

Dell EMC NetWorker Module for SAP

Version 19.1

Administration Guide

302-005-546

REV 01

Copyright © 2009-2019 Dell Inc. or its subsidiaries. All rights reserved.

Published May 2019

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS-IS." DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners.
Published in the USA.

Dell EMC
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.DellEMC.com

CONTENTS

Figures		9
Tables		11
Preface		13
Chapter 1	Overview of NMSAP Features	17
	Road map for NMSAP operations.....	18
	Terminology that is used in this guide.....	19
	Importance of backups and the backup lifecycle.....	19
	NMSAP features for all supported applications.....	20
	Scheduled backups.....	20
	Manual backups.....	20
	Client Direct feature.....	21
	Deduplication backups and restores with Data Domain.....	21
	Backups and restores with CloudBoost.....	22
	Backup configuration wizard.....	23
	NMSAP features specific to SAP HANA.....	24
	SAP HANA backups of redo logs.....	25
	SAP HANA backups with a dynamic backup prefix.....	25
	SAP HANA delta backups.....	25
	SAP HANA multitenant database container mode.....	26
	Support of SAP HANA 2.0 SPS 00.....	26
	SAP HANA scale-out environments.....	27
	SAP HANA system replication.....	27
	Internationalization with NMSAP HANA.....	28
	NMSAP features specific to SAP Oracle.....	28
	Restores of Fujitsu NetWorker Module for SAP R/3 backups.....	28
	Probe-based (event-based) backups.....	29
	Snapshot-based backups and restores.....	29
	Restartable backups.....	30
	Cluster and Oracle RAC support.....	30
	Directory backups and restores.....	30
	Oracle ASM and Exadata support.....	31
	Internationalization with NMSAP Oracle.....	32
	NMSAP Oracle recovery wizard.....	33
	Secure storage password and role-based secure storage.....	34
	Simplified scheduled backup configuration of multiple databases....	35
	Virtualization support.....	35
	NMSAP and associated software.....	36
	NetWorker software.....	36
	SAP server software.....	37
	SAP HANA software.....	37
	Oracle server software.....	37
	NMSAP software components.....	37

Chapter 2	Configuration for NMSAP HANA Operations	39
	Configuration road map for SAP HANA operations.....	40
	Verifying the NMSAP software requirements.....	40
	Configuring scheduled backups with the wizard.....	41
	Configuring scheduled backups with the wizard for SAP HANA delta backups.....	43
	Configuring scheduled backups with the wizard in an SAP HANA MDC system.....	43
	Configuring scheduled backups without the wizard.....	45
	Setting up the NMSAP parameter file and configuration file.....	45
	Configuring parallelism for SAP HANA operations.....	56
	Enabling the parameter file in SAP HANA Studio.....	57
	Configuring the data protection policy with NMC.....	57
	Configuring the Client resource without the wizard.....	59
	Configuring manual backups.....	62
	Configuring automatic backups of SAP HANA redo logs.....	62
	Configuring Data Domain Boost backups.....	63
	Requirements for DD Boost backups.....	63
	Best practices for DD Boost backups.....	64
	Configuring Client Direct with DD Boost backups.....	64
	Configuring storage node with DD Boost backups.....	66
	Configuring CloudBoost backups.....	66
	Best practices for CloudBoost backups.....	66
	Configuring CloudBoost backups to use Client Direct.....	67
	Configuring CloudBoost backups to use a storage node.....	67
	Configuring NMSAP backups to AFTD storage.....	68
	Configuring Client Direct backups to AFTD.....	68
	Configuring storage node backups to AFTD.....	68
Chapter 3	NMSAP HANA Operations	71
	Performing scheduled backups of SAP HANA data.....	72
	Testing scheduled backups.....	72
	Monitoring scheduled backups.....	72
	Canceling scheduled backups.....	73
	Performing manual backups and recovery with SAP HANA Studio.....	73
	Performing manual backups with SAP HANA Studio.....	73
	Deleting backups with SAP HANA Studio.....	74
	Performing restore and recovery with SAP HANA Studio.....	75
	Performing manual backups and recovery with the SAP HANA CLI.....	78
	Performing manual backups with the SAP HANA CLI.....	79
	Canceling manual backups.....	80
	Checking NMSAP backups with the SAP HANA CLI.....	81
	Performing recovery with the SAP HANA CLI.....	81
	Preparing for SAP HANA disaster recovery.....	82
	SAP HANA scale-out requirements.....	83
Chapter 4	Configuration for NMSAP Oracle Operations	85
	Configuration road map for NMSAP Oracle operations.....	86
	Verifying the NMSAP software requirements.....	86
	Configuring I18N support.....	88
	Requirements for I18N support.....	88
	Configuring I18N support on UNIX.....	88
	Choosing either backint or RMAN as the backup and restore utility.....	88
	Specifying backint as the backup and restore utility.....	89

	Specifying RMAN as the backup and restore utility.....	90
	Configuring scheduled backups with the wizard.....	91
	Configuring scheduled backups without the wizard.....	93
	Configuring the NMSAP parameters without the wizard.....	93
	Configuring the data protection policy with NMC.....	113
	Configuring the Client resource without the wizard.....	115
	Configuring manual backups.....	118
	Configuring restartable backups.....	119
	Configuring scheduled restartable backups with the wizard.....	119
	Configuring scheduled restartable backups without the wizard....	119
	Configuring manual restartable backups.....	120
	Configuring Data Domain Boost backups.....	120
	Requirements for DD Boost backups.....	120
	Best practices for DD Boost backups.....	121
	Configuring Client Direct with DD Boost backups.....	121
	Configuring storage node with DD Boost backups.....	123
	Configuring CloudBoost backups.....	123
	Best practices for CloudBoost backups.....	124
	Configuring CloudBoost backups to use Client Direct.....	124
	Configuring CloudBoost backups to use a storage node.....	125
	Configuring NMSAP backups to AFTD storage.....	125
	Configuring Client Direct backups to AFTD.....	125
	Configuring storage node backups to AFTD.....	126
	Configuring probe-based backups.....	126
	Configuring a probe-based backup.....	126
	User-defined probes.....	129
	Example probe-based backup with multiple probes.....	129
Chapter 5	NMSAP Oracle Operations	131
	Performing scheduled backups of SAP Oracle data.....	132
	Testing scheduled backups.....	132
	Monitoring scheduled backups.....	133
	Canceling scheduled backups.....	133
	Restarting failed scheduled backups.....	133
	Performing manual backups.....	134
	Running manual backups.....	134
	Monitoring manual backups.....	135
	Canceling manual backups.....	135
	Restarting failed manual backups.....	135
	Reviewing backup and restore session reports.....	136
	Verifying backup information in the NetWorker indexes.....	137
	Performing data restore and recovery.....	138
	Performing data restore and recovery with the NMSAP recovery wizard.....	138
	Performing data restore and recovery without the NMSAP recovery wizard.....	140
	Restarting a restore for files that failed a restore.....	143
	Requirements for disaster recovery.....	144
	Recovering from a disaster.....	144
	Restoring the required Oracle and SAP BR*Tools files.....	144
	Recovering an SAP Oracle database after disaster.....	146
Chapter 6	SAP Oracle in Cluster and RAC Environments	147
	SAP Oracle cluster systems.....	148

	Client parameter setting for cluster systems.....	148
	NSR_PHYSICAL_HOST_LICENSE setting for cluster systems....	148
	Configuring scheduled backups in a cluster with the wizard.....	149
	Configuring scheduled backups in a cluster without the wizard...	150
	Configuring manual backups in a cluster.....	150
	Configuring Data Domain deduplication backups in a cluster.....	150
	Configuring probe-based backups in a cluster.....	151
	Restoring data in a cluster.....	151
	Oracle RAC systems.....	151
	Configuring Oracle RAC backups.....	151
	Configuring backups with Backint.....	152
	Configuring backups with RMAN.....	152
	Restoring Oracle RAC data.....	154
Chapter 7	NMSAP Oracle Snapshot Backups and Restores	155
	Snapshot operations with NetWorker Snapshot Management.....	156
	Types of NSM backups.....	157
	Snapshot backup.....	157
	Clone to conventional media.....	157
	ProtectPoint backup or clone.....	157
	Types of NSM restores.....	158
	Restore from snapshot or ProtectPoint copies (backup or clone)....	158
	Restore from clone on secondary storage (conventional media)..	159
	Rollback restore.....	159
	Backup and restore data flows with NSM.....	160
	Configuring NMSAP snapshot backups with NSM.....	162
	Configuring Device resources for NSM backups.....	165
	Configuring Pool resources for NSM backups.....	165
	Configuring Client resources manually for NSM backups.....	165
	Configuring the NMSAP parameters for NSM operations.....	166
	Configuring the NSM parameters.....	166
	Settings for OCFS2 system with remote data mover.....	169
	Testing NMSAP backups and restores with NSM.....	170
	Example parameter settings for NSM backups.....	171
	Reviewing the NMSAP NSM backup records.....	172
Chapter 8	NMSAP Oracle Split-Mirror Backups and Restores	173
	Split-mirror backups and restores.....	174
	Basic split-mirror backup and restore data flows.....	174
	Manual split-mirror backup data flow.....	174
	Scheduled split-mirror backup data flow.....	175
	Restore of split-mirror backup data flow.....	176
	Configuring the production host for split-mirror backups.....	176
	Configuring Oracle software on the production host.....	176
	Configuring BR*Tools on the production host.....	176
	Configuring NMSAP on the production host.....	177
	Configuring the mount host for split-mirror backups.....	177
	Configuring Oracle software on the mount host.....	177
	Configuring BR*Tools on the mount host.....	177
	Configuring NMSAP on the mount host.....	179
	Configuring the snapshot software for split-mirror backups.....	179
	Configuring the NetWorker server for split-mirror backups.....	179
	Configuring a cluster environment for split-mirror backups.....	180

	Examples of parameters for split-mirror backups.....	181
	Parameter settings on the production host.....	181
	Parameter settings on the mount host.....	181
Appendix A	Examples of SAP Oracle Command Options	183
	Examples of brbackup and brarchive command syntax and options.....	184
	Examples of brrestore command syntax and options.....	185
	Examples of brrecover command syntax and options.....	186
Appendix B	Troubleshooting and Error Messages	189
	Verifying the release information.....	190
	Generating diagnostic logs.....	190
	Setting the debugging options for RMAN operations.....	191
	Backup and restore problems.....	191
	NMSAP error messages.....	194
Glossary		197

CONTENTS

FIGURES

1	Configuration wizard fields for a scheduled backup of MDC databases.....	44
2	Specifying the parameter file in SAP HANA Studio.....	57
3	Configuring automatic log backups in SAP HANA Studio.....	63
4	Specifying backup settings in SAP HANA Studio.....	74
5	Specifying backup deletion settings in SAP HANA Studio.....	75
6	Specifying the recovery type in SAP HANA Studio.....	76
7	Selecting the backup catalog for a single database container of SAP HANA 2.0 in SAP HANA Studio.....	77
8	Selecting the data backup in SAP HANA Studio.....	78
9	NSM snapshot and clone to secondary storage data flow with NMSAP.....	161
10	NSM snapshot restore data flow with NMSAP.....	162

FIGURES

TABLES

1	Revision history.....	13
2	Style conventions.....	14
3	NMSAP and associated software components.....	37
4	Mapping of SAP HANA and NetWorker backup levels.....	43
5	Supported hdbbackint parameters.....	46
6	Supported nsrsapsv parameters.....	52
7	NetWorker Client resource attributes for NMSAP scheduled backups	60
8	Configuring a Data Domain backup.....	65
9	Supported backint parameters.....	95
10	Supported nsrsapsv parameters.....	105
11	Supported NSR_* parameters for RMAN.....	111
12	NetWorker Client resource attributes for NMSAP scheduled backups	116
13	Configuring a Data Domain backup.....	122
14	NetWorker Probe resource attributes for NMSAP backups.....	127
15	Typical configuration for NSM operations.....	156
16	Supported types of NSM backups.....	157
17	Supported types of NSM restores.....	158
18	NMSAP NSM parameters in parameter file initDBSID.utl.....	166
19	Common parameters in NSM configuration file, nmsapps.cfg.....	167
20	NSM parameters for ProtectPoint for VMAX operations only.....	168
21	NSM parameters for ProtectPoint with RecoverPoint operations only.....	169
22	Options for brbackup and brarchive commands.....	184
23	Options for brrestore command.....	185
24	Options for brrecover command.....	186
25	NMSAP backup or restore problems.....	191
26	NMSAP error messages.....	194

TABLES

Preface

As part of an effort to improve product lines, periodic revisions of software and hardware are released. Therefore, all versions of the software or hardware currently in use might not support some functions that are described in this document. The product release notes provide the most up-to-date information on product features.

If a product does not function correctly or does not function as described in this document, contact a technical support professional.

Note

This document was accurate at publication time. To ensure that you are using the latest version of this document, go to the Support website <https://www.dell.com/support>.

Purpose

This document describes how to configure and use the NetWorker Module for SAP (NMSAP) version 19.1.

Audience

This document is intended for system administrators who are responsible for configuring NMSAP and maintaining backup and recovery systems.

Users of this guide must be familiar with the following topics:

- SAP terminology and concepts, especially those related to SAP HANA and Oracle database backup and recovery
- Backup and recovery procedures
- Disaster recovery procedures

Revision history

The following table presents the revision history of this document.

Table 1 Revision history

Revision	Date	Description
01	May 20, 2019	Initial release of this document for NMSAP version 19.1.

Related documentation

You can find additional publications for this product release and related NetWorker products at the Support website.

The *NetWorker E-LAB Navigator* at <https://elabnavigator.emc.com/eln/elhome> provides details about supported environments and platforms.

Special notice conventions that are used in this document

The following conventions are used for special notices:

NOTICE

Identifies content that warns of potential business or data loss.

Note

Contains information that is incidental, but not essential, to the topic.

Typographical conventions

The following type style conventions are used in this document:

Table 2 Style conventions

Bold	Used for interface elements that a user specifically selects or clicks, for example, names of buttons, fields, tab names, and menu paths. Also used for the name of a dialog box, page, pane, screen area with title, table label, and window.
<i>Italic</i>	Used for full titles of publications that are referenced in text.
Monospace	Used for: <ul style="list-style-type: none"> • System code • System output, such as an error message or script • Pathnames, file names, file name extensions, prompts, and syntax • Commands and options
<i>Monospace italic</i>	Used for variables.
Monospace bold	Used for user input.
[]	Square brackets enclose optional values.
	Vertical line indicates alternate selections. The vertical line means or for the alternate selections.
{ }	Braces enclose content that the user must specify, such as x, y, or z.
...	Ellipses indicate non-essential information that is omitted from the example.

You can use the following resources to find more information about this product, obtain support, and provide feedback.

Where to find product documentation

- <https://www.dell.com/support>
- <https://community.emc.com>

Where to get support

The Support website <https://www.dell.com/support> provides access to product licensing, documentation, advisories, downloads, and how-to and troubleshooting information. The information can enable you to resolve a product issue before you contact Support.

To access a product-specific page:

1. Go to <https://www.dell.com/support>.
2. In the search box, type a product name, and then from the list that appears, select the product.

Knowledgebase

The Knowledgebase contains applicable solutions that you can search for either by solution number (for example, KB000xxxxxx) or by keyword.

To search the Knowledgebase:

1. Go to <https://www.dell.com/support>.
2. On the **Support** tab, click **Knowledge Base**.
3. In the search box, type either the solution number or keywords. Optionally, you can limit the search to specific products by typing a product name in the search box, and then selecting the product from the list that appears.

Live chat

To participate in a live interactive chat with a support agent:

1. Go to <https://www.dell.com/support>.
2. On the **Support** tab, click **Contact Support**.
3. On the **Contact Information** page, click the relevant support, and then proceed.

Service requests

To obtain in-depth help from Licensing, submit a service request. To submit a service request:

1. Go to <https://www.dell.com/support>.
2. On the **Support** tab, click **Service Requests**.

Note

To create a service request, you must have a valid support agreement. For details about either an account or obtaining a valid support agreement, contact a sales representative. To get the details of a service request, in the *Service Request Number* field, type the service request number, and then click the right arrow.

To review an open service request:

1. Go to <https://www.dell.com/support>.
2. On the **Support** tab, click **Service Requests**.
3. On the **Service Requests** page, under **Manage Your Service Requests**, click **View All Dell Service Requests**.

Online communities

For peer contacts, conversations, and content on product support and solutions, go to the Community Network <https://community.emc.com>. Interactively engage with customers, partners, and certified professionals online.

How to provide feedback

Feedback helps to improve the accuracy, organization, and overall quality of publications. You can send feedback to DPAD.Doc.Feedback@emc.com.

CHAPTER 1

Overview of NMSAP Features

This chapter includes the following topics:

- [Road map for NMSAP operations](#)..... 18
- [Terminology that is used in this guide](#)..... 19
- [Importance of backups and the backup lifecycle](#).....19
- [NMSAP features for all supported applications](#).....20
- [NMSAP features specific to SAP HANA](#)..... 24
- [NMSAP features specific to SAP Oracle](#).....28
- [NMSAP and associated software](#).....36
- [NMSAP software components](#)..... 37

Road map for NMSAP operations

Use the following road map to configure the NetWorker Module for SAP (NMSAP) software, and perform backups and restores with NMSAP on an SAP HANA host or SAP Oracle host.

NOTICE

Before you click a cross-reference, check the page number of the current topic in the guide in case you must return to the same location from the cross-referenced topic.

Procedure

1. Review the *NetWorker Module for SAP Release Notes* for the most up-to-date information about NMSAP.
2. Ensure that you have installed or updated NMSAP according to the instructions in the *NetWorker Module for SAP Installation Guide*.
3. Review the information in this chapter about the major features of NMSAP.
4. Configure and perform operations in an SAP HANA environment:
 - Configure backups according to information in [Configuration for NMSAP HANA Operations](#) on page 39.
 - Perform backups and restores according to information in [NMSAP HANA Operations](#) on page 71.
5. Configure and perform operations in an SAP Oracle environment:
 - In a stand-alone SAP Oracle environment:
 - Configure regular (nonsnapshot) backups according to information in [Configuration for NMSAP Oracle Operations](#) on page 85.
 - Perform regular backups and recovery according to information in [NMSAP Oracle Operations](#) on page 131.
 - For SAP Oracle in a cluster or RAC environment, configure and perform backup and recovery according to information in [SAP Oracle in Cluster and RAC Environments](#) on page 147.
 - Configure and perform NMSAP Oracle snapshot backups according to information in [NMSAP Oracle Snapshot Backups and Restores](#) on page 155.
 - Configure and perform NMSAP Oracle split-mirror backups according to information in [NMSAP Oracle Split-Mirror Backups and Restores](#) on page 173.
6. Use the following information to troubleshoot any issues with NMSAP operations:
 - [Troubleshooting and Error Messages](#) on page 189
 - *NetWorker Module for SAP Release Notes*

Terminology that is used in this guide

The term *SAP Oracle* that is used throughout this document refers to an SAP environment with an Oracle database.

The generic sections of this guide use the term *transaction logs* for the logs that are required to recover data that is backed up by NMSAP. The different applications that NMSAP supports use application-specific terms for the logs, such as archived logs and redo logs.

In this guide, the UNIX references apply to both UNIX and Linux operating systems, unless specified otherwise. The Windows references apply to all the supported Microsoft Windows operating systems, unless specified otherwise.

Unlike the NetWorker software that uses the term *recover* for all backup retrieval activities, NMSAP processes distinguish between the *restore* and *recovery* of a database:

- *Restore* means to retrieve datafiles from a backup and store the files on a disk.
- *Recover* means to apply the database transaction logs to update the database to a specific point-in-time and to make the database consistent.

The glossary provides details about the terms that are used in this guide.

Importance of backups and the backup lifecycle

You must perform regular backups of specific data to prepare for the recovery of the database system.

For the complete protection of a database system or application system, a viable backup strategy must include regular backups of the following data:

- Database or application data
- Transaction (or archived) logs
- Configuration and control files for a database or application

These backups are important for the following reasons:

- Without backups, you cannot restore a database at all.
- Without transaction logs, you can restore a database only to the time of its last consistent backup.
- Without the configuration files and control files, you cannot re-create the database setup or application setup.

The NetWorker server maintains an online client file index and online media database, which together comprise the online indexes. During an NMSAP backup, the NetWorker server makes an entry in the online client file index and records the location of the data in the online media database. These entries provide recovery information that is required for all backed-up data.

The NetWorker server manages the backup lifecycle of NMSAP data through the retention policy. Specify this policy for each file and NetWorker save set respectively before the backup time. You can specify the policy by setting the NetWorker Client resource retention attribute or the `NSR_SAVESET_RETENTION` parameter.

The retention policy determines how long save set entries are maintained in the media database on the NetWorker server.

When a backup file entry expires from the NetWorker client index, NMSAP is unable to restore the specified file. You can use the NetWorker `scanner` program to re-

create the missing entry if the volume of the NetWorker save set containing the save file is not recycled. You cannot recover a backup after a save set's retention policy expires and the volume that contains the save set is recycled.

The *NetWorker Administration Guide* provides details.

Note

The NetWorker server backup by default backs up the bootstrap and client index information. The NetWorker disaster recovery documentation describes how to prepare for NetWorker server disaster recovery.

NMSAP features for all supported applications

NMSAP is an add-on module for the NetWorker server and client software that provides backup and recovery services for SAP HANA and SAP Oracle data. NMSAP provides a backup and restore interface between the SAP backup and restore interfaces, the NetWorker server, and the NetWorker Management Console (NMC).

The following topics describe the common NMSAP features that are supported for both SAP HANA and SAP Oracle operations. [NMSAP features specific to SAP HANA](#) on page 24 and [NMSAP features specific to SAP Oracle](#) on page 28 describe the NMSAP features that are supported only for SAP HANA or SAP Oracle operations.

Scheduled backups

An NMSAP backup can be a scheduled backup or a manual backup.

You can configure a scheduled backup to use a calendar time or to use probe settings that detect when the system meets specific conditions. The NetWorker server starts the scheduled backup according to the backup configuration settings.

Note

NMSAP does not support probe-based (event-based) scheduled backups of SAP HANA data.

Manual backups

You can start a manual backup at any time, on demand, by running the required SAP command on the NMSAP client host.

NOTICE

A NetWorker data protection policy applies only to a scheduled backup, and defines the workflow, action, backup group, and other required settings for a scheduled backup. NetWorker features that are related to a data protection policy, such as the clone action and the protection period, apply only to scheduled backups and do not apply to manual backups. [Configuring the data protection policy with NMC](#) on page 57 provides more details about data protection policies.

Review the following application-specific considerations:

- With all SAP HANA versions, an automatic log backup is considered to be a manual backup. The log backups are not cloned like scheduled backups. To clone the logs, perform a manual clone operation by using the `nsrclone` command.

- With SAP HANA version 2.0, a backint catalog backup is considered to be a manual backup. The catalog backups are not cloned as part of the scheduled backup operation. To clone the catalog backups, perform a manual clone operation by using the `nsrclone` command.
- Due to a limitation, an NMSAP Oracle RMAN backup on Windows is considered to be a manual backup, even when the NetWorker server initiates the backup.

Client Direct feature

NMSAP supports the Client Direct feature, which enables client backups to bypass the NetWorker storage node and perform one of the following operations:

- Send deduplicated backup data directly to DD Boost devices.
- Send backup data directly to advanced file type devices (AFTDs).
- Send backup data directly to CloudBoost devices.

The Client Direct feature, also known as direct file access or DFA, reduces bandwidth usage and bottlenecks at the storage node, and provides highly efficient transmission of backup data. A Client Direct backup uses the storage node only to coordinate the backup and manage the device.

If an NMSAP backup cannot use the Client Direct feature due to the permissions or accessibility to the target device, the backup uses the storage node instead.

The *NetWorker Module for SAP Release Notes* describes the software requirements of an NMSAP Client Direct backup.

Deduplication backups and restores with Data Domain

NMSAP supports deduplication backups and restores with an Data Domain system. You can configure the Data Domain system as NetWorker advanced file type devices (AFTDs), virtual tape library (VTL) devices, or Data Domain Boost (DD Boost) devices.

A Data Domain deduplication backup to an AFTD, VTL, or DD Boost device can be a manual or scheduled backup, including a probe-based backup. NMSAP supports backups to DD Boost devices over IP or Fibre Channel (FC).

Note

NMSAP supports both the Data Domain IPv6 and mixed IPv4/IPv6 networks.

The first Data Domain backup backs up all the specified data and achieves the least amount of data deduplication, referred to as compression or global compression in Data Domain documentation. Subsequent Data Domain backups achieve improved deduplication rates as the backups identify more redundant data blocks.

Do not use NMSAP encryption or compression for backups to a Data Domain system. The encryption or compression decreases the data deduplication ratio.

Backups to VTL or AFTD devices on Data Domain

An NMSAP backup to a Data Domain system that is configured as a NetWorker VTL or NetWorker AFTD device sends all the data to the Data Domain system where the deduplication occurs. During a restore, the Data Domain system converts the stored data to its original nondeduplicated format before sending the data over the network.

Backups to DD Boost devices

NMSAP can use the Client Direct feature or the NetWorker storage node to perform backups to DD Boost devices.

An NMSAP backup to a Data Domain system that is configured as a DD Boost device can take advantage of the DD Boost feature, which consists of two components:

- The DD Boost library API enables the NetWorker software to communicate with the Data Domain system.
- The distributed segment processing (DSP) component reviews the data that is stored on the Data Domain system and sends only unique data for storage.

DSP enables deduplication of the backup data on the NetWorker storage node or the NMSAP client directly. Deduplication on the NetWorker storage node can be used when the NMSAP client does not have direct access to the Data Domain system or when DD Boost does not support the NMSAP client's operating system. With deduplication on the storage node, all the data is sent from the NMSAP client to the storage node and only the unique blocks are sent from the storage node to the target device.

To reduce the amount of transferred data, NMSAP can use the DD Boost components to deduplicate the data locally. NMSAP then sends only the unique blocks directly to the target device through direct file access (DFA) technology (Client Direct feature). A Client Direct backup uses the storage node only to coordinate the backup and manage the device.

By default, NMSAP tries to perform a Client Direct backup. If the NMSAP client does not have direct access to the DD Boost device on the Data Domain system, then the backup is automatically routed through the storage node.

During a restore, if the NMSAP client has direct access to the DD Boost device, then the client restores data directly from the device. The client performs the restore directly from the device regardless of whether the backup was done directly from the NMSAP client or through the storage node. If the NMSAP client cannot access the data directly, then the restore process uses the traditional method with the storage node. Regardless of the restore method that is used, the Data Domain system converts the stored data to its original nonduplicated state before sending the data over the network.

Backups and restores with CloudBoost

NMSAP supports backups and restores with an CloudBoost appliance. You can configure the CloudBoost system as a NetWorker CloudBoost device.

A CloudBoost backup to a CloudBoost device can be a manual backup or a scheduled backup, including a probe-based backup.

NMSAP can perform CloudBoost backups through either the Client Direct workflow or the NetWorker storage node workflow:

1. CloudBoost backups using Client Direct—With the Client Direct workflow, NMSAP uses the CloudBoost components to send the data directly to the target device, bypassing the storage node. This configuration eliminates the sending of data over the network between the NMSAP client and the storage node. NMSAP sends the data directly from the NMSAP client to the CloudBoost appliance.
2. CloudBoost backups using a remote storage node—With the NetWorker storage node workflow, NMSAP sends all the data to a remote storage node, which sends the data to the target device. NMSAP uses this workflow if the NMSAP client

does not have direct access to the CloudBoost appliance or if the Client Direct workflow is not possible for other reasons.

By default, NMSAP tries to perform a Client Direct backup. If the NMSAP client does not have direct access to the CloudBoost appliance or if the Client Direct workflow is not possible for other reasons, then the backup is automatically routed through the storage node.

During a restore, if the NMSAP client has direct access to the CloudBoost appliance, then the client restores data directly from the device, regardless of whether the backup was done directly from the NMSAP client or through the storage node. If the NMSAP client cannot access the data directly, then the restore process reverts to the traditional method that uses the storage node.

You must configure a CloudBoost backup with a supported CloudBoost device according to the appropriate instructions:

- NMSAP HANA: [Configuring CloudBoost backups](#) on page 66
- NMSAP Oracle: [Configuring CloudBoost backups](#) on page 123

Backup configuration wizard

NMSAP supports the backup configuration wizard, which is a Java application that you run from NMC to configure a scheduled backup. If the configuration wizard supports the environment, use the wizard when possible to create a backup configuration.

The configuration wizard provides the recommended method to create and modify an NMSAP Oracle configuration for a snapshot backup with NSM. The wizard ensures the correct sequence of configuration steps and the verification of configuration dependencies.

The wizard provides the option of a typical or custom configuration, depending on the amount of detail that is needed for a specific backup configuration. The typical workflow enables you to configure a backup with fewer clicks by using default backup settings.

A scheduled backup configuration that is created with the wizard is not saved as client-side parameters and configuration files, but as attributes in the Client resource on the NetWorker server. The wizard can use the NMSAP parameters and configuration files that you used with earlier NMSAP releases as input templates to generate a new wizard configuration.

You can optionally save the backup settings that are created with the wizard to an NMSAP parameter file (`initDBSID.utl`) and configuration file (`nsrsapsv.cfg`) on the NMSAP client host. You can use these files for diagnostic or reference purposes.

Configure some NetWorker resources and settings outside of the wizard with the NMC program, for example:

- Device resources
- Media Pool resources
- NetWorker user privileges

The wizard does not support the modification of a scheduled backup configuration that was created without the wizard.

The wizard does not support the configuration of the following types of NMSAP Oracle backups:

- RMAN backups
 - Split-mirror backups
 - Probe-based (event-based) backups
-

Note

An NMSAP Client resource that is created with the wizard can be associated with a probe by selecting the Probe attribute in the Client resource in NMC, outside of the wizard.

NMSAP features specific to SAP HANA

An SAP HANA database holds most of the data in memory but also uses persistent storage on disk. During normal database operations, the data is automatically saved from memory to the disk at regular intervals. All the data changes are also captured in the redo log on the disk, which is updated after each committed database transaction. The data on disk must be backed up to ensure protection against a disk failure.

NMSAP is integrated with the SAP HANA BACKINT interface program, `hdbbackint`, to provide the backup, deletion, inquiry, and recovery services for SAP HANA database data and redo logs.

Based on the features that SAP HANA supports, NMSAP supports the following SAP HANA data operations:

- Manual and scheduled backups
-

Note

You can configure scheduled backups with the backup configuration wizard.

- Online backups
 - Full database backups
 - Redo log backups
 - Recovery of a database to the most recent state, a specific point-in-time, a specific data backup, or a log position
 - Recovery to the original host or an alternate host
 - Deduplication backups to and restores from a Data Domain system that is configured as a NetWorker virtual tape library (VTL), advanced file type device (AFTD), or DD Boost device
 - Client Direct backups to an AFTD or DD Boost device
-

Note

For SAP HANA operations, NMSAP does not support probe-based (event-based) backups or restartable backups.

NMSAP works with the following SAP HANA interfaces on the database server to perform backup and restore operations:

- SAP HANA command line interface (CLI) with the `hdbsql` command
- SAP HANA Studio GUI
- SAP DBA Cockpit in The Computing Center Management System (CCMS) GUI

SAP HANA requires that restore and recovery is performed on a Linux system with the same architecture as the backup system:

- An SAP HANA backup that is performed on a Linux x64 system can be restored only to a Linux x64 system.
- An SAP HANA backup that is performed on a PowerLinux 64-bit big-endian system can be restored only to a PowerLinux 64-bit big-endian system.

The *NetWorker E-LAB Navigator* at <https://elabnavigator.emc.com/eln/elhome> provides details about the NMSAP support of Linux systems. The SAP HANA documentation provides details about any specific limitations related to the SAP HANA operations.

The following topics describe the NMSAP features that are supported only for SAP HANA backup and restore operations.

SAP HANA backups of redo logs

The SAP HANA database server automatically performs periodic backups of the redo logs for a database. You do not run the log backups with any backup commands as is the case for database backups.

You can use the SAP HANA Studio to configure the frequency of automatic log backups and whether the BACKINT interface is used for the log backups.

SAP HANA backups with a dynamic backup prefix

NMSAP supports the dynamic generation of a timestamp for the backup prefix, which is used in the name of the SAP HANA backup files. The timestamp produces a unique identifier for a HANA backup.

You can specify that a dynamically generated timestamp, `YYYY_MM_DD_HH_MI_SS`, is appended to the backup prefix before a HANA backup starts, which creates a unique identifier for the backup. If the text for the HANA backup prefix is not specified, then the timestamp is used for the backup prefix. As a result, you can restore to a particular backup file, based on both the prefix text and the timestamp.

Note

The timestamp is different than the backup save time because the timestamp is generated before the backup starts and is passed to HANA database server through the backup command.

To specify the dynamic generation of a timestamp for the backup prefix:

- For a wizard configuration, select **Append the timestamp to the backup file prefix** on the **Specify the SAP HANA Information** page in the NMSAP wizard.
- For a client-side configuration, set the parameter `HANA_DYNAMIC_PREFIX` in the `nsrsapsv.cfg` configuration file.

SAP HANA delta backups

NMSAP supports the delta backups of SAP HANA databases. SAP HANA SPS 10 revision 100 and later supports the delta backups.

A delta backup can be an incremental or differential backup:

- An incremental backup stores the data that has changed since the last full or delta data backup.
- A differential backup stores the data that has changed since the last full data backup.

With NetWorker server 9.1 or later, NMSAP supports the following operations:

- Scheduled HANA delta backups by using the NMC GUI.
- Manual HANA delta backups by using either the SAP HANA Studio GUI or the CLI program `hdbssql`.
- Manual recovery of delta backups by using the SAP HANA Studio GUI.

NOTICE

To prevent potential issues with the restore of delta backups, ensure that the HANA backup catalog and NetWorker indexes remain synchronized. If you delete an SAP HANA backup or save set from the NetWorker server, delete the corresponding backup entries manually from the HANA backup catalog. For manual backups, if a retention time was configured for the save sets, then you must delete the corresponding backup from the HANA backup catalog immediately after the expiration time.

Without the recommended deletions, the HANA catalog and NetWorker server indexes can become unsynchronized and the delta backups can be performed without a corresponding full backup, which can cause restore issues.

The latest chain of full and delta backups might have been deleted from the NetWorker server but the NetWorker indexes might still contain older backup chains. Issues can occur when the HANA catalog still contains the latest backup chain.

In this case, when you request a delta backup, NMSAP finds the older full backup and does not promote the delta backup to a full backup. SAP HANA also finds the latest full backup in the HANA catalog and performs the delta backup. Potential data loss can occur during a subsequent restore when the delta backup cannot be applied against a previous full/delta backup chain. The only way to restore the data would be to use full/delta backups of the older chain, plus archived log backups that correspond to the deleted chain and the latest delta.

SAP HANA multitenant database container mode

SAP HANA SPS 9 introduced the new functionality known as multitenant database container (MDC) that enables SAP HANA to run multiple tenant databases within a single SAP HANA system. An SAP HANA MDC system has one master system database named SYSTEMDB, which is used for system administration, and any number of tenant databases.

NMSAP supports the following SAP HANA operations:

- Backup of the system database and multiple tenant databases by using the system database administrator credentials with the NMSAP HANA wizard.
- Backup of an individual tenant database by using the tenant database administrator credentials with the NMSAP HANA wizard.
- Backup of SAP HANA MDC databases by using either the SAP HANA Studio GUI or the CLI program `hdbssql`.
- Recovery of SAP HANA MDC databases by using either the SAP HANA Studio GUI or the CLI program `hdbssql`.

Note

Ensure that the `hdbbackint` operational log file has the 0666 permission setting.

Support of SAP HANA 2.0 SPS 00

NMSAP supports SAP HANA 2.0 SPS 00. Review the SAP HANA 2.0 user documentation for a complete list of all the new backup and recovery features,

including details about how to enable and configure the features. The following list highlights several of the new features:

- SAP HANA 2.0 SPS 00 supports data encryption in the persistence layer for both data and log volumes. SAP HANA volume encryption can impact the deduplication rates on the Data Domain systems.
- SAP HANA 2.0 SPS 00 supports the user-configurable interval mode for log backups. The interval mode enables the creation of log backups after the service-specific timeout is reached, instead of when the log segment becomes full. A log backup can include multiple log segments. The interval mode setting limits the number of log backups in high-transaction databases, which reduces the impact on the databases. You can configure the interval mode by setting the following parameter in the SAP HANA `global.ini` file:

```
log_backup_interval_mode = service
```

- SAP HANA 2.0 requires that the backup catalog backups and transaction log backups be configured separately. In previous SAP HANA releases, the backup catalog was automatically saved as part of the transaction log backups. Ensure that both the backup catalog backups and transaction log backups are configured to use NMSAP through the Backint interface.

Due to SAP HANA limitations, the following issue might occur during the NMSAP operations:

- SAP HANA 2.0 SPS 00 REV 00 might report an error during a multitenant database container (MDC) restore operation that is otherwise successful. The SAP Notes 2222121 and 2395530 provide details about this limitation.

SAP HANA scale-out environments

SAP HANA software supports high availability on an SAP HANA scale-out appliance that contains multiple nodes.

NMSAP supports backups and restores in an SAP HANA scale-out multinode environment. You must meet specific requirements in the SAP HANA scale-out environment as described in [SAP HANA scale-out requirements](#) on page 83.

SAP HANA system replication

NMSAP supports SAP HANA system replication by using the Backint API. The SAP HANA Administration Guide provides details about the configuration and operation of SAP HANA system replication environments.

All the systems that participate in the SAP HANA system replication cluster must use the same NetWorker client resource to perform the restore operations. Only the active primary node writes the backups to the client resource.

Note

After takeover occurs, ensure that the original primary system does not continue to write backups by using the NetWorker client resource. If the original primary system continues to write the backups, corruption of the backup catalog can occur and prevent the recovery of the SAP HANA system.

All the nodes in an SAP HANA system replication cluster must use the same system username and user ID (UID), to enable the restore operations. Otherwise, a permissions error can occur during a restore on a secondary node of a backup that was performed on the primary node.

Internationalization with NMSAP HANA

SAP HANA only supports UNICODE for internationalization. NMSAP HANA supports UNICODE for backups and restores. For example, the backup prefix in the NMSAP backup command can include Japanese characters.

Note

I18N support is distinguished from localization (L10N) support, in which the software user interface and operational messages are translated into localized languages. This NMSAP release does not provide L10N support.

NMSAP features specific to SAP Oracle

NMSAP interacts with SAP BR*Tools to provide backup and recovery services for Oracle database data and logs and other SAP files. NMSAP is integrated with the SAP Oracle BACKINT interface program, `backint`, and also with the BR*Tools Oracle Recovery Manager (RMAN) interface.

NMSAP supports the following SAP Oracle data operations and environments:

- Manual and scheduled backups, including probe-based scheduled backups
- Online and offline backups
- Database, tablespace, and datafile backups
- Redo log backups
- Restartable backups
- Recovery to the most recent state or a specific point-in-time
- Recovery to the original host or an alternate host or location
- Restores of Fujitsu NetWorker Module for SAP R/3
- Deduplication backups and restores with a Data Domain system
- Client Direct backups to an AFTD
- Cluster and Oracle RAC environments
- Directory backups and restores
- Snapshot backups and restores
- Split-mirror backups and restores
- Oracle ASM and Exadata
- Configuration with the backup configuration wizard
- Configuration with the recovery configuration wizard
- Internationalization
- Virtualization

The following topics describe the NMSAP features that are supported only for NMSAP Oracle backup and restore operations.

Restores of Fujitsu NetWorker Module for SAP R/3 backups

NMSAP can restore backups that were performed with Fujitsu NetWorker Module for SAP R/3 version 3.0 on an operating system that this NMSAP release supports. The

NetWorker E-LAB Navigator at <https://elabnavigator.emc.com/eln/elhome> provides details about the operating systems that NMSAP supports.

If the backup with Fujitsu NetWorker Module for SAP R/3 used advanced backup compression with GZIP or BZIP2, NMSAP automatically uncompresses the backup during the restore.

If you convert from using Fujitsu NetWorker Module for SAP R/3 to using NMSAP, you must configure backups of SAP Oracle data according to the NMSAP documentation. For example, NMSAP operations ignore the following options if they are set:

- Fujitsu-specific compression options GZIP and BZIP2
- Other Fujitsu-specific parameters, such as `files_per_save` and `device_server`

Probe-based (event-based) backups

You can configure NMSAP probe-based (event-based) scheduled backups to be triggered when the system meets specific conditions within a scheduled backup window. You can specify the conditions by the number of transaction (archived) logs that are generated, or by the time that has elapsed since the previous probe-based backup. NMSAP also supports user-defined probes.

NMSAP does not support probe-based backups for Oracle snapshot backups with NetWorker Snapshot Management (NSM).

Snapshot-based backups and restores

Snapshot technology provides enhanced protection and improved availability of data and greatly reduces the use of resources on the production host to perform backups.

Snapshot backups of Oracle data with NMSAP create point-in-time (PIT) copies of production data on primary storage devices, such as VMAX (Symmetrix), VNX Block (CLARiiON), and XtremIO.

You can optionally perform a clone operation after a snapshot backup, to create a cloned copy of the snapshot data on conventional storage, such as a Data Domain device or tape.

NMSAP supports two types of snapshot-based backups and restores:

- Snapshot backups and restores that use the NetWorker Snapshot Management (NSM) feature. If you use the NSM feature, you can restore from either a snapshot or a cloned copy of a snapshot. [NMSAP Oracle Snapshot Backups and Restores](#) on page 155 provides details.

Note

An NSM backup is supported through a scheduled backup. A ProtectPoint backup with NSM is the only type of NSM backup that is also supported through a manual backup.

- Split-mirror backups and restores that use user-created scripts working with any other software that supports the BR*Tools split-mirror backup interface. If you use the split-mirror feature, you can restore from conventional storage only. [NMSAP Oracle Split-Mirror Backups and Restores](#) on page 173 provides details.

You can optionally configure an NSM snapshot backup as a Client Direct backup. By default, NMSAP with NSM tries to use the Client Direct feature for both of the following operations:

- Rolling over the snapshot to conventional storage during a snapshot and clone backup
- Restoring from conventional storage during a restore from clone

If a proxy host (mount host) is used, Client Direct operations occur between the proxy host and the device. If a Client Direct operation is not possible, then the backup or restore is automatically routed through the storage node.

Restartable backups

NMSAP supports scheduled and manual restartable backups of Oracle data through the NetWorker checkpoint restart feature and the SAP BR*Tools `brbackup -fillup <bkup_log>` option. This option enables you to restart an NMSAP client backup from a known good point that is called a checkpoint. During the restarted backup, NMSAP does not back up files that were successfully backed up during the failed backup.

NMSAP scheduled restartable backups require SAP BR*Tools version 7.10 or later. The manual restartable backups work with all the supported NetWorker and BR*Tools versions.

For NMSAP restartable backups, the checkpoint granularity is at the save set level. When you restart a backup, a successfully completed save set from the prior failed backup is not backed up, but a failed save set is backed up.

The NetWorker concept of a partial save set does not apply to NMSAP restartable backups. An NMSAP save set cannot exist in a partial state. Either the save set completes in its entirety or is marked as failed. You can achieve NMSAP checkpoint granularity by dividing the SAP data into several save sets, where the number of save sets is greater than the backup parallelism.

Note

The checkpoint ID of an NMSAP restarted backup is not displayed in the NMC GUI under **Media > Disk Volumes > *targeted_backup_volume* > Volume Save Sets**.

You might need to run `brrestore` multiple times to complete a restore from checkpoint restarted backups if the original backup was completed with multiple restarts.

Cluster and Oracle RAC support

NMSAP supports backups and restores of Oracle operating system cluster and Oracle Real Application Clusters (RAC) systems.

Directory backups and restores

NMSAP supports backups and restores of nondatabase files and directories through the following commands:

```
brbackup -m {sap_dir | ora_dir | all_dir | full_directory_path}
brrestore -m full_directory_path
```

Note

Due to an issue in the SAP BR*Tools interface, you cannot back up directories and files with names that contain white space. The SAP note 898787 provides more details on this issue.

The restore granularity of a directory backup that is performed with the `brbackup` command is the entire directory. You cannot restore a subset of files from a directory backup.

NMSAP supports the following four directory backup modes that the SAP BR*Tools suite provides:

- `sap_dir`—This mode backs up SAP-related directories, including the following directories:
 - `/sapmnt/DBSID`
 - `/usr/sap/DBSID`
 - `/usr/sap/trans`
- `ora_dir`—This mode backs up `$ORACLE_HOME` with the exception of the following subdirectories, if they exist:
 - `$ORACLE_HOME/sapdatan`
 - `$ORACLE_HOME/origlog`
 - `$ORACLE_HOME/mirrlog`
- `all_dir`—This mode combines the `sap_dir` and `ora_dir` modes.
- `full_directory_path`—This mode backs up the user-specified directory.

You can perform a directory backup as either a manual backup or a scheduled backup that is configured with the `nonwizard` method.

Note

NMSAP does not support a scheduled directory backup that is configured with the `wizard` method.

Back up nondatabase files and directories only after an SAP upgrade or Oracle upgrade. Directory backups with NMSAP are not a replacement for file system backups. To protect the file system environment, use the NetWorker file system interface.

Run backups of nondatabase files and directories separately from database backups. Create a separate Client resource for the backup of nondatabase files and directories.

Oracle ASM and Exadata support

NMSAP supports Oracle Automatic Storage Management (ASM) and Oracle Exadata through the BR*Tools RMAN interface only.

NMSAP supports Oracle Exadata in both of the following configurations:

- Exadata Database Machine
- Exadata Storage Server, attached to an external database server

NMSAP supports the same environment for Oracle Exadata (including the Oracle database versions, operating system versions, BR*Tools versions, and NetWorker versions) that NMSAP supports for Oracle RAC. The *NetWorker E-LAB Navigator* at <https://elabnavigator.emc.com/eln/elhome> describes the environment support.

Install and configure NMSAP on each Exadata database server in the same way that you install and configure NMSAP for Oracle RAC. The installation and configuration procedures are described in both the *NetWorker Module for SAP Installation Guide* and this administration guide.

To perform backups and restores of Exadata, follow the instructions for Oracle RAC environments in this administration guide.

If the Oracle Exadata database servers are connected to a NetWorker remote storage node, then the following requirements apply to the connection:

- The only supported protocol is IP, over InfiniBand or other networks like Ethernet. Native InfiniBand or any protocol other than IP is not supported.
- There could be multiple network interfaces on the Oracle Exadata database servers to the storage node, such as one for an InfiniBand connection and one for an Ethernet connection. In such a case, configure the network settings and the NetWorker Client resource to send the backup data from the Oracle Exadata server to the remote storage node over the preferred network, such as InfiniBand. The configuration details are available in the NetWorker documentation.

Internationalization with NMSAP Oracle

NMSAP Oracle provides internationalization (I18N) support that enables you to monitor, back up, and restore non-ASCII data from NMSAP clients. For example, a NetWorker server with an ASCII locale can view and manage backups from an NMSAP client with a Chinese locale. Also, a NetWorker server with a Chinese locale can view and manage backups from an NMSAP client with an ASCII locale.

Note

I18N support is distinguished from localization (L10N) support, in which the software user interface and operational messages are translated into localized languages. This NMSAP release does not provide L10N support.

I18N support assumes the use of NMSAP with the following I18N products:

- Internationalized operating system
- Unicode version of BR*Tools
- NetWorker server and client that support I18N

Note

NMSAP support of non-ASCII environments is limited by the I18N support that is provided by Oracle, BR*Tools, the NetWorker client, and the underlying operating system.

You must configure I18N support according to [Configuring I18N support](#) on page 88.

Support of non-ASCII characters

The NMSAP client supports non-ASCII characters for the following items:

- Full pathnames of the parameter file and configuration file, for example, `initDBSID.utl`.
- Full pathnames of the operational log files, for example, SAPBACKUP and SAPTRACE.
- Full pathnames of variables set in the `nsrsapsv.cfg` file, for example, `PATH`, `SAP_BIN`, `SAPTRACE`, and `SAPSWITCH`.

- Most strings that are passed as command line options to the NMSAP programs `nsrsapadm`, `nsrsapsv`, and `backint`. Exceptions are the Oracle username and password, which is an Oracle limitation, and the full pathname of the NMSAP scheduled backup configuration file (`nsrsapsv.cfg`), which is a NetWorker server limitation. [ASCII-only characters](#) on page 33 provides details.
- All NetWorker parameters that the NetWorker software supports.
- Environments that the scheduled backup wizard configures.

Note

The `NLS_LANG=AMERICAN.AMERICA.US7ASCII` parameter value is an example value or default value. This parameter setting occurs in the sample backup configuration file (`nsrsapsv.cfg`) that is shipped with the product or generated by the NMSAP wizard. You can change this setting to another value. The SAP documentation describes how to set the `NLS_LANG` parameter.

ASCII-only characters

Some Oracle, BR*Tools, and NetWorker software configuration settings that are used with the NMSAP client do not support I18N and must use ASCII characters. Read the product documentation for complete details.

Examples of ASCII character requirements are as follows:

- Oracle requires ASCII characters for the following items:
 - `ORACLE_HOME` environment variable
 - Oracle database instance name *DBSID*
- BR*Tools requires ASCII characters for the following items:
 - Connection strings (database username and password) to the SAP Oracle database
 - Oracle datafiles, log files, control files, parameter file names
 - Oracle tablespace names
 - `SAPARCH`, `SAPBACKUP`, `SAPCHECK`, and `SAPREORG` variable settings in the `nsrsapsv.cfg` file
- NetWorker software and NMSAP require ASCII characters for the following items:
 - NetWorker client, server, pool, and expiration policy parameters, which are set in the NMSAP parameter file (`initDBSID.utl`)
 - NMSAP scheduled backup configuration file (`nsrsapsv.cfg`) pathname, which is passed to the Backup Command attribute in the NetWorker Client resource

NMSAP Oracle recovery wizard

NMSAP Oracle supports the Oracle recovery wizard, which is a Java application that you run from NMC to configure and run an SAP with Oracle restore and recovery. If the wizard supports the environment, use the wizard whenever possible to perform the SAP with Oracle restore and recovery operations.

You can run the recovery wizard from the NetWorker Console Administration window, which you can start on any supported host by using a web browser session and by specifying the Console server URL.

The NMSAP Oracle recovery wizard can configure and run the following types of restore and recovery:

- Complete database recovery to the time of the failure, with only the needed files being restored.
- Whole database reset to the time of the selected backup (online backups excluded).
- Point-in-time recovery of a whole database or restore of selected tablespaces.
- Restore of selected datafiles or tablespaces only, including a relocation of data if required.
- Restore and recovery of SAP Oracle data to a different database on either the same host or a different host, by using backups of the original database.

Note

The recovery wizard does not support the restore and recovery of a database to a different database instance on a different host.

The NMSAP recovery wizard enables you to start a restore or recovery immediately or schedule the operation to start at a future time.

The NMSAP recovery wizard does not support the following features:

- Cluster or Oracle RAC systems
- Oracle RMAN recovery

The following additional sources describe the wizard:

- Descriptive inline text in the wizard
- Online help in the wizard
- *NetWorker Module for SAP Release Notes*

Secure storage password and role-based secure storage

SAP Kernel 7.20 Patch Level 100 introduced a new method for the secure storage of the SAP database user or password to improve the security of database connections. With BR*Tools Kernel 7.20 Patch 27 or later, you can avoid using the OPS\$ database users. You can store the BR*Tools connection data for the database in a BR*Tools specific Secure Storage in File System (SSFS).

The SAP Note 1764043 provides details about how to configure the storage of the BR*Tools user or password in secure storage.

Note

An NMSAP backup does not save the SSFS data. If the SSFS data becomes unavailable, you can restore the data by using other configured authentication methods, such as database authentication or OS authentication. Alternatively, you can rerun the procedure to store the database user and password securely.

You can enable the secure storage password for NMSAP backups by setting `NSR_BRTOOLS_SECURE_PASSWORD=TRUE` in the `nsrsapsv` configuration file or in the wizard. This setting causes the BR*Tools binaries `brbackup` and `brarchive` to run with the `-u //` option.

With BR*Tools Kernel 7.20 Patch 30 or later, you can also use role-based storage of the BR*Tools user and password in the secure storage. This storage assigns the DBA and OPER roles to OS users without the OS users having to belong to the Oracle OS groups `dba` and `oper`.

OS users who are configured for role-based storage must perform the DBA action only with the BR*Tools. Typically, OS users can call all the BR*Tools programs with the

DBA role. OS users with the OPER role can call only `brarchive`, `brbackup`, and `brconnect`. The SAP Note 1764043 provides details about how to configure the role-based storage of the BR*Tools user and password in secure storage.

You can enable role-based secure storage for NMSAP backups by setting `NSR_BRTOOLS_SECURE_ROLE=OS_group_name` in the `nsrsapsv` configuration file or in the wizard, where `OS_group_name` is the name of the OS group that is configured for secure storage. This setting causes the BR*Tools binaries `brbackup` and `brarchive` to run with the `-u //OS_group_name` option.

Note

If you enable both the secure storage password and role-based secure storage for NMSAP backups, then the secure storage password setting takes precedence.

Do not specify database authentication with the `nsrsapadm` command if you have set the `NSR_BRTOOLS_SECURE_PASSWORD` or `NSR_BRTOOLS_SECURE_ROLE` parameter. Database credentials are ignored if either of these parameters is set.

You can use different authentication methods during backups and restores, provided that all the authentication methods are configured according to the SAP and Oracle documentation. For example, you can back up by using the secure role method and then restore by using database authentication.

Simplified scheduled backup configuration of multiple databases

NMSAP Oracle supports the scheduled backup of multiple databases on the same client host by using a single NetWorker Client resource.

When you configure a scheduled backup without the wizard, you can specify multiple databases in the Save Set attribute of a single Client resource. You do not need to configure a separate Client resource for each database.

When you use a single Client resource for multiple databases, you also use a single NMSAP configuration file, `nsrsapsv.cfg`, and specify unique parameter settings for each database. You can still use multiple `initDBSID.utl` files for the backup.

The following settings determine whether NMSAP backs up the multiple databases simultaneously or sequentially:

- Parallelism attribute setting in the NetWorker Client resource.
- `NSR_PARALLELISM` parameter setting.
- Setting of the number of backup sessions/channels in the backup configuration wizard.

During NetWorker scheduled backups, if the number of current running backup sessions is greater than the Parallelism attribute setting in the NetWorker Client resource, a newly started scheduled backup runs sequentially. The *NetWorker Administration Guide* provides details about the NetWorker client parallelism.

Virtualization support

NMSAP supports several types of virtualization software, such as VMware, Solaris zones, and Microsoft Hyper-V. The *NetWorker E-LAB Navigator* at <https://elabnavigator.emc.com/eln/elhome> provides details about supported environments and platforms.

Note

Install NMSAP in a guest operating system.

VMware support

NMSAP supports regular backups and restores of SAP Oracle databases on a VMware virtual machine (VM) on an ESX server.

NMSAP also supports the following advanced features of a VMware ESX server:

- **VMotion**—The VMotion feature enables migration of virtual machines from one ESX server to another while the servers are on. The migration is seamless to the applications that run on the virtual machines so users do not experience disconnections. The backup or restore remains uninterrupted if a migration occurs during an NMSAP backup or restore. VMware documentation describes the virtual machine requirements for VMotion.
- **Distributed Resource Scheduler (DRS)**—The DRS feature enables dynamic balancing and allocation of resources across multiple ESX servers. Depending on the DRS policies set by the user, the DRS can migrate a virtual machine or recommend that users migrate a virtual machine to a different ESX server by using VMotion. DRS can also start (at boot-up) a virtual machine on a different ESX server. If a migration occurs during an NMSAP backup or restore, the backup or restore remains uninterrupted because this feature uses VMotion.
- **High Availability (HA)**—The HA feature enables the restart of VMware on the same ESX server, on a different ESX server, or on a physical machine, depending on the type of VMware cluster configured. During a restart, users are disconnected and must reconnect.
If a restart occurs during an NMSAP backup or restore, the backup or restore fails:
 - Manually restart a manual backup or restore when the guest operating system restarts.
 - For a scheduled backup, the NetWorker server retries the backup if the Retries setting in the backup action resource has a nonzero value.

Solaris zones support

NMSAP supports Solaris global zones, whole root zones, and sparse root zones. The *NetWorker Module for SAP Installation Guide* provides installation details for sparse root zone environments.

NMSAP and associated software

NMSAP works with different types of software in an NMSAP environment: NetWorker, SAP server, SAP HANA database system, Oracle server.

NetWorker software

The NetWorker software provides services to protect an enterprise against data loss. The basic NetWorker products include the NetWorker server, client, storage node, and the NetWorker Management Console (NMC).

The NetWorker Snapshot Management (NSM) feature is in the NetWorker extended client package. NMSAP can use NSM to create a snapshot (point-in-time) copy of SAP Oracle data on a client host, which serves as a snapshot backup. NMSAP can then back up the snapshot to conventional storage.

Note

NMSAP does not support snapshot operations with an SAP HANA database system.

SAP server software

The SAP server software includes the BR*Tools utilities that NMSAP uses for the backup, restore, and inquiry of SAP Oracle databases. BR*Tools consist of `brbackup`, `brarchive`, `brrecover`, `brrestore`, and other utilities.

SAP HANA software

The SAP HANA database server software includes the SAP HANA utilities that NMSAP uses for the backup and restore of SAP HANA databases. The SAP HANA utilities include the SAP HANA CLI with the `hdbsql` command that is used to run backups. SAP GUIs, such as SAP HANA Studio, are also used for backups and restores.

Oracle server software

The Oracle software includes the RMAN utilities for backup, restore, and inquiry operations. The use of RMAN with NMSAP and BR*Tools software is optional because you can use the NMSAP `backint` program as the sole backup and restore software.

If you configure RMAN to back up SAP Oracle databases, the `backint` program also backs up the SAP configuration files, logs, and other files that RMAN does not back up. [Choosing either backint or RMAN as the backup and restore utility](#) on page 88 provides details.

NMSAP software components

The following table lists the NMSAP software components that are referenced in this guide. On Microsoft Windows systems, most of these files are in the directory `NetWorker_install_directory\nsr\bin`.

Table 3 NMSAP and associated software components

Component	Description
<code>backint[.exe]</code>	NMSAP program interface to SAP BR*Tools, which provides backup, restore, and inquire functionality.
<code>hdbbackint</code>	NMSAP program for SAP HANA operations, which provides backup, restore, inquire, and delete functionality.
<code>init_hana_nmsap.utl</code>	Configuration file template that specifies the variables that are used by the <code>hdbbackint</code> program for manual backups and restores of SAP HANA data, and for scheduled backups that are not configured through the wizard. Copy this template file and name the copied file <code>initDBSID.utl</code> , where <code>DBSID</code> is the name of the SAP HANA database instance to be backed up.

Table 3 NMSAP and associated software components (continued)

Component	Description
init_oracle_nmsap.utl	Configuration file template that specifies the variables that are used by the <code>backint</code> program for manual backups and restores of SAP Oracle data, and for scheduled backups that are not configured through the wizard. Copy this template file and name the copied file <code>initDBSID.utl</code> , where <code>DBSID</code> is the name of the SAP Oracle database instance to be backed up.
libnworasap.xx (UNIX) orasbt.dll, nsrsbtconsap.exe (Windows)	RMAN media management utilities.
man pages (UNIX only)	Reference for NMSAP commands.
nsrhanara hanara.jar hanara_res.jar	NMSAP scheduled backup configuration wizard files that are used for HANA backup configuration.
nsrsapadm[.exe]	NMSAP program that encrypts login information in the <code>nsrsapsv.cfg</code> file for the user who performs a scheduled backup through a client-side configuration.
nsrsapprobe[.exe]	Program that probes for the number of generated archived logs as a condition that triggers a probe-based backup.
nsrsapra[.exe] nsrsaprachild[.exe] sapra.jar sapra_res.jar	NMSAP scheduled backup configuration wizard files that are used for BR*Tools (Oracle) backup configuration.
nsrsaprc[.exe]	Recovery program that runs the BR*Tools executables for SAP Oracle.
nsrsapsv[.exe]	Scheduled backup program that runs the BR*Tools executables for SAP Oracle and the HANA <code>hdbsql</code> commands for SAP HANA.
nsrsapsv.cfg	Configuration file template for the <code>nsrsapsv</code> scheduled backup program for backups that are not configured through the wizard. Copy this template file and save the original file with its default settings. On UNIX, this file is in the <code>/etc</code> directory.
nwsldreg.xml	SAP Solution Manager registration file.

CHAPTER 2

Configuration for NMSAP HANA Operations

This chapter includes the following topics:

- [Configuration road map for SAP HANA operations](#)..... 40
- [Verifying the NMSAP software requirements](#)..... 40
- [Configuring scheduled backups with the wizard](#)..... 41
- [Configuring scheduled backups without the wizard](#)..... 45
- [Configuring manual backups](#)..... 62
- [Configuring automatic backups of SAP HANA redo logs](#)..... 62
- [Configuring Data Domain Boost backups](#)..... 63
- [Configuring CloudBoost backups](#)..... 66
- [Configuring NMSAP backups to AFTD storage](#)..... 68

Configuration road map for SAP HANA operations

Use the following instructions to configure the NMSAP software for the SAP HANA data operations.

Procedure

1. [Verifying the NMSAP software requirements](#) on page 40.
2. To configure either scheduled or manual backups, use the following instructions:
 - [Configuring scheduled backups with the wizard](#) on page 41.
 - [Configuring scheduled backups without the wizard](#) on page 45.
 - [Configuring manual backups](#) on page 62.
3. [Configuring automatic backups of SAP HANA redo logs](#) on page 62.
4. [Configuring Data Domain Boost backups](#) on page 63 (only for backups to DD Boost devices).
5. [Configuring NMSAP backups to AFTD storage](#) on page 68 (only for backups to AFTD devices).

Verifying the NMSAP software requirements

Verify that the NMSAP software environment meets the basic requirements.

Procedure

1. Ensure that you have correctly installed and configured the SAP HANA software before you configure the NMSAP environment. The SAP documentation provides instructions.

Note

On the SAP HANA server with HANA 2.0 or later, ensure that you install the SAP host agent package manually. Otherwise, the NMSAP configuration wizard cannot find the SAP HANA instance.

2. Ensure that you have installed and enabled the NetWorker client software and NMSAP on each SAP HANA server that requires backup and recovery services. The platform-specific NetWorker installation guide and the *NetWorker Module for SAP Installation Guide* provide instructions.

3. Ensure that you have configured the basic NetWorker resources on the NetWorker server to enable backups and restores. The basic resources include the NetWorker Server resource, Client resource, Device resource, and the Pool and Label Template resources.

Ensure that the following storage resources are configured:

- Storage node that owns the backup storage devices.
- Backup storage devices.

Configure a Device resource for each supported storage device that is used for backups and restores.

- Label templates for labeling the backup volumes.

- Media pools for sorting and storing the backup data.

Configure the volumes in each Pool resource to receive specific types of backup data, such as tablespaces or archived logs. In the Pool resources, leave the Save Sets attribute blank because NMSAP sets the Save Sets during each backup.

The *NetWorker Administration Guide* provides details on how to configure NetWorker resources.

4. Ensure that you have granted the NetWorker server User Group resource privileges to the SAP user who performs the SAP HANA operations. You can set the User Group resource with NMC or the `nsradmin` program. If you use restricted datazones (RDZs), then you can also grant the required privileges by using the Users and Privileges fields of the RDZ resource. The *NetWorker Administration Guide* provides details.

The SAP user requires specific privileges:

- To run backups and restores, you must have the following default privileges:
 - Monitor NetWorker
 - Back Up Local Data
 - Recover Local Data
 - To review backup information in NetWorker indexes, for example, with the `nsrinfo` and `mminfo` commands requires the Operate NetWorker privilege.
 - To configure a backup, you must have the Configure NetWorker privilege.
 - To delete a backup from the NetWorker server requires the Change Application Settings privilege and any prerequisite privileges.
5. If you use a firewall, then ensure that you have ensured NMSAP connectivity. Configure the corresponding ports for the NetWorker server as required.

The *NetWorker Administration Guide* provides details.

Configuring scheduled backups with the wizard

You can create or modify a scheduled backup configuration with the NMSAP wizard.

Before you begin

Ensure that you meet the following requirements before you use the configuration wizard:

- You have installed the required NetWorker releases on the NMC server, NetWorker server, and NMSAP client hosts as described in the *NetWorker E-LAB Navigator*.
- On the NetWorker server that contains the configuration, the NMC user that starts the wizard (the wizard user) has the Configure NetWorker privilege and all its prerequisite privileges.
- Communication between the NMC server, NetWorker server, and NMSAP client uses NetWorker `nsrauth` authentication. The NetWorker documentation provides the requirements for `nsrauth` authentication.
- You have configured the NMSAP software environment as described in [Verifying the NMSAP software requirements](#) on page 40.

- If a user store key is used in the scheduled backup, then either the root user or a non-root user has created the user store key. You create a user store key with the SAP HANA `hdbuserstore` tool, as described in the SAP HANA documentation. The credentials that are provided in the user store key are the credentials of a user that has SAP HANA backup privileges, such as the SYSTEM user. In the **hdbsql user** field in the wizard, specify the user that created the key. This user runs the `hdbsql` program during the scheduled backup.

Procedure

1. In the NMC **Enterprise** window, right-click the NetWorker server name, and then select **Launch Application**.

The *NetWorker Administration Guide* provides details on how to access the NMC interfaces.

2. In the **Administration** window, click **Protection**.
3. Start the wizard by using the proper method:
 - To create a NetWorker Client resource for NMSAP, right-click **Clients** in the left pane and then select **New Client Wizard**.
 - To modify a NetWorker Client resource that was previously created with the wizard for NMSAP, right-click the client name in the right pane and then select **Modify Client Wizard**.
4. On each wizard page that appears, specify the options and values that are required for the backup configuration. Each wizard page includes an online help button that you can click to access descriptions of the fields and options on the page.

You can click a link in the wizard steps panel to go directly to the page that you want to modify. The number of steps that are shown in the steps panel varies according to the chosen configuration type.

Note

To specify that a dynamically generated timestamp is appended to the backup prefix for a HANA backup, select **Append the timestamp to the backup file prefix** on the **Specify the SAP HANA Information** page in the wizard.

5. On the wizard page titled **Client Configuration Summary**:
 - To create the configuration, click **Create**.
 - To modify the configuration, click **Back**.

After you finish

After you complete the backup configuration with the wizard, ensure that a data protection policy is also configured on the NetWorker server to define the backup workflow and other required settings for the scheduled backup. [Configuring the data protection policy with NMC](#) on page 57 provides details.

Configuring scheduled backups with the wizard for SAP HANA delta backups

NMSAP supports SAP HANA delta backups. When you use the NMSAP wizard to configure a scheduled backup of SAP HANA data, you can specify the backup level in the Policy Action Wizard in NMC.

If the backup level is unspecified, NMSAP performs a full backup only when a previous full backup does not exist. Otherwise, NMSAP performs an incremental backup that anchors to the last full backup.

The following table shows the SAP HANA backup levels and the corresponding backup levels with the NetWorker server 9.1 or later.

Table 4 Mapping of SAP HANA and NetWorker backup levels

SAP HANA backup levels	NetWorker backup levels
full	Full
differential	Cumulative Incr
incremental	Incr

Configuring scheduled backups with the wizard in an SAP HANA MDC system

When you use the NMSAP wizard to configure a scheduled backup in an SAP HANA MDC system, you can configure the backup on the individual database level.

You can configure the following backups in the typical and custom backup workflows:

- In the **Typical scheduled backup** workflow, you can either back up the whole database system with the specified SID or back up a single tenant database with the local administration privileges.
- In the **Custom scheduled backup** workflow, you can select any databases to back up from the specified database system.

You must specify the correct type of credentials for the preferred backup type:

- For a scheduled backup of the SYSTEMDB database and any number of tenant databases, specify the credentials of the system database administrator.

These credentials provide the access and backup privileges to the SAP HANA SYSTEMDB database. You then select the databases for backup in the wizard. All the databases are backed up through a single NetWorker client resource.

- For a scheduled backup of a single tenant database, specify the credentials of the tenant database administrator.

These credentials provide the access and backup privileges to the particular tenant database. You then specify the name of the tenant database for backup in the wizard.

To configure the preferred type of MDC database backup, follow the NMSAP wizard procedure in the preceding topic and complete the following additional steps.

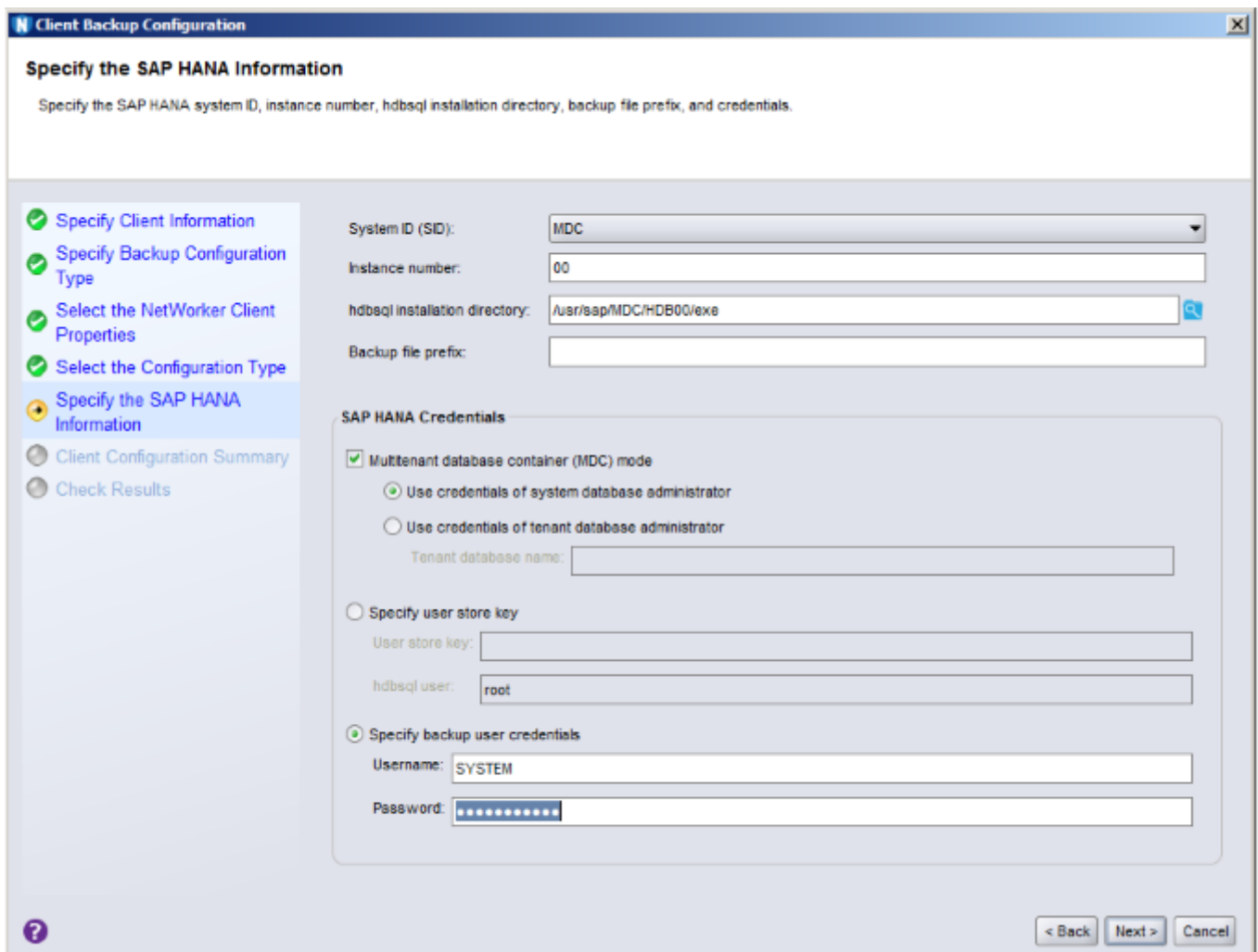
Procedure

1. On the **Select the Configuration Type** page, select the required type of backup configuration:
 - **Typical scheduled backup**

- **Custom scheduled backup**
2. On the **Specify the SAP HANA Information** page:
 - a. Select **Multitenant database container (MDC) mode**.
 - b. Select one of the following credential options:
 - **Use credentials of system database administrator**
 - **Use credentials of tenant database administrator**
 - c. If you selected to use the credentials of the tenant database administrator, type the tenant database name in the **Tenant database name** text box.
 - d. Select **Specify backup user credentials**, and then complete the **Username** and **Password** text boxes for the system database administrator or tenant database administrator as required.

The following example shows the wizard fields on the **Specify the SAP HANA Information** page for the configuration of a scheduled backup of multiple MDC databases.

Figure 1 Configuration wizard fields for a scheduled backup of MDC databases



3. (Custom scheduled backup only) On the **Select the Databases (Optional)** page, select the MDC databases for the backup.

Configuring scheduled backups without the wizard

As an alternative to the wizard configuration, you can create or modify a scheduled backup configuration by performing the following tasks.

Procedure

1. [Setting up the NMSAP parameter file and configuration file](#) on page 45
2. [Configuring parallelism for SAP HANA operations](#) on page 56
3. [Enabling the parameter file in SAP HANA Studio](#) on page 57
4. [Configuring the data protection policy with NMC](#) on page 57

Results

The NMC interface provides NetWorker Device, Media Pool, and other resource settings that are not available in the wizard.

If a user store key is used in the scheduled backup, then either the root user or a non-root user has created the user store key. You create a user store key with the SAP HANA `hdbuserstore` tool, as described in the SAP HANA documentation. The credentials that are provided in the user store key are the credentials of a user that has SAP HANA backup privileges, such as the SYSTEM user. Specify the user store key in the `HANA_USR_KEY` parameter in the `nsrsapsv` configuration file. If a non-root user creates the key, then specify this user in the `HANA_OS_USR` parameter. The user that created the key runs the `hdbsql` program during the scheduled backup. The required `nsrsapsv` parameters are described in the following topic.

Setting up the NMSAP parameter file and configuration file

For all SAP HANA operations except scheduled backups that are configured with the wizard, set the required parameters in the `hdbbackint` parameter file on the NMSAP client as described in [NMSAP hdbbackint parameters](#) on page 45.

For scheduled backups configured without the wizard, also set the required parameters in the `nsrsapsv` configuration file on the NMSAP client as described in [NMSAP nsrsapsv parameters](#) on page 52.

Note

For scheduled backups configured with the wizard, you do not need to set any parameters. The configuration wizard sets all the required parameters in the NetWorker Client resource attributes.

NMSAP hdbbackint parameters

The parameters in the `hdbbackint` parameter file provide the client, server, pool, deduplication, parallelism, and other values to the NMSAP `hdbbackint` program.

Make a copy, such as `initDBSID.utl`, for your own use of the original parameter file template, `/etc/init_hana_nmsap.utl`, installed with NMSAP. Then you can customize the parameters in the copied file for the SAP HANA operations.

Note

When you uninstall NMSAP, the system deletes the original template file and any settings you made in the file.

NOTICE

If you use this file for scheduled backups, you do not need to set the `NSR_SERVER` parameter in the file. However, if you do set the parameter, the parameter setting on the NetWorker server takes precedence.

To set parameters in your copy of the `hdbbackint` parameter file, `initDBSID.utl`, use the following format:

```
parameter=value
```

Follow these guidelines:

- To use parameters, uncomment and modify the parameters as required.
- Parameter names and values are case-sensitive.
- Set all mandatory parameters.
- If you do not set an optional parameter, the default value of the parameter is used.

The following table describes the `hdbbackint` parameters that NMSAP supports.

Table 5 Supported `hdbbackint` parameters

Parameter	Description	Default and valid values
<code>DDBOOST_COMPRESSED_RESTORE</code>	<p>Specifies whether to perform a compressed restore that uses the DD Boost workflow. A compressed restore uses less bandwidth by restoring the backed-up data in a compressed form from the Data Domain system to the application host.</p> <p>A compressed restore can be beneficial in a constrained bandwidth environment, but may impact the restore performance due to the usage of compression resources on the Data Domain system and application host.</p> <p>Optional for a restore through the command line.</p>	<ul style="list-style-type: none"> • FALSE (default) = Do not perform a compressed restore that uses the DD Boost workflow. • TRUE = Perform a compressed restore that uses the DD Boost workflow.
<code>NSR_AES_ENCRYPTION</code>	<p>Specifies whether to encrypt backup data with 256-bit AES encryption.</p> <p>Optional for a backup.</p> <p>Setting this parameter to TRUE excludes the use of the <code>NSR_COMPRESSION</code> and <code>NSR_CHECKSUM</code> parameters, which you must set to FALSE. If you set more than one of these parameters to TRUE, the priority order is: <code>NSR_COMPRESSION</code>, <code>NSR_CHECKSUM</code>, <code>NSR_AES_ENCRYPTION</code>.</p> <p>NOTICE</p> <p>If the encryption phrase has changed between the time of the backup and the time when the backup is restored, <code>NSR_ENCRYPTION_PHRASES</code> must include the original phrase to enable the recovery.</p>	<ul style="list-style-type: none"> • FALSE (default). • TRUE.

Table 5 Supported `hdbbackint` parameters (continued)

Parameter	Description	Default and valid values
<code>NSR_CHECKSUM</code>	<p>Specifies whether to perform a cyclic redundancy check (CRC) on the backup data.</p> <p>Optional for a backup.</p> <p>Setting this parameter to TRUE excludes the use of the <code>NSR_AES_ENCRYPTION</code> and <code>NSR_COMPRESSION</code> parameters, which you must set to FALSE. If you set more than one of these parameters to TRUE, the priority order is: <code>NSR_COMPRESSION</code>, <code>NSR_CHECKSUM</code>, <code>NSR_AES_ENCRYPTION</code>.</p>	<ul style="list-style-type: none"> FALSE (default). TRUE.
<code>NSR_CLIENT</code>	<p>Specifies the NetWorker client hostname to use for the client file index for the current backup or restore.</p> <p>Mandatory for an SAP HANA scale-out environment. Select one node to use for the client file index, such as the master node.</p>	<ul style="list-style-type: none"> Local physical host (default). Valid NetWorker client hostname.
<code>NSR_COMPRESSION</code>	<p>Specifies whether to compress the data during a backup before the data passes over the network or is written to the backup device. The compression can speed up the backup process. Compression increases CPU usage on the SAP server, but reduces the amount of data that is sent to the NetWorker storage node.</p> <p>Optional for a backup.</p> <p>NMSAP supports only the default NetWorker encryption algorithm. NMSAP does not support backup compression with GZIP or BZIP2.</p> <p>Setting this parameter to TRUE excludes the use of the <code>NSR_AES_ENCRYPTION</code> and <code>NSR_CHECKSUM</code> parameters, which you must set to FALSE. If you set more than one of these parameters to TRUE, the priority order is: <code>NSR_COMPRESSION</code>, <code>NSR_CHECKSUM</code>, <code>NSR_AES_ENCRYPTION</code>.</p>	<ul style="list-style-type: none"> FALSE (default). TRUE.
<code>NSR_DATA_DOMAIN_INTERFACE</code>	<p>Specifies the network interface to use to send backup data to the DD Boost device. Optional for a manual backup only.</p> <p>Set this parameter if you have a Fibre Channel (FC) connection to the DD Boost device. Set this parameter together with <code>NSR_DEVICE_INTERFACE=DATA_DOMAIN</code>. If you do not set <code>NSR_DEVICE_INTERFACE</code> to <code>DATA_DOMAIN</code>, then this parameter is ignored.</p>	<ul style="list-style-type: none"> IP (default) = Backup data is sent over an IP network to the DD Boost device. Any = Backup data is sent over either an IP or FC network to the DD Boost device, depending on the available device. Fibre Channel = Backup data is sent over an FC network to the DD Boost device.

Table 5 Supported `hdbbackint` parameters (continued)

Parameter	Description	Default and valid values
<p>NSR_DATA_VOLUME_POOL</p>	<p>Specifies the NetWorker Media Pool resource, which is defined on the NetWorker server and receives backup data from the SAP HANA server.</p> <p>Optional for a manual backup.</p> <hr/> <p>Note</p> <p>This parameter is ignored for a scheduled backup.</p> <p>If required, specify the associated storage node by setting the Storage Nodes attribute in the NetWorker Client resource (NMC diagnostic mode must be enabled).</p> <hr/> <p>To use different pools for a database backup and log backup:</p> <ol style="list-style-type: none"> 1. Create two separate <code>initDBSID.utl</code> parameter files, one for the database backup and one for the log backup. 2. Set this pool parameter to a different NetWorker Media Pool resource in each of the two parameter files. 3. In the SAP HANA Studio GUI, on the Configuration tab of the Backup editor: <ol style="list-style-type: none"> a. Clear the checkbox beside Use the same parameter file for data backup and log backup. b. Type the corresponding parameter file name in the Backint Parameter File text box under both Data Backup and Log Backup. 	<ul style="list-style-type: none"> • Most appropriate pool, which the NetWorker server selects (default). • Valid name of a NetWorker volume pool.
<p>NSR_DEBUG_LEVEL</p>	<p>Specifies the level of debug messages that <code>hdbbackint</code> writes to the debug log file.</p> <p>Optional for a backup or restore.</p>	<ul style="list-style-type: none"> • 0 (default, no debugging). • 0 to 9.
<p>NSR_DEVICE_INTERFACE</p> <hr/> <p>Note</p> <p>This parameter is deprecated. It is supported in the current NMSAP release, but will be unsupported in a future release.</p> <hr/>	<p>Specifies whether the backup is always stored on the Data Domain device from the specified pool.</p> <p>Optional for a manual deduplication backup with the Data Domain media type only. Set the parameter when the backup pool contains a mixture of Data Domain devices and other types of devices. For example: AFTD, tape, and so on.</p> <hr/> <p>Do not set for a scheduled deduplication backup. Instead, set the Data Domain Backup attribute in the NetWorker Client resource when the pool has mixed devices for a scheduled deduplication backup.</p>	<ul style="list-style-type: none"> • Undefined (default) = Backup data might be stored on any device from the pool that NetWorker selects. • DATA_DOMAIN = Backup data is always stored on the Data Domain device.

Table 5 Supported `hdbbackint` parameters (continued)

Parameter	Description	Default and valid values
<code>NSR_DIAGNOSTIC_DEST</code>	<p>Specifies the directory of the <code>hdbbackint</code> diagnostic logs.</p> <p>Optional for a backup or restore.</p>	<ul style="list-style-type: none"> <code>/nsr/applogs/</code> (default on Linux). Valid directory pathname.
<code>NSR_DIRECT_ACCESS</code>	<p>Specifies the method that is used to perform a backup to a Data Domain device or an AFTD.</p> <p>Optional for a manual backup.</p> <p>If the target device is on a Data Domain system:</p> <ul style="list-style-type: none"> Data is deduplicated on the NMSAP client when the Client Direct feature is enabled. Data is deduplicated on the storage node when the Client Direct feature is disabled. <p>This parameter is ignored during scheduled backups with NetWorker server release 8.0 or later and during restores.</p> <p>For scheduled backups, you can enable the Client Direct feature with the Client Direct setting in the wizard or the Client resource.</p>	<ul style="list-style-type: none"> Default (default) = The backup tries to use the Client Direct feature to bypass the storage node and write data directly to the target device. If the backup cannot use this feature, then the backup uses the storage node. No = The backup does not try to use the Client Direct feature. The backup uses the storage node only. Yes = The backup tries to use the Client Direct feature. If the backup cannot use this feature, then the backup fails. <hr/> <p>Note</p> <p>The Yes value is deprecated. The value is supported in the current NMSAP release, but will be unsupported in a future release.</p>
<code>NSR_DPRINTF</code>	<p>Specifies whether NetWorker core debug messages are written to the NMSAP debug log file.</p> <hr/> <p>Note</p> <p><code>NSR_DPRINTF</code> applies only if <code>NSR_DEBUG_LEVEL</code> is set to a value greater than 0. Use this parameter for debugging purposes with assistance from Customer Support only.</p> <hr/> <p>Optional for a backup or restore.</p>	<ul style="list-style-type: none"> FALSE (default) = NetWorker core debug messages are not written to the NMSAP debug log file. TRUE = NetWorker core debug messages are written to the NMSAP debug log file.
<code>NSR_ENCRYPTION_PHRASES</code>	<p>Specifies the original phrase to enable the recovery. You can specify multiple phrases to try for the recovery.</p> <p>Mandatory if the <code>NSR_AES_ENCRYPTION</code> phrase has changed between the time of the backup and the time when the backup is restored.</p>	<ul style="list-style-type: none"> Encryption phrase from the Datazone Pass Phrase attribute in the NetWorker Server resource (default). Encryption phrase that is used at the time of the backup.
<code>NSR_NWPATH</code>	<p>Specifies the pathname of the directory that contains the NetWorker binaries.</p>	<ul style="list-style-type: none"> Platform-specific default location of the NetWorker client binaries (default).

Table 5 Supported `hdbbackint` parameters (continued)

Parameter	Description	Default and valid values
	<p>Recommended for a backup or restore if the NetWorker software is installed in a nondefault location.</p>	<ul style="list-style-type: none"> Valid pathname of the NetWorker software directory.
<p>NSR_PARALLELISM</p>	<p>Specifies the maximum number of concurrent data streams to send to or from the NetWorker server during a backup or restore, for each <code>hdbbackint</code> program that SAP HANA runs for the backup or restore.</p> <p>SAP HANA SPS 11 introduced the SAP HANA parameter <code>parallel_data_backup_backint_channels</code> that enables SAP HANA to split a data backup into multiple channels. NMSAP saves each SAP HANA channel as a separate save set, and each save set uses a single data stream. The NMSAP <code>NSR_PARALLELISM</code> parameter limits the maximum number of concurrent data streams, and new streams start when other streams complete. Configuring parallelism for SAP HANA operations on page 56 provides more details.</p> <p>The <code>parallel_data_backup_backint_channels</code> parameter does not apply to a restore. A restore uses the same number of streams as were used during the backup.</p> <hr/> <p>Note</p> <p>Prior to SAP HANA SPS 11, an SAP HANA backup always has a parallelism value of 1 per <code>hdbbackint</code> process. If the SAP HANA parameter <code>parallel_data_backup_backint_channels</code> is set in SAP HANA SPS 11 or later, the default value of this <code>NSR_PARALLELISM</code> parameter is 8.</p> <hr/> <p>Optional for a restore.</p> <p>With SAP HANA SPS 11 or later, optional for a backup.</p>	<ul style="list-style-type: none"> 8 (default). Positive integer number. <hr/> <p>Note</p> <p>For a scheduled backup, this parameter setting must be less than or equal to the Parallelism attribute value in the NetWorker Client resource. If multiple backups run concurrently on the client host, the total of all the <code>NSR_PARALLELISM</code> settings must be less than or equal to the Parallelism attribute value.</p> <p>During the recovery of an SAP HANA 2.0 backup, the value must be equal to or greater than the parameter value during the backup.</p> <hr/>
<p>NSR_RECOVER_POOL</p>	<p>Specifies the name of the NetWorker volume pool to use for a restore. You can use this option to restore data from a specified volume pool if there are multiple copies (clones) of the backup in different volume pools.</p> <p>Optional for a restore.</p>	<ul style="list-style-type: none"> Pool that the NetWorker server selects (default). Valid name of a NetWorker volume pool that contains a cloned backup to use for a restore.

Table 5 Supported `hdbbackint` parameters (continued)

Parameter	Description	Default and valid values
	<p>Note</p> <p>If required, specify the associated storage node by setting the Recover Storage Nodes attribute in the NetWorker Client resource (NMC diagnostic mode must be enabled).</p>	
NSR_SAVESET_NAME	<p>Specifies a suffix to use in the backup save set name.</p> <p>Optional for a manual backup.</p> <p>This parameter is ignored during scheduled backups.</p>	<ul style="list-style-type: none"> • <code>SID_data</code> for a data backup, <code>SID_log</code> for a log backup (default). The default save set names are as follows: <ul style="list-style-type: none"> ▪ SAPHANA:<code>SID_data</code> for a data backup ▪ SAPHANA:<code>SID_log</code> for a log backup • If <code>hdbbackint</code> cannot detect the backup type, then the default save set name is SAPHANA:<code>SID</code>. • Customized suffix to use in the save set name. The resulting save set name is as follows: SAPHANA:<code>user-specified_string</code>
NSR_SAVESET_RETENTION	<p>Specifies the date when the save set becomes recyclable and the associated data on the volume can be overwritten.</p> <p>Optional for a manual backup.</p> <hr/> <p>Note</p> <p>This parameter is ignored for a scheduled backup.</p>	<ul style="list-style-type: none"> • Retention policy that is specified in the NetWorker Client resource for the client (default). • Valid date in <code>nsr_getdate(3)</code> format.
NSR_SERVER	<p>Specifies the hostname of the NetWorker server that NMSAP uses.</p> <p>Mandatory for a manual backup, restore, or inquire operation.</p> <hr/> <p>Note</p> <p>You do not need to set this parameter for a scheduled backup, but if you set the parameter, the value must match the server that started the backup or an error occurs.</p>	<ul style="list-style-type: none"> • Local host (default). • NetWorker server hostname.

NMSAP nsrsapsv parameters

The `nsrsapsv` parameters provide environmental and other values to the NMSAP scheduled backup program, `nsrsapsv`.

You can use these parameters to perform the following operations among others:

- Specify the locations of required files and programs, such as `hdbsql`.
- Specify the SAP HANA database instance to back up.
- Specify the credential information that is required to log in to the database server and perform a scheduled backup.

You can set the parameters in the wizard or in the `nsrsapsv` configuration file for nonwizard configurations.

Make a copy, such as `nsrsapsv.cfg`, for your own use of the original configuration file template, `/etc/nsrsapsv.cfg`, installed with NMSAP. Then you can customize the parameters in the copied file for scheduled backups. Ensure that the configuration file has read permissions for the group and other users.

Note

When you uninstall NMSAP, the system deletes the original template file and any settings you made in the file.

To set parameters in your copy of the `nsrsapsv` configuration file, use the following format and guidelines:

- Use this format for each parameter setting:

```
parameter_name = parameter_value
```

- To use parameters in a scheduled backup, uncomment and modify the parameters as required.
- Parameter names and values are case-sensitive.
- Use full pathnames for parameters that specify a pathname or a file name.
- Specify the full pathname of the configuration file in the Backup Command attribute of the Client resource for the scheduled backup. [Configuring the Client resource without the wizard](#) on page 59 describes the Client resource attributes.

The following table describes the parameters in the `nsrsapsv` configuration file that NMSAP supports.

Table 6 Supported `nsrsapsv` parameters

Configuration parameter	Description	Default and valid values
DATABASES	<p>Depending on the TENANT_ADMIN setting, this parameter specifies the names of one or more databases to back up in an SAP HANA system that uses the multitenant database container (MDC) mode.</p> <p>If TENANT_ADMIN is FALSE and the system database administrator credentials are used, then set this parameter to one or more database names.</p>	<ul style="list-style-type: none"> • Undefined (default). • If TENANT_ADMIN= FALSE, one or more database names, separated by commas. For example: DATABASES=SYSTEMDB or DATABASES=DB0 or

Table 6 Supported `nsrsapsv` parameters (continued)

Configuration parameter	Description	Default and valid values
	If <code>TENANT_ADMIN</code> is <code>TRUE</code> and the tenant database administrator credentials are used, then set this parameter to the name of single tenant database.	<p>DATABASES=SYSTEMDB,DB0,DB1</p> <ul style="list-style-type: none"> If <code>TENANT_ADMIN</code>= <code>TRUE</code>, a tenant database name. For example: <code>DATABASES=DB0</code>
<code>HANA_BACKUP_PREFIX</code>	Specifies a prefix to use for the backup name. Optional for a scheduled backup that is configured without the wizard.	<ul style="list-style-type: none"> Undefined (default). Valid prefix for the backup name. For example: <code>MY_DATA_BACKUP</code>
<code>HANA_BIN</code>	<p>Specifies the pathname of the location of the <code>hdbsql</code> program file.</p> <p>Mandatory for a scheduled backup that is configured without the wizard.</p> <p>This location is added to the <code>PATH</code> environment variable so that the <code>hdbsql</code> program can be found.</p>	<ul style="list-style-type: none"> Undefined (default). Valid full pathname of the <code>hdbsql</code> program location. For example: <code>/usr/sap/SID/HDBnn/exe/</code> where <code>nn</code> is the database instance number
<code>HANA_DYNAMIC_PREFIX</code>	<p>Specifies whether to append a dynamically generated timestamp, in the form <code>YYYY_MM_DD_HH_MM_SS</code>, to the backup prefix for a scheduled backup. The timestamp is appended to the backup prefix before a HANA backup starts, which creates a unique identifier for the backup.</p> <p>Optional for a scheduled backup.</p>	<ul style="list-style-type: none"> <code>FALSE</code> (default) = A timestamp is not appended to the backup prefix. <code>TRUE</code> = A timestamp is appended to the backup prefix. If the backup prefix is not specified, then the timestamp is used for the backup prefix.
<code>HANA_INSTANCE</code>	<p>Specifies the instance number of the SAP HANA database for a backup.</p> <p>Mandatory for a scheduled backup that is configured without the wizard if the <code>HANA_USR_KEY</code> parameter is not set.</p>	<ul style="list-style-type: none"> Undefined (default). Valid instance number between 00 and 99.
<code>HANA_MDC</code>	<p>Specifies whether the SAP HANA database system for the backup is configured to use the MDC mode.</p> <p>Set this parameter to <code>TRUE</code> if you use the MDC mode.</p>	<ul style="list-style-type: none"> <code>FALSE</code> (default) = SAP HANA system is in the single container mode. <code>TRUE</code> = SAP HANA system is in the MDC mode.
<code>HANA_OS_USR</code>	<p>Specifies the name of the user that created the user store key to be used in the scheduled backup.</p> <p>Mandatory if a non-root user created the user store key that is specified in <code>HANA_USR_KEY</code>.</p>	<ul style="list-style-type: none"> <code>root</code> (default). Name of the user that created the user store key that is specified in <code>HANA_USR_KEY</code>.
<code>HANA_SID</code>	Specifies the system ID (SID) of the SAP HANA database.	<ul style="list-style-type: none"> Undefined (default). Valid SAP HANA SID.

Table 6 Supported `nsrsapsv` parameters (continued)

Configuration parameter	Description	Default and valid values
	Mandatory for a scheduled backup that is configured without the wizard.	
HANA_USR_KEY	<p>Specifies a user store key, which securely stores the SAP HANA database username, password, and instance number.</p> <p>Optional if the SAP HANA database user credentials are specified with the <code>HANA_USR_PASSWD</code> setting.</p>	<ul style="list-style-type: none"> • Undefined (default). • Valid user store key, created by the <code>HANA_OS_USR</code> user with the <code>SAP HANA hdbuserstore</code> tool. The credentials that are provided in the user store key must be the credentials of a user that has SAP HANA backup privileges, such as the <code>SYSTEM</code> user. The SAP HANA documentation provides details about the <code>hdbuserstore</code> tool.
HANA_USR_PASSWD	<p>Specifies an encrypted value that contains the username and password of the SAP HANA database user.</p> <p>Optional if the SAP HANA database user credentials are specified with the <code>HANA_USR_KEY</code> setting.</p>	<ul style="list-style-type: none"> • Undefined (default). • Uneditable encrypted value set by running the <code>nsrsapadm -P hana -z file_name</code> command as the root user, where <code>file_name</code> is the full pathname of the <code>nsrsapsv</code> configuration file. Follow the instructions from the <code>nsrsapadm</code> command to complete the encryption.
LD_LIBRARY_PATH	<p>Specifies the pathname of the SAP HANA 2.0 C++ runtime library.</p> <p>Optional for a SAP HANA backup.</p>	<ul style="list-style-type: none"> • <code>\$DIR_EXECUTABLE</code> (default). • Valid pathname of the C++ library as shipped by SAP.
PATH	<p>Specifies the pathname of the NetWorker client binary file and any other required search pathnames.</p> <p>Optional for a scheduled backup that is configured without the wizard.</p> <p>The specified value is appended to the <code>PATH</code> environment variable. To specify multiple search pathnames, use one of the following two methods:</p> <ul style="list-style-type: none"> • <code>PATH=d:\dir1;d:\dir2;d:\dir1\dir2\dir3</code> • <code>PATH=d:\dir1</code> <code>PATH=d:\dir2</code> <code>PATH=d:\dir1\dir2\dir3</code> 	<ul style="list-style-type: none"> • Undefined (default). • Valid pathnames that are separated by semicolons.
POSTCMD	Specifies a postprocessing script to run after a scheduled backup:	<ul style="list-style-type: none"> • Undefined (default). • Valid full pathname of a postprocessing script file. The

Table 6 Supported `nsrsapsv` parameters (continued)

Configuration parameter	Description	Default and valid values
	<ul style="list-style-type: none"> The postprocessing script file might need permissions that enable execution by the root user. The script must return a zero value when it succeeds, and a nonzero value when it fails. The first line of the script must contain the following interpreter directive: #!/bin/sh <p>Optional for a scheduled backup that is configured without the wizard.</p> <hr/> <p>Note</p> <p>If the scheduled backup fails, the postprocessing script still runs. If the postprocessing script fails, an error message appears but the scheduled backup succeeds.</p>	<p>pathname must not contain any spaces.</p> <ul style="list-style-type: none"> If the value is undefined or invalid, a postprocessing script does not run after the scheduled backup.
PRECMD	<p>Specifies a preprocessing script to run before a scheduled backup:</p> <ul style="list-style-type: none"> The preprocessing script file might need permissions that enable execution by the root user. The script must return a zero value when it succeeds, and a nonzero value when it fails. The return of a nonzero value causes the scheduled backup to fail. The first line of the script must contain the following interpreter directive: #!/bin/sh <p>Optional for a scheduled backup that is configured without the wizard.</p> <hr/> <p>Note</p> <p>If the preprocessing script fails, NMSAP does not perform a scheduled backup, an error message appears, and any postprocessing script does not run.</p>	<ul style="list-style-type: none"> Undefined (default). Valid full pathname of a preprocessing script file. The pathname must not contain any spaces. If the value is undefined or invalid, a preprocessing script does not run before the scheduled backup.
TENANT_ADMIN	<p>Specifies whether the supplied credentials are for the SYSTEMDB database administrator or a tenant database administrator. The DATABASES parameter specifies the database names for the SAP HANA system that uses the MDC mode.</p> <p>You can supply the credentials in a user store key.</p>	<ul style="list-style-type: none"> FALSE (default) = The supplied credentials are for the SYSTEMDB database administrator. TRUE = The supplied credentials are for the administrator of a tenant database.

Configuring parallelism for SAP HANA operations

For the recovery of an SAP HANA 2.0 backup, you must set the `NSR_PARALLELISM` parameter in the `hdbbackint` parameter file to a value that is equal to or greater than the `NSR_PARALLELISM` value during the backup.

Other than for an SAP HANA 2.0 recovery, you can optionally set the `NSR_PARALLELISM` parameter in the `hdbbackint` parameter file to specify a multistream backup or restore. This parameter interacts with the SAP HANA parameter `parallel_data_backup_backint_channels` to determine the parallelism during an SAP HANA backup or restore.

The following settings determine whether NMSAP backs up the multiple databases simultaneously or sequentially:

- Parallelism attribute setting in the NetWorker Client resource.
- `NSR_PARALLELISM` parameter setting.
- Setting of the number of backup sessions/channels in the backup configuration wizard.

During NetWorker scheduled backups, if the number of current running backup sessions is greater than the Parallelism attribute setting in the NetWorker Client resource, a newly started scheduled backup runs sequentially. The *NetWorker Administration Guide* provides details about the NetWorker client parallelism.

For a multistream backup starting with SAP HANA SPS 11, NMSAP can use multiple SAP HANA channels to write the backup data for each SAP HANA service. NMSAP uses a separate SAP HANA channel to write each stream of data to the NetWorker server. You can set the SAP HANA parameter `parallel_data_backup_backint_channels` to specify the number of channels to use for the backup, up to a maximum of 32 channels. SAP HANA opens the corresponding number of pipe files for the backup, and NMSAP saves each stream as a separate save set.

You set the `NSR_PARALLELISM` parameter in the `hdbbackint` parameter file to specify the maximum number of concurrent backup or restore streams. For example, if the `parallel_data_backup_backint_channels` parameter is set to 12 on the SAP HANA server, then 12 streams are used for the backup, which produces 12 save sets. If the `hdbbackint NSR_PARALLELISM` parameter is set to 6, then a maximum of 6 streams are backed up concurrently, and new streams start as other streams complete. [NMSAP hdbbackint parameters](#) on page 45 provides more details about the `NSR_PARALLELISM` parameter.

A restore uses the same number of streams as the backup, and ignores the `parallel_data_backup_backint_channels` parameter setting. The `NSR_PARALLELISM` parameter controls the number of concurrent streams in the same way for both the backup and restore.

Enabling the parameter file in SAP HANA Studio

Specify the location of the `hdbbackint` parameter file in SAP HANA Studio. On the **Configuration** tab of the **Backup** editor, type the complete pathname of the parameter file in the **Backint Parameter File** text box.

Note

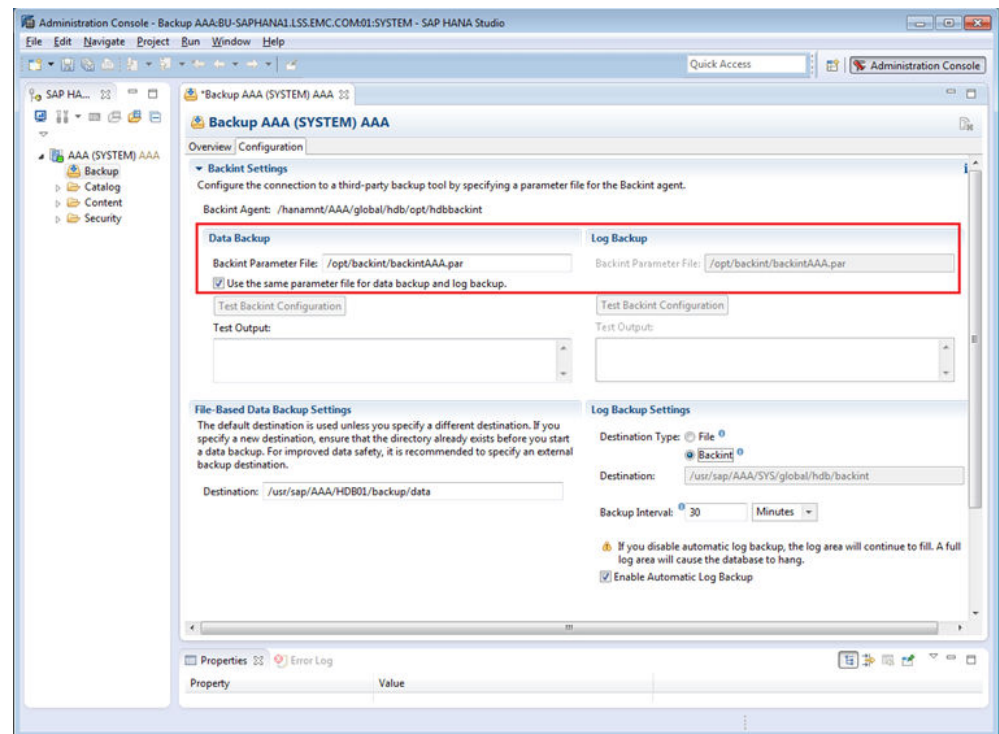
The same configuration file is used for all the SAP HANA CLI and SAP HANA Studio operations.

You can specify separate configuration files for the database backup and log backup.

You can also select **Use the same parameter file data backup and log backup** to use the same configuration file for both types of backups.

The following figure shows a configuration example in SAP HANA Studio 1.0 SPS 5.

Figure 2 Specifying the parameter file in SAP HANA Studio



Configuring the data protection policy with NMC

Create a data protection policy for an NMSAP scheduled backup. A policy acts as a container for the backup workflow, action, and group. When you configure the data protection policy, you create and assign the Client resource, group, policy, workflow, and backup action that define the settings for the scheduled backup.

An NMSAP scheduled backup is defined as a type of action within a workflow in the NetWorker server. The Client resource that is created for the backup is assigned to a group, which is assigned to the workflow. The workflow itself is assigned to the data protection policy.

Perform the following steps to configure the data protection policy for an NMSAP scheduled backup. The *NetWorker Administration Guide* and NMC online help provide details on how to use NMC to configure the required NetWorker resources and settings.

NOTICE

Data protection policy configurations do not apply to client-initiated or manual NMSAP backups.

Procedure

1. Open the NMC Administration interface, where you perform all the policy configuration procedures:
 - a. In the NMC **Enterprise** window, right-click the NetWorker server name, and then select **Launch Application**.
The **Administration** window appears.
 - b. In the **Administration** window, click **Protection**.
The *NetWorker Administration Guide* provides details on how to access the NMC interfaces.

2. Ensure that the NetWorker Client resource is configured to define the backup data that the protection policy manages. You can configure the Client resource with or without the configuration wizard:
 - Create or modify the Client resource with the wizard according to [Configuring scheduled backups with the wizard](#) on page 41.
 - Create or modify the Client resource without the wizard according to [Configuring the Client resource without the wizard](#) on page 59.
3. Ensure that a backup group, also known as a protection group, is created to contain the Client resource.

Each group can be assigned to only one workflow, and each workflow applies to only one group. You can assign a group to a workflow either when you create or edit the group, or when you create or edit the workflow.

When you create the backup group, you specify the group properties and add the Client resource to the group. The *NetWorker Administration Guide* provides details on how to create and edit a group in the NMC Administration interface. Follow the procedures for a basic client group.

4. Ensure that the backup policy is created for the scheduled backup.

A policy can contain one or more workflows, but you can assign a workflow to only one policy.

When you create a policy, you specify the policy name and notification settings. The *NetWorker Administration Guide* provides details on how to create and edit the policy in the NMC Administration interface.

After you create a policy, create the workflows and actions for the policy.
5. Ensure that the backup workflow is created for the scheduled backup policy.

The workflow can include a single action as the traditional NMSAP backup. The workflow can optionally include a check connectivity action before the backup action.

The workflow can also optionally include a clone action after the backup action, to create a cloned copy of the backup save sets. Alternatively, you can create a

separate workflow for the clone action and run the clone operation separately from the backup.

When you create a workflow, you specify the following information:

- Start time and schedule window for the action or sequence of actions.
- How often the workflow runs.
- The order of actions to perform.
- The group of Client resources on which the actions occur.

You can create the actions for the workflow either when you create the workflow or separately.

The *NetWorker Administration Guide* provides details on how to create and edit the workflow in the NMC Administration interface.

6. Ensure that the backup action is created for the scheduled backup workflow.

For a regular (nonsnapshot) scheduled backup, create a traditional backup action. You can create actions for a workflow either when you create the workflow or separately.

When you create the backup action, you specify the backup level for each day of the weekly or monthly schedule. You also specify the destination storage node, destination pool, retention period for the backup, and any advanced options as required.

Note

If you want to override the storage node, pool, or retention period setting for a specific client, you can specify the corresponding attribute in the Client resource. The attribute settings in the Client resource override the settings in the backup action.

Optionally, you can create a check connectivity action to precede the backup action and a clone action to follow the backup action in the workflow.

The *NetWorker Administration Guide* provides details on how to create and edit an action by using the Policy Action Wizard. When you create the backup action for the NMSAP scheduled backup with the Policy Action Wizard:

- From the **Action Type** list, select **Backup**.
- From the secondary action list, select **Traditional**.

Configuring the Client resource without the wizard

On the NetWorker server, you can configure a NetWorker Client resource in the NMC program, without using the wizard.

Configure a NetWorker Client resource for each SAP HANA server (NMSAP client) that requires backup, restore, and inquiry services. Customize the Client resource for an NMSAP scheduled backup by setting the resource attributes.

You can create and edit a Client resource through the Client Properties dialog box in the NMC Administration interface. You must enable the NMC diagnostic mode to view the advanced attributes in the Client resource. The *NetWorker Administration Guide* and online help provide details.

Note

It is recommended that you specify the schedule (backup level), storage node, pool, and retention period in the backup action as part of the data protection policy configuration, not in the Client resource.

If a client requires different settings from other clients in the same backup group, then you can set the specific attributes in the Client resource. In the backup action that you create with the Policy Action Wizard in NMC, you can select **Client Can Override** in the **Client Override Behavior** field. Then, the attribute settings in the Client resource override the properties that are set in the backup action, which is created for the data protection policy.

For example, you can set the retention period to 1 month in the backup action for all clients and then set a 3-month retention in the Client resource for a specific client. Also, you can set a pool in the backup action for all clients and then set a different pool in the Client resource for a specific client.

To override the backup schedule that is specified in the policy-based configuration, you can select or customize one of the preconfigured schedules available in the NetWorker server. You can also create a custom schedule. Then you can select the new schedule in the Schedule attribute of the Client resource. The *NetWorker Administration Guide* provides details on preconfigured and custom schedules.

Set the required Client resource attributes in NMC as shown in the following table. The table lists the basic attributes first, followed by the advanced attributes. You can view the basic attributes in the Client Properties dialog box without enabling the NMC diagnostic mode. To view the advanced attributes, enable the NMC diagnostic mode as described in the *NetWorker Administration Guide*.

Table 7 NetWorker Client resource attributes for NMSAP scheduled backups

Attribute	NMC tab	Description
Basic attributes:		
Aliases	Globals (1 of 2)	Specify all known aliases for the NMSAP host.
Backup command	Apps & Modules	Specify the command to be used for a scheduled backup, either: <code>nsrsapsv -T saphana</code> which only the wizard can configure (cannot be manually set) or <code>nsrsapsv -T saphana -f file_pathname</code> which uses the settings of the NMSAP configuration file (<code>nsrsapsv.cfg</code>). Here, <code>file_pathname</code> is the full pathname of the NMSAP configuration file that is created on the NMSAP client host as described in NMSAP nsrsapsv parameters on page 52. The pathname can contain only ASCII characters and can be no longer than 64 characters.
Checkpoint enabled	General	SAP HANA operations ignore this attribute.
Directive	General	Leave blank. NMSAP does not support global directives.
Name	General	Specify the hostname of the SAP server host where the NMSAP software is installed.

Table 7 NetWorker Client resource attributes for NMSAP scheduled backups (continued)

Attribute	NMC tab	Description
Parallelism	Globals (1 of 2)	Specify the maximum number of concurrent backup and restore sessions to use for a backup operation. You can use this Client resource attribute instead of the parallelism setting in the parameter file or the wizard configuration.
Protection group list	General	Specify the NetWorker backup group to use for a scheduled backup.
Remote access	Globals (2 of 2)	Specify the OS username and fully qualified hostname (IP) of a remote host, used to enable backups in an SAP HANA scale-out environment and restores of the backups to that remote system: <ul style="list-style-type: none"> For an SAP HANA scale-out backup, specify <i>sap_user@hana_host</i> for each host in the scale-out environment. For restore of a backup from this host to a different destination host, specify <i>sap_user@different_host</i>.
Remote user, Password	Apps & Modules	SAP HANA operations ignore these attributes.
Save set	General	Specify the database to be backed up. Use the following format for the save set name: <i>SAPHANA:DBSID</i> where <i>DBSID</i> is the database instance.
Advanced attributes:		
Backup target disks	Globals (2 of 2)	Specify an ordered list of device names of backup devices that the NetWorker server can assign for this client, bypassing the Storage Nodes attribute. This global attribute setting applies to each instance of the client. The devices can be either local or remote to the NetWorker server, but must not belong to a dedicated storage node. Each device must have a Device resource that is configured with the Media Type attribute setting of <i>adv_file</i> or Data Domain.
Checkpoint granularity	General	SAP HANA operations ignore this attribute.
Client direct	General	Select this attribute to enable the Client Direct feature for a scheduled backup to a DD Boost device, CloudBoost device, or AFTD. If a Client Direct backup is not possible, the backup routes the data through the storage node instead of sending the data directly from the client to the storage device.
Data Domain backup	Apps & Modules	Optionally select this attribute to ensure that the deduplication backup is always stored on a DD Boost device when the backup pool contains a mixture of DD Boost devices and other types of devices.
Data Domain interface	Apps & Modules	Specify the interface over which the backup occurs to a Data Domain device. This option is used only when you enable Data Domain Backup for the client. Select the correct setting for the attribute: <ul style="list-style-type: none"> Fibre Channel—The backup uses a Fibre Channel (FC) interface. IP—The backup uses an IP interface. Any—The backup uses either an FC or IP interface, depending on the available Data Domain device.

Table 7 NetWorker Client resource attributes for NMSAP scheduled backups (continued)

Attribute	NMC tab	Description
		<p>Note</p> <p>To enable a restore from a Data Domain device over an FC interface, set this attribute to Fibre Channel.</p>
Pool	General	Specify the pool to use for a backup.
Retention policy	General	Specify the minimum length of time that must elapse before backed-up data is eligible to be overwritten on the backup media.
Schedule	General	Select the NetWorker backup schedule to use for a scheduled backup.
Scheduled backup	General	For scheduled backups only. Select the checkbox to enable the Client resource for a scheduled backup.
Storage Nodes	Globals (2 of 2)	Specify the name of each storage node to which the database server can back up data. The database server backs up to the first active enabled storage node in the order that is listed in the attribute. The default storage node name, nsrserverhost, represents the NetWorker server.

Configuring manual backups

Complete the required steps to configure an NMSAP manual backup.

Procedure

1. Complete all the steps that are described in [Verifying the NMSAP software requirements](#) on page 40.
2. Configure the `hdbbackint` parameter file, `initDBSID.utl`, with the settings for the required NetWorker server and the other backup parameters.

Note

For a manual backup, the settings in the NMSAP parameter file take precedence over settings in the NetWorker Client resource.

[NMSAP hdbbackint parameters](#) on page 45 provides details.

Configuring automatic backups of SAP HANA redo logs

Complete the required steps in SAP HANA Studio to configure the automatic backups of SAP HANA redo logs.

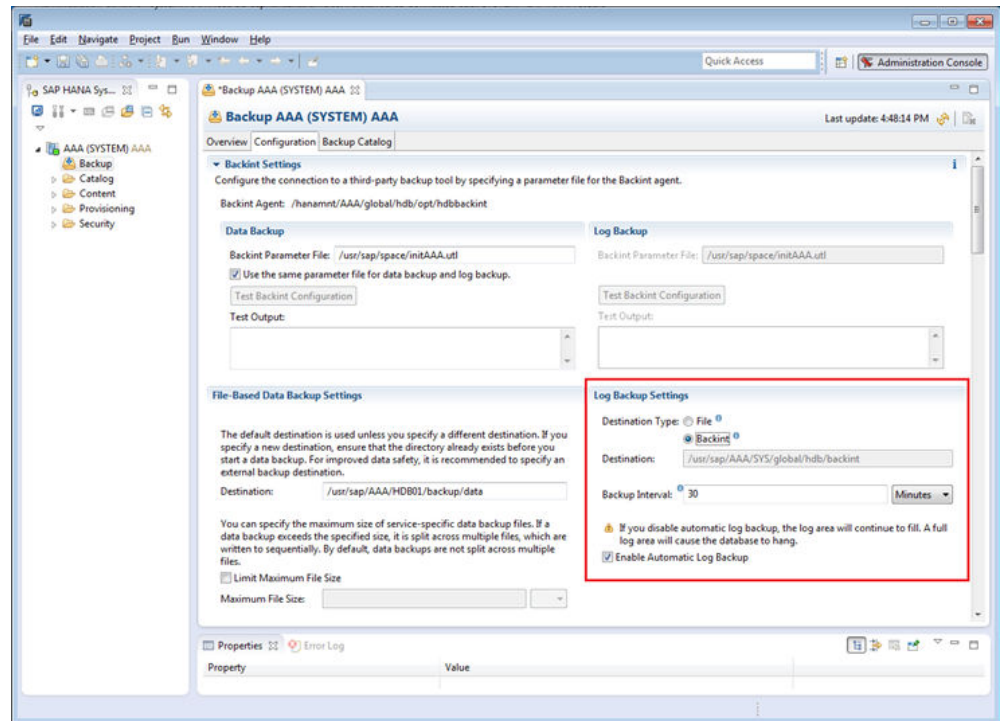
On the **Configuration** tab of the **Backup** editor, complete the settings in the **Log Backup Settings** group box:

Procedure

- Select **Enable Automatic Log Backup**.
- For **Destination Type**, select **Backint**.
- For **Backup Interval**, specify the log backup interval. Type the numeric value in the text box, and select the unit of time, such as **Minutes**, from the menu.

The following figure shows a configuration example in SAP HANA Studio 1.0 SPS 5.

Figure 3 Configuring automatic log backups in SAP HANA Studio



Configuring Data Domain Boost backups

This topic provides specific information about using DD Boost with NMSAP. The *NetWorker Data Domain Boost Integration Guide* provides additional information about the DD Boost configuration and initial setup.

Follow the requirements, best practices, and configuration procedures in this topic for a deduplication backup that uses only DD Boost devices. The content in this topic does not apply to a deduplication backup that uses AFTD or VTL devices.

The NetWorker documentation describes how to configure a Data Domain backup to AFTD or VTL devices. [Configuring NMSAP backups to AFTD storage](#) on page 68 also describes how to configure a Client Direct backup to AFTD devices.

Requirements for DD Boost backups

Before you configure a Data Domain deduplication backup with a DD Boost device, ensure that the NetWorker client and server releases support the DD Boost device. The *NetWorker Module for SAP Release Notes* provides details.

NMSAP supports three types of configurations for Data Domain deduplication backups:

- Deduplication using Client Direct—This configuration eliminates the sending of data over the network between the NMSAP client and the storage node. The deduplicated data is sent directly from the NMSAP client to the DD Boost device.
- Deduplication on a remote storage node—This configuration decreases the amount of network traffic between the storage node and Data Domain system by

sending only the unique blocks over the network. However, deduplication requires all the data to be sent over the network between the NMSAP client and the storage node.

- Deduplication on a local storage node (on the NMSAP client)—This configuration has similar performance to deduplication using Client Direct. However, this configuration requires a storage node on the NMSAP client and additional memory resources.

Best practices for DD Boost backups

Deduplication backups and restores with a Data Domain system are recommended for large databases with high data change rates. A daily change rate of more than 5 percent is a high change rate.

During planning and configuration of a deduplication backup, keep in mind the following best practices that can improve the backup performance:

- Do not use NMSAP backup encryption because the encryption decreases the data deduplication ratio.
- Do not use NMSAP backup compression because the compression decreases the data deduplication ratio.
- Use Client Direct access to a Data Domain device for backups and restores to eliminate data transfer between the NMSAP client and NetWorker storage node. However, using this feature requires an additional 24 MB of memory per data stream on the NMSAP client and also increases the NMSAP CPU usage.

Data Domain and NetWorker documentation describes the requirements for deduplication backups.

Configuring Client Direct with DD Boost backups

You can configure a scheduled or manual backup to a DD Boost device that uses the Client Direct feature to deduplicate data on the NMSAP host. The backup passes only unique data blocks directly to the device, bypassing the storage node.

Procedure

1. Review [Best practices for DD Boost backups](#) on page 64.
2. Configure the DD Boost device, and then enable the Data Domain system for NetWorker operations. The *NetWorker Data Domain Boost Integration Guide* provides details.
3. For a Client Direct backup to a DD Boost device over Fibre Channel, ensure that the SAP user has the correct device permissions as described in the following article:

Fibre Channel Devices with Products using DD Boost in Linux/UNIX Environment
(Document ID dd95007)

Use the document ID to search for the article on the Support website at <https://support.emc.com>.

Note

This step is not required for a backup through the storage node.

4. Associate the backup with a pool that contains the DD Boost device, which is configured in step 2:

- For a scheduled backup, associate the required media pool with the Client resource by using the NMC program. The *NetWorker Administration Guide* and NMC online help provide details about using the NMC program.
 - For a manual backup, set the `NSR_DATA_VOLUME_POOL` parameter to the required pool. [Configuring manual backups](#) on page 62 provides details.
5. Follow the configuration instructions in the following table, similar to the instructions for configuring a nondeduplication backup.
 6. For a Client Direct backup, use the default configuration settings. The Client Direct feature is enabled by default.

With Client Direct enabled, NMSAP tries to perform a Client Direct backup. If a Client Direct backup is not possible, NMSAP performs a backup through the storage node.

Note

The Client Direct setting in the Client resource or wizard field takes precedence over the `NSR_DIRECT_ACCESS` setting in the `initDBSID.utl` parameter file.

Table 8 Configuring a Data Domain backup

Type of Data Domain deduplication backup	Configuration instructions	Additional instructions to use DD Boost over Fibre Channel or if the pool contains Data Domain and other types of devices
Scheduled backup that is configured with the wizard	Configuring scheduled backups with the wizard on page 41	On the Client Backup Options wizard page: <ul style="list-style-type: none"> • Select the Data Domain backup. • Select the proper Data Domain interface. Ensure that you select the Fibre Channel setting if you want to use an FC interface.
Scheduled backup that is configured without the wizard	Configuring scheduled backups without the wizard on page 45	In the Client resource of the NMSAP client: <ul style="list-style-type: none"> • Select the Data Domain Backup attribute. • Select the proper setting of the Data Domain Interface attribute. Ensure that you select the Fibre Channel setting if you want to use an FC interface.
Manual backup	Configuring manual backups on page 62	In the <code>initDBSID.utl</code> parameter file: <ul style="list-style-type: none"> • Set <code>NSR_DEVICE_INTERFACE=DATA_DOMAIN</code>. NSR_DEVICE_INTERFACE provides details. • Set <code>NSR_DATA_DOMAIN_INTERFACE</code> to the proper interface value. Ensure that you set the Fibre Channel value if you want to use an FC interface. NSR_DATA_DOMAIN_INTERFACE provides details.

Configuring storage node with DD Boost backups

You can configure a scheduled backup or manual backup to a DD Boost device, where the backup does not try to use the Client Direct method but instead deduplicates data on a storage node.

Procedure

1. Follow step 1 to step 5 in [Configuring Client Direct with DD Boost backups](#) on page 64.
2. Ensure that the Client Direct feature is disabled by following the correct procedure:
 - For a manual backup, set `NSR_DIRECT_ACCESS=No` in the `initDBSID.utl` parameter file. [NMSAP hdbbackint parameters](#) on page 45 provides details on the parameter.
 - For a scheduled backup, clear the Client Direct checkbox in the wizard or disable the Client Direct attribute in the NetWorker Client resource.

Configuring CloudBoost backups

This topic provides specific information about using CloudBoost with NMSAP. The latest version of the *NetWorker with CloudBoost Integration Guide* provides additional information about the CloudBoost configuration and initial setup.

[Backups and restores with CloudBoost](#) on page 22 describes the NMSAP support of backups with a CloudBoost device.

You can use the following information to configure a CloudBoost backup to a supported CloudBoost device:

- NetWorker documentation describes the configuration of a CloudBoost backup to a CloudBoost device.
- [Configuring CloudBoost backups to use Client Direct](#) on page 67 and [Configuring CloudBoost backups to use a storage node](#) on page 67 describe the configuration of a backup to a CloudBoost device through either the Client Direct method or a storage node.

Best practices for CloudBoost backups

Before you configure a CloudBoost backup with a CloudBoost device, ensure that the NetWorker client and server releases support the CloudBoost appliance. The *NetWorker E-LAB Navigator* provides details.

Use Client Direct access for CloudBoost backups to eliminate data transfer between the NMSAP client and NetWorker storage node.

CloudBoost and NetWorker documentation describes the requirements for CloudBoost backups.

Configuring CloudBoost backups to use Client Direct

You can configure a scheduled backup or manual backup to a CloudBoost device that uses the Client Direct feature on the NMSAP host and passes data directly to the CloudBoost device, bypassing the storage node.

Procedure

1. Review [Best practices for CloudBoost backups](#) on page 66.
2. Configure and enable the CloudBoost appliance for NetWorker operations. The latest version of the *NetWorker with CloudBoost Integration Guide* provides details.
3. Configure and enable the CloudBoost devices for NetWorker operations. The latest version of the *NetWorker with CloudBoost Integration Guide* provides details.
4. Associate the backup with a pool that contains the CloudBoost device that is configured in steps 2 and 3:
 - For a scheduled backup, associate the required media pool and storage node with the backup action by using the NMC program. Use the CloudBoost appliance as the storage node. The *NetWorker Administration Guide* and NMC online help describe how to use the NMC program.
 - For a manual backup:
 - Set the NSR_DATA_VOLUME_POOL parameter to the required pool. [NMSAP hdbbackint parameters](#) on page 45 provides details on the parameter.
 - Specify the CloudBoost appliance as the storage node in the NetWorker Client resource attributes. [Configuring the Client resource without the wizard](#) on page 59 provides details.
5. For a Client Direct backup, use the default configuration settings, except set NSR_DIRECT_ACCESS=Yes for a manual backup. The Client Direct feature is enabled by default.

With Client Direct enabled, NMSAP tries to perform a Client Direct backup. If a Client Direct backup is not possible, NMSAP reverts to a backup through the storage node.

Note

The Client Direct setting in the wizard field or Client resource takes precedence over the NSR_DIRECT_ACCESS parameter setting.

Configuring CloudBoost backups to use a storage node

You can configure a scheduled backup or manual backup to a CloudBoost appliance, where the backup does not try to use the Client Direct method but instead transfers the backup data through a storage node.

Procedure

1. Follow step 1 to step 4 in [Configuring CloudBoost backups to use Client Direct](#) on page 67.
2. Ensure that the Client Direct feature is disabled:

- For a manual backup, set `NSR_DIRECT_ACCESS=No` in the `initDBSID.utl` parameter file. [NMSAP hdbbackint parameters](#) on page 45 provides details on the parameter.
- For a scheduled backup, clear the Client Direct checkbox in the wizard or disable the Client Direct attribute in the NetWorker Client resource.

Configuring NMSAP backups to AFTD storage

You can configure an NMSAP scheduled or manual backup to an AFTD as either a Client Direct backup or a backup that sends data through a storage node.

Configuring Client Direct backups to AFTD

Complete the required steps to configure a scheduled or manual backup that uses Client Direct to an AFTD.

Procedure

1. Configure an AFTD by using either the Device Wizard or the NMC device properties window.

The *NetWorker Administration Guide* provides complete details about AFTD configurations, including considerations for Client Direct clients.
2. Ensure that the NMSAP client has the required access to the AFTD through CIFS. The *NetWorker Administration Guide* provides details.
3. Associate the backup with a pool that contains the AFTD configured in step 1.
4. Follow the required configuration instructions:
 - [Configuring scheduled backups with the wizard](#) on page 41.
 - [Configuring scheduled backups without the wizard](#) on page 45.
 - [Configuring manual backups](#) on page 62.
5. For a Client Direct backup, use the default configuration settings. The Client Direct feature is enabled by default.

With Client Direct enabled, NMSAP tries to perform a Client Direct backup. If a Client Direct backup is not possible, NMSAP performs a traditional backup through the storage node.

Configuring storage node backups to AFTD

Complete the required steps to configure a scheduled or manual backup to an AFTD where the backup does not try to use the Client Direct method but instead sends data through a storage node.

Procedure

1. Follow step 1 to step 4 in [Configuring Client Direct backups to AFTD](#) on page 68.
2. Ensure that the Client Direct feature is disabled by following the required procedure:
 - For a manual backup, set `NSR_DIRECT_ACCESS=No` in the `initDBSID.utl` parameter file. The `NSR_DIRECT_ACCESS` information in [Table 5](#) on page 46 provides details.

- For a scheduled backup, clear the Client Direct checkbox in the wizard or disable the Client Direct attribute in the NetWorker Client resource.

CHAPTER 3

NMSAP HANA Operations

This chapter includes the following topics:

- [Performing scheduled backups of SAP HANA data](#) 72
- [Performing manual backups and recovery with SAP HANA Studio](#) 73
- [Performing manual backups and recovery with the SAP HANA CLI](#) 78
- [Preparing for SAP HANA disaster recovery](#) 82
- [SAP HANA scale-out requirements](#) 83

Performing scheduled backups of SAP HANA data

You can use the following procedures to test, monitor, and cancel scheduled NMSAP backups of SAP HANA data.

The *NetWorker Administration Guide* provides information about restarting checkpoint enabled backups.

Testing scheduled backups

You can configure scheduled NMSAP backups to run automatically according to the backup schedules. After you configure a scheduled backup, you can manually test the backup with NMC.

Before you begin

Before you test a scheduled backup, ensure that you meet the following requirements:

- You have correctly set up the software environment. You have provided read and write access to a common parent directory for all the files that are associated with the backup. [Verifying the NMSAP software requirements](#) on page 40 provides details.
- You have created the NetWorker Client resource with a correctly configured save set and backup command.
- You have assigned the Client resource to a backup group.
- You have assigned the backup group to a workflow.
- You have assigned the backup workflow to a data protection policy.

Procedure

1. Start the NMC console server. The *NetWorker Administration Guide* and NMC online help provide details on how to access the NMC interfaces.
2. To open the **Administration** window, right-click the NetWorker server name in the NMC **Enterprise** window, and then select **Launch Application**.
3. In the **Monitoring** window, right-click the workflow name for the backup, and then select **Start** from the list box.

Note

Instead of starting only one workflow, you can start all the workflows in a particular policy by right-clicking the policy name and selecting **Start**.

4. Click **Yes** in the confirmation box.
The scheduled backup starts.

Monitoring scheduled backups

You can monitor a scheduled backup and the activities for specific backup policies, workflows, and actions by using the **Monitoring** window in NMC.

Note

The location of information in the **Monitoring** window might vary in different NMC releases.

The **Policies** pane and **Actions** pane in the **Monitoring** window display backup status information during and after a scheduled backup.

The *NetWorker Administration Guide* provides details about viewing scheduled backup information in NMC.

In addition to monitoring a database backup in NMC, you can use the database activity logs, if supported, to monitor the backup results from the database server.

Canceling scheduled backups

You can cancel a scheduled backup by using the following procedure.

The following results occur if you cancel a backup before completion:

- None of the backed-up data might be recoverable.
- The **Volume Save Sets** are marked as incomplete in NMC.

You can cancel a scheduled backup in progress from the NMC program.

Procedure

1. Open the NMC **Administration** window. The *NetWorker Administration Guide* provides details on how to access the NMC interfaces.
2. Select the backup workflow in the **Monitoring** window.
3. Right-click the backup workflow, and then select **Stop**.

The scheduled backup stops after you click **Yes** in the confirmation box.

To manually start a canceled backup process from the beginning, right-click the backup workflow to start and select **Start**. Ensure that the backup successfully completes without interruption.

Performing manual backups and recovery with SAP HANA Studio

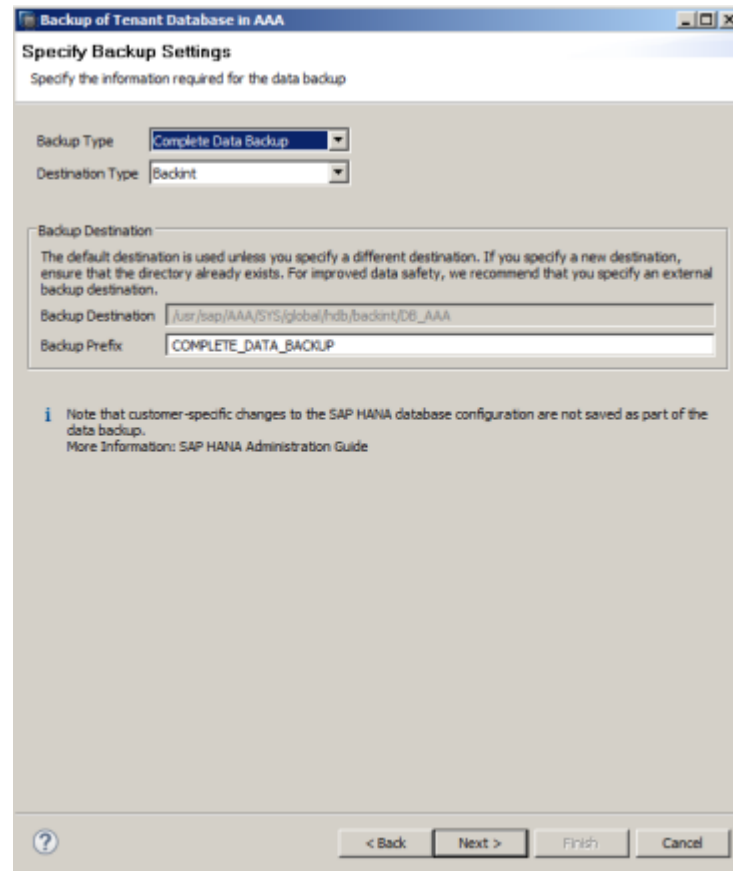
You can run the SAP HANA Studio GUI to perform backups, backup deletions, restores, and recovery with NMSAP. The SAP HANA documentation provides details about the SAP HANA Studio procedures.

You can perform operations with SAP HANA Studio after you have completed the configurations in [Configuration road map for SAP HANA operations](#) on page 40.

Performing manual backups with SAP HANA Studio

In SAP HANA Studio, specify the database for backup and enable the backup to use the BACKINT interface.

For example, the **Specify Backup Settings** dialog box appears as follows with SAP HANA SPS 10.

Figure 4 Specifying backup settings in SAP HANA Studio

Complete the required settings in the **Specify Backup Settings** dialog box:

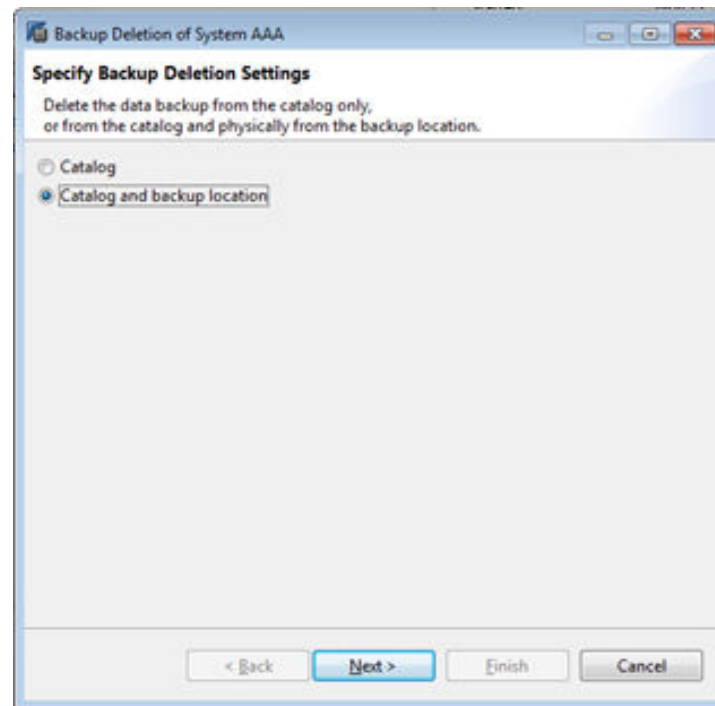
Procedure

- In the **Backup Type** field with SAP HANA SPS 10 or later, select one of the backup types:
 - **Complete Data Backup**
 - **Differential Data Backup**
 - **Incremental Data Backup**
- In the **Destination Type** field, select **Backint**.
- In the **Backup Prefix** field, optionally type a prefix for the backup name. If you specify a prefix, then the backup name includes the prefix, *prefix_databackup_#_#*.

Deleting backups with SAP HANA Studio

In SAP HANA Studio, select the backup catalog option for the required SID and select a database backup for deletion from the backup catalog list.

The **Specify Backup Deletion Settings** dialog box appears as follows.

Figure 5 Specifying backup deletion settings in SAP HANA Studio

Select the required type of deletion:

Procedure

- To delete the backup from the backup catalog only, select **Catalog**.

Note

This **Catalog** deletion does not modify any save sets or file information on the NetWorker server.

- To delete the backup from both the backup catalog and the NetWorker server, select **Catalog and backup location**.

Performing restore and recovery with SAP HANA Studio

In SAP HANA Studio, select the recovery option for the required SID.

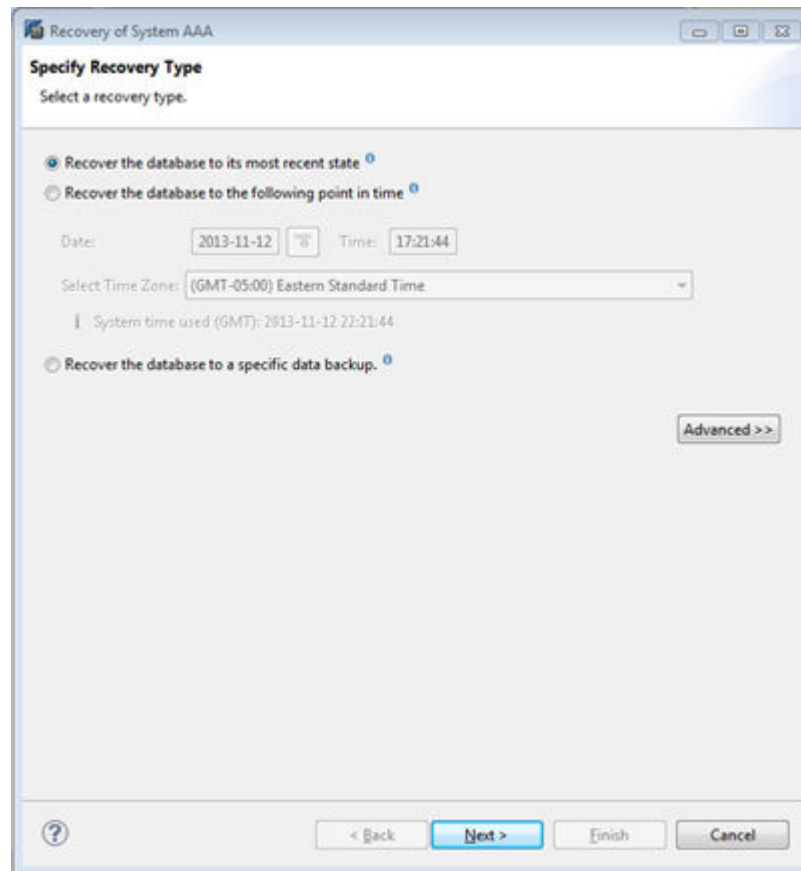
Note

You must run the restore and recovery of SAP HANA MDC databases as the system database administrator user through the SYSTEMDB database. The SYSTEMDB database must be available during the recovery of a tenant database. The *SAP HANA Administration Guide* provides details about the recovery procedures in an MDC system.

Procedure

1. Select the type of recovery in the **Specify Recovery Type** dialog box, which appears as follows.

Figure 6 Specifying the recovery type in SAP HANA Studio



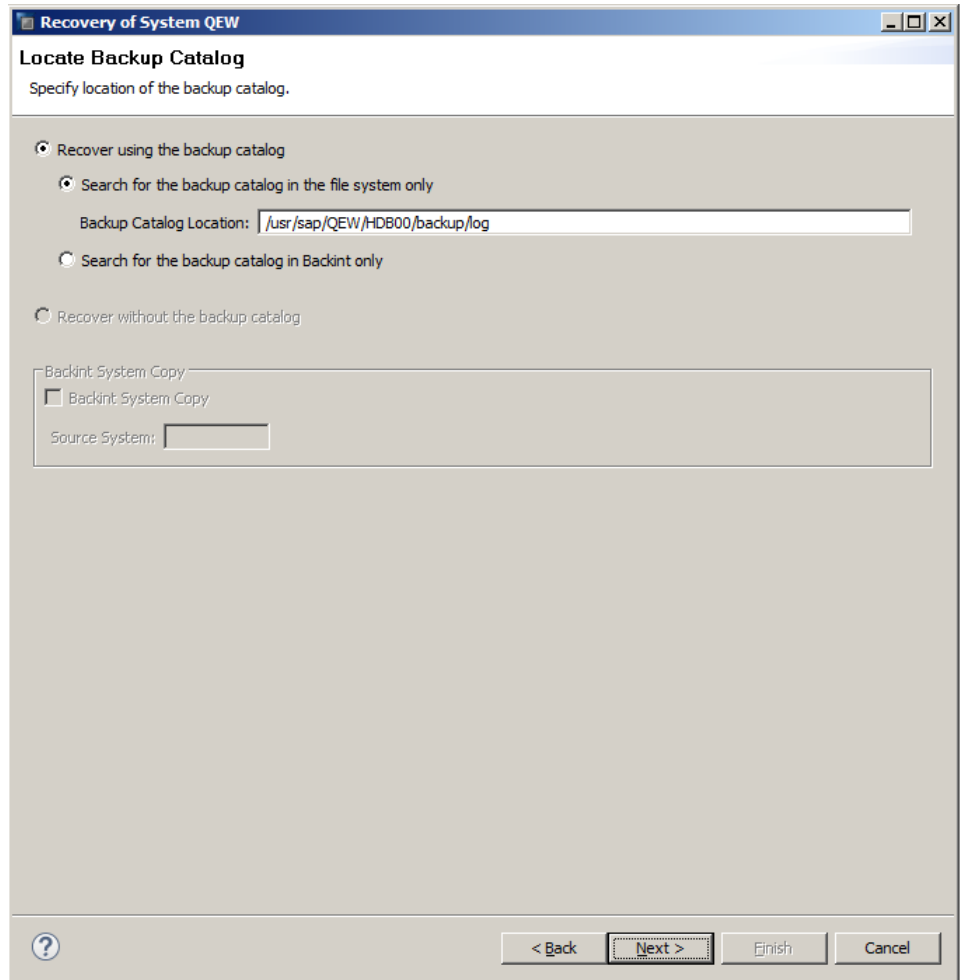
Select the type of recovery from the displayed choices:

- To recover the database as close as possible to the current time, select **Recover the database to its most recent state**.
 - To recover the database to a specific point-in-time, select **Recover the database to the following point in time**.
 - To restore only the specified data backup, select **Recover the database to a specific data backup**.
 - In an exceptional case only when a previous recovery has failed, click **Advanced**, and then select **Recover the database to the following log position**.
2. For SAP HANA 2.0 or later, specify the location of the backup catalog in the **Locate Backup Catalog** dialog box, which appears as follows. Select to search for the backup catalog in the file system or Backint, as appropriate for your particular system.

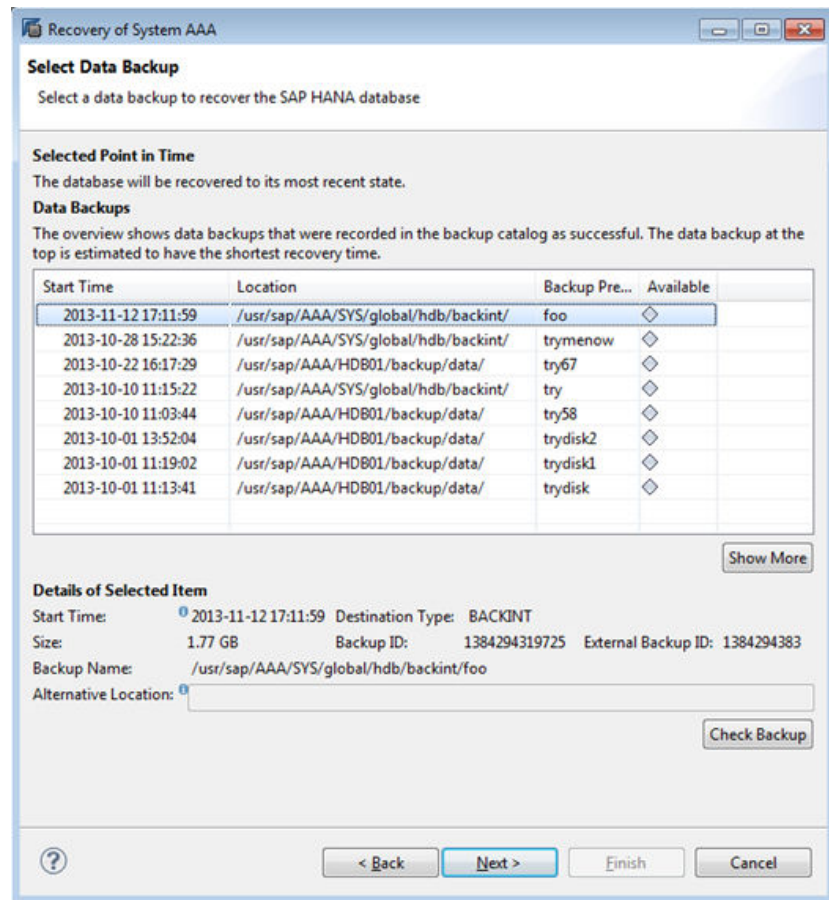
Note

For SAP HANA 2.0 or later, ensure that `catalog_backup_parameter_file` or `catalog_backup_using_backint` is set as required for the system in the SAP HANA configuration at **SystemDB > Configuration > global.ini**.

Figure 7 Selecting the backup catalog for a single database container of SAP HANA 2.0 in SAP HANA Studio



3. Select the database backup for the restore or recovery in the **Select Data Backup** dialog box, which appears as follows.

Figure 8 Selecting the data backup in SAP HANA Studio

- (Optional) Select to perform an inquire operation that checks the backup availability by selecting the backup in the list and clicking **Check Backup**. The **Available** column displays a green or red icon, which is based on the physical availability of the backup.

The recovery progress is displayed for each service, including the name server, index server, and statistics server. A confirmation message appears when the backup is complete.

Performing manual backups and recovery with the SAP HANA CLI

You can run the SAP HANA CLI to perform manual NMSAP backups of SAP HANA data.

Starting with SAP HANA SPS 07, you can run the SAP HANA CLI to perform recovery of NMSAP backups, and run specific maintenance commands to check the availability and integrity of data and log backups.

The SAP HANA documentation provides details about the SAP HANA CLI procedures.

You can perform operations with the SAP HANA CLI after you have completed the configurations in [Configuration road map for SAP HANA operations](#) on page 40.

Performing manual backups with the SAP HANA CLI

You can run the appropriate `hdbssql` command to perform a database backup.

The following example shows an `hdbssql` backup command:

```
hdbssql -U user_key "backup data using backint ('/usr/sap/SID/SYS/global/hdb/backint/prefix' )"
```

where:

Procedure

- *user_key* is the user key created with the SAP HANA `hdbuserstore` tool. SAP HANA documentation provides details about the tool.

Note

The user key must be created by the same OS user that runs the `hdbssql` command.

- *SID* is the system ID of the SAP HANA system. `/usr/sap/SID/SYS/global/hdb/backint/` is the backup pathname of the location where the SAP HANA database server creates the pipes. This backup pathname is optional in the `hdbssql` command.
- *prefix* is an optional prefix for the backup name. If you specify *prefix* in the `hdbssql` command, then the backup name will include the prefix, *prefix_databackup_#_#*.

Note

You must specify either the backup pathname or the prefix in the `hdbssql` command. When you specify one of these items, the other item becomes optional in the command.

The SAP HANA documentation provides details about how to use the `hdbssql` command for backups.

Performing manual backups with the SAP HANA CLI in an MDC system

You must specify the correct credentials and database name in the `hdbssql` command to perform a manual backup of an SAP HANA MDC database.

For a manual backup of the master system database SYSTEMDB, you must specify the system database administrator credentials with the `hdbssql` command.

For a manual backup of a tenant database, you can specify either the system database administrator credentials or the tenant database administrator credentials with the `hdbssql` command. However, do not try to use the system database administrator credentials for a direct connection to a tenant database.

Note

Use the system database administrator credentials to connect to a target database only through the SYSTEMDB database. Use the tenant database administrator credentials to connect directly to the target database.

For example, the following command backs up the tenant database DB0 by using a connection to the SYSTEMDB database through the system database administrator credentials:

```
hdbsql -i 00 -u system_database_administrator_username -p
system_database_administrator_password [-U user_key] -d SYSTEMDB
"backup data for DB0 using backint ('/usr/sap/SID/SYS/global/hdb/
backint/DB_DB0/prefix')"
```

The following command backs up the tenant database DB0 by using a direct connection to the database through the tenant database administrator credentials:

```
hdbsql -i 00 -u tenant_database_administrator_username -p
tenant_database_administrator_password [-U user_key] -d DB0 "backup
data using backint ('/usr/sap/SID/SYS/global/hdb/backint/DB_DB0/
prefix')"
```

Canceling manual backups

You can cancel a manual backup by running the appropriate SQL command with the backup ID of the running data backup.

Procedure

1. Determine the backup ID of the running data backup by using the monitoring view M_BACKUP_CATALOG, which provides an overview of information about backup and recovery activities.

To determine the backup ID, run the following SQL command:

```
select BACKUP_ID from "M_BACKUP_CATALOG" where
entry_type_name = 'complete data backup' and state_name =
'running' order by sys_start_time desc;
```

2. To cancel the running data backup, run the following SQL command:

```
backup cancel backup_ID
```


Checking NMSAP backups with the SAP HANA CLI

Starting with SAP HANA SPS 07, you can run the `hdbbackupcheck` and `hdbbackupdiag` commands to check the integrity and availability of NMSAP backups.

Using the `hdbbackupcheck` command to check backup integrity

You can run the `hdbbackupcheck` command to check the integrity of a data or log backup. The command reads part of the backup, checks the metadata for correctness and consistency, and checks the content for any changes.

The following example command checks the integrity of an NMSAP backup:

```
./hdbbackupcheck -v --backintParamFile /usr/sap/space/space_hana/
init.ddp.utl /usr/sap/AAA/SYS/global/hdb/backint/
foooo_databackup_0_1 -e 1396019304
```

In this command, the backup file name is the pipe name provided by SAP HANA during the backup. The pathname is the location where the pipes were created. The `-e` option provides the external backup ID of the backup file. You can find all these values in the `M_BACKUP_CATALOG_FILES` view.

The SAP Note 1869119 provides details about the `hdbbackupcheck` command.

Using the `hdbbackupdiag` command to check backup availability

You can run the `hdbbackupdiag` command to check the backup availability.

The following example command checks the availability of an NMSAP backup:

```
./hdbbackupdiag --check -i 1393886826664 --useBackintForCatalog
--backintDataParamFile /nsr/res/initAAA.utl
--backintLogParamFile /nsr/res/initAAA-logs.utl
```

Ensure that you use the `--useBackintForCatalog` option.

The SAP Note 1873247 provides more details about the `hdbbackupdiag` command.

Performing recovery with the SAP HANA CLI

Starting with SAP HANA SPS 07, you can use an SQL command to perform a recovery of an NMSAP backup.

Note

The SAP HANA Studio GUI is the recommended method to perform a restore and recovery.

You must be logged in to the SAP HANA system as the OS user `sidadm` to run the recovery SQL command. In a scale-out multinode environment, you must run the command from the master node.

The recovery command must first include the `HDBSettings.sh` and `recoverSys.py` scripts in that order. The `HDBSettings.sh` script sets the environment for recovery. The `recoverSys.py` script processes the recovery SQL command and performs the database recovery.

The following example command performs a recovery of an NMSAP backup:

```
./HDBSettings.sh recoverSys.py --command="recover database until
timestamp '2014-02-28 00:00:00' using data path ('/usr/sap/AAA/SYS/
global/hdb/backint/') using log path ('/usr/sap/AAA/SYS/global/hdb/
backint/') using BACKUP_ID 1593520382350" --wait
```

You must include the `--wait` option for proper completion of the `recoverSys.py` script.

The SPS 07 version of the *SAP HANA Administration Guide* provides details about the SQL command syntax of the recovery command.

Performing recovery with the SAP HANA CLI in an MDC system

For the recovery of an SAP HANA MDC database with the SAP HANA CLI, the user must log in to the SAP HANA SYSTEMDB database and run the required `recover` command.

For example, run the following command to recover the NMSAP backup of SAP HANA MDC database:

```
RECOVER DATABASE FOR DBO UNTIL TIMESTAMP '2015-08-29 01:25:25'
USING DATA PATH ('/usr/sap/AAA/SYS/global/hdb/backint/DB_DBO/')
USING LOG PATH ('/usr/sap/AAA/HDB00/backup/log/DB_DBO') USING
BACKUP_ID 1440811502099 CHECK ACCESS USING BACKINT
```

The *SAP HANA Administration Guide* provide details about the `recover` command and procedures in an SAP HANA MDC system.

Preparing for SAP HANA disaster recovery

For a comprehensive disaster recovery plan, ensure that you can reconstruct the computing environment and all the SAP HANA server files that are associated with maintaining data on the application host.

Use the following guidelines to prepare for a disaster recovery of the SAP HANA server host:

- Maintain accurate and complete records of the network and system configurations. Keep all the original software media and the following items in a safe location:
 - Original operating system media and patches
 - Device drivers and device names
 - File system configuration
 - IP addresses and hostnames
- To ensure the recovery of customer-specific settings of the database, ensure that you back up the SAP HANA configuration files by following the *SAP HANA Administration Guide*. These files are not backed up during database backups.
- Ensure that you have a current full backup of the database and all the redo logs as required for a recovery of the database to the current time.

Plan to perform the following tasks during a disaster recovery:

Procedure

1. Set up the SAP HANA database system to the same configuration as when the data was backed up.
2. Set up the `hdbbackint` parameter file to be used during the recovery, including the client parameter setting. Set the client parameter to the hostname of the host where the data was backed up. [Setting up the NMSAP parameter file and configuration file](#) on page 45 provides details.
3. Ensure that all the required database and log backup images are available.
4. To recover the database and redo logs, run SAP HANA Studio. Ensure that you select the **Initialize Log Area** option in the SAP HANA Studio database recovery wizard.

SAP HANA scale-out requirements

You can perform SAP HANA backups in an SAP HANA scale-out multinode environment.

Ensure that you meet the following configuration requirements in an SAP HANA scale-out environment:

- You have set up the database in the scale-out environment according to the SAP HANA documentation.
- You have installed the NMSAP software on each node and configured the NMSAP software according to the instructions in the preceding chapter.
- For each node in the system, you have configured a corresponding Client resource in the NetWorker server.
- For a nonwizard configuration, you have set the client parameter in the `hdbbackint` parameter file as described in [NSR_CLIENT](#). You have enabled the parameter file as described in [Enabling the parameter file in SAP HANA Studio](#) on page 57. Ensure that each node in the system can access this parameter file. For example, place the parameter file in a shared location.
- For a wizard configuration, you have set the client parameter in the **Advanced Options** table in the wizard.
- Specify the following values in the Remote Access attribute in the Client resource of the client where the backup runs:

```
host=node_x
host=node_y
...
```

Specify the host values for all the nodes in the system except the node that is specified in the client parameter.

CHAPTER 4

Configuration for NMSAP Oracle Operations

This chapter includes the following topics:

- [Configuration road map for NMSAP Oracle operations](#)..... 86
- [Verifying the NMSAP software requirements](#)..... 86
- [Configuring I18N support](#)..... 88
- [Choosing either backint or RMAN as the backup and restore utility](#)..... 88
- [Configuring scheduled backups with the wizard](#)..... 91
- [Configuring scheduled backups without the wizard](#)..... 93
- [Configuring manual backups](#)..... 118
- [Configuring restartable backups](#)..... 119
- [Configuring Data Domain Boost backups](#)..... 120
- [Configuring CloudBoost backups](#)..... 123
- [Configuring NMSAP backups to AFTD storage](#)..... 125
- [Configuring probe-based backups](#)..... 126

Configuration road map for NMSAP Oracle operations

Use the following instructions to configure the NMSAP Oracle operations on a single host, outside of a cluster or Oracle RAC system.

Procedure

1. [Verifying the NMSAP software requirements](#) on page 86.
2. [Configuring I18N support](#) on page 88.
3. [Choosing either backint or RMAN as the backup and restore utility](#) on page 88.
4. To configure either scheduled or manual backups, use the correct instructions:
 - [Configuring scheduled backups with the wizard](#) on page 91.
 - [Configuring scheduled backups without the wizard](#) on page 93.
 - [Configuring manual backups](#) on page 118.

[Configuring restartable backups](#) on page 119 describes how to configure a restartable scheduled or manual backup.

[Configuring probe-based backups](#) on page 126 describes how to configure a probe-based scheduled backup.

5. [Configuring Data Domain Boost backups](#) on page 120 (only for backups to DD Boost devices).
6. [Configuring NMSAP backups to AFTD storage](#) on page 125 (only for backups to AFTD devices).

Verifying the NMSAP software requirements

Verify that the NMSAP software environment meets the basic requirements.

Procedure

1. Ensure that you have correctly installed and configured the Oracle software and SAP software before you configure the NMSAP environment.

The Oracle and SAP documentation provides instructions.

Note

You can recover only datafiles for which you had read permission on the operating system when you backed up the datafiles.

Grant read access to the datafiles to a DBA operating system group. Granting the read access enables the restore of the data by a different user or to a different host.

2. Ensure that you have installed and enabled the NetWorker client software and NMSAP on each SAP Oracle server requiring backup and recovery services.

The platform-specific NetWorker installation guide and the *NetWorker Module for SAP Installation Guide* provide instructions.

3. Ensure that you have correctly linked the NMSAP RMAN management library/utility if you use the BR*Tools RMAN feature on UNIX.

The *NetWorker Module for SAP Installation Guide* provides details.

4. Ensure that the NMSAP `backint` executable is in the same directory as BR*Tools, or you have set `util_path=full path to directory containing backint` in the BR*Tools initialization profile `initDBSID.sap` with BR*Tools 7.10 or later.

The owner of `backint` must be set to root on UNIX.

5. Ensure that you have set the uid bit for the `backint` program if you will restore to raw device files on UNIX. You can set the uid bit for `backint` by typing the following command:

```
chmod 4755 backint
```

Note

In rare cases, you must set the uid bit to enable restores to file systems on UNIX.

6. Ensure that you have configured the basic NetWorker resources on the NetWorker server to enable backups and restores. The basic resources include the NetWorker Server resource, Client resource, Device resource, and the Pool and Label Template resources.

Ensure that the following storage resources are configured:

- Storage node that owns the backup storage devices.
- Backup storage devices.

Configure a Device resource for each supported storage device that is used for backups and restores.

- Label templates for labeling the backup volumes.
- Media pools for sorting and storing the backup data.

Configure the volumes in each Pool resource to receive specific types of backup data, such as tablespaces or archived logs. In the Pool resources, leave the Save Sets attribute blank because NMSAP sets the Save Sets during each backup.

The *NetWorker Administration Guide* provides details on how to configure NetWorker resources.

7. Ensure that you have granted the NetWorker server User Group resource privileges to the SAP user who performs the NMSAP operations. You can set the User Group resource with NMC or the `nsradmin` program. If you use restricted datazones (RDZs), then you can also grant the required privileges by using the Users and Privileges fields of the RDZ resource. The *NetWorker Administration Guide* provides details.

The SAP user requires specific privileges:

- To run backups and restores requires only the following default privileges:
 - Monitor NetWorker
 - Back Up Local Data
 - Recover Local Data
- To review backup information in NetWorker indexes, for example, with the `nsrinfo` and `mminfo` commands requires the Operate NetWorker privilege.
- To configure a backup requires the Configure NetWorker privilege.

8. If you use a firewall, then you have ensured NMSAP connectivity. Configure the corresponding ports for the NetWorker server as required.
The *NetWorker Administration Guide* provides details.
9. To enable scheduled backups with NMSAP Oracle, ensure that the Oracle parameter `BACKUP_TAPE_IO_SLAVES` is set to `FALSE`.

Configuring I18N support

[Internationalization with NMSAP Oracle](#) on page 32 describes the internationalization (I18N) features that NMSAP supports. You must meet the I18N requirements and complete any configuration steps to enable NMSAP I18N support.

Requirements for I18N support

NMSAP I18N support requires the following I18N products:

- Internationalized operating system
- Unicode version of BR*Tools
- NetWorker server and client that support I18N

The NetWorker documentation describes the NetWorker I18N requirements.

Note

The I18N support that is provided by Oracle, BR*Tools, the NetWorker client, and the underlying operating system limits the NMSAP support of non-ASCII environments.

[Internationalization with NMSAP Oracle](#) on page 32 and the *NetWorker Module for SAP Release Notes* provide more information.

Configuring I18N support on UNIX

Use the following procedure to configure I18N support of the NMSAP client host on UNIX only.

Procedure

1. Log in as the root user.
2. Shut down the NetWorker services.
3. Set the `LC_ALL` environment variable to the required locale.

For example, in a Japanese locale on Solaris, set `LC_ALL` as follows:

```
# nsr_shutdown
# export LC_ALL=ja_JP.eucJP
# /etc/init.d/networker start
```

4. Restart the NetWorker services.

Choosing either backint or RMAN as the backup and restore utility

The SAP BR*Tools software coordinates all the backup, restore, and inquiry operations of SAP Oracle data. You can configure the BR*Tools software to use either

the NMSAP `backint` program or the Oracle RMAN program with the NMSAP RMAN media management library to perform these operations. The following examples describe how you can specify the program to use.

The `brbackup` and `brarchive` programs back up the Oracle data and the BR*Tools profiles, log files, and backup catalogs that are required for disaster recovery. NMSAP operations always use `backint` to back up and restore these files, regardless of the method that is selected for Oracle data backups and restores. Therefore, even if you use RMAN for an Oracle backup, configure the same backup for `backint` operations to ensure that the backup succeeds.

Specifying `backint` as the backup and restore utility

If you want to use the NMSAP `backint` program for backup, restore, and inquiry operations for the Oracle database, then create a BR*Tools initialization profile with the required settings.

Procedure

1. With a text editor, open the BR*Tools initialization profile `initDBSID.sap`, usually located in the following directory:
 - On UNIX or Linux: `$ORACLE_HOME/dbs`
 - On Microsoft Windows: `%ORACLE_HOME%\DATABASE`
2. Set the backup device type parameter to use the `backint` program by specifying one of the following settings:

```
backup_dev_type = util_file
```

or

```
backup_dev_type = util_file_online
```

Note

Set `backup_dev_type = util_file_online` for online backups to decrease the amount of time each tablespace remains in hot backup mode, resulting in a smaller number of generated transaction logs.

3. Set the `util_par_file` parameter to use the NMSAP parameter file, `initDBSID.utl`:
 - On UNIX or Linux:

```
util_par_file = ?/dbs/initDBSID.utl
```

where `?` is `$ORACLE_HOME`.

- On Microsoft Windows:

```
util_par_file = ?\database\initDBSID.utl
```

where `?` is `%ORACLE_HOME%`.

[NMSAP backint parameters](#) on page 95 describes how to configure the parameter file. The SAP documentation describes how to use the `backint` program.

Specifying RMAN as the backup and restore utility

To use the Oracle RMAN utility with the NMSAP media management library for backup, restore, and inquiry operations for the Oracle database, create a BR*Tools initialization profile with the following settings.

Procedure

1. With a text editor, open the BR*Tools initialization profile `initDBSID.sap`, usually located in the following directory:
 - On UNIX or Linux: `$ORACLE_HOME/dbs`
 - On Microsoft Windows: `%ORACLE_HOME%\DATABASE`
2. Set the backup device type parameter to use the RMAN program:

```
backup_dev_type = rman_util
```

The `rman_util` value ensures that the NMSAP RMAN interface backs up the Oracle database data and the NMSAP `backint` interface backs up the BR*Tools metadata (configuration files, backup catalog, and so on).

Note

Do not use the `rman_disk` or `rman_stage` value because these values cause BR*Tools to back up the metadata without using NMSAP and NetWorker.

3. Set the NMSAP parameters for RMAN either in the `rman_send` parameter line or in the same `initDBSID.utl` file that is used to set the `backint` parameters of the metadata backup.

It is recommended that you set the NMSAP parameters in the `initDBSID.utl` file. In this case, also set the `SBT_LIBRARY` and `CONFIG_FILE` parameters. Complete the following steps to set all the required parameters:

- a. In the `initDBSID.utl` file, set the NMSAP parameters for RMAN as described in [NMSAP parameters for RMAN backups and restores](#) on page 111.
- b. Set `SBT_LIBRARY` and `CONFIG_FILE` in the `rman_parms` parameter line in `initDBSID.sap`:
 - Set `SBT_LIBRARY` to the pathname of the RMAN library.
 - Set `CONFIG_FILE` to the pathname of the `initDBSID.utl` file.
- c. Set the `util_par_file` parameter to use the `initDBSID.utl` file, as described in [Specifying backint as the backup and restore utility](#) on page 89.

For example, after you set the NMSAP parameters for RMAN in the `initDBSID.utl` file, complete the following settings in `initDBSID.sap`:

```
backup_dev_type = rman_util
rman_channels = 2
rman_parms = "SBT_LIBRARY=/usr/lib/libnworasap.so,
```

```
ENV=(CONFIG_FILE=/db/app/oracer/product/11.2.0/dbhome/dbs/
initCER.utl)";
util_par_file = /db/app/oracer/product/11.2.0/dbhome/dbs/
initCER.utl
```

Note

As an alternative to setting NMSAP parameters in the `initDBSID.utl` file, you can set the NMSAP parameters in the `rman_send` parameter line in the `initDBSID.sap` file. Uncomment the `rman_send` parameter line and set the parameter to include each required NMSAP (NSR_*) parameter. In this case, you do not set `CONFIG_FILE`, but you still set `SBT_LIBRARY`. Use the following syntax:

```
rman_send = "NSR_ENV=(NSR_var1=value1, NSR_var2=value2, ...)"
```

For example, the following setting sends the same value to all the allocated channels:

```
rman_send = "NSR_ENV=(NSR_CLIENT=bu-client, NSR_SERVER=bu-libra)"
```

The following setting sends the channel-specific values:

```
rman_channels = 2
rman_send = ("channel sbt_1 'NSR_ENV=(NSR_CLIENT=client_name_1) '",
"channel sbt_2 'NSR_ENV=(NSR_CLIENT=client_name_2) '")
```

The SAP documentation describes how to use the BR*Tools with RMAN program for backup and restore operations.

Configuring scheduled backups with the wizard

You can create or modify a scheduled backup configuration with the NMSAP wizard.

Before you begin

Ensure that you meet the following requirements before you use the configuration wizard:

- You have installed the required NetWorker releases on the NMC server, NetWorker server, and NMSAP client hosts as described in the *NetWorker E-LAB Navigator*.
- On the NetWorker server that contains the configuration, the NMC user that starts the wizard (the wizard user) has the Configure NetWorker privilege and all its prerequisite privileges.
- Communication between the NMC server, NetWorker server, and NMSAP client uses NetWorker `nsrauth` authentication. The NetWorker documentation provides the requirements for `nsrauth` authentication.
- You have configured the NMSAP software environment as described in [Verifying the NMSAP software requirements](#) on page 86.

Procedure

1. In the NMC **Enterprise** window, right-click the NetWorker server name, and then select **Launch Application**.

The *NetWorker Administration Guide* provides details on how to access the NMC interfaces.

2. In the **Administration** window, click **Protection**.
3. Start the wizard by using the correct method:
 - To create a NetWorker Client resource for NMSAP, right-click **Clients** in the left pane, and then select **New Client Wizard**.
 - To modify a NetWorker Client resource that was previously created with the wizard for NMSAP, right-click the client name in the right pane, and then select **Modify Client Wizard**.
4. On each wizard page that appears, specify the options and values that are required for the backup configuration. Each wizard page includes an online help button that you can click to access descriptions of the fields and options on the page.

You can click a link in the wizard steps panel to go directly to the page you want to modify. The number of steps that are shown in the steps panel varies according to the chosen configuration type.

5. If you use the wizard to modify a configuration and you select to change a database user's password or OS user's password, the wizard enables you to apply that password change to other backup configurations with the same credentials. The feature enables easy password changes across different server-side configurations as follows:
 - If you use database authentication on the client host and you select to change the password for a specific database (Net service name) and database username, the password change is applied to all the backup configurations that use the same database and username on the host.

Note

If you use the same username for different databases on the same host, you can select an option to apply the same password change to all the backup configurations of all the databases with that username.

- If you select to change the password for a specific OS username, the password change is applied to all the NMSAP backup configurations that use the same OS username on the host.
6. On the wizard page titled **Client Configuration Summary**:
 - To create the configuration, click **Create**.
 - To modify the configuration, click **Back**.

After you finish

After you complete the backup configuration with the wizard, ensure that a data protection policy is also configured on the NetWorker server to define the backup workflow and other required settings for the scheduled backup. [Configuring the data protection policy with NMC](#) on page 113 provides details.

Configuring scheduled backups without the wizard

As an alternative to the wizard configuration, you can create or modify a scheduled backup configuration by performing the following tasks.

Procedure

1. [Configuring the NMSAP parameters without the wizard](#) on page 93.
2. [Configuring the data protection policy with NMC](#) on page 113.

The NMC interface provides NetWorker Device, Media Pool, and other resource settings that are not available in the wizard.

Configuring the NMSAP parameters without the wizard

Procedure

1. Ensure that you have correctly configured the NMSAP software environment as described in [Verifying the NMSAP software requirements](#) on page 86.
2. On the NMSAP client, copy the `init_oracle_nmsap.utl` and `nsrsapsv.cfg` template files (supplied with the NMSAP installation) with new names for the database instance, and then configure the files for the backup.

[NMSAP parameters for backups and restores](#) on page 94 provides configuration details.

3. Encrypt the SAP operating system username and the password, and if required, the Oracle database username and password:
 - a. On the NMSAP client, log in as the root user or administrator, and then type the following NMSAP command:

```
nsrsapadm -P oracle -z config_file_pathname
```

where `config_file_pathname` is the full pathname of the NMSAP backup configuration file, `nsrsapsv.cfg`, that is used for the backup.

- b. Follow the prompt instructions for the encryption.

Type the correct values at the command prompts:

- Type the SAP user's operating system username and password at the following prompts:

```
Enter Operating System username:
Enter password:
```

This username and password are stored in encrypted form as the `OS_USR_PASSWD` parameter value in the configuration file.

Note

If the `brbackup` or `brarchive` binary has the sticky bit set, ensure that the operating system username is set correctly:

- For database or tablespace backups, the operating system username must be the name of the `brbackup` owner.
- For archive log backups, the operating system username must be the name of the `brarchive` owner.

For example, the operating system username must be `oracle` for the following file permission:

```
-rwsr-sr-x 1 oracle oinstall 10588975 Dec 1 21:48 brbackup
```

- If Oracle database authentication is used, type the SAP user's Oracle database username and password at the subsequent prompts:

```
Enter Oracle Database username:
Enter password:
```

This username and password are stored in encrypted form as the `ORACLE_USR_PASSWD` parameter value in the configuration file.

The configuration file is updated with the encrypted password authorizations.

4. On the NMSAP client, configure the BR*Tools initialization profile `initDBSID.sap` with the following parameters:
 - Backup device type (`backup_dev_type`)
 - Backup utility configuration file (`util_par_file`)

[Choosing either backint or RMAN as the backup and restore utility](#) on page 88 provides details.

NMSAP parameters for backups and restores

For all NMSAP Oracle operations except scheduled backups that are configured with the wizard, set the required parameters in the `backint` parameter file on the NMSAP client as described in [NMSAP backint parameters](#) on page 95. RMAN backups use the `backint` program to back up metadata.

For RMAN backups and restores, also set NMSAP parameters as described in [NMSAP parameters for RMAN backups and restores](#) on page 111.

For NMSAP scheduled backups configured without the wizard, also set the required `nsrsapsv` parameters in the NMSAP configuration file as described in [NMSAP nsrsapsv parameters](#) on page 103.

Set certain SAP parameters in the `initDBSID.sap` file, as described in the relevant sections of this guide.

Note

For scheduled backups configured with the wizard, you do not need to set any parameters. The configuration wizard sets all the required parameters in the NetWorker Client resource attributes.

NMSAP backint parameters

The parameters in the `backint` parameter file provide the client, server, pool, deduplication, parallelism, and other values to the NMSAP `backint` program.

Make a copy, such as `initDBSID.utl`, for your own use of the original parameter file template, `init_oracle_nmsap.utl`, installed with NMSAP.

Note

When you uninstall NMSAP or upgrade NMSAP to a new release, the system deletes the original template file and any settings you made in the file.

The template file is located in the following directory:

- On Linux and UNIX: `/etc/init_oracle_nmsap.utl`
- On Windows: `NetWorker_install_directory\nsr\bin\init_oracle_nmsap.utl`

NOTICE

If you use this file for scheduled backups, you do not need to set the `NSR_SERVER` parameter in the file. However, if you set the parameter, the parameter setting must match the corresponding attribute on the NetWorker server or an error occurs. Any other settings that are specified in this file, such as the pool name, take precedence over the corresponding setting on the NetWorker server.

To set parameters in your copy of the `backint` parameter file, `initDBSID.utl`, use the following format:

```
parameter=value
```

Follow these guidelines:

- To use parameters, uncomment and modify the parameters as required.
- Parameter names and values are case-sensitive.
- Set all the mandatory parameters.
- If you do not set an optional parameter, then the default value of the parameter is used.

The following table describes the `backint` parameters that NMSAP supports.

Table 9 Supported `backint` parameters

Parameter	Description	Default and valid values
<code>DDBOOST_COMPRESSED_RESTORE</code>	<p>Specifies whether to perform a compressed restore that uses the DD Boost workflow. A compressed restore uses less bandwidth by restoring the backed-up data in a compressed form from the Data Domain system to the application host.</p> <p>A compressed restore can be beneficial in a constrained bandwidth environment, but may impact the restore performance due to the usage of</p>	<ul style="list-style-type: none"> • FALSE (default) = Do not perform a compressed restore that uses the DD Boost workflow. • TRUE = Perform a compressed restore that uses the DD Boost workflow.

Table 9 Supported `backint` parameters (continued)

Parameter	Description	Default and valid values
	<p>compression resources on the Data Domain system and application host.</p> <p>Optional for a restore through the command line or recovery wizard.</p>	
GROUP_BY_FS	<p>If you set this parameter to TRUE, the operation ignores the <code>SAVESETS</code> parameter and groups save sets by file system instead of file size. This efficient grouping of files can improve performance of scheduled backups, index searches, and restore times.</p>	<ul style="list-style-type: none"> FALSE (default). TRUE.
NSR_AES_ENCRYPTION	<p>Specifies whether to encrypt backup data with 256-bit AES encryption.</p> <p>Setting this parameter to TRUE excludes the use of the <code>NSR_COMPRESSION</code> and <code>NSR_CHECKSUM</code> parameters, which you must set to FALSE. If you set more than one of these parameters to TRUE, the priority order is: <code>NSR_COMPRESSION</code>, <code>NSR_CHECKSUM</code>, <code>NSR_AES_ENCRYPTION</code>.</p> <div style="border: 1px solid black; background-color: #0056b3; color: white; padding: 2px; text-align: center; margin: 10px 0;">NOTICE</div> <p>If the encryption phrase has changed between the time of the backup and the time the backup is restored, the <code>NSR_ENCRYPTION_PHRASES</code> parameter must include the original phrase to enable the recovery.</p>	<ul style="list-style-type: none"> FALSE (default). TRUE.
NSR_ARCH_LOGS_SEQUENTIAL	<p>Specifies whether NMSAP backs up archive logs in alphabetical order to optimize the log removal (cleanup) during an archive log backup. Setting this parameter to TRUE causes the <code>backint</code> program to back up archive logs in alphabetical order, which speeds up the log cleanup process during the archive log backup.</p> <p>Optional for manual and scheduled backups of archive logs with <code>brarchive</code>.</p>	<ul style="list-style-type: none"> FALSE (default). TRUE. <hr/> <p>Note</p> <p>When you use the nondefault value TRUE, the load balancing parameter <code>GROUP_BY_FS</code> is ignored during the <code>brarchive</code> backup.</p>
NSR_CHECKSUM	<p>Specifies whether to perform a cyclic redundancy check (CRC) on the backup data. Setting this parameter to TRUE excludes the use of the <code>NSR_AES_ENCRYPTION</code> and <code>NSR_COMPRESSION</code> parameters, which you must set to FALSE. If you set more than one of these parameters to TRUE, the priority order is: <code>NSR_COMPRESSION</code>, <code>NSR_CHECKSUM</code>, <code>NSR_AES_ENCRYPTION</code>.</p>	<ul style="list-style-type: none"> FALSE (default). TRUE.
NSR_CLIENT	<p>Specifies the NetWorker client hostname to use for the client file index for the current backup or restore.</p>	<ul style="list-style-type: none"> Local physical host (default).

Table 9 Supported `backint` parameters (continued)

Parameter	Description	Default and valid values
	If you use NMSAP to back up or restore a virtual cluster client, set this value to the virtual node name.	<ul style="list-style-type: none"> Valid NetWorker client hostname.
NSR_COMPRESSION	<p>Specifies whether to compress the data during a backup before the data passes over the network or is written to the backup device. The compression can speed up the backup process. Compression increases CPU usage on the SAP Oracle server, but reduces the amount of data that is sent to the NetWorker storage node. NMSAP supports only the default NetWorker encryption algorithm. NMSAP does not support backup compression with GZIP or BZIP2.</p> <p>Setting this parameter to TRUE excludes the use of the <code>NSR_AES_ENCRYPTION</code> and <code>NSR_CHECKSUM</code> parameters, which you must set to FALSE. If you set more than one of these parameters to TRUE, the priority order is: <code>NSR_COMPRESSION</code>, <code>NSR_CHECKSUM</code>, <code>NSR_AES_ENCRYPTION</code>.</p>	<ul style="list-style-type: none"> FALSE (default). TRUE.
NSR_DATA_DOMAIN_INTERFACE	<p>Specifies the network interface to use to send backup data to the DD Boost device. Optional for a manual backup only.</p> <p>Set this parameter if you have a Fibre Channel (FC) connection to the DD Boost device. Set this parameter together with <code>NSR_DEVICE_INTERFACE=DATA_DOMAIN</code>. If you do not set <code>NSR_DEVICE_INTERFACE</code> to <code>DATA_DOMAIN</code>, then this parameter is ignored.</p>	<ul style="list-style-type: none"> IP (default) = Backup data is sent over an IP network to the DD Boost device. Any = Backup data is sent over either an IP or FC network to the DD Boost device, depending on the available device. Fibre Channel = Backup data is sent over an FC network to the DD Boost device.
NSR_DATA_VOLUME_POOL	<p>Specifies the NetWorker Media Pool resource that is defined on the NetWorker server, which receives backup data from the SAP Oracle server.</p> <p>Mandatory for a manual snapshot backup. Optional for a manual nonsnapshot backup.</p> <hr/> <p>Note</p> <p>A scheduled backup ignores this parameter.</p> <p>If required, specify the associated storage node by setting the Storage Nodes attribute in the NetWorker Client resource (NMC diagnostic mode must be enabled).</p> <hr/> <p>To use multiple pools to separate data:</p>	<ul style="list-style-type: none"> Most appropriate pool, which the NetWorker server selects (default). Valid name of a NetWorker volume pool.

Table 9 Supported `backint` parameters (continued)

Parameter	Description	Default and valid values
	<p>1. Create separate <code>initDBSID.utl</code> parameter files.</p> <p>2. To specify the parameter file name to use at the command line with <code>brbackup</code> or <code>brarchive</code>, use the <code>-r</code> option.</p> <p>For example, a pool that is named ARCHData is used specifically for archive logs. You can create a separate parameter file for archive logs, for example, named <code>archiveC11.utl</code>, and set the pool attribute to ARCHData. To use the pool to back up the archive logs, type this command at the command line:</p> <pre>brarchive -u sys/admin -d util_file -r archiveC11.utl -m all -s save</pre>	
NSR_DEBUG_LEVEL	Specifies the level of debug messages that <code>backint</code> writes to the debug log file.	<ul style="list-style-type: none"> 0 (default, no debugging). 0 to 9.
NSR_DEVICE_INTERFACE Note This parameter is deprecated. It is supported in the current NMSAP release, but will be unsupported in a future release.	<p>Specifies whether the backup is always stored on the Data Domain device from the specified pool. Optional for manual deduplication backups with the Data Domain media type only. Set the parameter when the backup pool contains a mixture of Data Domain devices and other types of devices. For example: AFTD, tape, and so on.</p> <p>Do not set for scheduled deduplication backups. Instead, set the Data Domain Backup attribute in the NMSAP Client resource when the pool has mixed devices for a scheduled deduplication backup.</p>	<ul style="list-style-type: none"> Undefined (default) = The backup data might be stored on any device from the pool that NetWorker selects. DATA_DOMAIN = The backup data is always stored on the Data Domain device.
NSR_DIAGNOSTIC_DEST	Specifies the directory of the <code>backint</code> diagnostic logs.	<ul style="list-style-type: none"> Default location on UNIX: <code>/nsr/applogs/</code> Default location on Windows: <code>C:\Program Files\EMC NetWorker\nsr\applogs</code>
NSR_DIRECT_ACCESS	<p>Specifies the method that is used to perform a backup to a Data Domain device or an AFTD. Optional for a manual backup with any NetWorker server release or a scheduled backup with NetWorker server release earlier than 8.0. If the target device is on a Data Domain system:</p> <ul style="list-style-type: none"> Data is deduplicated on the NMSAP client when the Client Direct feature is enabled. Data is deduplicated on the storage node when the Client Direct feature is disabled 	<ul style="list-style-type: none"> Default (default) = The backup tries to use the Client Direct feature to bypass the storage node and write data directly to the target device. If the backup cannot use this feature, the backup uses the storage node. No = The backup does not try to use the Client Direct feature. The backup uses the storage node only.

Table 9 Supported `backint` parameters (continued)

Parameter	Description	Default and valid values
	<p>This parameter is ignored during scheduled backups with NetWorker server release 8.0 or later and during restores. For scheduled backups with NetWorker server release 8.0 or later, you can enable the Client Direct feature with the Client Direct setting in the wizard or the Client resource.</p>	<ul style="list-style-type: none"> Yes = The backup tries to use the Client Direct feature. If the backup cannot use this feature, the backup fails. <hr/> <p>Note</p> <p>The Yes value is deprecated. The value is supported in the current NMSAP release, but will be unsupported in a future release.</p>
NSR_DPRINTF	<p>Specifies whether NetWorker core debug messages are written to the NMSAP debug log file.</p> <hr/> <p>Note</p> <p>NSR_DPRINTF applies only if NSR_DEBUG_LEVEL is set to a value greater than 0. Use this parameter for debugging purposes with assistance from Customer Support only.</p> <hr/> <p>Optional for a backup or restore.</p>	<ul style="list-style-type: none"> FALSE (default) = NetWorker core debug messages are not written to the NMSAP debug log file. TRUE = NetWorker core debug messages are written to the NMSAP debug log file.
NSR_ENCRYPTION_PHRASES	<p>Specifies the original phrase to enable the recovery. You can specify multiple phrases to try for the recovery.</p> <p>Mandatory if the NSR_AES_ENCRYPTION phrase has changed between the time of the backup and the time the backup is restored.</p>	<p>Any valid string. For example:</p> <p>NSR_ENCRYPTION_PHRASES = <i>"phrase 1" , "phrase 2"</i></p> <p>Enclose each phrase in double quotes, and separate phrases with a comma. Do not use a comma after the last phrase.</p>
NSR_NWPATH	<p>Specifies the pathname of the directory that contains the NetWorker binaries. Recommended if the NetWorker software is installed in a nondefault location.</p>	<ul style="list-style-type: none"> Platform-specific default location of the NetWorker client binaries (default). Valid directory pathname of the NetWorker client binaries.
NSR_PARALLELISM	<p>Specifies the number of save sets or save streams to send simultaneously to the NetWorker server. Typically, this setting must be equal to the sum of the "target sessions" for all the devices that are dedicated to the NMSAP backup or restore. Configure the NetWorker server to support this parallelism value or greater. Configuring the Client resource without the wizard on page 115 provides details about the parallelism setting in the Client resource.</p> <hr/> <p>Note</p> <p>The NSR_PARALLELISM value is reduced if the value is greater than the SAVESETS parameter value.</p>	<ul style="list-style-type: none"> 8 (default). Any positive integer.

Table 9 Supported `backint` parameters (continued)

Parameter	Description	Default and valid values
		<p>Note</p> <p>For a scheduled backup, this parameter setting must be less than or equal to the Parallelism attribute value in the NetWorker Client resource. If multiple backups run concurrently on the client host, the total of all the NSR_PARALLELISM settings must be less than or equal to the Parallelism attribute value.</p>
NSR_PHYSICAL_HOST_LICENSE	<p>Specifies whether NMSAP is licensed per cluster node or per virtual cluster name in an active-passive cluster environment.</p> <p>Optional in an active-passive cluster.</p>	<ul style="list-style-type: none"> FALSE (default) = NMSAP is licensed per virtual cluster name in the active-passive cluster. TRUE = NMSAP is licensed per cluster node in the active-passive cluster.
NSR_RAW_DEVICE_SKIP_BYTES	<p>Specifies to omit unwanted data from recovery on a raw device. Specifies the initial amount of data to skip.</p> <p>Note</p> <p>When you adjust the amount of data to skip, you require expert knowledge of the operating system and the volume manager specifications.</p>	<ul style="list-style-type: none"> Undefined (default). Valid device name, followed by an equal sign and the amount of data to skip in bytes, kilobytes, megabytes, or gigabytes: NSR_RAW_DEVICE_SKIP_BYTES= /raw/dev1=skip[B K M G] <p>Specify multiple devices by separating the devices with a colon.</p> <p>For example, the following setting skips 8 KB for the raw device /dev/rdisk/c2t4d0s5:</p> <p>NSR_RAW_DEVICE_SKIP_BYTES= /dev/rdisk/c2t4d0s5=8K</p>
NSR_RECOVER_POOL	<p>Specifies the name of the NetWorker volume pool to use for a restore. You can use this option to restore data from a specified volume pool if there are multiple copies (clones) of the backup in different volume pools.</p> <p>Optional for restores. Supported for the following types of restores:</p> <ul style="list-style-type: none"> Restore of a nonsnapshot backup. Restore of a ProtectPoint snapshot backup on a Data Domain system. 	<ul style="list-style-type: none"> Pool that the NetWorker server selects (default). Valid name of a NetWorker volume pool that contains a cloned backup to use for a restore.

Table 9 Supported `backint` parameters (continued)

Parameter	Description	Default and valid values
	<p>Note</p> <p>If required, specify the associated storage node by setting the Recover Storage Nodes attribute in the NetWorker Client resource (NMC diagnostic mode must be enabled).</p>	
NSR_RELOCATION_DEST	For a relocated restore, specifies a new root directory for SAP datafiles when <code>SAPDATA_HOME</code> is changed but the structure of subdirectories under <code>SAPDATA_HOME</code> is not modified.	<ul style="list-style-type: none"> Undefined (default). Same value as the new <code>SAPDATA_HOME</code> value.
NSR_SAVESET_NAME	<p>Specifies a customized save set name for a backup. The save set name must start with <code>backint:</code> or the backup will fail.</p> <p>Optional for manual backups.</p> <p>Note</p> <p>Scheduled backups ignore this parameter. The Save Set attribute in the Client resource determines the save set name for scheduled backups.</p>	<ul style="list-style-type: none"> <code>backint:DBSID</code> (default). User-specified value for the save set name that starts with <code>backint:</code>. For example, if the parameter value is <code>backint:backup1</code>, then the save set name is <code>backint:backup1</code>. <p>Note</p> <p>It is required that you include <code>backint:</code> at the start of the parameter value.</p>
NSR_SAVESET_RETENTION	<p>Specifies the retention policy of a manual backup, as the date when the save set becomes recyclable.</p> <p>Optional for a manual backup.</p> <p>Note</p> <p>This parameter overrides the retention policy that is specified in the NetWorker Client resource. Scheduled backups ignore this parameter.</p>	<ul style="list-style-type: none"> Retention policy that is specified in the NetWorker Client resource for the client (default). Valid date in <code>nsr_getdate(3)</code> format.
NSR_SERVER	<p>Specifies the hostname of the NetWorker server that the NMSAP <code>backint</code> program uses for backup, restore, and inquiry sessions.</p> <p>Note</p> <p>You do not need to set this parameter for a scheduled backup, but if you set the parameter, the value must match the server that started the backup or an error occurs.</p>	<ul style="list-style-type: none"> Local host (default). NetWorker server hostname.
NSR_SS_FORMAT	Specifies the naming convention for the backup save sets. This parameter can be used with the <code>NSR_SAVESET_NAME</code> parameter.	<ul style="list-style-type: none"> old (default). new. old_pid.

Table 9 Supported `backint` parameters (continued)

Parameter	Description	Default and valid values
	<p><code>NSR_SS_FORMAT</code> specifies whether a certain value is added to the base save set name. For a manual backup, the base save set name is as follows:</p> <ul style="list-style-type: none"> When <code>NSR_SAVESET_NAME</code> is not set: backint:<i>DBSID</i> When <code>NSR_SAVESET_NAME</code> is set to backint:<i>value</i>: backint:<i>value</i> <hr/> <p>Note</p> <p>The <code>NSR_SAVESET_NAME</code> parameter setting must start with backint:.</p> <hr/> <p>The <code>NSR_SS_FORMAT</code> setting determines the save set name that is used:</p> <ul style="list-style-type: none"> When set to "old" or not set, the unchanged base save set name is used. When set to "new", the save set name is <i><base_save_set_name>:<full_pathname_of_first_file_in_save_set></i>. <p>If you set each save set to store one file, the value of "new" simplifies the process of browsing the media database. The media database shows each file name as part of the save set name.</p> <ul style="list-style-type: none"> When set to "old_pid", the save set name is <i><base_save_set_name>_<backint_process_ID></i>. When set to "new_pid", the save set name is <i><base_save_set_name>_<backint_process_ID>:<full_pathname_of_first_file_in_save_set></i>. <p>Optional for manual and scheduled backups.</p>	<ul style="list-style-type: none"> new_pid.
RAW_DIR	<p>Specifies the directories for raw disk partitions on UNIX only. Any files below these directories are considered to be raw disk partitions. Do not set this parameter to the <code>/dev</code> or <code>/devices</code> directories, which are already treated as raw devices.</p> <hr/> <p>Note</p> <p>The listed partitions are pointed to by the symbolic links under <code>\$(SAPDATA_HOME)/sapraw/TBS_number/</code>.</p>	<ul style="list-style-type: none"> Undefined (default). Directory pathnames of the raw disk partitions, which are separated by a semicolon (;). For example: RAW_DIR = /oracle/data;/sap/data
SAVESETS	<p>Specifies the number of save sets to divide the files on a client and distribute the backup load. If the value is equal to or greater than the number of database</p>	<ul style="list-style-type: none"> 20 (default). Any positive integer.

Table 9 Supported `backint` parameters (continued)

Parameter	Description	Default and valid values
	<p>files, then a separate save set is made for each file. If the value is less than the number of database files, then a save set might contain more than one file.</p> <hr/> <p>Note</p> <p>All the Oracle BR*Tools metadata files are backed up in a single save set by default when the total size of the files is less than 2 MB. This feature reduces the backup overhead and impact on the NetWorker server. This parameter is ignored if the <code>GROUP_BY_FS</code> parameter is set to <code>TRUE</code>.</p>	
<code>SNAPSHOT_OBJECTS</code>	<p>Configuring the NMSAP parameters for NSM operations on page 166 provides details about the NSM parameters.</p>	

NMSAP `nsrsapsv` parameters

The `nsrsapsv` parameters provide environmental and other values to the NMSAP scheduled backup program, `nsrsapsv`.

You can use these parameters to perform the following operations among others:

- Specify the nondefault locations of required programs and files.
- Configure the system-specific environment variables.
- Identify the specific SAP Oracle database to back up.
- Specify the BR*Tools command and options that are used for scheduled backups.

You can set the parameters in the wizard or in the `nsrsapsv` configuration file, `nsrsapsv.cfg`, for nonwizard configurations. The template file is located in the following directory:

- On Linux and UNIX: `/etc/nsrsapsv.cfg`
- On Windows: `NetWorker_install_directory\nsr\bin\nsrsapsv.cfg`

Make a copy of the configuration file template before you customize the file for backups. You can use any preferred name or location for the customized configuration file. Ensure that the configuration file has read permissions for the group and other users.

Note

When you uninstall NMSAP or upgrade NMSAP to a new release, the system deletes the original template file and any settings you made in the file.

To set parameters in your copy of the `nsrsapsv` configuration file, `nsrsapsv.cfg`, use the following format and guidelines:

- Use this format for each parameter setting:

```
parameter_name = parameter_value
```

- If you back up multiple databases in a single backup configuration, specify the parameter settings in the configuration file as follows:

- For parameter settings common to all the databases, specify the parameter settings outside of the braces.
- For parameter settings unique to specific databases on the SAP Oracle client, group the parameter settings within braces.

The following example shows the correct positions of parameter settings in the configuration file:

```
# Global parameters common to all the databases
parameter1 = value
parameter2 = value
parameter3 = value

DBSID1 {
# Parameter settings for DBSID1
parameter4 = value1
parameter5 = value
}

DBSID2 {
# Parameter settings for DBSID2
parameter4 = value2
}
```

where *DBSID1* and *DBSID2* are Oracle database instances that appear on separate lines in the Save Set attribute of the Client resource for the scheduled backup.

A global parameter appears outside of all the braces. A database-specific parameter appears within the braces after a particular database SID.

- The following precedence rules apply to the parameter settings:
 - Global parameter settings apply to all the Oracle databases in the backup.
 - If a global parameter is set more than once, the last setting takes precedence over all the previous settings of the global parameter.
 - Database-specific parameter settings within braces apply only to the particular Oracle database instance and override the corresponding global parameter settings for the backup of that specific database.
 - If a parameter appears more than once within the same braces, the last setting takes precedence over all the previous settings of the parameter within the braces.
- To use parameters in a scheduled backup, uncomment and modify the parameters as required.
- Parameter names and values are case-sensitive.
- Use full pathnames for parameters that specify a pathname or a file name. The following items are not supported in pathnames and file names:
 - Special Oracle characters, such as ?
 - Environment variables, such as \$ORACLE_HOME and %ORACLE_HOME%
- Specify the full pathname of the configuration file in the Backup Command attribute of the Client resource for the scheduled backup. [Configuring the Client resource without the wizard](#) on page 115 describes the Client resource attributes.

The following table describes the parameters in the `nsrsapsv` configuration file that NMSAP supports.

Table 10 Supported `nsrsapsv` parameters

Configuration parameter	Description	Default and valid values
<p>BR_EXEC</p>	<p>Specifies the <code>brbackup</code> or <code>brarchive</code> command and its options that the <code>nsrsapsv</code> scheduled backup program runs.</p> <p>Mandatory for nonwizard configurations only. Do not use for wizard configurations.</p> <hr/> <p>Note</p> <p>Do not use the <code>-u</code> option, which identifies the username and password of the Oracle database administrator. Instead, encrypt the username and password by using the <code>nsrsapadm -P oracle -z file_name</code> command.</p> <p>Configuring the NMSAP parameters without the wizard on page 93 provides details about the username and password encryption.</p> <hr/> <p>Caution: If you save a wizard configuration to a file, such as <code>nsrsapsv.cfg</code>, the file contains the following parameters that the <code>nsrsapsv</code> program uses to generate the <code>brbackup</code> or <code>brarchive</code> command at runtime:</p> <ul style="list-style-type: none"> • BKUP_TYPE • BKUP_OBJECTS • TABLESPACE • DATAFILE • LOGS_NUM • LOGS_DEL • BRARCHIVE_CLI • BRBACKUP_CLI • SAP_CONFIG <p>Do not use these wizard parameters if you configured the <code>nsrsapsv.cfg</code> file manually.</p>	<ul style="list-style-type: none"> • <code>brbackup</code> (default). • <code>brbackup</code> or <code>brarchive</code> and command line options.
<p>DIR_LIBRARY</p>	<p>Specifies the pathname of the directory that contains the SAP Security Library, <code>SAPSECULIB</code>.</p>	<ul style="list-style-type: none"> • Undefined (default). • Valid full pathname of the <code>SAPSECULIB</code> directory. For example: <code>/usr/sap/SAP/SYS/exe/run</code>
<p>HOMEDRIVE</p>	<p>Specifies the drive name where Windows system files reside. Verify this setting by typing <code>set homedrive</code> at the command line. Optional. Use on Windows only.</p>	<ul style="list-style-type: none"> • Undefined (default). • Valid disk drive. For example: <code>C:</code>

Table 10 Supported `nsrsapsv` parameters (continued)

Configuration parameter	Description	Default and valid values
NLS_LANG	Specifies the language character set in the following format: LANGUAGE_TERRITORY.CHARACTERSET Mandatory parameter. The Oracle documentation provides details.	<ul style="list-style-type: none"> AMERICAN_AMERICA.US7ASCII (default). Valid Oracle setting for NLS_LANG variable.
NSR_BRTOOLS_SECURE_PASSWORD	Specifies whether to use the secure storage password feature, which stores the BR*Tools connection data for the database in a BR*Tools specific Secure Storage in File System (SSFS). BR*Tools Kernel 7.20 Patch 27 or later supports this secure storage password feature. Optional parameter.	<ul style="list-style-type: none"> FALSE (default). TRUE. <p>Note This parameter takes precedence over NSR_BRTOOLS_SECURE_ROLE and any specified database authentication.</p>
NSR_BRTOOLS_SECURE_ROLE	Specifies whether to use the role-based storage of the BR*Tools user and password in the secure storage. The role-based storage assigns the DBA and OPER roles to OS users without the OS users having to belong to the Oracle OS groups dba and oper. BR*Tools Kernel 7.20 Patch 30 or later supports this role-based secure storage feature. Optional parameter.	<ul style="list-style-type: none"> Undefined (default). Valid OS user group name to use for role-based secure storage. <p>Note This parameter takes precedence over any specified database authentication. NSR_BRTOOLS_SECURE_PASSWORD takes precedence over this parameter.</p>
NSR_SAP_SECURE_RUN	Hides the Oracle user password that is passed to the <code>brbackup -u</code> or <code>brarchive -u</code> command from operating system commands, such as <code>ps -ef</code> . Optional parameter. Use on UNIX only.	<ul style="list-style-type: none"> FALSE (default). TRUE.
NSR_SAP_USING_RMAN_OPTION	If you use RMAN to back up database files, set this parameter to TRUE. For example: NSR_SAP_USING_RMAN_OPTION=TRUE	<ul style="list-style-type: none"> FALSE (default). TRUE.
NSR_SAP_WAIT_BRTOOLS_DONE_MINS	Specifies how long (after the user terminates a backup) the <code>nsrsapsv</code> program waits for the <code>brbackup</code> program to do the following: <ul style="list-style-type: none"> Perform a cleanup routine. Remove tablespaces from backup status. 	<ul style="list-style-type: none"> 2 minutes (default). Positive number of minutes.
ORACLE_BIN	Specifies the pathname of the Oracle binaries location. The specified pathname is appended	<ul style="list-style-type: none"> \$ORACLE_HOME/bin (default).

Table 10 Supported `nsrsapsv` parameters (continued)

Configuration parameter	Description	Default and valid values
	<p>to the <code>PATH</code> environment variable so that all the Oracle binaries can be found.</p> <p>Mandatory only if the Oracle binaries are not in the default location, <code>\$ORACLE_HOME/bin</code>.</p>	<ul style="list-style-type: none"> Valid full pathname of the <code>bin</code> directory of the Oracle server installation.
ORACLE_HOME	<p>Specifies the pathname of the home directory of the Oracle server installation. Mandatory parameter.</p>	<ul style="list-style-type: none"> Undefined (default). Valid full pathname of the home directory of the Oracle server installation. For example: <code>/db/oracle/product/10.2.0</code>
ORACLE_SID	<p>Specifies the system identification (SID) for the Oracle instance to be backed up.</p> <p>Mandatory. For a nonwizard configuration, set this parameter either in the configuration file or in the Save Set field of the Client resource.</p> <p>For example, if the save set name in the NetWorker Client resource is <code>backint:SAP</code> and this parameter is not set in the configuration file, then <code>SAP</code> is used for the Oracle SID.</p>	<ul style="list-style-type: none"> Oracle SID derived from the save set name in the NetWorker Client resource that is used for the backup (default). A valid Oracle database SID.
ORACLE_USR_PASSWD	<p>Specifies an encrypted value that contains the SAP user's Oracle database username and password. Optional parameter.</p> <p>Do not manually add or edit this parameter. Use the <code>nsrsapadm -P oracle -z</code> command to set this parameter.</p> <p>Configuring the NMSAP parameters without the wizard on page 93 provides details about the username and password encryption.</p> <p>Passwords that you specify through the wizard are securely stored in a lockbox. The passwords are not stored in the configuration file.</p>	<ul style="list-style-type: none"> Undefined (default). Uneditable encrypted value set with the <code>nsrsapadm -P oracle -z</code> command.
OS_USR_PASSWD	<p>Specifies an encrypted value that contains the SAP user's operating system username and password.</p> <p>Mandatory parameter.</p> <p>Do not manually add or edit this parameter. Use the <code>nsrsapadm -P oracle -z</code> command to set this parameter.</p> <p>Configuring the NMSAP parameters without the wizard on page 93 provides details about the username and password encryption.</p>	<ul style="list-style-type: none"> Undefined (default). Uneditable encrypted value set with the <code>nsrsapadm -P oracle -z</code> command.

Table 10 Supported `nsrsapsv` parameters (continued)

Configuration parameter	Description	Default and valid values
	<p>Passwords that you specify through the wizard are not stored in the configuration file but are securely stored in a lockbox.</p>	
<p>PATH</p>	<p>Specifies the pathname of the NetWorker client binary file and any other required search pathnames.</p> <p>Optional parameter.</p> <p>The specified value is appended to the <code>PATH</code> environment variable. To specify multiple search pathnames, use one of the following two methods:</p> <ul style="list-style-type: none"> • <code>PATH=d:\dir1;d:\dir2;d:\dir1\dir2\dir3</code> • <code>PATH=d:\dir1</code> <code>PATH=d:\dir2</code> <code>PATH=d:\dir1\dir2\dir3</code> 	<ul style="list-style-type: none"> • Undefined (default). • Valid pathnames that are separated by semicolons on UNIX or colons on Windows.
<p>POSTCMD</p>	<p>Specifies a postprocessing script to run after a scheduled backup:</p> <ul style="list-style-type: none"> • The postprocessing script file might need permissions that allow execution by the root user. • The script returns a zero value when it succeeds, and a nonzero value when it fails. • On UNIX, the first line of the script contains the following interpreter directive: <code>#!/bin/sh</code> <p>Optional parameter.</p> <hr/> <p>Note</p> <p>If the scheduled backup fails, the postprocessing script still runs. If the postprocessing script fails, an error message appears but the scheduled backup succeeds.</p>	<ul style="list-style-type: none"> • Undefined (default). • Valid full pathname of a postprocessing script file. The pathname does not contain any spaces. <p>For example, instead of setting <code>POSTCMD</code> to <code>C:\Program Files\Legato\nsr\postcmd.bat</code>, set the parameter to <code>C:\Progra~1\Legato\nsr\postcmd.bat</code>.</p> <p>Also, instead of setting <code>POSTCMD</code> to <code>C:\Program Files\EMC NetWorker\nsr\postcmd.bat</code>, set the parameter to <code>C:\Progra~1\EMC NetWorker\nsr\postcmd.bat</code>.</p> <ul style="list-style-type: none"> • If the value is undefined or invalid, a postprocessing script does not run after the scheduled backup.
<p>PRECMD</p>	<p>Specifies a preprocessing script to run before a scheduled backup:</p> <ul style="list-style-type: none"> • The preprocessing script file might need permissions that allow execution by the root user. • The script returns a zero value when it succeeds, and a nonzero value when it 	<ul style="list-style-type: none"> • Undefined (default). • Valid full pathname of a preprocessing script file. The pathname does not contain any spaces. <p>For example, instead of setting <code>PRECMD</code> to <code>C:\Program Files\Legato\nsr</code></p>

Table 10 Supported `nsrsapsv` parameters (continued)

Configuration parameter	Description	Default and valid values
	<p>fails. The return of a nonzero value causes the scheduled backup to fail.</p> <ul style="list-style-type: none"> On UNIX, the first line of the script contains the following interpreter directive: <pre>#!/bin/sh</pre> <p>Optional parameter.</p> <hr/> <p>Note</p> <p>If the preprocessing script fails, NMSAP does not perform a scheduled backup, an error message appears, and any postprocessing script does not run.</p>	<p><code>\precmd.bat</code>, set the parameter to <code>C:\Program Files\Legato\nsr\precmd.bat</code>.</p> <p>Also, instead of setting <code>PRECMD</code> to <code>C:\Program Files\EMC NetWorker\nsr\precmd.bat</code>, set the parameter to <code>C:\Program Files\EMC NetWorker\nsr\precmd.bat</code>.</p> <ul style="list-style-type: none"> If the value is undefined or invalid, a preprocessing script does not run before the scheduled backup.
<p><code>SAP_BIN</code></p>	<p>Specifies the pathname of the location of the BR*Tools binary files.</p> <p>Mandatory parameter.</p> <p>This location should also be where the <code>backint</code> (UNIX) or <code>backint.exe</code> (Windows) executable resides, after it is manually moved to this location following the NMSAP installation.</p> <p>This location is added to the <code>PATH</code> environment variable so that the BR*Tools binaries and <code>backint</code> can be found.</p>	<ul style="list-style-type: none"> Undefined (default). Valid full pathname of the BR*Tools location. For example: <pre>/usr/sap/SAP/SYS/exe/run</pre>
<p><code>SAPDATA_HOME</code></p>	<p>Specifies the pathname of the root directory of the SAP Oracle datafiles. Mandatory parameter.</p> <p>The SAP documentation provides details.</p>	<ul style="list-style-type: none"> Undefined. Valid full pathname of the root directory of the SAP Oracle datafiles. For example: <code>d:\orant\SAP\</code>
<p>SAP-specific environment variables:</p> <ul style="list-style-type: none"> <code>SAPARCH</code> <code>SAPBACKUP</code> <code>SAPCHECK</code> <code>SAPREORG</code> <code>SAPTRACE</code> 	<p>Mandatory for <code>brbackup</code> to run correctly on Windows systems. These variables are normally set in the SAP environment on Windows. Examples:</p> <pre>SAPARCH=d:\orant\SAP\saparch SAPBACKUP=d:\orant\SAP\sapbackup SAPCHECK=d:\orant\SAP\sapcheck SAPCHECK=d:\orant\SAP\sapcheck SAPTRACE=d:\orant\SAP\saptrace</pre>	<ul style="list-style-type: none"> UNIX default: <code>\$ORACLE_HOME/sapxxx</code> where <code>xxx</code> is the suffix <code>arch</code>, <code>backup</code>, <code>check</code>, <code>reorg</code>, or <code>trace</code>. Windows default: None. Valid full pathname of the SAP log directory.

Table 10 Supported `nsrsapsv` parameters (continued)

Configuration parameter	Description	Default and valid values
SAPSWITCH	<p>Specifies an alternative location of the switch files during <code>file_online</code> backups. Optional parameter.</p> <p>For manual backups, set the parameter in the environment. For scheduled backups, the parameter supports both client-side and server-side configuration files.</p> <p>Do not set the parameter in the <code>backint</code> configuration file. Requires BR*Tools 7.1 or later. If you do not set the parameter correctly, the backup fails and logs a message in the <code>backint</code> debug log. For a successful backup, unset <code>SAPSWITCH</code> and remove the generated switch files.</p>	<ul style="list-style-type: none"> OS-dependent default location: <ul style="list-style-type: none"> On Windows: <code>%SAPBACKUP%</code> On UNIX: <code>\$ORACLE_HOME/sapbackup</code> Valid directory pathname with no spaces. For example: <code>d:\dir1</code>
Any <code>name_path= value</code> pair	<p>Appends values to any environment variable named <code>name_path</code>, such as <code>LD_LIBRARY_PATH</code>, <code>LIBPATH</code>, or <code>SHLIB_PATH</code>.</p> <p>Follow these guidelines:</p> <ul style="list-style-type: none"> If an environment variable with this name exists, then the specified value is appended to the existing value for the environment variable. If an environment variable with this name does not exist, then the environment variable is created. <p>Optional parameter.</p> <hr/> <p>Note</p> <p>Depending on the particular operating system, the <code>LD_LIBRARY_PATH</code>, <code>LIBPATH</code>, or <code>SHLIB_PATH</code> setting is mandatory in the environment. You must set <code>LD_LIBRARY_PATH</code>, <code>LIBPATH</code>, or <code>SHLIB_PATH</code> in the environment variable or in this parameter.</p>	<p>Any valid environment variable and pathname.</p> <p>For example:</p> <p><code>LD_LIBRARY_PATH=/u01/app/oracle/product/11.2.0/dbhome_1/lib</code></p>
Any <code>name= value</code> pair	<p>Adds any environment variable named <code>name</code>. If the environment variable specified by <code>name</code> exists, then the variable is overwritten.</p> <p>Optional parameter.</p>	<p>Any valid environment variable and value. For example:</p> <p><code>BR_TRACE=1</code></p> <p><code>BR_TRACE</code> is set to 1 in the environment, which instructs <code>brbackup</code> or <code>brarchive</code> to print out additional trace information.</p>

NMSAP parameters for RMAN backups and restores

If you select RMAN as the backup and restore utility as described in [Choosing either backupint or RMAN as the backup and restore utility](#) on page 88, then set the required NMSAP parameters for the RMAN backups and restores.

It is recommended that you can set the NMSAP parameters for RMAN backups and restores in the `initDBSID.utl` file, which you specify with the `CONFIG_FILE` parameter. [Specifying RMAN as the backup and restore utility](#) on page 90 provides details.

As an alternative, you can set the NMSAP parameters in the BR*Tools initialization profile `initDBSID.sap` with either the `rman_send` option or the `rman_parms` option.

Note

Set the NMSAP parameters with the `rman_send` option unless stated otherwise in the following table.

The BR*Tools initialization file is in the following directory:

- On UNIX or Linux: `$ORACLE_HOME/dbs`
- On Windows: `%ORACLE_HOME%\DATABASE`

The following table describes the NMSAP parameters to configure the RMAN backups and restores support.

Table 11 Supported NSR_* parameters for RMAN

Parameter	Description	Default and valid values
NSR_AES_ENCRYPTION	Corresponds to the <code>NSR_AES_ENCRYPTION</code> parameter in Table 9 on page 95.	
NSR_CHECKSUM	Corresponds to the <code>NSR_CHECKSUM</code> parameter in Table 9 on page 95.	
NSR_CLIENT	Corresponds to the <code>NSR_CLIENT</code> parameter in Table 9 on page 95.	
NSR_COMPRESSION	Corresponds to the <code>NSR_COMPRESSION</code> parameter in Table 9 on page 95.	
NSR_DATA_VOLUME_POOL	Corresponds to the <code>NSR_DATA_VOLUME_POOL</code> parameter in Table 9 on page 95.	
NSR_DEBUG_LEVEL	<p>Controls the amount of debug information that NMSAP writes to the debug log file, which is in the <code>NSR_DIAGNOSTIC_DEST</code> directory or in the default directory, <code>/nsr/apps/logs</code> (UNIX) or <code>NetWorker_install_path\apps\logs</code> (Windows).</p> <p>This parameter controls the debug level for debug messages that the RMAN operations generate.</p> <p>Optional parameter.</p>	<ul style="list-style-type: none"> • 0 (default, no debugging). • 0 to 9.

Table 11 Supported NSR_* parameters for RMAN (continued)

Parameter	Description	Default and valid values
	<p>Note</p> <p>If you set this parameter in the BR*Tools initialization profile <code>initDBSID.sap</code>, then ensure that you set this parameter with <code>rman_parms</code>, not with <code>rman_send</code>.</p>	
NSR_DEVICE_INTERFACE	Corresponds to the NSR_DEVICE_INTERFACE parameter in Table 9 on page 95.	
NSR_DIAGNOSTIC_DEST	<p>Specifies the directory location of all the NMSAP debug logs that are generated for an RMAN operation.</p> <p>Optional parameter.</p> <p>Note</p> <p>If you set this parameter in the BR*Tools initialization profile <code>initDBSID.sap</code>, then ensure that you set this parameter with <code>rman_parms</code>, not with <code>rman_send</code>.</p>	<ul style="list-style-type: none"> <code>/nsr/apps/logs</code> (UNIX) or <code>NetWorker_install_path\apps\logs</code> (Windows) (default). Valid pathname of the directory where NMSAP generates the debug logs.
NSR_DIRECT_ACCESS	Corresponds to the NSR_DIRECT_ACCESS parameter in Table 9 on page 95.	
NSR_DPRINTF	Corresponds to the NSR_DPRINTF parameter in Table 9 on page 95.	
NSR_ENCRYPTION_PHRASES	Corresponds to the NSR_ENCRYPTION_PHRASES parameter in Table 9 on page 95.	
NSR_NO_BUSY_ERRORS	<p>Specifies whether a scheduled backup fails immediately when the NetWorker server is busy or waits for the NetWorker server to accept the connection.</p> <p>Optional parameter.</p> <p>Note</p> <p>Always set this parameter to FALSE for proxy Oracle backups.</p>	<ul style="list-style-type: none"> FALSE (default) = The scheduled backup waits for the NetWorker server to accept the connection. TRUE = The scheduled backup fails immediately when the NetWorker server is busy.
NSR_NO_MULTIPLEX	<p>When set for a specific RMAN channel, specifies whether multiplexing is disabled during a backup on the NetWorker device that the RMAN channel uses. If you disable multiplexing, the backup cannot write other save sets to the device.</p> <p>Optional parameter.</p> <p>To optimize restore operations, RMAN requires that the NMSAP backups are not multiplexed.</p> <p>Setting the parameter to TRUE can affect the backup performance. For example, the</p>	<ul style="list-style-type: none"> FALSE (default) = Multiplexing is enabled on the device that the RMAN channel uses. TRUE = Multiplexing is disabled on the device that the RMAN channel uses. <p>Note</p> <p>If you use a random access NetWorker device, such as an advanced file device, do not set the parameter to TRUE.</p>

Table 11 Supported NSR_* parameters for RMAN (continued)

Parameter	Description	Default and valid values
	device can sit idle during part of the backup. If the performance is adversely affected, reset the parameter to FALSE.	
NSR_NWPATH	Corresponds to the NSR_NWPATH parameter in Table 9 on page 95.	
NSR_PHYSICAL_HOST_LICENSE	Corresponds to the NSR_PHYSICAL_HOST_LICENSE parameter in Table 9 on page 95.	
NSR_RETENTION_DISABLED	Specifies whether the NetWorker retention policy is disabled. Optional parameter. Set to TRUE to use Oracle policies only (not NetWorker policies) to manage the backup data lifecycle. Then the RMAN catalog and NetWorker indexes cannot become unsynchronized, such as when a NetWorker index entry expires but the corresponding RMAN catalog entry is not expired.	<ul style="list-style-type: none"> FALSE (default) = NetWorker retention policy is enabled and used to manage the lifecycle of the Oracle backup data. TRUE = NetWorker retention policies is disabled. You use only Oracle policies to manage the lifecycle of the Oracle backup data.
NSR_SAVESET_RETENTION	Corresponds to the NSR_SAVESET_RETENTION parameter in Table 9 on page 95.	
NSR_SERVER	Corresponds to the NSR_SERVER parameter in Table 9 on page 95.	

Configuring the data protection policy with NMC

Create a data protection policy for an NMSAP scheduled backup. A policy acts as a container for the backup workflow, action, and group. When you configure the data protection policy, you create and assign the Client resource, group, policy, workflow, and backup action that define the settings for the scheduled backup.

An NMSAP scheduled backup is defined as a type of action within a workflow in the NetWorker server. The Client resource that is created for the backup is assigned to a group, which is assigned to the workflow. The workflow itself is assigned to the data protection policy.

Perform the following steps to configure the data protection policy for an NMSAP scheduled backup. The *NetWorker Administration Guide* and NMC online help provide details on how to use NMC to configure the required NetWorker resources and settings.

NOTICE

Data protection policy configurations do not apply to client-initiated or manual NMSAP backups.

Procedure

1. Open the NMC Administration interface, where you perform all the policy configuration procedures:
 - a. In the NMC **Enterprise** window, right-click the NetWorker server name, and then select **Launch Application**.
The **Administration** window appears.

b. In the **Administration** window, click **Protection**. The *NetWorker Administration Guide* provides details on how to access the NMC interfaces.

2. Ensure that the NetWorker Client resource is configured to define the backup data that the protection policy manages. You can configure the Client resource with or without the configuration wizard:

- Create or modify the Client resource with the wizard according to [Configuring scheduled backups with the wizard](#) on page 91.
- Create or modify the Client resource without the wizard according to [Configuring the Client resource without the wizard](#) on page 115.

3. Ensure that a backup group, also known as a protection group, is created to contain the Client resource.

Each group can be assigned to only one workflow, and each workflow applies to only one group. You can assign a group to a workflow either when you create or edit the group, or when you create or edit the workflow.

When you create the backup group, you specify the group properties and add the Client resource to the group. The *NetWorker Administration Guide* provides details on how to create and edit a group in the NMC Administration interface. Follow the procedures for a basic client group.

4. Ensure that the backup policy is created for the scheduled backup.

A policy can contain one or more workflows, but you can assign a workflow to only one policy.

When you create a policy, you specify the policy name and notification settings. The *NetWorker Administration Guide* provides details on how to create and edit the policy in the NMC Administration interface.

After you create a policy, create the workflows and actions for the policy.

5. Ensure that the backup workflow is created for the scheduled backup policy.

The workflow can include a single action as the traditional NMSAP backup. The workflow can optionally include a check connectivity action before the backup action.

The workflow can also optionally include a clone action after the backup action, to create a cloned copy of the backup save sets. Alternatively, you can create a separate workflow for the clone action and run the clone operation separately from the backup.

When you create a workflow, you specify the following information:

- Start time and schedule window for the action or sequence of actions.
- How often the workflow runs.
- The order of actions to perform.
- The group of Client resources on which the actions occur.

You can create the actions for the workflow either when you create the workflow or separately.

The *NetWorker Administration Guide* provides details on how to create and edit the workflow in the NMC Administration interface.

6. Ensure that the backup action is created for the scheduled backup workflow.

For a regular (nonsnapshot) scheduled backup, create a traditional backup action. You can create actions for a workflow either when you create the workflow or separately.

When you create the backup action, you specify the backup level for each day of the weekly or monthly schedule. You also specify the destination storage node, destination pool, retention period for the backup, and any advanced options as required.

Note

If you want to override the storage node, pool, or retention period setting for a specific client, you can specify the corresponding attribute in the Client resource. The attribute settings in the Client resource override the settings in the backup action.

Optionally, you can create a check connectivity action to precede the backup action and a clone action to follow the backup action in the workflow.

The *NetWorker Administration Guide* provides details on how to create and edit an action by using the Policy Action Wizard. When you create the backup action for the NMSAP scheduled backup with the Policy Action Wizard:

- From the **Action Type** list, select **Backup**.
- From the secondary action list, select **Traditional**.

Configuring the Client resource without the wizard

On the NetWorker server, you can configure a NetWorker Client resource in the NMC program, without using the wizard.

Configure a NetWorker Client resource for each SAP Oracle server (NMSAP client) that requires backup, restore, and inquiry services. Customize the Client resource for an NMSAP scheduled backup by setting the resource attributes.

You can create and edit a Client resource through the Client Properties dialog box in the NMC Administration interface. You must enable the NMC diagnostic mode to view the advanced attributes in the Client resource. The *NetWorker Administration Guide* and online help provide details.

Note

It is recommended that you specify the schedule (backup level), storage node, pool, and retention period in the backup action as part of the data protection policy configuration, not in the Client resource.

If a client requires different settings from other clients in the same backup group, then you can set the specific attributes in the Client resource. In the backup action that you create with the Policy Action Wizard in NMC, you can select **Client Can Override** in the **Client Override Behavior** field. Then, the attribute settings in the Client resource override the properties that are set in the backup action, which is created for the data protection policy.

For example, you can set the retention period to 1 month in the backup action for all clients and then set a 3-month retention in the Client resource for a specific client. Also, you can set a pool in the backup action for all clients and then set a different pool in the Client resource for a specific client.

To override the backup schedule that is specified in the policy-based configuration, you can select or customize one of the preconfigured schedules available in the NetWorker server. You can also create a custom schedule. Then you can select the new schedule in the Schedule attribute of the Client resource. The *NetWorker Administration Guide* provides details on preconfigured and custom schedules.

Set the required Client resource attributes in NMC as shown in the following table. The table lists the basic attributes first, followed by the advanced attributes. You can view the basic attributes in the Client Properties dialog box without enabling the NMC diagnostic mode. To view the advanced attributes, enable the NMC diagnostic mode as described in the *NetWorker Administration Guide*.

Table 12 NetWorker Client resource attributes for NMSAP scheduled backups

Attribute	NMC tab	Description
Basic attributes:		
Aliases	Globals (1 of 2)	Specify all known aliases for the NMSAP host.
Backup command	Apps & Modules	Specify the command to be used for a scheduled backup, either: <code>nsrsapsv</code> which only the wizard can configure (cannot be manually set) or <code>nsrsapsv -f file_pathname</code> which uses the settings of the NMSAP configuration file (<code>nsrsapsv.cfg</code>). Here, <i>file_pathname</i> is the full pathname of the NMSAP configuration file that is created on the NMSAP client host as described in Configuring the NMSAP parameters without the wizard on page 93. The pathname can contain only ASCII characters and can be no longer than 64 characters. The default pathname is as follows: <ul style="list-style-type: none"> On Microsoft Windows: <code>NetWorker_install_directory\nsr\res\nsrsapsvDBSID.cfg</code> On UNIX: <code>/nsr/res/nsrsapsvDBSID.cfg</code> If the pathname contains spaces, you might need to add quotes around the pathname and add an extra backslash after each backslash, for example, "C:\Program Files\dir\file".
Checkpoint enabled	General	Select this attribute to enable a restartable backup.
Directive	General	Leave blank. NMSAP does not support global directives.
Name	General	Specify the hostname of the SAP server host where the NMSAP software is installed.
Parallelism	Globals (1 of 2)	Specify the maximum number of concurrent backup and restore sessions to use for a backup operation. You can use this Client resource attribute instead of the parallelism setting in the parameter file or the wizard configuration.
Protection group list	General	Specify the NetWorker backup group to use for a scheduled backup.
Remote access	Globals (2 of 2)	Specify the SAP username and fully qualified hostname (IP) of a remote host, used to enable backups in a cluster environment and restores of the backups to that remote system:

Table 12 NetWorker Client resource attributes for NMSAP scheduled backups (continued)

Attribute	NMC tab	Description
		<ul style="list-style-type: none"> For a cluster backup, specify <i>sap_user@physical_host</i> for each physical host in the cluster. For restore of a backup from this host to a different destination host, specify <i>sap_user@different_host</i>.
Remote user, Password	Apps & Modules	Recommended for backups on Windows systems. Not required on UNIX systems. These attributes specify the SAP user’s operating system username and password.
Save set	General	<p>Specify the database to be backed up. Use the following format for the save set name: backint:<i>DBSID</i></p> <p>For a client-side scheduled backup that you configured without the wizard, you can optionally specify multiple database instances on separate lines:</p> <p>backint:<i>DBSID1</i></p> <p>backint:<i>DBSID2</i></p> <p>where <i>DBSID1</i> and <i>DBSID2</i> are different database instances on the same SAP Oracle client.</p> <p>You can specify unique parameter settings for each database instance by grouping the parameter settings within braces in the <code>nsrsapsv</code> configuration file as described in NMSAP nsrsapsv parameters on page 103.</p>
Advanced attributes:		
Backup target disks	Globals (2 of 2)	<p>Specify an ordered list of device names of backup devices that the NetWorker server can assign for this client, bypassing the Storage Nodes attribute. This global attribute setting applies to each instance of the client.</p> <p>The devices can be either local or remote to the NetWorker server, but must not belong to a dedicated storage node. Each device must have a Device resource that is configured with the Media Type attribute setting of <code>adv_file</code> or Data Domain.</p>
Checkpoint granularity	General	All NMSAP operations ignore this setting.
Client direct	General	Select this attribute to enable the Client Direct feature for a scheduled backup to a DD Boost device, CloudBoost device, or AFTD. If a Client Direct backup is not possible, the backup routes the data through the storage node instead of sending the data directly from the client to the storage device.
Data Domain backup	Apps & Modules	Optionally select this attribute to ensure that the deduplication backup is always stored on a DD Boost device when the backup pool contains a mixture of DD Boost devices and other types of devices.
Data Domain interface	Apps & Modules	<p>Specify the interface over which the backup occurs to a Data Domain device. This option is used only when you enable Data Domain Backup for the client. Select the correct setting for the attribute:</p> <ul style="list-style-type: none"> Fibre Channel—The backup uses a Fibre Channel (FC) interface. IP—The backup uses an IP interface. Any—The backup uses either an FC or IP interface, depending on the available Data Domain device.

Table 12 NetWorker Client resource attributes for NMSAP scheduled backups (continued)

Attribute	NMC tab	Description
		<p>Note</p> <p>To enable a restore from a Data Domain device over an FC interface, set this attribute to Fibre Channel.</p>
Pool	General	Specify the pool to use for a backup.
Retention policy	General	Specify the minimum length of time that must elapse before backed-up data is eligible to be overwritten on the backup media.
Schedule	General	Select the NetWorker backup schedule to use for a scheduled backup.
Scheduled backup	General	For scheduled backups only. Select the checkbox to enable the Client resource for a scheduled backup.
Storage Nodes	Globals (2 of 2)	Specify the name of each storage node to which the database server can back up data. The database server backs up to the first active enabled storage node in the order that is listed in the attribute. The default storage node name, nrsrserverhost, represents the NetWorker server.

Configuring manual backups

Complete the required steps to configure an NMSAP manual backup.

Procedure

1. Complete all the steps that are described in [Verifying the NMSAP software requirements](#) on page 86.
2. Configure the NMSAP parameter file, `initDBSID.utl`, with the settings for the required NetWorker server and the other backup parameters.

Note

For a manual backup, the settings in the NMSAP parameter file take precedence over settings in the NetWorker Client resource.

[NMSAP backint parameters](#) on page 95 provides details.

3. Set the following parameters in the BR*Tools initialization profile `initDBSID.sap`:

- Backup device type (`backup_dev_type`)
- Backup utility configuration file (`util_par_file`)

[Choosing either backint or RMAN as the backup and restore utility](#) on page 88 provides details.

Configuring restartable backups

You can configure a scheduled restartable backup or a manual restartable backup for an NMSAP client.

You can configure a scheduled restartable backup either with the wizard or without the wizard. If you do not use the wizard, you must use individual settings in the NMC program.

Configuring scheduled restartable backups with the wizard

You can configure a scheduled restartable backup with the wizard by following the instructions in [Configuring scheduled backups with the wizard](#) on page 91 and performing the following additional steps.

Procedure

1. On the **Specify Backup Type and Data Options** page, select the **Checkpoint enabled** checkbox.
2. On the **Specify Performance and Additional Options** page:
 - a. Set the parallelism to the required value for the backup, which should be less than the number of files to be backed up.
 - b. Set the **Number of save sets** field to a value greater than the parallelism.
3. To enable the automatic restart of a failed backup:
 - a. Run the Policy Action Wizard in the NMC program, and set **Retries** to a value greater than zero in the backup action that is created for the scheduled backup.
 - b. In the corresponding workflow, set the **Restart Window** as required.

Note

If you do not enable automatic restart of a failed backup, you must restart the backup manually through the workflow restart option.

Configuring scheduled restartable backups without the wizard

You can configure a scheduled restartable backup without the wizard by following the instructions in [Configuring scheduled backups without the wizard](#) on page 93 and performing the following additional steps.

Procedure

1. On the **General** tab in the Client resource, select the **Checkpoint enabled** checkbox.

Note

NMSAP ignores the Checkpoint Granularity attribute during a checkpoint restartable backup. Changing the attribute setting has no impact on the NMSAP backup.

2. In the `backint` configuration file, `initDBSID.utl`, set the following parameters:

- Set `GROUP_BY_FS` to `FALSE`.
- Set `NSR_PARALLELISM` to the required value for the backup, which should be less than the number of files to be backed up.
- Set `SAVESETS` to a value greater than the parallelism.

[NMSAP backint parameters](#) on page 95 describes these `backint` parameters and how to set them.

3. To enable the automatic restart of a failed backup, use the Policy Action Wizard in the NMC program. Set **Retries** to a value greater than zero in the backup action that is created for the scheduled backup. In the corresponding workflow, you can set the **Restart Window** as required.

Note

If you do not enable automatic restart of a failed backup, you must restart the backup manually through the workflow restart option.

Configuring manual restartable backups

To configure a manual restartable backup, set the required parameters in the `backint` configuration file, `initDBSID.utl`, as described in step 2 of [Configuring scheduled restartable backups without the wizard](#) on page 119.

[Restarting failed manual backups](#) on page 135 describes how to restart a failed manual backup.

Configuring Data Domain Boost backups

This topic provides specific information about using DD Boost with NMSAP. The *NetWorker Data Domain Boost Integration Guide* provides additional information about the DD Boost configuration and initial setup.

Follow the requirements, best practices, and configuration procedures in this section for a deduplication backup that uses only DD Boost devices. The content in this section does not apply to a deduplication backup that uses AFTD or VTL devices.

The NetWorker documentation describes how to configure a Data Domain backup to AFTD or VTL devices. [Configuring NMSAP backups to AFTD storage](#) on page 125 also describes how to configure a Client Direct backup to AFTD devices.

Requirements for DD Boost backups

Before you configure a Data Domain deduplication backup with a DD Boost device, ensure that the NetWorker client and server releases support the DD Boost device. The *NetWorker Module for SAP Release Notes* provides details.

NMSAP supports three types of configurations for Data Domain deduplication backups:

- Deduplication using Client Direct—This configuration eliminates the sending of data over the network between the NMSAP client and the storage node. The deduplicated data is sent directly from the NMSAP client to the DD Boost device.
- Deduplication on a remote storage node—This configuration decreases the amount of network traffic between the storage node and Data Domain system by sending only the unique blocks over the network. However, deduplication requires

all the data to be sent over the network between the NMSAP client and the storage node.

- Deduplication on a local storage node (on the NMSAP client)—This configuration has similar performance to deduplication using Client Direct. However, this configuration requires a storage node on the NMSAP client and additional memory resources.

Best practices for DD Boost backups

During planning and configuration of a deduplication backup, keep in mind the following best practices that can improve the backup performance:

- Do not use database backup encryption or NMSAP backup encryption because the encryption decreases the data deduplication ratio.
- Do not use database backup compression or NMSAP backup compression because the compression decreases the data deduplication ratio.
- Use Client Direct access to a Data Domain device for backups and restores to eliminate data transfer between the NMSAP client and NetWorker storage node. However, using this feature requires an additional 24 MB of memory per data stream on the NMSAP client and also increases the NMSAP CPU usage.
- For RMAN backups only:
 - For database full backups, you can improve the deduplication ratio by not using RMAN multiplexing and by ensuring that the Oracle software does not concatenate data from different files in the same backup piece. To disable multiplexing and prevent concatenation, ensure that `rman_filesperset` is set to 1 in the BR*Tools initialization profile `initDBSID.sap`. The Oracle documentation describes RMAN multiplexing and the number of files in each backup set.
 - For database incremental backups or archived log backups, the Oracle software sends only the changed blocks. As a result, the deduplication ratio is typically low. To increase the backup throughput for these backups, set `rman_filesperset` to a larger value or do not set `rman_filesperset`. If you do not set `rman_filesperset`, then the Oracle software uses the default setting. The Oracle documentation provides more details about `rman_filesperset`.

Data Domain and NetWorker documentation describes the requirements for deduplication backups.

Configuring Client Direct with DD Boost backups

You can configure a scheduled backup or manual backup to a DD Boost device that uses the Client Direct feature to deduplicate data on the NMSAP host. The backup passes only unique data blocks directly to the device, bypassing the storage node.

Procedure

1. Review [Best practices for DD Boost backups](#) on page 121.
2. Configure the DD Boost device, and then enable the Data Domain system for NetWorker operations. The *NetWorker Data Domain Boost Integration Guide* provides details.
3. For a Client Direct backup to a DD Boost device over Fibre Channel, ensure that the SAP user has the correct device permissions as described in the following articles:

- *Fibre Channel Devices with Products using DD Boost in Linux/UNIX Environment* (Document ID dd95007)
- *Fibre Channel Devices with Products using DD Boost in Windows Environment* (Document ID dd95005)

Use the document ID to search for these articles on the Support website at <https://support.emc.com>.

Note

This step is not required for a backup through the storage node or a snapshot backup with NSM.

4. Associate the backup with a pool that contains the DD Boost device that is configured in step 2:
 - For a scheduled backup, associate the required media pool with the Client resource by using the NMC program. The *NetWorker Administration Guide* and NMC online help provide details about using the NMC program.
 - For a manual backup, set the `NSR_DATA_VOLUME_POOL` parameter to the required pool. [Configuring manual backups](#) on page 118 provides details about configuring a `backint` backup. [NSR_DATA_VOLUME_POOL](#) provides details about the parameter for RMAN backups.
5. Follow the configuration instructions in the following table, which are similar to the instructions for configuring a nondeduplication backup.
6. For a Client Direct backup, use the default configuration settings. The Client Direct feature is enabled by default.

With Client Direct enabled, NMSAP tries to perform a Client Direct backup. If a Client Direct backup is not possible, NMSAP performs a backup through the storage node.

Note

The Client Direct setting in the Client resource or wizard field takes precedence over the `NSR_DIRECT_ACCESS` setting in the `initDBSID.utl` parameter file.

Table 13 Configuring a Data Domain backup

Type of Data Domain deduplication backup	Configuration instructions	Additional instructions to use DD Boost over Fibre Channel or if the pool contains Data Domain and other types of devices
Scheduled backup that is configured with the wizard	Configuring scheduled backups with the wizard on page 91	On the Client Backup Options wizard page: <ul style="list-style-type: none"> • Select the Data Domain backup. • Select the proper Data Domain interface. Ensure that you select the Fibre Channel setting if you want to use an FC interface.
Scheduled backup that is configured without the wizard	Configuring scheduled backups without the wizard on page 93	In the Client resource of the NMSAP client: <ul style="list-style-type: none"> • Select the Data Domain Backup attribute. • Select the proper setting of the Data Domain Interface attribute. Ensure that you select the

Table 13 Configuring a Data Domain backup (continued)

Type of Data Domain deduplication backup	Configuration instructions	Additional instructions to use DD Boost over Fibre Channel or if the pool contains Data Domain and other types of devices
		Fibre Channel setting if you want to use an FC interface.
Manual backup	Configuring manual backups on page 118	In the <code>initDBSID.utl</code> parameter file: <ul style="list-style-type: none"> • Set <code>NSR_DEVICE_INTERFACE=DATA_DOMAIN</code>. NSR_DEVICE_INTERFACE provides details. • Set <code>NSR_DATA_DOMAIN_INTERFACE</code> to the proper interface value. Ensure that you set the Fibre Channel value if you want to use an FC interface. NMSAP backint parameters on page 95 provides details.

Configuring storage node with DD Boost backups

You can configure a scheduled backup or manual backup to a DD Boost device, where the backup does not try to use the Client Direct method but instead deduplicates data on a storage node.

Procedure

1. Follow step 1 to step 5 in [Configuring Client Direct with DD Boost backups](#) on page 121.
2. Ensure that the Client Direct feature is disabled by following the correct procedure:
 - For a manual backup, set `NSR_DIRECT_ACCESS=No` in the advanced option table in the wizard or in the `initDBSID.utl` parameter file. [NSR_DIRECT_ACCESS](#) provides details.
 - For a scheduled backup, clear the Client Direct checkbox in the wizard or disable the Client Direct attribute in the NetWorker Client resource.

Configuring CloudBoost backups

This topic provides specific information about using CloudBoost with NMSAP. The latest version of the *NetWorker with CloudBoost Integration Guide* provides additional information about the CloudBoost configuration and initial setup.

[Backups and restores with CloudBoost](#) on page 22 describes the NMSAP support of backups with a CloudBoost device.

You can use the following information to configure a CloudBoost backup to a supported CloudBoost device:

- NetWorker documentation describes the configuration of a CloudBoost backup to a CloudBoost device.
- [Configuring CloudBoost backups to use Client Direct](#) on page 124 and [Configuring CloudBoost backups to use a storage node](#) on page 125 describe the

configuration of a backup to a CloudBoost device through either the Client Direct method or a storage node.

Best practices for CloudBoost backups

Before you configure a CloudBoost backup with a CloudBoost device, ensure that the NetWorker client and server releases support the CloudBoost appliance. The *NetWorker E-LAB Navigator* provides details.

Use Client Direct access for CloudBoost backups to eliminate data transfer between the NMSAP client and NetWorker storage node.

CloudBoost and NetWorker documentation describes the requirements for CloudBoost backups.

Configuring CloudBoost backups to use Client Direct

You can configure a scheduled backup or manual backup to a CloudBoost device that uses the Client Direct feature on the NMSAP host and passes data directly to the CloudBoost device, bypassing the storage node.

Procedure

1. Review [Best practices for CloudBoost backups](#) on page 124.
2. Configure and enable the CloudBoost appliance for NetWorker operations. The latest version of the *NetWorker with CloudBoost Integration Guide* provides details.
3. Configure and enable the CloudBoost devices for NetWorker operations. The latest version of the *NetWorker with CloudBoost Integration Guide* provides details.
4. Associate the backup with a pool that contains the CloudBoost device that is configured in steps 2 and 3:
 - For a scheduled backup, associate the required media pool and storage node with the backup action by using the NMC program. Use the CloudBoost appliance as the storage node. The *NetWorker Administration Guide* and NMC online help describe how to use the NMC program.
 - For a manual backup:
 - Set the NSR_DATA_VOLUME_POOL parameter to the required pool. [NMSAP backint parameters](#) on page 95 provides details on the parameter.
 - Specify the CloudBoost appliance as the storage node in the NetWorker Client resource attributes. [Configuring the Client resource without the wizard](#) on page 115 provides details.
5. For a Client Direct backup, use the default configuration settings, except set NSR_DIRECT_ACCESS=Yes for a manual backup. The Client Direct feature is enabled by default.

With Client Direct enabled, NMSAP tries to perform a Client Direct backup. If a Client Direct backup is not possible, NMSAP reverts to a backup through the storage node.

Note

The Client Direct setting in the wizard field or Client resource takes precedence over the NSR_DIRECT_ACCESS parameter setting.

Configuring CloudBoost backups to use a storage node

You can configure a scheduled backup or manual backup to a CloudBoost appliance, where the backup does not try to use the Client Direct method but instead transfers the backup data through a storage node.

Procedure

1. Follow step 1 to step 4 in [Configuring CloudBoost backups to use Client Direct](#) on page 124.
2. Ensure that the Client Direct feature is disabled:
 - For a manual backup, set NSR_DIRECT_ACCESS=No in the `initDBSID.utl` parameter file. [NMSAP backint parameters](#) on page 95 provides details on the parameter.
 - For a scheduled backup, clear the Client Direct checkbox in the wizard or disable the Client Direct attribute in the NetWorker Client resource.

Configuring NMSAP backups to AFTD storage

You can configure an NMSAP scheduled or manual backup to an AFTD as either a Client Direct backup or a backup that sends data through a storage node.

Configuring Client Direct backups to AFTD

Complete the required steps to configure a scheduled or manual backup that uses Client Direct to an AFTD.

Procedure

1. Configure an AFTD by using either the Device Wizard or the NMC device properties window.

The *NetWorker Administration Guide* provides complete details about AFTD configurations, including considerations for Client Direct clients.
2. Ensure that the NMSAP client has the required access to the AFTD through CIFS. The *NetWorker Administration Guide* provides details.
3. Associate the backup with a pool that contains the AFTD configured in step 1.
4. Follow the required configuration instructions:
 - [Configuring scheduled backups with the wizard](#) on page 91.
 - [Configuring scheduled backups without the wizard](#) on page 93.
 - [Configuring manual backups](#) on page 118.
5. For a Client Direct backup, use the default configuration settings. The Client Direct feature is enabled by default.

With Client Direct enabled, NMSAP tries to perform a Client Direct backup. If a Client Direct backup is not possible, NMSAP performs a traditional backup through the storage node.

Configuring storage node backups to AFTD

Complete the required steps to configure a scheduled or manual backup to an AFTD where the backup does not try to use the Client Direct method but instead sends data through a storage node.

Procedure

1. Follow step 1 to step 4 in [Configuring Client Direct backups to AFTD](#) on page 125.
2. Ensure that the Client Direct feature is disabled by following the required procedure:
 - For a manual backup, set `NSR_DIRECT_ACCESS=No` in the `initDBSID.utl` parameter file. [NSR_DIRECT_ACCESS](#) provides details.
 - For a scheduled backup, clear the Client Direct checkbox in the wizard or disable the Client Direct attribute in the NetWorker Client resource.

Configuring probe-based backups

The NetWorker Probe resource is an optional feature that triggers backups when the system meets user-specified conditions. A probe-based backup is also referred to as an event-based backup.

Note

Unless the system meets the probe conditions, a scheduled backup group that is enabled for a probe does not run.

The system must meet the following conditions for a probe-based backup to be triggered:

- The current time is within a specified window of time. The backup window is defined by the probe start time and end time in the probe-enabled backup Group resource.
- The system meets one of the following conditions:
 - A specified amount of time has elapsed since the previous probe-based backup.
 - One probe or all the probes that are associated with the backup are successful, depending on the probe success criteria that are specified in the backup configuration. You can set the probe success criteria in the probe action.

Configuring a probe-based backup

To configure a probe-based NMSAP backup, you must configure the NetWorker Probe resource and then complete the scheduled backup configuration of the Client resource and other required settings.

Procedure

1. Create a separate NetWorker Probe resource for the supplied NMSAP `nsrsapprobe` program and any other program or script that checks for a user-defined condition. The Probe resource defines the conditions that trigger the probe-based backup.

NOTICE

Because a NetWorker Probe resource stores information on the state of database redo logs, the Probe resource must be associated with a single NetWorker Client resource only. Multiple databases configured through multiple Client resources require a separate Probe resource for each client.

You can associate a script written for a user-defined probe with more than one NetWorker Client resource.

The following table describes Probe resource attributes for NMSAP backups.

Table 14 NetWorker Probe resource attributes for NMSAP backups

Attribute	Description
Name	A unique name that identifies the Probe resource.
Probe Command	<p>Name of the program or script that triggers a probe-based backup.</p> <p>For example, the <code>nsrsapprobe</code> program supplied with NMSAP triggers a backup when the number of Oracle transaction (archived redo) logs generated since the last probe-based backup meets or exceeds the value of the <code>LOG_THRESHOLD</code> parameter.</p> <p>The Probe Command can be a user-defined program or script. User-defined probes on page 129 provides details.</p>
Command Options	<p>Required for the <code>nsrsapprobe</code> program only. A comma-separated list of parameters with their settings as follows:</p> <ul style="list-style-type: none"> • <code>LOG_THRESHOLD</code>—Mandatory. Specifies the number of Oracle transaction (archived redo) logs generated since the last probe-based backup, which will trigger a new probe-based backup. • <code>ORACLE_SERVICE</code>—Mandatory only when database authentication is specified as described in step 4. Specifies the Net service name for the Oracle database that is to be probed. <hr/> <p>Note</p> <p>If this Probe resource is associated with a Client resource that is configured with the wizard and contains the <code>ORACLE_SERVICE</code> parameter, then the values for <code>ORACLE_SERVICE</code> must match in both resources.</p> <hr/> <ul style="list-style-type: none"> • <code>NSR_DEBUG_DIR</code>—Optional. Specifies a valid directory pathname where debug information for probe operations is recorded in a <code>nsrsapprobe_pid.log</code> file. <hr/> <p>Note</p> <p>When you set <code>NSR_DEBUG_DIR</code>, you enable debugging of probe operations.</p> <hr/> <ul style="list-style-type: none"> • <code>TNS_ADMIN</code>—Mandatory if Oracle Net services files are installed in a nondefault location. Specifies the pathname of the nondefault location of the Oracle Net services files. <p>For example:</p> <pre>ORACLE_SERVICE=SAP.world, LOG_THRESHOLD=10</pre>

2. Configure the scheduled backup with or without the wizard by following the instructions in [Configuring the data protection policy with NMC](#) on page 113.

You must configure the required Client resource, group, backup policy, workflow, probe action, and backup action:

- a. Configure the Client resource with or without the configuration wizard. In the Probe Resource Name attribute of the Client resource, specify the name of the Probe resource from step 1. You can associate a Client resource with only one probe.

Note

The configuration wizard does not display the Probe Resource Name field. If you configure a Client resource with the wizard, you must then use NMC to edit the Client resource and set the attribute.

- b. Create the group to contain the Client resource by using the NMC Administration interface. The *NetWorker Administration Guide* provides details on the NMC interfaces.
- c. Create the backup policy and workflow by using the NMC Administration interface. You must assign the group to the workflow, and assign the workflow to the backup policy.
- d. Create the probe action and backup action by using the Policy Action Wizard in the NMC Administration interface:
 - When you create the probe action with the wizard, you must select **Probe** from the **Action Type** list.
 - When you create the backup action with the wizard, you must select **Backup** from the **Action Type** list, and select **Traditional** from the secondary action list.

You must assign the probe action and backup action to the workflow. In the workflow, the probe action must precede the backup action. The backup action is performed only if the probe conditions are met during the probe action.

3. Specify either OS authentication or Oracle database authentication for probe-based backups by using the wizard or by setting a parameter in the `nsrsapsv` configuration file:
 - To specify that probe-based backups use OS authentication, set the OS user credentials without setting the Oracle database user credentials. The OS user credentials are mandatory. For example, you can run the `nsrsapadm -P oracle -z file_pathname` command to encrypt the OS user credentials in the `OS_USR_PASSWD` parameter in the configuration file. [OS_USR_PASSWD](#) provides details.

Note

The OS user password is mandatory on Windows and optional on UNIX. The OS authentication requires `ORACLE_SID` to be set in the configuration file. Ensure that you have set up the OS authentication according to the Oracle documentation.

- To specify that probe-based backups use Oracle database authentication, also set the Oracle database user credentials. Then the probe-based backups will use database authentication by default. For example, you can run the `nsrsapadm -P oracle -z file_pathname` command to encrypt the Oracle database user credentials in the `ORACLE_USR_PASSWD` parameter in the configuration file. [ORACLE_USR_PASSWD](#) provides details.

User-defined probes

The user-defined script or program for probe-based backups must meet the following requirements:

- Name starts with `nsr` or `save`.
- Location is in the same directory that contains the NetWorker client binaries.
- Permissions of the script or program file include the execute permission.
- Returns one of the following code values when the script or program finishes running its probe:
 - 0—Signifies that the backup condition has been met.
 - 1—Signifies that the backup condition has not been met.
 - Other than 0 or 1—Signifies that an error occurred during the probe.

Example probe-based backup with multiple probes

You can configure a probe-based backup with multiple probes. If you select the checkbox **Start backup only after all probes succeed** in the probe action, then the backup starts only after all the probes succeed. Otherwise, the backup starts after any one of the probes succeed.

For example, a probe-based backup is triggered when both of the following conditions are true:

- At least 25 Oracle transaction log files are generated on an SAP Oracle client named, for example, `oraprod_host`. A Probe resource for this condition will use the supplied `nsrsapprobe` program.
- More than two tape drives are idle in a tape library attached to a NetWorker storage node named, for example, `libstore_host`, where the probe-based backup will be sent for storage. A second Probe resource for this condition will use a user-defined script named `nsrjukeboxprobe`.

To configure a probe-based backup with these two conditions, complete the following steps.

Procedure

1. Create the NetWorker Probe resource for the supplied `nsrsapprobe` program with the following attributes:
 - Name: `myxlogs`
 - Probe Command: `nsrsapprobe`
 - Command Options: `LOG_THRESHOLD=25`
2. Create a user-defined script, `nsrjukeboxprobe`, with execute permissions. Store the script in the same directory as the NetWorker binaries on `libstore_host`. When the script runs, it checks for the number of idle tape drives in the library, and returns one of the following values:
 - 0—If more than two tape drives are idle in the library.
 - 1—If two or fewer tape drives are idle in the library.
 - Other than 0 or 1—An error occurred during the probe and no backup will be performed.
3. Create a second NetWorker Probe resource for the user-defined probe with the following attributes:

- Name: myxdrives
 - Probe Command: nsrjukeboxprobe
 - Command Options: (blank)
4. Create a NetWorker Group resource named, for example, probe_group, and configure the required probe attributes with the **Probe Success Criteria** attribute set to **All**.
 5. Create a NetWorker Client resource for the NMSAP backup of oraprod_host with the following attributes:
 - Name: oraprod_host
 - Backup command: nsrsapsv -f
 - Protection group list: probe_group
 - Probe: myxlogs
 - Save set: backint:*DBSID*
 6. Create a NetWorker Schedule resource named skip_all and set the level to skip for each day in the schedule. This will enable a probe to run without running a backup.
 7. Create a Client resource for the libstore_host storage node with the skip-all schedule and the following attributes:
 - Name: libstore_host
 - Backup command: (blank)
 - Protection group list: probe_group
 - Probe: myxdrives
 - Save set: my_skip_set
 - Schedule: skip_all

CHAPTER 5

NMSAP Oracle Operations

This chapter includes the following topics:

- [Performing scheduled backups of SAP Oracle data](#)..... 132
- [Performing manual backups](#)..... 134
- [Reviewing backup and restore session reports](#)..... 136
- [Verifying backup information in the NetWorker indexes](#)..... 137
- [Performing data restore and recovery](#)..... 138
- [Requirements for disaster recovery](#)..... 144
- [Recovering from a disaster](#)..... 144

Performing scheduled backups of SAP Oracle data

You can use the following procedures to test, monitor, and cancel scheduled NMSAP backups of SAP Oracle data, not including snapshot backups.

The *NetWorker Administration Guide* provides information about restarting checkpoint enabled backups.

[NMSAP Oracle Snapshot Backups and Restores](#) on page 155 and [NMSAP Oracle Split-Mirror Backups and Restores](#) on page 173 describe how to perform NMSAP Oracle snapshot backups.

Testing scheduled backups

You can configure scheduled NMSAP backups to run automatically according to the backup schedules. After you configure a scheduled backup, you can manually test the backup with NMC.

Before you begin

Before you test a scheduled backup, ensure that you meet the following requirements:

- You have correctly set up the software environment. You have provided read and write access to a common parent directory for all the files that are associated with the backup. [Verifying the NMSAP software requirements](#) on page 86 provides details.
- You have created the NetWorker Client resource with a correctly configured save set and backup command.
- You have assigned the Client resource to a backup group.
- You have assigned the backup group to a workflow.
- You have assigned the backup workflow to a data protection policy.

Procedure

1. Start the NMC console server. The *NetWorker Administration Guide* and NMC online help provide details on how to access the NMC interfaces.
2. To open the **Administration** window, right-click the NetWorker server name in the NMC **Enterprise** window, and then select **Launch Application**.
3. In the **Monitoring** window, right-click the workflow name for the backup, and then select **Start** from the list box.

Note

Instead of starting only one workflow, you can start all the workflows in a particular policy by right-clicking the policy name and selecting **Start**.

4. Click **Yes** in the confirmation box.
The scheduled backup starts.

Monitoring scheduled backups

You can monitor a scheduled backup and the activities for specific backup policies, workflows, and actions by using the **Monitoring** window in NMC.

Note

The location of information in the **Monitoring** window might vary in different NMC releases.

The **Policies** pane and **Actions** pane in the **Monitoring** window display backup status information during and after a scheduled backup.

The *NetWorker Administration Guide* provides details about viewing scheduled backup information in NMC.

In addition to monitoring a database backup in NMC, you can use the database activity logs, if supported, to monitor the backup results from the database server.

Canceling scheduled backups

You can cancel a scheduled backup by using the following procedure.

The following results occur if you cancel a backup before completion:

- None of the backed-up data might be recoverable.
- The **Volume Save Sets** are marked as incomplete in NMC.

You can cancel a scheduled backup in progress from the NMC program.

Procedure

1. Open the NMC **Administration** window. The *NetWorker Administration Guide* provides details on how to access the NMC interfaces.
2. Select the backup workflow in the **Monitoring** window.
3. Right-click the backup workflow, and then select **Stop**.

The scheduled backup stops after you click **Yes** in the confirmation box.

To manually start a canceled backup process from the beginning, right-click the backup workflow to start and select **Start**. Ensure that the backup successfully completes without interruption.

To cancel the scheduled backup from the NMSAP client host, you can use the following command:

```
brbackup | brarchive -g abort | stop | term | kill
```

The SAP Note 1129197 provides details.

Restarting failed scheduled backups

You can enable the automatic restart of a failed scheduled backup. You can also manually restart a failed backup:

- To enable the automatic restart of a failed scheduled backup, use the **Advanced Options** page in the Policy Action Wizard in NMC. Set **Retries** to a value greater than zero in the backup action that is created for the scheduled backup. In the corresponding workflow, set the **Restart Window** as required.

- To manually start a canceled or failed backup from the beginning, right-click the workflow in the NMC GUI and select **Start**.
- If the first backup fails in a restarted scheduled backup but the restarted backup succeeds, then information about failed save sets might remain in the **Failed** area of the NMC window. The failed save set information only indicates that the initial backup attempt failed and does not reflect the final backup result.

To ensure that only the data that was not backed up in the failed backup is backed up again, configure the backup to take advantage of the checkpoint restart option, as described in [Configuring restartable backups](#) on page 119.

Note

If the restart does not occur within the NetWorker restart window, the next checkpoint-restart backup backs up all the data.

Performing manual backups

You can use the following procedures to perform manual NMSAP backups of SAP Oracle data, and also monitor and cancel the manual NMSAP backups.

Running manual backups

Before you run a manual backup, ensure that you meet the following requirements:

- You have correctly set up the software environment. You have provided read and write access to a common parent directory for all the files that are associated with the backup. [Verifying the NMSAP software requirements](#) on page 86 provides details.
- You have set the server parameter in the NMSAP parameter file, `initDBSID.utl`, for the required NetWorker server. [NMSAP backint parameters](#) on page 95 provides details.
- You have set the BR*Tools initialization profile `initDBSID.sap` with parameters for the following items:
 - Backup device type (`backup_dev_type`)
 - Backup the utility configuration file (`util_par_file`)

[Choosing either backint or RMAN as the backup and restore utility](#) on page 88 provides details.

You can perform a manual backup as illustrated by the following examples.

Procedure

1. Type the SAP backup command with the required parameters to back up the SAP Oracle database or the selected objects to the NetWorker server.

For example:

- Offline backup:

```
brbackup -m all -t offline [-d util_file]
```

- Online backup:

```
brbackup -m backup_objects -t online [-d util_file_online]
```

[Examples of SAP Oracle Command Options](#) on page 183 describes the available `brbackup` command options.

2. If you perform an online backup, run the following command to back up the archived redo logs:

```
brarchive
```

Note

Without the redo logs, you can recover a database that was backed up online only to the time of its last full backup.

3. Run the following command to back up nondatabase files or directories:

```
brbackup -m {sap_dir | ora_dir | all_dir |  
full_directory_path | nondatabase_file_path}
```

[Directory backups and restores](#) on page 30 provides details.

Monitoring manual backups

Operational messages about the status of manual NMSAP backups are displayed at the command line or GUI where the backup is started.

The NMC program provides a centralized view of the following activity:

- All the NetWorker server backup and restore activity.
- Device and library operations and managed events that require user intervention.

The *NetWorker Administration Guide* describes how to review NMC progress and completion messages.

[Troubleshooting and Error Messages](#) on page 189 describes how to review diagnostic messages and error messages.

Canceling manual backups

Cancel a running manual backup by performing one of the following steps:

Procedure

- Press **Ctrl-c** or the equivalent “attention” keyboard shortcut on the system.
- Type the following command:

```
brbackup | brarchive -g abort | stop | term | kill
```

The SAP Note 1129197 provides details.

Restarting failed manual backups

When a backup session fails, you can restart the backup operation from the beginning by rerunning the `brbackup` command.

Alternatively, you can restart the backup of only the files that failed to be backed up:

Procedure

1. On the NMSAP host, inspect the backup session log and troubleshoot the error messages. [Reviewing backup and restore session reports](#) on page 136 provides details.
2. To complete the backup, run the following command at the command line:

```
brbackup -f brbackup_log_name1[,brbackup_log_name2,...] |
yyyy-mm-ddhh.mi.ss | number_of_days | last
```

Example 1 Restarting failed backups

Run the required `brbackup` command to back up files that failed to be backed up:

- To back up the files that failed to be backed up during the last two backup sessions:
 1. Find the backup logs for these two sessions in the SAPBACKUP directory, for example, `beemhgkr.anf` and `beemhzwi.anf`.
 2. Run the following command for these logs:

```
brbackup -f beemhgkr.anf,beemhzwi.anf
```

- To back up the files that were not backed up during the last session, run the following command:

```
brbackup -f last
```

- To back up the files that failed to be backed up in all the sessions that were run in the last three days, run the following command:

```
brbackup -f 3
```

Reviewing backup and restore session reports

During backup sessions or restore sessions, the NMSAP `backint` program appends a report to a sessions log file on each NMSAP host.

The default location for the log is as follows:

- On Microsoft Windows: `NetWorker_install_directory\nsr\applogs`
- On UNIX or Linux: `/nsr/applogs`

The default format for the log file name is `backintDBSID.log.raw`.

This sessions log is in I18N format. Run the log through the NetWorker `nsr_render_log` utility to make the log readable.

Verifying backup information in the NetWorker indexes

The *NetWorker Administration Guide* provides details about the NetWorker online indexes.

You can use the `mminfo` and `nsrinfo` commands to review information about NMSAP scheduled backups and manual backups in the NetWorker online indexes:

- Query the backup information in the media database by using the `mminfo` command. For example:

```
mminfo -v -s NetWorker_server_hostname -c NMSAP_client_hostname
```

Note

The deduplication save set size (`size` field) reported by the `mminfo` command includes only the size of the NetWorker save set metadata.

Use the appropriate `mminfo` command option to obtain details about a Data Domain deduplication backup:

- To view only the save sets that are created as part of a Data Domain deduplication backup, use the `mminfo` command with the `-q DataDomain` option.
- To list the extended attributes for a deduplication backup, add the `-S` option, which provides information about the total size of the protected data and the amount of new data that was passed during the backup.

The following example shows the result for a Data Domain deduplication backup:

```
# mminfo -S -q DataDomain -c oak

ssid=3138980225 savetime=02/11/2013 07:29:31 AM (1360585771)
bu-staples:backint:SAP level=full sflags=vF
size=52440380 files=8 insert=02/11/2013
create=02/11/2013 complete=02/11/2013 browse=03/11/2013
11:59:59 PM retent=02/11/2014 11:59:59 PM

clientid=e78e210a-00000004-511148be-5119091d-00491100-7523d243
      *ACTUAL_HOST: bu-staples;
      *backup start time: 1360585771;
*ss data domain backup cloneid: 1360585772;
*ss data domain dedup statistics:
"v1:1360585772:52648196:52640041:904993";
      group: sapdd;
Clone #1: cloneid=1360585772 time=02/11/2013 07:29:32
AM retent=02/11/2014 flags=F
      frag@ 0 valid=3155757360 file/rec= 0/0
rn=0 last=02/11/2013
```

- Query the information about the backed-up files in the client file index by using the `nsrinfo` command. For example:

```
nsrinfo -s NetWorker_server_hostname NMSAP_client_hostname
```

The `nsrinfo` command can produce very verbose output.

The *NetWorker Command Reference Guide* and *NetWorker Administration Guide* describe the `nsrinfo` command and `mminfo` command.

Performing data restore and recovery

You can perform NMSAP restore and recovery operations on an SAP Oracle host by using the NMSAP recovery wizard or by using the SAP BrGui interface or the `brrestore` or `brrecover` command.

NMSAP can restore and recover only the data that you backed up with NMSAP or with the Fujitsu NetWorker Module for SAP R/3 version 3.0.

NOTICE

You can restore only the files for which you have read permission, as based on the files' operating system permissions at the time that the files were backed up.

On a UNIX or Linux system, the read permission is associated with the numeric user ID (UID) and group ID (GID), not the username or group name. Ensure that the UID and GID of the user that performs the restore matches the IDs associated with the files at backup time.

The following topics provide details about how to perform a restore and recovery with or without the NMSAP Oracle recovery wizard.

Performing data restore and recovery with the NMSAP recovery wizard

You can perform NMSAP restore and recovery operations on an SAP Oracle host by using the NMSAP recovery wizard.

Before you begin

Before you use the NMSAP recovery wizard, you must meet the following requirements:

- The NMC user that starts the wizard (the wizard user) has the Remote Access NetWorker privileges on the NetWorker server that contains the NMSAP client configuration.
- Communication between the NMC server, NetWorker server, and NMSAP client uses NetWorker `nsrauth` authentication. The NetWorker documentation provides requirements for `nsrauth` authentication.
- You have configured the NMSAP environment with all the requirements. [Verifying the NMSAP software requirements](#) on page 86 provides details.
- You have created the NetWorker Client resource for the NMSAP client by using one of the following methods:
 - Backup configuration wizard in NMSAP
 - Client-side configuration method without the wizard, where the value of the Save Set attribute of the Client resource has the `backint: prefix`

Note

The NMSAP recovery wizard does not support redirected restore and recovery.

You can use the following procedure to recover an entire database or a subset of database objects, such as a tablespace or a datafile.

Procedure

1. Start the **NetWorker Management Console** software.
2. Open the **Administration** window:
 - a. In the **Console** window, click **Enterprise**.
 - b. In the left pane, select a NetWorker server in the **Enterprise** list.
 - c. In the right pane, select the application.
 - d. From the **Enterprise** menu, click **Launch Application**.

The Administration window appears as a separate application.
3. In the **Administration** window, click **Protection**.
4. In the **Protection** window, click **Clients**.
5. To start the wizard, right-click the NMSAP client in the right pane, and then select **Recover**.
6. On each wizard screen that appears, specify the required values for the restore and recovery configuration.

Each wizard screen includes an online help button that you can click to access descriptions of all the fields and options on the screen.

You can select to start the restore or recovery immediately from the wizard or schedule the operation to start later.

Restoring from a checkpoint restarted backup with the recovery wizard

NMSAP 9.1 introduced support for use of the NMSAP recovery wizard to restore either all the database objects or any specified tablespaces and datafiles from a checkpoint restarted backup.

Perform the following steps to use the NMSAP recovery wizard for a restore of a checkpoint restarted backup. These steps assume that the restarted backup has been completed.

Procedure

1. Follow the instructions in the preceding topic to start the NMSAP recovery wizard.

On each wizard page, specify the required values for the particular operation. Each wizard page includes an online help button that you can click to access descriptions of the fields and options on the page.
2. On the **Select the Data Objects** page, select the last restarted backup that completed successfully. The following message appears on the wizard page:

```
This is a checkpoint restarted backup. All the saved database
objects are listed as follows.
```

The **Database Objects** pane displays all the database objects that were saved in the previous failed restarted backups, plus the objects that were saved in the last successful restarted backup.

Both the message about the checkpoint restarted backup and the list of all the database objects appear on this wizard page only when you select the last successful restarted backup.

Note

If you select a failed backup instead of the last successful restarted backup, then the **Database Objects** pane displays only the objects that were saved in that particular backup, not any objects that were saved in the previous failed restarted backups.

3. In the **Database Objects** pane, select the required database objects for the restore. You can select all or only some of the database objects:
 - To perform a restore of the whole database (with or without relocation), select all the database objects.
 - To restore only certain database files (with or without relocation), select only those datafiles.
4. On the **Select the Recovery Type or Restore Only** page, select **Copy selected datafiles without applying redo logs** to restore the database objects, including the saved objects from the previous failed restarted backups, with or without specifying the new location for the datafiles.

Performing data restore and recovery without the NMSAP recovery wizard

You can perform all NMSAP restore and recovery operations on an SAP Oracle host by using the SAP BrGui interface or the `brrestore` or `brrecover` command.

You can use the following procedure to recover an entire database or a subset of database objects, such as a tablespace or a datafile.

Procedure

1. (Optional) To restore the data to a different SAP Oracle host (destination host) than the one that was backed up:
 - On a UNIX or Linux system, ensure that the SAP user on the destination host has read permission to the backed-up files as described in the NOTICE in [Performing data restore and recovery](#) on page 138.
 - Follow the disaster recovery steps to re-create the environment and restore the configuration files and BR*Tools logs.
 - Perform the steps described in this procedure on the destination host.
2. To restore data from a DD Boost device over Fibre Channel, ensure that the SAP user has the correct device permissions as described in the following articles:
 - *Fibre Channel Devices with Products using DD Boost in Linux/UNIX Environment* (Document ID dd95007)
 - *Fibre Channel Devices with Products using DD Boost in Windows Environment* (Document ID dd95005)

Use the document ID to search for these articles on the Support website at <https://support.emc.com>.

Note

This step is not required for a restore through the storage node or a restore from a backup that was performed with NSM.

3. Ensure that you have configured the NMSAP environment with all the requirements. [Verifying the NMSAP software requirements](#) on page 86 provides details.
4. Ensure that you have configured the BR*Tools initialization profile `initDBSID.sap` for either `util_file` or `rman_util` as the backup device type. Otherwise, use the required `brrestore` options or `brrecover` options. [Choosing either backint or RMAN as the backup and restore utility](#) on page 88 provides details.
5. Ensure that you have configured the NMSAP parameter file, `initDBSID.utl`, for the required parameters:

- The `NSR_SERVER` parameter specifies the hostname of the NetWorker server that contains the backup to be restored.
- The `NSR_CLIENT` parameter specifies the hostname of the NMSAP host that was backed up if that host is different than the destination host.
- The `NSR_PARALLELISM` setting is the same as the setting that was used to create the backup. Typically, you set the parallelism to the number of target sessions that the devices accept, which must be equal to or less than the NetWorker parallelism.
- If you restore the SAP Oracle data to a new location and only the top common data directory changes but the subdirectory structure remains the same as it was at backup time, then `NSR_RELOCATION_DEST` can specify the new top data directory to improve the restore performance.

The BR*Tools programs determine the new destination directory, for example, `brrestore -m object=new_destination`.

If the common directory for files being restored, as determined by `brrestore`, does not match the path set with `NSR_RELOCATION_DEST`, then the restore ignores the `NSR_RELOCATION_DEST` setting.

- Optionally, `NSR_RECOVER_POOL` can specify the pool from which to restore the backup when multiple backup copies (clones) are available.

[NMSAP backint parameters](#) on page 95 and [Examples of brrestore command syntax and options](#) on page 185 describe these configurations.

6. Ensure that the backup to be restored exists before you perform a restore operation. For example, to inquire for the latest NMSAP BACKINT backup by using the BR*Tools verify functionality, type the following command:

```
brrestore -b last -verify only_conf
```

The BR*Tools documentation provides details on the `-verify` options.

You can also verify that the backup exists in the NetWorker indexes. [Verifying backup information in the NetWorker indexes](#) on page 137 provides details.

7. Prepare for the restore operation:
 - For a full restore, shut down the Oracle database instance.
 - For the restore of a single database object, take the database object offline.
8. Perform the restore operation by using the BR*Tools interfaces.

NOTICE

The `brrestore` program that is used for a restore operation first deletes all the original files to be restored before the program runs `backint` to restore the backed-up files. The `brrestore` program can be run directly from the command line or indirectly from the `brrecover` command or BrGui interface. You lose the original files if `brrestore` or `backint` fails.

Perform one of the following actions to prevent these issues:

- Restore the files to a different location that does not include any files by using the `-m` option and specifying the restore destination, for example:

```
brrestore -m tablespace_name=restore_directory
```

- Use the `brrestore -NFD` option to prevent deletion of the original files by `brrestore`.

To restore a restarted backup, specify each BR*Tools log produced by the initial backup and subsequent restart tries for the `brrestore` command or `brrecover` command. For example, if you started the NMSAP backup and the backup needed two restart tries before completion, run the `brrestore -b backup_log` command three times and use the proper log name each time. The list of BR*Tools catalog files is logged in both of the following locations:

- `backint` logs in the `nsr/appllogs` directory
- BR*Tools SAPBACKUP location

To restore data from a directory (nondatabase) backup, use the `brrestore -m non_db` command. When you restore the SAP directory data, prevent deletion of the BR*Tools and `backint` binaries during the restore by performing a relocated restore. For example, use the following command:

```
brrestore -m non_db=restore_directory
```

[Examples of SAP Oracle Command Options](#) on page 183 contains examples of the `brrestore` and `brrecover` commands and options. The SAP documentation provides details about these commands and other SAP commands.

9. To apply redo logs to recover a database, refer to the SAP and Oracle documentation.

[Reviewing backup and restore session reports](#) on page 136 provides details about backup and restore log information.

Restoring from a checkpoint restarted backup without the recovery wizard

When the checkpoint restart feature is enabled and you complete a backup by performing checkpoint restarts, a warning message might appear when you run `brrestore` to restore the backup. The warning message appears because the completed backup is stored in multiple save sets for the checkpoint restarted backup and `brrestore` cannot restore all the save sets in one restore operation.

The following type of warning message might appear when you run `brrestore` to restore the backup:

```
BR0437W File file_name to be restored was not backed up
```

Perform the following steps to complete the restore of the checkpoint restarted backup.

Procedure

1. Find the `brbackup` log file on which the restore is based.

The `brbackup` logs are located in the directory `%SAPDATA_HOME%\sapbackup`, with the file name extension `aff`. Check the time to find the log to which you want to restore.

2. Open the `brbackup` log file in a text editor, and find the following type of line in the file:

```
BR0091I <number> files were already saved in:
<previous1>.aff, <previous2>.aff,...
```

3. For each of the previous log files, run `brrestore` with the parameter `-b <previous_log_file>.aff`.

Restarting a restore for files that failed a restore

During a restore operation, NMSAP tries to restore all the requested files, even if some files fail to restore. When a restore session is complete, you can use the following procedure to restart the restore operation for files that failed to restore.

Procedure

1. On the NMSAP host, inspect the restore session log and troubleshoot the error messages for files that failed to restore. [Reviewing backup and restore session reports](#) on page 136 provides details.
2. Complete the restore by applying the `brrestore -f` command to the required `brrestore` logs.

Examples:

- To restore the files that failed to restore during the last two restore sessions:
 - a. Find the restore logs for these two sessions in the `SAPBACKUP` directory, for example, `reaxdwie.rsb` and `readwap.rsb`.
 - b. Type the following command for these logs:

```
brrestore -f reaxdwie.rsb, readwap.rsb
```

- To restore the files that were not restored during the last restore session, type the following command:

```
brrestore -f last
```

- To restore files that failed to restore in all the restore sessions that ran in the last three days, type the following command:

```
brrestore -f 3
```

Requirements for disaster recovery

For a comprehensive disaster recovery plan, fully reconstruct the computing environment and all the SAP Oracle server (NMSAP host) files that are associated with maintaining data. [Importance of backups and the backup lifecycle](#) on page 19 describes the impacts of incomplete protection.

Maintain accurate and complete records of the network and system configurations. Keep all the original software media and the following items in a safe location:

- Original operating system media and patches
- Original NetWorker media
- Device drivers and device names
- File system configuration
- IP addresses and hostnames
- NetWorker bootstrap and client index information

You need the NetWorker server bootstrap and client index information to perform disaster recovery of the NetWorker server, which is a separate procedure that is not covered in this chapter.

The *NetWorker Disaster Recovery Guide* describes how to recover the NetWorker server and a NetWorker client or storage node from various types of disasters.

Recovering from a disaster

To recover from a disaster, first restore lost Oracle and SAP configuration files and lost BR*Tools backup log files according to the following instructions. After you restore these files, you can perform a database point-in-time recovery or a whole database reset according to the instructions in [Performing data restore and recovery](#) on page 138.

Restoring the required Oracle and SAP BR*Tools files

The following procedure is a concise version of the disaster recovery steps that are described in the SAP documentation. The steps are modified for the specific requirements of NMSAP. You can perform this procedure on the original host or a new host, both referred to as the destination host.

NOTICE

You can restore only the files for which you have read permission, as based on the files' operating system permissions at the time that the files were backed up.

On a UNIX or Linux system, the read permission is associated with the numeric user ID (UID) and group ID (GID), not the username or group name. The UID or GID of the user performing the restore must match the ID associated with the files at backup time.

Procedure

1. (Optional) To restore the data to a different SAP Oracle host (destination host) than the one backed up:
 - a. On the NetWorker server that contains the backup to be restored:
 - Create a generic Client resource for the destination host if one does not yet exist.
 - Set the Remote Access attribute in the Client resource of the backed-up NMSAP host to *sap_user@destination_host*.
 - b. Perform the following steps on the new destination host.
2. If the entire SAP Oracle system is lost:
 - a. Reinstall all the required software components as described in [NMSAP and associated software](#) on page 36.
 - b. Reconfigure the SAP data layout, such as the SAPDATA_HOME directory and its subdirectories, to the same state as before the disaster.
3. Load the storage volumes with the required Oracle and SAP configuration files and the BR*Tools backup log files on the NetWorker storage node.
4. Configure the BR*Tools profile file, *initDBSID-dr.sap*, and NMSAP parameter file, *initDBSID-dr.utl*, for recovery on the destination host.

Ensure that the NMSAP configuration file contains at least the following parameters:

- The `NSR_SERVER` parameter specifies the hostname of the NetWorker server that contains the backup to be restored.
 - The `NSR_CLIENT` parameter specifies the hostname of the NMSAP host that was backed up, if that host is different than the destination host.
5. On the destination host, start BR*Tools or BrGui and follow the onscreen instructions to perform a disaster recovery of profiles and logs.

For example, the following steps show how to use BR*Tools for disaster recovery of profiles and logs:

- a. In the **brtools** menu, select **Restore and Recovery**, and then select **Disaster recovery**.
- b. On the page **BRRECOVER options for disaster recovery**, set the location of the BR*Tools profile file and the NMSAP configuration file for use by `brrecover`.

Note

If you are restoring the original BR*Tools profile or NMSAP configuration file, ensure that the files used for the disaster recovery have different names or are stored in a different location than the original files to be restored.

- c. On the page **Device type for restoring profiles and log files from BRBACKUP | BRARCHIVE backup**, select **Backup utility**.
- d. On the page **Parameters for restoring profiles and log files from BRBACKUP backup utility**, specify the files to restore as they appear in the NetWorker client index.
- e. On the page **Restore of profiles and log files from BRBACKUP backup**, select the components that you want to restore.

The SAP documentation provides more details about disaster recovery.

Recovering an SAP Oracle database after disaster

After you restore the correct SAP BR*Tools profiles and logs on the NMSAP host, follow the normal BR*Tools recovery procedure to perform database point-in-time recovery or database reset.

[Performing data restore and recovery](#) on page 138 provides the procedure to recover an SAP Oracle database.

The SAP documentation provides more details about database recovery.

CHAPTER 6

SAP Oracle in Cluster and RAC Environments

This chapter includes the following topics:

- [SAP Oracle cluster systems](#).....148
- [Oracle RAC systems](#).....151

SAP Oracle cluster systems

A cluster environment consists of two or more linked hosts with shared storage, called cluster nodes, which work together to provide a resilient database processing platform.

In an active-passive cluster, some nodes are active while others are standby, waiting to take over the processing when an active node fails. A user can connect to the cluster by using a virtual cluster name or IP address, regardless of which nodes are active. You normally implement active-passive clusters for high availability solutions or to improve computer performance.

An Oracle Real Application Clusters (RAC) system provides a single database that multiple Oracle instances can access simultaneously as an active-active application cluster configuration.

This section describes the procedures for active-passive cluster configurations. [Oracle RAC systems](#) on page 151 describes the procedures for Oracle RAC configurations.

Client parameter setting for cluster systems

During an NMSAP backup, the NetWorker server creates entries about the backed-up data in the online client file index. During an NMSAP restore, you can retrieve the data by first searching the client file index.

The `NSR_CLIENT` parameter provides the following information to the NetWorker server:

- During a backup, the name of the NetWorker client whose index file is used to record the backup information.
- During a restore, the name of the NetWorker client whose index file is used to search for the data to be restored.

If you do not set the `NSR_CLIENT` parameter, NMSAP uses the name of the local host (cluster node), not the virtual cluster host, for the operations during cluster backups and restores. Because the local hostname can change over time and cause confusion and errors, use the virtual cluster name for the `NSR_CLIENT` parameter.

The value (default or explicitly defined) of `NSR_CLIENT` that is used for a backup must be the same as the `NSR_CLIENT` value used for the restore of that backup.

Set the `NSR_CLIENT` parameter to the virtual cluster hostname in a cluster environment to enable the restore of backup data no matter which cluster node was used during the backup.

NSR_PHYSICAL_HOST_LICENSE setting for cluster systems

By default, NMSAP is licensed per virtual cluster host and you require a license for each virtual cluster hostname that is backed up.

Set the parameter `NSR_PHYSICAL_HOST_LICENSE=TRUE` to enforce that NMSAP is licensed per cluster node, not per virtual cluster hostname.

[NSR_PHYSICAL_HOST_LICENSE](#) describes the parameter.

Configuring scheduled backups in a cluster with the wizard

You can use the wizard or nonwizard method to configure a scheduled backup with the Backint interface in a cluster. This topic describes the configuration procedure with the wizard.

Procedure

1. Ensure that the NetWorker server is remote and not a part of the cluster environment.
2. Ensure that you have installed NMSAP on a local disk on all the physical nodes of the cluster that are designated to perform a backup.
3. Follow the procedure for [Configuring scheduled backups with the wizard](#) on page 91, keeping in mind the following cluster-specific requirements:
 - On the **Specify the Client Name** page, type the name of the virtual host for the cluster, and then select the **Virtual Client** checkbox.
 - On the **Specify the Preprocessing, Postprocessing, and Additional Options (Optional)** page, in the **Advanced Options** table:
 - Set the `NSR_CLIENT` parameter to the virtual hostname. [Client parameter setting for cluster systems](#) on page 148 provides details.

Note

When you add the `NSR_CLIENT` parameter in the **Advanced Options** table, a pop-up message might state that this parameter is not recognized. You can ignore this message.

-
- To specify the correct NMSAP licensing if required, set the `NSR_PHYSICAL_HOST_LICENSE` parameter. [NSR_PHYSICAL_HOST_LICENSE setting for cluster systems](#) on page 148 provides details.
 - On the **Select the NetWorker Client Properties** page, add `sap_user@physical_host` to the **Remote Access** field for each physical host in the cluster.

Results

With the previous settings, the wizard performs the following actions:

- Creates a NetWorker Client resource for the virtual host with the usual settings for scheduled backups and the following additional settings:
 - The Backup Command attribute contains `-c virtual_client_name`.
 - The Remote Access attribute contains the `sap_user@physical_host` entries.
- If a NetWorker Client resource does not exist, creates a generic NetWorker Client resource for each physical node, with the Save Set attribute set to All and not assigned to a group.
- Grants access (ACL rights) to the Lockbox resource for the virtual host to the system/root user and `sap_user` on each physical host.

Note

If additional users need ACL rights to the Lockbox, you can add the users to the Lockbox resource directly in NMC.

Configuring scheduled backups in a cluster without the wizard

Use the following configuration procedure in a cluster to configure a scheduled backup without the wizard.

Procedure

1. Ensure that the NetWorker server is remote and not a part of the cluster environment.
2. Ensure that you have installed NMSAP on a local disk on all the physical nodes of the cluster that are designated to perform a backup.
3. Ensure that the configuration file and parameter file are stored in the same location on each physical node or on a shared disk.
4. Follow the procedure for [Configuring scheduled backups without the wizard](#) on page 93 to create the configuration for the virtual host, keeping in mind the following cluster-specific requirements:
 - If a NetWorker Client resource does not exist, create a generic NetWorker Client resource for each physical node. Set the Save Set attribute to All, and do not assign the resource to a group.
 - In the Remote Access attribute of the Client resource that you create for the virtual cluster host, add *sap_user@physical_host* for each node that requires access to the backup.

Note

You do not need to add *-c virtual_client_name* to the Backup Command attribute.

- Set the required parameters in the *initDBSID.utl* file:
 - Set the `NSR_CLIENT` parameter to the virtual client hostname. [Client parameter setting for cluster systems](#) on page 148 provides details.
 - Set the `NSR_PHYSICAL_HOST_LICENSE` parameter to specify the correct NMSAP licensing, if required. [NSR_PHYSICAL_HOST_LICENSE setting for cluster systems](#) on page 148 provides details.

Configuring manual backups in a cluster

To configure an NMSAP manual backup in a cluster, follow the instructions for configuring a scheduled backup without the wizard as described in [Configuring scheduled backups in a cluster without the wizard](#) on page 150.

The only difference in the manual backup configuration procedure is that you may configure a generic NetWorker Client resource for the virtual host.

Configuring Data Domain deduplication backups in a cluster

You must follow the required configuration procedures for a Data Domain deduplication backup in a cluster, depending on whether you use the wizard.

Use the appropriate procedures in a cluster.

Procedure

1. [Configuring scheduled backups in a cluster with the wizard](#) on page 149 or [Configuring scheduled backups in a cluster without the wizard](#) on page 150 or [Configuring manual backups in a cluster](#) on page 150.
2. [Configuring Client Direct with DD Boost backups](#) on page 121 or [Configuring storage node with DD Boost backups](#) on page 123 for the virtual cluster host.

Configuring probe-based backups in a cluster

You must follow the required configuration procedures for a probe-based backup in a cluster, depending on whether you use the wizard.

Use the appropriate procedures in a cluster.

Procedure

1. Configure a scheduled backup in the cluster according to [Configuring scheduled backups in a cluster with the wizard](#) on page 149 or [Configuring scheduled backups in a cluster without the wizard](#) on page 150.
2. Configure the probe-based backup according to [Configuring a probe-based backup](#) on page 126. Associate the Probe resource with the Client resource for the virtual client host.

Restoring data in a cluster

Follow the required procedure to restore data that was backed up from a shared disk of a virtual client.

Procedure

1. Set the `NSR_CLIENT` parameter in the NMSAP parameter file, `initDBSID.utl`, to the virtual client that holds the NetWorker index entries for the backup to be restored.
2. Follow the instructions for [Performing data restore and recovery](#) on page 138.

Oracle RAC systems

An Oracle Real Application Clusters (RAC) system is an active-active application cluster environment for parallelism and high availability. A node in an Oracle RAC system is a physical host or virtual host. An Oracle instance is a memory structure and a group of Oracle Server processes running on a node.

An Oracle database comprises datafiles that are used by the Oracle instances. All the instances share the same datafiles and control file. Each instance must have its own redo log files and its own archived redo logs.

A RAC system enables multiple Oracle instances across multiples nodes to access the same Oracle database simultaneously. Oracle RAC is based on a cluster software infrastructure that provides concurrent access to the same storage and the same datafiles from all the nodes in the cluster. All the database files reside on shared disks.

Configuring Oracle RAC backups

Refer to the Oracle documentation for details about the Oracle RAC setup. Ensure that you meet the following requirements for Oracle RAC backups on a single backup node with BR*Tools and NMSAP:

- One of the Oracle RAC instances, set as the dedicated database (DDB) instance, is used to perform all the database administration tasks. You can administer all the RAC instances from the DDB instance.
- You have created the BR*Tools log directories, such as `SAPBACKUP` and `SAPARCH`, on a shared file system.
- You have correctly configured Oracle SQL Net.
- You have set the required parameters, such as `parallel_instances` and `db_services`, in the SAP initialization file, `initDBSID.sap`, which is on the DDB instance.

Configuring backups with Backint

All the Oracle RAC backups that are performed with BR*Tools and NMSAP Backint run on the DDB instance. You install BR*Tools and NMSAP on that DDB instance host.

The backup configuration of the DDB instance is the same as for a stand-alone system. [Configuration for NMSAP Oracle Operations](#) on page 85 provides details.

The archived redo logs from all the instances are stored in a common shared location. The `brarchive` program backs up these logs. The program is started on only one RAC instance, usually the DDB instance.

For a probe-based backup, configure a RAC backup as usual. Complete the probe-based backup configuration according to [Configuring a probe-based backup](#) on page 126. Associate the Probe resource with the Client resource configured for the scheduled backup.

Note

In a RAC environment, the `LOG_THRESHOLD` parameter setting in the Probe resource specifies the total number of logs that all the RAC nodes (in a cluster) generated since the last probe-based backup.

Configuring backups with RMAN

Refer to the Oracle documentation for details about the Oracle RAC setup. Ensure that you meet the following requirements for Oracle RAC backups that are performed as concurrent RMAN backups on multiple nodes:

- You have specified the RMAN utility for the backups and restores as described in [Choosing either backint or RMAN as the backup and restore utility](#) on page 88.
- You have installed NMSAP on each RAC node host to be used for backups or restores.
- All the nodes in a backup use the same type of network connection, for example:
 - Direct connection to a Data Domain device for a Client Direct backup.
 - Fibre Channel connection for a DFC backup.
- You have selected one node as the client that stores all the backup entries for the RAC system in the NetWorker client file index. Select either one of the physical nodes in the RAC system or the virtual RAC host.
- You have created a generic NetWorker Client resource for each RAC node host to be used for backups and restores.
- For scheduled backups, you have created an NMSAP specific Client resource for the host that stores the backup index entries.

- You have set the required parameters in the BR*Tools initialization profile, `initDBSID.sap`:
 - To distribute the backup load to multiple RAC nodes, set the `rman_rac_dist` parameter:

```
rman_rac_dist = yes
```

- Set the `rman_channels` parameter to specify the number of concurrent backup streams. When `rman_rac_dist` is set to **yes**, set `rman_channels` to a value greater than 1, preferably a multiple of the number of RAC nodes. For example, set the following value for a RAC system with two nodes to run two backup streams on each RAC node:

```
rman_channels = 4
```

- In the `rman_send` parameter setting, set the `NSR_CLIENT` parameter to the hostname of the client that stores the backup index entries. For example:

```
rman_send="NSR_ENV=(NSR_CLIENT=vRACHost) "
```

[Specifying RMAN as the backup and restore utility](#) on page 90 provides details on setting parameters in the BR*Tools initialization profile.

- You have set the `NSR_CLIENT` parameter in the `backint` parameter file, `initDBSID.utl`, to the same value as the `NSR_CLIENT` parameter in the `rman_send` setting. [NMSAP backint parameters](#) on page 95 provides details on the `backint` parameter file.

Note

This `NSR_CLIENT` parameter setting ensures that the BR*Tools metadata is stored in the same client index as the backup data. The `backint` program backs up the metadata during an RMAN backup.

- For distributed RAC operations (`rman_rac_dist = yes`), you have connected to the database with a specific database username, for example, by using the `-u system/password` option. The database user has the SAPDBA, SYSDBA, and SYSOPER roles.
- For a probe-based backup, you have configured a RAC backup as usual. Complete the probe-based backup configuration according to [Configuring a probe-based backup](#) on page 126. Associate the Probe resource with the Client resource that is configured for the scheduled backup.

Note

In a RAC environment, the `LOG_THRESHOLD` parameter setting in the Probe resource specifies the total number of logs that all the RAC nodes (in a cluster) generated since the last probe-based backup.

Restoring Oracle RAC data

To restore Oracle RAC data, run the BR*Tools commands, such as `brrestore` or `brrecover`, on the DDB instance.

You can restore all the required archived redo logs with a single `brrestore` command. You can specify the instance name and which logs must be restored with the `brrestore -a` command.

For example, the following command restores the archived logs with sequence numbers from 40 to 50 that belong to the instance ORA2:

```
brrestore -a 40-50,ORA2
```

CHAPTER 7

NMSAP Oracle Snapshot Backups and Restores

This chapter includes the following topics:

- [Snapshot operations with NetWorker Snapshot Management](#).....156
- [Types of NSM backups](#)..... 157
- [Types of NSM restores](#).....158
- [Backup and restore data flows with NSM](#)..... 160
- [Configuring NMSAP snapshot backups with NSM](#).....162
- [Testing NMSAP backups and restores with NSM](#)..... 170
- [Example parameter settings for NSM backups](#)..... 171
- [Reviewing the NMSAP NSM backup records](#).....172

Snapshot operations with NetWorker Snapshot Management

NetWorker Snapshot Management (NSM) backups and restores provide snapshot-based protection and availability of data on supported types of primary storage, for example, VNX Block (CLARiiON), VMAX (Symmetrix), or XtremIO. NMSAP works with NSM to provide this protection for SAP Oracle data.

The NSM functionality is available as part of the NetWorker extended client software. The NSM documentation provides additional details about NSM backups and restores.

NMSAP supports scheduled backups for all the supported types of NSM backups.

NMSAP supports manual (client-initiated) backups for only the supported types of ProtectPoint backups:

- NSM ProtectPoint backups of data on a VMAX array to a Data Domain system.
- NSM ProtectPoint with RecoverPoint backups of data on an XtremIO array to a Data Domain system.

Note

The term *ProtectPoint* in this guide refers to both a ProtectPoint operation with NSM and a ProtectPoint with RecoverPoint operation with NSM, unless stated otherwise.

The term *snapshot* in this guide refers to both a storage-only snapshot backup with NSM and a ProtectPoint backup with NSM.

NMSAP backups with NSM do not use the BR*Tools disk-volume backup interface that is introduced in BR*Tools 7.10.

The following table lists the required software components for NSM backups and restores.

Table 15 Typical configuration for NSM operations

Computer or device	Required software or configuration
Oracle production server host	Oracle server, SAP BR*Tools, NetWorker client, NMSAP
Mount host	NetWorker client, NetWorker storage node
Storage array	Storage array that NMSAP supports with NSM, for example, VMAX, VNX Block, or XtremIO
NetWorker server host	NetWorker server, NetWorker storage node, NetWorker client
Data Domain	Required only for ProtectPoint operations, vdisk service is enabled

Types of NSM backups

NMSAP supports all types of NSM backup operations as described in the following table. The following topics provide more details.

Table 16 Supported types of NSM backups

Backup type	Snapshot retention	Location of stored data
Snapshot backup	Permanent	Primary storage
Clone to NetWorker conventional media	Permanent	Secondary storage, such as AFTD or tape
ProtectPoint backup or clone to NetWorker ProtectPoint device	Permanent	Data Domain (DD) vdisk

Snapshot backup

A snapshot backup creates a permanent point-in-time (PIT) copy or snapshot of SAP Oracle data. The snapshot backup stores the snapshot on the primary storage system where it is available for performing snapshot restores or for creating a clone of the snapshot to secondary storage. The secondary storage, also known as conventional media, can be an AFTD or DD Boost device. You can schedule a snapshot backup to occur many times in a single day with minimal impact to the SAP Oracle server or network.

A group of SAP Oracle datafiles in the snapshot is referred to as a snap set. You configure a NetWorker data protection policy for a scheduled backup to control the lifecycle of the snap set. The policy specifies the frequency of snapshot backups and the minimum amount of time that snapshot copies are retained before being recycled or released.

The NetWorker data protection policies do not apply to a manual ProtectPoint backup. The manual backup uses either user-set options or default options, such as the retention period.

Clone to conventional media

You can use NetWorker to perform a clone backup of the snapshot, which creates a cloned copy of the snapshot on secondary storage, such as an AFTD or DD Boost device. NSM can use a mount host that is different from the production host to clone or roll over the backup to secondary storage. The NSM documentation provides details about when you must use a mount host.

By using the NetWorker data protection policy, you can perform the clone backup immediately after the snapshot backup in the same backup workflow. Alternatively, you can perform the clone backup in a separate workflow.

The permanent snapshot is retained on the primary storage and is available to NMSAP for performing snapshot restores for the period that the NetWorker policies specify.

ProtectPoint backup or clone

You can use NMSAP for an NSM ProtectPoint backup to create a permanent point-in-time copy of the data from a VMAX array to a DD vdisk device. You can use NMSAP

for an NSM ProtectPoint with RecoverPoint backup to create a permanent point-in-time copy of the data from an XtremIO array to a DD vdisk device.

You can configure either of two types of ProtectPoint backups:

- A backup directly to the DD vdisk device.
You can then use NMSAP to restore directly from the backup on the Data Domain system.
- A backup that creates a snapshot on the VMAX or XtremIO array, followed by a clone backup that backs up the snapshot to the DD vdisk device. The initial snapshot remains on the VMAX or XtremIO array, and the clone copy resides on the DD vdisk device.
You can then use NMSAP to restore from either the snapshot on the array or the clone copy on the Data Domain system.

Types of NSM restores

NMSAP supports all types of NSM restores as described in the following table. The following topics provide details.

Table 17 Supported types of NSM restores

Restore type	Data is retrieved from
Restore from snapshot or ProtectPoint copies (backup or clone)	Mounted snapshot from storage array or DD
Restore from clone of snapshot or ProtectPoint backup on secondary storage (conventional media)	Secondary storage
Rollback restore	Unmounted snapshot on storage array ProtectPoint backup on DD, with a rollback restore at the storage array level ProtectPoint with RecoverPoint backup on DD, with a rollback restore at the consistency group level

The `RESTORE_TYPE_ORDER` parameter in the user-defined NSM configuration file specifies the type of NSM restore. [Configuring the NSM parameters](#) on page 166 provides details.

Restore from snapshot or ProtectPoint copies (backup or clone)

A snapshot restore is a file-level restore from a snapshot, performed by automatically mounting the snapshot to the mount host and copying back to the requested location.

To minimize the recovery time, use the application host to which you are recovering as the mount host, if possible.

Restore from clone on secondary storage (conventional media)

A restore from a clone on a secondary storage system is the same as a traditional restore without NSM. However, this type of restore still occurs through NSM.

Rollback restore

A rollback restore is a restore of an entire snapshot back to the same source devices on the SAP Oracle server. The rollback restore uses the storage array capabilities and the Data Domain capabilities for a ProtectPoint operation. A rollback restore does not support relocation of the database to a different host because the relocation requires the reverse synchronization of the data between the snapshot and its original source.

Use the NSM documentation to determine any limitation with the rollback on a particular storage array or in a ProtectPoint workflow.

NOTICE

A rollback restore is a destructive restore because the rollback overwrites the entire contents of a snapshot unit, such as a volume or disk. The backup file systems must exist on the source LUNs before the restore; re-create the file systems if required. Ensure that there is no extra file system on the source LUNs. Otherwise, the restore might fail.

A ProtectPoint with RecoverPoint backup and rollback restore occur at the consistency group level, regardless of which objects are included in the backup command. As a best practice for a ProtectPoint with RecoverPoint rollback restore, when you perform the backup or rollback restore, do not exclude the logs or any database files that are part of the RecoverPoint consistency group being backed up or restored. If any LUNs in the backed-up consistency group contain objects that were not included in the backup command, ensure that you manually unmount those LUNs before the rollback restore and then manually mount the LUNs back after the restore.

Safety checks during a rollback restore

During a rollback restore, NSM performs safety checks by default. The safety checks ensure that there are no files, directories, partitions, or volumes (data targets) on the rollback target LUN other than those restored with NSM. If there are additional such data targets on the target LUN that are not included in the restore session, NSM fails the rollback restore as a safety precaution to prevent the overwriting of data.

For a rollback restore of a RecoverPoint consistency group, the safety checks also ensure that all the XtremIO LUNs of the target consistency group are included in the rollback restore. If some of the LUNs do not contain data objects that are being restored, then the safety check and rollback restore both fail.

To override the safety checks, you can use the `psrollback.res` file. In the file, you must list all the files and directories to be excluded from the rollback safety checks. For a rollback restore of a RecoverPoint consistency group, you must also list in the file all the mount points of the LUNs to be excluded from the rollback safety checks.

NOTICE

Use the `psrollback.res` file with extreme caution to prevent possible data corruption. If you use this file to override the safety checks, the rollback restore might overwrite some database files that were not included in the restore session, such as Oracle online redo logs, which could result in data loss.

On Linux or Solaris SPARC, if a disk is configured with partitions, you can perform a rollback restore only if you list the entire disk in the `psrollback.res` file. The rollback restore then overwrites the entire disk. For example, if `/fs1` and `/fs2` are configured with partitions `/dev/sdc1` and `/dev/sdc2` respectively, then you must enable the rollback restore of `/fs1` by listing the entire disk `/dev/sdc` in `psrollback.res`. The rollback restore overwrites the entire disk `/dev/sdc`, so `/fs2` is also restored.

If a logical volume manager (LVM) controls the file system of an application host, then you must list in the `psrollback.res` file all the physical disks that belong to the LVM volume group. For example, if a volume group contains the disks `/dev/sdc` and `/dev/sdd`, and `/fs1` is the mount point of the file system, then the `psrollback.res` file must include the following lines:

```
/fs1/lost+found
/fs1/test
/dev/sdc
/dev/sdd
```

The `psrollback.res` file location is as follows:

- On UNIX systems: `/nsr/res/psrollback.res`
- On Windows systems: `C:\Program Files\EMC NetWorker\nsr\res\psrollback.res`

Example 2 Overriding the safety checks during a rollback restore

If you are restoring `/fs1/data1.df` and `/fs1/data2.df` but there are other files in the `/fs1` directory, such as the files `lost+found` and `test`, you can exclude these other files from the safety checks during a rollback restore if you do not need these files. To exclude the files, list the file pathnames in the `psrollback.res` file:

```
more /nsr/res/psrollback.res
```

```
/fs1/lost+found
/fs1/test
```

Backup and restore data flows with NSM

You can start an NSM backup by automatic or manual invocation of the NetWorker scheduled backup through the NetWorker data protection policies.

You can also use a manual backup for either an NSM ProtectPoint backup from VMAX to DD, or an NSM ProtectPoint with RecoverPoint backup from XtremIO to DD. For example, you can start the manual backup with an SAP Oracle `brbackup` command.

In general terms, an NSM backup includes the following processes.

Procedure

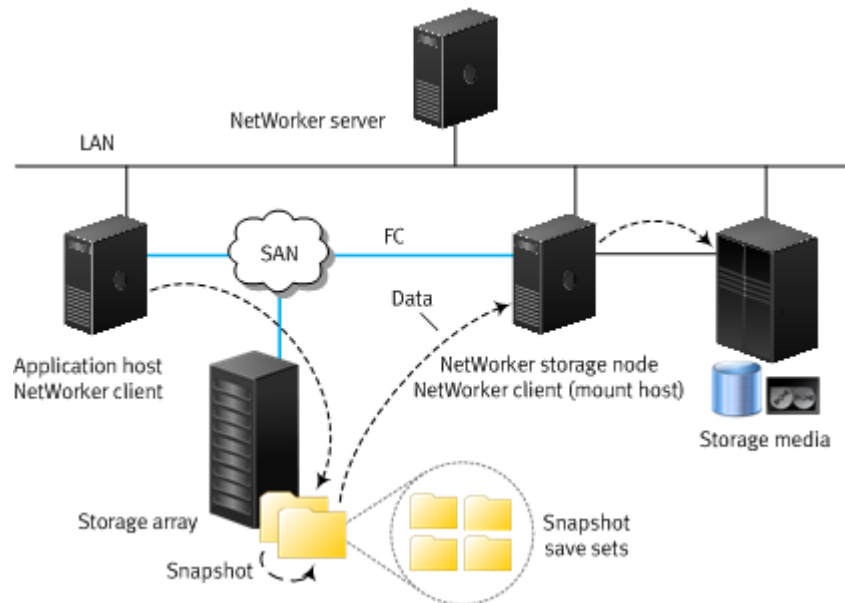
1. For a scheduled backup, the NetWorker server starts the NMSAP `nsrsapsv` process, which runs the SAP `brbackup` command. For a manual backup, the user starts the SAP Oracle backup.
2. The SAP `brbackup` program runs the NMSAP `backint` program, which then communicates with NSM.
3. On the SAP Oracle server host, NSM takes a point-in-time snapshot of the Oracle data on the primary storage. NSM uses an application programming interface (API) specific to the storage system to take the snapshot. Optionally for storage-only snapshots, the snapshot is mounted on the mount host for validation.
4. At the end of the NSM snapshot backup, the NetWorker server updates the online client index and media database with information about the backup. The *NetWorker Administration Guide* describes the NetWorker server and client services.

If the backup workflow includes a clone action, NSM and the NetWorker software also produce a clone copy on secondary storage as described in the NSM documentation.

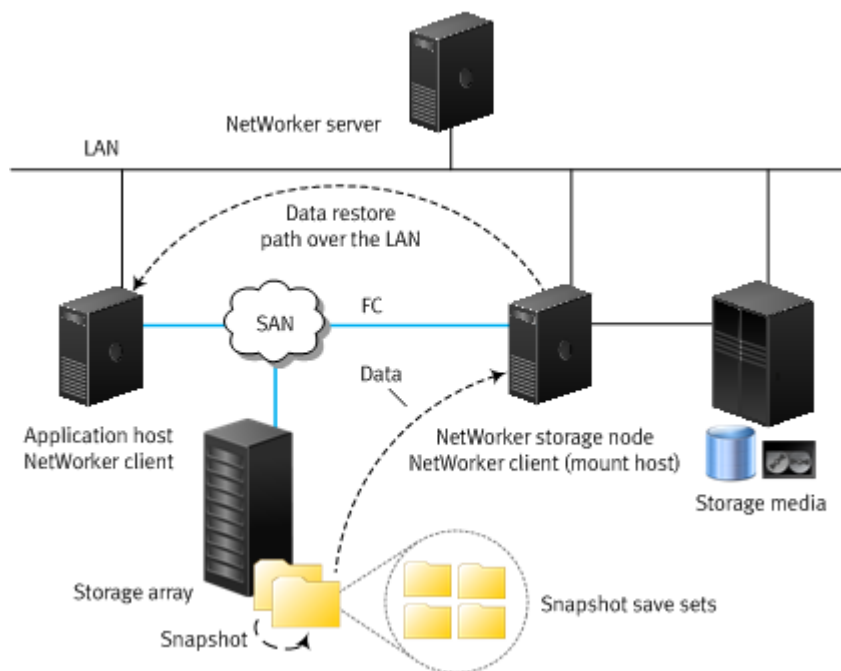
Results

The following figure illustrates the data flow of an NSM snapshot and clone operation to secondary storage in an NMSAP environment. This example environment does not include support for ProtectPoint workflows with a VMAX or XtremIO array and a Data Domain system. The NSM feature provides the snapshot backup functionality as part of the NetWorker extended client software.

Figure 9 NSM snapshot and clone to secondary storage data flow with NMSAP



The following figure illustrates the data flow of an NSM snapshot restore in an NMSAP environment. The NetWorker storage node restores data from the snapshot target volume to the production source volume. This example environment does not include support for ProtectPoint workflows with a VMAX or XtremIO array and a Data Domain system.

Figure 10 NSM snapshot restore data flow with NMSAP

Configuring NMSAP snapshot backups with NSM

You must configure the required NetWorker resources and parameters for NMSAP snapshot backups with NSM. The client backup configuration wizard is recommended for configuring the Client resource and parameter settings. You can also use the manual configuration method without the wizard.

The following configuration steps apply to scheduled NSM backups. If you perform only manual (client-initiated) backups, then you can use the configuration wizard or you can manually create an NMSAP configuration file to use on the client host.

Note

To create the required lockbox entries for RecoverPoint and XtremIO operations, you must use the backup configuration wizard first, before you create the NetWorker client resource manually. For example, in the wizard, you can select **EMC ProtectPoint for RecoverPoint** as the type of storage, and then you must enter the RecoverPoint username and password information. The lockbox is created when the Client resource is created with the configuration wizard.

For a manual backup that you perform with the native CLI, you can specify a retention time for the backup by setting the `NSR_SAVESET_RETENTION` parameter value in UNIX time format. Use the same parameter setting in both the NMSAP and NSM configurations. Set the parameter in the NMSAP configuration file.

Procedure

1. Ensure that you have configured the SAP Oracle database layout to store the datafiles on the primary storage that NSM supports.

Note

Do not store the Oracle database control file or any SAP directories, except *sapdata*, on the same volume (snapshot unit) as the datafiles that are backed up through NSM backups. You cannot back up specific types of Oracle files, such as control files, through an NSM backup. This limitation is an Oracle constraint. The Oracle documentation for the particular Oracle server version describes the Oracle file types that do not support snapshot backups.

2. Ensure that you have installed both NMSAP and the NetWorker extended client software on the database host according to the instructions in the following documents:
 - *NetWorker Module for SAP Installation Guide*
 - NetWorker documentation
3. Ensure that you have installed the NetWorker extended client software on the mount host and correctly configured the Client resource for the mount host.
4. Review [Types of NSM backups](#) on page 157 to determine which type of snapshot backup to perform.
5. Ensure that you have completed the basic database server configuration and NetWorker configuration according to [Configuration road map for NMSAP Oracle operations](#) on page 86.
6. Use the configuration wizard to configure the Client resource and parameter settings for the snapshot backup. The wizard is the recommended configuration method. Follow the information in [Configuring scheduled backups with the wizard](#) on page 91, but ignore any cross-reference.

On the **Select the Backup Configuration Type** page in the wizard:

- a. In the **Available Applications** table, select **SAP** as the application type.
- b. Select the checkbox for **Enable NetWorker Snapshot Management on the selected application**.
- c. Click **Next**.

On the **Select the Snapshot Management Options** page, select the type of storage array or storage appliance where the snapshots are created:

- **EMC VMAX/Symmetrix**
- **EMC ProtectPoint for VMAX3** (Select for ProtectPoint for VMAX operations)
- **EMC ProtectPoint for RecoverPoint** (Select for ProtectPoint for XtremIO operations)
- **EMC VNX/CLARiiON**

Only the arrays or ProtectPoint options that the application supports on the client operating system appear as available.

The NSM documentation provides details on all the other snapshot-specific fields in the configuration wizard. Provide the required information on all the wizard pages to complete the configuration.

Note

If you specify an NMSAP parameter file, `initDBSID.utl`, as a template in the wizard, the file must not include the `NSR_PROXY_PFILE` parameter setting. Otherwise, the settings in the `NSR_PROXY_PFILE` file override the settings in the NMSAP parameter file.

7. If you cannot use the wizard method for some reason, complete the following steps:
 - a. For online database backups, complete one of the following settings:
 - In the `initDBSID.sap` file, set `backup_device_type=util_file_online`.
 - In the `nsrsapsv.cfg` file, set the `BR_EXEC` parameter's CLI option to `-d util_file_online`.
-

Note

If you set `backup_device_type` to `util_file`, the database stays in backup mode for the duration of the backup and generates a larger number of transaction logs.

- b. Configure the Client resource according to [Configuring Client resources manually for NSM backups](#) on page 165.
 - c. Configure the required parameters:
 - [Configuring the NMSAP parameters for NSM operations](#) on page 166
 - [Configuring the NSM parameters](#) on page 166
8. For a scheduled snapshot backup, configure the backup group, policy, workflow, and action according to the "Data Protection Policies" chapter in the latest *NetWorker Snapshot Management Integration Guide*.

When you create the backup action for the snapshot backup with the Policy Action Wizard:

 - From the **Action Type** list, select **Backup**.
 - From the secondary action list, select **Snapshot**.
 - From the **Minimum Retention Time** list, specify the minimum amount of time to retain the snapshot backup. After this time has elapsed, the snapshot can be recycled to release resources that are needed for new backups.

When you create an optional clone action to follow the backup action in the snapshot backup workflow, select **Clone** from the **Action Type** list in the Policy Action Wizard.
9. To enable NSM backups with an OCFS2 system and a remote data mover, ensure that you meet the requirements in [Settings for OCFS2 system with remote data mover](#) on page 169.
10. Test the NSM snapshot backup configuration according to [Testing NMSAP backups and restores with NSM](#) on page 170.

Configuring Device resources for NSM backups

Configure a Device resource for each conventional storage device to be used during NMSAP Oracle backups to conventional storage. You must mount the devices.

Configuring Pool resources for NSM backups

Ensure that you configure a pool to support NSM backups. You configure the Pool resource by using the same method as for a regular NMSAP backup. However, the specified backup device must be an advanced file type.

For NSM backups, in addition to creating snapshots on the storage array (or DD for ProtectPoint backups), NMSAP and NSM must save the following types of data:

- Snapshot save set records.
- Any application files that cannot be backed up through a snapshot workflow. These files are backed up through a traditional workflow.

Ensure that you include the required devices in the NSM backup pool:

- For snapshot backups, include an AFTD or DD Boost device in the pool that is used for the NSM backups.
- For ProtectPoint backups, in addition to the preceding devices, include a NetWorker ProtectPoint device in the same pool. The *NetWorker Snapshot Management Integration Guide* describes how to create the NetWorker ProtectPoint device.

For a scheduled NSM backup, you specify the pool name in the **Destination Pool** field of the backup action, which you create for the snapshot backup as part of the policy-based configuration.

Note

The Pool attribute setting in the Client resource can override the **Destination Pool** setting in the backup action.

The *NetWorker Snapshot Management Integration Guide* provides additional details and describes the pool configuration that is required for a snapshot clone to conventional media or to another ProtectPoint device.

If you perform an NSM ProtectPoint backup as a manual backup, then specify the destination pool in the `NSR_DATA_VOLUME_POOL` parameter in the NMSAP configuration.

Configuring Client resources manually for NSM backups

Configure the NetWorker Client resource manually for the database server host according to [Configuring the Client resource without the wizard](#) on page 115.

The following Client resource requirements for the database server host apply to NSM snapshot backups:

- The Retention Policy attribute in the Client resource applies only to the NetWorker media database entries for NSM backups on secondary storage.
- For NSM backups that use a mount host, the Remote Access attribute must include the mount hostname.

Create a NetWorker Client resource for the mount host according to the NSM documentation.

NMSAP appends “:PS:” to the save set name during an NSM backup to identify NSM save sets.

Configuring the NMSAP parameters for NSM operations

The following table describes the NMSAP parameters set in the parameter file `initDBSID.utl` for NSM backups or restores.

The first example in [Example parameter settings for NSM backups](#) on page 171 provides a basic example configuration for NSM backups.

Table 18 NMSAP NSM parameters in parameter file `initDBSID.utl`

NMSAP NSM parameter	Description	Default and valid values
NSR_PROXY_PFILE	Full pathname of a configuration file that contains NSM specific parameters. Configuring the NSM parameters on page 166 describes how to set the parameters.	<ul style="list-style-type: none"> • Undefined (default). • Full pathname of the NSM configuration file.
SNAPSHOT_OBJECTS	<p>Specifies whether to perform an NSM snapshot backup or a traditional nonsnapshot backup of the SAP Oracle database files, archived redo log files, and metadata files. The metadata files include the SAP Oracle profiles and catalogs.</p> <p>NMSAP performs a nonsnapshot backup of any files that do not reside on a snapshotable volume and any file type that is not specified in this parameter setting.</p> <hr/> <p>Note</p> <p>It is recommended that you perform a nonsnapshot backup of the metadata files because the metadata files are very small in size and number.</p> <hr/>	<ul style="list-style-type: none"> • Undefined (default) = Perform a nonsnapshot backup of the database files, log files, and metadata files. • One or more of the following values, which are separated by a comma: <ul style="list-style-type: none"> ▪ DATA = Perform a snapshot backup of the database files. ▪ LOGS = Perform a snapshot backup of the archived redo log files. ▪ METADATA = Perform a snapshot backup of the metadata files. <hr/> <p>Note</p> <p>METADATA must be used with DATA or LOGS or both.</p> <hr/> <p>The following setting specifies a snapshot backup of the database and log files and a nonsnapshot backup of the metadata files:</p> <p>SNAPSHOT_OBJECTS = DATA, LOGS</p>

Configuring the NSM parameters

You can set the NSM parameters in the NSM configuration file for backups or restores. As an alternative for backups, you can set the NSM parameters in the Application Info attribute of the NetWorker Client resource. As an alternative for recovery or restore, you can set the NSM parameters in the **Advanced Options** table in the NMSAP recovery wizard.

Specify the NSM configuration file by its complete file pathname, for example, `/nsr/res/nmsapps.cfg`, in the `NSR_PROXY_PFILE` parameter in the NMSAP parameter file, `initDBSID.utl`.

Some parameters in the NSM configuration file have corresponding parameters in the NMSAP parameter file, `initDBSID.utl`. Do not specify values for these parameters in the NSM configuration file. If you set a corresponding parameter in the NSM configuration file, it overrides the equivalent parameter in the NMSAP parameter file. [Table 9](#) on page 95 lists the parameters in the NMSAP parameter file.

List each parameter in the configuration file or the Application Info attribute on a separate line, in the following format:

```
parameter_name=parameter_value
```

where:

- *parameter_name* is the parameter name, such as `NSR_SNAP_TYPE`.
- *parameter_value* is the parameter value, such as `emcclar`.

The following tables describe the supported NSM parameters. The first table lists the common parameters for all NSM operations. The other two tables list the NSM parameters specifically for ProtectPoint for VMAX operations and ProtectPoint with RecoverPoint (for XtremIO) operations. The lists are not exhaustive. The NSM documentation provides details on the NSM parameters.

Note

If you use the NMSAP recovery wizard, then you can set the NSM parameters, such as `NSR_SNAP_TYPE` or `NSR_PS_DEBUG_LEVEL`, in the **Advanced Options** table on the **Specify the Performance and Additional Options (Optional)** page in the wizard.

Table 19 Common parameters in NSM configuration file, `nmsapps.cfg`

NSM parameter	Description	Default and valid values
<code>NSR_DATA_MOVER</code>	Mandatory if the NSM backup uses a mount host that is different from the NSM client host (<code>NSR_CLIENT</code>). Specifies the hostname or IP address of the NSM mount host.	<ul style="list-style-type: none"> • Hostname of the local application host (default). • Valid hostname or IP address of the mount host.
<code>NSR_MAX_STREAMS</code>	Optional. Specifies the maximum number of restore streams.	<ul style="list-style-type: none"> • Setting of the NMSAP <code>NSR_PARALLELISM</code> parameter (default). • An integer value.
<code>NSR_PS_DEBUG_LEVEL</code>	Optional. Specifies the NSM debug level.	<ul style="list-style-type: none"> • 0 (default, no debugging). • 0 to 9.
<code>NSR_PS_SAVE_PARALLELISM</code>	Optional. Specifies the maximum number of concurrent save streams per NSM backup. This parameter is only used when cloning the snapshot to secondary storage.	<ul style="list-style-type: none"> • Setting of the NMSAP <code>NSR_PARALLELISM</code> parameter (default). • An integer value.
<code>NSR_SNAP_TYPE</code>	Mandatory for ProtectPoint with RecoverPoint, otherwise optional. Specifies the snapshot platform or a ProtectPoint backup.	<p>The value must be lowercase, for example:</p> <ul style="list-style-type: none"> • <code>symm-dmx</code> for VMAX platform • <code>emcclar</code> for VNX Block platform

Table 19 Common parameters in NSM configuration file, `nmsapps.cfg` (continued)

NSM parameter	Description	Default and valid values
	If the value is unspecified, NSM queries the BRC service to select the most appropriate value.	<ul style="list-style-type: none"> protectpoint for a ProtectPoint backup
RESTORE_TYPE_ORDER	<p>Optional. Specifies the type of restore to perform.</p> <p>If you specify multiple values, the system tries each type of restore in the specified order until a restore operation is successful.</p> <hr/> <p>Note</p> <p>For NMSAP, a rollback operation terminates if one of the following conditions is true:</p> <ul style="list-style-type: none"> You have specified <code>brrestore</code> file relocation. Nonrequested files exist in the <code>brrestore</code>-requested file systems. These files could become corrupted after a rollback. 	<ul style="list-style-type: none"> pit:conventional (default) <p>One or more of the following values, where each value is delimited from the others by a colon (:):</p> <ul style="list-style-type: none"> pit—Specifies a snapshot (PIT) restore. conventional—Specifies a restore from conventional storage media. rollback—Specifies a rollback restore from a PIT copy.

Table 20 NSM parameters for ProtectPoint for VMAX operations only

Parameter	Description	Default and valid values
NSR_DD_VDISK_RESTORE_DEVGRPNAME	<p>Mandatory for a ProtectPoint for VMAX restore directly from Data Domain except for a rollback restore.</p> <p>Specifies the DD vdisk device group in the vdisk device pool that contains the restore LUNs to use for the restore of the ProtectPoint backup directly from Data Domain. The restore does not involve a VMAX system.</p>	<ul style="list-style-type: none"> Undefined (default). Valid name of a DD vdisk device group.
NSR_DD_VDISK_RESTORE_POOLNAME	<p>Mandatory for a ProtectPoint for VMAX restore directly from Data Domain except for a rollback restore.</p> <p>Specifies the name of the DD vdisk device pool to use for the restore of a ProtectPoint backup directly from Data Domain. The specified device pool must contain the restore LUNs that are provided on the restore host.</p>	<ul style="list-style-type: none"> Undefined (default). Valid name of a DD vdisk device pool.

Table 21 NSM parameters for ProtectPoint with RecoverPoint operations only

Parameter	Description	Default and valid values
NSR_DD_VDISK_RESTORE_DEVGRPNAME	Optional for a ProtectPoint with RecoverPoint restore. Not used for a rollback restore. Specifies the DD vdisk device group in the vdisk device pool that contains the restore LUNs to use for the restore of the ProtectPoint with RecoverPoint backup.	<ul style="list-style-type: none"> Undefined (default). Valid name of a DD vdisk device group.
NSR_DD_VDISK_RESTORE_POOLNAME	Optional for a ProtectPoint with RecoverPoint restore. Not used for a rollback restore. Specifies the name of the DD vdisk device pool to use for the restore of a ProtectPoint with RecoverPoint backup. The specified device pool must contain the restore LUNs.	<ul style="list-style-type: none"> Undefined (default). Valid name of a DD vdisk device pool.
NSR_SNAP_TECH	Mandatory for ProtectPoint with RecoverPoint operations only. Specifies the RecoverPoint replication type for a backup or restore.	<ul style="list-style-type: none"> Undefined (default). RP_CDP—Notifies NSM that local copies will be used to access a bookmark. RP_CRR—Notifies NSM that remote copies will be used to access a bookmark.
RP_APPLIANCE_NAME	Mandatory for ProtectPoint with RecoverPoint operations. Specifies the hostname or IP address of the RecoverPoint management host. Note You must run the backup configuration wizard to create the mandatory lockbox that stores the password for the RecoverPoint user.	<ul style="list-style-type: none"> Undefined (default). Valid hostname or IP address of the RecoverPoint management host.

Settings for OCFS2 system with remote data mover

If you use an OCFS2 system and a remote data mover for NSM backups, ensure that you meet the following requirements:

- You allocate extra slots when you create an OCFS2 volume, as required to mount a device on a host outside of the RAC environment. Oracle recommends that you allocate two more slots than the number of nodes that will mount a device. For example, allocate four node slots for a two-node cluster, allocate eight slots for a six-node cluster, and so on.
- On the data mover host:
 - Ensure that the OCFS2 software is installed and running.
 - Ensure that unique OCFS2 node numbering is correctly set up.

No special configuration is required if a local data mover is used (local to one of the RAC nodes). Oracle provides support notes and documentation on how to prepare to use cloned OCFS volumes.

Testing NMSAP backups and restores with NSM

You can test NMSAP backups and restores with NSM by running the required procedures.

Before you test NMSAP backups and restores with NSM, ensure that you have configured the required NetWorker resources and NMSAP configuration files as described in [Configuring NMSAP snapshot backups with NSM](#) on page 162.

Procedure

1. Test a scheduled NSM backup by right-clicking the backup workflow name in the **Monitoring** window of the NMC Administration interface and then selecting **Start**. The *NetWorker Administration Guide* and NMC online help provide details on the NMC interfaces.

The backup test is successful if the `backint` log reports the following message:

```
n of n PS files reported
```

where *n* is the number of files requested that reside on an NSM disk.

If you encounter a problem, check the NMSAP `backint` log and NSM log. Common problems are listed as follows:

- NSM does not manage the target file.
- The NSM daemon or service, `nsrpsd`, is not running.
- The NSM configuration file, `symm.res`, must be modified if it is used. The file is used only in VMAX storage configurations.
- The `NSR_PROXY_PFILE` file must be configured correctly.

For additional troubleshooting, set the following parameters in the `initDBSID.utl` file to generate diagnostic logs for Customer Support:

```
NSR_DEBUG_LEVEL = 9
NSR_DPRINTF = TRUE
```

To obtain NSM debug logs, set the following parameter in the `NSR_PROXY_PFILE` file:

```
NSR_PS_DEBUG_LEVEL=9
```

2. Ensure that the backup to be restored exists before you perform a restore operation. For example, to inquire for the latest NMSAP BACKINT backup by using the BR*Tools verify functionality, type the following command:

```
brrestore -b last -verify only_conf
```

The BR*Tools documentation provides details on the `-verify` options.

You can also verify that the backup exists in the NetWorker indexes. [Reviewing the NMSAP NSM backup records](#) on page 172 provides details.

3. Test a restore with the following command:

```
brrestore
```

The restore test is successful if a `backint` log reports the following message:

```
n of n PS files reported
```

where *n* is the number of files requested that reside on the primary storage that NSM supports.

Example parameter settings for NSM backups

The following examples include settings in the NMSAP parameter file, `initDBSID.utl`, and the NSM configuration file, `nmsapps.cfg`, for NMSAP backups and restores with NSM.

The following example provides typical settings in the `backint` parameter file `initDBSID.utl`:

```
NSR_PROXY_PFILE = /nsr/res/nmsapps_backup.cfg
SNAPSHOT_OBJECTS = DATA
```

The following examples provide typical settings in the NSM configuration file. The NSM parameters for specific primary storage are set in the `/nsr/res/nmsapps_backup.cfg` file, which is specified with the `NSR_PROXY_PFILE` parameter in the NMSAP parameter file:

- For VNX Block:

```
NSR_DATA_MOVER=datamover.emc.com
NSR_SNAP_TYPE=emcclar
EMCCLAR_SNAP SUBTYPE=Clone
FRAME_IP=10.5.167.17:10.5.167.18
```

- For VMAX:

```
NSR_DATA_MOVER=datamover.emc.com
NSR_SNAP_TYPE=symm_dmx
```

- For ProtectPoint:

```
NSR_DATA_MOVER=datamover.emc.com
NSR_SNAP_TYPE=protectpoint
```

- For ProtectPoint with RecoverPoint:

```
NSR_DATA_MOVER=datamover.emc.com
NSR_DD_VDISK_RESTORE_DEVGRPNAME=DG_a018_rp211
NSR_DD_VDISK_RESTORE_POOLNAME=ledma018_RP163_restore_1
```

```
NSR_SNAP_TECH=RP_CDP
NSR_SNAP_TYPE=protectpoint
RP_APPLIANCE_NAME=ledmd163
```

Reviewing the NMSAP NSM backup records

The NetWorker server records information about each NMSAP NSM backup in the online client file index and media database. The NetWorker client file index for NMSAP NSM backups is stored under the `saporacle` namespace, same as used for nonsnapshot NMSAP backups.

Use the `nsrinfo` and `mminfo` commands to query the online NetWorker indexes:

- To query the NetWorker client file index, type the `nsrinfo` command. For example:

```
nsrinfo [-v] -n saporacle -s NetWorker_server client
```

where *client* is the SAP Oracle server hostname.

- To query the NetWorker media database, type the `mminfo` command. For example:

```
mminfo [-v] [-N backint:DBSID:PS:] -s NetWorker_server -c client
```

where *client* is the SAP Oracle server hostname.

The *NetWorker Command Reference Guide* and the UNIX man pages describe these NetWorker commands.

CHAPTER 8

NMSAP Oracle Split-Mirror Backups and Restores

This chapter includes the following topics:

- [Split-mirror backups and restores](#)..... 174
- [Basic split-mirror backup and restore data flows](#)..... 174
- [Configuring the production host for split-mirror backups](#)..... 176
- [Configuring the mount host for split-mirror backups](#).....177
- [Configuring the snapshot software for split-mirror backups](#)..... 179
- [Configuring the NetWorker server for split-mirror backups](#)..... 179
- [Configuring a cluster environment for split-mirror backups](#)..... 180
- [Examples of parameters for split-mirror backups](#)..... 181

Split-mirror backups and restores

NMSAP in cooperation with the snapshot technology software supports BR*Tools split-mirror backups with a split-command interface.

NMSAP supports split-mirror backups of SAP Oracle data that are stored on a storage array, such as VMAX (Symmetrix), VNX Block (CLARiiON), HP, Hitachi, or IBM.

Note

The NMSAP split-mirror backup implementation does not support the SAP `splitint` interface.

Split-mirror backups that are created with NMSAP and BR*Tools require the installation of the snapshot technology software components.

Basic split-mirror backup and restore data flows

A split-mirror backup includes the following basic processes:

- Snapshot technology software “splits” the disks on the primary storage array, which creates a snapshot copy or replica of the database.
- Snapshot technology mounts the replica onto the backup host or mount host, enabling the NMSAP `backint` program to access the files to be backed up. The software can optionally synchronize the disks at a later time, if required.
- The NMSAP `backint` program backs up the snapshot data from the mount host to conventional storage.

Note

The SAP split-mirror backup framework does not support the backup of archived redo logs. To protect the SAP environment, configure NMSAP on the production host to back up the archived logs at least once a day.

Manual split-mirror backup data flow

You start a manual split-mirror backup on the mount host by running the SAP `brbackup` command.

During a manual split-mirror backup, the following process occurs:

Procedure

1. The `brbackup` program contacts the production database to determine the location of objects to be backed up. For an online backup, the program also creates a copy of the control file on the mount host.
2. The `brbackup` program prepares the production database for the backup:
 - For an online backup, the program puts the required tablespaces into backup mode.
 - For an offline backup, the program shuts down the database, if required.
3. The `brbackup` program runs the script that the `split_cmd` parameter specifies in the `initDBSID.sap` file.
4. The `split` script runs the proper command for the specified snapshot technology software.

5. The script returns control to `brbackup`.
6. The `brbackup` program completes the operations with the production database:
 - For an online backup, the program takes the tablespaces out of backup mode.
 - For an offline backup, the program restarts the database, if required.
7. The `brbackup` program runs the NMSAP `backint` program on the mount host.
8. The `backint` program establishes a connection with the NetWorker server, backs up the data to conventional storage, and records the backups in the NetWorker server catalog.
9. The `brbackup` program records the backup in its own catalog on the mount host and makes a copy of the catalog on the production host.
10. (Optional) The `brbackup` program runs the script that the `resync_cmd` parameter specifies in the `initDBSID.sap` file to resynchronize the mirror disks.

Results

By default, NMSAP stores backup entries in the NetWorker client file index under the name of the client that NMSAP backs up, in this case the mount host. The backup entries can be recorded under the Oracle production host by setting the NMSAP client parameter to the production host.

Note

To simplify the restore, store both the data and logs under the same NetWorker client name, where the client is either the production host or the mount host:

- Data that is backed up through the split-mirror framework.
 - Archived logs that are backed up outside of the framework.
-

Scheduled split-mirror backup data flow

Scheduled split-mirror backups are scheduled through the NetWorker server.

At the scheduled backup start time, the following process occurs:

Procedure

1. The NetWorker server contacts the NetWorker client on the mount host.
2. The NetWorker client calls the NMSAP `nsrsapsv` scheduled backup program.
3. The `nsrsapsv` program sets the environment that is required to run the `brbackup` program and runs the `brbackup` program, as configured in the NMSAP `nsrsapsv.cfg` configuration file.
4. The backup then follows the same steps as a manual split-mirror backup.

Restore of split-mirror backup data flow

The restore and recover operations for split-mirror backups are the same as for normal NMSAP backups and do not use the snapshot technology software.

You can restore the backup data to either the mount host or the production host by running the `brrestore` command on the destination host.

Configuring the production host for split-mirror backups

Configuration of the production host for split-mirror backups requires the configuration of the Oracle, BR*Tools, and NMSAP software on the production host.

Configuring Oracle software on the production host

Follow the Oracle documentation for details about how to create an Oracle database on the production host.

The following configurations apply specifically to split-mirror backups.

Procedure

1. Preferably, use the same `ORACLE_HOME` and user operating system account on both the production host and mount host.
2. Ensure that the database is in archived log mode.
3. Ensure that the following database files are on the storage array:
 - Database files
 - Control file
 - Parameter file (`initDBSID.ora`)
 - Redo log files
 - Archived logs
 - Dump files
4. Configure and start the Oracle Net services. This step enables the mount host to connect to the production database.
5. Grant `sysoper` and `sysdba` privileges to the SAP database user for BR*Tools operations.

Configuring BR*Tools on the production host

Follow the SAP documentation for details about how to configure BR*Tools on the production host.

The following configurations apply specifically to split-mirror backups.

Procedure

1. Preferably, use the same paths and values for SAP-specific parameters, such as `SAPBACKUP` and `SAPARCH`, on both the production host and mount host.
2. On Windows, use NFS to share the `%SAPBACKUP%` directory on the production host with the mount host.

Ensure that the Oracle and SAP user and services on the mount host have read and write permissions on the `%SAPBACKUP%` directory. The permissions are

required to copy the control file to the `%SAPBACKUP%` directory during a split-mirror backup.

Note

On Windows, the `brrestore` command might fail to restore the Oracle database control file, generated during an online split-mirror backup, and the BR*Tools backup catalogs. Split-mirror backups on Windows use NFS sharing, which enables these files to be backed up from their location in the `%SAPBACKUP%` directory. However, the NFS sharing does not enable NMSAP to find the expected request file in the NetWorker index. Restore these files by using NetWorker file system tools, such as the `recover` command or the client graphical user interface.

Configuring NMSAP on the production host

You can optionally install NMSAP on the production host.

This installation enables the following operations:

- Backup of Oracle archived logs, which must be performed outside of the split-mirror backup framework.
- Recovery of the backups directly to the production host instead of the mount host.

Configuring the mount host for split-mirror backups

Configuration of the mount host for split-mirror backups requires the configuration of the Oracle, BR*Tools, and NMSAP software on the mount host.

Configuring Oracle software on the mount host

Follow the Oracle documentation for details about how to configure the Oracle software on the mount host.

The following configurations apply specifically to split-mirror backups.

Procedure

1. Preferably, use the same `ORACLE_HOME` and user operating system account on both the production host and mount host.
2. Configure and start the Oracle Net services. This step enables the mount host to connect to the production database.
3. Either copy the `initDBSID.ora` parameter file from the production host to the mount host, or create an `initDBSID.ora` file that contains the following parameters:
 - `db_name=SID of the production database`
 - `control_files=(location of the control file on the production host, location2)`

Configuring BR*Tools on the mount host

Follow the SAP documentation for details about how to configure BR*Tools on the mount.

Complete the following configurations specifically for split-mirror backups.

Procedure

1. Preferably use the same paths and values for SAP-specific parameters, such as `SAPBACKUP` and `SAPARCH`, on both the production host and mount host.
2. Create the `split` command script by following the snapshot software documentation.
3. Set the following parameters in the `initDBSID.sap` initialization profile:
 - `split_cmd` = *location of the snapshot technology software split command script*
 - `primary_db` = *SID of the production database*

Note

For a single-host configuration where the mount host is the same as the production host, set this parameter to the LOCAL keyword:
`primary_db = LOCAL`

-
- `orig_db_home` = *\$SAPDATA_HOME on the production host*
-

Note

This parameter is required when the replica is mounted onto a different directory than the production database, for example, in a single-host environment.

4. In a two-host UNIX environment, set the following parameters in the `initDBSID.sap` file:
 - `remote_host` = *production database host*
 - `stage_copy_cmd` = `rcp | ftp | scp`
Set only one of these values.

Note

Ensure that the SAP user on the mount host is allowed to perform the specified command on the production host.

5. In a Windows environment, mount the shared `%SAPBACKUP%` directory under the same path as on the production host.

Note

The `%SAPBACKUP%` directory must be shared because SAP split-mirror backups do not support FTP or RCP on Windows.

6. Set the following parameters in the `initDBSID.sap` file, or specify them as command line options of the `brbackup` command:

Note

The command line options take precedence over the corresponding parameters set in the `initDBSID.sap` file:

- `backup_type = online_split | offline_split`
 - `backup_dev_type = util_file`
 - `util_par_file = location of the NMSAP config utl file`
-

7. Set the required SAP environment variables:

- `$SAPDATA_HOME = location of the replica`
- Set other required variables, for example, `$SAPBACKUP`, as described in the BR*Tools documentation.

Configuring NMSAP on the mount host

[Configuration for NMSAP Oracle Operations](#) on page 85 describes how to configure NMSAP.

For scheduled backups, ensure that the `nsrsapsv.cfg` file on the mount host contains the following setting:

`PATH = location of the snapshot technology software binaries to be run as part of the split command`

Note

The NMSAP wizard does not support the configuration of split-mirror backups. You must manually configure scheduled backups.

Configuring the snapshot software for split-mirror backups

Follow the proper software documentation for details about how to configure the software to perform a consistent split and mount the replica on a mount host so that the replica is accessible to the NMSAP `backint` program.

Configuring the NetWorker server for split-mirror backups

[Configuration for NMSAP Oracle Operations](#) on page 85 describes how to configure the NetWorker server for NMSAP manual backups and scheduled backups.

The following requirements apply specifically to split-mirror backups.

Procedure

1. Configure the NetWorker Client resource for the production host with the following attribute settings:
 - Protection group list: None, unless this resource is configured for archived log backups
 - Remote access: `SAP_user@mount_host`
2. Configure the NetWorker Client resource for the mount host with the following attribute settings:

- Save set: backint:*DBSID*
- Protection group list: *NMSAP group*
- Backup command: *nsrsapsv -f location of nsrsapsv.cfg file*
- Remote access: *SAP_user@production_host*

Configuring a cluster environment for split-mirror backups

[SAP Oracle in Cluster and RAC Environments](#) on page 147 describes how to configure a cluster environment for scheduled backups.

Complete the following steps for split-mirror backups.

Procedure

1. Configure the required production host software on each physical node of the cluster.
2. Configure the required mount host software on a computer that is located outside of the cluster.

Note

Only a production host can be in a cluster environment. The mount host must be a stand-alone host.

3. Store the parameter file, *initDBSID.utl*, and the configuration file, *nsrsapsv.cfg*, in the same location on each physical node or on a shared drive.
4. Use the virtual node name for the production hostname.
5. On the NetWorker server, create and configure the NetWorker Client resource for each physical node with the following settings:
 - Generic NetWorker resource (not specific to NMSAP)
 - Protection group list: None
6. On the NetWorker server, create, and configure the NetWorker Client resource for the virtual node with the following settings:
 - Protection group list: None, unless this resource is configured for archived log backups
 - Remote access:
 - *SAP user@physical node #1*
 - *SAP user@physical node #2*
 - *SAP user@mount host*
7. Configure the NetWorker Client resource for the mount host with the following settings:
 - Save set: backint:*DBSID*
 - Protection group list: *NMSAP group*
 - Backup command: *nsrsapsv -f location of nsrsapsv.cfg file*

- Remote access: *SAP_user@virtual_node*

Examples of parameters for split-mirror backups

The following examples show parameters that must be set in the Oracle, BR*Tools, and NMSAP configuration files on the production host and mount host for split-mirror backups and restores.

Parameter settings on the production host

Modify the following Oracle configuration files on the production host according to the requirements of the environment. In these examples, the production host is named bu-erie.

initSAP.ora

```
control_files = (H:\oradata\SAP\sapdata1\cntrl\ctrlSAP.ctl,
                H:\oradata\SAP\sapdata2\cntrl\ctrlSAP.ctl,
                H:\oradata\SAP\saparch\cntrl\ctrlSAP.ctl)
background_dump_dest = H:\oradata\SAP\saptrace\background
user_dump_dest = H:\oradata\SAP\saptrace\usertrace
log_archive_dest = H:\oradata\SAP\saparch
log_archive_format = SAParch%t_%s_%r
```

listener.ora

```
SID_LIST_LISTENER =
(SID_LIST =
(SID_DESC =
(SID_NAME = SAP)
(ORACLE_HOME = C:\oracle\product\10.2.0\db_1)
)
)
```

Parameter settings on the mount host

Modify the following Oracle and BR*Tools configuration files on the mount host according to the requirements of the environment. In these examples, the production host is named bu-erie.

initSAP.ora

```
db_name=SAP
control_files = (H:\oradata\SAP\sapdata1\cntrl\ctrlSAP.ctl,
                H:\oradata\SAP\sapdata2\cntrl\ctrlSAP.ctl,
                H:\oradata\SAP\saparch\cntrl\ctrlSAP.ctl)
```

tnsnames.ora

```
SAP =
(DESCRIPTION =
(AADDRESS = (PROTOCOL = TCP) (HOST = bu-erie) (PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
```

```

        (SERVICE_NAME = SAP)
    )
)

```

initSAP.sap

```

split_cmd = F:\oracle\product\brtools\7.00\online_split.cmd
backup_type = online_split
primary_db = SAP
backup_dev_type = util_file
util_par_file = initsAP.utl
orig_db_home = H:\oradata\SAP

```

Note

If the mount host is the same as the production host, then set `primary_db = LOCAL`.

nsrsapsv.cfg

```

BR_EXEC=brbackup -m all -d util_file -r
F:\oracle\product\10.2.0\db_1\database\initSAP.utl -p
F:\oracle\product\10.2.0\db_1\database\initSAP.sap
ORACLE_HOME=F:\oracle\product\10.2.0\db_1
DBSID=SAP
NLS_LANG = AMERICAN AMERICA.US7ASCII
SAPBACKUP=\\bu-erie\I\oradata\SAP\sapbackup
SAPDATA_HOME=H:\oradata\SAP
SAP_BIN=F:\oracle\product\brtools\7.00
Path=C:\Program Files\EMC\rm\client\bin

```

APPENDIX A

Examples of SAP Oracle Command Options

This appendix includes the following topics:

- [Examples of brbackup and brarchive command syntax and options](#)..... 184
- [Examples of brrestore command syntax and options](#)..... 185
- [Examples of brrecover command syntax and options](#)..... 186

Examples of brbackup and brarchive command syntax and options

You can use the SAP `brbackup` and `brarchive` commands with the NMSAP program from any command prompt.

Examples of the syntax and options for these commands are as follows:

```
brbackup [-c force] [-d {util_file | util_file_online | rman_util}] [-m {all | all_data | full | incr | tablespace_list | file_ID | file_ID1_range | file_list}] [-p profile] [-q check] [-r parameter_file] [-t {online | offline | offline_force | online_split | offline_split}] [-u user/password] [-w [use_dbv | only_config]]
```

```
brarchive [-c force] [-d {util_file | rman_util}] [-f stop] [-m delay_time] [-p profile] [-q check] [-r parameter_file] [-u user/password]
```

Options that are enclosed in brackets ([]) are optional. Options that are enclosed in braces ({ }) must use at least one of the enclosed options. The following table lists examples of the command options.

The SAP documentation provides complete details about the command syntax and options for the `brbackup` and `brarchive` commands.

Note

The command line options overwrite the corresponding parameters set in the initialization profile `initDBSID.sap`.

Table 22 Options for `brbackup` and `brarchive` commands

Option	Description
<code>-c force</code>	Suppresses most of the confirmation messages that interrupt the backup process.
<code>-d {util_file util_file_online rman_util}</code>	Specifies to use NMSAP with <code>backint</code> or RMAN for the backup or archive.
<code>-f stop</code>	Instructs <code>brarchive</code> to wait for the next offline redo log file that Oracle writes, and then send the file to <code>backint</code> for archiving.
<code>-m database_objects_to_back_up</code>	Specifies the database objects to back up, for example, the whole database, selected tablespaces or datafiles, incremental RMAN backup, and so on. The <code>brbackup</code> program uses this option.
<code>-m delay_time</code>	Specifies the delay time between Oracle creating the offline redo log file and sending datafiles to the database in standby mode. The <code>brarchive</code> program uses this option.
<code>-m nondatabase_objects_to_back_up</code>	Specifies what nondatabase files or folders to back up. Use one of the following keywords: <code>sap_dir</code> , <code>ora_dir</code> , <code>all_dir</code> , <code>full_directory_path</code> . The <code>brbackup</code> program uses this option.
<code>-p profile</code>	Specifies a BR*Tools initialization profile if the file does not have the default name or is not stored in the default location.

Table 22 Options for `brbackup` and `brarchive` commands (continued)

Option	Description
<code>-r parameter_file</code>	Specifies the parameter file, <code>initDBSID.utl</code> , that NMSAP <code>backint</code> uses during the backup or archive process.
<code>-t backup_type</code>	Instructs <code>brbackup</code> and NMSAP <code>backint</code> what type of backup to perform. During an online backup, to reduce the number of redo logs that Oracle generates, use this option with the <code>-d util_file_online</code> option.
<code>-u user/password</code>	Specifies the username and password of the Oracle database administrator.
<code>-w use_dbv only_config</code>	Verifies the backup after the files are backed up. Helps detect possible hardware problems. The <code>use_dbv</code> option performs the backup, followed by a restore of the backup to a temporary location. This option approximately doubles the backup time.

Examples of `brrestore` command syntax and options

You can use the SAP `brrestore` command with the NMSAP `backint` program from any command prompt.

An example of the syntax and options for this command is as follows:

```
brrestore [-c force] [-d {util_file | rman_util}] [-f last | brtools_log1,
brtools_log2,... | yyyy-mm-dd hh-mmss | number_of_days] [-m {all | all_data |
full | incr | tablespace_list | file_ID | file_ID1_range | file_list | non_db}]
[-p profile] [-q check] [-r parameter_file]
```

Options in brackets ([]) are optional. Options in braces ({ }) must use at least one of the enclosed options. The following table lists examples of the command options.

The SAP documentation provides complete details about the command syntax and options for the `brrestore` command.

Table 23 Options for `brrestore` command

Option	Description
<code>-c force</code>	Suppresses most of the confirmation messages that interrupt the restore process.
<code>-d {util_file rman_util}</code>	Specifies to use NMSAP with <code>backint</code> or RMAN for the restore.
<code>-f restore_to_complete</code>	Specifies which restores to restart to restore missing files.
<code>-m objects_to_restore</code>	Specifies the database objects to restore, for example, the whole database, selected tablespaces or datafiles, and incremental RMAN backup.
<code>-m non_db</code>	Specifies the restore of data from a directory (nondatabase) backup.

Table 23 Options for `brrestore` command (continued)

Option	Description
<code>-p profile</code>	Specifies a BR*Tools initialization profile if the file does not have the default name or is not stored in the default location.
<code>-r parameter_file</code>	Specifies the parameter file, <code>initDBSID.utl</code> , that NMSAP <code>backint</code> uses during the restore process.

Examples of `brrecover` command syntax and options

You can use the SAP `brrecover` command with the NMSAP program from any command prompt.

An example of the syntax and options for this command is as follows:

```
brrecover [-c force] [-d {util_file | rman_util}] [-p profile]
[-pit yyyy-mo-dd hh.mi.ss] [-r parameter_file] [-scn scn]
[-t complete | dbpit | tspit | reset | restore | apply | disaster]
[-tsp tablespace_name | tablespace_name_list] [-u user/password]
```

For example:

```
brrecover -t complete -p initGC2.sap
```

The following table lists examples of the command options.

The SAP documentation provides complete details about the command syntax and options for the `brrecover` command.

Table 24 Options for `brrecover` command

Option	Description
<code>-c force</code>	Suppresses most of the confirmation messages that interrupt the recovery process.
<code>-d {util_file rman_util}</code>	Recovers NMSAP backups that are performed with <code>backint</code> (<code>util_file</code>) or RMAN (<code>rman_util</code>).
<code>-p profile</code>	Specifies a BR*Tools initialization profile if the file does not have the default name or is not stored in the default location.
<code>-pit yyyy-mo-dd hh.mi.ss</code>	Recovers the database or tablespaces for a specific point-in-time.
<code>-r parameter_file</code>	Specifies the parameter file, <code>initDBSID.utl</code> , which NMSAP <code>backint</code> uses during the backup or archive process.
<code>-scn scn</code>	Recovers the database to the specified Oracle system change number.
<code>-t complete dbpit tspit reset restore apply disaster</code>	Specifies the type of recovery: <ul style="list-style-type: none"> complete: complete database recovery dbpit: database point-in-time recovery tspit: tablespace point-in-time recovery reset: whole database reset

Table 24 Options for `brrecover` command (continued)

Option	Description
	<ul style="list-style-type: none"> • restore: restore of individual backup files • apply: apply offline redo log files (archive logs) • disaster: disaster recovery
<p><code>-tsp <i>tablespace_name</i> <i>tablespace_name_list</i></code></p>	<p>Recovers a single specified tablespace or the tablespaces that are listed in the specified file.</p>
<p><code>-u <i>user/password</i></code></p>	<p>Specifies the username and password of the Oracle database administrator.</p>

APPENDIX B

Troubleshooting and Error Messages

This appendix includes the following topics:

- [Verifying the release information](#)..... 190
- [Generating diagnostic logs](#)..... 190
- [Setting the debugging options for RMAN operations](#)..... 191
- [Backup and restore problems](#)..... 191
- [NMSAP error messages](#).....194

Verifying the release information

When making queries or requests to a Customer Support representative, provide specific information about the NMSAP software that you are using.

To verify the release information for the installation, use the proper command or procedure:

- On UNIX, type the following command as the root user:

```
what file_name | more
```

where *file_name* is the name of an NMSAP binary file, for example, *backint* or *nsrsapsv*.

- On Linux, type the following command as the root user:

```
strings file_name | grep "@(#)"
```

where *file_name* is the name of an NMSAP binary file, for example, *backint*, *hdbbackint*, or *nsrsapsv*.

- On Windows:
 1. Locate the NMSAP binary file, for example, *backint.exe* or *nsrsapsv.exe*.
 2. Right-click the file, and select **Properties**.
 3. In the **Properties** window, click the **Version** tab to display the version information.

Generating diagnostic logs

To generate diagnostic logs, set the following parameters:

Procedure

- Set `NSR_DIAGNOSTIC_DEST` if you do not want to use the default location for the *backint* or *hdbbackint* diagnostic logs, which is `/nsr/applogs` (UNIX) or `NetWorker_installation_path\nsr\applogs` (Windows).
- To debug a failed scheduled backup only, set `NSR_DEBUG_LEVEL=9` in the NMSAP configuration file or in the **Advanced Options** table in the wizard.
- Set `NSR_DEBUG_LEVEL=9` in the `initDBSID.utl` file or in the **Advanced Options** table in the wizard.

Note

The recommended debug level is 9. Use this debug level for testing and Customer Support diagnostics only.

Do not leave the debug settings in place for an extended time because the log files can quickly increase in size.

- Set `NSR_DPRINTF=TRUE` in the `initDBSID.utl` file or in the **Advanced Options** table in the wizard.

Setting the debugging options for RMAN operations

To debug an NMSAP backup or restore that uses RMAN, set the `NSR_DEBUG_LEVEL` parameter in the BR*Tools initialization profile `initDBSID.sap`.

To specify a nondefault location for the NMSAP debug logs generated for the RMAN operation, also set the `NSR_DIAGNOSTIC_DEST` parameter.

To specify that the NetWorker core debug messages are written to the NMSAP debug log file, also set the `NSR_DPRINTF` parameter to `TRUE`. This parameter applies only if `NSR_DEBUG_LEVEL` is set to a value greater than 0.

Note

Set the `NSR_DEBUG_LEVEL`, `NSR_DIAGNOSTIC_DEST`, and `NSR_DPRINTF` parameters by using the `rman_parms` parameter in the `initDBSID.sap` file, not the `rman_send` parameter.

For example:

```
rman_parms="ENV=(NSR_DEBUG_LEVEL=9)"
```

On a Windows system, when you use `rman_parms` to set a parameter, the parameter value remains in effect for all subsequent allocated channels and for all RMAN sessions until one of the following events occurs:

- You shut down the Oracle database.
- You set the parameter to a different value by using the `rman_parms` option for subsequent allocated channels.
- You unset the parameter for the channel by using the `rman_parms` option, as in the following example:

```
rman_parms="ENV=(NSR_DEBUG_LEVEL=,NSR_DIAGNOSTIC_DEST=)"
```

Backup and restore problems

The following table provides guidelines for solving problems that might occur during an NMSAP backup or restore.

Table 25 NMSAP backup or restore problems

Problem	Possible reason or solution
The data is not backed up by using the settings in the Client resource on the NetWorker server.	NMSAP uses the Client resource settings only for scheduled backups. For manual backups, specify the settings in the <code>initDBSID.utl</code> file. Specify the client settings in the <code>initDBSID.utl</code> file on the SAP Oracle server. NMSAP backint parameters on page 95 provides details.
The bootstrap notification report was not printed to the printer specified in the Group resource on the NMSAP server.	Bootstrap notification reports are not generated after a manual NMSAP backup. Monitoring manual backups on page 135 describes the generation of a bootstrap notification report.

Table 25 NMSAP backup or restore problems (continued)

Problem	Possible reason or solution
An online backup of an Oracle tablespace is taking a long time.	Oracle software creates more online redo logs during an online backup than during an offline backup. This occurrence might prolong the online backup.
After a backup, the parallelism setting in the NMSAP operation log, <code>backintDBSID.log.raw</code> , is different from the configuration setting.	The <code>backint</code> program adjusts the parallelism setting during the backup session depending on other parameters, such as when the number of files within the backup session is lower than the server parallelism setting.
A specified backup of an Oracle directory failed.	NMSAP does not support the backup of directories. Specify each database object within the directory to back up and then perform the backup.
You are unable to view the files that are backed up to the NetWorker server from the BrGui program on the SAP Oracle server.	Ensure that the SAP user has proper privileges to view the information, for example, the Operate NetWorker privilege.
On UNIX systems, if the path of an Oracle file contains a chained symbolic link (a link that points to another link), then the backup succeeds but the file restore might fail.	The SAP program does not support chained symbolic links. SAP Note 27428 provides details.
If the configuration wizard fails to create a scheduled backup, an error message might indicate that authentication is denied, or denied for <code>username</code> . The lockbox with the database connection credentials was not accessible by the superuser on the client host where the backup failed and the message appeared.	<p>Use the NMC program to ensure that the Lockbox resource is created for the particular client and the Users attribute contains the superuser of the client. The <i>NetWorker Administration Guide</i> describes the lockbox password management.</p> <p>Delete the NSR Peer Information resource for the NetWorker client from the NSRLA database on the NetWorker server. This deletion causes the NetWorker server to create a new NSR Peer Information resource for the client. The topic "Deleting the NSR Peer Information resource" in the <i>NetWorker Security Configuration Guide</i> provides more details.</p> <p>To check for invalid NSR Peer Information resources, you can run the following command:</p> <pre data-bbox="660 1318 1461 1392">nsradmin -s server_name -p nsrexecd -C "NSR peer information"</pre> <p>To automatically correct the resource errors, you can run the <code>nsradmin</code> command with the <code>-y</code> option. The <i>NetWorker Command Reference Guide</i> provides details on the command and options.</p>
<p>After you upgrade or reinstall the NetWorker server, you might encounter an authentication error. This type of error causes a backup to fail because the authentication information in the NSRLA database on the NetWorker server does not match the client credentials.</p> <p>The following error messages might appear:</p> <pre data-bbox="121 1812 636 1946">Authentication error; why = Server rejected credential Unable to obtain the user credentials from the lockbox due to the following error: 'error_message'</pre>	<p>As a solution, delete the NSR Peer Information resource for the NetWorker client from the NSRLA database on the NetWorker server. This deletion causes the NetWorker server to create a new NSR Peer Information resource for the client. The topic "Deleting the NSR Peer Information resource" in the <i>NetWorker Security Configuration Guide</i> provides more details.</p> <p>To check for invalid NSR Peer Information resources, you can run the following command:</p> <pre data-bbox="660 1864 1461 1946">nsradmin -s server_name -p nsrexecd -C "NSR peer information"</pre>

Table 25 NMSAP backup or restore problems (continued)

Problem	Possible reason or solution
<p>Unable to retrieve the password using <code>lockbox_name</code> for client <code>client_name</code>. Failed to retrieve password from lockbox. Password could not be retrieved from lockbox.</p>	<p>To automatically correct the resource errors, you can run the <code>nsradmin</code> command with the <code>-y</code> option. The <i>NetWorker Command Reference Guide</i> provides details on the command and options.</p>
<p>An NMSAP scheduled backup might fail with SAP HANA 2.0 and display the following error message:</p> <pre data-bbox="129 653 627 699">/lib64/libstdc++.so.6: version `CXXABI_1.3.8' not found</pre>	<p>In SAP HANA 2.0 on Linux RHEL systems, <code>hdbsql</code> requires the C++ runtime library that supports <code>CXXABI_1.3.8</code> or later. NMSAP requires a symbolic link to be created under the <code>SAP_BIN</code> directory (<code>hdbsql</code> location), pointing to the SAP provided <code>libstdc++.so.6</code> library. Typically, SAP HANA creates this symbolic link. If the symbolic link is missing, manually create the symbolic link under the <code>SAP_BIN</code> directory, pointing to the library.</p>
<p>The NMSAP HANA backup wizard might fail with an error message that it cannot connect to the HANA database.</p>	<p>In SAP HANA 2.0 on Linux RHEL systems, <code>hdbsql</code> requires the C++ runtime library that supports <code>CXXABI_1.3.8</code> or later. NMSAP requires a symbolic link to be created under the <code>SAP_BIN</code> directory (<code>hdbsql</code> location), pointing to the SAP provided <code>libstdc++.so.6</code> library. Typically, SAP HANA creates this symbolic link. If the symbolic link is missing, manually create the symbolic link under the <code>SAP_BIN</code> directory, pointing to the library.</p>
<p>When the SAP Security Library <code>SAPSECULIB</code> is installed, an NMSAP Oracle backup might fail with the following error message:</p> <pre data-bbox="129 1083 627 1150">BR1301W Error message from likeyplib: 543 likey_init: Couldn't load SAPSECULIB</pre>	<p>Set the <code>DIR_LIBRARY</code> parameter either in the advanced option table in the client configuration wizard or in the <code>nsrsapsv</code> configuration file. If you started the backup manually, set <code>DIR_LIBRARY</code> in the system environment.</p>
<p>With SAP HANA 2.0 or later, an NMSAP HANA backup configuration with the configuration wizard might fail with the following error message:</p> <pre data-bbox="129 1352 627 1461">Unable to perform automatic detection of the SAP HANA installation. Verify that the SAP HANA is installed correctly before proceeding with the wizard configuration.</pre>	<p>The SAP host agent file <code>saphostctrl</code> must be installed in the <code>/usr/sap/hostctrl/exe</code> directory to enable the NMSAP wizard to detect the SAP HANA installation. With SAP HANA 2.0 or later, the SAP host agent is bundled with the SAP HANA server installation. Before you use the NMSAP wizard with SAP HANA 2.0 or later, perform the following steps to install the SAP host agent manually:</p> <ol style="list-style-type: none"> Go to the required directory: <pre data-bbox="695 1478 1465 1524">cd /<path_to_SID>/global/hdb/saphostagent_setup/</pre> Run the following command to install the SAP host agent: <pre data-bbox="695 1604 1465 1650">./saphostexec -install</pre>

NMSAP error messages

The following table lists possible error messages that might appear in the `backintDBSID.log.raw` file.

Table 26 NMSAP error messages

Error message	Description	Solution
BACKUP: Bad input line: <i>line</i> INQUIRE: Bad input line: <i>line</i> RESTORE: Bad input line: <i>line</i>	One of the lines in the input file had a bad format. There must be only one or two specifications on each input line (file name and size, if it is a special file).	Check the input file that the BR*Tools binary generated to ensure that the file has the correct format. If not and this error recurs, contact SAP Customer Support.
Cannot connect to server: <i>error</i>	The <code>backint</code> program was unable to connect to the NetWorker server to start reading the media database.	Ensure that you specify the correct NetWorker server. Check the log file to see if any other messages refer to this problem.
Cannot reopen <i>file_name</i> as stderr	The <code>backint</code> program was unable to open a log file for writing.	Check the permissions on the file that is listed in the message and the permissions on the directory.
Cannot start session with server: <i>error</i>	The <code>backint</code> program was unable to start reading the media database on the NetWorker server.	Ensure that you specify the correct NetWorker server. Check the log file to see if any other messages refer to this problem.
Checking for deletion of semaphore file: <i>error</i>	The system could not confirm the existence of the semaphore file due to a system error.	Check to see if the <code>.switch.sem</code> file is still in the <code>SAPBACKUP</code> directory. If so, delete the file before running the SAP backup again.
Empty input file	The input file that contains the list of files that require backup or restore is empty.	Ensure that you have selected database objects for backup or restore.
Error opening input file: <i>error</i>	The operation could not open the input file that lists all the files to be backed up or restored. The file might not exist, or the file might not have read permissions.	Ensure that the input file exists and is readable.
Error opening output file: <i>error</i>	The operation could not open the output file for the reason specified.	Check the permissions on the output file and directory, and check for sufficient disk space to create a file.
Error: <i>file_name</i> isn't a regular file, raw partition, or directory.	The <code>backint</code> program does not support the file type, such as a symbolic link or a named pipe.	Check the file name to see what type of file is being backed up. If <code>brbackup</code> requests a backup of special files, contact SAP Customer Support.
Error: Too many symlinks	There are too many (more than 100) symbolic links to save.	Consider restructuring the directories to eliminate the extra symbolic links if the list of database files to be backed up contains more than 100 symbolic links.
Error: unexpected inquire case.	The files that are requested in the input file do not match the SAP <code>backint</code> specification. Valid file specifications include:	Check the backup input file that <code>brbackup</code> generated. If the input file appears to be the wrong format, contact SAP Customer Support.

Table 26 NMSAP error messages (continued)

Error message	Description	Solution
	<ul style="list-style-type: none"> • #NULL is specified for a backup ID, with or without a file name. • A file name is specified with a backup ID. • A backup ID is specified without a file name. 	
File <i>file_name</i> not found in index, no attempt to recover will be made	The NetWorker software did not save the file name that is specified for recovery. The file name does not appear in the client file index.	Check the specified file name to ensure that the name is correct. Check previous backups to determine whether the file was saved in a previous backup.
File was <i>file_name</i> , lstat error	NMSAP tried to obtain information for a symbolic link that does not exist or NMSAP cannot access because permission is denied.	Check the file to ensure that the file exists and is a valid symbolic link.
Improperly formatted backup id: <i>backup ID</i>	The backup ID is incorrect. The backup ID must specify either a number or the word #NULL.	Check the input file <code>brrestore</code> generated to ensure that the file has the correct format. If not and this error keeps occurring, contact SAP Customer Support.
Lookup failed on <i>file_name</i> (<i>backup_ID</i>)	The <code>backint</code> program was trying to look up a file name or backup ID in the client file index, but the index query failed. The next message must explain why the index query failed.	Check the next error message to determine why the index query failed.
Non-recursive directory backup is not supported at this time	You have tried to back up a directory. NMSAP does support the backup of directories.	Select specific database objects to back up from the BrGui program and restart the backup.
Not enough savesets configured. Increase "SAVESETS" setting.	The number of save sets to be backed up exceeds the current setting for the allowed number of save sets.	Increase the allowed number of save sets by setting the <code>SAVESETS</code> parameter. Table 9 on page 95 provides details.
Open param file: <i>file_name</i> , error: <i>error_message</i>	Unable to open the <code>backint</code> parameter file, <code>initDBSID.utl</code> .	Try to open the parameter file for <code>backint</code> in any text editor. If you are unable to open the parameter file, replace the file with the original file from the NMSAP installation package.
Opening switch list file for online backup: <i>error</i>	When performing an online backup, <code>backint</code> tried to open a file to communicate with <code>brbackup</code> . This file could not be opened for the specified reason.	Check if the <code>.switch.lis</code> file exists in the <code>SAPBACKUP</code> directory. If so, check the permissions on this file. Normally, NMSAP deletes and re-creates this file for every tablespace to be switched into backup mode.
Opening switch log file for online backup: <i>error</i>	When performing an online backup, <code>backint</code> expects <code>brbackup</code> to provide a log file of the tablespaces that were switched into or out of backup mode.	Check if the <code>.switch.log</code> file is still in the <code>SAPBACKUP</code> directory. If so, delete the file before running the SAP backup again.
Opening switch semaphore file for online backup: <i>error</i>	When performing an online backup, <code>backint</code> tries to open a file to communicate with <code>brbackup</code> . You cannot open this file for the reason specified.	Check if the <code>.switch.sem</code> file exists in the <code>SAPBACKUP</code> directory. If so, check this file's permissions. Normally, NMSAP deletes and re-creates this file for every tablespace to be switched into backup mode.

Table 26 NMSAP error messages (continued)

Error message	Description	Solution
Switch log file indicates an error.	The <code>brconnect</code> program indicated in the switch log file that there was an error switching one of the tablespaces into or out of backup status. This error is a fatal error in the <code>backint</code> specification.	Investigate the error messages in the switch log file to determine the problem. Check the SAP installation or the SAP documentation to determine the problem.
Unable to allocate memory: <i>error</i>	The <code>backint</code> program was unable to allocate memory.	Check the memory usage on the computer.
Unable to execute child <code>backint</code> process.	The <code>backint</code> process could not run a subprocess to backup an individual save set.	Ensure that the <code>backint</code> binary is in the directory from which <code>brbackup</code> or <code>brrestore</code> runs. Check the log file for any other messages that might help pinpoint the problem.
Unable to find pid <i>process ID</i> in list of files	The <code>backint</code> program checked the status of a subprocess created to save individual files. However, the subprocess ID did not match any of the expected process IDs.	Ensure that all the files were saved by checking the rest of the messages from the backup process. In particular, check for the message “ <i>x</i> of <i>y</i> files saved at <i>time</i> .” Retry the backup if all the files were not saved.
Unable to open output file: <i>error</i>	The output file could not be opened due to the specified error.	Check the permissions on the output file and directory, and check for sufficient disk space to create a file.
Unable to query with savetime and filename both absent	The <code>backint</code> program tried to find a file in the client file index, but neither the save time nor the file name were provided.	Check the input file for any incorrect file information.
Use absolute path name for: <i>file_name</i>	The file name that was specified in the input file was not an absolute pathname. Without a full pathname, the file could not be restored or inquired.	Check the input file <code>brrestore</code> generated to ensure that the file has the correct format. If not and this error recurs, contact SAP Customer Support.

GLOSSARY

This glossary contains the definitions of terms found in this manual. Most of the terms are specific to the NMSAP software. For terms specific to the NetWorker software, refer to the latest *NetWorker Administration Guide*.

A

- active-active application cluster** Type of cluster configuration where a group of linked virtual or physical hosts with shared storage, called cluster nodes, can access the database data from multiple nodes concurrently.
- active-passive cluster** Type of cluster configuration where the data server runs on the active physical node, and other nodes are passive nodes that maintain data updates and wait to take over if the active node fails.
- administrator** Person who normally installs, configures, and maintains software on network computers, and who adds users and defines user privileges.
- attribute** Name or value property of a resource.
- autochanger** See [library](#).

B

- backup** 1. Duplicate of database or application data, or an entire computer system, stored separately from the original, which can be used to recover the original if it is lost or damaged.
2. Operation that saves data to a volume for use as a backup.
- backup level** See [level](#).
- backup volume** A volume used to store backup data. NetWorker backup data cannot be stored on an archive volume or a clone volume.
- bootstrap** Save set that is essential for disaster recovery procedures. The bootstrap consists of three components that reside on the NetWorker server: the media database, the resource database, and a server index.
- BR*Tools** SAP backup utilities, specifically the `brbackup`, `brrestore`, `brarchive`, and `brrecover` programs.

C

- client** Host on a network, such as a computer, workstation, or application server whose data can be backed up and restored with the backup server software.

Client Direct	Feature that enables clients to deduplicate backup data and send it directly to AFTD or DD Boost storage devices, bypassing the NetWorker storage node. The storage node manages the backup devices but does not handle the backup data.
client file index	Database maintained by the NetWorker server that tracks every database object, file, or file system backed up. The NetWorker server maintains a single index file for each client computer. The tracking information is purged from the index after the browse time of each backup expires.
client-initiated backup	See manual backup .
client-side configuration	Backup configuration that is created without the configuration wizard. The configuration is performed by using the NetWorker Management Console and the configuration files or parameters that are stored on the client host, as compared to a server-side configuration. See server-side configuration .
clone	<ol style="list-style-type: none"> 1. Duplicate copy of backed-up data, which is indexed and tracked by the NetWorker server. Single save sets or entire volumes can be cloned. 2. Type of mirror that is specific to a storage array.
clone volume	Exact duplicate of a backup or archive volume. NetWorker software can index and track four types of volumes (backup, archive, backup clone, and archive clone). Save sets of these different types may not be intermixed on one volume. Clone volumes may be used in exactly the same way as the original backup or archive volume.
CloudBoost device	Logical storage device that is created on a CloudBoost appliance and is used to store NetWorker backups. Each device appears as a folder on the CloudBoost appliance and appears with a storage volume name in NMC.
cluster nodes	A group of linked virtual or physical hosts with shared storage in a cluster, which work together and represent themselves as a single host called a virtual cluster host.
configuration wizard	Wizard that is integrated with the NetWorker Management Console GUI, which you can use to configure scheduled backups and also configure and run data restore and recovery. The NetWorker modules support the recovery wizard for specific applications.
Console server	See NetWorker Management Console (NMC) .
conventional storage	Storage library attached to the NetWorker server or storage node, used to store backups or snapshot backups. Also known as secondary storage. See primary storage .

D

daemon	Process on UNIX systems that runs in the background and performs a specified operation at predefined times or in response to certain events.
database	<ol style="list-style-type: none"> 1. Collection of data arranged for ease and speed of update, search, and retrieval by computer software. 2. Instance of a database management system (DBMS), which in a simple case might be a single file containing many records, each of which contains the same set of fields.

Data Domain device	Logical storage device created on a Data Domain system, used to store deduplicated NetWorker backups. Each device appears as a folder on the Data Domain system and appears with a storage volume name in NMC. A Data Domain device is also known as a DD Boost device.
DBA (database administrator)	Person who is typically responsible for installing, configuring, and maintaining database systems.
DBSID	Variable representing the name of the SAP Oracle database instance.
DD Boost	Optimized library and communication framework with a special Data Domain API that allows the backup software to define and interact with storage devices on the Data Domain system.
deduplication backup	Type of backup in which redundant data blocks are identified and only unique blocks of data are stored. When the deduplicated data is restored, the data is returned to its original native format.
deprecated feature	Feature that is supported in the current release of the product but will be unsupported and removed in a future release.
device	<ol style="list-style-type: none"> 1. Storage folder or storage unit that can contain a backup volume. A device can be a tape device, optical drive, autochanger, or disk connected to the server or storage node. 2. General term that refers to storage hardware. 3. Access path to the physical drive, when dynamic drive sharing (DDS) is enabled.
direct file access (DFA)	See Client Direct .
disaster recovery	Restore and recovery of data and business operations in the event of hardware failure or software corruption.
distributed segment processing (DSP)	Part of the DD Boost interface, which enables data deduplication to be performed on a host before the data is sent to the Data Domain system for storage.
drive	Hardware device through which media can be read or written to. See device .
E	
event-based backup	See probe-based backup .
expiration date	Date when a volume changes from read/write to read-only.
F	
firewall	Security software designed to prevent unauthorized access to or from a private network.
full backup	Type of backup that backs up all data objects or files, including the transaction logs contained in databases, regardless of when they last changed. See level .

G

group One or more client computers that are configured to perform a backup together, according to a single designated schedule or set of conditions.

H

high-availability system System of multiple computers configured as cluster nodes on a network that ensures that the application services continue despite a hardware or software failure. Each cluster node has its own IP address with private resources or disks that are available only to that computer.

host Computer on a network.

I

incremental backup See [level](#).

instance Combination of processes that runs each time a database starts up.

Internationalization (I18N) Process of adapting software to accept input and output of data in various languages and locales.

J

jukebox See [library](#).

L

label Electronic header on a volume used for identification by a backup application.

level Backup configuration option that specifies how much data is saved during a scheduled or manual backup:

- A full backup backs up all data objects or files, regardless of when they last changed.
- An incremental backup backs up only data objects or files that have changed since the previous backup.

library Hardware device that contains one or more removable media drives, as well as slots for pieces of media, media access ports, and a robotic mechanism for moving pieces of media between these components. Libraries automate media loading and mounting functions during backup and recovery. The term library is synonymous with autochanger, autoloader, carousel, datawheel, jukebox, and near-line storage.

localization (L10N) Translation and adaptation of software for the user language, time formats, and other conventions of a specific locale.

M

- manual backup** Backup that a user performs from the client, also known as an unscheduled, on-demand, or ad hoc backup.
- media** Physical storage, such as a disk file system or magnetic tape, to which backup data is written. **See** [volume](#).
- media index** Database that contains indexed entries of storage volume location and the life cycle status of all data and volumes managed by the NetWorker server. Also known as media database.
- media pool** **See** [pool](#) .
- mount host** Host used in NSM backups that is separate from the database server host, with access to the primary storage unit. During a backup to conventional storage, either the database server host or mount host backs up a point-in-time copy (snapshot) from the primary storage to conventional storage.
- multiplex** To simultaneously write data from more than one save set to the same storage device.

N

- NetWorker Management Console (NMC)** Software program that is used to manage NetWorker servers and clients. The NMC server also provides reporting and monitoring capabilities for all NetWorker processes.
- NetWorker Module for SAP (NMSAP)** Add-on module for NetWorker software that provides backup, restore, and storage management solutions for supported SAP database software.
- NetWorker server** Computer on a network that runs the NetWorker server software, contains the online indexes, and provides backup and restore services to the clients and storage nodes on the same network.
- NetWorker Snapshot Management (NSM)** Technology that provides point-in-time snapshot copies of data. NetWorker software backs up data from the snapshot. This allows applications to continue to write data during the backup operation, and ensures that open files are not omitted.
- notification** Message sent to the NetWorker administrator about important NetWorker events.

O

- offline backup** Backup of database objects performed while the corresponding database or instance is shut down and unavailable to users. Also known as a cold backup.
- online backup** Backup of database objects performed while the corresponding database or instance is running and available to users. Also known as a hot backup.
- online indexes** Databases located on the NetWorker server that contain all the information pertaining to the client backups (client file index) and backup volumes (media index).
- Oracle Recovery Manager (RMAN)** Oracle utility that acts as an intelligent interface to Oracle databases for the backup and restore of Oracle database objects.

P

parallelism	Feature that enables a maximum number of concurrent streams of data during backup or restore operations. For example, parallelism values can be set for the NetWorker server, clients, pools, and groups.
pathname	Set of instructions to the operating system for accessing a file: <ul style="list-style-type: none"> • An absolute pathname indicates how to find a file by starting from the root directory and working down the directory tree. • A relative pathname indicates how to find a file by starting from the current location.
physical host	Node or host that forms part of a cluster.
point-in-time copy (PIT copy)	Fully usable copy of a defined collection of data, such as a consistent file system, database, or volume that contains an image of the data as it appeared at a specific point in time. A PIT copy is also called a snapshot or shadow copy.
policy	Set of defined rules for client backups that can be applied to multiple groups. Groups have dataset, schedule, browse, and retention policies.
pool	<ol style="list-style-type: none"> 1. NetWorker sorting feature that assigns specific backup data to be stored on specified media volumes. 2. Collection of NetWorker backup volumes to which specific data has been backed up.
primary storage	Server storage subsystem, such as a disk array, that contains application data and any persistent snapshots of data.
probe-based backup	Type of scheduled backup, also known as an event-based backup, where the NetWorker server initiates the backup only when specified conditions are met, as determined by one or more probe settings.
proxy backup	Backup of Oracle data that creates a point-in-time (snapshot) copy on primary storage through the NSM feature. The backup optionally backs up the snapshot to secondary storage. See snapshot backup .

R

recover	To restore data files from backup storage to a client and apply transaction (redo) logs to the data to make it consistent with a given point-in-time.
recyclable save set	Save set whose browse and retention policies have expired. Recyclable save sets are removed from the media database.
recyclable volume	Storage volume whose data has exceeded both its browse and retention policies and is now available to be relabeled and reused.
redo log	Transaction log file that records a history of all the transactions made to a database. Archived redo logs are backed up and used to recover a database to a specific point-in-time.

remote device	<ol style="list-style-type: none"> 1. Storage device that is attached to a storage node that is separate from the NetWorker server. 2. Storage device at an offsite location that stores a copy of data from a primary storage device for disaster recovery.
resource	Software component whose configurable attributes define the operational properties of the NetWorker server or its clients. Clients, devices, schedules, groups, and policies are all NetWorker resources.
resource database	NetWorker database of information about each configured resource.
restore	To retrieve individual data files from backup media and copy the files to a client without applying transaction logs.
restore from conventional storage	Type of restore that restores a proxy backup from a conventional storage medium, such as a tape or disk.
retention policy	NetWorker setting that determines the minimum period of time that backup data is retained on a storage volume and available for recovery. After this time is exceeded, the data is eligible to be overwritten.
RMAN	See Oracle Recovery Manager (RMAN) .
rollback restore	Process by which a snapshot is restored to its source or alternate location by using the capability of the storage array. A rollback restore destroys existing data on the target location.
S	
save	NetWorker command that backs up client files to backup media volumes and makes data entries in the online index.
save set	<ol style="list-style-type: none"> 1. Group of files or a file system copied to storage media by a backup or snapshot rollover operation. 2. NetWorker media database record for a specific backup or rollover.
save set ID (ssid)	Internal identification number assigned to a save set.
save stream	Data and save set information that is written to a storage volume during a backup. A save stream originates from a single save set.
scanner	NetWorker command used to read a backup volume when the online indexes are not available.
scheduled backup	Type of backup that is configured to start automatically at a specified time for a group of one or more NetWorker clients. A scheduled backup generates a bootstrap save set.
server-side configuration	Backup configuration that is performed through the configuration wizard, with settings saved on the NetWorker server, as compared to client-side configuration. See client-side configuration .
shared disk	Storage disk that is connected to multiple nodes in a cluster.

snapshot	Point-in-time, read-only copy of specific data files, volumes, or file systems on an application host. Operations on the application host are momentarily suspended while the snapshot is created on a proxy host. Also called a PiT copy, image, or shadow copy.
snapshot backup	Snapshot created on a storage array as a backup. Previously called instant backup.
snapshot policy	Sets of rules that control the life cycle of snapshots. These rule specify the frequency of snapshot creation, how long snapshots are retained, and which snapshots will be backed up to conventional storage media.
snapshot restore	Restore from a snapshot backup. Previously called instant restore.
snapshot save set	Group of files or other data included in a single snapshot. Previously called a snapset.
storage device	See device .
storage node	Computer that manages physically attached storage devices or libraries, whose backup operations are administered from the controlling NetWorker server. Typically a “remote” storage node that resides on a host other than the NetWorker server.

T

tablespace	Database structure that consists of one or more data files.
target database	Database that the NetWorker server backs up as a safeguard against data loss.
transaction log	Record of named database transactions or list of changed files in a database, stored in a log file to execute quick restore and rollback transactions.

U

unscheduled backup	See manual backup .
---------------------------	-------------------------------------

V

volume	<ol style="list-style-type: none"> 1. Unit of physical storage medium, such as a disk or magnetic tape, to which backup data is written. 2. Identifiable unit of data storage that may reside on one or more computer disks.
volume name	Name that you assign to a backup volume when it is labeled.