domain.
- If the Microsoft SQL Server and the instant recovery vault reside on different machines and the SQL Server service account is a local account, the account must exist on the instant recovery host machine with the same credentials.

To perform instant recovery of a SharePoint Server (VSS-aware) backup:

1. Click the **Backup Sets** tab.
2. Select the backup you want to instantly recover.
3. On the **Restore** menu, click **Instant Recovery**.
4. Select a backup session, and then click **Next**.
5. Select the components to restore, and then click **Next**.
6. In the **Share name** box, type the share name that is used to connect to the instant recovery data, and then click **Next**. Users must map to this computer and this share to access the data.
7. Configure the Microsoft SQL Server Instance (on the Microsoft SharePoint Server) that will attach to the instant recovery share.
8. Click **Finish**. A popup Instant Recovery Status dialog box appears.

6.2.6 Performing instant recovery (SQL Server)

Before performing instant recovery of a Microsoft SQL Server backup:

- The DS-Client service account must be run under a local administrator account and have write access to the instant recovery vault.
- The credentials used to access the Microsoft SQL Server database when performing an instant recovery must have sufficient rights to create the database.
- The Microsoft SQL Server service account must be running and configured with sufficient credentials to operate in the Windows domain of the database server so that it can accept the data from the instant recovery vault.
- If the Microsoft SQL Server and instant recovery vault reside on the same machine, the SQL Server service account must be able to access the local instant recovery folder.
- If the Microsoft SQL Server and instant recovery vault reside on different machines and the SQL Server service account is a domain account, the SQL Server and instant recovery host machine must be on the same domain.
- If the Microsoft SQL Server and the instant recovery vault reside on different machines and the SQL Server service account is a local account, the account must exist on the instant recovery host machine with the same credentials.

To perform instant recovery of a SQL Server (VSS-aware) backup:

1. Click the **Backup Sets** tab.
2. Select the backup you want to instantly recover.
3. On the **Restore** menu, click **Instant Recovery**.
4. Select a backup session, and then click **Next**.
5. Select the components to restore, and then click **Next**.
6. In the **Share name** box, type the share name that is used to connect to the instant recovery data, and then click **Next**. Users must map to this computer and this share to access the data.
7. Configure the Microsoft SQL Server Instance that will attach to the instant recovery share.
8. Click **Finish**.

6.2.7 Performing instant recovery (VMware vCenter)

Before performing instant recovery of a VMware vCenter Server backup:

- You must have a VMware vCenter Server account with administrator privileges.
- The DS-Client service account must have full rights to access the instant recovery vault to create VSS snapshots and shares.

IMPORTANT: The DS-Client service account must belong to an administrators group. Disable UAC on the local storage host machine if you receive an access denied error.

- You must have additional permission to access the remote local storage computer. The credentials used by the DS-Client service account must have full rights to access the remote instant recovery storage computer WMI and create VSS snapshot and shares (or NFS shares).
- NFS must be installed on the instant recovery vault. Regardless of the disk type of the source virtual machine:
  - For Windows DS-Clients, the disk type of the restored virtual machine will always be Thick Eager Zeroed.
  - For Linux DS-Clients, the disk type of the restored virtual machine will always be Thin.
- All ESXi hosts of the target vCenter must have name resolution to the instant recovery vault. You can add the computer name and IP address of the instant recovery vault to the hosts file of every ESXi host on the target vCenter or add the “computer name and IP address” entry for the instant recovery vault to the DNS server that is used by the ESXi hosts of the target vCenter.

To perform instant recovery of a VMware vCenter Server backup:

1. Click the **Backup Sets** tab.
2. Select the backup want to instantly recover.
3. On the **Restore** menu, click **Instant Recovery**.
4. Select a backup session, and then click **Next**.
5. Select the components to restore, and then click **Next**.
6. If you are using a Windows DS-Client, type the share name used to connect to the instant recovery data, and then click **Next**. DS-Client automatically mounts the share to the selected vCenter using the IP address and credentials.
7. If you are using a Linux DS-Client, type the name of the subfolder you want to create on the instant recovery vault. DS-Client automatically mounts this folder to the selected vCenter using the IP address and credentials .

8. Configure the vCenter that mounts the instant recovery NFS share (Windows) or Snapshot clone subfolder (Linux).
9. Click **Finish**.

6.2.8 Performing a session-level delete

You can perform a session-level delete to remove instant recovery data from backup sessions stored in the instant recovery vault.

To perform a session-level delete:

1. Click the **Backup Sets** tab.
2. Select the backup containing the instant recovery data that you want to delete.
3. On the **Sets** menu, point to **Delete**, and then click **Session Level Delete**.
4. Select the backup session that you want to delete from the instant recovery vault.
5. Click **Finish**.

6.2.9 Performing a machine-level delete

You can perform a machine-level delete to remove virtual machines that have been recovered in the instant recovery vault for VMware vCenter Server backups.

To perform a machine-level delete:

1. Click the **Backup Sets** tab.
2. Select the VMware vCenter Server backup containing the virtual machines that you want to delete.
3. On the **Sets** menu, point to **Delete**, and then click **Machine Level Delete**.
4. Select the virtual machines that you want to delete from the instant recovery vault.
5. Click **Finish**.

IMPORTANT: If you want to delete a VMware vCenter Server backup that is configured for instant recovery, you must first perform a machine-level delete of all its instant recovery virtual machines.

6.3 Renaming a backup

You can rename a backup if required.

To rename a backup:

1. Click the **Backup Sets** tab.
2. Select the backup you want to rename.
3. On the **Sets** menu, point to **Backup Sets**, and then click **Properties**.
4. Click the **Set Info** tab.
5. In the **Set name** box, type the new name of the backup.
6. Click **OK**.

6.4 Activating or suspending a backup

A backup is active by default. When a backup is active, DS-Client performs the scheduled tasks assigned to the backup and the backup name is displayed in black.

When a backup is suspended, DS-Client no longer performs the scheduled tasks assigned to the backup and the backup name is displayed in gray.

To suspend a backup:

1. Click the **Backup Sets** tab.
2. Select the backup you want to suspend.
3. On the **Sets** menu, point to **Backup Sets**, and then click **Suspend**.

To activate a backup:

1. Click the **Backup Sets** tab,.
2. Select the suspended backup you want to activate.
3. On the **Sets** menu, point to **Backup Sets**, and then click **Activate**.

6.5 Synchronizing a backup

The first time you perform a backup, DS-Client retrieves the selected files from the backup source and sends the files to the DS-System. Information realted to those files is saved in both the DS-Client database and the DS-System online storage.

Each backup has a backup log table in the DS-Client database. For various reasons, the backup log can get out of synchronization with the DS-System online storage. If this occurs, a Normal synchronization process is automatically run during the next Weekly Admin process or scheduled backup.

By default, Weekly Admin performs a synchronization only on backups marked Out of Sync. To have it perform synchronization on all backups, you must configure the **AdminSkipSync** advanced configuration parameter. For more information, see Section 2.1.8, “Configuring the advanced settings”, on page 37.

NOTE: If you perform DS-System based synchronization, you cannot use the “deleted from source…” option to recover orphaned backups because the information related to files that have been deleted from the source is no longer available on the DS-System. To retrieve this information, you must recover the dsclient and dsdelta databases by running a daily or weekly admin on the production DS-Client, and then recover the dsclient and dsdelta databases to another DS-Client. Only then will the restore wizard show exactly the same information in both DS-Clients when performing a restore.

To synchronize a backup:

1. Click the **Backup Sets** tab.
2. Select the backup you want to synchronize.
3. On the **Sets** menu, click **Backup Sets**, and then **Synchronize**.
4. Under **Synchronization method**, select one of the following options:
   - **Normal –** Compares the DS-Client database backup log with the DS-System's online storage and updates where required.
   - **Check only** – Performs a check of the synchronization between the DS-Client database backup log and the DS-System online storage and identifies if inconsistencies exist. No corrective action is taken.
   - **DS-System based** – Synchronizes the DS-Client database backup log with the DS-System online storage.
5. Click **Synchronize**.

6.6 Migrating a backup

Migration allows you to continue using a backup and its accumulated backup data if the physical location of the backup source files or the source computer's name, IP address, or operating system is changed. Migration is also part of the process of recovering an orphaned backup. For more information, see Section 6.10, "Recovering an orphaned backup", on page 549.

When migrating a backup, consider the following:

- You cannot migrate a backup containing special backup items such as Windows System State and Services Database to a different operating system. To migrate a backup containing these items, you must delete all generations of the special backup items and remove them from the backup.
- When migrating items from one file system to another, verify that the backup item options are compatible on the new file system.
- If you perform a bare metal restore from a migrated backup, ensure that you only restore operating system files from the same backup session. Otherwise, you might restore a combination of incompatible files from different versions of the operating system.
- If you move data to another server and keep the same path format for the data, the DS-Client continues to back up data incrementally for the migrated backup. For example, if you move data from `e$\data` to `e$\data` on the new server, the DS-Client processes incremental backups for those files.
- If you move data to another server but do not keep the same path format for the data, the DS-Client performs an initial backup. For example, if you move data from `e$\data` to `e$\newlocation\data` on the new server, the DS-Client sends new masters of files after migration.

NOTE: DS-Client supports the migration of standalone Microsoft Exchange Server backups to DAG backups. It does not support the migration from DAG to standalone.

To migrate a backup:

1. Click the **Backup Sets** tab.
2. Select the backup you want to migrate.
3. On the **Sets** menu, point to **Backup Sets**, and then click **Migrate**.
4. Select the backup source location to which you want to migrate the backup, and then click **Next**.

5. For each existing location in the Source column, specify the share to which the data should be migrated in the Destination column, and then click **Next**.

NOTE: If the physical location of the source data has changed, the share that you select in the destination column is the new location of the source item. The DS-Client restricts the migration to a one-to-one match so you cannot select the same destination share for two different source shares.

---

6. Ensure that the new path that has been assigned to each backup item is correct, add more items if required, and then click **Next**.
7. Select the required options, and then click **Finish**.

NOTE: The backup item options that are available depend on the network to which you are migrating the backup and can differ from the options that were previously available when creating the backup.

IMPORTANT: We recommend that you synchronize the backup after performing a migration. For more information, see Section 6.5, “Synchronizing a backup”, on page 544.

6.7 Cloning a backup

You can clone an existing backup with all its backup items and options, except the retention rule, schedule, and name of the backup. This feature is only available in the FullFeatured DS-Client (Windows, Linux, or Mac).

To clone a backup:

1. Click the **Backup Sets** tab.
2. Select the backup you want to clone.
3. On the **Sets** menu, point to **Backup Sets**, and then click **Clone**.
4. Configure a retention rule if required, and then click **Next**.
5. Configure a schedule if required, and then click **Next**.
6. Configure the options for the backup, and then click **Finish**.

6.8 Converting a backup

When you convert a Local-only backup to an Online backup:

- All backed up data in the Local-only path is copied to the DS-System.
- The backup type is changed from Local-only to Online.
- The backup continues to save a copy of the data locally in the local storage path.
- The number of generations that remain in local storage depends on the retention settings of the backup. For more information, see Section 11.4, “Local Storage Tool”, on page 629.

NOTE: The conversion process from Local-only to Online is irreversible once the data has been completely copied to the DS-System online storage.

To convert a backup:

1. Click the **Backup Sets** tab.
2. Select the Local-only backup you want to convert.
3. On the **Sets** menu, point to **Backup Sets**, and then click **Convert**.
4. When prompted to confirm that you want to convert the backup, click **Yes**. The backup cannot back up new data until the conversion process is either completed or canceled.

6.9 Validating a backup

The validation process verifies the restorability of online data. To avoid transmitting large amounts of data, DS-Client sends the encryption keys to DS-System where it performs the data validation. Although the keys are sent in encrypted format to the DS-System and immediately discarded once the validation is complete, you must accept, acknowledge, and agree to send the encryption keys.

NOTE: You must be a DS-Client administrator to schedule or perform validation.

For each file generation, DS-System:

1. Checks the file header, delta linking, and library linking.
2. Tries to validate the data by performing a virtual restore. The data is decrypted and decompressed to generate the original file signature. If the process fails due to a decryption or decompression problem, the validation fails.

3. Compares the validation signature with the original one. If they do not match, the validation fails.

For validation failures:

- If a file originally did not have a signature that is needed for validation, a warning appears.
- If the validation fails due to networking issues, validation skips the file and reports the errors in both the DS-System and DS-Client event logs.
- If a file corruption is detected (including if the digital signatures do not match), the file and all files that depend on it are moved to the DS-System trash. The DS-System marks the corresponding backup as out of sync and a corresponding error appears in both the DS-System and DS-Client event logs.

The validation process is disk I/O intensive on the DS-System side because the digital signature of each file must be checked. The process is similar to a restore, except the data is deleted after comparing the signatures. It is recommended that you schedule the validation process at less resource-intensive times.

The scheduled validation has the option to resume from the point of interruption of the previous scheduled validation process. To determine the interruption point, the files are processed in sequence based on the share ID, directory ID, file ID and generation. On demand validations do not have the resume mechanism.

NOTE: Validation is not available for statistical backups, since there is no data on the DS-System to validate.

To validate a backup:

1. Click the **Backup Sets** tab.
2. Select the backup you want to validate.
3. On the **Restore** menu, click **Validation**.
4. Do the following:
   a) In the **Private Key** box, type the private key for the DS-Client.
   b) In the **Account Key** box, type the account key for the DS-Client.
   c) Under **Selections**, select the type of validation you want to perform. The options are as follows:
      - **All online data –** Validates all generations of files in the backup.
      - **Selective –** Allows you to specify the files to validate.
   d) Click **Next**:.
5. Select the directories you want to validate, and then click **Finish**.

6.10 Recovering an orphaned backup

A backup becomes orphaned when the backup settings are lost from the DS-Client database and the backup data still exists in the DS-System. This can occur when the DS-Client database is deleted, corrupted, or overwritten with an older version. Orphaned backups are detected during Daily Admin or Weekly Admin activities. You must recover an orphaned backup before you can perform backup and restore activities on the backup.

When you run a backup for the first time for a backup, DS-Client retrieves all the selected files and folders from the backup source and sends them to DS-System. All the information related to those files and folders (files headers and directories descriptors) is saved both in the DS-Client database and in the DS-System online storage.

When you run subsequent backups, DS-Client checks if the files previously backed up are available on the source. If they are not available, the corresponding entries will be updated with a special flag in the DS-Client database. This information (related to deleted files and folders) is not sent to DS-System. When you install a second DS-Client for DR purposes using the same CRI info as the original DS-Client, these files will not be deleted from source information when you recover the orphaned backups. You must recover the dsclient and dsdelta database (run a daily or weekly admin on the production DS-Client), and then restore the dsclient and dsdelta databases to the DR DS-Client. The restore wizard displays the same info in both DS-Clients when you restore an orphaned backup.

To recover an orphaned backup:

1. On the **Setup** menu, click **System Activities**.
2. Beside **Repair DS-Client Database**, click **Repair**.
3. In the **Repair DS-Client** dialog box, select **Orphaned backup sets**, and then click **OK**.
4. In the **Backup Set Recovery** dialog box, select the backup that you want to recover.

NOTE: Orphaned Microsoft 365 backups are displayed under a blank server name in the selection tree in the and in the **Backup Sets** tree. The name of the backup will be recovered after migration.

---

5. If you are prompted to provide information on the orphaned backup, click **Set Info**. In the **Recovery Info** dialog box, do the following:
   a) In the **Owner** box, select the owner of the backup. By default, the user account that you have used to log on to the DS-Client is the owner of the recovered backup.
   b) In the **Network provider** box, select the network provider for the backup.
   c) Click **Save**.

6. In the **Backup Set Recovery** dialog box, click **Recover**. The backup is recreated in the DS-Client database and synchronized.

NOTE: You can now perform restore activities on the recovered backup to an alternate location.

---

7. If you want to perform restore activities on the recovered backup to the original location, you must manually reconfigure the backup properties as follows:

   a) On the **Backup Sets** tab, select the recovered backup. On the **Sets** menu, point to **Backup Sets**, and then click **Properties**.

   b) In the **Set Properties** dialog box, on the **Share** tab (Windows) or **Connection Options** tab (Linux), specify the credentials to access the backup source, and then click **Apply**.

8. If you want to perform backup activities on the recovered backup, you must do one of the following:

   - Migrate the backup (see Section 6.6, “Migrating a backup”, on page 545) and then activate the backup (see Section 6.4, “Activating or suspending a backup”, on page 543).
   - Manually reconfigure the backup properties as follows:

     a) On the **Backup Sets** tab, select the recovered backup. On the **Sets** menu, point to **Backup Sets**, and then click **Properties**.

     b) In the **Set Properties** dialog box, on the **Share** tab (Windows) or **Connection Options** tab (Linux), specify the credentials to access the backup source, and then click **Apply**.

     c) On the **Items** tab, click **Edit**, specify the items to back up, and then click **Apply**.

     d) To assign a schedule to the backup, on the **Schedule** tab, select **Scheduled**, select the schedule in the **Available schedules** list, and then click **Apply**.

     e) To assign a retention rule to the backup, on the **Retention** tab, select **Use a specific retention rule**, select the retention rule in the list, and then click **Apply**.

     f) Click **OK**.

     g) Activate the backup (see Section 6.4, “Activating or suspending a backup”, on page 543).

6.11 Changing the ownership of a backup

The owner of a backup is the user who creates the backup. Administrators can change the ownership of a backup.

To change the ownership of a backup:

1. Click the **Backup Sets** tab.
2. Select the backup whose ownership you want to change.
3. On the **Sets** menu, point to **Backup Sets**, and then click **Change Owner**.
4. Beside the **To** box, click **[>>]**. Select the new owner for the backup, and then click **Select**.
5. To change the DS-Client database so that the new owner of the backup is reflected in the Activity Log, select the **Change Activity Log** check box.
6. To change the ownership of only this backup to the new owner, select the **This backup** option.
7. To change the ownership of all backups associated with the current owner to the new owner, select the **All backup sets** option.
8. Click **OK**.

6.12 Changing the permissions of a backup

By default, only the administrator and the owner of the backup have permissions to view, change, back up, restore, and delete a backup or the items in it. Backup operators can change a schedule or perform on-demand backups. You can add or modify a user's permissions to a backup.

1. Browse the Backup Sets tree and select the required backup.
2. On the **Sets** menu, point to **Backup Sets**, and then click **Permissions**.The **Permissions** dialog box displays a list of users with permissions to the backup apart from the owner or administrator.
3. To add permissions for a user or group, click **Add**.
4. In the **Add Permission for Users and Groups** dialog box, users and groups only appear if they currently exist in the DS-Client database; they are added to the DS-Client database when they have logged on to DS-Client at least once.
5. Select the user or group you will define permissions for.
6. In the **Permission Type** section, select or clear the required permission, and then click **Add**. The Permissions dialog box is automatically updated.

6.13 Configuring the properties of a backup

You can modify some properties of a backup after it has been created. Backup options define the way a backup is handled during the backup process. Some options are specific to the type of server that is being backed up.

1. Click the Backup Sets tab.
2. Select the backup. whose properties you want to configure.
3. On the **Sets** menu, point to **Backup Sets**, and then click **Properties**.
4. Use the following tabs to configure the backup properties.

Properties tab	Function
Items	Displays the backup items and item options.
Retention	Displays the backup retention rules.
Options	Displays the backup options.
Notification	Displays the backup notification options.
Schedule	Displays the backup schedule.
Set Info	Displays information about the backup including the backup name. If the multitenant feature is enabled, you can select a customer to which to assign the backup.
Share	Displays information about the backup share.
Connection	Displays the credentials used for connection to the backup source or dump for certain kinds of backups.
Database	Displays the credentials used for database backups.
Advanced Options	Displays the backup advanced options (Windows DS-Client).

5. Click **OK**.

6.13.1 Modifying share access properties

In some situations you might have to change the user name and password associated with a backup (for example, when you are creating a backup for a user with limited LAN access rights). These credentials are used to connect to items of a backup that are on the LAN.

1. Browse the Backup Sets tree and select the required backup.
2. On the **Sets** menu, point to **Backup Sets**, and then click **Properties**.
3. In the **Backup Set Properties** dialog box, click **Share**.
4. Beside the **Connect as** box, click the **[>>]** button.
5. In the **Modify Network Credentials** dialog box, do the following:
   a) Type a new user name and/or a new password to be associated with this backup.
   b) In the **From** list, select the machine where DS-Client will verify user information.
   c) Click **OK** to save your changes.

NOTE: For Windows DS-Clients, if the share is on the local DS-Client computer and you are logged on to DS-User as an administrator, you can use the DS-Client Account (the user name and password used by the DS-Client service).

---

6. In the **Backup Set Properties** dialog box, click **OK** to save the changes.

6.13.2 Modifying connection information (Exchange Server)

1. Browse the Backup Sets tree and select the required backup.
2. On the **Sets** menu, point to **Backup Sets**, and then click **Properties**.
3. In the **Backup Set Properties** dialog box, click **Connection**.
4. Configure the required information, and then click **OK**.

6.13.3 Modifying connection information (Email)

1. Browse the Backup Sets tree and select the required backup.
2. On the **Sets** menu, point to **Backup Sets**, and then click **Properties**.
3. In the **Backup Set Properties** dialog box, click **Connection**.
4. Click **>>** and modify the credentials used by the backup.
5. Click **OK** to save the changes.

6.13.4 Modifying connection options (Linux DS-Client)

1. Browse the Backup Sets tree and select the required backup.
2. On the **Sets** menu, point to **Backup Sets**, and then click **Properties**.
3. In the **Backup Set Properties** dialog box, click **Connection Options**.
4. Click the **Connection Options** tab. The number of available options depends on the kind of backup and whether the data source is local or remote. For details on these options, see the online help for the dialog box.
5. Configure the required information, and then click **OK**.

6.13.5 Modifying a backup name

1. Browse the Backup Sets tree and select the required backup.
2. On the **Sets** menu, point to **Backup Sets**, and then click **Properties**.
3. In the **Backup Set Properties** dialog box, click **Set Info**.
4. In the **Set Name** box, type a new name.
5. Click **OK** or **Apply**.

6.14 Deleting backups and backup data

IMPORTANT: The system does not automatically delete backups or backup data. This process must be performed by an authorized user. Apply caution when performing this process because data cannot be recovered after being deleted.

You can delete backups and remove backed up files or file generations that are stored in the DS-System online storage.

Delete type	Description
Selective Delete	Allows you to delete data that you specify from a single backup.
Assisted Delete	Allows you to delete data that has been removed from source for multiple backups.
Remove Backup	Delete all files of a single backup or remove a single backup from DS-Client.

NOTE: If two-factor authentication is enabled on the DS-Client, you can delete backups and backed up files or file generations only if you are an authorized user listed in the two-factor authentication settings for the DS-Client. For more information, see Section 2.5, “Configuring the two-factor authentication settings”, on page 66.

The basic delete methods simply remove a generation from online storage. However, when the delete is combined with some other features, there are some additional considerations:

- **Remove a backup set** – This deletes all online data of a backup and also removes the backup itself.
- **Selective delete** – This is the simplest delete method. You browse backups with the Delete Wizard and pick the specific files to delete.
- **Assisted delete** – This is a faster method to remove obsolete data from multiple backups. It only selects backup data that was removed from the backup source and was detected by DS-Client.
- **Generation recycling (passive delete)** – All backup items must have a maximum number of online generations. For backup data that does not change often, you can have only 1 generation online even after several backups. However, data that changes often will have multiple generations. Once a file reaches its maximum number of generations, the oldest generation gets overwritten by the next backup. To prevent loss of these old generations, configure the backup with the **BLM (Infinite Generations)** option, which moves the old generation to BLM Archiver.
- **Delete because of retention** – Any data that is not retained when a retention rule is enforced will be deleted.

The following options can affect deletes or delete behavior:

- Move to BLM (Archiving) — If BLM Archiving is available, every delete situation will have the **Move to BLM** option.
  - If the backup is configured with the **BLM (Infinite Generations)** option, the Move to BLM is always selected. If DS-System cannot move the deleted data to BLM, the delete will fail.
- DS-System delete lock (from service provider) — If your service provider has applied a **Delete Lock** to your customer account or to this specific DS-Client, the following will occur:
  - You will see a warning message in the Activity Log when a delete activity is performed.
  - If possible, DS-System moves the deleted data to BLM.
  - The delete will fail if DS-System cannot move the deleted data to BLM. If the delete was a passive delete (e.g. generation recycling), the maximum generation configuration will be overruled and the surplus generations will accumulate online.
- BLM delete lock (from service provider) — If your service provider has applied a **Delete Lock** to your customer account or to this specific DS-Client on the BLM Archiver, the following will occur:
  - You will not be able to **Confirm Destruction** of any destruction requests.
  - You will see an error in the BLM Activity Log when a data destruction confirmation activity is performed.

NOTE: BLM is only accessible to end-users via a DS-NOC web site.

- Deleting a VMware vCenter Server backup with Local DS-VDR enabled — Before deleting a VMware vCenter Server backup with the Local DS-VDR option enabled, ensure that the DS-Client is connected to its Local DS-VDR Tool. For more information, see Section 2.6, “Configuring the Local DS-VDR Tool”, on page 68.

6.14.1 Performing a selective delete

You can delete specific files from a backup and the DS-System online storage. The backup will continue to exist and scheduled backups will continue to run.

To perform a selective delete:

1. Browse the Backup Sets tree and select the required backup.
2. On the **Sets** menu, point to **Delete**, and then click **Selective Delete**.

   Options in this first page allow you to narrow down the display of files and directories from which to select for deletion.
3. Select the method by which data is to be selected for deletion. The default is **Time-based data selection**. You can use the option **Placeholder/stub selection** if the data source is managed by a recognized HSM system.
4. Select the period from which backup data is to be deleted.
5. If required, customize the delete using these options **Leave last generations online** and **Only data removed since (days ago)**, and then click **Next**.
6. Select the options that you require:
   - **Archived data placeholders –** These options relate to displaying generations that have already been 'pushed' to BLM from online storage. Select what you want to display in the next dialog box of the Delete Wizard (include archived files, exclude archived files, or show only archived files).
   - **Move to BLM –** Select if you want to send a copy of all files selected for deletion to BLM.
7. Click **Next**. The contents of the tree are determined by the options specified in previous pages.
8. Browse the **Directories Tree** and select the directories you want to delete.
9. Click **Finish** to start the delete process.
10. (If two-factor authentication is enabled) In the **Two-factor Authentication Validation** dialog box, in the **Authentication Code** box, type the authentication code that you have received from the DS-System, and then click **Validate**.

NOTE: The authentication code is sent to the email address that is associated with your user account in the two-factor authentication settings for the DS-Client. The code is valid for two hours. To request an authentication code be resent to you, click **Resend**.

To delete individual files:

1. Follow the same steps as Section 6.14.1, “To perform a selective delete:”, on page 557 until you reach the **Select directories/files to delete** page.
2. Browse the **Directories Tree** to the directory that contains files you want to delete.
3. Click **Show Files**.
4. Browse the **Files List** and select the files you want to delete.
   - To view a list of the files you have selected for deletion and the full path to each file, click **Selection** to open the **Delete Selection** dialog box.
5. Click **Finish** to start the delete process.
6. (If two-factor authentication is enabled) In the **Two-factor Authentication Validation** dialog box, in the **Authentication Code** box, type the authentication code that you have received from the DS-System, and then click **Validate**.

NOTE: The authentication code is sent to the email address that is associated with your user account in the two-factor authentication settings for the DS-Client. The code is valid for two hours. To request an authentication code be resent to you, click **Resend**.

6.14.2 Performing an assisted delete

You can delete obsolete data that has been removed from the backup source. The backup will continue to exist and scheduled backups will continue to run.

NOTE: During each backup session, DS-Client identifies files that have been removed from the source. Files that have been removed from the source after the most recent backup session are not yet identified and will not be deleted.

The granularity of the assisted delete operation depends on the type of DS-Client:

- **Windows DS-Client** – Performs deletion at the directory level for File system and DS-MLR backups. You can delete directories that have been removed from the source but cannot delete individual files removed from the source. Based on your search criteria, directories that have been removed from the backup source are automatically displayed.
- **Linux or Mac DS-Client** – Performs deletion at the file level for File system (Local, NAS, NFS, UNIX-SSH) backups. You can delete directories that have been removed from the source and directories containing file(s) that have been

removed from the source. Based on your search criteria, files that have been removed from the backup source or directories containing files that have been removed from the backup source are automatically displayed.

NOTE: When you select directories containing files that are removed from the source in Linux or Mac DS-Clients, only obsolete files will be deleted from those directories.

To perform an assisted delete:

1. On the **Sets** menu, point to **Delete**, and then click **Assisted Delete**.
2. If you are using a Windows DS-Client, select the method by which data will be selected for deletion.
   - If you select **Time based data selection**, continue to step 3.
   - If you select **Placeholder/stub selection**, select one of the two criteria, and continue to step 4. You can use this option if the data source is managed by a recognized HSM system.

   NOTE: For Linux or Mac DS-Clients, only time-based data selection is available. Continue in step 3.

   ---

3. Do the following:
   a) In the **From** box, specify a start date and time. No data before this date and time will be deleted.
   b) In the **To** box, specify an end date and time. No data after this date and time will be deleted.
   c) In the **Leave last** box, enter the number of generations you want to retain online. If you specify a number, you will only be able to select directories that have more generations available for delete than this number.
   d) Under **Filter**, specify the date and time from which you want to display deleted items that have been removed from the source computer. This allows you to remove backed up directories or files that were intentionally deleted from your source.

   NOTE: Windows DS-Clients compare directories in its logs with the directories backed up on the DS-System. Linux or Mac DS-Clients compares files in its logs with the files backed up on the DS-System.

   ---

   e) If required, select one of the following options:

- **Move to BLM** – Copies the backed up data in the DS-System online storage to the BLM Archiver prior to deleting the data. If this option is unavailable but the check box is selected, it means the data must be moved to the BLM Archiver. This occurs if the backup has the BLM (Infinite Generations) option selected.
- **Use new archive package** – If you selected Move to BLM, you can select this option to create a new archive package on the BLM Archiver. Otherwise, the archive request is added to the current archive package on the BLM Archiver. Archive packages are specific to a particular backup.
- **Session Label** – If you selected Move to BLM, you can type a label for the archive package. Each archive package is automatically time-stamped, but a label can make it easier to find.

NOTE: These options are only available if BLM has been enabled as a DS-Tool for DS-Client. For DS-Client to complete the above BLM requests, BLM must also be registered with the DS-System.

f) Click **Next**.

4. Select the directories or files you want to delete, and then click **Finish**.

Assisted Delete - Select how you want to delete

1. Clear selections in this dialog box if required. Directories that do not match the delete period or filter selections are unavailable for selection.
2. Click **Finish** to start the delete process.
3. (If two-factor authentication is enabled) In the **Two-factor Authentication Validation** dialog box, in the **Authentication Code** box, type the authentication code that you have received from the DS-System, and then click **Validate**.

NOTE: The authentication code is sent to the email address that is associated with your user account in the two-factor authentication settings for the DS-Client. The code is valid for two hours. To request a new authentication code, click **Resend**.

Assisted Delete - Select Backup Set / Directory

This dialog box appears with the automatic selection(s) for delete from online, based on the selections made in the Assisted Delete - Select how you want to delete dialog box.

Backup Set List	• Windows DS-Clients: Selected directories will be deleted. • Linux/Mac DS-Clients: Files in the selected directories will be deleted. If the entire directory was deleted, the directory will also be removed from online. Clear a check box to keep the corresponding directory. All other backups\directories (that cannot be selected) do not fit the Assisted Delete selection parameters.
Finish	Click to have DS-Client connect to DS-System and delete the selected items from online storage.

Placeholder/stub selection [Windows DS-Clients only] You can use this option if you are using a third-party storage management solution that migrates infrequently used files from the source, and leaves a small (size) placeholder/stub in its place. This assumes that the third-party storage management solution is where you want to protect that data (and the DS-System storage is not necessary). If DS-Client detects a placeholder / stub is created on the source (by the Windows “offline” attribute), the corresponding file on DS-System is deleted, based on the selected conditions (see below).
Keep the last placeholder / stub and subsequent generations • The last placeholder or stub will be kept on DS-System, as well as any full file generations that appear after that latest placeholder/stub.
Keep all placeholders / stubs • All placeholders or stubs will be kept on DS-System, as well as any full file generations that appear after that latest placeholder/stub.

Move to BLM • A copy of all data deleted from DS-System during this Assisted Delete will be moved to BLM (Backup Lifecycle Management). This option only appears if the BLM Module is enabled by your service provider. • **Use new archive package:** Select to use a new archive package. Otherwise, this Archive request will be added to the current archive package on the BLM Archiver. Archive packages are specific to a particular backup. Each BLM Request will be added to an Archive Package until it reaches a specified limit (# of files, size, time). • **Session Label:** Each Archive Package is automatically time-stamped, but you must add your own label (alphanumeric string) to demand BLM requests. This will make it easier to search an Archive Package.

6.14.3 Deleting a backup

You can delete a backup and all its associated data from the DS-System online storage and the instant recovery vault (if applicable).

NOTE: You can also delete a backup that is marked incomplete in its initial backup status. For more information, see Section 11.1.3, “Monitoring the status of an initial backup”, on page 620.

To delete a backup:

1. Click the **Backup Sets** tab.
2. Select the backup you want to delete.
3. On the **Sets** menu, point to **Delete**, and then **Remove Backup Set**.
4. When prompted to delete the backup, do the following:

   a) If required, select one of the following options:

   - **Move to BLM** – Copies the backed up data in the DS-System online storage to the BLM Archiver prior to deleting the data. If this option is unavailable but the check box is selected, it means the data must be moved to the BLM Archiver. This occurs if the backup has the BLM (Infinite Generations) option selected.
   - **Use new archive package** – If you selected Move to BLM, you can select this option to create a new archive package on the BLM Archiver. Otherwise, the archive request is added to the current archive package on the BLM Archiver. Archive packages are specific to a particular backup.
   - **Session Label** – If you selected Move to BLM, you can type a label for the archive package. Each archive package is automatically time-stamped, but a label can make it easier to find.

   NOTE: These options are only available if BLM has been enabled as a DS-Tool for DS-Client. For DS-Client to complete the above BLM requests, BLM must also be registered with the DS-System.

   b) Click **OK**. When prompted to confirm that you want to delete the backup, press **Y.** To cancel, press any other key.

5. If two-factor authentication is enabled, in the **Authentication Code** box, type the authentication code that you receive from the DS-System, and then click **Validate**.

NOTE: The authentication code is sent to the email address associated with your user account. The code is valid for two hours. To request an authentication code be resent to you, click **Resend**.

6.14.4 Deleting local-only backup data

Local-only backup data is stored in a default local storage path that is defined for the DS-Client or a specific path defined for a backup. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.

You can delete Local-only backups using one of the following methods:

- On demand from the Delete Wizard
- By a retention rule (Enforce Retention), either scheduled or on demand. Local-only backups use the Online Storage retention options (and not the Local Storage retention options, which apply only to Online backups configured with the “Save on local storage” option.). This is because the Local-only backups behave exactly like Online backups with the exception of the data storage location.

NOTE: If enabled, two-factor authentication is required.

- By automatic generation recycling, when a backup file reaches its maximum number of generations.

NOTE: Two-factor authentication does not apply if you modify the maximum number of generations.

6.15 Cleaning local-only trash

When Local-only backup files are deleted by the DS-Client, the deleted data is moved to a trash folder in the local storage path. This is a safe delete feature that helps prevent the accidental or inadvertent deletion of data. You should periodically clean the Local-only trash folder(s) as deleted data accumulates.

To clean the local-only trash:

1. On the **Tools** menu, click **Clean Local-only Trash**.
2. In the **Clean data deleted at least** box, enter the number of days the data must be deleted before it can qualify to be removed from the local-only trash.
3. In the **Local Storage Path** box, select the local storage path defined on the DS-Client that contains the deleted data you want to remove. Otherwise, all local storage paths on DS-Client will be cleaned by default.
4. Click **OK**.

NOTE: You can also schedule this process. For more information, see Section 3.1, “Configuring a schedule”, on page 90.

6.15.1 Modifying database information (SQL Server - Classic)

To modify the database information:

1. Browse the Backup Sets tree, right-click the backup you require, and select **Properties**.
2. In the **Backup Set Properties** dialog box, click the **Database** tab.

   If **Access integrated with share** is selected, you can edit only the credentials from the **Dump location** section. Windows authentication will be performed when the DS-Client connects to the database.

   NOTE: Even though you can select this option, it does not work if your network is using Windows Integrated Security.

   ---

3. Click **OK** to save the changes.

7 Working with VM replication sets (Windows)

VM replication allows you to replicate virtual machines from one VMware vCenter Server to another and initiate failover and failback.

NOTE: VM replication is not supported in a Grid DS-Client configuration.

A VM replication set does not back up data to the DS-System online storage. Data is transferred between the source DS-Client on which you create the VM replication set and the destination DS-Client. The first time replication is performed, the entire virtual machine is replicated. Subsequent replication activities are incremental.

To optimize your networking configuration and avoid conflicts between multiple DS-Clients that share the same IP address, you can specify the ports used by the source DS-Client and destination DS-Client. The DS-Client has two methods of replicating virtual machines:

- **Online replication** – The source DS-Client sends replication data directly from the source virtual machine to the destination DS-Client. The snapshot is replicated to the target virtual machine on the destination server and is then ready to be used for failover.

  NOTE: To configure a VM replication set to perform online replication, you must clear the Initial replication option.

- **Offline replication** – The source DS-Client saves the replication data of the source virtual machine in a folder on a local disk location as an Initial VMR Set. You then copy that folder to a local disk on the destination DS-Client machine and specify the location to import the data. The destination DS-Client places the replicated snapshot into the replication target virtual machine on the destination server. The snapshot is then ready to be used for failover.

  NOTE: To configure a VM replication set to perform offline replication, you must select the Initial replication option.

7.1 Licensing considerations

Your service provider must allocate sufficient VM replication licenses based on either native capacity or the number of virtual machines. To view the VM replication storage quota, on the **Setup** menu, click **View Quotas**.

A VM Replication license based on capacity takes into account the native size of the disks as defined in the virtual machine configuration.

7.2 Credential considerations

When entering the credentials for the source and destination VMware vCenter Server, we recommend the following:

- For a domain user, type both the domain and user name in the following format: domain\username. For example: `dchv\user126`
- For a local user, type only the user name without the domain. For example: `user126`
- Ensure DS-Client users have administrative privileges or access to the C:\ProgramData\boost_interprocess\dsclient_replication folder to perform the following tasks for VM replication:
  - Create or modify a VM replication set
  - Start the VM replication process
  - Import the initial VMR set (initial VM replication data) for offline VM replication
  - Perform failover or failback

NOTE: You must set these permissions after starting the DS-Client and the VM Replication service for the first time.

7.3 Configuration considerations

- Ensure the source DS-Client can connect to the destination DS-Client.
- Ensure the version of the virtual machines to be replicated is supported on both the source and destination servers.
- Ensure the virtual machine name does not contain the following characters: %, &, *, $, #, @, !, \, /, :, *, ?, “, <, >, |, ;, ‘
- Ensure VMware Tools is installed on the guest operating system of the virtual machine for application consistent snapshots.
- Ensure at least two DS-Clients belong to a VM replication group. The source DS-Client performs replication for the source virtual machine and the destination DS-Client performs replication for the target virtual machine. The DS-Client on which you create a VM replication set is the source DS-Client of the VM replication set. Your service provider must ensure that multiple DS-Clients sharing the same IP address use different ports to avoid conflicts.

- Ensure the VMRServiceStart advanced configuration parameter value is set to Yes. For more information, see Section 2.1.8, “Configuring the advanced settings”, on page 37.

NOTE: If the VMRServiceStart parameter is disabled, existing VM replication sets will be inaccessible. If the parameter is enabled, you will be able to create VM replication sets and run replication as long as the DS-Client has sufficient VM replication capacity for its VMR license.

- Ensure the value of the VMRSourcePort advanced configuration parameter is set to the port the DS-Client will use for VM replication processes and the port is open in the firewall for the DS-Client machine. This value is set to 8090 by default and is equivalent to the source DS-Client port number. For more information, see Section 2.1.8, “Configuring the advanced settings”, on page 37.
- If you have changed the VM replication port settings on multiple DS-Clients, stop and restart each affected DS-Client Service one at a time. Wait until the DS-Client Service on one machine has successfully restarted before you stop and restart the DS-Client Service on another machine.
- DS-Client replicates all hard disks on the source virtual machine. However, network devices. such as network adapters) and other peripheral components that are used by the source virtual machine are not replicated.

7.4 Creating a VMware vCenter Server replication set

This section describes how to create a VMware vCenter Server replication set.

7.4.1 Selecting the kind of VM replication set

1. On the **Sets** menu, click **New Backup Set**.
2. Under **DS-Client replication sets**, select **VM Replication**.
3. Click **Next**.

7.4.2 Selecting the VM replication type

VMware vSphere snapshot replication is selected by default. Click **Next**.

7.4.3 Specifying the source server

1. Select **VM Replication** and select the **Ask for Network Credentials** check box.
2. In the **Path** box, type the IP address of the source VMware vCenter Server, and then click **Next**.
3. When prompted, type the credentials to connect to the source VMware vCenter Server, and then click **OK**.

7.4.4 Selecting the items to replicate

1. Under **Shares & Directories List**, select the virtual machine(s) you want to replicate and then click **Add**. Sub-directories are included by default.
2. To remove an item from the list, under **Replicated Items selected**, select the item, and then click **Remove**.
3. Click **Next**.

7.4.5 Specifying replication item options

1. To configure maximum number of generations you want to be available for both failover and failback, double click the **Max Gen** cell, and then enter the value.
2. Click **Next**.

7.4.6 Specifying the destination for the replication set

NOTE: Before you being, ensure sufficient **VM Replication Capacity** is available. For more information, see Section 7.1, “Licensing considerations”, on page 565.

---

1. In the **Destination DS-Client** box, select the DS-Client you want to use as the destination computer for the replication set.
2. In the **Destination Port** box, select the port used by the destination DS-Client you selected.
3. In the **Hypervisor IP** box, enter the IP address of the destination server.
4. In the **User name** and **Password** boxes, type the credentials for the DS-Client to connect to the destination server. The user must have the required permissions to write data to the destination server.
5. In the **Destination Datacenter** box, select the datacenter on the destination VMware vCenter Server. The replication target virtual machine is located in the selected DataCenter.

6. Click **Next**.

7.4.7 Specifying destination for VM replication

1. In the **Host** box, select a host for the replication target virtual machine.
2. In the **Datastore** box, select a datastore where the files of the replication target virtual machine and other required files will be stored. If a you do not specify a datastore, the first available datastore is used as the default.
3. In the **Folder** box, select a folder under which the target virtual machines will be organized. If you do not select a folder, the root level of the VMware vCenter Server is used as the default folder.
4. To apply the global settings to all the virtual machines displayed in the table, click **Clear Overrides**.
5. To override the global settings for an individual virtual machine in the table and specify custom settings, do the following:
   a) Click in the **Host** cell and specify a host for the replication target virtual machine.
   b) Click in the **Datastore Setting** cell and specify a datastore for the replication target virtual machine.
   c) Click in the **Folder** cell and specify a folder under which the target virtual machines will be organized.
   d) Click the **Destination Machine/Folder** cell to rename the replication target virtual machine. By default, the replication target virtual machine is given the same name as the source virtual machine.
6. Click **Next**.

7.4.8 Specifying the replication set options

1. To perform online VM replication, clear the **Initial replication** check box.
2. To perform offline VM replication, select the **Initial replication** check box. When prompted, select a local disk location to which the DS-Client will save the replication data, and then click **Add**.

NOTE: If you selected the Initial replication check box, make a note of the local disk location that you specify. After the source DS-Client performs the offline VM replication process, you must copy the replication data from the specified location to a local disk on the destination DS-Client.

---

3. In the **Stop on errors** box, enter the maximum number of errors at which the replication process will be stopped. A value of 0 means the DS-client does not stop the replication process regardless of the number of errors.
4. Click **Next**.

7.4.9 Specifying notification options

IMPORTANT: The email and pager options are available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

1. To configure a notification, do one of the following:
   - To add a notification, click **Add**.
   - To modify a notification, select the notification, and then click **Modify**.

   NOTE: To delete a notification, select the notification, and then click **Delete**.

2. To send an email notification, select **E-Mail**, and then do the following:
   a) To send the email notification to the DS-Client administrator, select **Administrator**.
   b) To send an email to another recipient, select **Other**, and then specify the recipient’s email address.
   c) To send detailed backup information, select the **Detailed notification** check box.
   d) To include a detailed file-level backup log as an attachment, select the **Attach detailed log** check box.
   e) To compress the detailed log, select the **Compress** check box.
   f) To send detailed backup information, select the **Detailed notification** check box.
   g) To include a detailed file-level backup log as an attachment, select the **Attach detail log** check box.

h) To send the email notification in HTML format, select the **Send E-Mail using HTML format** check box.

NOTE: The email option is available only if the DS-Client has been configured for email notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

i) Click **OK**.

3. To send a pager notification, select **Pager**. The notification will be sent to the pager account configured for the DS-Client.

NOTE: The pager option is available only if the DS-Client has been configured for pager notifications. For more information, see Section 2.1.3, “Configuring the notification settings”, on page 27.

4. In the **Completion** box, specify under what conditions a notification will be sent, and click **OK**. The options are as follows:
   - **All** – Notification will be sent under all conditions.
   - **Successful** – Notification will be sent if an activity is completed successfully without errors or warnings.
   - **Completed with warnings** – Notification will be sent if an activity is completed with at least one warning event.
   - **Complete with errors** – Notification will be sent if an activity is completed with at least one error event.
   - **Incomplete** – Notification will be sent if an activity is not completed successfully.
5. Under **Send SNMP traps when**, configure the DS-Client to send SNMP traps when the backup has completed successfully, completed with warnings, completed with errors, or is incomplete.
6. Click **Next**.

7.4.10 Assigning a schedule

NOTE: When Enforce Retention or Perform BLM tasks are selected in a schedule with a VM replication set assigned to it, no action related to those tasks are performed for the VM replication set.

1. To assign a schedule to the replication set, do one of the following:
   - To create or edit a schedule, click **New** or **Edit**. For more information, see Section 3.1, “Configuring a schedule”, on page 90.
   - To assign a schedule to the backup, select **Scheduled.** In the **Available schedules** box, select an existing schedule.
   - If you don’t want to assign a schedule to the backup, select **Not scheduled**.
2. Click **Next**.

7.4.11 Naming the VM replication set

Type a name for the replication set and click **Next**

7.5 Performing on-demand replication

Before performing on-demand replication, ensure the source virtual machine on the source server does not contain any snapshots. For information on how to manage snapshots, see the *VMware* documentation.

1. In the **Backup Sets** tree, right-click the VM replication set with the virtual machine(s) you need to replicate, and then click **Replicate Now**.
2. In the **Select items for on-demand replication** dialog box, ensure the virtual machine(s) you want to replicate are selected, and then click **Next**.
3. In the **Select options for on-demand replication** dialog box, specify the value for **Stop on errors** if necessary. Otherwise, keep the default value, 0.
4. Click **Finish**. The replication process varies depending on whether the replication set is configured for offline (Initial replication) or online VM replication (default).

7.6 Performing offline replication

Offline replication is intended to reduce the transmission time between the source DS-Client and destination DS-Client, especially when performing replication of large virtual machines. Offline replication requires copying the initial replication data and importing the initial VMR set.

7.6.1 Copying the initial replication data

You must copy the VM replication data from a local disk on the source DS-Client to a local disk on the destination DS-Client.

1. Locate the initial VM replication data the source DS-Client has placed in a specified local disk specified in the **Initial Backup Settings** dialog box when you created the VM replication set.
2. Copy the folder containing the initial VM replication data and place the folder on a local disk on the destination DS-Client.
3. Specify the path for the destination DS-Client to import the initial VM replication data. For detailed instructions on how to import the initial VM replication data, see Section 7.6.2, “Importing the Initial VMR set”, on page 573.

   After importing the data, the destination DS-Client will replicate the source virtual machine to the target virtual machine on the destination server.

7.6.2 Importing the Initial VMR set

You must import the VM replication data from the destination DS-Client into the replication target virtual machine on the destination VMware vCenter Server. The snapshot is then ready to be used for failover

1. On the destination DS-Client, on the **VM Replication** menu, click **Import Initial VMR Set**.
2. In the **Select Path to Import** dialog box, do the following:
   a) Select the computer on which you have placed the folder containing the initial VM replication data.

   NOTE: You must copy the VM replication data to the local disk of the destination DS-Client computer.

   b) Select the directory path to the folder that contains the initial VM replication data, and then click **OK**.
3. In the **VMR Offline Configuration** dialog box, do the following:
   a) In the list of VM replication sets that are available for importing, select the VM replication set that you want to import.
   b) Click **Import** to start the process.

This destination DS-Client sends the data to the destination server. After that is finished, the source virtual machine is replicated on the destination server.

7.7 Performing a failover

You can perform a failover on a replicated virtual machine. After the virtual machine on the source server has been replicated to the destination server, the replicated virtual machine on the destination server is ready for failover.

Before performing a failover, you can select from multiple replicated generations. If a target virtual machine is being used after failover, it is available for failback.

1. On the **VM Replication** menu, click **All Replicated Machines**. Under **Items ready for failover**, each row displays a source virtual machine replicated to the destination server.
2. In the **Generations** column, verify that the replicated generation you want to use is available for each virtual machine on which you plan to perform a failover. By default, the most recent replicated generation is selected.

   NOTE: To select another generation from a list of successfully replicated generations of the virtual machine, click the Generations column in the corresponding row, and then click Browse.

3. To perform a failover on one virtual machine, click **Failover** in the corresponding row to start the failover process.

   NOTE: The selected generation of the virtual machine is powered on from the destination server. You can then start using the target virtual machine.

4. To perform a failover on multiple virtual machines concurrently, select the virtual machines, and then click **Trigger** to start the failover process.

   NOTE: DS-Client has no limit on concurrent failover activities. The selected generation of each selected virtual machine is powered on from the destination server. You can then start using the target virtual machines.

7.8 Performing a failback

You can perform a failback on a replicated virtual machine from the destination DS-Client.

IMPORTANT: Ensure the existing source virtual machine has been deleted and all notifications are resolved. To retain the existing source virtual machine, clone the virtual machine before deleting it. Do not delete a partially restored source virtual machine from a previous failback that has been stopped or has failed.

1. On the **VM Replication** menu, click **All Replicated Machines**.
2. Under **Items ready for failback**, do one of the following:
   - To perform a failback on one virtual machine, click **Failback** in the corresponding row.

- To perform a failback on multiple virtual machines concurrently, select the virtual machines, and then click **Trigger**. You can perform a maximum of three concurrent failbacks.

NOTE: If a replication set consists of folders containing multiple virtual machines with files located on different datastores, you must perform a failback of these virtual machines concurrently to the same datastore or perform a failback of each virtual machine to a different datastore. When performing a failback to different datastores, ensure the first failback is completed before performing another failback.

3. In the **Select the Source Host and Datastore for Failback** dialog box, do the following for each virtual machine on which you are performing a failback:

   a) Verify the original host and original datastore.

   b) In the **Failback to host** list, select the target host for failback.

   c) In the **Failback to datastore** list, select the target datastore for failback.

   d) To start the failback process, click **Failback**.

NOTE: During the failback process all changes to the active virtual machine are preserved and transmitted to the target host and datastore on the destination server, and the restored generation is powered on.

When the failback process is complete, you can perform replication on the source DS-Client to ensure all changed data is replicated to the destination DS-Client. Subsequent replication activities after failback will transmit only incremental changes to the destination server. To allow incremental replication, you must not delete the virtual machine at the destination server.

IMPORTANT: If the failback process stops or fails, restart the process. Do not delete a source virtual machine that has only been partially restored in a previous failback attempt.

8 Viewing logs

You can view logs to see past activities and events that occurred on the DS-Client. The logs are stored in the DS-Client database. Old logs are cleared from the database based on the advanced configuration settings. You can also clear logs from the database manually. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30).

DS-Client dumps all detailed logs to the asigra_archivlog folder. By default, this is located in the DS-Client installation directory, but can be configured using the **LogArchivePath** advanced configuration parameter. For more information, see Section 2.1.8, “Configuring the advanced settings”, on page 37.

For Grid DS-Clients, if the **LogArchivePath** parameter is not configured, each node writes to the its local asigra_archivlog folder for the activity it performs. However, DS-User can access only the detailed log on the main node. To ensure the detailed log for all sessions is accessible, configure **LogArchivePath** to a UNC path that can be accessed by all nodes.

NOTE: Logs older than the defined retention period are automatically deleted by the Admin processes. However, for each existing backup, the last 10 activities will be preserved even if they exceed the retention period for logs. So some backups with only a few activities might retain old logs indefinitely or until the backup itself is deleted.

If a DS-Client fails to start, it will record errors in the operating system event log:

- For Windows, the errors are logged in the Event Viewer.
- For Linux, the errors are logged in the following locations:

  ```
  /tmp/dsclient.err
  /tmp/dsclient.out
  /var/log/messages
  ```

- For Mac, the errors are logged in the following locations:

  ```
  /Library/Logs
  /var/log
  ```

8.1 Viewing the Activity Log

The Activity Log displays the activities that occurred on the DS-Client.

To view the Activity Log:

1. On the **Logs** menu, click **Activity Log**.
2. To filter the results, under **Select by**, do the following:
   a) To specify a different start date and time, beside the **From** box, click **[...]**. No activities before this date and time will be displayed.
   b) To specify a different end date and time, beside the **To** box, click **[...]**. No activities after this date and time will be displayed.
   c) To filter by activity, from the **Activity** box, select the activity.
   d) To filter by activity type, from the **Type** box, select the activity type.
   e) To filter by activity ID, select the **ID** check box, and then enter the ID.
   f) To filter by node or backup, beside the **Node/Set** box, click **[>>]**. Select the node or backup, and then click **Select**.
   g) To filter by backup schedule, from the **Schedule** box, select the schedule.
   h) To filter by retention rule, from the **Retention** box, select the retention rule.
   i) To filter by user, select one of the following options:
      - **Owner** — Searches for activities performed by the backup owner.
      - **Performed by** — Searches for activities performed by the specified user.
   j) To filter by node, in the **Node ID** box, select the node.

NOTE: This option is available only when connected to a Grid DS-Client.

---

3. Click **Find**. The following information is displayed:

Column	Description
Username	Name of the user who performed the activity. This column is empty if the activity was scheduled.
Activity	Type of activity.
Owner	Name of the owner of the backup
Customer	Name of the customer associated with the backup. This column is displayed only when using the multitenant feature.
Description	Description of the activity.
Node ID	DS-Client node associated with the activity. This column is displayed only when connected to a Grid DS-Client.
Warnings	Number of warnings that occurred during the activity.
Errors	Number of errors that occurred during the activity.
Start	Date and time the activity started.
End	Date and time the activity completed.
Duration	Length of time between the activity's start and end times.
Files	Number of files that were transferred or processed by the activity. For CDP backups that are currently running, this information is updated every 30 minutes.
Online	Amount of data transferred to or from online storage. For activities that do not transfer data, the value represents the amount of data processed. For CDP backups that are currently running, this information is updated every 30 minutes.
Transmitted Amount	Amount of data transmitted between the DS-Client and the DS-System. For activities that do not require a connection to the DS-System, this value represents the amount of data processed after deduplication and compression.
Completion	Status of the activity. Activities that appear in black are still in progress or have completed. Activities that appear in red did not complete. For more details, check the Event Log.
ID	Unique identification number of the activity.
Note	Additional information about the activity.

Table 1 Activity Log

4. To view a detailed log of all files that were affected by a backup or restore activity, click **Detailed Log**. Select a filter, and then click **Find**. You can narrow the search by using the filter options under **Path Filter**.

NOTE: When you search a detailed log, you are searching for a file stored in the asigra_archivlog folder. By default, the logs constantly accumulate.

---

5. To view event information for an activity, select the activity, and then click **Event Log**. For more information, see Section 8.2, “Viewing the Event Log”, on page 580.

6. Click **Close**.

8.2 Viewing the Event Log

The Event Log displays the errors, warnings, and information messages that occurred on the DS-Client for the selected period.

To view the Event Log:

1. On the **Logs** menu, click **Event Log**.By default, the log displays all the events for the current day.
2. To filter the results, under **Select by**, do the following:
   a) To specify a different start date and time, beside the **From** box, click **[...]**. No activities before this date and time will be displayed.
   b) To specify a different end date and time, beside the **To** box, click **[...]**. No activities after this date and time will be displayed.
   c) To view events of a specific type, in the **Type** box, select an event.
   d) To view events associated with a specific user, in the **User** box, type the user name.
   e) To view events associated with a specific category, in the **Category** box, select a category.
   f) To view events associated with a specific ID, select the **ID** check box, and then enter an ID number.
   g) To view events associated with a specific event number, type the number in the **Event#** box.
3. To exclude specific events from the Event Log, click **Exclude**, and then do the following:
   a) To add an event to the exclusion list, in the **Event #** box, type the associated event number, and then click **Add**.
   b) To delete an event from the exclusion list, select the associated event number, and then click **Remove**.
   c) To remove all event from the exclusion list, click **Clear**.
   d) To select a particular event, click **Select**. In the **Select Event #** dialog box, select an event, click **Select**, and then click **OK**. This event number is then displayed in the **Exclude Event #** dialog box.
   e) Click **OK**.

4. Click **Find**. The following information is displayed:

Column	Description
Icon	Event type (Information, Warning or Error).
Time	Date and time the event occurred.
User	Name of the user associated with the event. This column is empty if the activity was scheduled.
Category	Category of the event.
Event #	Event ID number.
ID	Unique ID that distinguishes one event from another.
Text	Additional information associated with the event.
Node ID	DS-Client node associated with the event. This column is displayed only when connected to a Grid DS-Client.
Description	Description of the event.

Table 2 Event Log

5. Click **Close**.

8.3 Viewing the Audit Trail

The Audit Trail displays a record of all changes made to the DS-Client database

To view the Audit Trail:

1. On the **Logs** menu, click **Audit Trail**.
2. To filter the results, under **Select by**, do the following:
   a) To specify a different start date and time, beside the **From** box, click **[...]**. No activities before this date and time will be displayed.
   b) To specify a different end date and time, beside the **To** box, click **[...]**. No activities after this date and time will be displayed.
   c) To view the Audit Trail for an operation, in the **Operation** box, select the operation.
   d) To view the Audit Trail for a user, in the **User** box, type the user name.
   e) To view the Audit Trail for a table in the database, in the **Table** box, select the table.
3. Click **Find**. The following information is displayed:

Column	Description
Icon	Operation type.
Time	Date and time the database change occurred.
User	Name of the user who performed the database change.
Operation	Type of database operation.
Table	Database table that was changed.
Description	Description of the database change that occurred.

Table 3 Audit Log

4. Click **Close**.

9 Working with reports

You can generate, print, or export reports based on activities performed on the DS-Client. You can also create custom reports based on the data from the DS-Client database tables.

NOTE: If you are logged into DS-Client as a member of the Administrators group, you will be able to view only reports that include DS-Client users.

9.1 Configuring the font for reports

You can customize the font used in PDF reports that the DS-Client service generates for each DS-User.

To configure the font for reports:

1. On the **Reports** menu, click **Report Setup**.
2. Under **Report Font**, click **Select**.
3. Browse for a font file, and then click **Open**.
4. Click **OK**.

9.2 Generating a global report for multiple DS-Clients

Global Reports display the selected report for multiple DS-Clients in the same session. Global reports require a list of DS-Clients and credentials so that the DS-User can connect and generate the reports. You must specify at least one DS-Client either individually or in a group by using the Auto Search feature.

NOTE: A toolbar at the top of the report has icons that you can use to navigate, print, or save the report.

To generate a global report for multiple DS-Clients:

1. On the **Reports** menu, point to **Global Reports**, and then select the global report you want to generate.
2. Beside **DS-Client(s)**, click **[...]**, and then do one of the following:
   - To add a DS-Client connection, click **Add**.

- To edit a DS-Client connection, select the connection, and then click **Modify**.

NOTE: To delete a DS-Client connection, select the connection, and then click **Remove**.

3. In the **New / Modify DS-Client Connection Entry** dialog box, do the following:
   a) In the **Name** box, type a name for the DS-Client connection.
   b) Beside the **IP Address** box, click **[...]**. Type the IP address of the DS-Client, and then click **Add.**
   c) In the **User Name** box, type the user name you want to use to access the DS-Client.
   d) In the **Password** box, type the password of the user you want to use to access the DS-Client.

   NOTE: These credentials must administrator privileges.

   e) In the **From** box, select the domain or server on which the user name and password will be verified.
   f) Click **OK**.
4. To add DS-Clients using the auto search feature, do the following:
   a) Click **Auto Search**.
   b) Select the DS-Clients you want to add, and then click **Add Selected**. To add multiple DS-Clients, hold down the CTRL key.
   c) Enter the user name and password that is valid on all the selected DS-Clients, and then click **OK**.

   NOTE: If you do not have common credentials with sufficient permissions, you must specify each DS-Client individually.

   d) Click **Close**.
5. To save the DS-Client connection entry list and credentials to the DS-User configuration file (user.ini), click **Save**. Enter the key to lock the credentials, and then click **OK**.

6. To load an existing DS-Client connection list and credentials from a DS-User configuration file (user.ini), click **Load**. Enter the key to unlock the credentials, and then click **OK**.

   NOTE: You can only save one set of DS-Client connection entries.

7. Click **OK**.

9.3 Generating a Backup Groups Report

The Backup Groups Report displays the usage by user groups.

NOTE: A toolbar at the top of the report has icons that you can use to navigate, print, or save the report.

To generate a Backup Groups Report:

1. Do one of the following:
   - To generate a Backup Groups Report for a single DS-Client, on the **Reports** menu, click **Backup Groups**.
   - To generate a Backup Groups Report for multiple DS-Clients, on the **Reports** menu, point to **Global Reports**, and then click **Backup Groups**.

   NOTE: If you have selected the multitenant feature, you can select the customer for which you want to generate the report. The report will display data only for the backups associated with the customer.

2. If you are generating a global report, beside **DS-Client(s)**, click **[...]**, and then select the DS-Clients for which you want to generate the global report.

   NOTE: For more information, see Section 9.2, “Generating a global report for multiple DS-Clients”, on page 583.

3. In the **Group Name** box, type the name of the group for which you want to create a report or click **[>>]** and select a group. By default this box is blank, and the report displays a summary for all the groups.
4. Under **Set Type**, select the backup types you want to display in the report. The options are as follows:
   - **Online** – Data from all online backups.
   - **Statistical** – Data from all statistical backups.

- **Self-contained** – Data from all current self contained backups.
- **Local-only** – Data from all Local-only backups.
- **Local DS-VDR** – Data from all Local DS-VDR backups (DS-System data storage and transmission amounts do not apply).
- **Instant Recovery** – Data from all instant recovery backups.

5. Click **OK**. The following information is displayed:

Report Header	
Account No.	Customer account number.
Account Name	Name of the customer account.
DS-Client No.	Number of the DS-Client covered in the report.
Customer Name	Customer that was selected when the report was generated, if the multitenant feature was selected.
Report Details	
DS-Client Report	DS-Client computer name.
Group	Group name.
Set Type	Types of backups described in the report.
Printing date	Day the report was printed.
Report Columns	
Group	Group name.
User Name	Users belonging to the group.
Full Name	Name associated with the user.
Files	Number of files currently stored online.
Online Amount	Total amount of space the files occupy online.

Table 1 Backup Groups Report

6. To print the report, click the **Print** icon on the menu bar.
7. To export the report to a file, click the **Save** icon on the menu bar.

9.4 Generating a Backup Items Report

The Backup Items Report displays information about each backup associated with a DS-Client.

NOTE: A toolbar at the top of the report has icons that you can use to navigate, print, or save the report.

To generate a Backup Items Report:

1. Do one of the following:
   - To generate a Backup Items Report for a single DS-Client, on the **Reports** menu, click **Backup Items**.
   - To generate a Backup Items Report for multiple DS-Clients, on the **Reports** menu, point to **Global Reports**, and then click **Backup Items**.

   NOTE: If you have selected the multitenant feature, you can select the customer for which you want to generate the report. The report will display data only for the backups associated with the customer.

2. If you are generating a global report, beside **DS-Client(s)**, click **[...]**, and then select the DS-Clients for which you want to generate the global report.

   NOTE: For more information, see Section 9.2, “Generating a global report for multiple DS-Clients”, on page 583.

3. Under **Set Type**, select the backup types you want to display in the report. The options are as follows:
   - **Online** – Data from all online backups.
   - **Statistical** – Data from all statistical backups.
   - **Self-contained** – Data from all current self contained backups.
   - **Local-only** – Data from all Local-only backups.
   - **Local DS-VDR** – Data from all Local DS-VDR backups (DS-System data storage and transmission amounts do not apply).
   - **Instant Recovery** – Data from all instant recovery backups.
4. Click **OK**. The following information is displayed:

Report Header	
Account No.	Customer account number.

Table 2 Backup Items Report

Account Name	Name of the customer account.
DS-Client No.	Number of the DS-Client covered in the report.
Customer Name	Customer that was selected when the report was generated, if the multitenant feature was selected.
Report Details	
DS-Client Report	DS-Client computer name.
Set Type	Types of backups described in the report.
Printing date	Day the report was printed.
Report Column	
Backup Set	Source server, backup name, and backup owner.
Set Type	Type of backup.
Backup Items	Individual backup items specified in the backup. • A double-plus sign (++) indicates this backup item includes sub-directories. • A single-plus sign (+) indicates this backup item does not include sub-directories. • A minus-sign (-) indicates that this is an “Exclude” backup item.

Table 2 Backup Items Report

5. To print the report, click the **Print** icon on the menu bar.
6. To export the report to a file, click the **Save** icon on the menu bar.

9.5 Generating a Backup / Restore Report

The Backup / Restore Report provides a detailed breakdown of each user's daily backup and restore activities during the specified report period.

NOTE: A toolbar at the top of the report has icons that you can use to navigate, print, or save the report.

To generate a Backup / Restore report:

1. Do one of the following:
   - To generate a Backup/Restore Report for a single DS-Client, on the **Reports** menu, click **Backup / Restore**.
   - To generate a Backup/Restore Report for multiple DS-Clients, on the **Reports** menu, point to **Global Reports**, and then click **Backup / Restore**.

   NOTE: If you have selected the multitenant feature, you can select the customer for which you want to generate the report. The report will display data only for the backups associated with the customer.

2. If you are generating a global report, beside **DS-Client(s)**, click **[...]**, and then select the DS-Clients for which you want to generate the global report.

   NOTE: For more information, see Section 9.2, “Generating a global report for multiple DS-Clients”, on page 583.

3. If you are generating an individual report, in the **Node/Set** box, type the name of the backup node and/or backup name that you want to view. By default this box is blank, allowing you to view the activities of all nodes or backups.
4. In the **Owner** box. type the name of the user whose activities you want to view. By default this box is blank, allowing you to view the activities of all users.
5. To specify a different start date and time, beside the **From** box, click **[...]**. No activities before this date and time will be displayed.
6. To specify a different end date and time, beside the **To** box, click **[...]**. No activities after this date and time will be displayed.
7. Under **Set Type**, select the backup types you want to display in the report. The options are as follows:
   - **Online** – Data from all online backups.
   - **Statistical** – Data from all statistical backups.

- **Deleted** – Data from all deleted backups. This uses data from the Activity Log.
- **Self-contained** – Data from all current self contained backups.
- **Local-only** – Data from all Local-only backups.
- **Local DS-VDR** – Data from all Local DS-VDR backups (DS-System data storage and transmission amounts do not apply).
- **Instant Recovery** – Data from all instant recovery backups.

8. Click **OK**. The following information is displayed:

Report Header	
Account No.	Customer account number.
Account Name	Name of the customer account.
DS-Client No.	Number of the DS-Client covered in this report.
Customer Name	Customer that was selected when the report was generated, if the multitenant feature was selected.
Report Details	
DS-Client Report	DS-Client computer name.
Set Type	Types of backups described in the report.
Period	Period covered by the report.
User Name	Name of the user.
Backup Set(s)	Name of the backup.
Printing date	Day the report was printed.
Report Columns	
User Name	User who performed the backup or restore and the date of the operation. Each day listed beneath a user name represents a day within the report period when either a backup or restore activity occurred for the user.
Activities	Total duration of all the backup or restore activities and the total number of sessions for the user.
Backup Activities	Number of files backed up, the size of data backed up, and the number of connections made to perform the backup.
Restore Activities	Number of files restored, the size of data restored, and the number of connections to perform the restore.

Table 3 Backup/Restore Report

9. To print the report, click the **Print** icon on the menu bar.
10. To export the report to a file, click the **Save** icon on the menu bar.

9.6 Generating a Backup Sets Report

The Backup Sets Report displays information about backups for each DS-Client.

NOTE: A toolbar at the top of the report has icons that you can use to navigate, print, or save the report.

To generate a Backup Sets Report:

1. Do one of the following:
   - To generate a Backup Sets Report for a single DS-Client, on the **Reports** menu, click **Backup Sets**.
   - To generate a Backup Sets Report for multiple DS-Clients, on the **Reports** menu, point to **Global Reports**, and then click **Backup Sets**.

   NOTE: If you have selected the multitenant feature, you can select the customer for which you want to generate the report. The report will display data only for the backups associated with the customer.

2. If you are generating a global report, beside **DS-Client(s)**, click **[...]**, and then select the DS-Clients for which you want to generate the global report.

   NOTE: For more information, see Section 9.2, “Generating a global report for multiple DS-Clients”, on page 583.

3. Under **Set Type**, select the backup types you want to display in the report. The options are as follows:
   - **Online** – Data from all online backups.
   - **Statistical** – Data from all statistical backups.
   - **Self-contained** –Data from all current self contained backups.
   - **Local-only** – Data from all Local-only backups.
   - **Local DS-VDR** – Data from all Local DS-VDR backups (DS-System data storage and transmission amounts do not apply).
   - **Instant Recovery** – Data from all instant recovery backups.
4. Click **OK**. The following information is displayed:

Report Header	
Account No.	Customer account number.
Account Name	Name of the customer account.

Table 4 Backup Sets Report

DS-Client No.	Number of the DS-Client covered in this report.
Customer Name	Customer that was selected when the report was generated, if the multitenant feature was selected.
Report Details	
DS-Client Report	DS-Client computer name.
Set Type	Types of backups described in the report.
Printing date	Day the report was printed.
Report Columns	
Backup Set	Backup sets defined on the DS-Client.
Connect As	User name being used to connect to the share/application.
Files	Number of files in each backup, including file generations.
Protected Size	Protected size of the backup data, which is the original, uncompressed amount of all the backup generations stored. • For Online backups, this is the amount of data protected in the DS-System Online storage. • For Statistical backups, this is the amount of data that would be protected if they were Online backups. • For Self-contained and Local-only backups, this is the amount of data protected in the corresponding local storage.
Stored Size	This column only appears if it is enabled from the DS-System. • For Online backups, this is the actual amount stored in the DS-System Online storage. DS-Client retrieves the current Stored Size amount from DS-System at the end of any successful backup, retention or delete process, as well as during any Weekly Admin or Daily Admin process. • This column does not apply for Statistical, Self-contained and Local-only backups.
Last Backup	Date of the most recent backup for the share.
Status	The status of the backup.

Table 4 Backup Sets Report

5. To print the report, click the **Print** icon on the menu bar.
6. To export the report to a file, click the **Save** icon on the menu bar.

9.7 Generating a Backup Trends Report

The Backup Trends Report displays usage statistics.

NOTE: A toolbar at the top of the report has icons that you can use to navigate, print, or save the report.

To generate a Backup Trends Report:

1. Do one of the following:
   - To generate a Backup Trends Report for a single DS-Client, on the **Reports** menu, click **Backup Trends**.
   - To generate a Backup Trends Report for multiple DS-Clients, on the **Reports** menu, point to **Global Reports**, and then click **Backup Trends**.

   NOTE: If you have selected the multitenant feature, you can select the customer for which you want to generate the report. The report will display data only for the backups associated with the customer.

2. If you are generating a global report, beside **DS-Client(s)**, click **[...]**, and then select the DS-Clients for which you want to generate the global report.

   NOTE: For more information, see Section 9.2, “Generating a global report for multiple DS-Clients”, on page 583.

3. If you are generating an individual report, in the **Node/Set** box, type the name of the backup node and/or backup name that you want to view. By default this box is blank, allowing you to view the activities of all nodes or backups.
4. In the **Owner** box. type the name of the user whose activities you want to view. By default, this box is blank, allowing you to view the activities of all users.
5. To specify a different start date and time, beside the **From** box, click **[...]**. No activities before this date and time will be displayed.
6. To specify a different end date and time, beside the **To** box, click **[...]**. No activities after this date and time will be displayed.
7. Under **Set Type**, select the backup types you want to display in the report. The options are as follows:
   - **Online** – Data from all online backups.
   - **Statistical** – Data from all statistical backups.
   - **Deleted** – Data from all deleted backups. This uses data from the Activity Log.

- **Self-contained** – Data from all current self contained backups.
- **Local-only** – Data from all Local-only backups.
- **Local DS-VDR** – Data from all Local DS-VDR backups (DS-System data storage and transmission amounts do not apply).
- **Instant Recovery** – Data from all instant recovery backups.

8. Under **Summary**, specify if you want the trends grouped by week or by month.
9. Click **OK**. The following information is displayed:

Report Header	
Account No.	Customer account number.
Account Name	Name of the customer account.
DS-Client No.	Number of the DS-Client covered in this report.
Customer Name	Customer that was selected when the report was generated, if the multitenant feature was selected.
Report Details	
DS-Client Report	DS-Client computer name.
Set Type	Types of backups described in the report.
Period	Period covered by the report.
User Name	Name of the user.
Backup Set(s)	Name of the backup.
Printing date	Day the report was printed.
Report Columns	
Week / Month	Week or month number.
Date	Period for the specified week or month.
Files	Total number of files backed up.
Total Size	Total size of all the files backed up.
Backup Time	Total duration of backups).

Table 5 Backup Trends Report

10. To print the report, click the **Print** icon on the menu bar.
11. To export the report to a file, click the **Save** icon on the menu bar.

9.8 Generating a Backup Users Report

The Backup Users Report displays every user associated with a backup on the DS-Client.

NOTE: A toolbar at the top of the report has icons that you can use to navigate, print, or save the report.

To generate a Backup Users Report:

1. Do one of the following:
   - To generate a Backup Users Report for a single DS-Client, on the **Reports** menu, click **Backup Users**.
   - To generate a Backup Users Report for multiple DS-Clients, on the **Reports** menu, point to **Global Reports**, and then click **Backup Users**.

   NOTE: If you have selected the multitenant feature, you can select the customer for which you want to generate the report. The report will display data only for the backups associated with the customer.

2. If you are generating a global report, beside **DS-Client(s)**, click **[...]**, and then select the DS-Clients for which you want to generate the global report.

   NOTE: For more information, see Section 9.2, “Generating a global report for multiple DS-Clients”, on page 583.

3. Under **Set Type**, select the backup types you want to display in the report. The options are as follows:
   - **Online** – Data from all online backups.
   - **Statistical** – Data from all statistical backups.
   - **Self-contained** – Data from all current self contained backups.
   - **Local-only** – Data from all Local-only backups.
   - **Local DS-VDR** – Data from all Local DS-VDR backups (DS-System data storage and transmission amounts do not apply).
   - **Instant Recovery** – Data from all instant recovery backups.
4. To view the report, click **OK**. The following information is displayed:

Report Header	
Account No.	Customer account number.

Table 6 Backup Users Report

Account Name	Name of the customer account.
DS-Client No.	Number of the DS-Client covered in this report.
Customer Name	If the multitenant feature is enabled, displays the customer that was specified when the report was generated. The report displays only information about backups associated with the specified customer.
Report Details	
DS-Client Report	DS-Client computer name.
Set Type	Types of backups described in the report.
Printing date	Day the report was printed.
Report Columns	
User Name	Name of each user associated with at least one backup.
Full Name	Full name of each user who created the backup.
Connect As	Credentials being used to access the backup's share.
Backup Set	Share and name of each backup on the DS-Client.
Online Limit	Maximum limit that each user can store online.
Online Amount	Amount that each user currently has online.

Table 6 Backup Users Report

5. To print the report, click the **Print** icon on the menu bar.
6. To export the report to a file, click the **Save** icon on the menu bar.

9.9 Generating a Restorable Volume Report

The Restorable Volume Report displays information about restorable files.

NOTE: A toolbar at the top of the report has icons that you can use to navigate, print, or save the report.

To generate a Restorable Volume Report:

1. Do one of the following:
   - On the **Reports** menu, click **Restorable Volume**.
   - On the **Reports** menu, point to **Global Reports**, and then click **Restorable Volume**.
2. If you are generating a global report, beside **DS-Client(s)**, click **[...]**, and then select the DS-Clients for which you want to generate the global report.

NOTE: For more information, see Section 9.2, “Generating a global report for multiple DS-Clients”, on page 583.

3. Under **Set Type**, select the backup types you want to display in the report. The options are as follows:

   - **Online** – Includes data from all online backups.
   - **Statistical** – Includes data from all statistical backups.
   - **Self-contained** – Includes data from all current self contained backups.
   - **Local-only** – Includes data from all Local-only backups.
   - **Local DS-VDR** – Includes data from all Local DS-VDR backups (DS-System data storage and transmission amounts do not apply).
   - **Instant Recovery** – Includes data from all instant recovery backups.

   NOTE: If the multitenant feature is enabled, you can select the customer for which you want to generate the report. The report will only display data for the backups associated with the customer.

4. To view the report, click **OK**. The following information is displayed:

Report Header	
Account No.	Customer account number.
Account Name	Name of the customer account.
DS-Client No.	Number of the DS-Client covered in this report.
Customer Name	If the multitenant feature is enabled, displays the customer that was specified when the report was generated. The report displays only information about backups associated with the specified customer.
Report Details	
DS-Client Report	DS-Client computer name.
Set Type	Types of backups described in the report.
Printing date	Day the report was printed.
Report Columns	
Backup Set	Backup sets on the DS-Client.
With deleted data (Native Size)	Latest generation of files, including files deleted from the backup source that are still backed up online. • **Files –** Number of files available for restore. • **Restorable Size –** Original protected size of the files as they were on the backup source.
Without deleted data	Latest generation of files, excluding files deleted from the backup source that are still backed up online. • **Files** – Number of files available for restore. • **Restorable Size –** Original protected size of the files as they were on the backup source.
Last Backup	Most recent date a scheduled backup was performed.

Table 7 Restorable Volume Report

5. To print the report, click the **Print** icon on the menu bar.

6. To export the report to a file, click the **Save** icon on the menu bar.

9.10 Generating a Restore Activities Report

The Restore Activities Report can be created on demand to show the restore activities performed by the DS-Client.

NOTE: A toolbar at the top of the report has icons that you can use to navigate, print, or save the report.

To generate a Restore Activities Report:

1. On the **Reports** menu, click **Restore Activities**.
2. In the **From Date** box, specify the start date for the report. No activities before this date will be displayed.
3. In the **To Date** box, specify the end date for the report. No activities after this date will be displayed.
4. In the **Backup Type** box, select a backup type.
5. If the multitenant feature is enabled, you can select the customer for which you want to generate the report. The report will only display data for the backups associated with the customer.
6. Under **Order report by,** select whether you want to sort the report by machine, backup name, or restore date.
7. To view the report, click **OK**. The following information is displayed:

Report Header	
Account No.	Customer account number.
Account Name	Name of the customer account.
DS-Client No.	Number of the DS-Client covered in this report.
Customer Name	If the multitenant feature is enabled, displays the customer that was specified when the report was generated. The report displays only information about backups associated with the specified customer.
Restore Details	
DS-Client Report	DS-Client computer name.
Backup Type	Types of backups described in the report.
Order By	Sort order.
Period	Period covered by the report.
Printing date	Day the report was printed.
Report Columns	

Table 8 Restore Activities Report

Activity ID	Unique activity ID.
Machine Name	Name of the original backup source machine.
Backup Set Name	Backup set name.
Restore Reason	Restore reason specified by user that performed the restore.
# of Files Restored	Number of files restored.
Stored Amount Restored (MB)	Size of the restored files based on the space they occupy in the DS-System, including compression.
Native Amount Restored (MB)	Size of the restored files based on the space they occupy after being restored and decompressed to the target machine.
Restore Start Time	Time when the restore process started.
Restore End Time	Time when the restore process completed.
Duration	Total duration of the restore process.

Table 8 Restore Activities Report

8. To print the report, click the **Print** icon on the menu bar.
9. To export the report to a file, click the **Save** icon on the menu bar.

9.11 Generating a Statistical Summary Report

The Statistical Summary Report displays usage statistics.

NOTE: A toolbar at the top of the report has icons that you can use to navigate, print, or save the report.

To generate a Statistical Summary report:

1. Do one of the following:
   - On the **Reports** menu, click **Statistical Summary**.
   - On the **Reports** menu, point to **Global Reports**, and then click **Statistical Summary**.
2. If you are generating a global report, beside **DS-Client(s)**, click **[...]**, and then select the DS-Clients for which you want to generate the global report.

   NOTE: For more information, see Section 9.2, “Generating a global report for multiple DS-Clients”, on page 583.

3. If you are generating an individual report, in the **Node/Set** box, type the name of the backup node and/or backup name that you want to view. By default this box is blank, allowing you to view the activities of all nodes or backups.
4. In the **Owner** box. type the name of the user whose activities you want to view. By default this box is blank, allowing you to view the activities of all users.

5. In the **From Date** box, specify the start date for the report. No activities before this date will be displayed.
6. In the **To Date** box, specify the end date for the report. No activities after the this date will be displayed.
7. Under **Backup set type to include**, select the backup types you want to display in the report. The options are as follows:
   - **Online** – Includes data from all online backups.
   - **Statistical** – Includes data from all statistical backups.
   - **Self-contained** – Includes data from all current self contained backups.
   - **Local-only** – Includes data from all Local-only backups.
   - **Local DS-VDR** – Includes data from all Local DS-VDR backups (DS-System data storage and transmission amounts do not apply).
   - **Instant Recovery** – Includes data from all instant recovery backups.

   NOTE: If the multitenant feature is enabled, you can select the customer for which you want to generate the report. The report will only display data for the backups associated with the customer.
8. Under **Group report by,** select whether you want to group the report by machine, backup, or user.
9. To update the statistics before you preview or print the report, select the **Gather new statistics before preview** check box. If this option is selected, DS-Client runs an update statistics process as part of the Daily/Weekly Admin. This can take some time, depending on the size of the database.

   NOTE: The **Statistics updated on** box displays the last time the DS-Client statistics were updated.
10. To view the report, click **OK**. The following information is displayed:

Report Header	
Account No.	Customer account number.
Account Name	Name of the customer account.
DS-Client No.	Number of the DS-Client covered in this report.
Customer Name	If the multitenant feature is enabled, displays the customer that was specified when the report was generated. The report displays only information about backups associated with the specified customer.
Report Details	

Table 9 Statistical Summary Report

DS-Client Report	DS-Client computer name.
Set Type	Types of backups described in the report.
Period	Period covered by the report.
Statistics updated on	Date when the statistics were gathered.
Printing date	Day the report was printed.
User Name	Name of the user.
Backup Set(s)	Name of the backup.
Report Columns	
Machine Name / Backup Set / User	Indicates if the report is sorted by machine, backup, or user.
Date	Each line corresponds to a specific day.
New Files	• **#** – Number of new files • **Amount (MB)** – Amount of data (MB) in the new files
Backed Up Files	• **# –** Total number of files backed up • **Amount (MB) –** Amount of data in the backed up files • **Transmitted (MB) –** Total size of files transmitted (this only includes the successfully transmitted amount) • **Compression Ratio** – Ratio achieved = Amount/ Transmitted
Transmitted Amount (MB)	Total amount transmitted from DS-Client to DS-System, including amounts transmitted for incomplete or failed backups.
Files Stored Off Site	• **# –** Total number of backup files stored off-site • **Amount (MB) –** Total size of the backed up files This includes each generation of a file. For example three generations of a 10MB file would show 3 files and 30MB transmitted. Only generations that are still online are counted. This column refers to the amount of data before compression, encryption, common file elimination, master/delta processing.
Backup time (min.)	Total backup time (per day) for the corresponding computer / backup / user.

Table 9 Statistical Summary Report

11. To print the report, click the **Print** icon on the menu bar.
12. To export the report to a file, click the **Save** icon on the menu bar.

9.12 Viewing a Load Summary Report

The Load Summary Report can help you analyze the load on the DS-Client computer for a selected period. If you observe high values at a particular time, you should consider rescheduling the activities to distribute the load more evenly. If you observe high values at all times, you should consider using a more powerful computer or delegate some backups to another DS-Client.

The DS-Client service automatically collects data for these statistics at one minute intervals. Every five minutes, the DS-Client service updates an internal table with the peak amounts for the following statistics:

Send amount	Peak amount transmitted to the DS-System (KB/sec)
Receive amount	Peak amount received from the DS-System (KB/sec)
CPU load	CPU utilization (0-100%)
Memory load	Memory utilization (0-100%)
Memory committed	Amount of allocated memory (in MB)
Activities	Number of DS-Client activities

NOTE: You must have sufficient rights to view information about each backup.

To view a Load Summary Report:

1. On the **Reports** menu, click **Load Summary**.
2. In the **Chart Type** box, select the type of chart you want to view.
3. To filter the results, under **Select by**, do the following:
   a) In the **From** box, specify the start date for the report. No activities before this date will be displayed.
   b) In the **To** box, specify the end date for the report. No activities after this date will be displayed. By default, this is set to the current date.
   c) In the **Interval** box, select the interval for the horizontal axis of the report.
4. To change the load summary content, click **Series**, and then do the following:
   a) Add or change as many items as required. To select all the items, click **Select All.** It is recommended to view only two or three items at a time to keep the display manageable.
   b) Click **OK**.
5. To update the information, click **Refresh**.
6. Click **Close**.

9.13 Viewing an Online File Summary Report

The Online File Summary Report displays a list of files in the DS-System online storage. Using this report you can identify duplicate files that are being backed up.

To view an Online File Summary Report:

1. On the **Reports** menu, click **Online File Summary**.
2. To filter the results, do the following:

a) In the **Filter** box, type the filter you want to apply to the report. For example, you can search for files that match a specific pattern (e.g. *.doc).

b) In the **Category** box, select the category of files you want to display in the report. The options are as follows:

- **All** – Displays all category of files.
- **All files** - Displays all files.
- **Duplicate files** - Displays files that have more than one copy, minus one for each unique common file group.
- **Changed and new files** - Displays files that are new or have changed from the start of the search period.
- **Unchanged files** - Displays files that have not changed since the start of the search period.

c) In the **Duplication** box, enter the number of duplicate files that must exist.

d) To display only the totals, select the **Totals only** check box.

e) In the **Share/Set** box, specify the specific shares on the LAN that you want to search.

a) To select the types of backups you want to include in the report, click **Set Types**. Select the backup type, and then click **OK**. The options are as follows:

- **Online** – Includes data from all online backups.
- **Self-contained** – Includes data from all current self contained backups.
- **Local-only** – Includes data from all Local-only backups.
- **Instant Recovery** – Includes data from all instant recovery backups.

3. Click **Find**. The process scans all the backup files on the DS-System. For each row, a file is counted only once even if there are multiple generation of the file. The following information is displayed:

Column	Description
Category	Category of files.
Files	Number of files.
Files (%)	Percentage of the total number of files.
Size (MB)	Size of the files.
Size (%)	Percentage of the total size.

NOTE: The **Status** box displays the status of the online search.

4. In the **Last** box, enter the last number of days for which you want to display information.
5. To view detailed information about a row, select the row, and then click **Detail**. Each line represents a unique file. If more than one copy exists, the duplication amount is indicated in that column. Do the following:
   a) To view duplicate instances of a specific file, click **Show Duplicates**. You should monitor backups to ensure duplication is considered.
   b) Click **Close**.

NOTE: A maximum of 50,000 files can be displayed. If the scan returns more than this number, the results are sectioned.

---

6. To view a pie chart of a row, select the row, click **Chart**, and then do the following:
   a) In the **View type** box, select the category you want to view.
   b) Select whether you want to view the information by files or by size.
   c) Click **Close**.
7. Click **Close**.

9.14 Viewing a Storage Summary Report

The Storage Summary Report allows you to analyze the trends for online amount, number of files, and backup time. There are two types of statistics: primary (such as online, files, and backup files) and derived (all of the incremental amounts). A primary statistic reflects a real number obtained from the statistics. A derived statistic is linked to a primary statistic and is obtained by subtracting the previous statistic from the current one.

NOTE: The Storage Summary Report uses storage information from the last Daily Admin process.

To view a Storage Summary Report:

1. On the **Reports** menu, click **Storage Summary**.
2. In the **Chart Type** box, select the type of chart you want to view.
3. To filter the results, under **Select by**, do the following:
   a) In the **From** box, specify the start date for the report. No activities before this date will be displayed.
   b) In the **To** box, specify the end date for the report. No activities after this date will be displayed. By default, this is set to the current date.
   c) In the **Owner** box. type the name of the user whose activities you want to view. By default this box is blank, allowing you to view the activities of all users.
   d) In the **Node/Set** box, specify backup node and/or backup that you want to view. By default this box is blank, allowing you to view the activities of all nodes or backups.
   e) To update the information, click **Refresh**.
4. To configure the chart details, under **Chart options**, do the following:
   a) In the **Interval** box, select the interval for the horizontal axis of the report.
   b) In the **View** box, select whether you want to view a chart or a list.
5. Under **Backup set type**, select the types of backups you want to include in the report. The options are as follows:
   - **Online** – Includes data from all online backups.
   - **Statistical** – Includes data from all statistical backups.
   - **Self-contained** – Includes data from all current self contained backups.
   - **Local-only** – Includes data from all Local-only backups.
   - **Local DS-VDR** – Includes data from all Local DS-VDR backups (DS-System data storage and transmission amounts do not apply).

- **Instant Recovery** – Includes data from all instant recovery backups.

6. To change the load summary content, click **Series**, and then do the following:

   a) Under **Backup Time**, select the backup time statistics (in minutes) that you want to view. The options are as follows:

      - **Average** – The average duration of all scheduled and on-demand backup sessions for the selected period.
      - **Actual** – The total duration of all scheduled and on-demand backup sessions for the selected period.

   b) Under **Files**, select the file statistics that you want to view. The options are as follows:

      - **Total** – The total number of files stored online, including all generations.
      - **Inc** – The increment to the total files. This is a derived figure.
      - **New** – The total number of new backed up files. These are files backed up for the first time.
      - **Backup** – The total number of files backed up for the selected period.
      - **Inc Backup** – The increment to the backup files. This is a derived figure.

   c) Under **Amount**, select the amount statistics (in MB_) that you want to view. The options are as follows:

      - **Total Online** – The total amount stored online.
      - **Inc Online** – The increment to the total online. This is a derived figure.
      - **New Online** – The total amount for the new backed up files.
      - **Transmitted** – The total amount of data transmitted to DS-System, including the effects of compression, DS-Delta and DS-Library.
      - **Inc Transmitted** – The increment to the transmitted amount. This is a derived figure.
      - **Online Backup** – The total amount of data backed up for the selected period.
      - **Inc Online Backup** – The increment to the online backup. This is a derived figure.

   d) Click **OK**.

7. Click **Close**.

9.15 Exporting information about backups

You can export information about a DS-Client backup to a file.

NOTE: Depending on the DS-Client account configuration set by your service provider, some additional columns might be visible.

To export information about backups:

1. Do one of the following:
   - On the **Reports** menu, point to **Export**, and then click **Backup Sets Info**.
   - On the **Reports** menu, point to **Global Reports**, and then click **Export Backup Sets Info**.
2. In the **File Format** box, select the format to which you want to export the information about backups.
3. If you selected Comma separated values (*.csv) as the format type, in the **Field Delimiter** box, select the field separators (tab, comma, semi-colon) you want to use for the exported data.
4. Beside the **Save As** box, click the corresponding icon to save the file. The export file contains the following information:

Column	Description
ID	Unique backup ID number.
Name / Description	Description of the backup.
Restorable Files	Number of files available for restore without deleted data. This is the size that would be displayed when selecting to restore the entire backup. Deleted data is backed up files that no longer exist on the source computer.
Restorable Amount	Amount (in bytes) of data available for restore.
Restorable Files	Number of files available for restore with deleted data.
Restorable Amount	Amount (in bytes) of files available for restore with deleted data.
Protected Generation Count	Total number of file generations stored on the DS-System.
Protected Amount	Amount (in bytes) of the data storage on the DS-System (as it appears in the Backup Set's Properties > Set Info - Online Amount).
Last Backup	The Last Backup column indicates the most recent date a backup was performed for that share.
Files not picked up by Last Backup	Files that were not backed up by the last backup session. If the backup was not interrupted by the user ("User Stop"), this is the number (amount) of files that did not change.
Amount not picked up by Last Backup	Amount (in bytes) of the above.

9.16 Creating a custom report

The custom reports feature allows you to create your own reports based on the data provided from the database tables. A third-party application called JasperReports (https://www.jaspersoft.com/) is required to create a customized report using the exported data set. This feature is intended for advanced users.

9.16.1 Exporting a data set file for a custom report

Before you can generate a custom report, you must export a data set file containing the fields from the database. To generate multiple custom reports, you must use the data fields to create a reusable custom report template.

To create a data set file:

1. On the **Reports** menu, click **Customized Data**.
2. Do the following:
   a) In the **Data Set** box, do one of the following:
      - To create a data set, click **<New>**.
      - To use an existing data set, select the data set from the list,
   b) In the **View** box, select the view. A view is a predefined group of tables from the database. You can select only one view per data set.
   c) Click **Next**.

NOTE: Data set selections are saved in the DS-User configuration file (user.ini).

---

3. Do the following:
   a) To add a data field, in the **Available Columns** list, select the data field you want to add, and then click **Add**.
   b) To remove a data field, in the **Selected Columns** list, select the data field you want to remove, and then click **Remove**.

   NOTE: To select multiple fields, use the SHIFT or CTRL keys.

   ---

   c) To change the order of the data fields, select the data field, and then click **Up** or **Down**. This is the order the data fields will be written.
   d) Click **Next**.
4. Do the following:

a) To add a data field, in the **Available Columns** list, select the data field you want to add, and then click **Add**.

b) To remove a data field, in the **Selected Columns** list, select the data field you want to remove, and then click **Remove**.

NOTE: To select multiple fields, use the SHIFT or CTRL keys.

---

c) To change the order of the data fields, select the data fields, and then click **Up** and **Down**. This is the order the data fields will be written.

NOTE: If you do not make a selection, data will be written as it is read from the database. This sort order is not used by JasperReports.

---

d) Click **Next**.

5. Do the following:

a) In the **Filter Column**, select the data field that you want to filter.

b) Configure the available filter options for the data field. The **Filter Value Column** displays how the filter will be applied to the data field.

NOTE: If you do not set any filters, all data is exported. If you set a filter, only data that matches the filter is exported. If the filter value is left blank, no filter will be applied and all data for that field will be returned.

---

c) Click **Next**.

6. Do the following:

a) To save the data set settings (except for data filters) in the DS-User configuration file (user.ini) so that you can reuse the same data set, select the **Save data set settings** check box.

b) In the **Data Set Name** box, type a name for the data set.

c) To export the data set to a file, select the **Export data to file** check box.

d) Click **Next**.

7. Review the summary to ensure that the data set is customized as required, and then click **Finish**.

8. If you selected the **Export data to file** option, save the data set as an XML or CSV file.

NOTE: To create a custom report template using JasperReports, you must save the exported data set file in XML format. After you have created the jasper file, copy it to the local \report subdirectory where DS-User is installed. If the folder does not exist, create it.

9.16.2 Creating a custom report using exported data

After you have exported a data set file, you can create a custom report using the exported data set.

To create a custom report:

1. On the **Reports** menu, click **Customized Reports**.
2. Do the following:
   a) In the **Template name** box, select a custom report template.
   b) In the **File name** box, the path to the custom report template is displayed.
   c) In the **Query string** box, the internal query that was specified when the report was created using JasperReports is displayed.
   d) In the **View** box, the view that the data set is based on is displayed.
   e) Click **Next**.
3. Do the following:
   a) In the **Filter Column**, select the data field that you want to filter.
   b) Configure the available filter options for the data field. The **Filter Value Column** displays how the filter will be applied to the data field.

      NOTE: By default, all data is displayed in the report. If you set a filter, the custom report will display only data that matches the filter.

   c) Click **Next**.
4. Do the following:

a) To add a data field, in the **Available Columns** list, select the data field you want to add, and then click **Add**.

b) To remove a data field, in the **Selected Columns** list, select the data field you want to remove, and then click **Remove**.

NOTE: To select multiple fields, use the SHIFT or CTRL keys.

---

c) To change the order of the data fields, select the data fields, and then click **Up** and **Down**. This is the order the data fields will be written.

NOTE: If you do not make a selection, data will be written as it is read from the database.

---

d) Click **Next**.

5. Click **Finish**.

10 Working with a Grid DS-Client (Windows)

In high-performance environments, you can maximize DS-Client processing and distribute the load across two or more computers using a Grid DS-Client configuration. In this configuration, the DS-Client software is installed on multiple computers called nodes that are configured to use the same database.

- The Grid DS-Client is composed of one main node and one or more leaf nodes.Each node in the grid configuration, including the main node, performs its own backup and restore activities.
- The main node accepts DS-User connections and manages all running activities to ensures that the leaf nodes do not run conflicting activities. The leaf nodes perform activities as instructed by the main node.
- If the main node fails, all activities running on the node stop. However, activities on the leaf nodes continue to run. A new main node is selected from the running leaf nodes.
- If the leaf node fails, all activities running on that node will stop. However, activities on the main node and the other leaf nodes will continue to run.

NOTE: For detailed instructions on how to install a Grid DS-Client, see the *Client Software Installation Guide*.

Since the DS-User can only connect to the main node, which is chosen randomly from the running nodes, ensure that the DS-User is configured with the IP address of each node in the Grid DS-Client. For more information, see Section 2.2, “Configuring the initialization settings”, on page 60.

NOTE: This is not necessary if DS-User and all DS-Client nodes are in the same subnet. By default, a DS-User can see all running DS-Clients in the same subnet.

For Grid DS-Clients, the database server saves a copy of the DS-Client databases in the DS-Client buffer of the node that performs the Daily Admin or Weekly Admin activities. By default, this folder is:

```
C:\Program Files\CloudBackup\DS-Client\db_buffer
```

The Daily / Weekly Admin activity is allocated by the main node to a leaf node with a lower load.

NOTE: The location for the DS-Client database dump folder can be configured using the **DSCDBDumpPath** parameter. For more information, see Section 2.1.8, “Configuring the advanced settings”, on page 37.

When you connect to a Grid DS-Client, a **Grid** menu is activated and the following dialog boxes will have an additional option to select by the Node ID:

- Activity Log Viewer (Logs > Activity Log)
- Load Summary (Reports menu > Load Summary)
- DS-Client System Status (Setup > System Activities > System)
- DS-Client Advanced Configurations (Setup > Configuration > Advanced tab)

10.1 Managing a Grid DS-Client

You can view the status of a Grid DS-Client configuration and perform several management tasks, including stopping a node or exporting the IP address of the nodes in the Grid DS-Client configuration.

To manage a Grid DS-Client:

1. On the **Grid** menu, click **Grid Status**.
2. To view a visual representation of the Grid DS-Client configuration, click the **Graph** tab. To change the format, in the **Graph Layout** box, select **Linear** or **Star**.
3. To view a detailed list of all the nodes in the Grid DS-Click configuration, click the **List** tab.
4. To stop a node, do the following:
   a) Select the **List** tab.
   b) Select the node that you want to stop, and then click **Stop Node**.
   c) Under **Stop the selected DS-Client service**, select one of the following options:
      - **Wait for all running activities to complete** – Stops the DS-Client on the selected node after all the current activities have completed. No new activities will be allowed.
      - **Stop when all activities complete or force stop after [...] minute(s)** – Stops the DS-Client on the selected node after all the current activities have completed or forces a stop after the specified time has elapsed. No new activities will be allowed.
   d) Under **Stop Type**, specify whether you want to shut down the computer, reboot the computer, or stop DS-Client service only.
   e) Click **OK**.
5. To export the Grid DS-Client IP address (internal or external) to a text file, do the following:
   a) Click **Export**.
   b) Beside **Address Type**, select one of the following options:

- **Internal Address** – Exports the internal (LAN) IP addresses to a text file that can be used to configure DS-Users with a Grid DS-Client.
- **External Address** – Exports the external (WAN) IP addresses. to a text file that can be used to configure external DS-Users with a Grid DS-Client.

c) Click **OK**.

d) Select the destination format and location, and then click **Save**.

NOTE: The text file can be imported when configuring a DS-Client. For more information, see Section 2.2.1, “Configuring the connection settings”, on page 60.

---

6. In the **Refresh Every** box, enter the refresh interval for the data. To refresh the information immediately, click **Refresh**.
7. Click **Close**.

10.2 Viewing the Grid DS-Client Log

The Grid DS-Client Log displays all events related to the Grid configuration.

To view the Grid DS-Client Log:

1. On the **Grid** menu, click **Grid Log**.
2. To filter the results, under Select by, do the following:

   a) To specify a different start date and time, beside the **From** box, click **[...]**. No activities before this date and time will be displayed.

   b) To specify a different end date and time, beside the **To** box, click **[...]**. No activities after this date and time will be displayed.

   c) To filter by event type, from the **Event Type** box, select the event type.
3. Click **Find**. The following information is displayed:

Column	Description
Icon	Severity of the event.
Time	Date and time the event occurred.
Node ID	Grid ID of the node.
IP Address	IP address of the node.
Event	Event ID.
Text	Description of the event.

Table 1 Grid DS-Client Log

4. Click **Close**.

11 Using premium backup and recovery services

There are several premium backup and recovery services that you can use.

11.1 Initial backups

The DS-Client service is designed to perform automated backups to an off-site location. The DS-Client service backs up only incremental changes after the first backup. This requires an adequate communication link between DS-Client and DS-System that will allow backup of any modified data in the given time frame.

The first, full baseline backup often requires transferring a large amount of data. If the communication link between the DS-Client and the DS-System cannot handle this large transfer in a reasonable amount of time (for example, a few days), you can consider using the initial backup feature.

Two tools are available to help you to determine the size of your baseline backup and whether initial backup will be a more efficient method.

- You can use the LAN Storage Discovery Tool to analyze your LAN. For more information, see Chapter 12, “Using LAN Storage Discovery Tool”.
- You can use Statistical backups to calculate the amount of data to transmit. Divide this number by your communications bandwidth to estimate how long the first backup will take.

The initial backup feature allows you to back up to local buffer locations that are either directly connected to DS-Client or visible on the LAN and then to ship that media (for example, disks) to your service provider. Your service provider will import the initial backup data from a media that is either attached to DS-System or connected via a LAN connection. Once the initial backup data is imported into DS-System, you can perform subsequent scheduled and on-demand backups.

When running initial backups, consider the following best practices:

- The path specified must accommodate the size of the incoming data.
- The file system on the initial backup buffer must be able to handle the size of the incoming files.
- When running several initial backups at the same time, ensure the device where the initial buffer is located can handle the I/O load. If too many initial backup processes are sending data to the same path at the same time, the sessions might stop and errors will be reported.
- All Initial backups written to the same initial backup path must be completed before the physical media is sent to your service provider. To verify, click **Status** on the **Initial Backup** menu.
- Always check the DS-Client Activity Log and the Event Viewer at the end of every initial backup session to ensure that no errors are reported.

- If the initial backup session is interrupted, it can be resumed by starting another backup session. However, you must first synchronize the backup. The other option is to reset the backup as Incomplete (on the **Initial Backup** menu, click **Status**, select the backup, and then click **Mark Incomplete**), and then rerun the initial backup from the beginning.

To use the initial backup service:

1. Ensure that your DS-Client is already registered with DS-System.
2. Configure the initial backup path.
3. Create an initial backup.
4. Perform a on-demand backup of the initial backups.
5. Monitor the status of the initial backups.
6. Ship the initial backup buffer media to your service provider.

11.1.1 Configuring the initial backup path

You must have at least one path configured to perform an initial backup. You can configure as many initial backup paths as you need. These are local disks or UNC path locations (Windows DS-Client) that can be shipped to your service provider.

NOTE: You should plan to assign each initial backup path only to backups from the same DS-Client. After being assigned to the backups of one DS-Client, the initial backup path is also called the initial backup buffer of that DS-Client.

---

1. On the **Initial Backup** menu, click **Path**.
2. To add an initial backup path, click **Add**, and then do one of the following:
   - For Windows DS-Clients, do the following:
     a) Beside the **Computer** box, click **>>**, and then select the computer on which you want to add the initial backup path.
     b) Beside the **Directory** box, click **>>**, and then select the directory on the computer where you want to add the initial backup path.
     c) Under **Select encryption method**, select an encryption method for the metadata.
     d) If you selected **Encrypt with specified key**, you must type or import the alphanumeric key of up to 32 characters for the encryption. You can also export this key in encrypted format to a text file for distribution.
     e) Click **OK**.
   - For Linux DS-Clients, do the following:

a) Beside the **Backup Path** box, click **>>**, and then select the directory on the computer where you want to add the initial backup path.

b) Under **Metadata encryption**, select an encryption method for the metadata.

c) If you selected **User-defined**, you must type or import the alphanumeric key of up to 32 characters for the encryption. You can also export this key in encrypted format to a text file for distribution.

d) Click **OK**.

NOTE: The encryption methods are available only to backups. For VM replication sets, the replication data is encrypted using a randomly generated encryption key.

3. To specify different credentials for an initial backup path, select the path, and then click **Credentials**. This option is available only on Windows DS-Clients.
4. To refresh the initial backup path list, click **Refresh**.
5. To delete an initial backup path, select the path, and then click **Delete**.
6. Click **Close**.

11.1.2 Creating an initial backup

When creating a backup, you can configure the path location to which the initial backup data will be sent. You can also use the initial backup option in any backups on which a backup has never been performed.

Before you can use the initial backup option, at least one initial backup path must have already been configured. For more information, see Section 11.1.1, “Configuring the initial backup path”, on page 618.

NOTE: Each initial backup path should be assigned only to backups from the same DS-Client. After being assigned to the backups of one DS-Client, the initial backup path is also called the initial backup buffer of that DS-Client.

To create an initial backup:

1. Access the initial backup option in one of two ways:
   - When creating a new backup, do the following:
     a) On the **Sets** menu, click **New Backup Set**.
     b) Proceed through the selection of the backup kind, backup source location, backup items, and backup item options.

c) Select **Initial Backup**.

- In the Backup Sets tree, browse and select an existing backup on which backup has never been performed.

  a) On the **Sets** menu, point to **Backup Sets**, and then click **Properties**.

  b) Click the **Options** tab.

  c) Select **Initial Backup**.

2. In the **Initial Backup Settings** dialog box, select the **Initial Backup** path for this backup, and then click **OK**.

The initial backup data is placed in the initial backup path, or initial backup buffer, assigned to the backup.

11.1.3 Monitoring the status of an initial backup

You can view the status of each backup that has been configured for initial backup. Backup sets are displayed only before their initial backup data has been successfully imported into the DS-System.

NOTE: Scheduled and on-demand backups of initial backups are not allowed until after the initial backup data has been successfully imported into DS-System.

When the status of all the backups sharing the same initial backup buffer is completed, you can place the data in the initial backup buffer onto a physical media and ship the physical media to your service provider.

NOTE: If data on multiple initial backup buffers needs to placed onto the same physical media, ensure that the data from each initial backup buffer is placed in a separate clearly labeled folder.

To monitor the status of an initial backup:

1. On **Initial Backup** menu, click **Status**.
2. To change the status of an initial backup to completed, select the backup and then click **Mark Completed**.

   NOTE: You might want to do this if some backup data is in the buffer. For example, if the initial backup was interrupted.

3. To change the status of an initial backup to incomplete, select the backup and then click **Mark Incomplete**.

NOTE: You might want to do this to change the initial backup path or run another backup.

---

4. To update the list, click **Refresh**.
5. Click **Close**.

11.2 Disc/tape backups

The DS-Client service is designed to perform automated backups to an off-site location. However, if you need to restore a large amount of data (due to a server crash or other disaster), the communication link between DS-Client and DS-System might not allow the restore process to be completed in a reasonable amount of time. In these cases, you can use the Disc/Tape feature to have the required data written to media and shipped to your physical location.

To reduce your down time, you can ask your service provider to write the required data to Disc/Tape media (snapshot of latest generation only). This must be done for each backup you need. DS-System copies all requested files to Disc/Tape media in encrypted format, the Disc/Tape media is shipped to the DS-Client's physical location, and the required data is restored from Disc/Tape media attached to the DS-Client (or through the LAN).

The disc/tape feature is available only when the following prerequisites are met:

- Your service provider/administrator has a software license that includes Disc/Tape as a DS-Tool.
- DS-System is configured for Disc/Tape Service. This includes making adequate buffer space and a media writer (e.g. CD/DVD burner) available and adding the appropriate media to DS-System.
- Disc/Tape is selected as a DS-Tool in DS-Client.

Using this feature you can copy backed up files from DS-System to any media supported by your service provider (e.g. CD/DVD, Tape, Hard Disk Drive, or USB). You can also have a copy of backed up data on hand (at your location). Data on the Disc/Tape media must be restored through DS-Client.

11.2.1 Requesting a disc/tape backup

Disc/Tape Request is a restore feature that allows you to obtain restored data via a media of your choice (e.g. CD/DVD, Tape, Hard Disk, or USB). The requested data will be delivered through that media instead of the network.

You can select files from a backup that you want to restore. Based on your selections, DS-System places a copy of the requested files into a buffer directory. From that buffer, your service provider/administrator can copy the requested files onto your specified medium and then mail or deliver the media to you. Upon receiving the media, you can retrieve the data on it through DS-User.

To request a disc/tape backup:

1. From the backups tree, select the backup for which you want to request a disc/tape backup.
2. On the **Restore** menu, point to **Disc/Tape**, and then click **Request**.
3. Do the following:
   a) In the **Media** box, select the media that you want to use for the disc/tape request. This is defined by your service provider in the DS-System.
   b) Under **Options**, select one of the following options:
      - **Snapshot (latest generation of all files)** – Creates a snapshot of the latest version of all files in the backup.
      - **Selective (customize Disc/Tape request)** – Allows you to select the directories and files you want to restore.
   c) Click **Next**.
4. If you selected the **Selective (customize Disc/Tape request)** option, do the following:
   a) Under **Directories Tree**, select the directories and files that you want to restore.
   b) To display the number of files and calculate the total amount based on your selection, select the **Calculate amount** check box.
   c) To view the items you have selected, click **Selection**.
   d) To configure advanced options, click **Advanced**.
   e) Click **Finish**.
5. In the **Disc/Tape Mailing Information** dialog box, enter the required mailing information for your disc/tape shipment, and then click **OK**.

DS-System mirrors all the selected files from the request process to a buffer directory on the DS-System. Your service provider will then make the disc/tape order from this buffer.

NOTE: This backup will not be accessible (for backup) until your service provider makes the disc/tape.

11.2.2 Viewing the status of a disc/tape request

You can view the status of your disc/tape request. Once DS-System has resolved the requested files in its database, the order status will show Purchased. However, the backup files must not be altered by subsequent backups or any other process with write access to the backup files. The backup is locked until your service provider can replicate the requested files to the media you requested.

To view the status of a disc/tape request:

1. On the **Restore** menu, point to **Disc/Tape**, and then click **Orders**. The following information is displayed:

Order ID	Unique sequential order number.
Backup Set	Backup set you requested to be burned to a disc or tape.
Time Issued	Time the request was made.
Status	Latest status message from the DS-System): • **Purchased** - The disc/tape order has been submitted to the DS-System. • **Finished** - The disc/tape order has been written to the requested media by the DS-System. • **Mailed** - The disc/tape has been mailed.
Media	Number of discs/tapes that will be sent.
Type	Media type you have selected.
Options	Indicates if the request is for a: • Snapshot - the latest generation of all files in the backup • Selective Restore - customized request for specific files / folders
Files Failed	Number (if any) of files that were not successfully processed.

2. To update the list, click **Refresh**.
3. Click **Close**.

11.2.3 Restoring from a disc/tape backup

After the disc/tape media has been delivered or downloaded, you can restore from it at your convenience.

To restore from a disc/tape backup:

1. On the **Restore** menu, point to **Disc/Tape**, and then click **Restore from**.
2. Beside the **Computer** box, click **>>**, and then select the computer.
3. Beside the **Directory** box, click **>>**, and then select the directory.
4. In the **Encryption key** box, type or import the alphanumeric key of up to 32 characters for the encryption key.
5. Click **OK**.

11.3 Backup Lifecycle Management (BLM)

The Backup Lifecycle Management (BLM) Module works with DS-Client, DS-System, and a BLM Archiver to extend the options for your backed up data. Data stored in the BLM Archiver is billed on a different scale as compared to the online (DS-System) data.

Restore from BLM is a feature that allows you to restore data from the BLM Archiver if you have data that has been previously sent to the BLM Archiver via a BLM request.

Data stored by the BLM Archiver is accumulated into archive packages. An additional step is to create a restorable image of the archive data that is readable by the DS-Client. Each restorable image represents data from a single backup though it can contain multiple generations of files.

NOTE: If the BLM Module is enabled for the DS-Client, an additional Time-Push feature is available for retention. See Chapter 4, “Working with retention rules”.

11.3.1 Configuring a backup for BLM

Backup sets are configured to save a specific number of generations. After a backup item reaches this number of generations, the oldest will be overwritten with each new generation backed up.

When you configure a backup for BLM, DS-Client will instruct DS-System to send a copy of the oldest generation (that is about to be overwritten) to the BLM Archiver.

To configure a backup for BLM:

1. Click the **Backup Sets** tab.
2. Right-click the backup you want to configure for BLM, and then select **Properties**.
3. Click the Options tab.
4. Select the **BLM (Infinite Generations)** check box.
5. Click **OK**.

11.3.2 Performing an on-demand BLM request

You can perform an on demand BLM Request for any existing backup with backed up data online. The backup does not have to be configured with the BLM (Infinite Generations) option. BLM Requests can be performed as follows:

- According to schedule from DS-Client
- On demand from DS-Client

NOTE: An alternative is to contact your service provider and have them perform the BLM Request from the DS-System side on demand.

To perform an on-demand BLM request:

1. Click the **Backup Sets** tab.
2. Select the backup on which you want to perform an on-demand BLM request.
3. On the **Backup** menu, click **BLM Request**.
4. Select the backup items you want to copy to the BLM archive, and then click **Next**.
5. Do the following:

a) In the **Archive Label** box, type a label for the archive package.

b) To use a new archive package, select the **Close archive packages** check box, and then specify when the archive package will be closed. Once an archive package is closed, no new data will be added. Subsequent archiving requests will create a new archive package.

c) To allow the archive package to contain references to older archive packages, select the **Reference previous archive package(s)** check box. This can save space by removing data redundancy.

d) Under **Generations to include**, specify if you want the archive package to contain the latest generation or all generations of the items selected.

e) Click **Finish**.

11.3.3 Configuring a BLM schedule

You can create a new BLM schedule or edit an existing schedule by adding a detail to copy files to BLM.

To configure a BLM schedule:

1. Click the **Backup Schedules** tab.
2. Select the schedule you want to configure.
3. On the **Schedule** menu, click **Edit Schedule**.
4. Under **Tasks**, select the **4. Perform BLM** check box.

NOTE: For more information, see Section 3.1, “Configuring a schedule”, on page 90.

To schedule a backup for BLM:

You can assign a BLM schedule to the required backup. The backup does not have to be configured with the BLM (Infinite Generations) option.

1. Click the **Backup Sets** tab.
2. Select the backup you want to configure.
3. On the **Sets** menu, point to **Backup Sets**, and then click **Properties**.
4. Click the **Schedule** tab.
5. Select a **Schedule**, and then click **OK**.

11.3.4 Restoring from the BLM Archiver

Once data has been sent to BLM Archiver, you can request to have any generation in the archive written to media and shipped to you. Restoring data from the BLM Archiver requires the following steps:

1. Obtain a BLM restorable image of the archived data you want to restore. There are two ways to do so:
   - If you have installed DS-NOC, you can create a BLM restorable image of your archived data and download the image via DS-NOC. Before you can create a BLM restorable image via DS-NOC, you must do the following:
     - Ensure the required BLM Archiver has been added to DS-NOC.
     - The **Restorable Image Save Path** specified in DS-NOC is a legitimate and available path on the BLM Archiver machine.

     For detailed instructions on how to add a new BLM Archiver and how to access restorable images for data recovery, see the *DS-NOC User Guide*.
   - You can obtain a BLM restorable image of your archived data from your service provider or backup administrator. Your service provider or backup administrator can then create a BLM restorable image of your requested data and deliver the image to you in a way that allows you to make the image accessible to DS-Client.
2. Retrieve the data in the BLM restorable image. For more information, see Section 11.2.3, “Restoring from a disc/tape backup”, on page 624.

11.3.5 Converting from tape to BLM

For Windows DS-Clients, you can convert data from tape backups into BLM format archive packages. These archive packages can then be sent to your service provider to import to the BLM Archiver for off-site storage.

To convert from tape to BLM, ensure the following requirements are met:

- The tape drive must be directly connected to the DS-Client computer.
- The tape format must be MTF (Microsoft Tape Format).

NOTE: Special operating system backups that were created using the tape backup utility (e.g. System State) are not restorable.

To convert from tape to BLM:

1. Load the tape(s) that you want to convert.
2. On the **Initial Backup** menu, click **Tape Conversion to BLM**. The tape converter automatically counts how many physical tapes are in the drives. Initially, all tapes appear under Unidentified Tapes.

1. To change a tape, open the tape drive door, and take a tape out from its slot.
2. Close the tape drive door. Allow Windows to perform its inventory so the removed tape will be marked as offline.
3. Open the tape drive door again and put the new tape in the empty slot.
4. Close the tape drive door. Windows will identify the new tape.
5. After Windows identifies the tape, click **Refresh** to update the DS-Client's list from the tape library's memory. After a Tape has been identified, all the backups on that tape appear in the list.

NOTE: You can only convert from a tape that has been identified.

---

6. Do the following:
   a) To scan a tape for information about the backup data on the tape, select the tape, and then click **Identify Tape**.
   b) Select the level that you want to convert, and then click **Next**.
      - **Computer Name –** Converts all backups listed for that computer.
      - **Backup Set –** Converts the highlighted backup.
7. Select the data to convert, and then click **Next**. By default, the entire backup is selected.
8. Do the following:
   a) Under **Before Conversion**, if the tape is in MTF format, DS-Client can convert the data without entering any password(s).
   b) Under **After Conversion,** specify the location where DS-Client will save the archive package. Type a label for the BLM session and backup name to help you identify the archive package after it is imported to the BLM Archiver.
   a) Click **Next**.
9. Click **Finish**.

When the conversion is completed, the data in the target path can be shipped to your service provider to import to the BLM Archiver. After the data has been imported to the BLM Archiver, you can request Restorable Images. For more information, see Section 11.3.4, "Restoring from the BLM Archiver", on page 627.)

11.4 Local Storage Tool

The Local Storage Tool must be enabled by your service provider from the DS-System to allow the DS-Client to save backup data to a local disk or UNC path.

If a restore is required, the file can be quickly restored at LAN speed from the local environment without connecting through the IP WAN to DS-System.

NOTE: Local storage does not apply during the initial backup process. Any backups configured for local storage will ignore the setting until the initial backup is transferred to the DS-System online storage.

When a file in a backup configured with local storage is created or modified, the backup process sends it to both DS-System and the local storage. If a file was previously backed up on DS-System, but there is no copy of the file on the local storage (for example, it was backed up before the backup was marked for local storage), the backup process sends it only to local storage. If for some reason the file cannot be saved locally, it is still sent to the DS-System and an error is logged.

Local storage behaves differently for backups assigned to a retention rule:

- **Without Retention —** Local storage keeps a copy of the latest generation of the backup files (as well as online, offsite at the DS-System).
- **With Retention —** The same number of generations are backed up to local storage as are on DS-System. Ensure there is enough space in the Local Storage, and perform the “Enforce Retention” process regularly. For more information, see Chapter 11, “Using premium backup and recovery services”.

NOTE: In both cases, when a new backup session occurs and an existing generation of a file is replaced by a new one, the old generation of the file is deleted after the new one is saved on the local storage. This means there must be enough free space on the local storage to accommodate both generations.

By default, DS-Client tries to restore from local storage first. For missing files or older generations, DS-Client retrieves them from DS-System online storage.

The local storage cache is an option that you can configure for a backup to define a disk location for the temporary storage of backup data if the connection to DS-System is lost while a backup is in progress and all configured retries fail. Once DS-Client reestablishes the connection, it sends the data in the local storage cache to the DS-System.

When sending data to the local storage cache, DS-Client processes the data from the source and saves the data as a full backup in a compressed and encrypted format on the local storage cache. If the connection from DS-Client to the DS-System is maintained throughout the entire backup activity, the local storage cache is not used.

IMPORTANT: By default, the local storage cache location is the same as the local storage path. Whatever path you select, ensure it has sufficient capacity to store the backup data. When used, the local storage cache supports the total amount of data that needs to be master processed and backed up in a compressed and encrypted format for a backup.

11.4.1 Local storage vs local storage cache

By default, local storage and the local storage cache use the same default storage location as defined in Section 11.4.2, “Setting the default local storage path”, on page 632.

However, local storage and the local storage cache have the following differences:

Function	Local Storage	Local Storage Cache
Used when	Data is to be kept locally and online.	Connection to DS-System is not available.
DS-System connection	Yes	No
Types of generations	Regular	Master and delta pointers
Number of generations	Up to 30 days	Infinite
Common file elimination	No	No
Compression	Yes	Yes
Restore	Yes	No

Data is sent to the local storage location at the same time the data is processed by DS-Client to be sent to the DS-System. Data is sent to the local storage cache only when the connection to the DS-System is not available.

By default, data is saved in the local storage as regular generations in compressed format, but is not encrypted. Data is saved in the local storage cache as a master generation that includes additional information that determines which blocks of data from within that file are required for delta generations. When the connection between the DS-Client and DS-System is reestablished, DS-Client moves the required files from the local storage based on the backup configuration in the format they were stored in the local storage cache (encrypted and compressed) and sends only delta generations to DS-System. As a result, DS-Client can still process master/delta (Incremental forever) generations when performing backup using the Local Storage Cache option. Similarly, the local storage can include encrypted as well as unencrypted data, depending on when the files were

processed during a particular backup activity. Files are released from the local storage cache one-by-one as their successful transmission to the DS-System is confirmed between DS-System and DS-Client.

The configured number of generations for the items in a backup does not take effect when data is sent to the local storage cache. For example, a backup is configured to store a maximum of three generations of data on the DS-System Online Storage. It can store more than three generations of data in the Local Storage Cache if DS-System is unavailable and/or DS-Client did not finish moving the data from the Local Storage Cache to the DS-System. All generations will be sent to DS-System whenever possible as regular generations or Master/Delta generations and DS-System processes them as it would process any generations sent directly to it (e.g. it will mark generations as recycled when required, it will trigger reconstruction when required, etc.). By default, the Local Storage will store the latest generation of all the files processed for a backup. However, if Local Storage Retention is enabled and assigned to a backup with Local Storage Options enabled, DS-Client will store all generations that meet the criteria specified in the Local Storage Retention rules in the Local Storage.

DS-Client can restore data directly from the local storage and can connect to DS-System to retrieve only data that does not exist in the Local Storage (configure this behavior from the Restore Wizard, before triggering the restore activity). Data from the Local Storage Cache cannot be restored until it has been transferred to DS-System.

DS-Client performs basic checks to ensure the validity of the files from the local storage cache on transfer to DS-System. If DS-Client determines that a file is corrupt, it removes the file information from the DS-Client database and determines if the files needs to be backed up again in the next backup session.

If a backup is marked as out-of-sync and DS-Client cannot connect to DS-System to perform synchronization, then DS-Client cannot run backup to the local storage cache. DS-Client administrators must ensure that sufficient local storage disk space is available to accommodate all data in the local storage or local storage cache for all the configured backups. If data exists in the local storage cache for a selected backup, that data must first be transferred to DS-System, and only afterwards can DS-Client perform subsequent backups for that backup directly to DS-System. Suspending a backup configured with the local storage cache will not allow the local storage cache copy process to be triggered and to connect to DS-System to move the data.

11.4.2 Setting the default local storage path

By default, the default local storage path is not configured. This means none of the local storage options are available. Once configured, **Save on Local Storage** appears in the New Backup Set Wizard and **Use Local Storage** appears on the Options tab in the Backup Set Properties dialog box.

To set the default local storage path:

1. On the **Setup** menu, click **Configuration**.
2. In the **DS-Client Configuration** dialog box, click **Parameters**.
3. In the **Local Storage Path** box, type the default path to use.

NOTE: Ensure that the DS-Client service account has read/write access to the local storage path.

---

4. Click **OK**.

11.4.3 Configuring a backup with local storage

Once the local storage path is configured, the next backup session sends data to local storage.

To configure a backup with local storage:

1. Click the **Backup Sets** tab.
2. Select the backup that you want to configure with local storage.
3. On the **Sets** menu, point to **Backup Sets**, and then click **Properties**.
4. Click the **Options** tab.

NOTE: For new backups, this feature is activated on the Choose the name for this backup page of the Backup Set Wizard.

---

5. Beside **Use Local Storage**, select the **Save** check box. By default, the backup will use the default local storage path defined in Section 11.4.2, “Setting the default local storage path”, on page 632.
6. To specify a different local storage path for the backup, click **>>**. In the **Path** box, type a different patch, and then click **OK**.
7. Click **OK**.

11.4.4 Configuring a backup to use the local storage cache

The local storage cache extends the capability of the local storage (local attached disk or UNC path) to provide a cache if the connection between the DS-Client and DS-System is interrupted during a backup session. This lowers the chances of missing a backup session. Data accumulates in the local storage cache until the DS-Client reestablishes the connection to DS-System.

For backups using this option, the DS-Client sends data to the local storage cache in the following situations:

- The connection between the DS-Client and DS-System is lost during a backup activity and the connection cannot be reestablished after the configured number of retries. To change the number of retries, configure the **Attempt to reconnect** settings. For more information, see Section 2.1.5, “Configuring the parameter settings”, on page 30.
- DS-Client cannot establish a connection with DS-System for a scheduled or on-demand backup activity.
- The backup activity is stopped from the DS-System-side and the DS-Client fails to reconnect to DS-System based on the configured number of retries.
- (Windows DS-Client only) The backup activity starts and data still exists in the local storage cache for the backup.

If a DS-Client tries to connect to a DS-System and cannot establish the connection, DS-Client will process the data and save it in the local storage cache. Once DS-Client can reconnect to the DS-System, it triggers a local storage cache copy process to send to the DS-System each generation of the required files in the required format (master / delta / regular). For interrupted backups, the DS-Client runs a synchronization activity and then proceeds with the local storage cache copy process.

NOTE: DS-System considers the local storage cache copy process to be a backup activity and applies the same priority and backup locking rules to it.

To configure a backup to use the local storage cache:

1. Click the **Backup Sets** tab.
2. Select the backup to which you want to use the local storage cache.
3. On the **Sets** menu, point to **Backup Sets**, and then click **Properties**.
4. Click the **Options** tab.

5. Beside **Use Local Storage**, select the **Cache** check box. By default, the backup will use the default local storage path set in Section 11.4.2, “Setting the default local storage path”, on page 632.

NOTE: When creating a new backup, you select the **Transmission cache on Local Storage** check box on the Choose the name for this backup page in the Backup Set Wizard.

---

6. To specify a different local storage path for this specific backup, click the **[>>]** button. Data that is cached by this feature is saved in this local storage path in a sub-folder called `\Cache`.
7. Click **OK**.

11.5 Multitenant DS-Clients

The multitenant feature allows you to assign a backup to a specific customer when creating a new backup or updating the properties of an existing backup. When you assign a backup to a customer, the backup is displayed under the customer name in the backups tree.

By default, administrators and backup operators have access to all existing customers in DS-Client and can assign backups to these customers as required. Regular users only have access to customers within their own group or to customers who have been assigned to them by an administrator.

11.5.1 Activating the multitenant feature

To use the multitenant functionality, you must enable the multitenant feature. Only an administrator can enable the multitenant feature.

To activate the multitenant feature:

1. Click **Setup** menu, click **Configuration**.
2. Click the **Advanced** tab.
3. In the **Category** box, select **Miscellaneous**.
4. In the **Parameter** box, select **Multitenant**.
5. In the **Value** box, select **Yes**.
6. Click **OK**.

DS-Client enters multitenant mode. Existing backups that have not been categorized under any customer are displayed under Unspecified Customer.

11.5.2 Configuring a multitenant DS-Client

To use the multitenant feature, you must configure customers and assign the customers to a user or group.

NOTE: The users and groups to which you want to assign customers must already exist on the DS-Client machine and must have been configured in DS-Client. For more information, see Section 2.1.7, “Configuring the user and group settings”, on page 35.

To configure the multitenant feature:

1. On the **Setup** menu, click **multitenant**.
2. Under **Customers**, do the following:
   a) To add a customer, click **Add**. To edit a customer, select the customer, and then click **Modify**.

   NOTE: To delete a customer, select the customer, and then click **Delete**.

   b) In the **Name** box, type a name for the customer.
   c) In the **Contact** box, type the name of the contact person associated with this customer.
   d) In the **Address** box, type the mailing address of the customer.
   e) In the **Note** box, type any additional information about the customer.
   f) Click **OK**.
3. Under **Users & Groups**, do the following:
   a) To assign a user or group to a customer, click **Add**. To edit a user or group assignment, select the user or group, and then click **Modify**.

   NOTE: To delete a user or group, select the user or group, and then click **Delete**.

   b) In the **Name** list, select a user or group.
   c) In the **Customer** list, select the customer that you want to assign to the user or group.
   d) In the **Note** box, type any additional information about the user or group.
   e) Click **OK**.
4. Click **Close**.

11.6 Snapshot Manager (Linux)

The Snapshot Manager feature integrates the DS-User with storage volumes to manage their native SnapVault feature. You can use the DS-User to transfer volumes\qtrees to another volume without having to use the scripting required by native storage management software. DS-Client does not process any data from the storage.

NOTE: Your service provider must enable the Snapshot Manager feature from DS-System.

To use the Snapshot Manager feature, you must have the following:

- SnapVault ONTAP Primary license for the source NetApp storage,
- SnapVault ONTAP Secondary license for the destination NetApp storage.

NOTE: If the source and the destination volumes are on the same filer, then the two licenses are required on the same filer.

The initial transfer from source to destination is triggered immediately after the snapshot transfer is created. Each subsequent scheduled or on-demand transfer performs an incremental transfer (only the changes since the last update, as determined by the storage's management software). After completion of each scheduled or on-demand data transfer, a new snapshot is created for the destination volume. After the new snapshot is created on the destination volume, the Snapshot Retention policy is applied to the volume's snapshots.

11.6.1 Configuring a storage device

The DS-Client must be configured to connect to each storage device that will be used for a snapshot transfer. The storage device must be running and be accessible by the DS-Client.

To configure storage device:

1. On the **Snapshot Manager** menu, click **Register Storage**.
2. Do one of the following:
   - To add a storage device, click **New**.
   - To edit a storage device, select the device, and then click **Edit**.

   NOTE: To delete a storage device, select the device, and then click **Delete**.

3. In the **New / Edit Storage** dialog box, do the following:
   a) In the **Vendor** box, select the storage device type. Only NetApp is currently supported.
   b) In the **Name** box, type a name for the storage device.
   c) In the **Address** box, type the IP address of the storage device.
   d) In the **Port** box, enter the port number for accessing the API. The port must be open on the storage device.
   e) In the **User Name** box, type the name of a user on the storage device who has permission to execute the API commands on the storage device.
   f) In the **Password** box, type the password for the user on the storage device.
   g) To use the HTTPS protocol to access the API, select the **Use HTTPS Protocol** check box. The protocol must be enabled on the storage device.
   h) Click **OK**.
4. Click **Close**.

11.6.2 Configuring a snapshot retention policy

You can configure the retention policies the DS-Client can apply to the snapshots taken by the Snapshot Manager. Each configured snapshot transfer can be assigned to one retention policy. A retention policy is applied at the volume level so that all snapshot transfers for the same volume have the same retention policy.

IMPORTANT: Once retention is enforced, deleted snapshots cannot be restored.

To configure a snapshot retention policy:

1. On the **Snapshot Manager** menu, click **Snapshot Retention**.
2. Do one of the following:
   - To add a retention policy, click **New**.
   - To edit a retention policy, select the policy, and then click **Edit**.

   NOTE: To delete a retention policy, select the policy, and then click **Delete**.

3. In the **New / Edit Snapshot Retention** dialog box, do the following:
   a) In the **Name** box, type a name for the retention policy.
   b) In the **Latest** box, enter the number of the most recent snapshots you want to retain.
   c) In the **Hourly** box, enter the number of hours you want to retain snapshots, and then specify if you want to retain snapshots closest to the beginning or end of hour.
   d) In the **Daily** box, enter the number of days you want to retain snapshots, and then specify if you want to retain snapshots closest to the beginning or end of the day.
   e) In the **Weekly** box, enter the number of weeks you want to retain snapshots, and then specify if you want to retain snapshots closest to the beginning or end of the week.
   f) In the **Monthly** box, enter the number of months you want to retain snapshots, and then specify if you want to retain snapshots closest to the beginning or end of the month.
   g) In the **Yearly** box, enter the number of years you want to retain snapshots, and then specify if you want to retain snapshots closest to the beginning or end of the year.
   h) Click **OK**.
4. Click **Close**.

11.6.3 Configuring a snapshot schedule

You can configure the schedules the DS-Client can use for snapshot transfer. Each configured snapshot transfer can be assigned to one snapshot schedule. A schedule is applied at volume level so that all snapshot transfers for the same volume have the same schedule.

To configure a snapshot schedule:

1. On the **Snapshot Manager** menu, click **Snapshot Schedule**.
2. Do one of the following:
   - To add a snapshot schedule, click **New**.
   - To edit a snapshot schedule, select the schedule, and then click **Edit**.

   NOTE: To delete a snapshot schedule, select the schedule, and then click **Delete**.

3. In the **New / Edit Snapshot Schedule** dialog box, do the following:
   a) In the **Name** box, type a name for the snapshot schedule.
   b) On the **Weekdays** tab, select the days of the week that you want the schedule to run.
   c) On the **AM** tab, select the hours in the morning that you want the schedule to run.
   d) On the **PM** tab, select the hours in the afternoon and evening that you want the schedule to run.
   e) Click **OK**.
4. Click **Close**.

11.6.4 Configuring a snapshot transfer

The initial data transfer is run from the source storage device to the destination storage device. After the data is transferred, a snapshot is created.

Each subsequent transfer that is run transfers any missing data (the differential) from the source to the destination so that both have the same data. After the data transfer is complete, a snapshot is created to record the state of the data.

To configure a snapshot transfer:

1. On the **Snapshot Manager** menu, click **Snapshot Transfer**.
2. Click **Snapshot Transfer Setup**.
3. Select the source storage device from which the data will be read, and then click **Next**.

NOTE: To configure a storage device, click **[...]**. For more information, see Section 11.6.1, “Configuring a storage device”, on page 637.

---

4. Select the volume or qtree on the source storage device that will be protected, and then click **Next**.

NOTE: Although all existing volume/qtrees appear in the list, you cannot select a replicated qtree or volume containing a replicated qtree as the source.

---

5. Select the destination storage device where the data will be copied, and then click **Next**.

NOTE: To configure a storage device, click **[...]**. For more information, see Section 11.6.1, “Configuring a storage device”, on page 637.

---

6. Select the volume on the destination storage device where the data will be copied, and then click **Next**.
7. Select a snapshot retention policy for the destination volume, and then click **Next**.

NOTE: To configure a retention policy, click **[...]**. For more information, see Section 11.6.2, “Configuring a snapshot retention policy”, on page 638.

---

8. Select a snapshot schedule for the destination volume, and then click **Next**.

NOTE: To configure a snapshot schedule, click **[...]**. For more information, see Section 11.6.3, “Configuring a snapshot schedule”, on page 639.

9. Type a name for the snapshot transfer. Configure the bandwidth throttle and type a description.
10. Click **Finish**.

11.6.5 Restoring a snapshot transfer

You can restore a snapshot from a snapshot transfer to a new volume on the same or a different storage device.

To restore a snapshot transfer:

1. On the **Snapshot Manager** menu, click **Snapshot Transfer**.
2. Right-click the snapshot transfer containing the snapshot you want to restore, and then click **Restore**.
3. Select the snapshot you want to restore, and then click **Next**.
4. Select the destination storage device from which you want to restore the snapshot, and then click **Next**.

NOTE: To configure a storage device, click **[...]**. For more information, see Section 11.6.1, “Configuring a storage device”, on page 637.

5. Select the volume on the destination storage device from which you want to restore, and then click **Next**.
6. Select the destination qtree. You can also type a new qtree name to create it.
7. Specify a bandwidth throttle limit for the storage device.
8. Click **Finish**.

11.6.6 Deactivating a snapshot transfer

You can deactivate a snapshot transfer to stop any new incremental data transfers. You can still perform restores from a deactivated snapshot transfer because all snapshots in the destination remain even when deactivated.

To deactivate a snapshot transfer:

1. On the **Snapshot Manager** menu, click **Snapshot Transfer**.
2. Right-click the snapshot transfer you want to deactivate, and then click **Deactivate**.
3. When the system prompts you to confirm that you want to deactivate the snapshot transfer, click **Yes**.

11.6.7 Reactivating a snapshot transfer

When a snapshot transfer has been deactivated, the mapping from the source to the destination is broken. If you choose to reactivate a snapshot transfer, you must remap the source. To do this, you must select a source that contains at least one common snapshot that exists on the destination volume/qtree.

The storage device automatically selects the latest common snapshot between the source and destination to synchronize and use for the differentials on subsequent snapshot transfers.

To reactivate a snapshot transfer:

1. On the **Snapshot Manager** menu, click **Snapshot Transfer**.
2. Right-click the snapshot transfer you want to reactivate, and then click **Re-activate**.
3. Select the source storage device containing the snapshot transfer you want to reactivate, and then click **Next**.
4. Select the volume or qtree on the source storage device, and then click **Next**.
5. Specify a bandwidth throttle limit for the storage device and type a description.
6. Click **Finish**.

12 Using LAN Storage Discovery Tool

You can use the LAN Storage Discovery Tool to analyze your storage by scanning the shares on your network. This is useful to identify duplicate files on the network or shares that are contained within other shares. LAN Storage Discovery reports can be generated using the information from the file summary.

Analyzing your LAN storage before performing the initial backup is important to provide a clear view of the data on your network. The most important information is the redundancy (duplication) and frequency of data changes.

To analyze your LAN, you must first discover the shares using a list of credentials you provide and then select the share list you want to scan. Tools to manage and monitor the discovery and scan processes are also provided.

The scan process is run by the DS-Client and can be scheduled. You can generate several reports to analyze the scanned information for duplication, data growth trends, file access, and file type distribution. You can also generate summary and detailed reports as well as export the reports to a file.

12.1 LAN Storage Discovery best practices

The LAN Storage Discovery process can be resource intensive because DS-Client must connect to each target share, read the files in the share, and prepare a signature for each file to report on common files, largest file sizes, file types, etc. Consider the following when using the LAN Storage Discovery Tool:

- Use a Windows DS-Client to scan a Windows network and a Linux client to scan a Linux network.
- Schedule the LAN Discovery process to run after business hours and set an end time so that it does not interfere with your network or users.

  Shares that have been recently scanned will not be in priority sequence. Only shares that have not been scanned will receive priority for the scanning process when the schedule is triggered again.
- Create a special Domain Administrator account that can access all the shares that must be scanned. This will simplify the credentials configuration required on the DS-Client and reduce the potential for connection errors during the LAN Discovery process.

  If using a Domain Administrator account is not an option, you can create the same local Administrator account on each server that will be scanned.
- After the share discovery process completes, a share list is displayed that can contain duplicate shares, which are shares that are included in other shares. Disable the duplicate shares because you do not need to scan the files twice.
- Ignoring small files can reduce the network load and the total time required for the scan process.

- Adjust the number of threads used to scan shares. If the number is high, the network will be busier. However, the total time for the scan process will be less than if the number of threads is smaller.

NOTE: During a scan process, the network and I/O of the scanned machines and the DS-Client database server will normally remain under a constant heavy load.

12.2 Scanning for shares on the LAN

The first step in the LAN Storage Discovery process is to scan your LAN for available shares. You must configure the range of your network that will be analyzed. The range can include a network provider, domain, or computer. A list of credentials can also be provided for the process.

If the shared path can be retrieved, the discovery process automatically analyzes the overlapping of shares. By default, overlapped shares will be disabled for scanning to avoid false duplication counting.

LAN Storage Discovery on Windows DS-Client supports the following:

- Microsoft Windows Network
- NetWare Services
- NFS

LAN Storage Discovery on Linux and Mac DS-Clients supports the following:

- NAS
- NFS
- SSH

NOTE: Soft links and device files will be silently skipped. Hard links will be treated as regular files. If two hard links point to the same file, they will be considered as duplicates of each other.

To scan for shares on the LAN:

1. On the **Tools** menu, point to **LAN Storage Discovery**, and then click **Share Discovery**.
2. Do the following:

a) In the **Path** box, type the IP address or name of the computer on your network that you want to discover.

NOTE: For Linux or Mac DS-Clients, you must include the connection protocol before the IP address or computer name. For example, `UNIX-SSH\10.123.45.6` or `UNIX-SSH\localhost`).

---

b) For Linux DS-Clients, once the protocol is specified, the following options are available depending on the network protocol selected:

- **Ask for credentials** – Prompts you to type a valid user name and password for the selected network resource.
- **Ask For NAS API credentials** (NAS only) – Prompts you to type valid connection information for the selected NAS protocol.
- **sudo as an alternate user** (UNIX-SSH only) – Shows the credentials that the DS-Client will use to access data on the network resource. After successful login to the remote source, sudo will be performed to use these credentials.
- **Advanced Connection Option** (UNIX-SSH only) – This is the default for the DS-Client to run a PERL script. To edit the settings, click **[...]**, and then type the path to the script language on the target computer.

c) In the **Filter** box, type the filter you want to apply to the list of items in the network tree. For example, you can enter the first letters of the computer name you want. This feature does not support wild card characters.

NOTE: To select all the filtered shares that meet the criteria, select the **Select All Filtered** check box.

---

d) To add an item to the scan, select the item, and then click **Add**.

e) For large scan lists, it can be faster to import from a text file. To import a list of items from a text file, do the following:

1. Prepare a text file with a simple list of computer IP addresses / names on separate lines.
2. Click **Import** and browse for the text file. When you open the file, the DS-Client will ping each address in the list and check the connectivity. You can skip or include all the addresses that failed to respond.

f) To remove a item from the discovery list, select the item, and then click **Remove**.

g) To remove any previously scanned shares with a scanned size of 0, select the **Clean share list** check box.

h) Click **Next**.

3. Do the following:

   a) To add credentials for the LAN share discovery process, click **Add**.

   b) To edit credentials, select the credentials, and then click **Modify**.

   NOTE: To delete credentials, select the credentials, and then click **Delete**.

   c) In the **Connect as** box, type the user name

   d) In the **Password** box, type the password.

   e) In the **From** box, if applicable select the computer where the DS-Client will verify your credentials. Normally this will be the same as the server that you are connecting to. However if the computer running DS-Client is a member of a domain, you can select from the available list of domains.

   f) In the **Priority** box, enter the priority for the credentials that the DS-Client will use to attempt to scan the shares. The lower the number, the higher the priority.

   g) Click **OK**.

   h) If you have already scanned the LAN, each scanned share has been assigned the best suited credentials. To overwrite these credentials, select the **Overwrite existing share credentials** check box.

   i) Click **Finish**.

12.3 Configuring scanned shares

After you run a share discovery process, a share list is generated with the credentials to connect to each share. Discovered shares are automatically enabled or disabled depending on if they are already included in other shares or if a connection cannot be established. Each subsequent share discovery process adds new shares to the discovered share list. You can manually remove specific shares.

NOTE: The **Clean shares list** option applies only to shares with a scanned size of 0 from the last scan shares process.

The scan process is applied to the list of shares found by the discovery process, which automatically disables shares in the following scenarios:

- The share is covered by other shares.
- There are not enough credentials to retrieve the information from the share.
- The share is not supposed to be scanned (e.g. read-only media such as DVD).

NOTE: You can manually enable or disable the status of a share.

By default, the credentials used to discover the share are set as the scan credentials for the share by the discovery process. However, the credentials used for scanning can be changed for shares from DS-User.

To speed up the scanning process, you can configure the system to skip files that are smaller than a specific size. The number of scanning threads is also configurable to provide scalability.

The scan process can be scheduled or started on demand. The best practice is to schedule it to run several times over a period, such as a few weeks, to get more accurate statistical information on data growth and changes. This helps with the estimation of storage and other requirements before going into production.

To configure scanned shares:

1. On the **Tools** menu, point to **LAN Storage Discovery**, and then click **Scan Shares**.
2. To display the shares on the LAN that were discovered by the share discovery process, click **Share List**, and then do the following:
   a) To allow share to be scanned, select the share, and then click **Enable**.
   b) To remove a share from the list, click **Remove**.

c) To remove a share from the scan process, select the share, and then click **Disable**.

NOTE: The share discovery process automatically disables shares that it detects to be redundant or inaccessible.

d) To configure the reparse point settings for a share, select the share, click **Follow Reparse Point**, and then select one of the following options:

- **Follow** – Follows reparse points in a scanned share. A reparse point is a link to a different location (directory or device). This results in a larger amount scanned.
- **Don't follow** – Ignores reparse points in a scanned share.
- **Reverse follow setting** – Inverts the share setting.

e) Click **Close**.

3. To skip files smaller than a specified size, select the **Skip files smaller than** check box, and then specify the size of the files to be skipped.
4. To remove files smaller than the specified size from the database, select the **Delete scanned files from DB** check box.
5. In the **Threads** box, enter the number of the threads to use for the scan.
6. Click **Scan**.

NOTE: The first scan processes all shares. In subsequent scans, you can enable or disable shares. For example, if you want to do a quick scan of only one share.

12.4 Monitoring scanned shares

The Scan Monitor displays real-time information about scanned shares on the LAN.

To monitor scanned shares:

1. On the **Tools** menu, point to **LAN Storage Discovery**, and then click **Scan Monitor**.
2. To display all disabled shares, select the **Show disabled shares** check box.
3. In the **Refresh every... seconds** box, enter the refresh interval.
4. To update the results, click **Refresh**.
5. Click **Close**.

12.5 Generating a LAN File Summary Report

A LAN File Summary Report displays a list of the scanned files on the network. Filters are available so you can analyze a particular group of files. This is useful for identifying changed or duplicate files.

To generate a LAN File Summary Report:

1. On the **Tools** menu, point to **LAN Storage Discovery**, and then click **LAN File Summary**.

1. On the **Reports** menu, click **Online File Summary**.

2. To filter the results, do the following:

   a) In the **Filter** box, type the filter you want to apply to the report. For example, you can search for files that match a specific pattern (e.g. *.doc).

   b) In the **Category** box, select the category of files you want to display in the report. The options are as follows:

   - **All** – Displays all category of files.
   - **All files** - Displays all files.
   - **Duplicate files** - Displays files that have more than one copy, minus one for each unique common file group.
   - **Duplicate groups** - Displays unique common file groups. All identical files are members of a unique file group.
   - **Changed and new files** - Displays files that are new or have changed from the start of the search period.
   - **Unchanged files** - Displays files that have not changed since the start of the search period.
   - **Not accessed files** - Displays files that have not been accessed since the start of the search period.

   c) In the **Duplication** box, enter the number of duplicate files that must exist.

   d) To display only the totals, select the **Totals only** check box.

   e) In the **Share/Set** box, specify the specific shares on the LAN that you want to search.

3. Click **Find**. The following information is displayed:

Column	Description
Category	Category of files.
Files	Number of files.
Files (%)	Percentage of the total number of files.
Size (MB)	Size of the files.
Size (%)	Percentage of the total size.

4. In the **Last** box, enter the last number of days for which you want to display information.
5. To view detailed information about a row, select the row, and then click **Detail**. Each line represents a unique file. If more than one copy exists, the duplication amount is indicated in that column. Do the following:
   a) To view duplicate instances of a specific file, click **Show Duplicates**. You should monitor backup sets to ensure duplication is considered.
   b) Click **Close**.

NOTE: A maximum of 50,000 files can be displayed. If the scan returns more than this number, the results are sectioned.

---

6. To view a pie chart of a row, select the row, click **Chart**, and then do the following:
   a) In the **View type** box, select the category you want to view.
   b) Select whether you want to view the information by files or by size.
   c) Click **Close**.
7. Click **Close**.

12.6 Generating an Access Report

An Access Report displays a list of the scanned files on the network based on the time they were last accessed. The report is based on a specified interval (days, weeks, months, or years).

To view the Access Report:

1. On the **Tools** menu, point to **LAN Storage Discovery**, and then click **Access**.
2. To specify a report interval, click **New Report**., and then do the following:
   a) Click **Add**.
   b) Select the color that you want to view in the graph for the report.
   c) In the **Modified Time** box, enter a report interval.

NOTE: To remove a report interval, select the interval, and then click **Remove**.

---

   d) In the **Share** box, specify if you want to view all shares or a specific share.
   e) Click **OK**.

3. To view the report by size, select **View by size**.
4. To view the report by number of files, select **View by number of files**.
5. Click **Close**.

12.7 Generating an Extensions Report

An Extensions Report displays a list of the scanned files on the network based on the extension. The Top Report displays the top file extensions. The Customized Report displays a list of specific file extensions.

To view the Extensions Report:

1. On the **Tools** menu, point to **LAN Storage Discovery**, and then click **Extensions**.
2. To search for the most frequent file extensions, do the following:
   a) Click **Top Report**.
   b) In the **Select top** box, enter the number of the top file extensions you want to view.
   c) To view the largest file extensions, select **With greatest size**.
   d) To view the most frequent file extensions, select **With biggest count**.
   e) In the **Share** box, specify if you want to view all shares or a specific share.
   f) To include the total of all other files from the searched shares, select the **Include Total** check box.
   g) Click **OK**.
3. To search for selective file extensions, do the following:
   a) Click **Customize Report**.
   b) Click **Add**.
   c) Select the color that you want to view in the graph for the report.
   d) In the **Extensions** box, type the extension without a period (e.g. txt, exe, dll, pdf).
   e) To include items in the graph that represent the total of all other file extensions from the searched shares, select the **Include Other** check box.

   NOTE: To remove an extension, select the extension, and then click **Remove**.

   f) In the **Share** box, specify if you want to view all shares or a specific share.

g) Click **OK**.

4. To view the report by size, select **View by size**.
5. To view the report by number of files, select **View by number of files**.
6. Click **Close**.

12.8 Generating a File Size Report

A File Size Report displays a list of the largest scanned files on the network and allows you to search for duplicates.

To generate a File Size Report:

1. On the **Tools** menu, point to **LAN Storage Discovery**, and then click **Large Files**.
2. In the **Select Top** box, enter the number of the top largest files you want to view.
3. To search for the largest files that are duplicated, select the **Duplicated at least** check box, and then enter the number of times the file must be duplicated.
4. In the **Share** box, specify if you want to view all shares or a specific share.
5. Click **Find**.
6. Click **Close**.

12.9 Generating a Growth Report

A Growth Report displays a list of the scanned files on the network based on growth over time. The report displays the data patterns for the LAN or a specific share. You provide the period for analysis and the report displays the files and size for each interval that falls within the specified period.

To generate a Growth Report:

1. On the **Tools** menu, point to **LAN Storage Discovery**, and then click **Growth**.
2. In the **View** box, select the type of the report (bar chart, line chart, or table)
3. In the **From** box, specify the start date for the report.
4. In the **To** box, enter the end date for the report.
5. In the **Interval** box, enter the interval for the report.
6. In the **Share** box, specify if you want to view all shares or a specific share.
7. In the **Type** box, specify if you want to view the total or new files only.

8. Click **Find**.
9. Click **Close**.

12.10 Generating a Share Usage Report

A Share Usage Report displays a list of the scanned files on the network grouped by owner of the specified shares.

To generate a Share Usage Report:

1. On the **Tools** menu, point to **LAN Storage Discovery**, and then click **Share Usage**.
2. In the **Share** box, specify if you want to view all shares or a specific share.
3. Click **Find**.
4. Click **Close**.

12.11 Generating a Virtual Machines Summary Report

The Virtual Machines Summary Report displays a list of virtual machines in a VMware vCenter Server environment on your network.

To generate a Virtual Machines Summary Report:

1. On the **Tools** menu, point to **LAN Storage Discovery**, and then click **Virtual Summary Report**.
2. To scan a VMware vCenter Server:
   a) In the **VM Type** box, select **VMware**.
   b) In the **vCenter** box, type the IP address of the VMware vCenter Server that you want to scan.
   c) In the **User Name** and **Password** boxes, enter the credentials of a user with sufficient privileges on the VMware vCenter Server.
   d) Click **Discover Machines**.
3. To scan a Microsoft Hyper-V Server:
   a) In the VM Type box, select Hyper-V.
   b) In the Host box, type the IP address of the Microsoft Hyper-V Server that you want to scan.
   c) In the User Name and Password boxes, enter the credentials of a user with sufficient privileges on the Microsoft Hyper-V Server.
   d) Click Discover Machines.

4. To perform an additional scan to obtain more detailed information, select the virtual machines, and then click **Get Machine Properties**.

   NOTE: To select multiple virtual machines, use CTRL+SHIFT or click **Select All**.

5. To view the information in a report, click **Virtual Access Report**, and then do the following:

   a) To select time intervals for sorting the information, click **New Report**.

   a) Click **Add**.

   b) Select the color that you want to view in the graph for the report.

   c) In the **Modified Time** box, enter a report interval.

      NOTE: To remove a report interval, select the interval, and then click **Remove**.

   d) In the **Center / Host** box, specify if you want to view all virtual machines or only VMware vCenter Servers.

   e) Click **OK**.

6. Click **Close**.

12.12 Exporting reports

You can export generated reports in HTML and Excel format.

To export reports:

1. On the **Tools** menu, point to **LAN Storage Discovery**, and then click **Generate Reports**.

2. Select the report that you want to export. The report options are as follows:

Report	Description
Share Usage	Displays the total number and protected size of the files on the scanned shares, including duplicate files.
Largest Files	Displays the largest files on the scanned shares and the percentage size compared to the entire network.
Largest Duplicates	Displays the largest duplicate files on the scanned shares as well as the total size and number of duplicate files compared to the entire network.
Ownership (Windows only)	Displays the total number of files on the scanned shares owned by a specific user.

Report	Description
File Type Distribution	Displays the distribution of file types on the scanned shares, sorted by space or file number. For each file type, you can select the top largest files from the entire network.
Partition Size (Windows only)	Displays the total, free, and used disk space on each partition of the scanned machines.
Access Report / Dormant Files	Displays the total amount of data and files modified over a specified interval on the scanned shares.
Growth and Modified Files	Displays the number of files and size created or modified for each share over the specified period.
SQL Server Size (Windows only)	Displays how much space is allocated for the Microsoft SQL Server for each computer on the scanned shares.
Exchange Server Size (Windows only)	Displays all .edb and .pst files on the scanned shares, including their directory, file name, and size.
All Duplicate Files	Displays a list of duplicate files larger than a specified amount on the scanned shares. This report is not generated by default.

3. To specify the options that are applicable to a report, click the report, and then make your selections on the right.
4. To place a copy of the exported reports in a ZIP file that can be uploaded to the DS-NOC, select **Package all reports for DS-NOC when generating reports**.
5. To export the selected reports, click **Generate**.
6. When prompted, select the location on the network for saving the reports.
7. To view the exported reports, go to the export location, and then click **index.html**

13 Using Unprotected LAN Resource Discovery Tool

You can use the Unprotected LAN Resource Discovery Tool to scan shares on your LAN and generate a list of nodes or shares that are not currently part of any backup on the DS-Client.

NOTE: A scan can only detect unprotected resources for the current DS-Client.

13.1 Scanning for unprotected LAN resources

You can scan for unprotected resources or shares on your LAN. After completion, a list of the shares that the DS-Client does not currently backup is generated. You can choose to have the wizard automatically create backups for these shares.

1. On the **Tools** menu, point to **Unprotected LAN Resource**, and then click **Discovery**.
2. Do the following:
    a) In the **Path** box, type the IP address or name of the computer you want to scan.
    b) To add a network item to the scan, select the item, and then click **Add**.
    c) To exclude a network item from the scan, select the item, and then click **Exclude**. The item's parent must already be in the discovery list.
    d) To add or exclude a specific subnet, click **Subnet**, and the do the following:
        1. In the **Subnet address** box, type the first three parts of the IP address followed by a 0 in the last part to signify the subnet. For example, 12.34.56.0 searches all resources on the ".56" subnet.
        2. To add the subnet, click **Add**.
        3. To exclude the subnet, click **Exclude**.
    e) To add or exclude scanned network items that were discovered by the previous scan, click **Select**, and then do the following:
        1. To add the scanned network item, select the item, and then click **Add**.
        2. To exclude the scanned network item, select the item, and then click **Exclude**.
    f) To remove a network item from the discovery list, select the item, and then click **Remove**.
    g) Click **Next**.
3. Do the following:

a) To add credentials for the discovery scan process, click **Add**.

b) To edit credentials, select the credentials, and then click **Modify**.

NOTE: To delete credentials, select the credentials, and then click **Delete**.

---

c) In the **Connect as** box, type the user name

d) In the **Password** box, type the password.

e) In the **From** box, if applicable select the computer where the DS-Client will verify your credentials. Normally this will be the same as the server that you are connecting to. However if the computer running DS-Client is a member of a domain, you can select from the available list of domains.

f) In the **Priority** box, enter the priority for the credentials that the DS-Client will use to attempt to scan the shares. The lower the number, the higher the priority.

g) Click **OK**.

h) Click **Next**.

4. Do the following:

a) Select the **Scheduled** option.

NOTE: To remove a schedule, select the **Not scheduled** option.

---

b) In the **Available schedules** box, select the schedule that you want to assign for the scanning process, and then click **OK**.

NOTE: If you are an administrator of backup operator you can create or edit a schedule by clicking **New** or **Edit**.

---

c) Click **Next**.

5. Do the following:

a) To create a backup for each unprotected computer that the scan identifies, select the **Create new backup set for unprotected computers/shares** check box.

b) In the **Owner** box, select the owner of any backup created by this process.

c) In the **Schedule** box, select the schedule to apply to any backup created by this process.

d) To include the Windows System State backup item for a new computers, select the **Add System State for new compute**r check box.

e) To include the Windows Services Database backup item for new computers, select the **Add Service Database for new computer** check box.

f) To send an email notification on completion of the scan, select the **Send notification** check box.

g) In the **E-mail** box, type the email address of the recipient for the email notification.

h) Beside **Format**, select whether you want th email notification to be in **HTML** or **Plain Text** format.

i) Click **Next**.

6. Do the following:

a) In the **Attempt to reconnect** box, enter the number of times the scan process will attempt to reconnect and the interval between attempts.

b) In the **Number of threads for scanning** box, enter the number of scan threads to be used by the process.

c) To start the immediately, select the **Start scan now** check box.

d) Click **Finish**.

13.2 Viewing the list of unprotected LAN resources

You can view the list of unprotected computers and shares on your LAN that have been discovered in the most recent scan. Unprotected computers and shares are not currently backed up by the DS-Client.

To view the list of unprotected LAN resources:

1. On the **Tools** menu, point to **Unprotected LAN Resource**, and then click **Node Summary** or **Share Summary**.
2. To email the results of the scan, click **E-mail,** and then do the following:

a) In the **Send results to following e-mail addresses** box, type the email addresses to which you want the results of the scan to be sent. Separate multiple addresses with a semi-colon (;) or a comma (,).

b) Beside **Format**, specify whether you want the email to be in **HTML** or **Plain Text** format.

c) Click **OK**.

3. To exclude a computer from the next scan, select the computer, and then click **Exclude**.
4. To view a list of unprotected shares on a computer, select the computer, and then click **Shares**.

5. To view a list of the backups that have been automatically created in the last scan process, click **Backup Set**.
6. To filter the results based on the server type, in the **Server type** box, select a category, and then click **Refresh**.
7. Click **Close**.

To view the list of unprotected shares:

1. On the **Tools** menu, point to **Unprotected LAN Resource**, and then click **Share Summary**.
2. To email the results of the scan, click **E-mail,** and then do the following:
   a) In the **Send results to following e-mail addresses** box, type the email addresses to which you want the results of the scan to be sent. Separate multiple addresses with a semi-colon (;) or a comma (,).
   b) Beside **Format**, specify whether you want the email to be in **HTML** or **Plain Text** format.
   c) Click **OK**.
3. To exclude a computer from the next scan, select the computer, and then click **Exclude**.
4. To filter the results based on the server name, in the **Server name** box, select a computer, and then click **Refresh**.
5. To filter the results by share type, in the **Share type** list, select a category, and then click **Refresh**.
6. Click **Close**.