NetBackup™ Web UI Microsoft SQL Server Administrator's Guide

Release 8.3

VERITAS™

NetBackup Web UI Microsoft SQL Server Administrator's Guide

Last updated: 2020-07-28

Legal Notice

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

This chapter includes the following topics:

About the NetBackup web UI

The NetBackup web user interface provides the following features:

- Ability to access the master server from a web browser, including Chrome and Firefox.
  For details on supported browsers for the web UI, see the NetBackup Software Compatibility List.
- 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 such as security, backup management, or workload protection.
- Management of NetBackup security settings, certificates, API keys, and user sessions.
- 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.

- Workload administrators can subscribe assets to the protection plans that meet the SLO, monitor protection status, and perform self-service recovery of virtual machines. The web UI supports the following workloads:
  - Cloud
  - Microsoft SQL Server
  - Oracle
  - Red Hat Virtualization (RHV)
  - VMware
- Usage reporting tracks the size of backup data on your master servers. You can also easily connect to Veritas Smart Meter to view and manage NetBackup licensing.

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 access that the user has to any workload assets, protection plans, or credentials. A user can have multiple roles, allowing for full and flexible customization of user access.
- 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). You cannot use the web UI if you have NetBackup Access Control (NBAC) enabled.

Monitor NetBackup jobs and events

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

- The dashboard displays an overview of NetBackup jobs, certificates, tokens, security events, and usage reporting.
  The dashboard widgets that display depend on a user's RBAC role and permissions.
- Email notifications can be configured so administrators receive notifications when job failures occur. NetBackup supports any ticketing system that can receive inbound email.

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

Protection plans offer the following benefits:

- 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.
- With the necessary RBAC permissions, a workload administrator can create and manage protection plans, including the backup window and retention. See *NetBackup Web UI Administrator's Guide* for details on the roles permissions.
- A workload administrator can select the protection plans to use to protect assets or intelligent groups.

Self-service recovery

The NetBackup web UI makes it easy for a workload administrator to recover VMs or databases. 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 that are introduced with the new web user interface.

Table 1-1 Web user interface terminology and concepts

Term	Definition
Administrator	A user that has complete access and permissions to NetBackup and all of the interfaces, including the NetBackup web UI. The root, administrator, and Enhanced Auditing user all have complete access to NetBackup. In the *NetBackup Web UI* guides, the term *NetBackup administrator* also refers to a user that has full permissions for NetBackup. Usually in reference to a user of the NetBackup Administration Console. Also see *role*.
Asset group	See *intelligent group*.
Asset	The data to be protected, such as physical clients, virtual machines, and database applications.

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

Term	Definition
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.
Classic policy	In the NetBackup web UI, indicates that a legacy policy protects the asset. Legacy policies are created with the NetBackup Administration Console.
External certificate	A security certificate that is issued from any CA other than NetBackup.
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. For VMware and RHV, these groups appear under the tab **Intelligent VM groups**.
Instant access	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.
NetBackup certificate	A security certificate that is issued from the NetBackup CA.
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.
RBAC	Role-based access control. Administrators 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. The web UI is not supported with NetBackup Access Control (NBAC) and cannot be used if NBAC is enabled.
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 mange recovery of specific databases and the credentials that are needed for backups and restores.

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

Term	Definition
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 *Subscribe* as *Add protection*.
Unsubscribe, from a protection plan	*Unsubscribe* 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, or Cloud.
Workflow	An end-to-end process that can be completed using the NetBackup web UI. For example, you can protect and recover VMware and Cloud assets beginning with NetBackup 8.1.2.

Sign in to the NetBackup web UI

Authorized users can sign in to a NetBackup master server from a web browser, using the NetBackup web UI. The following sign-in options are available:

- Sign in with a user name and password
- Sign in with a certificate or smart card
- Sign in with single sign-on (SSO)

Sign in with a user name 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 master server using a user name and password

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

   https://*masterserver*/webui/login

   The *masterserver* is the host name or IP address of the NetBackup master 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	*username*	**jane_doe**
Windows user	*DOMAIN\username*	**WINDOWS\jane_doe**
UNIX user	*username@domain*	**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://*masterserver*/webui/login

   The *masterserver* is the host name or IP address of the NetBackup master 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 master server using SSO

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

   https://*masterserver*/webui/login

   The *masterserver* is the host name or IP address of the NetBackup master 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 master 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 (user name 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**.

Chapter 2

About NetBackup for SQL Server

This chapter includes the following topics:

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 plan 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
Protection plans	The following benefits are included: ■ 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	SQL Server protection plans support the following: ■ 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	The following features are available for backups and restores: ■ 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 verison 8.3. ■ 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.
Stream-based backups and restores	Stream-based backup and restore of SQL Server objects with SQL Server's high-speed virtual device interface.

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

Feature	Description
Snapshot backups and instant access databases	NetBackup can perform backups of SQL Server with snapshot methodology. 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.
Support for VMware backups that protect SQL Server	Support for application-consistent, full backups of VMware computers using snapshots. Use of NetBackup Accelerator can also increase the speed of backups. See the following documents for more information. NetBackup for VMware Administrator's Guide NetBackup Administrator's Guide, Volume I

Chapter 3

Managing Microsoft SQL Server

This chapter includes the following topics:

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 Microsoft 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 availabile.

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.

Select or add credentials to SQL Server instances or replicas

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

See "About Microsoft SQL Server credentials" on page 22.

To select or add 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**.

   Each replica in an availability group must be registered with credentials.
4. Choose one of the following options. Specific RBAC permissions are required to be able to select or to add credentials to a SQL Server asset.

   See the NetBackup Web UI Administrator's Guide or contact your NetBackup administrator for assistance.

Select from existing credentials	Select the credential that you want to use for the selected assets and click **Next**.
Add credentials	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**.

5. The **Permissions** screen displays the roles that have access to the credential.

If you have the necessary RBAC permissions, you can do one or more of the following:

- Add another RBAC role to give it access to the credential.
- Edit the permissions that a role has for a credential.
- Remove a role.

6 Click **Next**. Review the credential settings and click **Finish**.

The registered date reflects the date and time the credential was added or updated and does not indicate if the credentials are valid.

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.

About Microsoft 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 3-1 Options to register credentials

Option to register credentials	Environment and configuration
Use these specific credentials (recommended)	■ 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. **Configuration requirements** 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. 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.

Table 3-1 Options to register credentials *(continued)*

Option to register credentials	Environment and configuration
Use credentials that are defined locally on the client	■ 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. **Configuration requirements** 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. You must also configure the logon account for the NetBackup services.

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.

See the *NetBackup for SQL Server Administrator's Guide* or ask your NetBackup administrator for assistance.

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.

See the *NetBackup for Microsoft SQL Server Administrator's Guide*.

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 must have the SQL Server “sysadmin” role.
- 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.

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. 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** to register instances, both services must use the same logon account. If you use the setting **Use these specific credentials** to register instances, the services can use the same logon or separate logon accounts.
4. Open the **NetBackup Legacy Network Service**.

5 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** to register instances, both services must use the same logon account. If you use the setting **Use these specific credentials** to register instances, the services can use the same logon or separate logon accounts.

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

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

See "Configuring local security privileges for SQL Server" on page 25.

Configuring local security privileges for SQL Server

If you use the option **Use these specific credentials** to create a credential, 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 Run the group policy update command (group policy update) for this change to take effect:

```
gpupdate /Force
```

5 If the NetBackup Client Service and the NetBackup Legacy Network Service use this account to log on, restart these services.

6 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.

Manage Microsoft SQL Server credentials

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

To edit a Microsoft 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 **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 "Select or add credentials to SQL Server instances or replicas" on page 21.

   You may omit credentials at this time. The instance is marked as unregistered and the **Registered** column is empty.
7. Click **Finish**.

Chapter 4

Protecting Microsoft SQL Server

This chapter includes the following topics:

Protect Microsoft SQL Server assets

The following procedure describes how to subscribe an Microsoft 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:

- 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.
- 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 protect Microsoft SQL Server assets

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	■ On the **Instances** tab, select the box for the instance that you want to protect.
An individual database	■ 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	■ On the **Availability groups** tab click the box for the availability group name.
An individual availability database	■ 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	■ 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)	On the **Instances** tab, select the instance name depending on if you want to protect the cluster or a node in the cluster: ■ 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 master 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 35.
- 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 31.
- **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 32.

6 Click **Protect**.

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

Edit protection settings for a 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 31.
- See "Performance tuning and configuration options" on page 32.

To edit protection settings for a 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 **Edit protection**.

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 31.
- **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 32.

5 Click **Protect**.

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 4-1

Option	Description
Recurrence (frequency)	Note: This setting can only be edited for Microsoft SQL Server transaction log schedules. How frequently or when to run the backup.
Keep for (retention)	Note: This setting can only be edited for Microsoft SQL Server transaction log schedules. How long to keep the files that were backed up by the schedule.
Backup 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 4-2 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 master 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.
VDI timeout (seconds)	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 jobs is 600. Range is 300–2147483647.
Use Microsoft SQL Server compression	Enable this option to use SQL Server to compress the backup image. If you enable SQL Server compression, do not enable NetBackup compression. SQL Server compression is not supported for snapshot backups.
Skip unavailable (offline, restoring, etc.) databases	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. 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.
Create copy-only backup	This option allows SQL Server to create an out-of-band backup so that it does not interfere with the normal backup sequence.

Table 4-2 Performance tuning and configuration options *(continued)*

Field	Description

Perform Microsoft SQL Server checksum	Choose one of the following options for SQL Server backup checksums:
	■ 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.
	  ■ 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.

Convert incremental backup to full backup	If no previous full backup exists for the database, then NetBackup converts a differential backup to a full backup. 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: ■ 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. 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.
Convert transaction log backup to full backup	If no previous full backup exists for the database, then NetBackup converts a transaction backup to a full backup. 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. 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.

Table 4-2 Performance tuning and configuration options *(continued)*

Field	Description
Availability database backup preference	This option determines where backups of availability groups occur. Ensure that you select a setting for databases and a setting for transaction logs. ■ **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. **Backup preference for individual availability databases** Note the following behavior when you select a protection plan to protect individual availability databases. ■ 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	This option backs up the active part of the transaction log and then marks it inactive or empty. This option is enabled by default.

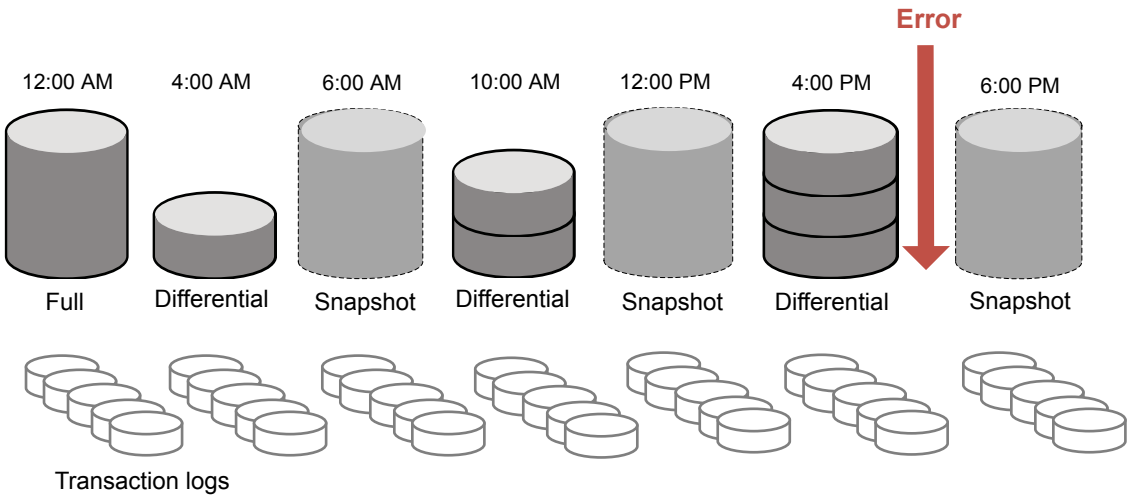
Using copy-only snapshot backups to affect how differentials are based

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 (see Figure 4-1). 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 4-1 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 4-3

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 4-3 *(continued)*

Method	Description
VSS	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. Provider type: ■ 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. Snapshot attribute: ■ 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	For any snapshots with any data that is configured over Volume Manager volumes. ■ 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.

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 4-4 Protection status of Microsoft 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 **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**.

Chapter 5

Restoring Microsoft SQL Server

This chapter includes the following topics:

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

- You must have the RBAC permissions to restore to an alternate location.
- NetBackup must have the ability to communicate with the destination client.

To perform a complete database recovery

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

A standalone database	Locate and select the database: ■ On the **Instances** tab, click on the instance that contains the database you want to restore. ■ On the **Databases** tab, click on the database that you want to restore.
A database that is part of a SQL Server cluster	Locate and select the database: ■ On the **Instances** tab, select the instance that belongs to the cluster. The **Host** name is the virtual name of the SQL Server cluster. ■ On the **Databases** tab, click on the database that you want to restore.
A database that is part of a SQL Server failover cluster instance (FCI)	On the **Instances** tab: ■ Select the instance name depending on how the FCI is protected. The instance name, where the **Host** name is the cluster name of the FCI. The instance name, where the **Host** name is one of the physical node names of the FCI. ■ On the **Databases** tab, click on the database that you want to restore.
A SQL Server host that uses multiple NICs	On the **Instances** tab, select one of the following: ■ Select the instance name depending on how the host is protected. The instance name, where the **Host** name is the private interface name of the SQL Server host. The instance name, where the **Host** name is the private interface name of the virtual SQL Server. ■ On the **Databases** tab, click on the database that you want to restore.

3. Click the **Recovery points** tab.
4. Select the full, differential, or transaction log image that you want to restore.
5. From the **Actions** menu select **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**.

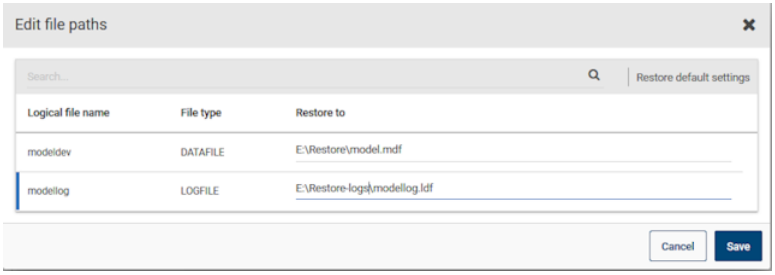
7 Select the host, instance, and database for recovery. You have the following options.

- You can restore to the original host, instance, and database.
- To restore to a different instance, type the name in the **Instance** field.
- To select a different host and instance, click **Change instance**.
- To 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**.

10 For the **Database recovery state after restore**, select **Recover**.

11 Select the other recovery options.

See "Options for Microsoft SQL Server restores" on page 45.

12 Choose a **Consistency check** option to perform after the restore.

See “Options for Microsoft SQL Server restores” on page 45.

13 Click **Next**.

14 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.
- 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 Locate the name of the database that you want to restore.

A standalone database	Locate and select the database: ■ On the **Instances** tab, click on the instance that contains the database you want to restore. ■ On the **Databases** tab, click on the database that you want to restore.
A database that is part of a SQL Server cluster	Locate and select the database: ■ On the **Instances** tab, select the instance that belongs to the cluster. The **Host** name is the virtual name of the SQL Server cluster. ■ On the **Databases** tab, click on the database that you want to restore.

A database that is part of a SQL Server failover cluster instance (FCI)	On the **Instances** tab: ■ Select the instance name depending on how the FCI is protected. The instance name, where the **Host** name is the cluster name of the FCI. The instance name, where the **Host** name is one of the physical node names of the FCI. ■ On the **Databases** tab, click on the database that you want to restore.
A SQL Server host that uses multiple NICs	On the **Instances** tab, select one of the following: ■ Select the instance name depending on how the host is protected. The instance name, where the **Host** name is the private interface name of the SQL Server host. The instance name, where the **Host** name is the private interface name of the virtual SQL Server. ■ On the **Databases** tab, click on the database that you want to restore.

3 Click the **Recovery points** tab.

4 Select the full, differential, or transaction log that you want to restore. From the **Actions** menu select **Restore single recovery point**.

5 (Conditional) For a transaction log image, 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**.

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

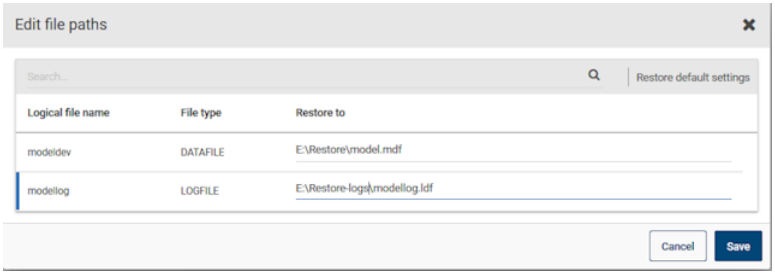
- You can restore to the original host, instance, and database.

- To restore to a different instance, type the name in the **Instance** field.
- To select a different host and instance, click **Change instance**.
- To restore to a different database, type the name in the **Database name** field.

7 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 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:



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

9 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 Microsoft SQL Server restores” on page 45.

10 Click **Next**.

11 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**.

12 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 Microsoft SQL Server restores

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

Table 5-1 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. ■ **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 Microsoft SQL Server service must have full access permission to the `SQLStandBy` folder.

Table 5-1 Recovery options *(continued)*

Option	Description
Consistency check	The consistency check to perform after the restore. Output from the consistency check is written to the SQL Server client progress log. ■ **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	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.
VDI timeout	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.

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.

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
  - 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**.

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 Select the following settings:

- **Restoring**
- **Overwrite existing database**

See “Options for Microsoft SQL Server restores” on page 45.

11 Click **Next**. Then click **Start recovery**.

12 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.
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

- 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**.

9 Select the following settings:

- **Recover**
- **Overwrite existing database**

See "Options for Microsoft SQL Server restores" on page 45.

10 Click **Next**. Then click **Start recovery**.

11 When the restore completes, add the database to the availability group using the **Skip initial data synchronization** option.

12 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.

13 In the NetBackup web UI, on the left select **Workloads > Microsoft SQL Server**.

14 Click on the **Availability groups** tab and then click on the availability group name.

15 On the **Replicas** tab, click on the instance that is hosted on the secondary replica.

16 On the **Databases** tab, click on the database that you want to restore.

17 Click the **Recovery points** tab and locate the image that you restored to the primary replica.

18 From the **Actions** menu select **Perform complete database recovery**.

19 For the transaction log, select the same point in time or log mark that you did for the primary replica.

20 Select the following settings:

- **Restoring**
- **Overwrite existing database**

See "Options for Microsoft SQL Server restores" on page 45.

21 Click **Next**. Then click **Start recovery**.

22 When the restore completes, join the database to the availability group.

23 Repeat step 12 through step 22 for additional replicas in the availability group.

Chapter 6

Instant access

This chapter includes the following topics:

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.
- - 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 nignix 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).
  - Before you start the storage configuration, ensure that the new BYO nginx configuration entry: `/etc/nginx/conf.d/byo.conf` is part of the HTTP section of the original: `/etc/nginx/nginx.conf` file.
  - 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 master 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 6-1 Hardware configuration requirement

CPU	Memory	Disk
■ 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.	■ 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.	Disk size depends on the size of your backup. Refer to the hardware requirements for NetBackup and Media Server Deduplication Pool (MSDP).

Things to consider before you configure an instant access database

Note the following about the instant access SQL Server feature:

- The Microsoft SQL Server backup with following backup options or scenarios does not support Microsoft SQL instant access:
  - Application Aware Backups (VMware)
  - Stream based Backups
  - NBU backup compression
  - Legacy SQL server backup (BCH backup)
  - File group or file backups
  - PFI backups (backup option: Retain snapshot for Instant Recovery or SLP management)
  - MSSQL DB Mirroring (only support is to create as a standalone IA DB)
  - MSSQL Cluster Setup (only support is to create as a standalone IA DB)
- To ensure that instant access works effectively after the storage server and master server are upgraded from an earlier NetBackup version, restart NetBackup Web Service on the upgraded master server with the following commands:
  - /usr/openv/netbackup/bin/nbwmc stop
  - /usr/openv/netbackup/bin/nbwmc start

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 user name 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 57.
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 ?.

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 ?.

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. From the action menu on the right of the row, select **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 6-2 Recovery options

Option	Description
Database recovery state after restore	Select the state for the database after the restore. ■ **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 Microsoft SQL Server service must have full access permission to the `SQLStandBy` folder.
Consistency check	The consistency check to perform after the restore. Output from the consistency check is written to the SQL Server client progress log. ■ **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.

Table 6-2 Recovery options *(continued)*

Option	Description
VDI timeout	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.

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 6-3 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.
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 6-4

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?	Perform the steps in the following order: **1** Install the required nginx service version. **2** Ensure that the new BYO nginx configuration entry: `/etc/nginx/conf.d/byo.conf` is part of the HTTP section of the original: `/etc/nginx/nginx.conf` file. **3** Run the command: `/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo`
BYO	How can I resolve the following issue in the vpfs-config.log file that is raised from: `Verifying that the MSDP REST API is available via https on port 10087`	Perform the steps in the following order: **1** Install the `policycoreutils` and `policycoreutils-python` packages through yum tool. **2** Add the following rules that SELinux for Nginx requires to bind on the 10087 port. ■ `semanage port -a -t http_port_t -p tcp 10087` ■ `setsebool -P httpd_can_network_connect 1` **3** Run the following command: `/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo`

Table 6-4 *(continued)*

Applicable for	Frequently asked question	Answer
BYO	Instant Access for BYO uses a self-signed certificate by default and only supports *.pem external certificate. How do I replace it with a certificate signed by external CA (*.pem certificate), if required?	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. **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 `<PDDE Storage Path>/spws/var/keys/spws.cert` with the certificate and replace `<PDDE Storage Path>/spws/var/keys/spws.key` with the private key. **5** Run the following command to reload the certificate: `/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo`
BYO	How can I disable media automount for the instant access livemount share in gnome? 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. The mounted disk content source is from the `.../meta_bdev_dir/...` folder under livemount share, while the mount target is in the `/run/media/...` folder.	Follow the guideline to disable the gnome automount: https://access.redhat.com/solutions/20107

Table 6-4 *(continued)*

Applicable for	Frequently asked question	Answer

BYO	How can I resolve the following issue in the `/var/log/vpfs/vpfs-config.log` file?
	`**** Asking the NetBackup Webservice to trust the MSDP webserver (spws) ****`
	`/usr/openv/netbackup/bin/nblibcurlcmd failed (1):`
		Perform the steps in the following order:
		1 Ensure that your NetBackup master server is up and there is no firewall blocking the connection between the NetBackup master server and storage server..
		2 Run the following command on storage server to verify the connection status:
		`/usr/openv/netbackup/bin/bpclntcmd -pn`
		3 After the NetBackup master server is up and connection between the NetBackup master server and storage server is allowed, run the following command:
		`/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo`

BYO	How can I enable host-based authentication and secure logon for Samba share so that the MSSQL instant access works on specific windows clients? The clients windows version and the background are listed at the following link: https://support.microsoft.com/en-us/help/4046019/guest-access-in-smb2-disabled-by-default-in-windows-10-and-windows-ser	Perform the steps in the following order: **1** In the storage server (one time operation) where the Samba share is exported from: ■ Override the following Samba option to disable the guest logon: `map to guest = Never` ■ Create user credentials for Samba. ■ `smbpasswd -a spws` Set Samba password for Samba user **spws**) ■ `smbpasswd -e spws` 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.

Table 6-4 *(continued)*

Applicable for	Frequently asked question	Answer
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?	Perform the steps in the following order: **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.