

NetBackup™ Web UI Microsoft SQL Server Administrator's Guide

Release 9.1

VERITAS™

Last updated: 2021-06-02

Legal Notice

Copyright © 2021 Veritas Technologies LLC. All rights reserved.

Veritas, the Veritas Logo, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third-party software for which Veritas is required to provide attribution to the third party ("Third-party Programs"). Some of the Third-party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the Third-party Legal Notices document accompanying this Veritas product or available at:

<https://www.veritas.com/about/legal/license-agreements>

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. Veritas Technologies LLC SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

<http://www.veritas.com>

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

<https://www.veritas.com/support>

You can manage your Veritas account information at the following URL:

<https://my.veritas.com>

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)

CustomerCare@veritas.com

Japan

CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

<https://sort.veritas.com/documents>

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

NB.docs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

<http://www.veritas.com/community/>

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1	Introducing the NetBackup web user interface	7
	7
	About the NetBackup web UI	7
	Terminology	9
	Sign in to the NetBackup web UI	10
	Sign out of the NetBackup web UI	12
Chapter 2	About NetBackup for SQL Server	13
	Overview of NetBackup for SQL Server	13
Chapter 3	Installation and host configuration	16
	Planning the installation of NetBackup for SQL Server	16
	Configuring SQL Server hosts and user permissions	17
	Installing the Veritas VSS provider for vSphere	18
	Configuring the NetBackup services for SQL Server backups and restores	19
	Configure local security privileges for SQL Server	20
Chapter 4	Monitoring NetBackup	22
	The NetBackup dashboard	22
	Monitoring jobs	22
	Filter jobs in the job list	23
Chapter 5	Managing SQL Server discovery and credentials	24
	24
	About discovery of SQL Server objects	24
	Discover advanced or basic availability groups on demand	25
	Discover databases on demand	26
	Discover read-scale availability groups	26
	Browse SQL Server assets	26
	About SQL Server credentials	29
	Add credentials to SQL Server instances or replicas	30
	Manage SQL Server credentials	32

	Remove SQL Server instances	32
	Manually add a SQL Server instance	33
Chapter 6	Managing protection plans for SQL Server	34
	About protecting SQL Server availability groups	34
	Create a protection plan to protect SQL Server assets	35
	Schedules and retention	38
	Performance tuning and configuration options	38
	Using copy-only snapshot backups to affect how differentials are based	41
	Snapshot methods	42
	Protect a SQL Server availability group that crosses NetBackup domains	43
Chapter 7	Protecting SQL Server	46
	Add SQL Server assets to a protection plan	46
	Edit protection settings for a Microsoft SQL Server asset	48
	View the protection status of databases, instances, or availability groups	49
	Remove protection from SQL Server assets	50
Chapter 8	Restoring SQL Server	52
	Requirements for restores of SQL Server	52
	Perform a complete database recovery	53
	Recover a single recovery point	56
	Options for SQL Server restores	59
	Restore a database (non-administrator users)	60
	Select a different backup copy for recovery	61
	Restore a SQL Server availability database to a secondary replica	64
	Restore a SQL Server availability database to the primary and the secondary replicas	66
Chapter 9	Using instant access with SQL Server	69
	Prerequisites when you configure an instant access SQL Server database	69
	Hardware configuration requirement of instant access	71
	Things to consider before you configure an instant access database	71
	Configure Samba users for SQL Server instant access	72
	Configure an instant access database	73

	View the livemount details of an instant access database	75
	Delete an instant access database	76
	Options for NetBackup for SQL Server instant access	76
	NetBackup for SQL Server terms	77
	Frequently asked questions	78
Chapter 10	Protecting SQL Server with VMware backups	83
	About protecting an application database with VMware backups	83
	Create a protection plan to protect SQL Server data with a VMware backup	84
	Backup options and Advanced options	85
	Exclude disks from backups	87
	Snapshot retry options	87
	Protect SQL Server data with a VMware backup	88
	Restore SQL Server databases from a VMware backup	89
Chapter 11	Troubleshooting	90
	Troubleshooting credential validation	90
	Troubleshooting VMware backups and restores of SQL Server	91
	SQL Server log truncation failure during VMware backups of SQL Server	92

Introducing the NetBackup web user interface

This chapter includes the following topics:

- [About the NetBackup web UI](#)
- [Terminology](#)
- [Sign in to the NetBackup web UI](#)
- [Sign out of the NetBackup web UI](#)

About the NetBackup web UI

The NetBackup web user interface provides the following features:

- Ability to access the primary server from a web browser, including Chrome and Firefox. For details on supported browsers for the web UI, see the [NetBackup Software Compatibility List](#).
Note that the NetBackup web UI may behave differently for different browsers. Some functionality, for example a date picker, may not be available on all browsers. These inconsistencies are due to the capabilities of the browser and not because of a limitation with NetBackup.
- A dashboard that displays a quick overview of the information that is important to you.
- Role-based access control (RBAC) that lets the administrator configure user access to NetBackup and to delegate the tasks for workload protection.
- Protection of assets is achieved through protection plans, job management, and visibility of the protection status of assets.

Alternatively, policy management is also available for a limited number of policy types. More information about these policy types is available:

- Workload administrators can create protection plans, subscribe assets to the protection plans that meet the SLO, monitor protection status, and perform self-service recovery of assets.

Note: The NetBackup web UI is best viewed at a 1280x1024 or higher screen resolution.

Access control in the NetBackup web UI

NetBackup uses role-based access control to grant access to the web UI. Access control is accomplished through roles.

- A role defines the operations that a user can perform and the features that the user can access in the web UI. For example, access to any workload assets, protection plans, or credentials.
- RBAC is only available for the web UI and the APIs.
Other access control methods for NetBackup are not supported for the web UI and APIs, with the exception of Enhanced Auditing (EA).

Monitor NetBackup jobs

The NetBackup web UI lets administrators more easily monitor NetBackup job operations and identify any issues that need attention.

Protection plans: One place to configure schedules, storage, and storage options

Protection plans offer the following benefits:

- A default workload administrator can select the protection plans to use to protect assets.
- With the necessary RBAC permissions, a workload administrator can create and manage protection plans, including the backup schedules and storage that is used.
- In addition to schedules for backups, a protection plan can also include a schedule for replication and long-term retention.
- When you select from your available storage, you can see any additional features available for that storage.

Self-service recovery

The NetBackup web UI makes it easy for a workload administrator to recover VMs, databases, or other asset types applicable to that workload.

For the workloads that support the instant access feature, users can mount a snapshot for immediate access to a VM's files or to a database.

Terminology

The following table describes the concepts and terms in web user interface.

Table 1-1 Web user interface terminology and concepts

Term	Definition
Asset group	See <i>intelligent group</i> .
Asset	The data to be protected, such as physical clients, virtual machines, and database applications.
Backup now	An immediate backup of an asset. NetBackup performs a one-time, full backup of an asset using the selected protection plan. This backup does not affect any scheduled backups.
Intelligent group	Allows NetBackup to automatically select assets for protection based on the criteria (queries) that you specify. An intelligent group automatically stays up-to-date with changes in the production environment. These groups are also referred to as asset groups. These groups appear under the tab Intelligent VM groups or Intelligent groups .
Instant access	Note: Instant access is supported only a select number of workloads. An instant access VM or database that is created from a NetBackup backup image is available almost instantaneously, achieving a near-zero recovery time objective. NetBackup mounts the snapshot directly on the backup storage device and the snapshot is treated as a normal VM or database.
Protection plan	A protection plan defines when backups are performed, how long the backups are retained, and the type of storage to use. Once a protection plan is set up, assets can be subscribed to the protection plan.

Table 1-1 Web user interface terminology and concepts (*continued*)

Term	Definition
RBAC	Role-based access control. The role administrator can delegate or limit access to the NetBackup web UI through the roles that are configured in RBAC. Note: The roles that you configure in RBAC do not control access to the NetBackup Administration Console or the CLIs.
Role	For RBAC, defines the operations that a user can perform and the assets or objects that they can access. For example, you can configure a role to manage recovery of specific databases and the credentials that are needed for backups and restores.
Storage	The storage to which the data is backed up, replicated, or duplicated (for long-term retention).
Subscribe, to a protection plan	The action of selecting an asset or an asset group to subscribe to a protection plan. The asset is then protected according to the schedule in the plan. The web UI also refers to <i>Subscribe as Add protection</i> .
Unsubscribe, from a protection plan	<i>Unsubscribe</i> refers to the action of removing protection or removing an asset or asset group from a plan.
Workload	The type of asset. For example, VMware, RHV, AHV, or Cloud.

Sign in to the NetBackup web UI

Authorized users can sign in to a NetBackup primary server from a web browser, using the NetBackup web UI.

The following sign-in options are available:

- [Sign in with a username and password](#)
- [Sign in with a certificate or smart card](#)
- [Sign in with single sign-on \(SSO\)](#)

Sign in with a username and password

Only authorized users can sign in to NetBackup web UI. Contact your NetBackup security administrator for more information.

To sign in to a NetBackup primary server using a username and password

- 1 Open a web browser and go to the following URL.

`https://primaryserver/webui/login`

The *primaryserver* is the host name or IP address of the NetBackup primary server that you want to sign in to.

- 2 Enter your credentials and click **Sign in**.

For example:

For this type of user	Use this format	Example
Local user	<i>username</i>	jane_doe
Windows user	<i>DOMAINusername</i>	WINDOWS\jane_doe
UNIX user	<i>username@domain</i>	john_doe@unix

Sign in with a certificate or smart card

You can sign in to NetBackup web UI with a smart card or digital certificate if you are an authorized user. Contact your NetBackup security administrator for more information.

To use a digital certificate that is not on a smart card, you must first upload the certificate to the browser's certificate manager. See the browser documentation for instructions or contact your certificate administrator for more information.

To sign in with a certificate or smart card

- 1 Open a web browser and go to the following URL.

`https://primaryserver/webui/login`

The *primaryserver* is the host name or IP address of the NetBackup primary server that you want to sign in to.

- 2 Click **Sign in with certificate or smart card**.
- 3 When your browser prompts you, select the certificate.

Sign in with single sign-on (SSO)

You can sign in to NetBackup web UI with the single sign-on (SSO) option if SAML is configured as an identity provider in your NetBackup environment. Contact your NetBackup security administrator for more information.

To sign in to a NetBackup primary server using SSO

- 1** Open a web browser and go to the following URL.

`https://primaryserver/webui/login`

The *primaryserver* is the host name or IP address of the NetBackup primary server that you want to sign in to.

- 2** Click **Sign in with single sign-on**.
- 3** Follow the steps as provided by your administrator.

On subsequent logons, NetBackup signs you in automatically to the primary server.

Sign out of the NetBackup web UI

Note that NetBackup automatically signs you out of the web UI after 24 hours, which is the maximum time that is allowed for a user session. After that time NetBackup requires that you sign in again. You can also sign out if you want to change the sign-in option that you want to use (username and password, smart card, or single sign-on (SSO)).

To sign out of the NetBackup web UI

- ◆ On the top right, click the profile icon and click **Sign out**.

About NetBackup for SQL Server

This chapter includes the following topics:

- [Overview of NetBackup for SQL Server](#)

Overview of NetBackup for SQL Server

The NetBackup web UI provides the capability for backups and restores of SQL Server databases. Instances are automatically discovered in the NetBackup environment and SQL Server administrators can select one or more protection plans that contain the wanted storage, backup, and tuning settings.

The NetBackup web UI lets you perform the following operations:

- View discovered instances, databases, or availability groups.
- Select protection plans to protect SQL Server assets.
- Restore databases.
- Monitor restore operations.

In this guide, Microsoft SQL Server is referred to as SQL Server. NetBackup for Microsoft SQL Server is referred to as NetBackup for SQL Server.

Table 2-1 NetBackup for SQL Server features

Feature	Description
Integration with NetBackup role-based access control (RBAC)	The NetBackup Web UI provides RBAC roles to control which NetBackup users can manage SQL Server operations in NetBackup. The user does not need to be a NetBackup administrator to manage SQL Server operations. However, the user still must be a member of the Windows administrator group and have the SQL Server “sysadmin” role.
Protection plans	<p>The following benefits are included:</p> <ul style="list-style-type: none"> ■ Use a single protection plan to protect multiple SQL Server instances or instance databases or a plan to protect availability groups or availability databases. Instances can be spread over multiple clients. ■ Include a full, differential, and transaction log backup in the same policy. ■ Schedule frequent backups of transaction logs. ■ You are not required to know SQL Server commands or to write and use batch files. Instead, this feature automatically generates the batch files at run-time.
Management of SQL Server assets	NetBackup automatically discovers SQL Server instances and availability groups in the environment. You can also perform manual discovery. After instances or replicas are registered, the SQL Server workload administrator can select one or more protection plans to protect the SQL Server assets.
Authentication and credentials	<p>SQL Server protection plans support the following:</p> <ul style="list-style-type: none"> ■ Windows authentication and Windows Active Directory authentication. ■ With the proper configuration, you do not have to run the NetBackup service account as a privileged SQL Server user on the client.
Backup and restore features	<p>The following features are available for backups and restores:</p> <ul style="list-style-type: none"> ■ Backups and are managed entirely by the NetBackup server from a central location. Administrators can schedule automatic, unattended backups for instances on local or remote hosts across the network. ■ The NetBackup web UI supports the backup and restore of databases and transaction logs from one interface. Note: SQL Server recovery with the web UI requires that the SQL Server client is at version 8.3 or later. ■ Backup schedules for full, differential, or transaction log backups. ■ Manual backups and copy-only backups. ■ Support for high availability (HA) environments, including SQL Server clusters and availability groups. ■ Restore SQL Server objects to different locations (redirected restores). ■ Ability to use multiple stripes during a backup. ■ Tuning options that can improve the performance of backups.

Table 2-1 NetBackup for SQL Server features (*continued*)

Feature	Description
Stream-based backups and restores	Stream-based backup and restore of SQL Server objects with SQL Server's high-speed virtual device interface.
Snapshot backups and instant access databases	<p>NetBackup can perform backups of SQL Server with snapshot methodology.</p> <p>You can also create an instant access database from a NetBackup backup image. The database is available almost instantaneously, achieving a near-zero recovery time objective. NetBackup mounts the database's snapshot directly on the backup storage device and treats the snapshot as a normal database.</p>
Support for VMware backups that protect SQL Server	<p>Support for application-consistent, full backups of VMware computers using snapshots. Use of NetBackup Accelerator can also increase the speed of backups.</p> <p>See the following documents for more information.</p> <p>NetBackup for VMware Administrator's Guide</p> <p>NetBackup Administrator's Guide, Volume I</p>

Installation and host configuration

This chapter includes the following topics:

- [Planning the installation of NetBackup for SQL Server](#)
- [Configuring SQL Server hosts and user permissions](#)
- [Configuring the NetBackup services for SQL Server backups and restores](#)
- [Configure local security privileges for SQL Server](#)

Planning the installation of NetBackup for SQL Server

[Table 3-1](#) shows the installation steps that are required to run NetBackup for SQL Server.

Table 3-1 Installation steps for NetBackup for SQL Server

Step	Action	Description
Step 1	Verify the operating system and platform compatibility.	See the NetBackup Compatibility Lists .
Step 2	Verify that primary server has a valid license for NetBackup for SQL Server and any NetBackup options or add-ons that you want to use.	

Table 3-1 Installation steps for NetBackup for SQL Server (*continued*)

Step	Action	Description
Step 3	<p>Install the NetBackup client software on the computers that have the databases that you want to back up. The NetBackup for SQL Server agent is installed with the NetBackup client software.</p> <p>To use the new features that are included in NetBackup for SQL Server in NetBackup 9.1, upgrade your NetBackup for SQL Server clients to NetBackup 9.1. The NetBackup media server must use the same version as or a higher version than the NetBackup for SQL Server client.</p>	<p>Note the following:</p> <ul style="list-style-type: none"> ■ For SQL Server availability groups, install the client on each replica in the availability group where you want backups to occur. ■ In a SQL Server cluster environment, install the NetBackup client on each node in the cluster. Each node must have the same version of NetBackup. ■ In a VMware environment, install the NetBackup client software on the virtual machines that have SQL Server running. ■ If you have multiple NICs, install the NetBackup client using the private interface name. ■ If the SQL Server client is on a different host than the primary server or media server, then install the NetBackup client on that host.
Step 4	<p>To protect a read-scale availability group, you must have the SQL Server Native Client version 11.0.7462 ODBC driver or later installed on the availability group replicas.</p>	<p>This version of the driver lets you discover and browse databases on a read-scale availability group.</p>
Step 5	<p>To use NetBackup for SQL Server in a NetBackup cluster, verify that your cluster environment is supported and that the NetBackup cluster is configured correctly.</p>	<p>Review the following requirements:</p> <ul style="list-style-type: none"> ■ The NetBackup server software is installed and configured to work in a NetBackup cluster. ■ The NetBackup client software is installed and operational on each node to which NetBackup can failover. ■ A valid license must exist for NetBackup for SQL Server on each node where NetBackup server resides. <p>See the Software Compatibility List (SCL).</p> <p>See the NetBackup Installation Guide.</p> <p>See the NetBackup Clustered Master Server Administrator's Guide.</p>

Configuring SQL Server hosts and user permissions

The following table contains the prerequisites for users to run SQL Server backups and restores.

Table 3-2 Prerequisites for NetBackup hosts and user permissions

Step	Action	Description
Step 1	If you plan to perform VMware backups to protect SQL Server, install the Veritas VSS provider.	See "Installing the Veritas VSS provider for vSphere" on page 18.
Step 2	Configure the NetBackup Client Service and the NetBackup Legacy Network Service to access the SQL Server when NetBackup performs backups and restores.	See "Configuring the NetBackup services for SQL Server backups and restores" on page 19.
Step 3	If you want to use the option Use these specific credentials for SQL server credentials, an account other than Local System requires certain local security privileges.	These privileges are necessary since the NetBackup for SQL Server agent logs on as the SQL Server user when it accesses data. See "Configure local security privileges for SQL Server" on page 20.
Step 4	Approve each valid host mapping that NetBackup discovers.	NetBackup automatically discovers many shared names and cluster names that are associated with the NetBackup hosts in your environment. Perform this configuration in Security > Hosts on the primary server. Refer to the information on configuring host mappings in the NetBackup Web UI Administrator's Guide . Or, contact your NetBackup administrator for assistance.

Installing the Veritas VSS provider for vSphere

To use the Veritas VSS provider you must install it manually following installation of the NetBackup for Windows client. If the VMware VSS provider is installed, the installation program removes it and may require a restart of the computer.

To install the Veritas VSS provider

- 1 Browse to the following location:

`install_path\Veritas\NetBackup\bin\goodies\`
- 2 Double-click on the **Veritas VSS provider for vSphere** shortcut.
- 3 Follow the prompts.
- 4 When the utility has completed, restart the computer if prompted.
- 5 Following the restart, the utility resumes. Follow the prompts to complete the installation.

To uninstall the Veritas VSS provider

- 1 In the Control Panel, open **Add or Remove Programs** or **Programs and Features**.
- 2 Double-click on **Veritas VSS provider**.

The uninstall program does not automatically reinstall the VMware VSS provider.

Configuring the NetBackup services for SQL Server backups and restores

For policies and protection plans with the NetBackup web UI, NetBackup uses the NetBackup Client Service and the NetBackup Legacy Network Service to access the SQL Server when it performs backups and restores.

Note the following requirements for the NetBackup services logon account:

- The account has the fixed server role “sysadmin”. You can use a domain account, a member of BUILTIN\Administrators, or another account that has this role.
- (non-VMware backups) If you want to use Local System for the logon account, apply the SQL Server sysadmin role manually to the NT AUTHORITY\SYSTEM or the BUILTIN\Administrators group.
- (VMware backups) You must use an account other the Local System account as the logon account. Both services must use the same logon account.
- (VMware backups) If you choose to truncate logs, ensure that the account that runs the Microsoft SQL Server Service has full permissions for the NetBackup Legacy Network Service `temp` directory.

This directory is `C:\Users\user\AppData\Local\Temp`. *User* is the account that runs the NetBackup Legacy Network Service.

To configure the NetBackup services for SQL Server backups and restores

- 1 Log on to the Windows host with the account that has the SQL Server sysadmin role and any necessary local security privileges.
- 2 In the Windows Services application, open the **NetBackup Client Service**.
- 3 Configure the account as follows:
 - (non-VMware backups) Confirm that **Local System account** or a SQL Server administrator account is configured.
If you use the setting **Use credentials that are defined locally on the client** for instance credentials, both services must use the same logon account. If you use the setting **Use these specific credentials** for instance

credentials, the services can use the same logon or separate logon accounts.

- (VMware backups) Provide the name of the logon account and click **OK**. The account must include the domain name, followed by the user account, **domain_name\account**. For example, **recovery\netbackup**.

4 Open the **NetBackup Legacy Network Service**.

5 Configure the account as follows:

- (non-VMware backups) Confirm that **Local System account** or a SQL Server administrator account is configured.
 If you use the setting **Use credentials that are defined locally on the client** for instance credentials, both services must use the same logon account. If you use the setting **Use these specific credentials** for instance credentials, the services can use the same logon or separate logon accounts.
- (VMware backups) Provide the name of the logon account and click **OK**. Configure the same logon account for this service as you did for the NetBackup Client Service.

6 If you selected a different logon account, restart the services.

7 If you selected the option **Use these specific credentials** for instance or for replica credentials, an account other than Local System requires certain local security privileges.

See [“Configure local security privileges for SQL Server”](#) on page 20.

8 For virtual environments, configure the services on the necessary services.

- For VMware backups, configure the services for each host that you use to browse for backups and perform restores.
- For a SQL Server cluster, configure the services on each node in the cluster.
- For availability groups, configure the services on all replicas in the availability group where you want to run backups.

Configure local security privileges for SQL Server

If you use the option **Use these specific credentials** for instance or for replica credentials, an account other than Local System requires certain local security privileges. These privileges are necessary since the NetBackup for SQL Server agent logs on as the SQL Server user when it accesses data.

Note: This configuration applies to local security privileges only. For domain-level privileges, contact your domain administrator.

To configure the local security privileges

- 1** Open the **Local Security Policy**.
- 2** Click **Local Policies**.
- 3** In the **User Rights Assignment**, add the account to the following policies:
 - **Impersonate a client after authentication**
 - **Replace a process level token**
- 4** Restart the SQL Server.
- 5** If the NetBackup Client Service and the NetBackup Legacy Network Service use this account to log on, restart these services.
- 6** (non-VMware backups) For a SQL Server cluster, configure the local security privileges on each node in the cluster. For SQL Server availability groups, configure the services on all replicas where you want to run backups.

Monitoring NetBackup

This chapter includes the following topics:

- [The NetBackup dashboard](#)
- [Monitoring jobs](#)
- [Filter jobs in the job list](#)

The NetBackup dashboard

The NetBackup dashboard provides a quick view of the details that are related to your role in your organization.

Table 4-1 The NetBackup dashboard

Dashboard widget	Description
Jobs	Lists job information, including the number of active and queued jobs and the status of attempted and completed jobs.

Monitoring jobs

Use the **Jobs** node to monitor the jobs in your NetBackup environment and view the details for a specific job.

To monitor a job

- 1 On the left, click **Activity monitor > Jobs**.
- 2 Click on a job name that you want to view.
On the **Overview** tab you can view information about a job.
 - The **File List** contains the files that are included in the backup image.

- The **Status** section shows the status and the status codes that are related to the job. Click the status code number to view information about this status code in the Veritas Knowledge Base.
See the [NetBackup Status Codes Reference Guide](#).
- 3 Click the **Details** tab to view the logged details about a job. You can filter the logs by error type using the drop-down menu.
See “[Filter jobs in the job list](#)” on page 23.

Filter jobs in the job list

You can filter the jobs to display the jobs in a specific state. For example, you can display all of the active jobs or all of the suspended jobs.

To filter the job list

- 1 Click **Jobs**.
- 2 Above the job list, click the **Filter** option.
- 3 In the **Filter** window, select a filter option to dynamically change the jobs that are displayed. The filter options are as follows:
 - **All**
 - **Active**
 - **Done**
 - **Failed**
 - **Incomplete**
 - **Partially Successful**
 - **Queued**
 - **Successful**
 - **Suspended**
 - **Waiting for Retry**
- 4 Click **Apply Filters**.
- 5 To remove the selected filters, click **Clear All**.

Managing SQL Server discovery and credentials

This chapter includes the following topics:

- [About discovery of SQL Server objects](#)
- [Browse SQL Server assets](#)
- [About SQL Server credentials](#)
- [Add credentials to SQL Server instances or replicas](#)
- [Manage SQL Server credentials](#)
- [Remove SQL Server instances](#)
- [Manually add a SQL Server instance](#)

About discovery of SQL Server objects

NetBackup discovery runs regularly and gathers information for instances and for advanced and basic availability groups in your environment. (Read-scale availability groups must be discovered manually.) The data expires after one hour. The NetBackup Discovery Service (`nbdisco`) runs “shallow” discovery every 8 hours for instances and availability groups on the clients for that master server. The NetBackup Agent Request Service (NBARS) polls the master server every 5 minutes for any non-expired data.

Deep discovery includes discovery of databases and is performed in the following circumstances:

- After a full backup, an incremental backup, or a restore occurs

The client sends details when database data is changed and not more than every 15 minutes.

- When you run a manual discovery of databases or availability groups
- After you add credentials for the instances or replicas

By default, this service reports to the master server when it finds SQL Server instances. However, the user can turn off discovery for a specific client, with the `bpsetconfig` utility. See the `REPORT_CLIENT_DISCOVERIES` option in the [NetBackup Administrator's Guide, Volume I](#).

The client maintains a cache file `NB_instancename_cache_v1.0.dat` in the `NetBackup\dbext\mssql` directory for each instance. The file can be deleted and NetBackup recreates it after the next full backup when deep discovery data is sent again.

Confirmation messages in the web UI

A message `Starting the discovery of databases...` displays after you click **Discover databases** or **Discover availability groups**. This message only indicates that a request was made to start the discovery process. However, database discovery can fail for different reasons. For example, if the instance is not associated with valid credentials or the host cannot be reached. You can consider the deep discovery is successful when the message displays: `Successfully started the discovery of databases. Click Refresh to update the list.`

Discover advanced or basic availability groups on demand

You can manually start the NetBackup discovery process if you want to immediately discover advanced or basic availability groups or replicas or discover databases in your environment. The instances or replicas must have credentials before you can perform on-demand discovery.

To discover advanced or basic availability groups

- 1 On the left, click **Workloads > Microsoft SQL Server**.
- 2 Click on the **Availability groups** tab.
- 3 Click **Discover availability groups**.
- 4 Select the host and the instance that is associated with a replica in the availability group.

Note that only registered replicas are shown in this list.

- 5 Click **Discover**.

Discover databases on demand

You can manually start the NetBackup discovery process if you want to immediately discover instance databases or availability databases in your environment.

To discover databases

- 1 On the left, click **Workloads > Microsoft SQL Server**.
- 2 Click on the **Databases** tab.
- 3 Click **Discover databases**.
- 4 Select the host and the instance that is associated with the databases.
Note that only registered instances are shown in this list.
- 5 Click **Discover**.

Discover read-scale availability groups

Read-scale availability groups are not discovered automatically. You must specify one of the replicas in the availability group and manually start discovery.

To discover read-scale availability groups

- 1 On the left, click **Workloads > Microsoft SQL Server**.
- 2 Click on the **Instances** tab.
- 3 Select one of the replicas that is part of the availability group and click **Manage credentials**.
- 4 Follow the prompts to provide the credentials for the replica.
- 5 Click on the **Availability groups** tab.
- 6 Click **Discover availability groups**.
- 7 Select the host and the instance that is associated with a replica in the availability group.
Note that only registered replicas are shown in this list.
- 8 Click **Discover**.

Browse SQL Server assets

You can browse instances, databases, and availability groups to view their details such as how they are protected and recovery points that are available.

Note: Classic policy information is displayed for databases but not for instances or availability groups. The web UI indicates if a protection plan protects the instance or replica, but not if a classic policy does. However, when a backup using a classic policy is performed on an individual database, the **Protected by** column displays the classic policy name.

Browse SQL Server instances

On the **Instances** tab you can view and manage instances, including how they are protected and the instance credentials.

To browse SQL Server instances

- 1 On the left, click **Workloads > Microsoft SQL Server**.
- 2 Click the **Instances** tab.
- 3 To view the available actions for one or more instances, select the checkbox for the instances. Note that **Backup now** is only available when you select one instance.
- 4 To view the details for an instance, click the instance. You can perform the following tasks.
 - Perform an immediate backup of the instance by clicking **Backup now**.
 - Click **Add protection** to add the instance to a protection plan.
 - Click **Remove protection** to remove an instance from a protection plan.
 - To see the databases that are discovered the instance and their protection information and status, click on the **Databases** tab.
 - To view the roles that have access to the instance, click the **Permissions** tab.

Browse SQL Server availability groups

On the **Instances** tab you can view and manage availability groups, including how database and replica details and how the availability group is protected.

To browse SQL Server availability groups

- 1 On the left, click **Workloads > Microsoft SQL Server**.
- 2 To view the available actions for one or more availability groups, select the check box for the availability groups. Note that **Backup now** is only available when you select one availability group.
- 3 Click on an availability group to view its details. You can perform the following tasks.

- Click **Backup now** to perform an immediate backup of the instance.
- Click **Add protection** to add the availability group to a protection plan.
- Click **Remove protection** to remove an availability group from a protection plan.
- To see the databases that are discovered for the availability group and their protection information and status, click on the **Databases** tab.
- To see the replicas for the availability group and their protection information and status, click on the **Replicas** tab.
- To view the roles that have access to the availability group, click the **Permissions** tab.

Browse SQL Server databases

Note: Databases only appear on the **Databases** tabs if they meet one of the following criteria: A backup exists of the database, the database instance has validated credentials, or a manual discovery of databases was performed.

To browse SQL Server databases

- 1 On the left, click **Workloads > Microsoft SQL Server**.
- 2 Click the **Databases** tab.
- 3 To view the available actions for one or more databases, select the check box for each database. Note that **Backup now** is only available when you select one database.
- 4 To view the details for a database, click the database. You can perform the following tasks.
 - Click **Backup now** to perform an immediate backup of the instance.
 - Click **Add protection** to add the database to a protection plan.
 - Click **Remove protection** to remove a database from a protection plan.
 - To see the available recovery points for the database, click **Recovery points**.
 - To view the restore jobs for the database, click **Restore activity**.
 - To view the roles that have access to the database, click the **Permissions** tab.

About SQL Server credentials

To protect SQL Server, you must add (or register) credentials to the SQL Server instances or availability replicas. The NetBackup web UI supports Windows authentication and Windows Active Directory authentication. It does not support Mixed Mode or SQL Server authentication. Credentials are not supported at the database or the availability group level.

Table 5-1 Options to register credentials

Option to register credentials	Environment and configuration
<p>Use these specific credentials (recommended)</p>	<ul style="list-style-type: none"> ■ The SQL Server DBA provides the NetBackup administrator with the SQL Server user credentials. ■ The SQL Server DBA does not want the NetBackup services running as a privileged SQL Server user on the client. <p>Configuration requirements</p> <p>The user account that is used to register credentials must have the SQL Server “sysadmin” role and be a member of the Windows Administrators group.</p> <p>The NetBackup services can use the Local System logon account. If you want to use a different logon account, that account must also have certain local security privileges.</p>
<p>Use credentials that are defined locally on the client</p>	<ul style="list-style-type: none"> ■ The NetBackup services run as a privileged SQL Server user on the client. ■ The SQL Server DBA does not want to provide credentials to register instances or replicas. ■ The NetBackup administrator does not have access to the SQL Server credentials. <p>Configuration requirements</p> <p>The user account that is used to register credentials must have the SQL Server “sysadmin” role and be a member of the Windows Administrators group.</p> <p>You must also configure the logon account for the NetBackup services.</p>

Registering instances when SQL Server hosts are clustered or use multiple NICs

When NetBackup discovers a SQL Server cluster, it adds a single entry on the **Instances** tab. This instance represents all nodes in the cluster. The host name is the virtual name of the SQL Server cluster. When you add credentials for this instance NetBackup validates the credentials on the active node. The credentials must be valid for all nodes in the cluster.

When NetBackup discovers a SQL Server host that uses multiple NICs, it adds an entry using the NetBackup client name on the **Instances** tab. If you installed the NetBackup client using the public interface name, you must configure the NetBackup client name as the private interface name. Then add credentials to the instance with its private interface name. For a SQL Server cluster that uses multiple NICs, add credentials to the instance with the private virtual name of the SQL Server cluster.

Registering Microsoft SQL Server failover cluster instances (FCIs)

NetBackup discovers and displays failover cluster instances (FCIs) under the cluster name and the physical node names. For example, instance `FCI` is enumerated with both its physical nodes `hostvm10` and `hostvm11` and with its cluster name `sql-fci`. Databases that exist for FCIs are also enumerated with the node names and the cluster name. Depending on how you want to protect a database, add credentials to either the cluster name (that are valid for all nodes) or to a physical node name.

Validation of credentials

After you add credentials, NetBackup validates the credentials and starts database and availability group discovery. When discovery completes, the results are displayed on the **Databases** or the **Availability group** tab.

For a SQL Server cluster or if an availability group instance is part of SQL Server cluster, NetBackup validates the credentials on the active node. The credentials must be valid for all nodes in the cluster. For a SQL Server availability group, replicas are registered and validated individually. Note that the registered date reflects the date and time the credential was added or updated and does not indicate if the credentials are valid.

Add credentials to SQL Server instances or replicas

To allow for full discovery of SQL Server assets, you must add new credentials or select the existing server credentials for the instances or replicas. Review the requirements for the SQL Server credential option that you want to use.

See [“About SQL Server credentials”](#) on page 29.

Select existing credentials for SQL Server instances or replicas

You can select the credentials you want to apply to an instance or replica from the list of existing SQL Server credentials.

For availability groups, each replica in must be registered with credentials.

To select credentials for SQL Server instances or replicas

- 1 On the left, click **Workloads > Microsoft SQL Server**.
- 2 Click on the **Instances** tab.
- 3 Select the check box for the instances or replicas and click **Manage credentials**.
- 4 Choose **Select from existing credentials** and click **Next**.
- 5 Select the credential that you want to use for the selected assets and click **Next**.

NetBackup validates the credentials.

- 6 The database and the availability group discovery begin after the credentials are validated. However, these assets may not appear in the web UI immediately. They appear after the discovery process completes. Note that the dates reflect when the credential was added or updated and does not indicate if the credential is valid.

Add new credentials to SQL Server instances or replicas

If the credentials you want to apply to an instance or replica are not available, you can add them to NetBackup.

For availability groups, each replica in must be registered with credentials.

To add new credentials to SQL Server instances or replicas

- 1 On the left, click **Workloads > Microsoft SQL Server**.
- 2 Click on the **Instances** tab.
- 3 Select the check box for the instances or replicas and click **Manage credentials**.
- 4 Choose **Add credentials** and click **Next**.
- 5 Enter a credential name.
- 6 Select one of the following options:
 - **Use credentials that are defined locally on the client** and click **Next**.
 - **Use these specific credentials**
 Provide the **User name**, **password**, and **Domain** that are associated with the credentials. Click **Next**.

See [“About SQL Server credentials”](#) on page 29.

- 7 The **Permissions** screen displays the roles that have access to the credential.
- 8 Click **Next**.

The database and the availability group discovery begins after the credentials are validated. However, these assets may not appear in the web UI immediately. They appear after the discovery process completes. Note that the dates reflect when the credential was added or updated and does not indicate if the credential is valid.

Manage SQL Server credentials

Users with the proper RBAC permissions can view and manage the credentials for SQL Server instances.

To edit a SQL Server credential

- 1 On the left, click **Workloads > Microsoft SQL Server** and then click on the **Instances** tab.
- 2 Select the instance or replica that you want to edit and click **Manage credentials**.

Remove SQL Server instances

Use this procedure to remove the instances that no longer exist in your environment.

To remove a SQL Server instance

- 1 On the left, click **Workload > Microsoft SQL Server**, then click the **Instances** tab.
- 2 Locate and select the checkbox for the instance.
- 3 Click **Remove**.

Note: If you remove an instance, all assets that are associated with the deleted instance are no longer protected. You can still recover existing backup images, but backups of the instance fail.

Manually add a SQL Server instance

Newly discovered SQL Server instances are automatically displayed. However, you may not want to wait for the discovery service to discover a new instance. In this case you can add an instance manually.

To manually add a SQL Server instance

- 1 On the left, click SQL Server, then click the **Instances** tab.
- 2 Click **Add**.
- 3 Provide the **Host** name where the instance resides and the **Instance name**.
 - For a SQL Server cluster, the host name is the virtual name of the SQL Server cluster. You do not need to add each node in the cluster.
 - For a multi-NIC environment, the host name is the private interface name of the SQL Server host or of the virtual SQL Server.
 - For a failover cluster instance, enter the virtual name of the SQL Server cluster.
NetBackup enumerates the FCI under the physical node names and the cluster name.
- 4 Click **Next**.
- 5 Review the roles that have access to the instance. Click **Add** to give additional roles access to the instance.
- 6 Click **Manage credentials** to add the credentials for this instance.
See [“Add credentials to SQL Server instances or replicas”](#) on page 30.
You may omit credentials at this time. The instance is marked as unregistered and the **Registered** column is empty.
- 7 Click **Finish**.

Managing protection plans for SQL Server

This chapter includes the following topics:

- [About protecting SQL Server availability groups](#)
- [Create a protection plan to protect SQL Server assets](#)
- [Protect a SQL Server availability group that crosses NetBackup domains](#)

About protecting SQL Server availability groups

NetBackup for SQL Server supports backups and restores of SQL Server Always On and read-scale availability groups. For information on supported versions and environments, see the [Application/Database Agent Compatibility List](#).

You can protect an availability group environment in the following ways:

- With a protection plan that protects the preferred or the primary replica.
- If an availability group crosses multiple NetBackup domains, you can use Auto Image Replication (A.I.R.) to replicate the backup to the other NetBackup domains.
See [“Protect a SQL Server availability group that crosses NetBackup domains”](#) on page 43.

Note the following before you configure the protection plan:

- NetBackup can only fully protect the availability group environment if each replica on which backups occur is registered with credentials.
- NetBackup runs a backup job on each replica in the availability group. On the replicas which are not the backup source, the job skips the backup.

Limitations

Note the following limitations for backups of availability groups:

- NetBackup does not support the following types of backups for availability databases:
 - Backups of filegroups or files
 - VMware backups
 - A grouped snapshot backup
 - Backups of non-readable secondary replicas
 NetBackup can only back up databases in a replica when you allow user connections for the replica.
 If a secondary replica is the preferred replica and it is non-readable, the backup fails. If a secondary replica is not the preferred replica, NetBackup skips the backup of that replica.

SQL Server does not support the following types of backups on a secondary replica:

- Full backups
 If a full backup takes place on a secondary replica, NetBackup converts the full backup to a copy-only backup.
- Differential backups
 Backups of this type result in a failed backup.
- Copy-only transaction log backups
 Backups of this type result in a failed backup.

Create a protection plan to protect SQL Server assets

You can create a protection plan to perform scheduled backups of SQL Server assets.

To create a protection plan to protect SQL Server assets

- 1 On the left, click **Protection > Protection plans** and then click **Add**.
- 2 In **Basic properties**, enter a **Name**, **Description**, and select **Microsoft SQL Server** from the **Workload** list.
 (Optional) Add a policy name prefix. A prefix is appended to the policy name when NetBackup automatically creates a policy when users subscribe assets to this protection plan.

3 In **Schedules and retention**, click **Add**.

You can the frequency and the retention backup. You can set up the following backup schedules: **Full**, **Differential incremental**, or **Transaction log**.

In the **Attributes** tab:

- Select the **Backup type**, how often it runs, and how long to keep the backup for this schedule.

In the **Start window** tab:

- Define a **Start day**, **Start time**, **End day**, and **End time** for this schedule using the options available on the screen. Or you can drag your cursor over the time boxes to create the schedule.
- Use the options on the right to duplicate, remove, or undo changes to a schedule.

Click **Save** after all options are selected in the **Attributes** and the **Start window** tabs.

Review the **Backup schedule preview** window and verify that all schedules are set correctly.

- 4 In **Storage options**, configure the storage type per schedule you configured in step 3.

The options vary depending on storage options currently setup to work with NetBackup.

A protection plan can only use the storage that a NetBackup 8.1.2 or newer media server can access.

Storage option	Requirements	Description
Perform snapshot backups		<p>Performs a point-in-time, read-only, disk-based copy of a client volume. NetBackup backs up data from the snapshot, not directly from the client's primary or original volume. Snapshots cannot be used to perform differential backups or transaction log backups. In those cases NetBackup performs a stream-based backup.</p> <p>You can select from the following methods: Automatic, VxVM, or VSS. See "Snapshot methods" on page 42.</p> <p>Note that SQL Server dynamic file allocation can reduce the likelihood that any of the component files contain large areas of empty space. Also see the NetBackup for Microsoft SQL Server Administrator's Guide for details on the factors that can influence backup performance.</p>
Backup storage	OpenStorage is required for this option. Tape, storage unit groups, and Replication Director not supported.	Click Edit to select the storage target. Click Use selected storage after selecting the storage target.
Transaction log options		When you configure a transaction log schedule, you can choose to use the same storage that is used for database backups. Or, you can choose unique storage for transaction logs.

- 5 In **Backup options**, configure the options that you want.

Note: For availability groups, ensure that you select a **Availability database backup preference** setting for databases and for transaction logs.

See "[Performance tuning and configuration options](#)" on page 38.
- 6 In **Permissions**, review the roles that have access to the protection plan.

To give another role access to this protection plan, click **Add**. Select the **Role** in the table and customize the role by adding or removing permissions in the **Select permissions** section.
- 7 In **Review**, verify that the protection plan details are correct and click **Save**.

Schedules and retention

When you have the necessary RBAC permissions, you can adjust the following settings when you subscribe an asset to a protection plan.

Table 6-1

Option	Description
Recurrence (frequency)	Note: This setting can only be edited for SQL Server transaction log schedules. How frequently or when to run the backup.
Keep for (retention)	Note: This setting can only be edited for SQL Server transaction log schedules. How long to keep the files that were backed up by the schedule.
Start window	Set the window during which a backup can start.

Performance tuning and configuration options

When you have the necessary RBAC permissions, you can adjust the following settings when you subscribe an asset to a protection plan.

Table 6-2 Performance tuning and configuration options

Field	Description
Client buffers per stripe	(Stream-based backups only) This option affects buffer space availability. NetBackup uses this parameter to decide how many buffers to allocate for reading or writing each data stream during a backup operation. By allocating a greater number of buffers, you can affect how quickly NetBackup can send data to the NetBackup primary server. The default value for this option is 2, which allows double buffering. You may get slightly better performance by increasing this value to a higher value. Range is 1–32.
Maximum transfer size	(Stream-based backups only) This option is the buffer size used by SQL Server for reading and writing backup images. Generally, you can get better SQL Server performance by using a larger value. This option can be set for each backup operation. Calculated as 64 KB * 2 ^{MAX_TRANSFER_SIZE} . It ranges in size from 64 KB to 4 MB. The default is 4 MB.
Parallel backup operations	This option is the number of backup operations to start simultaneously, per database instance. Range is 1–32. The default is 1.

Table 6-2 Performance tuning and configuration options (*continued*)

Field	Description
VDI timeout (seconds)	<p>Determines the time-out interval for SQL Server Virtual Device Interface. The selected interval is applied to backups and restores of databases and of transaction logs.</p> <p>The default value for backups is 300. The default value for restore jobs is 600. Range is 300–2147483647.</p>
Use Microsoft SQL Server compression	<p>Enable this option to use SQL Server to compress the backup image. If you enable SQL Server compression, do not enable NetBackup compression.</p> <p>SQL Server compression is not supported for snapshot backups.</p>
Skip unavailable (offline, restoring, etc.) databases	<p>NetBackup skips any database with a status that prevents NetBackup from successfully backing up the database. These statuses include offline, restoring, recovering, and emergency mode, etc.</p> <p>NetBackup skips the backup of the unavailable database, but continues with the backup of the other databases that are subscribed to the protection plan. The backup completes with a status 0 and the job details indicate that the database was skipped.</p>
Create copy-only backup	<p>This option allows SQL Server to create an out-of-band backup so that it does not interfere with the normal backup sequence.</p> <p>See “Using copy-only snapshot backups to affect how differentials are based” on page 41.</p>
Perform Microsoft SQL Server checksum	<p>Choose one of the following options for SQL Server backup checksums:</p> <ul style="list-style-type: none"> ■ None. Disables the backup checksums. ■ To verify the checksums before the backup, choose one of the following options. Note that these options impose a performance penalty on a backup or restore operation. <ul style="list-style-type: none"> ■ Continue on error. If the backup encounters a verification error, the backup continues. ■ Fail on error. If the backup encounters a verification error, the backup stops.

Table 6-2 Performance tuning and configuration options (*continued*)

Field	Description
<p>Convert incremental backup to full backup</p>	<p>If no previous full backup exists for the database, then NetBackup converts a differential backup to a full backup.</p> <p>The agent determines if a full backup exists for each database. If no previous full backup exists, a differential backup is converted to a full as follows:</p> <ul style="list-style-type: none"> ■ If you select a database for a differential backup, the backup is converted to a full database backup. ■ For snapshot backup policies, a Full schedule must exist to successfully convert differential backups to full backups. <p>Note: NetBackup only converts a differential backup if a full backup was never performed on the database. If a full backup does not exist in the NetBackup catalog but SQL Server detects an existing full LSN, NetBackup performs a differential backup and not a full. In this situation, you can restore the full backup with native tools and any differentials with the NetBackup MS SQL Client. Or, if you expired the backup in NetBackup, you can import the full backups into the NetBackup catalog. Then you can restore both the full and the differential backups with the NetBackup MS SQL Client.</p>
<p>Convert transaction log backup to full backup</p>	<p>If no previous full backup exists for the database, then NetBackup converts a transaction backup to a full backup.</p> <p>This option also detects if a full recovery database was switched to the simple recovery model and back to the full recovery model. In this scenario, the log chain is broken and SQL Server requires a differential backup before a subsequent log backup can be created. If NetBackup detects this situation, the backup is converted to a differential database backup.</p> <p>Note: NetBackup only converts a transaction log backup if a full backup was never performed on the database. If a full backup does not exist in the NetBackup catalog but SQL Server detects an existing full LSN, NetBackup performs a transaction log backup and not a full. In this situation, you can restore the full backup with native tools and any differentials and log backups with the NetBackup MS SQL Client. Or, if the backup is expired, you can import the full backups into the NetBackup catalog. Then you can restore the full, differential, and log backups with the NetBackup MS SQL Client.</p>

Table 6-2 Performance tuning and configuration options (*continued*)

Field	Description
Availability database backup preference	<p>This option determines where backups of availability groups occur. Ensure that you select a setting for databases and a setting for transaction logs.</p> <ul style="list-style-type: none"> ■ None Perform the backup on the specified instance. Use this option when you intend to protect individual availability databases. Note: Do not select this option if you intend to protect availability groups. ■ Protect primary replica Backups always occur on the primary replica. This option applies to availability replicas and to instances that have both standard databases and availability databases. ■ Protect preferred replica Honors your SQL Server backup preferences. These preferences include the preferred replica, backup priority, and excluded replicas. Note that NetBackup initiates a backup job on each replica. The backup is skipped on any replica that isn't the intended backup source. This option applies to availability replicas and to instances that have both standard databases and availability databases. ■ Skip availability databases Skips any availability databases on the instance. Use this option when you intend to protect any instances that contain both standalone databases and availability databases and only want to protect the standalone databases. Note: Do not select this option if you intend to protect availability groups. <p>Backup preference for individual availability databases</p> <p>Note the following behavior when you select a protection plan to protect individual availability databases.</p> <ul style="list-style-type: none"> ■ If the preference for Databases is set to Skip availability databases, scheduled backups cannot succeed. Databases must have the setting None, Protect preferred replica, or Protect primary replica. ■ When a user selects Backup now to back up an availability database, the backup is performed on the selected node. The image is cataloged under the cluster name.
Truncate logs after backup	<p>This option backs up the active part of the transaction log and then marks it inactive or empty. This option is enabled by default.</p>

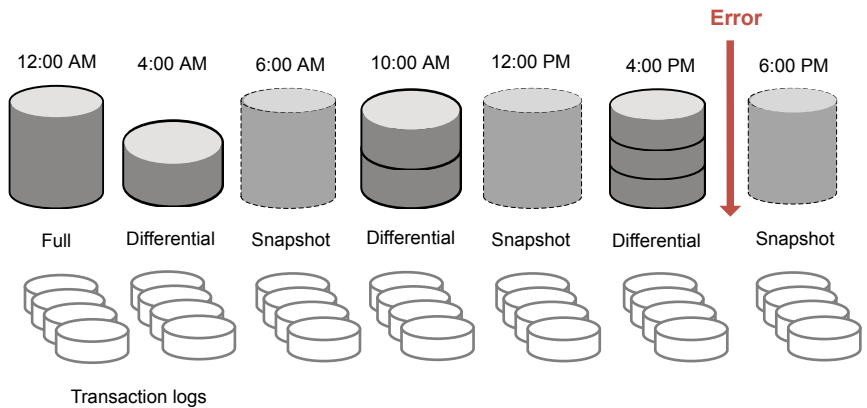
Using copy-only snapshot backups to affect how differentials are based

When you use both full backups and snapshot backups to protect SQL Server, the previous snapshot backup expires after the next snapshot backup is created. If you

require a point in time restore before the latest backup, the differentials are based on a snapshot backup that no longer exists. Alternatively, NetBackup lets you create copy-only backups that are out-of-band so the backup does not reset the differential baseline. Differential backups are then based on the last full backup.

If a failure occurs and is detected immediately, you can restore the last full backup. Then you can replay the necessary transaction logs to achieve recovery. However, if a failure is not detected until after the next full backup, then there are no snapshot backups available to restore. When you use copy-only backups, each differential is instead based on the last full backup that is not copy-only. You can restore the last full backup, restore the latest differential backup, then restore the necessary transaction log backups before the error occurred.

Figure 6-1 Recovering after an error when using full and copy-only backups



Snapshot methods

The following snapshot methods and options are available for snapshot backups. For more details see the [NetBackup Snapshot Client Administrator's Guide](#).

Table 6-3

Method	Description
Automatic	NetBackup selects a snapshot method when the backup starts. If necessary, NetBackup selects a different method for assets in the protection plan.

Table 6-3 (continued)

Method	Description
VSS	<p>VSS uses the Volume Shadow Copy Service of Windows. VSS is for local backup and it selects the actual snapshot method depending on which snapshot provider is configured on the client.</p> <p>Provider type:</p> <ul style="list-style-type: none"> ■ Automatic. NetBackup selects the available provider in this order: Hardware, Software, System. ■ System. Use the Microsoft system provider for a block-level copy on write snapshot. ■ Use the software provider to intercept the I/O requests at the software level between the file system and the volume manager. ■ Use the hardware provider for your disk array. <p>Snapshot attribute:</p> <ul style="list-style-type: none"> ■ Automatic. NetBackup selects the attribute. ■ Differential. Use a copy-on-write type of snapshot. ■ Plex. Use a clone or a mirror type of snapshot.
VxVM	<p>For any snapshots with any data that is configured over Volume Manager volumes.</p> <ul style="list-style-type: none"> ■ Resynchronize mirror in background. Select this option to allow more efficient use of backup resources. If two backups need the same tape drive, the second can start even though the resynchronize operation for the first job has not completed. ■ Wait for mirror sync completion. Select this option if full-sized instant snapshots are not available for backup until the mirror synchronization is complete. If the backup starts before the snapshot disks are fully synchronized with the source and the server does not have access to the source disks, then the backup fails. ■ Maximum number of volumes to resynchronize. The number of volume pairs that are resynchronized simultaneously. Accept the default if the I/O bandwidth in your clients and disk storage cannot support simultaneous synchronization of volumes. For the configurations that have sufficient I/O bandwidth, multiple volumes can be resynchronized simultaneously, to complete resynchronization sooner. A major factor in I/O bandwidth is the number and speed of HBAs on each client.

Protect a SQL Server availability group that crosses NetBackup domains

When you have an availability group that crosses NetBackup domains, you can use Auto Image Replication (A.I.R.) to replicate backup images to another NetBackup domain. The following configuration requirements exist:

- Configure the storage in the NetBackup source and target domains:
 - For OpenStorage, a disk appliance of the same type in each domain. The disk appliance type must support NetBackup Auto Image Replication (A.I.R.).

- For NetBackup deduplication, the storage that NetBackup can use for a Media Server Deduplication Pool in each domain.
- Configure the domain where the backups occur as the source domain. Then configure the domain where you want to restore the backups as the target domain.

To create a protection plan to protect a SQL Server availability group that crosses domains

- 1** On the left, click **Protection > Protection plans** and then click **Add**.
- 2** In **Basic properties**, enter a **Name** and **Description**.
- 3** From the **Workload** list, select **Microsoft SQL Server**.
- 4** In **Schedules and retention**, click **Add**.

You can set up a full, differential, or transaction log backup.

In the **Attributes** tab:

- Select the **Backup type**, how often it runs, and how long to keep the backup for this schedule.
- Select **Replicate this backup**.
 - The backup storage must be a source in a targeted A.I.R. environment. The **Replication target** is configured in step 5.
 - For more information about replication, review *About NetBackup Auto Image Replication* in the [NetBackup Administrator's Guide, Volume I](#).

In the **Start window** tab:

- Define a start window for this schedule using the options available on the screen. You can add multiple schedule windows for this schedule if needed.

Review the **Backup schedule preview** and verify that all schedules are set correctly.

- 5** In **Storage options**, configure the storage type per schedule you configured in step 5.

A protection plan can only use the storage that a NetBackup 8.1.2 or newer media server can access.

Storage option	Requirements	Description
Backup storage	OpenStorage is required for this option. Tape, storage unit groups, and Replication Director not supported.	Click Edit to select the storage target. Click Use selected storage after selecting the storage target.
Replication target	The backup storage must be a source in a targeted A.I.R. environment.	Click Edit to select the replication target master server. Select a master server and then select a storage lifecycle policy. Click Use selected replication target to return to the storage options screen.

- 6** In **Backup options**, select the options that you want.

From the **Availability database backup preference** list, choose one of the following:

- **Protect primary replica**
- **Protect preferred replica**

See “[Performance tuning and configuration options](#)” on page 38.

(Optional) Make any other changes to the tuning parameters.

- 7** In **Permissions**, review the roles that have access to this protection plan.
- 8** In **Review**, verify that the protection plan details are correct and click **Finish**.

Additional resources

[NetBackup Administrator’s Guide, Volume I](#)

[NetBackup Deduplication Guide](#)

[NetBackup OpenStorage Solutions Guide](#)

<http://www.netbackup.com/compatibility>

Protecting SQL Server

This chapter includes the following topics:

- [Add SQL Server assets to a protection plan](#)
- [Edit protection settings for a Microsoft SQL Server asset](#)
- [View the protection status of databases, instances, or availability groups](#)
- [Remove protection from SQL Server assets](#)

Add SQL Server assets to a protection plan

The following procedure describes how to subscribe an SQL Server asset to a protection plan. When you subscribe an asset to a protection plan, you assign predefined backup settings to the asset.

Note the following:

- For backups to be successful, a SQL Server instance or replica must have a valid credential configured for it in **Instances** tab.
See [“Add credentials to SQL Server instances or replicas”](#) on page 30.
- Your user account is assigned to the RBAC role **Default Microsoft SQL Server** or another role with the same permissions for protection plans and for SQL Server.
See [Default RBAC roles](#) and [RBAC permissions](#) in the [NetBackup Web UI Administrator’s Guide](#). Or, contact your NetBackup administrator for assistance.
- Ensure other requirements are met for the NetBackup environment and for non-administrator users.
See [“Configuring SQL Server hosts and user permissions”](#) on page 17.
- Databases only appear on the **Databases** tabs if they meet one of the following criteria: A backup exists of the database, the database instance has validated credentials, or a manual discovery of databases was performed.

To add SQL Server assets to a protection plan

- 1 On the left, click **Workloads > Microsoft SQL Server**.
- 2 Choose the asset or assets that you want to protect.

- | | |
|--|--|
| All the databases in an instance | <ul style="list-style-type: none"> ■ On the Instances tab, select the box for the instance that you want to protect. |
| An individual database | <ul style="list-style-type: none"> ■ On the Instances tab, click on the instance that contains the database you want to protect. ■ On the Databases tab, click the box for one or more databases. |
| An availability group | <ul style="list-style-type: none"> ■ On the Availability groups tab click the box for the availability group name. |
| An individual availability database | <ul style="list-style-type: none"> ■ On the Availability groups tab click on the availability group name that contains the database that you want to protect. ■ On the Databases tab, click the box for one or more databases. |
| A SQL Server cluster | <ul style="list-style-type: none"> ■ On the Instances tab, select the box for the instance that belongs to the cluster.
The Host name is the virtual name of the SQL Server cluster. |
| A SQL Server failover cluster instance (FCI) | <p>On the Instances tab, select the instance name depending on if you want to protect the cluster or a node in the cluster:</p> <ul style="list-style-type: none"> ■ The instance name, where the Host name is the cluster name of the FCI.
The backup is attempted on the active node. Both nodes must be hosts of the same primary server and the instances must have valid credentials registered. ■ The instance name, where the Host name is one of the physical node names of the FCI.
For the backup to succeed, this node must be the active node in the cluster. The backup is cataloged under the cluster name. |

A SQL Server host that uses multiple NICs On the **Instances** tab, select the instance:

- The instance name, where the **Host** name is the private interface name of the SQL Server host.
- The instance name for a SQL Server cluster that uses multiple NICs, where the **Host** name is the private interface name of the virtual SQL Server.

3 Click **Add protection**.

4 Select a protection plan and click **Next**.

- For a snapshot backup, look for a protection plan that lists **Snapshot options** and a **Snapshot method**.
See “[Snapshot methods](#)” on page 42.
- For an availability group, select a protection plan that has a configured **Availability database backup preference**, either **Protect primary replica** or **Protect preferred replica**.
Do not subscribe an availability group to a protection plan that has a setting of **None** or **Skip availability databases**.

5 If you have the necessary role permissions you can adjust one or more of the following settings:

- **Schedules and retention**
Change the backup start window. For transaction log schedules, you can also edit the frequency and the retention.
See “[Schedules and retention](#)” on page 38.
- **Backup options and Configuration options**
Adjust the performance tuning options or change or enable any options for the protection plan.
See “[Performance tuning and configuration options](#)” on page 38.

6 Click **Protect**.

The results of your choices appear under **Instances** or **Databases**.

Edit protection settings for a Microsoft SQL Server asset

If you have the necessary role permissions, you can edit certain settings for a protection plan, including schedules and other options.

- See “[Schedules and retention](#)” on page 38.

View the protection status of databases, instances, or availability groups

- See [“Performance tuning and configuration options”](#) on page 38.

To edit protection settings for a Microsoft SQL Server asset

- 1 On the left, click **Workloads > Microsoft SQL Server**.
- 2 Do one of the following:

Edit the settings for an instance	■ On the Instances tab, click on the instance that you want to edit.
Edit the settings for a database	■ On the Databases tab, click on the database that you want to edit.
Edit the settings for an availability group	■ On the Availability groups tab, click on the availability group that you want to edit.
Edit the settings for an availability database	■ On the Databases tab, click on the database that you want to edit.
- 3 Click **Customize protection > Continue**.
- 4 If you have the necessary role permissions you can adjust one or more of the following settings:
 - **Schedules and retention**
Change the backup start window.
For transaction log schedules, you can also edit the frequency and the retention.
See [“Schedules and retention”](#) on page 38.
 - **Backup options and Configuration options**
Adjust the performance tuning options or change or enable any options for the protection plan.
See [“Performance tuning and configuration options”](#) on page 38.
- 5 Click **Protect**.

View the protection status of databases, instances, or availability groups

You can view the protections plans that are used to protect instances or availability groups.

To view the protection status of databases, instances, or availability groups

- 1 On the left, click **Workloads > Microsoft SQL Server**.
- 2 Click on one of the following tabs: **Databases, Instances, or Availability groups**.
- 3 The **Protected by** column indicates how the asset is protected.

Table 7-1 Protection status of SQL Server assets

Protection type or status	Protected by column	
	Database	Instance or availability group
Asset is protected by a classic policy	Classic policy	Not protected Use the NetBackup Administration Console to see how classic policies are used to protect instances or availability groups.
Asset is protected by a protection plan	Protected	Protected
Asset is not protected by plan or a policy	Not protected	Not protected
A policy or protection plan protects the asset, but it is not backed up yet (no backup image exists).	Not protected Protected by column is blank.	Not protected

Remove protection from SQL Server assets

You can unsubscribe databases, instances, or availability groups from a protection plan. When the asset is unsubscribed, backups are no longer performed.

Note: When you unsubscribe an asset from a protection plan, there is a possibility that the asset displays **Classic policy** in the web UI. This situation can happen when an asset is subscribed to a protection plan and a backup runs for that asset. Then the asset is unsubscribed from the protection plan while it has a valid backup image. The web UI displays **Classic policy**, but there may or may not be an active policy protecting the asset.

To remove protection from an instance

- 1 On the left, click **Workloads > Microsoft SQL Server**.
- 2 Select the asset that you want to unsubscribe.

- Remove protection from an instance
 - On the **Instances** tab, click on the instance that you want to edit.
- Remove protection from a database
 - On the **Databases** tab, click on the database that you want to edit.
- Remove protection from an availability group
 - On the **Availability groups** tab, click on the availability group that you want to edit.
- Remove protection from an availability database
 - On the **Databases** tab, click on the database that you want to edit.

3 Click **Remove protection > Yes**.

The asset is listed as **Not protected**.

Restoring SQL Server

This chapter includes the following topics:

- [Requirements for restores of SQL Server](#)
- [Perform a complete database recovery](#)
- [Recover a single recovery point](#)
- [Options for SQL Server restores](#)
- [Restore a database \(non-administrator users\)](#)
- [Select a different backup copy for recovery](#)
- [Restore a SQL Server availability database to a secondary replica](#)
- [Restore a SQL Server availability database to the primary and the secondary replicas](#)

Requirements for restores of SQL Server

To restore perform restores of SQL Server, the following requirements exist:

- NetBackup services are correctly configured.
See [“Configuring SQL Server hosts and user permissions”](#) on page 17.
- Both administrators or non-administrators can perform restores. However, additional configuration steps are required for non-administrators.
Administrators must provide during the restore a user account that is a member of the Windows administrator group and a member of the local SQL Server sysadmin role.
Non-administrators must follow these additional steps for successful recovery:
See [“Restore a database \(non-administrator users\)”](#) on page 60.

- The user that signs into the NetBackup web UI is assigned to the RBAC role **Default Microsoft SQL Server Administrator** or another role with the same restore permissions for SQL Server.
See [Default RBAC roles](#) and [RBAC permissions](#) in the [NetBackup Web UI Administrator's Guide](#). Or, contact your NetBackup administrator for assistance.
- The security administrator has configured the necessary mappings for the hosts in **Security > Hosts**.
Refer to the information on [configuring host mappings](#) in the [NetBackup Web UI Administrator's Guide](#). Or, contact your NetBackup administrator for assistance.
- To restore to a different server (host), the following requirements and conditions exist:
 - NetBackup must have the ability to communicate with the destination client.
 - Non-administrator users can only perform restores from their own backups.

Perform a complete database recovery

A complete database recovery selects all the backup images that are necessary to restore the complete database and leaves the database in the recovered state, or ready to use.

To perform a complete database recovery

- 1 On the left, select **Workloads > Microsoft SQL Server**.
- 2 On the **Databases** tab, locate the database that you want to restore.

The **Host** name for the database differs depending on how the instance or the host is protected.

A database that is part of a SQL Server cluster

The **Host** name is the virtual name of the SQL Server cluster.

A database that is part of a SQL Server failover cluster instance (FCI)

The **Host** name is one of the following:

- The cluster name of the FCI
- The physical node names of the FCI

A SQL Server host that uses multiple NICs

The **Host** name is one of the following:

- The private interface name of the SQL Server host
- The the private interface name of the virtual SQL Server

3 Click **Actions > Recover**.

4 On the **Recovery points** tab, locate the full, differential, or transaction log image that you want to restore.

By default NetBackup uses the primary copy. To select a different copy, click **Copies**.

See “[Select a different backup copy for recovery](#)” on page 61.

5 Click **Actions > Perform complete database recovery**.

6 (Conditional) For a transaction log, select one of the following options.

Recovery point selected

Restore the database to the time indicated.

Point in time

Select a different point in time to which you want to restore the database.

Transaction log mark

- Choose whether to restore at or before the transaction mark.
- Enter the name of the transaction mark.
- To select a transaction mark that occurs after a certain date, select **After specific date and time**. Then specify the date and time.
- Click **Next**.

7 Select the host, instance, and database for recovery. You have the following options.

Restore to the original host, instance, and database.

Restore to a different instance.

Type the name in the **Instance** field.

Select a different host and instance,

Click **Change instance**.

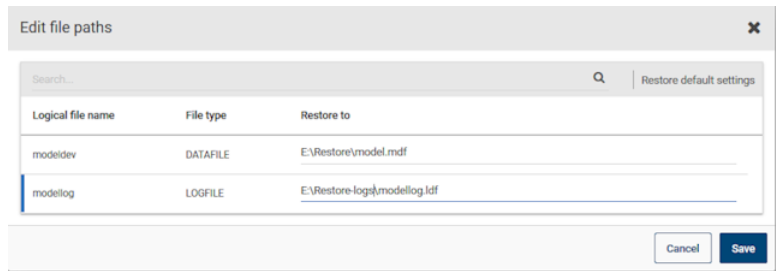
Restore to a different database.

Type the name in the **Database name** field.

8 Select the path to which you want to restore the database files. You have the following options:

- | | |
|--|--|
| Restore everything to the original directory | Restores all the files to the original directory that was backed up. |
| Restore everything to a different directory | Restores all the files to the directory that you enter in the Directory for restore field. |
| Restore files to different paths | Restores the individual files to the path that you enter. Click Edit file paths and click on any directory path to edit the restore path for that file. |

Example of a restore to different paths:



- 9** Enter the credentials of the instance that you want to restore to and click **Next**.
 The user account must be a member of the Windows administrator group and a member of the local SQL Server sysadmin role.
- 10** Select the recovery options.
- For the **Database recovery state after restore**, select **Recover**.
 - Choose a **Consistency check** option to perform after the restore.
 - Select any other recovery options.
- See [“Options for SQL Server restores”](#) on page 59.
- 11** Click **Next**.
- 12** On the **Review** page, review the restore options that you selected.
- At the top, click on the link that follows **Recovery set** to view the backup images that are required for the restore.
 - Click **Edit** to change the **Recovery target** settings or **Recovery options**.
 - Click **Start recovery**.

Recover a single recovery point

Perform a recovery of a single recovery point when you want to restore backup images in separate restore operations.

To restore to a different server (host), the following requirements exist.

- RBAC permissions to restore to an alternate location.
Refer to the [NetBackup Web UI Administrator's guide](#). Or, contact your NetBackup administrator for assistance.
- NetBackup must have the ability to communicate with the destination client.

To recover a single recovery point

1 On the left, select **Workloads > Microsoft SQL Server**.

2 On the **Databases** tab, locate the database that you want to restore.

The **Host** name for the database differs depending on how the instance or the host is protected.

A database that is part of a SQL Server cluster

The **Host** name is the virtual name of the SQL Server cluster.

A database that is part of a SQL Server failover cluster instance (FCI)

The **Host** name is one of the following:

- The cluster name of the FCI
- The physical node names of the FCI

A SQL Server host that uses multiple NICs

The **Host** name is one of the following:

- The private interface name of the SQL Server host
- The the private interface name of the virtual SQL Server

3 Click **Actions > Recover**.

4 On the **Recovery points** tab, locate the full, differential, or transaction log that you want to restore.

By default NetBackup uses the primary copy. To select a different copy, click **Copies**.

See [“Select a different backup copy for recovery”](#) on page 61.

5 Select **Actions > Restore single recovery point**.

6 (Conditional) For a transaction log image, select one of the following options and click **Next**.

Recovery point selected	Restore the database to the time indicated.
Point in time	Select a different point in time to which you want to restore the database.
Transaction log mark	<ul style="list-style-type: none">■ Choose whether to restore at or before the transaction mark.■ Enter the name of the transaction mark.■ To select a transaction mark that occurs after a certain date, select After specific date and time. Then specify the date and time.

7 Select the host, instance, and database for recovery. You have the following options.

Restore to the original host, instance, and database.

Restore to a different instance. Type the name in the **Instance** field.

Select a different host and instance, Click **Change instance**.

Restore to a different database. Type the name in the **Database name** field.

- 8 Select the path to which you want to restore the database files. You have the following options:

Restore everything to the original directory

Restores all the files to the original directory that was backed up.

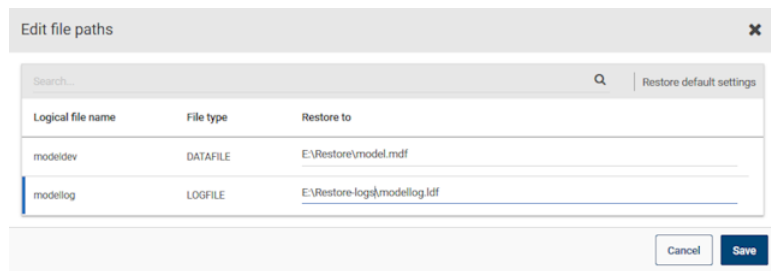
Restore everything to a different directory

Restores all the files to the directory that you enter in the **Directory for restore** field.

Restore files to different paths

Restores the individual files to the path that you enter. Click **Edit file paths** and click on any directory path to edit the restore path for that file.

Example of a restore to different paths:



- 9 Enter the credentials of the instance that you want to restore to and click **Next**.

The user account must be a member of the Windows administrator group and a member of the local SQL Server sysadmin role.

- 10 Select the recovery options.
 - Select the recovery state from the **Database recovery state after restore** options.
 - Select the other recovery options.
 - If you select the **Recover** option, choose a **Consistency check** option to perform after the restore.

See [“Options for SQL Server restores”](#) on page 59.

- 11 Click **Next**.

- 12 On the **Review** page, review the restore options that you selected.
 - At the top, click on the link that follows **Recovery set** to view the backup images that are required for the restore.

- Click **Edit** to change the **Recovery target** settings or **Recovery options**.
 - Click **Start recovery**.
- 13** When the restore completes, continue with the restore of differential incremental or transaction log backups.
- For each intermediate backup, for the **Database recovery state after restore** select **Restoring**.
 - For the final backup image, select **Recovered**.

Options for SQL Server restores

The following options exist when you perform restores of SQL Server.

Table 8-1 Recovery options

Option	Description
Verify backup image but do not restore	NetBackup processes the image for errors, but does not perform a restore. This option does not apply to snapshot images.
Database recovery state after restore	Select the state for the database after the restore. <ul style="list-style-type: none">■ Recover Restore the last image in a restore sequence and make the database ready for use.■ Restoring Restore an intermediate backup image. The database is left in a loading state so you can restore and apply additional backup images.■ Standby Create and maintain a standby during a transaction log and database restore. This option requires a standby undo log, which by default is placed in the same directory as the primary datafile. The account that runs the SQL Server service must have full access permission to the <code>SQLStandBy</code> folder.

Table 8-1 Recovery options (continued)

Option	Description
Consistency check	<p>The consistency check to perform after the restore. Output from the consistency check is written to the SQL Server client progress log.</p> <ul style="list-style-type: none"> ■ Do not perform Do not perform consistency checking. ■ Full check, including indexes Include indexes in the consistency check. Any errors are logged. ■ Full check, excluding indexes Exclude indexes from the consistency check. If indexes are not checked, the consistency check runs significantly faster but is not as thorough. Only the data pages and clustered index pages for each user table are included in the consistency check. The consistency of the non-clustered index pages is not checked. ■ Check catalog Check for consistency in and between system tables in the specified database. ■ Physical check only Perform a low overhead check of the physical consistency of the SQL Server database. This option only verifies the integrity of the physical structure of the page and the record headers. It also verifies the consistency between the pages' object ID and index ID and the allocation structures.
Overwrite the existing database	<p>Allows SQL Server to overwrite a database or any database files, if they already exist. If this operation is not available, contact your NetBackup administrator for the necessary RBAC permission.</p>
VDI timeout	<p>Determines the time out interval for SQL Server Virtual Device Interface. The selected interval is applied to backups and restores of databases and of transaction logs. The default value for backups is 300. The default value for restore operations is 600. Range is 300 - 2147483647.</p>

Restore a database (non-administrator users)

Non-administrators can perform restores of SQL Server. However, additional requirements and configuration steps are required.

The following requirements exist for a non-administrator:

- Is a member of the domain users group.
- Has the sysadmin role on the local SQL Server.
- Has full access control to the following:
 - `install_path\NetBackup\dbext\mssql` folder

- HKLM\SOFTWARE\ODBC registry hive
- *install_path*\NetBackup\logs\user_ops folder

Restore a database (non-administrator users)

- 1 Before you can perform a restore, you must do the following:
 - Add the non-administrator credentials to the SQL Server instance.
See [“Add credentials to SQL Server instances or replicas”](#) on page 30.
 - Perform a new backup of the database.
Locate the database and click **Action > Backup Now**.
- 2 When you perform the restore, provide the credentials that you used to register the instance.

Select a different backup copy for recovery

Beginning with NetBackup 9.1, the user can restore from the primary backup copy or choose from other available backup copies.

To select a different backup copy for recovery

- 1 Locate the full, differential, or transaction log that you want to restore.
- 2 Click **Copies** and locate the copy that you want.

In the example below, there is an additional copy for the transaction log on **Tape**.

April 30, 2021

Backup images/Recovery points	Backup type	
12:00 PM - 02:00 PM	1 Full, 1 Incremental, 6 Transaction log	
12:11:54 PM	Full	Copies > ⋮
12:26:41 PM	Incremental	Copies v ⋮
Storage	Storage server	Storage type
storage1 (Primary copy)	storageserver1	MSDP
storage2	storageserver1	AdvancedDisk
E:\storage3	storageserver1	
/storage4	storageserver2	

Perform complete database recovery

Recover single recovery point

- 3 You can then click the **Actions** menu for that copy to select the restore that you want to perform.


In this example, for the copy on **AdvancedDisk**, you can select either **Perform complete database recovery** or **Recover single recovery point**.

Edit the storage for recovery

In the example below, the **Recovery source** page of the recovery wizard displays the selected storage for recovery. If the images that are needed for recovery are not available on that storage, NetBackup automatically selects the primary images on the appropriate storage. You can change the storage if you don't want to use the automatic selections.

In this case, you selected a transaction log copy on AdvancedDisk storage. Because the full and incremental images were not available on the same storage, NetBackup automatically picked the copies on MSDP storage. You can click **Edit** to change the selected storage for the **Full** image.

Figure 8-1 Storage selected for recovery

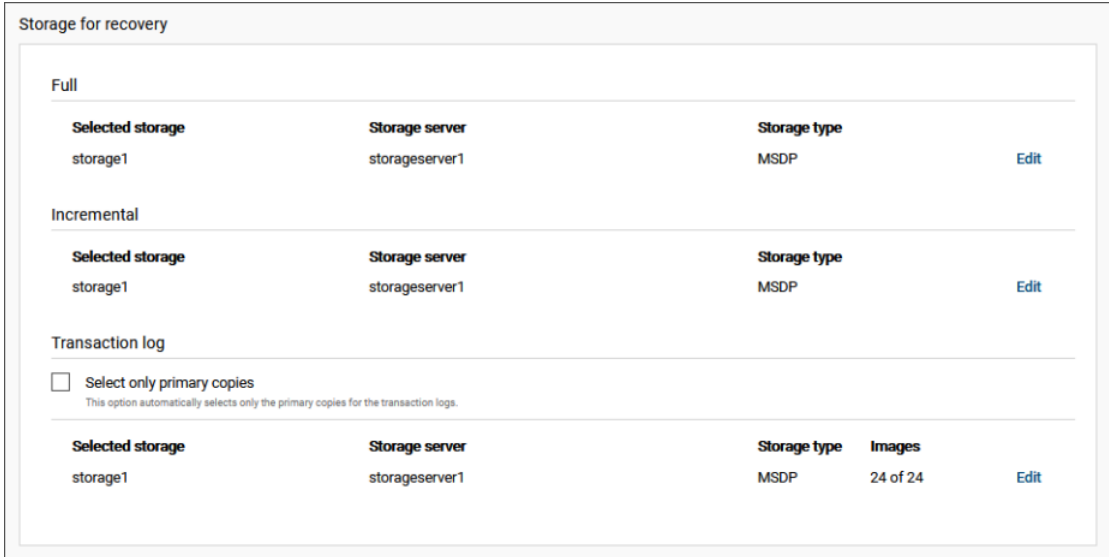
Storage for recovery			
Full			
Selected storage	Storage server	Storage type	
 storage1	storageserver1	MSDP	Edit
Incremental			
Selected storage	Storage server	Storage type	
storage2	storageserver2	AdvancedDisk	Edit

If you want to use only the primary copies for the recovery, click **Select only primary copies** (see [Figure 8-2](#)). Otherwise, you can click **Edit** to select the specific storage that you want to use (see [Figure 8-3](#)).

Figure 8-2 Select only primary copies of transaction logs

Storage for recovery			
Full			
Selected storage	Storage server	Storage type	
storage1	storageserver1	MSDP	Edit
Incremental			
Selected storage	Storage server	Storage type	
storage1	storageserver1	MSDP	Edit
Transaction log			
<input checked="" type="checkbox"/>	Select only primary copies This option automatically selects only the primary copies for the transaction logs.		
Selected storage	Storage server	Storage type	Images
storage1	storageserver1	MSDP	12 of 24
storage2	storageserver2	AdvancedDisk	12 of 24

Figure 8-3 Edit storage for transaction logs



Restore a SQL Server availability database to a secondary replica

This procedure describes how to restore a SQL Server availability database to a secondary replica. Follow this procedure if a secondary replica is unavailable for an extended time and needs to be synchronized with the primary. Or follow these instructions after you add a new secondary replica to the availability group.

To restore a SQL Server availability database to a secondary replica

- 1 Log on to the node that hosts the secondary replica and perform the following actions:
 - Close any connections to the database on the secondary replica.
 - Remove the secondary database from the availability group.
- 2 On the left, select **Workloads > Microsoft SQL Server**.
- 3 Click on the **Availability groups** tab and then click on the availability group name.
- 4 On the **Replicas** tab, click on the instance that is hosted on the secondary replica.

- 5 On the **Databases** tab, click on the database that you want to restore.
- 6 Click the **Recovery points** tab and locate the latest transaction log backup. By default NetBackup uses the primary copy. To select a different copy, click **Copies**.
See [“Select a different backup copy for recovery”](#) on page 61.
- 7 From the **Actions** menu select **Perform complete database recovery**.
- 8 Select one of the following options.

Recovery point selected	Restore the database to the time indicated.
Point in time	Select a different point in time to which you want to restore the database.
Transaction log mark	<ul style="list-style-type: none"> ■ Choose whether to restore at or before the transaction mark. ■ Enter the name of the transaction mark. ■ To select a transaction mark that occurs after a certain date, select After specific date and time. Then specify the date and time.

- 9 If the replicas in the availability group use different paths for the database file, select **Restore files to different paths** and edit the file path.
- 10 Enter the credentials of the instance that you want to restore to and click **Next**.
The user account must be a member of the Windows administrator group and a member of the local SQL Server sysadmin role.
- 11 Select the following settings:
 - **Restoring**
 - **Overwrite existing database**
 See [“Options for SQL Server restores”](#) on page 59.
- 12 Click **Next**. Then click **Start recovery**.
- 13 When the restore completes, join the database to the availability group.

Restore a SQL Server availability database to the primary and the secondary replicas

In some situations you may need to restore the SQL Server availability databases to both the primary and the secondary replicas. These situations can include when you restore databases:

- Following a disaster recovery
- After logical corruption of the databases
- To a clone of an availability group or test environment
- To an earlier point in time

You may want to perform this restore for the primary database in parallel with the restores for the secondary databases.

To restore a SQL Server availability database to the primary and the secondary replicas

- 1 Log on to the host of the primary replica and perform the following actions:
 - In SQL Server Management Studio, suspend data movement on the database and remove the database from the availability group.
 - Close any connections to the database.
 - Remove the primary database from SQL Server.
- 2 In the NetBackup web UI, on the left select **Workloads > Microsoft SQL Server**.
- 3 Click on the **Availability groups** tab and then click on the availability group name.
- 4 On the **Replicas** tab, click on the instance that is hosted on the primary replica.
- 5 On the **Databases** tab, click on the database that you want to restore.
- 6 Click the **Recovery points** tab and locate the latest transaction log backup. By default NetBackup uses the primary copy. To select a different copy, click **Copies**.
See [“Select a different backup copy for recovery”](#) on page 61.
- 7 From the **Actions** menu select **Perform complete database recovery**.
- 8 Select one of the following options.

Recovery point selected

Restore the database to the time indicated.

Restore a SQL Server availability database to the primary and the secondary replicas

Point in time	Select a different point in time to which you want to restore the database.
Transaction log mark	<ul style="list-style-type: none"> ■ Choose whether to restore at or before the transaction mark. ■ Enter the name of the transaction mark. ■ To select a transaction mark that occurs after a certain date, select After specific date and time. Then specify the date and time.

- 9 Enter the credentials of the instance that you want to restore to and click **Next**.
The user account must be a member of the Windows administrator group and a member of the local SQL Server sysadmin role.
- 10 Select the following settings:
 - **Recover**
 - **Overwrite existing database**
 See [“Options for SQL Server restores”](#) on page 59.
- 11 Click **Next**. Then click **Start recovery**.
- 12 When the restore completes, add the database to the availability group using the **Skip initial data synchronization** option.
- 13 Log on to the host of the secondary replica and complete the following steps:
 - Close any connections to the database on the secondary replica.
 - Remove the secondary database from SQL Server.
- 14 In the NetBackup web UI, on the left select **Workloads > Microsoft SQL Server**.
- 15 Click on the **Availability groups** tab and then click on the availability group name.
- 16 On the **Replicas** tab, click on the instance that is hosted on the secondary replica.
- 17 On the **Databases** tab, click on the database that you want to restore.
- 18 Click the **Recovery points** tab and locate the image that you restored to the primary replica.
- 19 From the **Actions** menu select **Perform complete database recovery**.
- 20 For the transaction log, select the same point in time or log mark that you did for the primary replica.

Restore a SQL Server availability database to the primary and the secondary replicas

- 21** Enter the credentials of the instance that you want to restore to and click **Next**.
The user account must be a member of the Windows administrator group and a member of the local SQL Server sysadmin role.
- 22** Select the following settings:
 - **Restoring**
 - **Overwrite existing database**See [“Options for SQL Server restores”](#) on page 59.
- 23** Click **Next**. Then click **Start recovery**.
- 24** When the restore completes, join the database to the availability group.
- 25** Repeat step [13](#) through step [24](#) for additional replicas in the availability group.

Using instant access with SQL Server

This chapter includes the following topics:

- [Prerequisites when you configure an instant access SQL Server database](#)
- [Things to consider before you configure an instant access database](#)
- [Configure Samba users for SQL Server instant access](#)
- [Configure an instant access database](#)
- [View the livemount details of an instant access database](#)
- [Delete an instant access database](#)
- [Options for NetBackup for SQL Server instant access](#)
- [NetBackup for SQL Server terms](#)
- [Frequently asked questions](#)

Prerequisites when you configure an instant access SQL Server database

The prerequisites are only applicable to Microsoft SQL Server instant access Build Your Own (BYO).

Prerequisites:

- The BYO server operating system version must be same as the latest appliance operating system version that is RHEL 7.6 and RHEL 7.7.

Prerequisites when you configure an instant access SQL Server database

- - Ensure that the Samba service is installed and the Samba share permission is allowed in the selinux policy using the following command

```
setsebool -P samba_export_all_rw=1
```
- The storage server with NGINX installed.
 - The NGINX version must be same as the one in the corresponding official RHEL version release. You need to install it from the corresponding RHEL yum source (epel).
 - Ensure that the `policycoreutils` and `policycoreutils-python` packages are installed from the same RHEL yum source (rhel server). Then run the following commands:
 - ```
semanage port -a -t http_port_t -p tcp 10087
```
    - ```
setsebool -P httpd_can_network_connect 1
```
- Ensure that the `/mnt` folder on the storage server is not mounted by any mount points directly. User mount points should be mounted to its subfolders.
- Enable the logrotate permission in selinux using the following command:

```
semanage permissive -a logrotate_t
```
- Instant access is only supported for SQL Server backup images when the following conditions are met:
 - Snapshots are enabled in the policy or the protection plan.
 - The backup is a full database backup.
 - The primary server, media server, storage server, and client must be at version 8.3 or later.
 - The storage server must be an appliance or BYO that meets the earlier specified prerequisites.

Note: Instant access for incremental and transaction log backups depends on the instant access capability of its base backup image.

Hardware configuration requirement of instant access

Table 9-1 Hardware configuration requirement

CPU	Memory	Disk
<ul style="list-style-type: none"> ■ Minimum 2.2-GHz clock rate. ■ 64-bit processor. ■ Minimum 4 cores; 8 cores recommended. For 64 TBs of storage, the Intel x86-64 architecture requires eight cores. 	<ul style="list-style-type: none"> ■ 16 GB (For 8 TBs to 32 TBs of storage) 1GB RAM for 1TB of storage. ■ 32 GBs of RAM for more than 32 TBs storage. ■ An additional 500MB of RAM for each live mount. 	<p>Disk size depends on the size of your backup. Refer to the hardware requirements for NetBackup and Media Server Deduplication Pool (MSDP).</p>

Things to consider before you configure an instant access database

Note the following about the instant access SQL Server feature:

- The SQL Server backup with the following backup options or scenarios does not support SQL Server instant access:
 - Application-aware backups (VMware)
 - Stream-based backups
 - NetBackup backup compression
 - Legacy SQL Server backups (with batch files)
 - File group or file backups
 - PFI backups (backup option: **Retain snapshot for Instant Recovery or SLP management**)
 - SQL Server database mirroring (only support is to create as a standalone IA database)
 - SQL Server clusters (only support is to create as a standalone IA database)
- Instant access does not support a restore of a filestream database. Restore the entire VM without instant access. Or restore the database without instant access. For details see the following article:
<https://www.veritas.com/docs/100048546>

- For instant access to work after an upgrade of the storage and the primary server from an earlier NetBackup version, restart NetBackup web service on the upgraded primary server with the following commands:
 - `/usr/opensv/netbackup/bin/nbwmc stop`
 - `/usr/opensv/netbackup/bin/nbwmc start`

Configure Samba users for SQL Server instant access

Starting with NetBackup 9.0 and later, you must first configure Samba users for SQL Server instant access on the corresponding storage server and enter the credentials on the client. This configuration is also required if you upgrade to NetBackup 9.0.

If the Samba service on a storage server is part of Windows domain, the Windows domain users can be used for Samba share. In this scenario, credentials are not required to access the share.

The following table describes the steps to be performed to add or manage Samba users if the Samba service is not part of Windows domain.

Table 9-2 Steps to add or manage Samba users

User	Steps
For NetBackup Appliance users	<p>For NetBackup Appliance, local users are also Samba users.</p> <p>To manage local users, logon to CLISH and select Main > Settings > Security > Authentication > LocalUser.</p> <p>The Samba password is the same as the appliance local user's logon password.</p>
For Flex Appliance users	<p>For a Flex Appliance application instance, log in to the instance and add any local user to Samba, as follows:</p> <ul style="list-style-type: none"> ◆ If you want, create a new local user with the following commands: <ul style="list-style-type: none"> ■ <code>#useradd <username></code> ■ <code>#passwd <username></code> <p>You can also use an existing local user.</p> ◆ Run the following commands to create user credentials for Samba and enable the user: <ul style="list-style-type: none"> ■ <code>smbpasswd -a <username></code> ■ <code>smbpasswd -e <username></code>

Table 9-2 Steps to add or manage Samba users (*continued*)

User	Steps
For Build Your Own (BYO) users	<p>For new users:</p> <ol style="list-style-type: none"> 1 Create a Linux user, then add the user to Samba. For example, the following commands create a <code>test_samba_user</code> for Samba service only. <pre># adduser --no-create-home -s /sbin/nologin test_samba_user</pre> <pre># smbpasswd -a test_samba_user</pre> 2 Enter a new SMB password. 3 Enter the new SMB password again. The new user is added. <p>For existing users: If you want to add an existing user to the Samba service, run the following command: <code>smbpasswd -a test_samba_user</code></p>

To automatically start the SQL Server database, ensure that you can access the share when you log on with the instance credentials from the web UI.

Configure an instant access database

Configure an instant access database and then start the database

You can configure an instant access database from a full, a transaction log, or an incremental backup. You can choose to add the database automatically to the SQL Server instance.

To configure an instant access database and then start the database

- 1 On the left, click **Microsoft SQL Server**.
- 2 On the **Databases** tab, click the database for which you want to configure the instant access database.
- 3 Click the **Recovery points** tab, then click the date on which the backup occurred.

The available images appear in rows with the backup timestamp for each image.

- 4 Right-click on the backup image and click **Actions > Configure instant access**.

- 5 (Conditional) For a full backup, after the instant access database is created you can add the database to the instance and start the database. Click **Yes > Next** for this option.
- 6 (Conditional) For a transaction log, select a replay option and click **Next**.
- 7 Review the recovery target and host name, instance name and make any wanted changes.
To change the host and instance, click **Change instance**.
- 8 In the **Database name** field, enter the instant access database name that you want to create.
- 9 Enter the username and password of the SQL Server instance for the recovery target.
- 10 Review the recovery options and make changes if needed and then click **Next**.
See [“Options for NetBackup for SQL Server instant access”](#) on page 76.
- 11 (Optional) To view a list of the backup images for the selected recovery point, click the link that displays the number of backup images.
- 12 Review the summary of the selected recovery target and recovery options.
Then click **Start recovery**.
- 13 After the instant access job starts, you can click on the **Restore activity** tab to view the progress.
See [“View the livemount details of an instant access database”](#) on page 75.

Configure an instant access database, but not start the database

You can configure an instant access database from a full backup. If you do not want to start the instant access database after it is created, you can enter the host name or select the name where you want to create the instant access database. After the instant access database is created, the database is not added to the instance but exported to a Samba share.

To configure an instant access database, but not start the database

- 1 On the left, click **Microsoft SQL Server**.
- 2 On the **Databases** tab, click the database for which you want to configure the instant access database.
- 3 Click the **Recovery points** tab, then click the date on which the backup occurred.

The available images appear in rows with the backup timestamp for each image.

- 4 Right-click on the backup image and click **Actions > Configure instant access**.
- 5 If you want to add the database to the instance and start the database, choose **No > Next**.
- 6 Select one of the following options for the recovery target:
 - To enter the recovery target host name, click **Enter host name**.
 - To select from a list of hosts, click **Select host name**
- 7 (Optional) To view a list of the backup images for the selected recovery point, click the link that displays the number of backup images.
- 8 Click **Start recovery**.
- 9 After the instant access job starts, you can click on the **Restore activity** tab to view the progress.

See [“View the livemount details of an instant access database”](#) on page 75.

View the livemount details of an instant access database

You can view the livemount details of an instant access database.

To view the livemount details of an instant access database

- 1 On the left, click **Microsoft SQL Server**.
- 2 Click the **Instant access databases** tab.
- 3 On the **Instant Access databases** tab, click the database for which you want to see the livemount details.

Mount ID	Unique ID for an instant access livemount.
Export path	Exported instant access livemount path from the storage server.
Recovery point ID	Unique ID of a recovery point.
Livemount path	UNC path of the instant access livemount on the Microsoft SQL client.
Export server	Server where the livemount share is exported from.

Delete an instant access database

You can delete an instant access database that may or may not be added to an instance.

To delete an instant access database

- 1 On the left, click **Microsoft SQL Server**.
- 2 Click the **Instant access databases** tab.
The tab lists the names of the configured instant access databases.
- 3 Select **Actions > Delete**.
- 4 Perform one of the following:
 - Your instant access database is added to an instance and is started.
Enter the SQL Server instance credentials and then click **Delete**.
 - Your instant access database is not added to an instance and is not started.
If you are sure that you want to delete the database, then click **Delete**.

Options for NetBackup for SQL Server instant access

The table describes the recovery options that are available when you perform instant access.

Table 9-3 Recovery options

Option	Description
Database recovery state after restore	<p>Select the state for the database after the restore.</p> <ul style="list-style-type: none"> ■ Recover Restore the last image in a restore sequence and make the database ready for use. ■ Restoring Restore an intermediate backup image. The database is left in a loading state so you can restore and apply additional backup images. ■ Standby Create and maintain a standby during a transaction log and database restore. This option requires a standby undo log, which by default is placed in the same directory as the primary datafile. The account that runs the SQL Server service must have full access permission to the <code>SQLStandBy</code> folder.

Table 9-3 Recovery options (*continued*)

Option	Description
Consistency check	<p>The consistency check to perform after the restore. Output from the consistency check is written to the SQL Server client progress log.</p> <ul style="list-style-type: none"> ■ Do not perform Do not perform consistency checking. ■ Full check, including indexes Include indexes in the consistency check. Any errors are logged. ■ Full check, excluding indexes Exclude indexes from the consistency check. If indexes are not selected, the consistency check runs significantly faster but is not as thorough. Only the data pages and clustered index pages for each user table are included in the consistency check. The consistency of the non-clustered index pages is not selected. ■ Check catalog Check for consistency in and between system tables in the specified database. ■ Physical check only Perform a low overhead check of the physical consistency of the SQL Server database. This option only verifies the integrity of the physical structure of the page and the record headers. It also verifies the consistency between the pages' object ID and index ID and the allocation structures.
VDI timeout	<p>Determines the time-out interval for SQL Server Virtual Device Interface. The selected interval is applied to backups and restores of databases and of transaction logs. The default value for backups is 300. The default value for restore operations is 600. Range is 300 - 2147483647.</p>

See [“Configure an instant access database”](#) on page 73.

NetBackup for SQL Server terms

The table describes the important terms that might be new to a SQL Server database administrator or a NetBackup administrator.

Table 9-4 NetBackup for SQL Server terms

Term	Definition
Full backup	A complete backup of the database that contains all of the data files and the log file. (Note that a full backup does not truncate the transaction log.)
Incremental backup	A backup of the changed blocks since the last full backup.
Transaction log	An ongoing record of updates that were made to a database.

Table 9-4 NetBackup for SQL Server terms (*continued*)

Term	Definition
Transaction log backup	Backs up the transactions that have occurred since the last transaction log backup. After a successful backup, the log is cleared so that new transactions can be written to the file. A transaction log backup can only be performed against a database that is configured to run in the full recovery model.
Restore	To copy data back to a SQL Server object.
Recovery	To bring a database online as a result of a restore.
SQL Server host	The host machine on which SQL Server resides. It may also refer to the virtual name of a cluster that supports a SQL Server installation.
SQL Server instance	A SQL Server installation. If an instance is not specified, it is considered the default SQL instance for the SQL host.

Frequently asked questions

Here are some frequently asked questions for Microsoft SQL instant access Build Your Own (BYO).

Table 9-5

Applicable for	Frequently asked question	Answer
BYO	How can I enable the Microsoft SQL instant access feature on BYO after storage is configured or upgraded without the nginx service installed?	<p>Perform the steps in the following order:</p> <ol style="list-style-type: none"> 1 Install the required nginx service version. 2 Ensure that the new BYO nginx configuration entry: <code>/etc/nginx/conf.d/byo.conf</code> is part of the HTTP section of the original: <code>/etc/nginx/nginx.conf</code> file. 3 Run the command: <code>/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo</code>

Table 9-5 (continued)

Applicable for	Frequently asked question	Answer
BYO	<p>How can I resolve the following issue in the <code>vpfs-config.log</code> file that is raised from: Verifying that the MSDP REST API is available via <code>https</code> on port 10087</p>	<p>Perform the steps in the following order:</p> <ol style="list-style-type: none"> 1 Install the <code>policycoreutils</code> and <code>policycoreutils-python</code> packages through yum tool. 2 Add the following rules that SELinux for Nginx requires to bind on the 10087 port. <ul style="list-style-type: none"> ■ <code>semanage port -a -t http_port_t -p tcp 10087</code> ■ <code>setsebool -P httpd_can_network_connect 1</code> 3 Run the following command: <pre data-bbox="803 734 1221 786">/usr/opens/pdde/vpfs/bin/vpfs_config.sh --configure_byo</pre>
BYO	<p>Instant Access for BYO uses a self-signed certificate by default and only supports *.pem external certificate.</p> <p>How do I replace it with a certificate signed by external CA (*.pem certificate), if required?</p>	<p>To configure the external certificate, perform the following steps. If the new certificate is already generated (the certificate must contain long and short host names for the media server), go to step 4.</p> <ol style="list-style-type: none"> 1 Create the RSA public or private key pair. 2 Create a certificate signing request (CSR). The certificate must contain long and short host names for the media server. 3 The External Certificate Authority creates the certificate. 4 Replace <code><PDDE Storage Path>/spws/var/keys/spws.cert</code> with the certificate and replace <code><PDDE Storage Path>/spws/var/keys/spws.key</code> with the private key. 5 Run the following command to reload the certificate: <pre data-bbox="803 1446 1221 1498">/usr/opens/pdde/vpfs/bin/vpfs_config.sh --configure_byo</pre>

Table 9-5 (continued)

Applicable for	Frequently asked question	Answer
BYO	<p>How can I disable media automount for the instant access livemount share in gnome?</p> <p>If the automount is enabled, the source folder is mounted from the livemount share in gnome and smaller disks appear. In this scenario, the instant access feature does not work properly.</p> <p>The mounted disk content source is from the <code>../meta_bdev_dir/...</code> folder under livemount share, while the mount target is in the <code>/run/media/...</code> folder.</p>	<p>Follow the guideline to disable the gnome automount:</p> <p>https://access.redhat.com/solutions/20107</p>
BYO	<p>How can I resolve the following issue in the <code>/var/log/vpfs/vpfs-config.log</code> file?</p> <pre>**** Asking the NetBackup Webservice to trust the MSDP webserver (spws) **** /usr/opensv/netbackup/bin/nblibcurlcmd failed (1):</pre>	<p>Perform the steps in the following order:</p> <ol style="list-style-type: none"> 1 Ensure that your NetBackup primary server is up and there is no firewall blocking the connection between the NetBackup primary server and storage server. 2 Run the following command on storage server to verify the connection status: <pre>/usr/opensv/netbackup/bin/bpcIntcmd -pn</pre> 3 After the NetBackup primary server is up and connection between the NetBackup primary server and storage server is allowed, run the following command: <pre>/usr/opensv/pdde/vpfs/bin/vpfs_config.sh --configure_byo</pre>

Table 9-5 (continued)

Applicable for	Frequently asked question	Answer
BYO and Flex Appliance	<p>How can I enable host-based authentication and secure logon for Samba share so that the MSSQL instant access works on specific windows clients?</p> <p>The clients windows version and the background are listed at the following link:</p> <p>https://support.microsoft.com/en-us/help/4046019/guest-access-in-smb2-disabled-by-default-in-windows-10-and-windows-ser</p>	<p>Perform the steps in the following order:</p> <ol style="list-style-type: none"> 1 In the storage server (one time operation) where the Samba share is exported from: <ul style="list-style-type: none"> ■ Override the following Samba option to disable the guest logon: <pre>map to guest = Never</pre> ■ Create user credentials for Samba. <ul style="list-style-type: none"> ■ <code>smbpasswd -a spws</code> Set Samba password for Samba user spws ■ <code>smbpasswd -e spws</code> Enable Samba user spws 2 For each Windows client, where the Samba share is accessed using the earlier credentials, save the spws credentials in the credential manager. 3 To save the samba credentials on a Windows client, open go to Control Panel > User Accounts > Credential Manager > Add a Windows Credential.. 4 In Internet or network address, enter the storage server domain name. 5 Enter the samba user name and password. Ensure that the user name is same as the user credentials that you created for Samba. 6 Click OK and ensure that you can access <code><storage server domain name></code> without a login prompt.

Table 9-5 (continued)

Applicable for	Frequently asked question	Answer
NetBackup Appliance	How can I enable host-based authentication and secure logon for Samba share so that the MSSQL instant access works on NetBackup Appliance and windows clients?	<p>Perform the steps in the following order:</p> <ol style="list-style-type: none"> 1 In the storage server (one time operation) where the Samba share is exported from, create new local user credentials for Samba with the following Appliance CLISH path: Main_Menu > Settings > Security > Authentication > LocalUser 2 In each Windows client, where the Samba share is accessed using the earlier credentials, save the new local user credentials in the credential manager. <p>For Appliance, the smb.conf file configuration already contains map to guest = Never.</p> <p>The local users are added to samba database automatically and the samba password is the same as the login password. Windows clients can access the appliance's samba share using credentials of the appliance's local users.</p> <p>Perform the steps in the following order:</p> <ol style="list-style-type: none"> 1 To manage appliance local users, go to the following CLISH path: Main_Menu > Settings > Security > Authentication > LocalUser 2 To save the samba credentials on a Windows client, open go to Control Panel > User Accounts > Credential Manager > Add a Windows Credential. 3 In Internet or network address, enter the storage server domain name. 4 Enter the samba user name and password. 5 Click OK and ensure that you can access <storage server domain name> without a login prompt.

Protecting SQL Server with VMware backups

This chapter includes the following topics:

- [About protecting an application database with VMware backups](#)
- [Create a protection plan to protect SQL Server data with a VMware backup](#)
- [Protect SQL Server data with a VMware backup](#)
- [Restore SQL Server databases from a VMware backup](#)

About protecting an application database with VMware backups

With a VMware backup policy and the Veritas VSS provider, NetBackup can create consistent, full backups of an application database that resides on a virtual machine.

VMware application backups let you:

- Use the existing database restore process to restore and recover data from VMware backups.
- Restore and recover databases from VMware backups to alternate clients. The target destination client can be a physical computer or a virtual machine.

Supported environments and configuration

See the following information on virtual systems compatibility:

https://www.veritas.com/content/support/en_US/doc/NB_70_80_VE

Veritas VSS provider

See [“Installing the Veritas VSS provider for vSphere”](#) on page 18.

Create a protection plan to protect SQL Server data with a VMware backup

A VMware protection plan can protect SQL Server data on a virtual machine. Users can then subscribe assets to that protection plan. Note that before you create a protection plan, you must perform additional configuration requirements:

- Configure all storage options.
- Configure the logon account for the NetBackup services.
See [“Configuring the NetBackup services for SQL Server backups and restores”](#) on page 19.
See [“Configure local security privileges for SQL Server”](#) on page 20.
- Review the auto-discovered mappings for the hosts in your environment. This action requires a security administrator or a role with similar RBAC permissions.

To create a protection plan to protect SQL Server data with a VMware backup

- 1 Configure the storage for the backup.
- 2 On the left, select **Protection > Protection plans** and then click **Add**.
- 3 In **Basic properties**, enter a **Name**, **Description**.
- 4 From the **Workload** list, select **VMware**.
- 5 (Optional) Indicate a **Policy name prefix** to append to the policy name. NetBackup automatically creates a policy when users subscribe assets to this protection plan.
- 6 In **Schedules and retention**, click **Add schedule**.
 - In the **Attributes** tab, select the **Full** backup type.
 - In the **Start window** tab, define the window during which the backup can start.
 - Click **Save** after all options are selected in the **Attributes** and the **Start window** tabs.
 - Review the **Backup schedule preview** window and verify that all schedules are set correctly.

See [“Schedules and retention”](#) on page 38.

Create a protection plan to protect SQL Server data with a VMware backup

- 7 In **Storage options**, select the storage to use for the backup.

A protection plan can only use the storage that a NetBackup 8.1.2 or newer media server can access.

Storage option	Requirements	Description
Backup storage	OpenStorage is required for this option. Tape, storage unit groups, and Replication Director not supported.	Click Edit . Select the storage target then click Use selected storage .

- 8 In **Backup options**, review the available options for the backup.

See [“Backup options and Advanced options”](#) on page 85.

- 9 Under **Allow restore of application data from virtual machine backups**, select **Microsoft SQL Server**

(Optional) Select **Truncate logs** if you want to truncate the transaction logs when the VMware snapshot of the virtual machine is complete.

- 10 In **Permissions**, review the roles that have access to protection plans.

To give another role access to this protection plan, click **Add**. Select the **Role** in the table and customize the role by adding or removing permissions in the **Select permissions** section.

See [Configure RBAC](#).

- 11 In **Review**, verify that the protection plan details are correct and click **Save**.

Backup options and Advanced options

The user can adjust the following settings when subscribing to a protection plan.

Backup options

Table 10-1 Backup options for protection plans

Option	Description
Select server or host to use for backups	The host that performs backups on behalf of the virtual machines. Users can choose Automatic to have NetBackup pick the media server, based on the storage unit. Or, the user can select another host from the list. These hosts are other media servers in the environment or hosts that are configured as an access host.

Table 10-1 Backup options for protection plans (*continued*)

Option	Description
If a snapshot exists, perform the following action	Specifies the action that NetBackup takes when a snapshot is discovered before NetBackup creates a new snapshot for the virtual machine backup. For example, users can choose to stop a backup if any snapshots exist. If snapshots are not automatically deleted, the performance of the virtual machine may eventually decline. Undeleted snapshots can cause restore failures due to lack of disk space.
Exclude selected virtual disks from backups	Specifies the virtual disks to exclude from backups. See “Exclude disks from backups” on page 87.

Advanced options

Table 10-2 Advanced options for protection plans

Option	Description
Enable virtual machine quiesce	By default, I/O on the virtual machine is quiesced before NetBackup creates the snapshot. In the majority of cases, you should use this default. Without quiescing file activity, data consistency in the snapshot cannot be guaranteed. If you disable the quiesce, you must analyze the backup data for consistency.
Allow the restore of application data from virtual machine backups	This option allows users to restore application data from full backups of the virtual machine. Note that in NetBackup 8.3 or earlier, application data for Microsoft Exchange Server or Microsoft SharePoint Server must be restored with the NetBackup Backup, Archive, and Restore interface. Data for Microsoft SQL Server must be restored with the NetBackup MS SQL Client. See the documentation for your NetBackup database agent for more details.
Transport mode	Specifies the transport mode to use for backups or how to read the data from the datastore. For more information on transport modes, see the vendor documentation for your virtualization environment.
Snapshot retry options	See “Snapshot retry options” on page 87.

Exclude disks from backups

Excluding virtual disks can reduce the size of the backup, but use these options carefully. They are intended only for the virtual machines that have multiple virtual disks.

Table 10-3 Options for excluding virtual disks

Exclude option	Description
All boot disks	<p>Consider this option if you have another means of recreating the boot disk.</p> <p>The virtual machine's boot disk is not included in the backup. Any other disks are backed up. Note: Data files are available in the restored data disks. However, you cannot start a virtual machine that is restored from this backup.</p>
All data disks	<p>Consider this option only if you have a separate protection plan that backs up the data disks.</p> <p>The virtual machine's data disks are not included in the backup. Only the boot disk is backed up. Note: When the virtual machine is restored from the backup, the virtual machine data for the data disk may be missing or incomplete.</p>
Exclude disks based on a custom attribute	<p>Use this option to allow the VMware administrator to use a custom attribute to control which disks are excluded from backups.</p> <p>The attribute must have comma-separated values of device controllers for the disks to be excluded. For example: <code>scsi0-0, ide0-0, sata0-0, nvme0-0</code>. The default value for this attribute is <code>NB_DISK_EXCLUDE_DISK</code>. Or, you can choose your own value. If you add disks to the custom attribute value between any differential backups, those disks are excluded from the next backup.</p> <p>The VMware administrator must use a VMware interface to apply the attribute to the disks to exclude. See the NetBackup Plug-in for VMware vSphere Web Client Guide or the NetBackup Plug-in for VMware vSphere Client (HTML5) Guide.</p>
Specific disks to be excluded	<p>Use this option to exclude a specific disk by the disk type, controller, and LUN that represent the virtual device node of the disk. Click Add to specify additional disks.</p> <p>If you add controllers between any differential backups, their disks are excluded from the next backup.</p>

Snapshot retry options

For most environments, the default values for the snapshot retry options are appropriate. It may be helpful to adjust these settings based on the size of the virtual machine and the processing load on the VMware server.

Table 10-4 Snapshot retry options

Option	Description
Maximum number of times to retry a snapshot	The number of times the snapshot is retried.
Maximum length of time to complete a snapshot	The time, in minutes, to allow the snapshot operation to complete. If snapshots do not complete, set this option to a specific period to force a time-out. Use the Maximum length of time to wait before a snapshot is retried setting to retry the snapshot at a later time.
Maximum length of time to wait before a snapshot is retried	The time to wait (in seconds) before the snapshot is retried.

Protect SQL Server data with a VMware backup

Use the following procedure to subscribe a VM that contains SQL Server data to a protection plan. When you subscribe an asset to a protection plan, you assign predefined backup settings to the asset.

Note: The RBAC role that is assigned to you must give you access to the assets that you want to manage and to the protection plans that you want to use.

To protect SQL Server data with a VMware backup

- 1 On the left, click **VMware**.
- 2 On the **Virtual machines** tab or **Intelligent VM groups** tab, click the box for the VM or the VM group and click **Add protection**.
- 3 Select a protection plan and click **Next**.
- 4 If you have the necessary role permissions you can adjust one or more of the following settings:
 - **Schedules and retention**
Change when backups occur and the backup start window.
See "[Schedules and retention](#)" on page 38.
 - **Backup options**
Adjust the server or host to use for backups, snapshot options, and exclude options.
See "[Backup options and Advanced options](#)" on page 85.
 - **Advanced options**

Change or enable any advanced options for the protection plan.

See [“Backup options and Advanced options”](#) on page 85.

The plan must allow for restores of SQL Server databases from a VMware image. **Microsoft SQL Server** must be enabled under **Allow restore of application data from virtual machine backups**. If you also want the backup to truncate logs, select **Truncate logs**.

5 Click **Protect**.

The results of your choices appear under **Virtual machines** or **Intelligent VM groups**.

Restore SQL Server databases from a VMware backup

The following steps describe how to use the NetBackup MS SQL Client to restore an SQL Server database from a full VMware backup. The NetBackup web UI does not currently support individual SQL server database restores from VMware backups.

To restore a SQL Server database from a VMware backup

- 1** Open the NetBackup MS SQL Client.
- 2** Browse for the backup images you want to restore.
- 3** Expand the database instance and the database.
- 4** Select the database image that you want to restore.

Only the **Recovered** recovery option is available for VMware backups of SQL Server.

5 Click **Restore**.

Troubleshooting

This chapter includes the following topics:

- [Troubleshooting credential validation](#)
- [Troubleshooting VMware backups and restores of SQL Server](#)
- [SQL Server log truncation failure during VMware backups of SQL Server](#)

Troubleshooting credential validation

[Table 11-1](#) describes the reasons that validation can fail for an instance, replica, or instance group.

Table 11-1 Reasons for credential validation failure

Status code or error	Description	Explanation
40	Could not validate credentials. Failed to connect to client: <client>.	The host name is invalid.
46	The validation operation timed out waiting for a response from the client	You cannot connect to the host because the host is down.
41	Validation of operating system user/password failed for client: <client>.	<ul style="list-style-type: none">▪ The host name is correct, but the user name or password is invalid.▪ The credentials use have the setting Use these specific credentials, but the user account does not have the required the local security privileges Impersonate a client after authentication and Replace a process level token. See "Configure local security privileges for SQL Server" on page 20.

Table 11-1 Reasons for credential validation failure (*continued*)

Status code or error	Description	Explanation
1939	The specified user does not have SQL Server System Administrator privileges.	The credentials do not have the “sysadmin” role and the validation fails.
Invalid configuration detected.	Invalid configuration detected. The service user for the NetBackup Client and NetBackup Legacy Network services must be the same user. Change the service users in the Windows Service Manager and try again.	The NetBackup Client Service or the NetBackup Legacy Network Service requires but does not use the same user for the logon account. See “Configuring the NetBackup services for SQL Server backups and restores” on page 19.

Troubleshooting VMware backups and restores of SQL Server

Note the following when you perform a VMware backup that protects an application:

- The Application State Capture (ASC) job contacts the NetBackup client on the guest virtual machine and catalogs the application data for recovery.
- One ASC job is created per VM, regardless of which applications are selected in policy.
- ASC messages are filtered to the ASC job details in the Activity Monitor.
- Failure results in the discovery job or parent job exiting with status 1.
- If you enable recovery for a particular application but that application does not exist on the VM, the ASC job returns Status 0.
- `bpfis` is run and simulates a VSS snapshot backup. This simulation is required to gain logical information of the application.

Table 11-2 Issues with using a VMware policy to protect SQL Server

Issue	Explanation
A database backup fails.	Databases are cataloged and protected only if they exist in a configuration that is supported for VMware backups. The following disks are not supported: raw device mapping (RDMs), Virtual Machine Disk (vmdk) volumes that are marked as independent, virtual hard disks (VHDs), RAID volumes, ReFS file systems, or an excluded Windows boot disk. NetBackup is installed on an excluded Windows boot disk. The ASC job detects this type of disk and treats it like an independent disk. Do not select the Exclude boot disk option if NetBackup is installed on the boot drive (typically C:).

Table 11-2 Issues with using a VMware policy to protect SQL Server
(continued)

Issue	Explanation
ASC job produces a status 1 (partially successful).	<p>You selected databases for backup that exist on both supported and on unsupported disks. See “A database backup fails” for unsupported disk information.</p> <p>Full-text catalog files exist on the mounted folders. The databases are not cataloged.</p>
The Application State Capture (ASC) job fails and the databases are not protected.	<p>When the ASC job fails, the VMware snapshot or backup continues. Application-specific data cannot be restored.</p> <p>When you query the SQL Server Management Studio (SSMS), it may show that the database was backed up. In this case, though the database was skipped, the snapshot was still successful.</p> <p>You disabled the Virtual Machine quiesce option.</p> <p>Database objects are on a VHD disk. No objects in the backup are not cataloged, including those that do not exist on the VHD.</p> <p>You excluded any data disks from the VMware policy, on the Exclude Disks tab. Be sure that any disks that you exclude do not contain database data.</p> <p>The VMware disk layout has changed since the last discovery. In this situation, you must force NetBackup to rediscover virtual machines by lowering the value of the Reuse VM selection query results for option. See the NetBackup for VMware Administrator's Guide.</p> <p>You cannot use a VMware incremental policy to protect SQL Server. However, the VMware backup job is successful.</p>
You can recover the entire virtual machine from the backup, but you cannot recover the databases individually.	<p>You did not select Microsoft SQL Server, which allows recovery of the databases from the virtual machine backups</p>

SQL Server log truncation failure during VMware backups of SQL Server

SQL Server transaction log truncation may fail during VMware backups of SQL Server if a database name contains special characters or if the %TEMP% directory path is too long. During SQL Server log truncation, the NetBackup for SQL Server

agent creates a temporary log backup. This backup specifies the current user's configured %TEMP% directory and database name as part of the destination backup device. SQL Server limits the path that can be used for backup devices to 259 characters. Under certain circumstances the SQL Server agent may generate a backup device that is longer than 259 character and cause log truncation to fail.

The following conditions cause failure:

- A configured %TEMP% directory that is longer than 259 characters.
- When the combined length of the database name and %TEMP% directory path is longer than 259 characters.

One workaround for this issue is to configure the %TEMP% directory so that the path is substantially less than 259 characters long.