Veeam Plug-ins for Enterprise Applications

Version 12

User Guide

March, 2023

> **NOTE**
>
> Read the End User Software License Agreement before using the accompanying software programs. Using any part of the software indicates that you accept the terms of the End User Software License Agreement.

Contents

Contacting Veeam Software

At Veeam Software we value feedback from our customers. It is important not only to help you quickly with your technical issues, but it is our mission to listen to your input and build products that incorporate your suggestions.

Customer Support

Should you have a technical concern, suggestion or question, visit the Veeam Customer Support Portal to open a case, search our knowledge base, reference documentation, manage your license or obtain the latest product release.

Company Contacts

For the most up-to-date information about company contacts and office locations, visit the Veeam Contacts Webpage.

Online Support

If you have any questions about Veeam products, you can use the following resources:

- Full documentation set: veeam.com/documentation-guides-datasheets.html
- Veeam R&D Forums: forums.veeam.com

About This Document

The document describes how to deploy, configure and use the following application plug-ins:

- Veeam Plug-in for SAP HANA
- Veeam Plug-in for Oracle RMAN
- Veeam Plug-in for SAP on Oracle
- Veeam Plug-in for Microsoft SQL Server

Intended Audience

This document is intended for database administrators, backup administrators, and other IT specialists who use Veeam to back up and restore SAP HANA, Oracle, and Microsoft SQL Server databases.

About Veeam Plug-ins for Enterprise Applications

Veeam Plug-ins for Enterprise Applications extend the functionality of Veeam Backup & Replication and allow you to create transactionally-consistent backups of SAP HANA, Oracle and Microsoft SQL Server databases.

- Veeam Plug-in for SAP HANA — an SAP-certified backup and recovery solution that allows you to back up and restore SAP HANA databases.
- Veeam Plug-in for Oracle RMAN — an Oracle-certified backup and recovery solution that allows you to back up and restore Oracle databases.
- Veeam Plug-in for SAP on Oracle — an SAP-certified backup and recovery solution that allows you to back up and restore Oracle databases to which an SAP application is connected.
- Veeam Plug-in for Microsoft SQL Server — a backup and recovery solution that allows you to back up and restore Microsoft SQL Server databases.
- Veeam Plug-in Management — Veeam Backup & Replication allows you to deploy Veeam Plug-ins on database servers and launch backup policies directly from the Veeam backup console.

> IMPORTANT
>
> Veeam Plug-ins store database and log backups in repositories added to the Veeam Backup & Replication infrastructure. Thus, to use Veeam Plug-ins, you must have a Veeam Backup & Replication server deployed in your infrastructure. To learn how to deploy Veeam Backup & Replication, see the Deployment section of the Veeam Backup & Replication User Guide.

Veeam Plug-in for SAP HANA

Veeam Plug-in for SAP HANA is an SAP-certified backup tool that integrates with SAP backint and allows you to store transactionally-consistent SAP HANA database backups and logs in repositories connected to Veeam Backup & Replication.

> **NOTE**
>
> If you want to protect the SAP HANA server itself, you can use the image-level and file-level backup functionality of Veeam Backup & Replication or Veeam Agent for Linux. Note that image- and file-level backups of SAP HANA servers do not guarantee transaction-consistency of database backups.

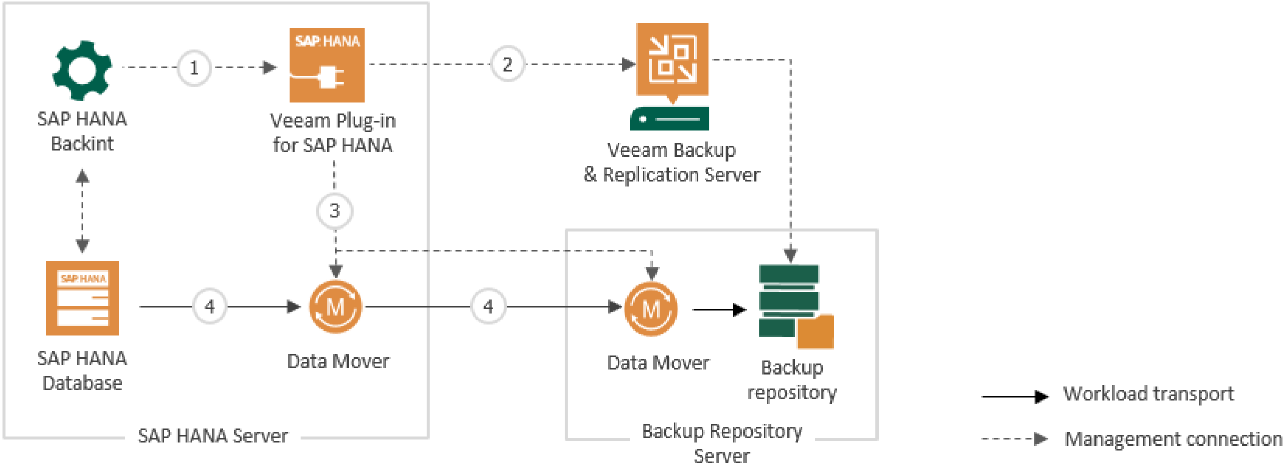
How Veeam Plug-in for SAP HANA Works

Veeam Plug-in acts as an agent between an SAP HANA server and Veeam backup repositories. The plug-in interacts with databases through the SAP HANA Backint component. Backint for SAP HANA is an API that enables Veeam Plug-in to directly connect to the SAP HANA database and send the database backup files to Veeam repositories.

Veeam Plug-in compresses, deduplicates database backups and transfers them to a backup repository connected to the Veeam Backup & Replication infrastructure. After you install and configure Veeam Plug-in on the SAP HANA server, you can perform all backup and restore operations with HDBSQL scripts and with native SAP HANA tools, such as SAP HANA Studio and SAP HANA Cockpit.

When Veeam Plug-in is configured, SAP Backint performs a database backup in the following way:

1. When you start a database backup, the SAP HANA Backint starts Veeam Plug-in services on the SAP HANA server.
2. Veeam Plug-in connects to the Veeam Backup & Replication server and creates a backup job (if it has not been created before). In the Veeam Backup & Replication console, Veeam backup administrators can use the backup job to monitor SAP HANA backups.
3. Veeam Plug-in starts Veeam Data Mover services on the SAP HANA server and on a backup repository. According to a specified number of parallel backint channels, Veeam Data Movers create channels to transfer backup data.
4. Veeam Data Movers transport backup data to the backup repository.



Planning and Preparation

Before you start to use Veeam Plug-in for SAP HANA, read the environment planning recommendations and make sure that your environment meets system requirements.

- System Requirements
- Required Permissions
- Used Ports
- Licensing
- Environment Planning
- Veeam Backup Repositories
- Access and Encryption Settings on Repositories

System Requirements

Before you start using Veeam Plug-in for SAP HANA, make sure the following requirements are met.

Supported OSes

Veeam Plug-in for SAP HANA is supported for the following OSes:

- **SLES for SAP Applications 15** (x86_64): GA, SP1, SP2, SP3.
- **SLES for SAP Applications 12** (x86_64): GA, SP1, SP2, SP3, SP4, SP5.
- **RHEL for SAP Solutions 8** (x86_64): 8.0, 8.1, 8.2, 8.4, 8.6.
- **RHEL for SAP Solutions 7** (x86_64): 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.9.

Supported SAP HANA Versions

Veeam Plug-in for SAP HANA supports the following versions of SAP HANA:

- **SAP HANA 2.0**: SPS 02, SPS 03, SPS 04, SPS 05 (only with Backint version 1.0), SPS06. Express Edition is not supported.
- **SAP HANA 1.0**: SPS12 and later.

> NOTE
>
> To check whether an OS version is compatible with the SAP HANA version you want to use, see the SAP HANA Administration Guide.

Veeam Backup & Replication

Mind the following compatibility of Veeam Backup & Replication and Veeam Plug-in versions:

- **Veeam Plug-in for SAP HANA 12** supports integration with Veeam Backup & Replication version 12.
- **Veeam Plug-in for SAP HANA 11** supports integration with Veeam Backup & Replication version 11, 11a Cumulative Patch P20211211.
- **Veeam Plug-in for SAP HANA 10.0.1.4854 (10a Cumulative Patch 20201202)** supports integration with Veeam Backup & Replication version 10, 11.
- **Veeam Plug-in for SAP HANA 10 (earlier than 10.0.1.4854)** supports integration only with Veeam Backup & Replication version 10.

Note that if you want to use the latest functionality, you must upgrade both Veeam Backup & Replication and Veeam Plug-in to the latest version.

Network

Veeam Plug-in should be able to establish a direct IP connection to the Veeam Backup & Replication server. Thus, Veeam Plug-in cannot work with the Veeam Backup & Replication server that is located behind the NAT gateway.

Permissions

User Rights on the SAP HANA Server

The account used for installing and updating Veeam Plug-in must have root privileges.

Veeam Backup Server User

- The account specified in the Veeam Plug-in configuration settings must be able to authenticate against the Veeam Backup & Replication server. For details, see Configuring Veeam Plug-in for SAP HANA.
- The account specified in the Veeam Plug-in configuration settings must be granted access rights on the Veeam backup repository where you want to store backups.

  To learn how to grant permissions on Veeam repositories, see Granting Permissions on Repositories.
- You can work with backups created by Veeam Plug-in only with the account used for creating the backups. If you want to use another account, see required permissions in Configuring Veeam Plug-in for SAP HANA.

Ports

To enable proper work of Veeam Plug-ins, make sure that the following ports are open.

SAP HANA Server

The following table describes network ports that must be opened to ensure proper communication of the SAP HANA server and backup infrastructure components.

From	To	Protocol	Port	Notes
SAP HANA server where Veeam Plug-in is installed	Veeam Backup & Replication server	TCP	10006	Default port used for communication with the Veeam Backup & Replication server. Note that data between Veeam Plug-ins and backup repositories is transferred directly, bypassing the Veeam Backup & Replication server.
	Backup repository server or gateway server*	TCP	2500 to 3300**	Default range of ports used as data transmission channels. For every TCP connection that a backup process uses, one port from this range is assigned.

* For NFS share, SMB share repositories, and Dell Data Domain, HPE StoreOnce deduplication storage appliances, Veeam Backup & Replication uses an auxiliary backup infrastructure component — gateway server. For details, see the Gateway Server section of the Veeam Backup & Replication User Guide.

** This range of ports applies to newly added backup infrastructure components. If you upgrade to Veeam Backup & Replication 10.0 from earlier versions of the product, the range of ports from 2500 to 5000 applies to the already added components.

Backup Repositories and Gateway Servers

On backup infrastructure components, Veeam Backup & Replication automatically creates firewall rules for the required ports. These rules allow communication between the components. Depending on the type of backup repositories that you use for Veeam Plug-in backups, the following ports must be open to allow communication between backup infrastructure components.

From	To	Protocol	Port	Notes
Veeam Backup & Replication server	Backup repository server or gateway server*	TCP	2500 to 3300**	Default range of ports used as data transmission channels. For every TCP connection that a backup process uses, one port from this range is assigned.
Direct Attached Storage				

From	To	Protocol	Port	Notes
Veeam Backup & Replication server	Linux server used as a backup repository or gateway server	TCP	22	Port used as a control channel from the Veeam Plug-in server to the target Linux host.
	Microsoft Windows server used as a backup repository or gateway server	TCP UDP	135, 137 to 139, 445	Ports used as a management channel from the Veeam Plug-in server to the Repository/Gateway server. Also, the ports are used to deploy Veeam components.
		TCP	6160, 6162	Default ports used by the Veeam Installer Service and Veeam Data Mover Service
Network Attached Storage				
Gateway server (specified in the SMB share repository settings)	SMB server	TCP	445	Default port used by the SMB transport protocol.
		TCP UDP	135, 137 to 139	SMB/Netbios name resolution for the SMB protocol (needed in some cases). For details, see the Used Ports section of the Veeam Backup & Replication User Guide.
Gateway server (specified in the NFS share repository settings)	NFS server	TCP UDP	111, 2049	Standard NFS ports used as a transmission channel from the gateway server to the target NFS share.
Dell Data Domain				
Veeam Backup & Replication server or **Gateway server**	Dell Data Domain For more information, see this Dell KB article.	TCP	111	Port used to assign a random port for the mountd service used by NFS and DDBOOST. Mountd service port can be statically assigned.
		TCP	2049	Main port used by NFS. To change the port, you can use the '`nfs set server-port`' command. Note that the command requires SE mode.

From	To	Protocol	Port	Notes
		TCP	2052	Main port used by NFS MOUNTD. To change the port, you can use the `'nfs set mountd-port'` command. Note that the command requires SE mode.
HPE StoreOnce				
Veeam Backup & Replication server or **Gateway server**	HPE StoreOnce	TCP	9387	Default command port used for communication with HPE StoreOnce.
			9388	Default data port used for communication with HPE StoreOnce.
ExaGrid				
Veeam Backup & Replication server	ExaGrid	TCP	22	Default command port used for communication with ExaGrid.
Quantum DXi				
Veeam Backup & Replication server	Quantum DXi	TCP	22	Default command port used for communication with Quantum DXi.

For detailed list of ports used by Veeam Backup & Replication server and backup repositories, see the Used Ports section of the Veeam Backup & Replication User Guide.

Licensing

To use the Veeam Plug-in functionality, you must have a valid Veeam Backup & Replication license. Licenses are installed and managed on the Veeam Backup & Replication server that is connected to the Veeam Plug-in server. If the license is not valid or out of resources, Veeam Plug-in backup jobs fail.

This guide provides information only on specifics of Veeam licenses for Veeam Plug-ins. For terminology and general information about Veeam Licensing, see Veeam Licensing Policy.

In this section:

- Licensed Objects
- Supported License Types and Packages
- Obtaining and Managing Licenses

Licensed Objects

If you are using any instance-based (Veeam Universal Licensing) license on your Veeam Backup & Replication, you don't need to install any additional license keys.

A machine where SAP HANA is deployed is assumed protected if it has been processed by a Veeam Plug-in backup job in the last 31 days. When you back up SAP HANA databases on one host, one License Unit is consumed from the Veeam Backup & Replication license. A machine protected by both Veeam Plug-in and Veeam Backup & Replication will consume a License Unit only once. For example, you have an SAP HANA server that you back up using Veeam Plug-in. You can also back up this server using image-level backup functionality of Veeam Backup & Replication. In this case, only one License Unit will be consumed.

NOTE

If you are using a legacy perpetual per-socket license, a license is required for each hypervisor CPU socket occupied by protected SAP HANA servers.

A socket is consumed from the license only if the hypervisor where protected servers reside is added to the Veeam Backup & Replication infrastructure. If the hypervisor is not added to the Veeam Backup & Replication infrastructure, an instance unit will be consumed from the license. To learn how to add a hypervisor to the Veeam Backup & Replication infrastructure, see the Virtualization Servers and Hosts section of the Veeam Backup & Replication User Guide.

IMPORTANT

If you have an SAP HANA Scale-Out Cluster, each node will consume one License Unit. The License Units are consumed for all cluster nodes, even if Veeam Plug-in is installed only on one of the nodes.

Supported License Types and Packages

You can use Veeam Plug-ins with the following license types and packages. Note that this guide contains information on specifics of Veeam license packages only for Veeam Plug-ins. For the full list of license packages, see Pricing and Packaging.

- **For Veeam Universal Licensing**:

  You can use Veeam Plug-ins with all license packages (*Veeam Backup Essentials, Veeam Backup & Replication, Veeam Availability Suite*).

  Note that if you use the *Rental* license type, functionality of Veeam Plug-ins is supported only for the *Enterprise Plus* edition of Veeam Backup & Replication.

- **For Perpetual Socket license**:

  Functionality of Veeam Plug-ins is supported only for the *Enterprise Plus* edition of Veeam Backup & Replication.

Obtaining and Managing Licenses

To learn how to install a license and monitor licensed objects, see the Licensing section in the Veeam Backup & Replication User Guide.

Environment Planning

Integration of SAP HANA and Veeam Plug-in requires additional environment planning. When you deploy the plug-in, keep in mind the following requirements and limitations.

Compression

Veeam Plug-in uses built-in compression functionality of Veeam Backup & Replication. If you want to disable the compression, do the following:

1. Open the `/opt/veeam/VeeamPluginforSAPHANA/veeam_config.xml` file with a text editor.
2. In the `veeam_config.xml` file, find the `<AgentParams />` line and add the following parameter:

```
<AgentParams compression="NoCompression" />
```

Scheduling

Veeam Plug-in forwards the backups created by SAP HANA integrated backup application to a Veeam backup repository. You can schedule backup operations with all SAP HANA relevant scheduling options like SAP HANA Cockpit (HANA Cockpit 2.0 SPS 06 or later version), SAP DB13 (NW 7.02 SP17 or later version) or external schedulers like cron, UC4, TWS and others.

To learn how to configure external schedulers, see the Veeam Plug-in for SAP HANA Best Practices.

> NOTE
>
> For SAP Management Software, make sure SAP HANA 2.0 systems are configured in the Multiple-Container mode. Otherwise, backups will fail with the following error: `[110091] Invalid path selection for data backup using backint`. For details, see the SAP HANA Multitenant Database Containers section of the SAP HANA Master Guide.

Veeam User Management

Veeam Plug-in for SAP HANA uses the Windows authentication methods of the Veeam Backup & Replication server to establish a connection to this server and to the target backup repository. It is recommended to create one specific user for each Veeam Plug-in server or for each scale-out cluster.

If this user will be later changed manually, the new user must have at least the *Veeam Backup Operator* and *Veeam Restore Operator* rights within the Veeam Backup & Replication user management. To learn how to assign Veeam Backup & Replication roles, see the Users and Roles section of the Veeam Backup & Replication Guide.

SAP HANA Backup Channels and Veeam Repository Task Slots

By default, SAP HANA uses one channel per data backup operation. You can configure SAP HANA to use additional channels. When multiple channels are used, SAP HANA distributes the data equally across available channels.

To control the number of parallel channels used for each SAP HANA Backint instance, you can edit the `parallel_data_backup_backint_channels` parameter in the SAP HANA `global.ini` file. For instructions, see the Multistreaming Data Backups with Third-Party Backup Tools section of the SAP HANA Administration Guide

> NOTE
>
> The number of multistreaming channels applies to all data backup services larger than 128GB. Data backup services smaller than 128GB use only one channel.

Basically, the more channels used in parallel, the faster is the data flow between SAP HANA and the source Veeam Transport Agent. However, the more channels used in parallel, the more resources are used on the SAP HANA server, network, Veeam backup repository, backup source and target disk systems. You should find the right mix between performance and resource allocation for your specific business need.

The following hardware resources are recommended based on tests on Skylake processors:

- **SAP HANA server**: 1 CPU core and 200 MB of RAM per currently used channel.
- **Backup repository server**: 1 CPU core and 1 GB of RAM per 5 currently used channels.

  These resources are recommended only if you use a dedicated backup repository for Veeam Plug-in backups. If you use the same backup repository for Veeam Plug-in backups and VM backups created by Veeam Backup & Replication or Veeam Agents, consider adding the mentioned above hardware resources based on usual load on your backup repository. For details on hardware requirements for a backup repository, see the System Requirements section of the Veeam Backup & Replication User Guide.

  We recommend to contact your Veeam system engineer to optimize the channel settings and resource allocation. Also, mind the following:

  - It is not recommended to use more than 64 channels in parallel as the overhead will reduce individual channel performance. Set the `max_recovery_backint_channels` setting in `global.ini` to 64 or below depending on available hardware resources.
  - It is recommended to use a separate backup repository for Veeam Plug-in backups.
  - If you want to improve backup performance, the SAP HANA buffer must be increased for additional used channels. For details, consult with your SAP HANA database administrator.
  - SAP HANA can back up individual databases and tenants in parallel. To optimize resources, you can back up databases sequentially.
  - If there are not enough available repository task slots, SAP HANA waits till repository task slots become available.
  - During restore, the order of repository task slots is ignored, and channels are used as requested by SAP HANA.
- **Veeam Backup & Replication server**: during manual metadata operations such as import of backup files, the Veeam Backup & Replication server needs additional 15 GB of RAM per 1 million files located in the same backup job folder.

You can use the following examples as a reference:

- **Example 1: Backing up all databases in parallel**

  In this example, there is a system with 2 tenant databases, each database has 4 services. The databases are backed up in parallel. The SAP HANA channel setting is 6. The following maximum repository task slots and SAP channels are used:

  - Up to 4 task slots/channels are used by SYSTEMDB and its 4 services (all below 128 GB)
  - Up to 6 task slots/channels are used for the index service of the tenant database 1 (the database is bigger than 128 GB)
  - Up to 3 task slots/channels are used for the rest of the 3 remaining services of the tenant database 1 (all below 128 GB)
  - Up to 6 task slots/channels are used for the index service of the tenant database 2 (the database is bigger than 128 GB)
  - Up to 3 task slots/channels are used for the rest of the 3 remaining services of the tenant database 2 (all below 128 GB)
  - If the log backups are below 128GB, you must reserve at least 3 channels for the log backup of SYSTEMDB, tenant database 1, and tenant database 2. These log backups are started automatically on their own schedule or when the maximum file size of the log file is reached.

  In total, for backup processes of all databases started in parallel you need up to 27 available task slots.

- **Example 2: Backup of all databases sequentially**

  In this example, there is system with 2 tenant databases, each database has 4 services. The databases are backed up sequentially. The SAP HANA channel setting is 6. The following maximum repository task slots and SAP channels are used:

  - Up to 6 task slots/channels are used for the index service of a tenant database (the database is bigger than 128 GB).
  - Up to 3 task slots/channels are used for the rest of the 3 remaining services of the same tenant database (all below 128 GB).
  - If the log backups are below 128GB, you must reserve at least 3 channels for the log backup of SYSTEMDB, tenant database 1, and tenant database 2. These log backups are started automatically on their own schedule or when the maximum file size of the log file is reached. Assuming that the log file backups are below 128 GB and do not use additional channels.

  In total, for backup processes of sequential started database backups, 12 task slots must be available.

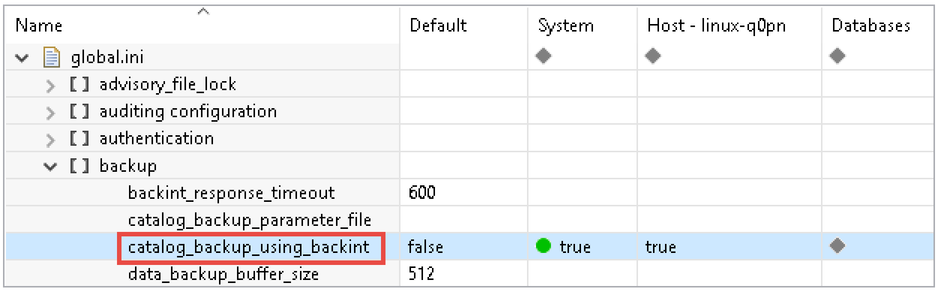
SAP HANA Encryption

Veeam Plug-in supports SAP HANA integrated encryption. The encryption processes are performed on the SAP HANA side. Veeam Plug-in is not involved in encryption processing.

Plan the protection of the encryption environment carefully. In case the encryption keys are lost, Veeam Plug-in can only provide an access to the encrypted backup file. You will have to decrypt data in SAP HANA. For details, see the Managing Data Encryption section of the SAP HANA Administration Guide.

SAP HANA Catalog Backup with Backint

To back up the SAP HANA catalog using Backint, change the settings of the **catalog_backup_using_backint** parameter in the **backup** section of the `global.ini`.



Name	Default	System	Host - linux-q0pn	Databases
global.ini		◆	◆	◆
[ ] advisory_file_lock				
[ ] auditing configuration				
[ ] authentication				
[ ] backup				
backint_response_timeout	600			
catalog_backup_parameter_file				
catalog_backup_using_backint	false	● true	true	◆
data_backup_buffer_size	512			

SAP HANA Backint Parameter File

Veeam Plug-in does not use the Backint parameter file. Leave these fields empty when asked for.

SAP HANA Scale-Out Cluster

Veeam Plug-in supports SAP HANA scale-out clusters with the following limitations:

- Due to design of SAP HANA databases, the same Veeam Plug-in configuration must be set on all scale-out cluster members, including stand-by nodes.
  - On all cluster nodes, Veeam Plug-in must be configured to transfer backups to the same repository.
  - Each cluster node must use the same credentials to connect to Veeam servers.
- All backup tasks across the SAP HANA scale-out cluster are performed in parallel.

SAP HANA System Replication Failover

SAP HANA does not allow you to back up from replicas. You can back up these databases only after a failover. To prepare the replication target system for backups after the failover, you can configure Veeam Plug-in as usual for a new scale-up or scale-out system. The Veeam backup job object will be created at first backup run and reflect the hostname of each system.

> **IMPORTANT**
>
> You must perform full database backup at least once after each failover or failback, so that SAP HANA starts to create automatic log backups.

After the failover, if you want to restore backups created before the failover, you must configure the plug-in to be able to access the backup files from the original source system:

1. Go to `/opt/veeam/VeeamPluginforSAPHANA` and run the Veeam Plug-in configuration tool with the following parameter.

```
VM2ADM:/opt/veeam/VeeamPluginforSAPHANA> SapBackintConfigTool --set-restor
e-server
```

2. Select the original source server.

```
Select source SAP HANA plug-in server to be used for system copy restore:
1. SAP-VM1
2. SAP-VM02
Enter server number: 1
```

3. Specify the backup repository where the required source server backup is stored.

```
Available backup repositories:
1. serv10_repo
Enter repository number: 1
```

4. Perform system copy restore. For instructions, see Recovering Databases to Other Servers.

5. Later, if you want to restore from the new backup chain created from the system replication server, you must run the command again and select the system replication server as a source for restore.

Hosting Environments

By default, Veeam Plug-in uses a hostname to create the Veeam Backup & Replication job object and a folder where the backups will be stored. If server names match, you can set the following entry in the Veeam configuration XML file (`/opt/veeam/VeeamPluginforSAPHANA/veeam_config.xml`) to be able to distinguish servers:

```
<PluginParameters customServerName="hostname.domain.tld" />
```

Example:

If your servers in multiple environments have the name *sap1* and the domains for the 2 environments are `customer1.local` and `customer2.local` you have to set the following entries:

```
<PluginParameters customServerName="sap1.customer1.local" />
<PluginParameters customServerName="sap1.customer2.local" />
```

Additional Files to Back Up

SAP HANA INI Files

SAP HANA does not back up the SAP configuration stored in INI files. Contact your SAP HANA database administrator to discuss the backup of the following files:

- `/usr/sap/<SID>/SYS/global/hdb/custom/config`
- `/usr/sap/<SID>/<INSTANCE>/<FQDN>`
- `/usr/sap/<SID>/SYS/global/hdb/custom/config`

Also, to backup SAP HANA configuration files, you can use file or image-level backup options of Veeam Backup & Replication or Veeam Agent for Linux.

SAP HANA Server for Disaster Recovery

You can use Veeam Backup & Replication or Veeam Agent to create an image-level backup of the SAP HANA server. Note that to create transaction-consistent backups, you must use pre-freeze and post-thaw scripts.

Veeam Plug-in Configuration File

To back up the configuration file of Veeam Plug-in, back up the following file: `/opt/veeam/VeeamPluginforSAPHANA/veeam_config.xml`

Backup Files Format

Veeam Plug-in stores backup files in the following formats:

- A .VAB file stores compressed and deduplicated copy of a SAP HANA database. Veeam Plug-in creates .VAB files for all types of backups.
- A .VASM file stores metadata that contain information about the backup. A .VASM file is created for each .VAB file. .VASM files are used by Veeam Backup & Replication to get data about Veeam Plug-in backups.
- A .VACM file stores metadata of a backup job object.

Veeam Plug-in backup file names match the backup file ID's (EBID) created by SAP HANA.

Veeam Backup Repositories

Veeam Plug-ins store backup files in repositories added to the Veeam Backup & Replication infrastructure. In this section, you can find the list of supported backup repositories and limitations for Veeam Plug-in backups.

Supported Backup Repositories

Veeam Plug-in for SAP HANA supports integration with the following types of repositories added to the Veeam Backup & Replication infrastructure:

- Windows Server
- Linux Server
- CIFS (SMB) Share
- Dell Data Domain
- HPE StoreOnce. If you plan to use HPE StoreOnce as a backup repository for Veeam Plug-in backups, the total number of stored files (data and metadata) must not exceed 3,000,000 per Catalyst store. If necessary, multiple Catalyst stores may be created on the same StoreOnce system.
- Quantum DXi
- NFS File Share
- ExaGrid. If you plan to use an ExaGrid appliance as a backup repository for Veeam Plug-in backups, mind the following:
  - Make sure the repository is configured as described in the ExaGrid section of the Veeam Backup & Replication User Guide.
  - In the `global.ini` settings of SAP HANA, you must set the `max_recovery_backint_channels` parameter value to a number lower than the number of repository task slots. ExaGrid recommends setting it to *1*, and adjust gradually if needed.
- Hardened Repository

You can also use scale-out backup repositories that contain repositories supported by Veeam Backup & Replication.

Backup Repository Limitations

- For Veeam Plug-in backups, the warning which indicates that free space on a storage device has reached a specified threshold is configured in the **veeam_config.xml** file of Veeam Plug-in. The warning settings in the Veeam Backup & Replication console does not affect this setting.

  To configure the warning settings, add the following parameter in the `/opt/veeam/VeeamPluginforSAPHANA/veeam_config.xml` file.

  ```
  <PluginParameters repositoryFreeSpacePercentWarning="10" />
  ```

- Due to specific design of SAP HANA backups, Veeam Plug-in does not use fast cloning. Backups transferred to repositories that use ReFS or XFS as a file system are processed the same way as with NTFS repositories.

- The plug-in configuration wizard will not show repositories where the **Encrypt backups stored in this repository option** is enabled. To learn how to disable the encryption option, see Access and Encryption Settings on Repositories.

- Make sure Veeam backup repositories have enough free space to store database backups and transaction log backups. If required, you can use a scale-out backup repository.

- Veeam extract utility cannot extract backup files created by Veeam Plug-in.

- For security reasons, it is recommended to use separate repositories for different users and grant access to backup repositories only for required users.

Scale-Out Backup Repositories

If you want to store Veeam Plug-in backups on scale-out backup repositories, mind the following:

- For Veeam Plug-in backups and backup copies, the *Performance* policy of a scale-out repository functions differently:

    a. Veeam Backup & Replication checks if there are extents without warning on free space insufficiency. If all extents have the warning, Veeam Backup & Replication uses an extent with the largest amount of free space that has a free task slot.

    b. If there are extents without the warning, Veeam Backup & Replication checks if there are incremental extents with free task slots. If there are no incremental extents with free task slots, Veeam Backup & Replication uses a full extent with the least amount of used task slots.

    c. If there are incremental extents with free task slots, Veeam Backup & Replication sends backup files to an incremental extent with the least amount of used task slots. If the amount of used tasks is the same, an extent with the largest amount of free space.

- If a scale-out repository is configured in the **Data locality** policy, repository extents will be selected according to the amount of free space for each SAP HANA Backint connection. If there are two extents with one slot on each extent, the backup will be launched in two streams (one on each extent).

- If you want to add a backup repository as an extent to a scale-out backup repository and Veeam Plug-in backups are present on this backup repository, you must do the following:

    a. In the Veeam Backup & Replication console, select Veeam Plug-in backup files that reside in this backup repository and remove them from configuration. For details, see Removing backups from configuration. Note that this action does not delete the backups from the repository.

    b. In the Veeam Backup & Replication console, delete the Veeam Plug-in backup job. For details, see Deleting Jobs.

    c. Add the repository as an extent to the scale-out repository. For details, see Extending Scale-Out Repositories.

    d. Rescan the scale-out repository. For details, see Rescanning Scale-Out Repositories.

    > NOTE
    >
    > Names of backup files and paths to backup files must contain only allowed characters:
    >
    > - Alphanumeric characters: `a-zA-Z0-9`
    > - Special characters: `_-.+=@^`
    > - Names of backup files and paths to backup files must not contain spaces.

e. On the Veeam Plug-in server, set the scale-out repository as the target for backups using the following command:

```
SapBackintConfigTool --set-repository
```

f. Map the imported backups using the following command:

```
SapBackintConfigTool --map-backup
```

Capacity Tier

You can configure Veeam Backup & Replication to transfer Veeam Plug-in backup files to a capacity tier. Both policies (Move policy, Copy policy) are supported for Veeam Plug-in backups with the following limitations:

- For Veeam Plug-in backup files, capacity tier does not verify whether data that is being moved is unique and has not been offloaded earlier. Thus, it is highly recommended to check the pricing plans of your cloud storage provider to avoid additional costs for offloading and downloading backup data.
- Capacity tier does not track dependencies of full and incremental Veeam Plug-in backup files. Thus, mind the following:
    - [For the Move policy] When backup files are transferred to the capacity tier, Veeam Backup & Replication takes into account only the creation time of backup files. Make sure that the operational restore window is not longer than the whole backup chain cycle period. Otherwise, you may encounter the scenario when full backup files are transferred to the capacity tier and their increment backup files still remain in the performance tier.
    - The capacity tier immutability expiration date does not have the additional block generation period. The immutability expiration date is based only on the number of days specified in settings of the object storage backup repository.
- If a scale-out repository is down, you cannot restore from the Veeam Plug-in backup files stored on the capacity tier. In this case, you can only import the backup files manually and then perform the data recovery operations.
- If you use a capacity tier that has been created in Veeam Backup & Replication version 10, you cannot transfer Veeam Plug-in backup files to a capacity tier. However, if you want to transfer them manually, do the following:
    - If the backup files are created by Veeam Plug-in version 10, upgrade the metadata of backup files as described in Upgrading Metadata Files to New Format.
    - Run the Set-VBRScaleOutBackupRepository PowerShell command with the –EnablePluginBackupOffload parameter to offload backup files to the capacity tier.
- If you want to restore from backups stored on the capacity extent, at least one performance extent must be available or you must switch the catalog_backup_using_backint parameter to the *False* state in the global.ini file. Otherwise, at the end of the restore process, SAP Backint will not be able to back up the catalog and restore will fail.

Hardened Repository

You can configure Veeam Backup & Replication to transfer Veeam Plug-in backup files to a hardened repository. The hardened repository helps to protect Veeam Plug-in backup files from loss as a result of malware activity or unplanned actions. Backup files in the hardened repository become immutable for the time period specified in the backup repository settings. During this period, backup files stored in the repository cannot be modified or deleted.

For Veeam Plug-in for SAP HANA backups, immutability works according to the following rules:

- Immutability is applied to backup (VAB) files and backup metadata (VASM) files. Backup job metadata (VACM) files are not immutable.
- Backup files become immutable for the configured time period (minimum 7 days, maximum 9999 days).
- The count of the immutability period starts when the backup metadata (VASM files) has been created during the backup job session.
- The immutability period is not extended for the active backup chain.
- Every 1 hour, the immutability service that runs in the background detects backup files that do not have the immutability flag and sets the immutability flag on the necessary backup files.

Data Restore from Hardened Repository

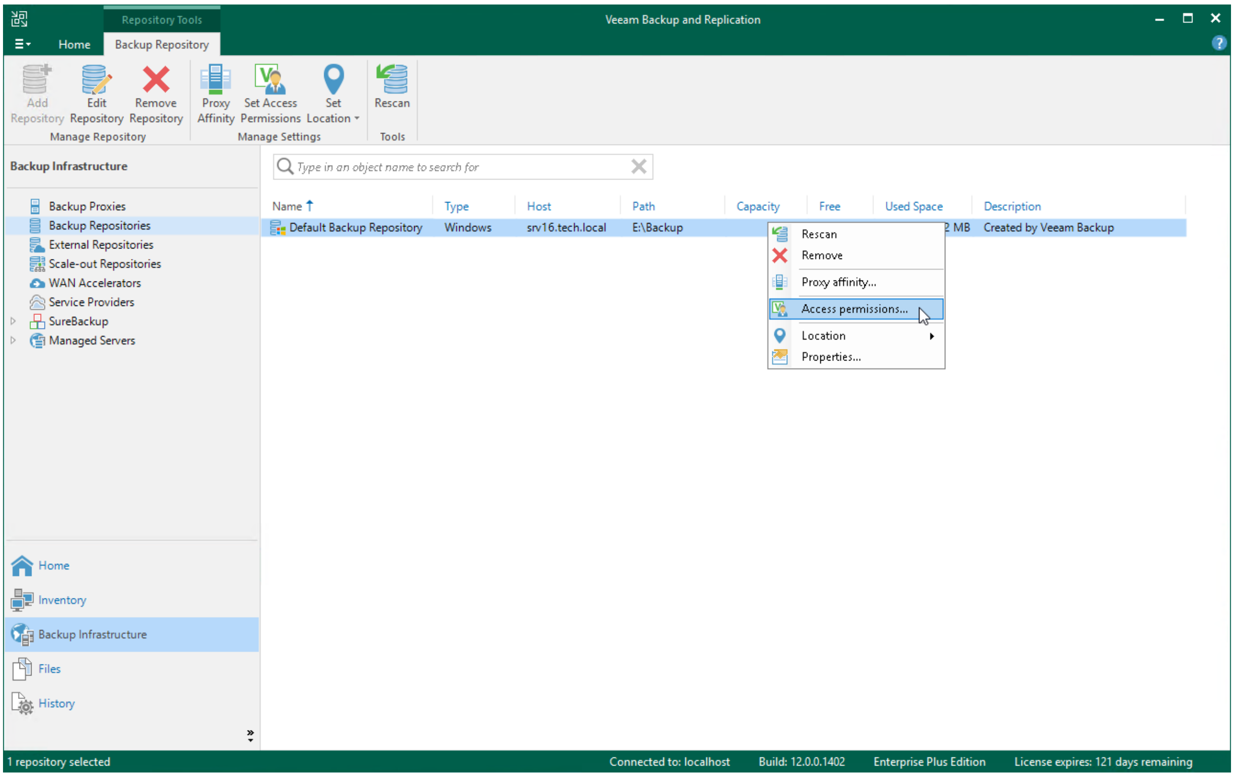
As a result of malware activity or unplanned actions, backup job metadata (VACM) files may become unavailable in the hardened repository. In this case, to restore data from the hardened repository, you must re-create the VACM file. For more information, see Restore from Hardened Repository.

Access and Encryption Settings on Repositories

When you configure Veeam Plug-in, you specify an account that must be used to connect to the Veeam Backup & Replication server. To be able to store backups in a backup repository, the specified account must have access permissions on the target backup repository.

To grant access permissions, do the following:

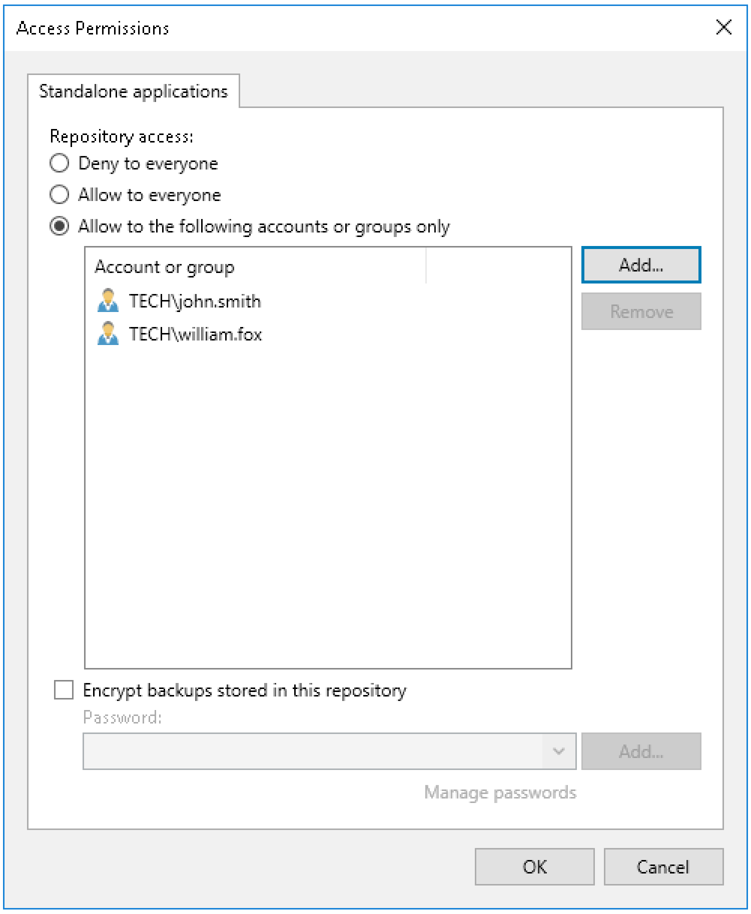
1. In Veeam Backup & Replication, open the **Backup Infrastructure** view.
2. In the inventory pane, click the **Backup Repositories** node or the **Scale-out Repositories** node.
3. In the working area, select the necessary backup repository and click **Set Access Permissions** on the ribbon or right-click the backup repository and select **Access permissions**.



Name	Type	Host	Path	Capacity	Free	Used Space	Description
Default Backup Repository	Windows	srv16.tech.local	E:\Backup			2 MB	Created by Veeam Backup

4. In the **Access Permissions** window, on the **Standalone applications** tab specify to whom you want to grant access permissions on this backup repository:
   - *Allow to everyone* — select this option if you want to grant repository access to any user. This option is equal to granting access rights to the *Everyone* group in Microsoft Windows (anonymous users are excluded). For security reasons, the option is not recommended for production environments.
   - *Allow to the following accounts or groups only* — select this option if you want only specific users to be able to store backups in this repository. Click **Add** to add the necessary users and groups to the list.
5. Veeam Plug-ins cannot send backups or backup copies to a backup repository where encryption is enabled. Thus, make sure that the **Encrypt backups stored in this repository** check box is not selected.

6. Click **OK**.



Access Permissions

Standalone applications

Repository access:

○ Deny to everyone

○ Allow to everyone

● Allow to the following accounts or groups only

Account or group
TECH\john.smith
TECH\william.fox

□ Encrypt backups stored in this repository

Password:

Deployment and Configuration

To deploy Veeam Plug-in, you must install the plug-in on a SAP HANA server and configure plug-in integration settings. In this section:

- Installing Veeam Plug-in for SAP HANA
- Configuring Veeam Plug-in for SAP HANA
- Automatic Configuration of Veeam Plug-in for SAP HANA
- Upgrading Plug-in for SAP HANA
- Importing Backups
- Upgrading Backup Files
- Uninstalling Plug-in for SAP HANA

This guide gives instructions on how to deploy Veeam Plug-in assuming that you have already deployed a Veeam Backup & Replication server and configured a backup repository. If you need instructions on how to deploy Veeam Backup & Replication, see the Veeam Backup & Replication User Guide for your platform.

You can also manage deployment, configuration and backup policies of Veeam Plug-ins using the Veeam Backup & Replication console. For details, see Veeam Plug-in Management.

Installing Plug-in for SAP HANA

Veeam Plug-in for SAP HANA is an additional component of Veeam Backup & Replication, and the installation package of the plug-in is included in the Veeam Backup & Replication installation ISO file.

You can install the plug-in using the `.RPM` package or extract the plug-in files from the `.TAR.GZ` archive. Depending on the type of package suitable for your OS, perform steps in one of the following guides:

- Installing Plug-in from .RPM Package
- Unpacking Plug-in from .TAR.GZ Archive

> **IMPORTANT**
>
> Mind the following:
>
> - Veeam Plug-in for SAP HANA must be installed on the SAP HANA server.
> - The `/opt/veeam` directory must be writable.
> - To install the plug-in, use the `sudo` command or a user with root privileges.
> - If you want to install Veeam Plug-in on an SAP HANA scale-out cluster, repeat the described installation process on all cluster nodes.

Installing Veeam Plug-in from .RPM Package

To install Veeam Plug-in, do the following:

1. Mount the Veeam Backup & Replication installation disk (`VeeamBackup&Replication_12.0.0.1420.iso`).

   If you deploy Veeam backup infrastructure for the first time, you can download the Veeam Backup & Replication installation disk image from the Veeam Backup & Replication: Download page.

2. Open the mounted disk image and go to the `/Plugins/SAP HANA/x64` directory.

3. Upload the `VeeamPluginforSAPHANA-12.0.0.1420-1.x86_64.rpm` file to the SAP HANA server.

4. To install Veeam Plug-in, run the following command:

```
rpm -i VeeamPluginforSAPHANA-12.0.0.1420-1.x86_64.rpm
```

Unpacking Veeam Plug-in from .TAR.GZ Archive

To extract plug-in files from the `.TAR.GZ` archive, perform the following:

1. Mount the Veeam Backup & Replication installation disk (`VeeamBackup&Replication_12.0.0.1420.iso`).

   If you deploy Veeam backup infrastructure for the first time, you can download the Veeam Backup & Replication installation disk image from the Veeam Backup & Replication: Download page.

2. Open the mounted disk image and go to the `/Plugins/SAP HANA/x64` directory.

3. Upload the `VeeamPluginforSAPHANA.tar.gz` file to the SAP HANA server.

4. Create the `/opt/veeam` directory.

```
mkdir /opt/veeam
```

3. In the terminal, open the folder that contains the `VeeamPluginforSAPHANA.TAR.GZ` archive.

4. Unpack the plug-in files from the archive to the `/opt/veeam` directory.

```
tar -xzvf VeeamPluginforSAPHANA.tar.gz -C /opt/veeam
```

Configuring Plug-in for SAP HANA

When you configure Veeam Plug-in settings, you set up integration settings between a SAP HANA server, Veeam Backup & Replication server and backup repositories where backup files will be stored. Veeam Plug-in uses the **SapBackintConfigTool** wizard to configure the integration settings. The wizard configures the SAP HANA Backint settings and creates the `/opt/veeam/VeeamPluginforSAPHANA/veeam_config.xml` file.

> NOTE
>
> - The configuration of Veeam Plug-in must be performed by a user with database administrator rights on all SAP HANA instances of the server.
> - The SAP HANA High Level Isolation mode is not supported.

See the following instructions:

- Veeam Plug-in Configuration
- Configuration of Veeam Plug-in on Multiple SAP HANA Instances
- Verifying Configuration of Veeam Plug-in for SAP HANA
- Configuration Tool Commands

Veeam Plug-in Configuration

To configure Veeam Plug-in, do the following:

1. Log in with operating system user (*<sid>adm* or a user with similar rights) and run the following command to launch the Veeam Plug-in configuration tool. You do not need root privileges if you have configured group access as described in the Required Permissions section.

   ```
   SapBackintConfigTool --wizard
   ```

   If you have extracted files form the .TAR.GZ archive, go to the `/opt/veeam/VeeamPluginforSAPHANA` folder and run the following command:

   ```
   ./SapBackintConfigTool --wizard
   ```

2. Specify the DNS name or IP address of your Veeam Backup & Replication server.

   ```
   Enter backup server name or IP address: serv02.tech.local
   ```

3. Specify the port which will be used to communicate with the backup server. Default port: *10006*.

   ```
   Enter backup server port number: 10006
   ```

4. Specify credentials to authenticate against the Veeam Backup & Replication server.

```
Enter username: serv02\administrator
Enter password for serv02\administrator:
```

IMPORTANT

Mind the following:

- You can work with backups created by Veeam Plug-in only with the account used for creating the backups. If you want to use another account, assign the *Veeam Backup Administrator* role or *Veeam Backup Operator* and *Veeam Restore Operator* roles to the account.

  To learn how to assign Veeam Backup & Replication roles, see the Users and Roles section of the Veeam Backup & Replication Guide.
- The account must have access permissions on the required backup repository. To learn how to configure access permissions and encryption settings on repositories, see Access and Encryption Settings on Repositories.

5. Select the backup repository where you want to store backups. In the terminal dialog, enter the number of the repository from the list of available repositories.

```
Available backup repositories:
1. serv10_repo
2. serv07_repo
Enter repository number: 1
Configuration result:
SID SH2 has been configured
```

IMPORTANT

- The used account must have access to Veeam backup repositories that you plan to use.
- Encryption must be disabled on the repository.

Otherwise, the repositories will not be listed as available. To learn how to configure access and encryption settings on repositories, see Access and Encryption Settings on Repositories.

If you start the wizard for the first time on an SAP HANA scale-out cluster, the wizard asks you for a cluster name. The cluster name will be used by Veeam Backup & Replication to identify the backup job for the cluster. Further runs of the wizard within the SAP HANA scale-out cluster will not ask for this entry again.

NOTE

[For SAP HANA 1.0] If the wizard finishes with an error that required `hdbbackint` symlink cannotbe created, see this Veeam KB.

Configuration of Veeam Plug-in on Multiple SAP HANA Instances

Configuration of Veeam Plug-in includes configuration or creation of the SAP HANA Backint symlinks on all SAP HANA instances. To be able to do this for multiple SAP HANA instances at the same time, the configuration must be performed by a user with root privileges. Alternatively, you can use an account from the *sapsys* user group to configure the plug-in and set the symlink for SAP HANA instances where the account has access rights. You can repeat the wizard under another account to configure additional SAP HANA instances.

Alternatively, you can configure a Linux security group. To do that, you must add all Veeam Plug-in admins to this security group and set the following rights:

```
chown root:<youradmingroup> /opt/veeam/VeeamPluginforSAPHANA/veeam_config.xml
chmod 664 /opt/veeam/VeeamPluginforSAPHANA/veeam_config.xml
```

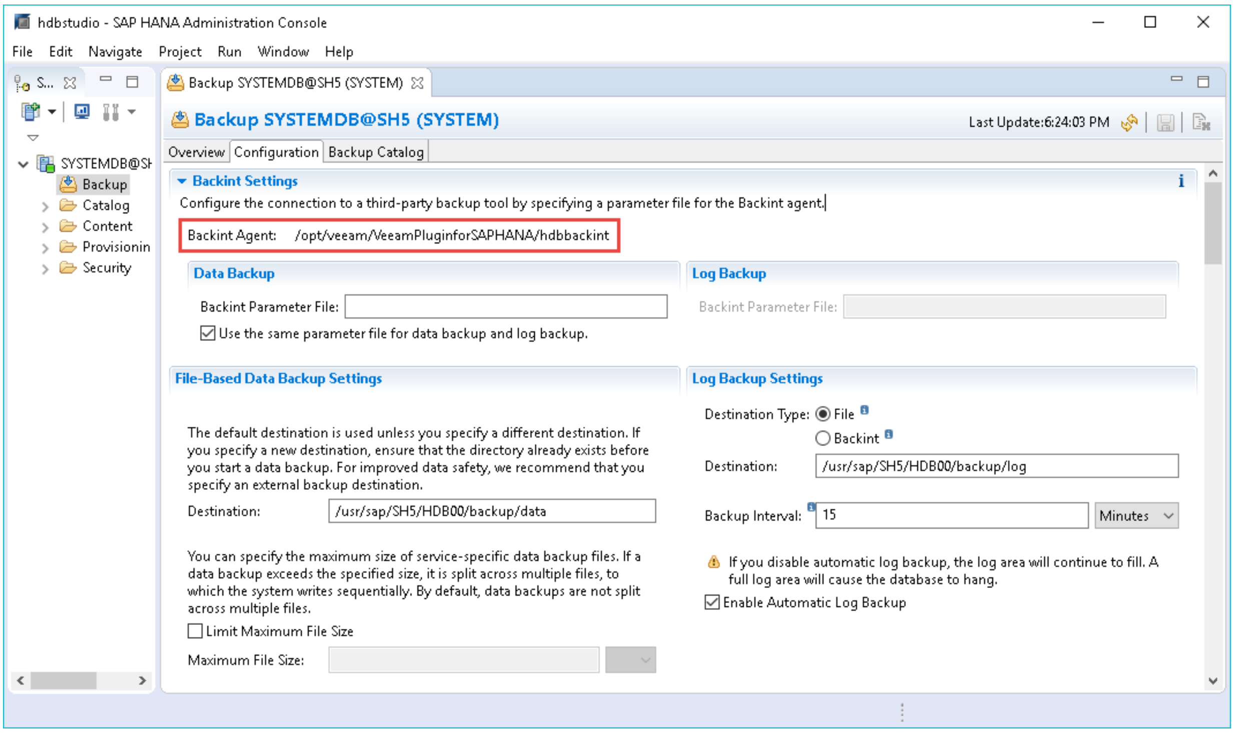
To learn about required permissions for backup and restore operations within SAP HANA, see the Authorization for Backup and Recovery section of the SAP HANA Administration Guide.

Verifying Configuration of Veeam Plug-in for SAP HANA

When you finish the plug-in configuration wizard, the plug-in creates a soft link in the `/hana/shared/<SID>/global/hdb/opt` directory.

To verify that the Backint Agent is configured correctly, do the following:

1. Connect to the database using SAP HANA Studio.
2. Go to `Backup/Configuration`.
3. In the **Backint Agent** field, make sure that the specified path leads to `/opt/veeam/VeeamPluginforSAPHANA/hdbbackint`.


hdbstudio - SAP HANA Administration Console
File Edit Navigate Project Run Window Help
S...
SYSTEMDB@SH
Backup
Catalog
Content
Provisionin
Security
Backup SYSTEMDB@SH5 (SYSTEM)
Overview Configuration Backup Catalog

Backup SYSTEMDB@SH5 (SYSTEM)

Last Update:6:24:03 PM

Backint Settings

Configure the connection to a third-party backup tool by specifying a parameter file for the Backint agent.

Backint Agent: /opt/veeam/VeeamPluginforSAPHANA/hdbbackint

Data Backup

Backint Parameter File:

☑ Use the same parameter file for data backup and log backup.

Log Backup

Backint Parameter File:

File-Based Data Backup Settings

The default destination is used unless you specify a different destination. If you specify a new destination, ensure that the directory already exists before you start a data backup. For improved data safety, we recommend that you specify an external backup destination.

Destination: /usr/sap/SH5/HDB00/backup/data

You can specify the maximum size of service-specific data backup files. If a data backup exceeds the specified size, it is split across multiple files, to which the system writes sequentially. By default, data backups are not split across multiple files.

☐ Limit Maximum File Size

Maximum File Size:

Log Backup Settings

Destination Type: ● File ○ Backint

Destination: /usr/sap/SH5/HDB00/backup/log

Backup Interval: 15 Minutes

If you disable automatic log backup, the log area will continue to fill. A full log area will cause the database to hang.

☑ Enable Automatic Log Backup

Configuration Tool Commands

Apart from running a configuration wizard, you can use the **SapBackintConfigTool** tool to change a specific parameter in the `veeam_config.xml` file or enable/disable Veeam Plug-in features.

See the list of available commands for **SapBackintConfigTool**:

Command	Description
--help	Shows the list of tool parameters.
--show-config	Shows configuration parameters.
--wizard	Starts the wizard to configure the plug-in settings. This wizard edits the `veeam_config.xml` file or creates a new one if the configuration file was removed from the `/opt/veeam/VeeamPluginforSAPHANA` directory.
--set-credentials <"serv\username"> <password>	Specifies credentials to log in to the Veeam Backup & Replication server.
--set-host <hostname>	Specifies the IP address or hostname of the Veeam Backup & Replication server.
--set-port <port_number>	Specifies a port number that will be used to communicate with the Veeam Backup & Replication server.
--set-repositories	Launches a wizard to select a backup repository. A backup repository is selected from repositories which are available in the connected Veeam Backup & Replication instance.
--set-restore-server	[for System Copy] Specifies the backup that will be copied.
--map-backup	Maps the imported backups.
--set-force-delete	Deletes backup files after specified days.
--configure-restore-from-copy	Enables restore from backup copy. Note that if you enable restore from backup copy, you cannot back up databases with Veeam Plug-in. To revert changes, you must disable restore from backup copy. Note that when you launch the command, the wizard will ask you to reconfigure the catalog backup from backint to disk.
--promote-backup-copy-to-primary	Maps the imported backup copy to a regular Veeam Plug-in backup chain.

Example:

To specify credentials that will be used to log in to the Veeam Backup & Replication server, use the plug-in configuration tool with the following command.

```
SapBackintConfigTool --set-credentials "serv02\Administrator" "password"
```

Automating Configuration of Plug-in for SAP HANA

To automate the configuration of Veeam Plug-in for SAP HANA, do the following:

1. Copy the `veeam_config.xml` file to other servers where you want to configure the plug-in.
2. The password stored in the configuration file is encrypted with a machine key. Thus, on each machine, after the `veeam_config.xml` file was copied, you must reset the password of the account used to log in to the Veeam Backup & Replication server. To reset the password, use the following command. Note that the operation requires *root* privileges.

```
SapBackintConfigTool --set-credentials <"serv\username"> <password>
```

Upgrading Plug-in for SAP HANA

Periodically, Veeam releases a new version of Veeam Backup & Replication that contains new features and bug fixes. The release package also contains a new version of Veeam Plug-ins.

If you want to upgrade Veeam Plug-in, note that Veeam Backup & Replication must be the same or later that the version of Veeam Plug-in. If you want to use the latest functionality, you must upgrade both Veeam Backup & Replication and Veeam Plug-in to the latest version. After the upgrade, you don't need to to re-run the Veeam Plug-in configuration wizard, the plug-in configuration files will be preserved.

> **IMPORTANT**
>
> Mind the following:
>
> - Version of Veeam Backup & Replication must be the same or later than the version of Veeam Plug-in. First, you must upgrade Veeam Backup & Replication, then you can upgrade Veeam Plug-ins. To learn how to upgrade Veeam Backup & Replication, see the Upgrading to Veeam Backup & Replication 12 section of the Veeam Backup & Replication User Guide.
> - Operations in the terminal of the Linux machine require root privileges.
> - If you want to upgrade Veeam Plug-in on an SAP HANA scale-out cluster, repeat the described upgrade process on all cluster nodes.

Before You Begin

Veeam Plug-in installation files are included in the installation disk image of Veeam Backup & Replication. You must upload the installation file to the SAP HANA server. To do this, perform the following steps.

1. Mount the Veeam Backup & Replication installation disk (`VeeamBackup&Replication_12.0.0.1420.iso`).
2. Open the mounted disk image and go to the `Plugins\SAP HANA\x64` directory.
3. Select the the Veeam Plug-in installation file and upload it to the SAP HANA server.

To learn how to upgrade Veeam Plug-in for SAP HANA, see the following guides:

- Upgrading Plug-in on Linux (RPM)
- Upgrading Plug-in on Linux (TAR.GZ)

Upgrading Plug-in on Linux (.RPM)

To upgrade Veeam Plug-in for SAP HANA from the `.RPM` package, perform the following:

1. Upload the new `VeeamPluginforSAPHANA-12.0.0.1420-1.x86_64.rpm` package to the SAP HANA server.
2. Run the following command. Note that the operation requires *root* privileges.

```
rpm -U VeeamPluginforSAPHANA-12.0.0.1420-1.x86_64.rpm
```

> **TIP**
>
> To find out which version of Veeam Plug-in is installed on your server, you can use the following command: `rpm -qa | grep VeeamPlugin*`

Upgrading Plug-in on Linux (.TAR.GZ)

To upgrade Veeam Plug-in for SAP HANA on a Linux machine from the `.TAR.GZ` archive, do the following:

1. Upload the `VeeamPluginforSAPHANA.tar.gz` file to the SAP HANA server.
2. In the terminal, open the folder that contains the `VeeamPluginforSAPHANA.TAR.GZ` archive.
3. Unpack the plug-in files from the archive to the `/opt/veeam` directory. Old Veeam Plug-in files will be replaced by new files.

```
tar -xzvf VeeamPluginforSAPHANA.tar.gz -C /opt/veeam
```

Importing Backup Files

If the Veeam Backup & Replication server has failed and you have restored it in a new location, you can copy the backup files to a new repository and re-map the Veeam Plug-in backup files.

Limitations and Prerequisites

Mind the following limitations:

- If backup files are not imported according to instructions given in this section, Veeam Plug-in backup and restore operations may fail.
- The repository from which you plan to import backups must be added to the Veeam Backup & Replication infrastructure. Otherwise you will not be able to access backup files.
- [For backups of scale-out clusters and servers with the `customServerName` option] To avoid mapping failure, the cluster name must be the same as the name used before importing backups.
- If you are importing backup files from a scale-out backup repository, the names of backup files and paths to backup files must contain only allowed characters:
    - Alphanumeric characters: `a-zA-Z0-9`
    - Special characters: `_-.+=@^`
    - Names of backup files and paths to backup files must not contain spaces.

How to Import Veeam Plug-in Backup Files

To import Veeam Plug-in backup files, do the following:

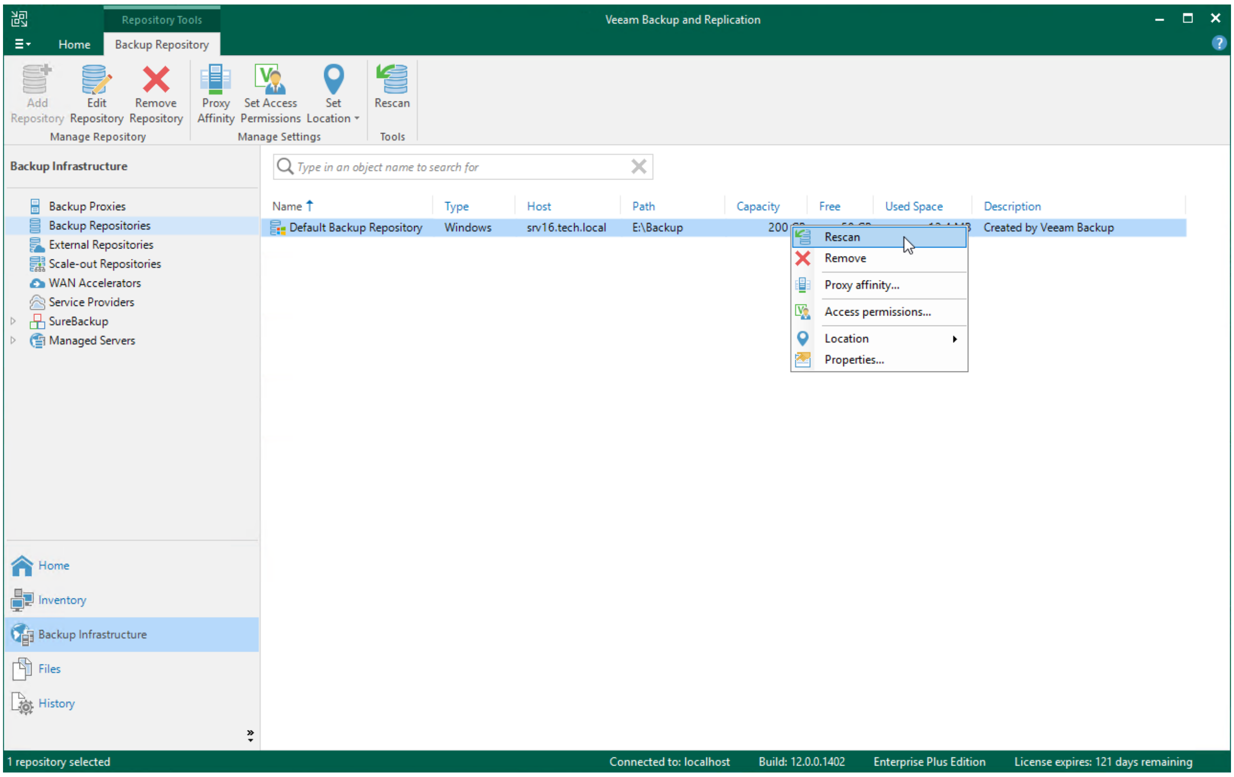
1. Copy the backup file folder to a backup repository or add a new backup repository with this folder as a subfolder.

    > **TIP**
    >
    > Each Veeam Plug-in backup file (.vab) has its own metadata file (.vasm). Make sure that you import backup files and all related metadata files. Also, you must import the backup job metadata file (.vacm) which is stored in the same folder.

2. Log in to the Veeam Backup & Replication console.
3. Open the **Backup Infrastructure** view.
4. In the inventory pane of the **Backup Infrastructure** view, select the **Backup Repositories** node.

5. In the working area, select the required backup repository and click **Rescan** on the ribbon. Alternatively, you can right-click the backup repository and select **Rescan**.

   During the rescan operation, Veeam Backup & Replication gathers information about backups that are currently available in the backup repository and updates the list of backups in the configuration database. After the rescan operation, backups that were not in this configuration database will be shown on the **Home** view in the **Backups > Disk (Imported)** node.



Name	Type	Host	Path	Capacity	Free	Used Space	Description
Default Backup Repository	Windows	srv16.tech.local	E:\Backup	200 [illegible]	[illegible]	[illegible]	Created by Veeam Backup

6. On the SAP HANA server, set the new repository as a target in the Veeam Plug-in settings:

```
sudo SapBackintConfigTool --set-repositories
Available backup repositories:
1. serv55.tech.local
2. serv07_repo
Enter repository number: 1
Configuration result:
SID SH2 has been configured
```

7. Start the Veeam Plug-in configuration wizard with the following parameter:

```
sudo SapBackintConfigTool --map-backup
```

Upgrading Backup Files

Since version 11, Veeam Plug-in uses a new format of backup files: instead of one metadata file for all backup files there are separate metadata files (.vasm) for each database backup file (.vab). The new metadata format allows to optimize the productivity of backup and restore operations.

For Veeam Plug-in 11, the backup files upgrade is not obligatory. However, in version 12, backup files created by Veeam Plug-in version 10 will not be supported.

> IMPORTANT
>
> If you do not upgrade backup files, you will get the following warning in the job session logs: *Backup metadata is not up to date. Please upgrade the backup*. If you want to disable the warning, see instructions in this Veeam KB.

Prerequisites

Before upgrading backup files, make sure the following requirements are met.

- Make sure that you have upgraded Veeam Plug-in on the source server. If the plug-in is not upgraded to version 11 and you upgrade the backup files, then all next backup job runs will fail.
- Make sure that you have disabled the backup job whose backup files you want upgrade. You must also disable the backup copy jobs that use these backup files as a source.
- If the backup files reside on the scale-out backup repository, all repository extents must be available. Also, the extents must not be in the seal or maintenance mode.
- If you want to upgrade backup files created by a backup copy job, you must meet the same requirements as for the backup job files.
- During the process of the metadata upgrade, you cannot run the target backup job and you cannot restore from the backup files.

  The upgrade process duration depends on the number of backup files in the backup set, type of the backup repository and workload level on the file system.

  For example, there are backup files of the SAP HANA server that contains 10 instances and is backed up every 15 minutes with the retention policy set for 2 weeks. The upgrade of backup files can have the following duration on not overloaded file systems:

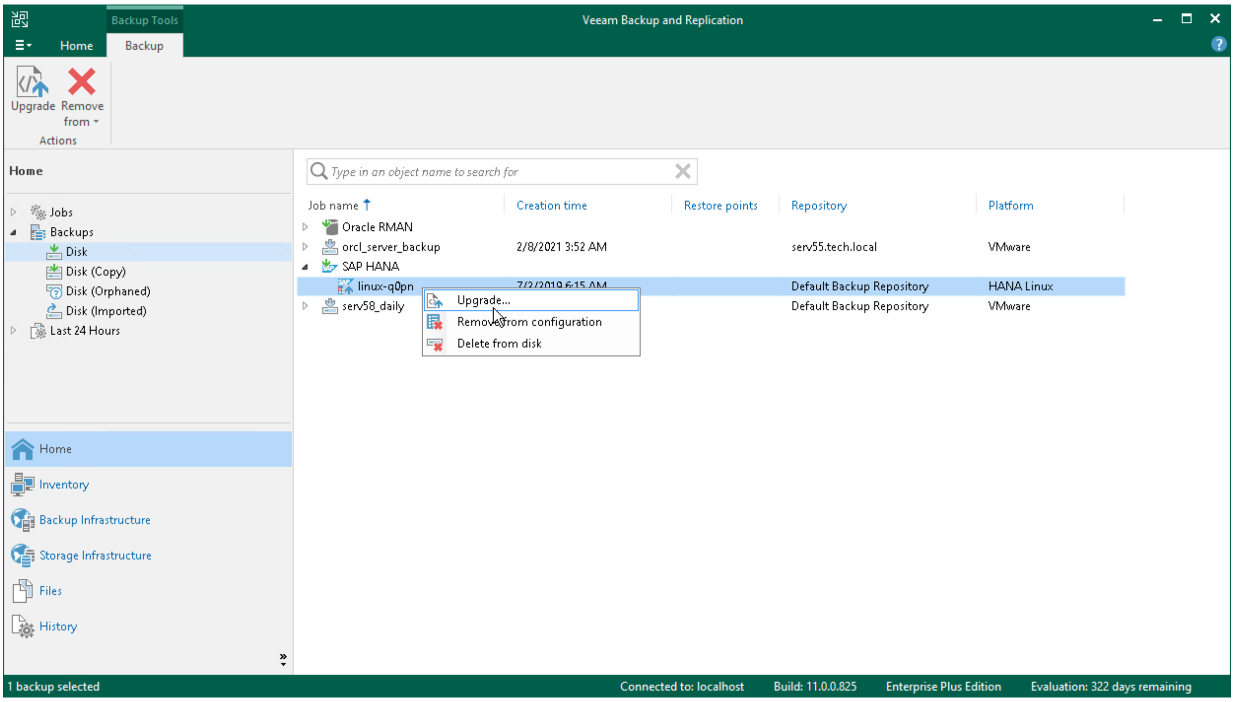
  - Microsoft Windows: 30 minutes
  - Linux: from 30 minutes to 3 hours
  - SMB/NFS: 1.5 hours
  - Data Domain Boost/Quantum DXi/ExaGrid/CIFS (SMB)/NFS file share: 3-4 hours
  - HPE StoreOnce: up to 10 hours (due to specifics of this repository type for processing large number of files)

Upgrading Backup Files in Veeam Backup & Replication Console

To upgrade backup files in the Veeam Backup & Replication console, do the following:

1. Open the **Home** view.
2. In the inventory pane, expand the **Backups** view and select **Disk**.
3. In the working area, right-click the job or the restore point and select **Upgrade**.

   Alternatively, you can select the job or the restore point and click **Upgrade** on the ribbon.



Job name	Creation time	Restore points	Repository	Platform
Oracle RMAN				
orcl_server_backup	2/8/2021 3:52 AM		serv55.tech.local	VMware
SAP HANA				
linux-q0pn	7/2/2019 6:15 AM		Default Backup Repository	HANA Linux
serv58_daily			Default Backup Repository	VMware

Uninstalling Plug-in for SAP HANA

To uninstall Veeam Plug-in for SAP HANA on a Linux machine, go to the directory with the Veeam Plug-in package and run the following command. Note that the operation requires *root* privileges.

```
rpm -e VeeamPluginforSAPHANA
```

Database Protection

After you configure Veeam Plug-in, you can back up databases with SAP HANA backup tools. Veeam Plug-in will automatically transfer data to the Veeam backup repository and store this data in Veeam proprietary format. The backup process itself is performed by SAP HANA Backint.

Keep in mind that examples in this section are provided only for demonstrating purposes. For details on full backup functionality of SAP HANA tools, see the SAP HANA Backup section of the SAP HANA Administration Guide.

> IMPORTANT
>
> Veeam Plug-in transfers backup data to the Veeam backup repository only when you perform the backup using SAP Backint.

To back up SAP HANA databases, you can use SQL commands or SAP HANA administration tools. For examples, see the following guides:

- Backing Up Databases Using SQL Commands
- Backing Up Databases with SAP HANA Studio
- Backing Up Databases with SAP HANA Cockpit
- Backup Job in Veeam Backup & Replication

Database Backup (HDBSQL Scripts)

After you configure Veeam Plug-in settings, you can use HDBSQL to back up and restore SAP HANA databases. For details on the HDBSQL backup, see the BACKUP DATA Statement section of the SAP HANA SQL and System Views Reference.

Prerequisites

Before the backup process, you can use the `hdbuserstore` tool to set secure storage of SAP HANA connection details.

To configure `hdbuserstore`, you must log in to SAP HANA HDBSQL as the operating system administrator (*<sid>adm*) and run the following commands. For details, see the Secure User Store section of the SAP HANA Security Guide.

```
sh4adm@linux-q0pn:/usr/sap/SH4/HDB01> hdbuserstore SET <key> hostname:30013@SID
<username> <password>
sh4adm@linux-q0pn:/usr/sap/SH4/HDB01> hdbsql -U <key>
```

Backing Up SAP HANA Databases Using Backint

To back up the database with Backint, use one of the following commands depending on which type of backup you want to perform:

- Full backup of a tenant database.

```
backup data for <TENANT_DATABASE_NAME> using backint ('backup_name_prefix'
);
```

- Differential backup of a tenant database.

```
backup data differential for <TENANT_DATABASE_NAME> using backint ('backup
_name_prefix');
```

- Incremental backup of a tenant database.

```
backup data incremental for <TENANT_DATABASE_NAME> using backint ('backup_
name_prefix');
```

- Full backup of a tenant database with the ASYNCHRONOUS option. The ASYNCHRONOUS option can be helpful if you monitor SAP HANA backups on another host and just want to run the backup command from a script. The option runs the backup job in the background and closes the current script session.

```
backup data for <TENANT_DATABASE_NAME> using backint ('backup_name_prefix'
) ASYNCHRONOUS;
```

- Full backup of SYSTEMDB.

```
backup data using backint ('backup_name_prefix');
```

- Differential backup of SYSTEMDB.

```
backup data differential using backint ('backup_name_prefix');
```

- Incremental backup of SYSTEMDB.

```
backup data incremental using backint ('backup_name_prefix');
```

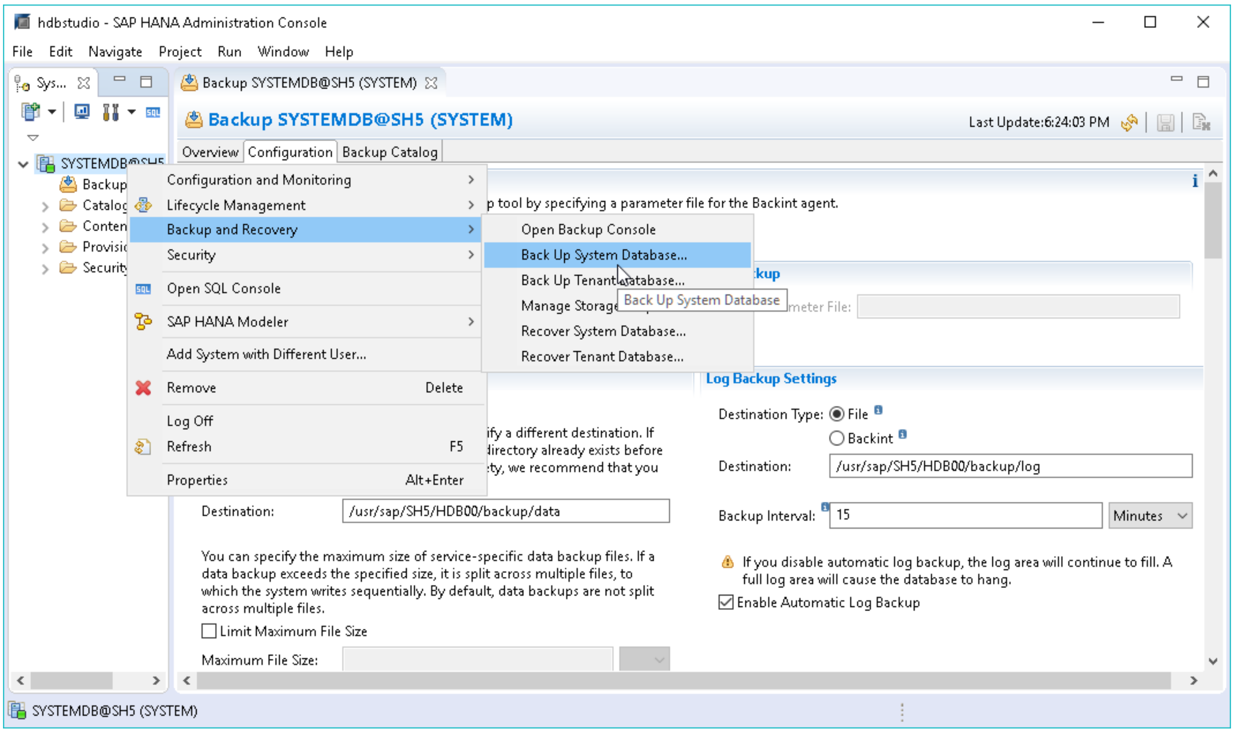
Database Backup (SAP HANA Studio)

After you configure Veeam Plug-in settings, you can back up your databases using SAP HANA Studio. Veeam Plug-in will automatically transform backup files to a Veeam backup repository.

The example provided below is for demonstration purposes only. For details on the full backup functionality of SAP HANA Studio, see the Creating Data Backups and Delta Backups section of the SAP HANA Administration Guide.

To perform Backint backup with SAP HANA Studio, do the following:

1. In SAP HANA Studio, connect to the database as a user with DATABASE ADMIN privileges.
2. In the **Systems** view, right-click the database.
3. Select **Backup and Recovery** and then select **Back Up System Database** or **Back Up Tenant Database**.



p tool by specifying a parameter file for the Backint agent.

ify a different destination. If directory already exists before ty, we recommend that you

Destination: /usr/sap/SH5/HDB00/backup/data

You can specify the maximum size of service-specific data backup files. If a data backup exceeds the specified size, it is split across multiple files, to which the system writes sequentially. By default, data backups are not split across multiple files.

☐ Limit Maximum File Size

Maximum File Size:

Destination Type: ● File ○ Backint

Destination: /usr/sap/SH5/HDB00/backup/log

Backup Interval: 15 Minutes

If you disable automatic log backup, the log area will continue to fill. A full log area will cause the database to hang.

☑ Enable Automatic Log Backup

4. In the backup wizard, specify backup settings:

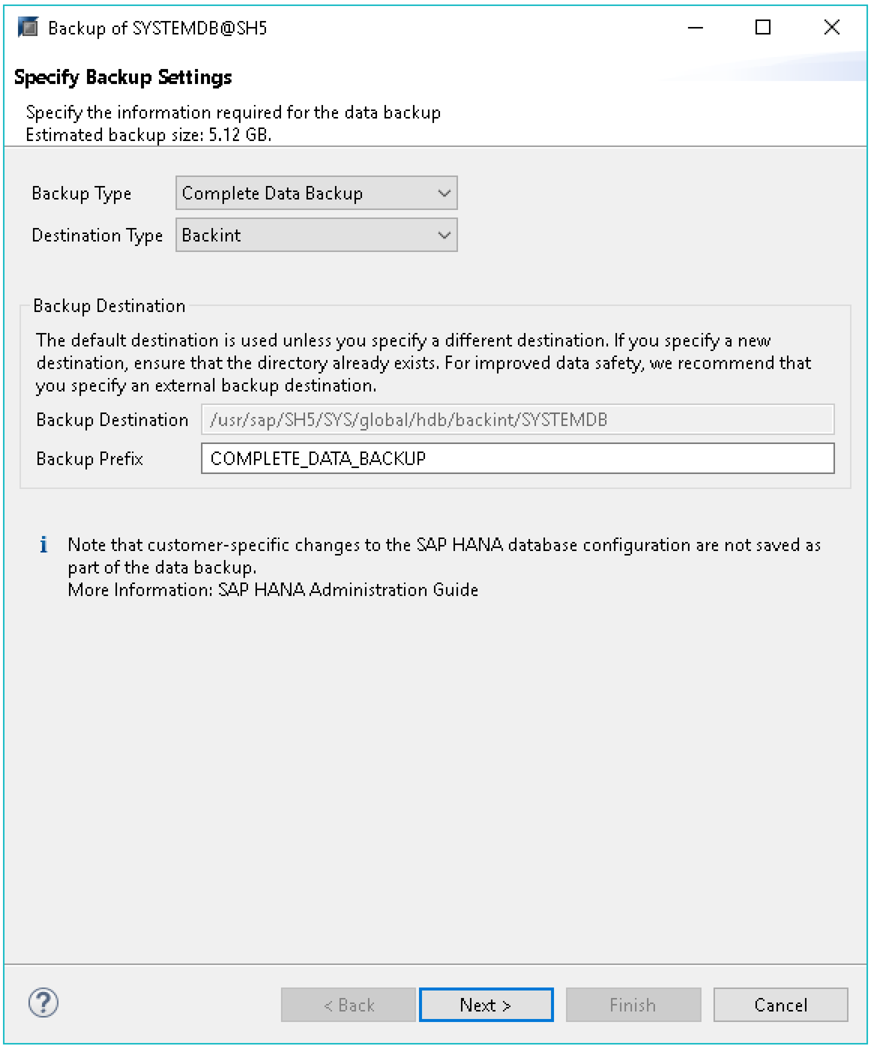
   a. Select the required backup type:

      - **Complete Data Backup**: backup of all data structures required to recover the database.
      - **Incremental Data Backup**: backup of data changed since the last full data backup or the last delta backup.
      - **Differential Data Backup**: backup of data changed since the last full data backup.

b. In the **Destination Type** list, select *Backint*. With this option selected, Veeam Plug-in will transfer the backup file to Veeam backup repository.

c. Change the default backup prefix, if needed.

d. Click **Next**.



Backup of SYSTEMDB@SH5

Specify Backup Settings

Specify the information required for the data backup
Estimated backup size: 5.12 GB.

Backup Type: Complete Data Backup

Destination Type: Backint

Backup Destination

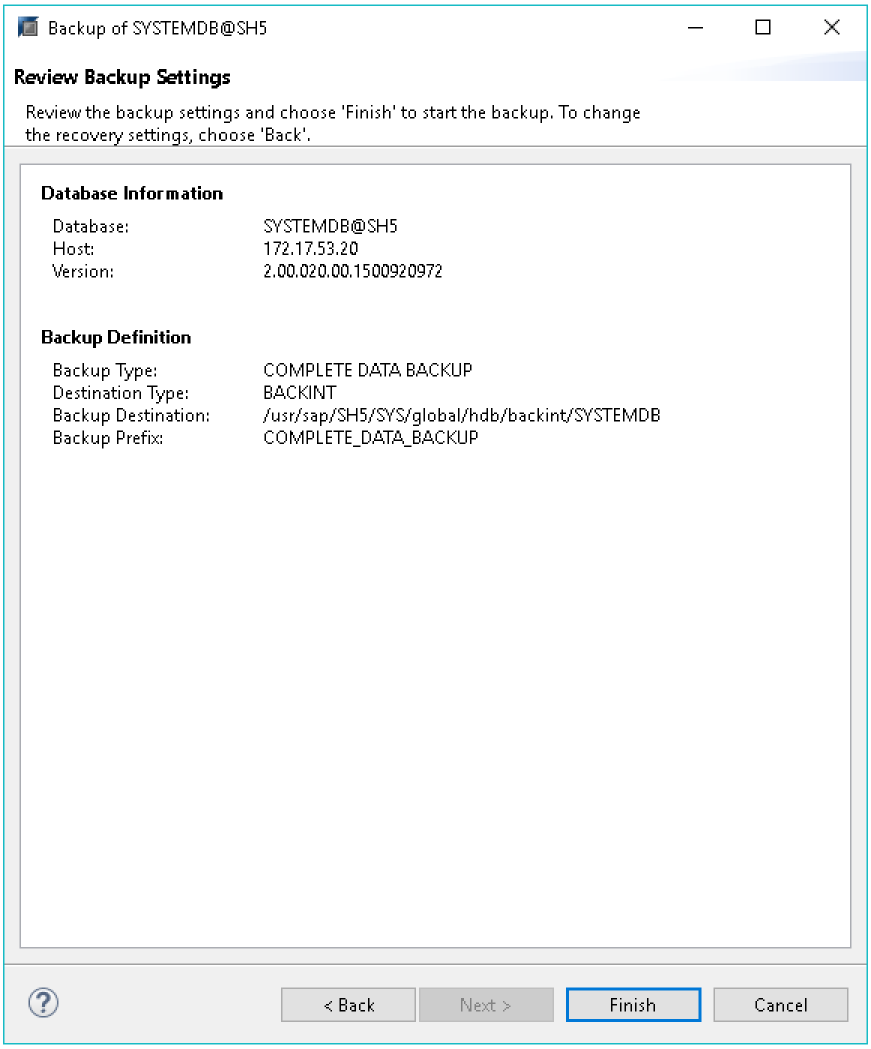
The default destination is used unless you specify a different destination. If you specify a new destination, ensure that the directory already exists. For improved data safety, we recommend that you specify an external backup destination.

Backup Destination: /usr/sap/SH5/SYS/global/hdb/backint/SYSTEMDB

Backup Prefix: COMPLETE_DATA_BACKUP

Note that customer-specific changes to the SAP HANA database configuration are not saved as part of the data backup.
More Information: SAP HANA Administration Guide

5. In the **Review Backup Settings** step of the wizard, click **Finish** to start the backup process.



Review Backup Settings

Review the backup settings and choose 'Finish' to start the backup. To change the recovery settings, choose 'Back'.

Database Information

Database:	SYSTEMDB@SH5
Host:	172.17.53.20
Version:	2.00.020.00.1500920972

Backup Definition

Backup Type:	COMPLETE DATA BACKUP
Destination Type:	BACKINT
Backup Destination:	/usr/sap/SH5/SYS/global/hdb/backint/SYSTEMDB
Backup Prefix:	COMPLETE_DATA_BACKUP

After you launch the backup process, SAP HANA Studio will back up the database, and Veeam Plug-in will forward backup files to the backup repository that is specified in the Veeam Plug-in settings.

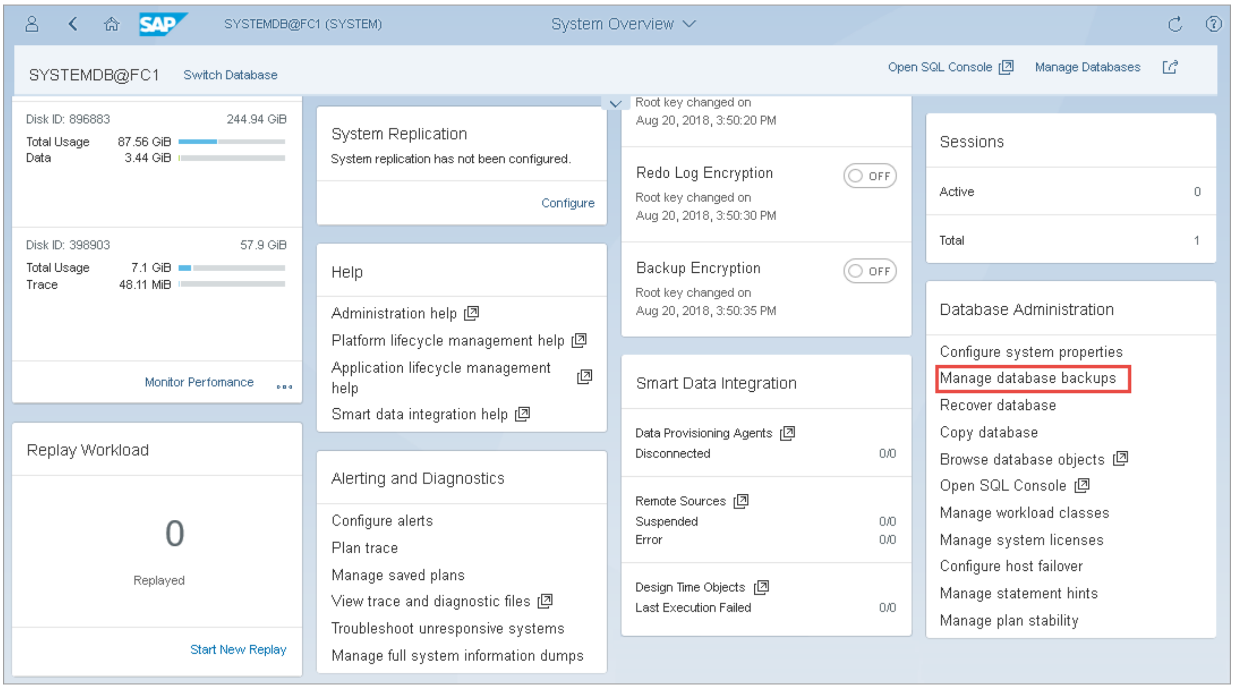
Database Backup (SAP HANA Cockpit)

After you configure Veeam Plug-in settings, you can back up your databases with SAP HANA Cockpit 2.0. You can perform complete, incremental, and differential backups of SYSTEMDB and tenant databases. Veeam Plug-in will automatically transform backup files to Veeam backup repository. Keep in mind that you must select the Backint option as a destination target.

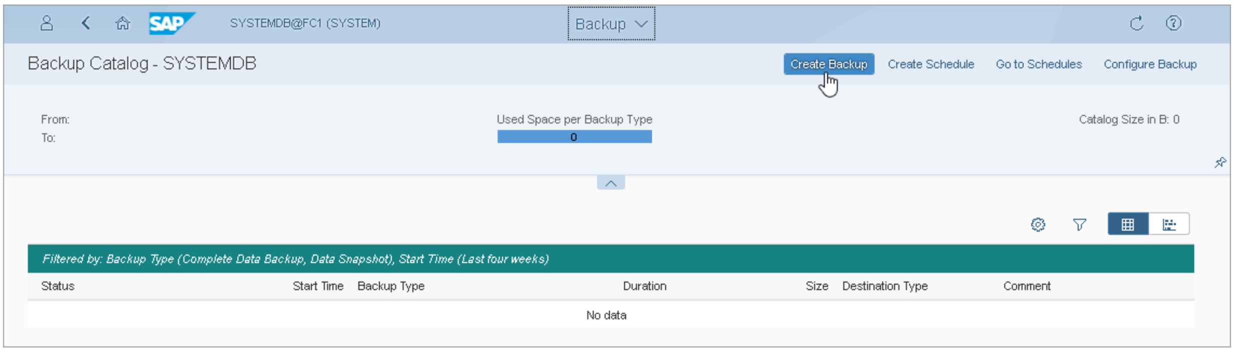
The example provided below is for demonstrating purposes only. For details on the full backup functionality of SAP HANA Cockpit, see the Create Data Backups and Delta Backups of the SAP HANA Administration Guide.

To perform Backint backup with SAP HANA Cockpit, do the following:

1. In the **System Overview** page, go to **Database Administration** and select **Manage Database Backups**.



2. At the **Backup Catalog** section, click **Create Backup**.



Filtered by: Backup Type (Complete Data Backup, Data Snapshot), Start Time (Last four weeks)

Status	Start Time	Backup Type	Duration	Size	Destination Type	Comment
			No data			

3. Specify backup settings:

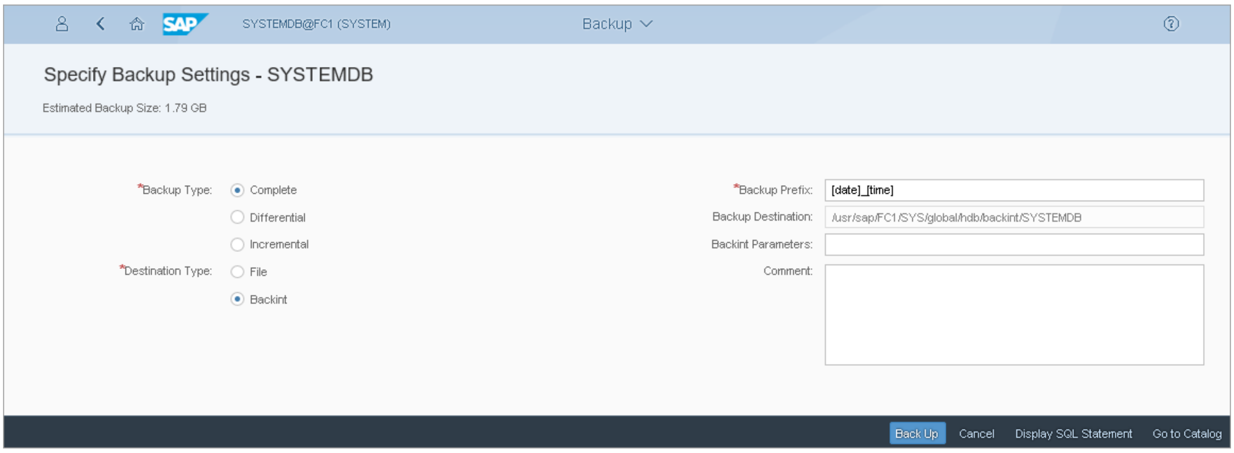
   a. Select the required backup type:

      - **Complete Data Backup**: backup of all data structures required to recover the database.
      - **Incremental Data Backup**: backup of data changed since the last full data backup or the last delta backup (incremental or differential).
      - **Differential Data Backup**: backup of data changed since the last full data backup.

   b. In the **Destination Type** setting, select *Backint*. With this option selected, Veeam Plug-in will transfer the backup to Veeam backup repository.

   c. Change the default prefix for the backup file, if needed.

   d. To start the backup, click **Back Up**.



Specify Backup Settings - SYSTEMDB

Estimated Backup Size: 1.79 GB

*Backup Type: ● Complete ○ Differential ○ Incremental

*Destination Type: ○ File ● Backint

*Backup Prefix: [date]_[time]

Backup Destination: /usr/sap/FC1/SYS/global/hdb/backint/SYSTEMDB

Backint Parameters:

Comment:

Backup Job in Veeam Backup & Replication

After you start a backup process with SAP HANA Backint, Veeam Backup & Replication creates a backup job. You can use this job to view the statistics on the backup process, generate backup job reports or you can also disable the backup job. You cannot launch or edit SAP HANA backup jobs in the Veeam Backup & Replication console. You can manage backup operations only on the SAP HANA side using SAP HANA Studio, SAP HANA Cockpit or HDBSQL.

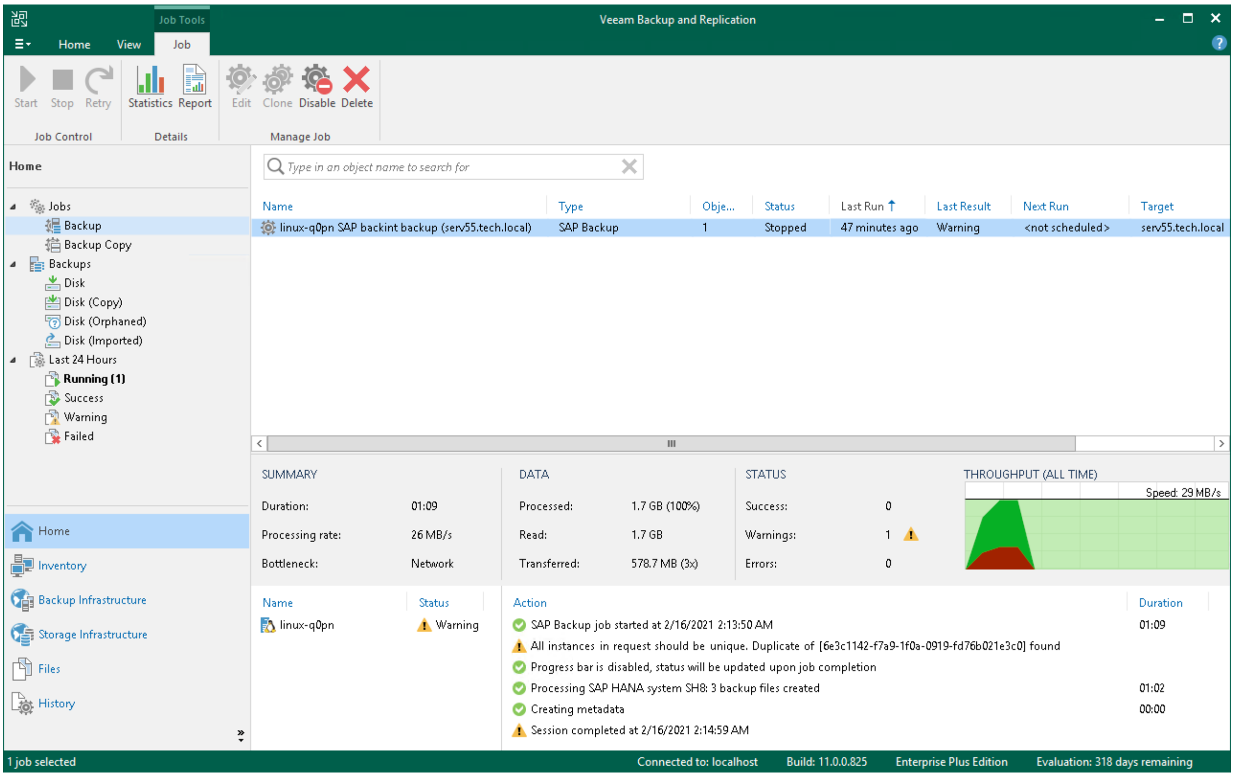
Mind the following regarding the naming of SAP HANA backup jobs:

- For a standalone SAP HANA server (scale-up), Veeam Backup & Replication generates the backup job name based on names of the SAP HANA server and selected repository.
- For a scale-out SAP HANA cluster: When you run the Veeam Plug-in configuration wizard for the first time in one of the SAP HANA cluster nodes, the wizard asks for the cluster name. The cluster name will be used in the backup job name along with the repository name.

> NOTE
>
> Due to specifics of the SAP HANA backup process, the progress bar of a running SAP HANA backup job is not available.

To view details of a backup job process, do the following.

1. Open the Veeam Backup & Replication console.
2. In the **Home** view, expand the **Jobs** node and click **Backup**.
3. In the list of jobs, select the SAP HANA backup job to see details of the current backup process or the last backup job session.



Name	Type	Obje...	Status	Last Run	Last Result	Next Run	Target
linux-q0pn SAP backint backup (serv55.tech.local)	SAP Backup	1	Stopped	47 minutes ago	Warning	<not scheduled>	serv55.tech.local

SUMMARY		DATA		STATUS	
Duration:	01:09	Processed:	1.7 GB (100%)	Success:	0
Processing rate:	26 MB/s	Read:	1.7 GB	Warnings:	1 ⚠
Bottleneck:	Network	Transferred:	578.7 MB (3x)	Errors:	0

THROUGHPUT (ALL TIME)

Name	Status
linux-q0pn	⚠ Warning

Action	Duration
✓ SAP Backup job started at 2/16/2021 2:13:50 AM	01:09
⚠ All instances in request should be unique. Duplicate of [6e3c1142-f7a9-1f0a-0919-fd76b021e3c0] found	
✓ Progress bar is disabled, status will be updated upon job completion	
✓ Processing SAP HANA system SH8: 3 backup files created	01:02
✓ Creating metadata	00:00
⚠ Session completed at 2/16/2021 2:14:59 AM	

1 job selected Connected to: localhost Build: 11.0.0.825 Enterprise Plus Edition Evaluation: 318 days remaining

Generating Backup Job Reports

Veeam Backup & Replication can generate reports with details about an SAP HANA backup job session performance. The session report contains the following session statistics: session duration details, details of the session performance, amount of read, processed and transferred data, backup size, compression ratio, list of warnings and errors (if any).

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the necessary job and click **Report** on the ribbon. You can also right-click the job and select **Report**.

Disabling Backup Job

You can disable SAP HANA backup jobs in the Veeam Backup & Replication console. If you disable the job, you will not be able to run SAP Backint backup commands on the SAP HANA server.

To disable a backup job:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the necessary job and click **Disable** on the ribbon. You can also right-click the job and select **Disable**.

Database Recovery

With the configured Veeam Plug-in you can restore SAP HANA databases from the backups that reside on the Veeam backup repository. All restore operations are performed on the SAP HANA side. To restore databases, you can use SAP HANA Cockpit, SAP HANA Studio, or HDBSQL.

Keep in mind that examples provided in this section are for demonstrating purposes only. To see the full restore functionality of SAP HANA tools, see the SAP HANA Recovery section of SAP HANA Administration Guide.

To learn how to recover SAP HANA databases from backups stored on Veeam repositories, see:

- Recovering Databases Using SQL Commands
- Recovering Databases with SAP HANA Studio
- Recovering SYSTEMDB with SAP HANA Cockpit
- Recovering Tenant Databases with SAP HANA Cockpit
- Recovering Databases to Other Servers
- Restore from Backup Copy
- Restore from Hardened Repository

Restoring Databases (HDBSQL Commands)

You can use HDBSQL to restore SAP HANA databases from backups stored on Veeam backup repositories. For details on the HDBSQL restore, see the RECOVER DATABASE Statement section of the SAP HANA SQL and System Views Reference.

To recover SAP HANA databases from backups stored on Veeam backup repositories, do the following:

1. Log in to SAP HANA HDBSQL as the HDB administrator. Use HDBUSERSTORE to securely store connection details on a client machine. For details, see the Secure User Store section of the SAP HANA Security Guide.

```
sh4adm@linux-q0pn:/usr/sap/SH4/HDB01> hdbuserstore SET <key> hostname:3001
3@SID <username> <password>
sh4adm@linux-q0pn:/usr/sap/SH4/HDB01> hdbsql -U <key>
```

2. Recover a tenant database to the latest state using Backint. As the timestamp, specify the current data and time or future date and time.

```
alter stop database <DATABASE_NAME>;
recover database for <DATABASE_NAME> until timestamp '2020-01-01 12:00:00'
using catalog backint;
```

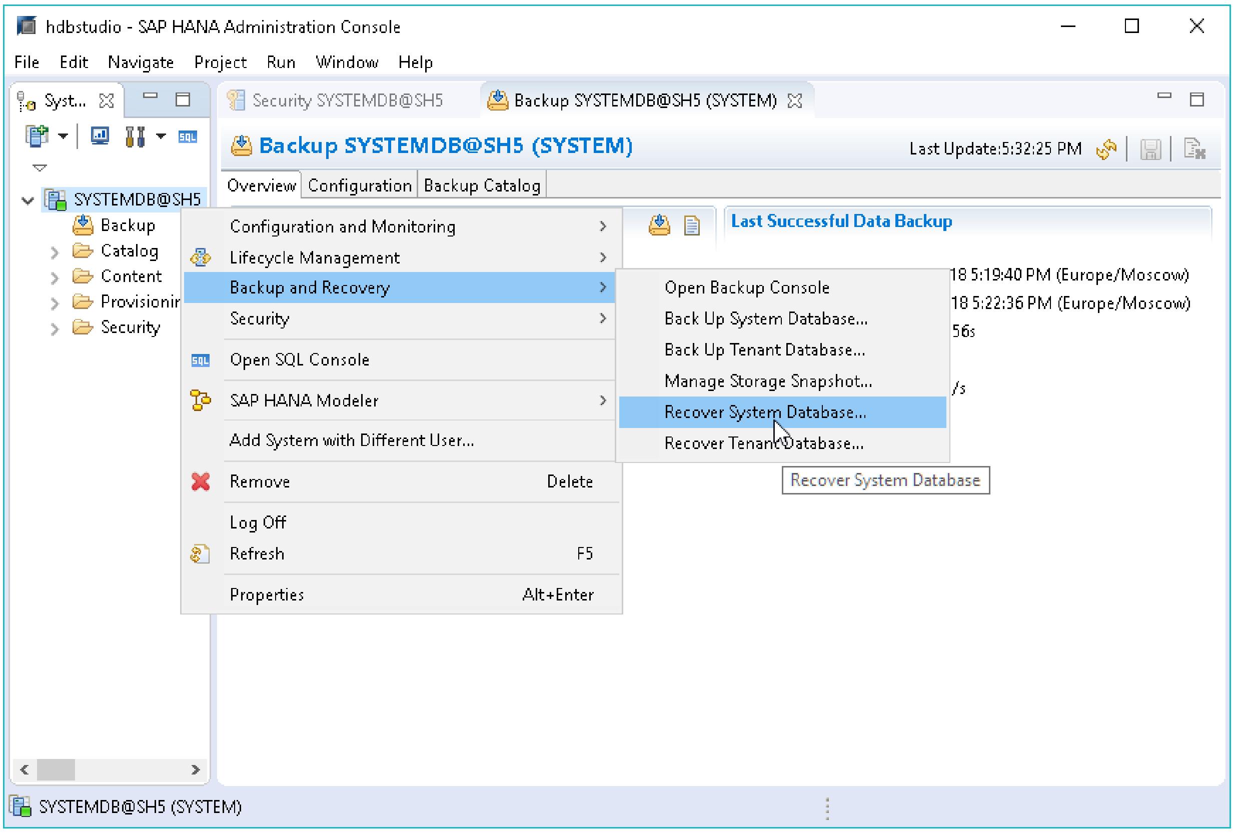
Restoring Databases (SAP HANA Studio)

You can restore SAP HANA databases from the Veeam Plug-in backups using SAP HANA Studio.

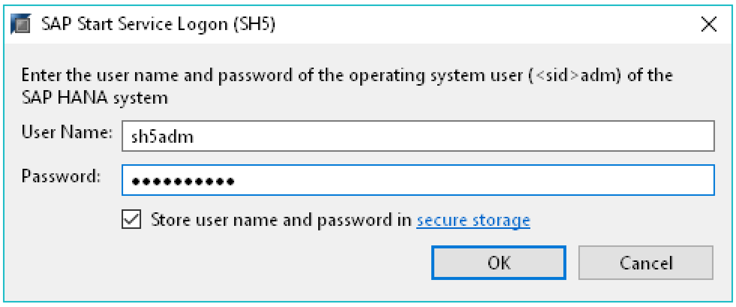
The example below is provided for demonstration purposes only. For details on the full restore functionality of SAP HANA tools, see the Recovering an SAP Database section of the SAP HANA Administration Guide.

To perform a Backint recovery from Veeam Plug-in backups, do the following:

1. Log in to SYSTEMDB as a user with DATABASE ADMIN privileges.
2. Right-click the SYSTEMDB database.
3. Click **Backup and Recovery** and select **Recover System Database** or **Recover Tenant Database**.


hdbstudio - SAP HANA Administration Console
File Edit Navigate Project Run Window Help
Syst...
SYSTEMDB@SH5
Backup
Catalog
Content
Provisionir
Security
Security SYSTEMDB@SH5
Backup SYSTEMDB@SH5 (SYSTEM)
Last Update:5:32:25 PM
Overview Configuration Backup Catalog
Last Successful Data Backup
Configuration and Monitoring
Lifecycle Management
Backup and Recovery
Security
Open SQL Console
SAP HANA Modeler
Add System with Different User...
Remove Delete
Log Off
Refresh F5
Properties Alt+Enter
Open Backup Console
Back Up System Database...
Back Up Tenant Database...
Manage Storage Snapshot...
Recover System Database...
Recover Tenant Database...
Recover System Database
18 5:19:40 PM (Europe/Moscow)
18 5:22:36 PM (Europe/Moscow)
56s
/s
SYSTEMDB@SH5 (SYSTEM)

4. Enter the operating system user credentials.



SAP Start Service Logon (SH5)

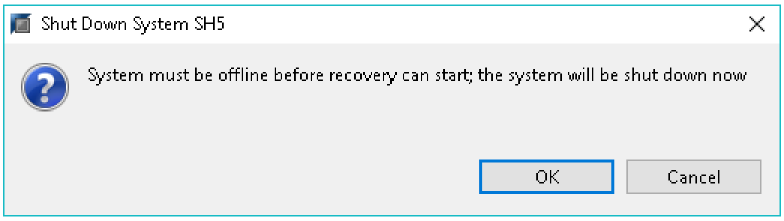
Enter the user name and password of the operating system user (<sid>adm) of the SAP HANA system

User Name: sh5adm

Password: ●●●●●●●●●●●

☑ Store user name and password in secure storage

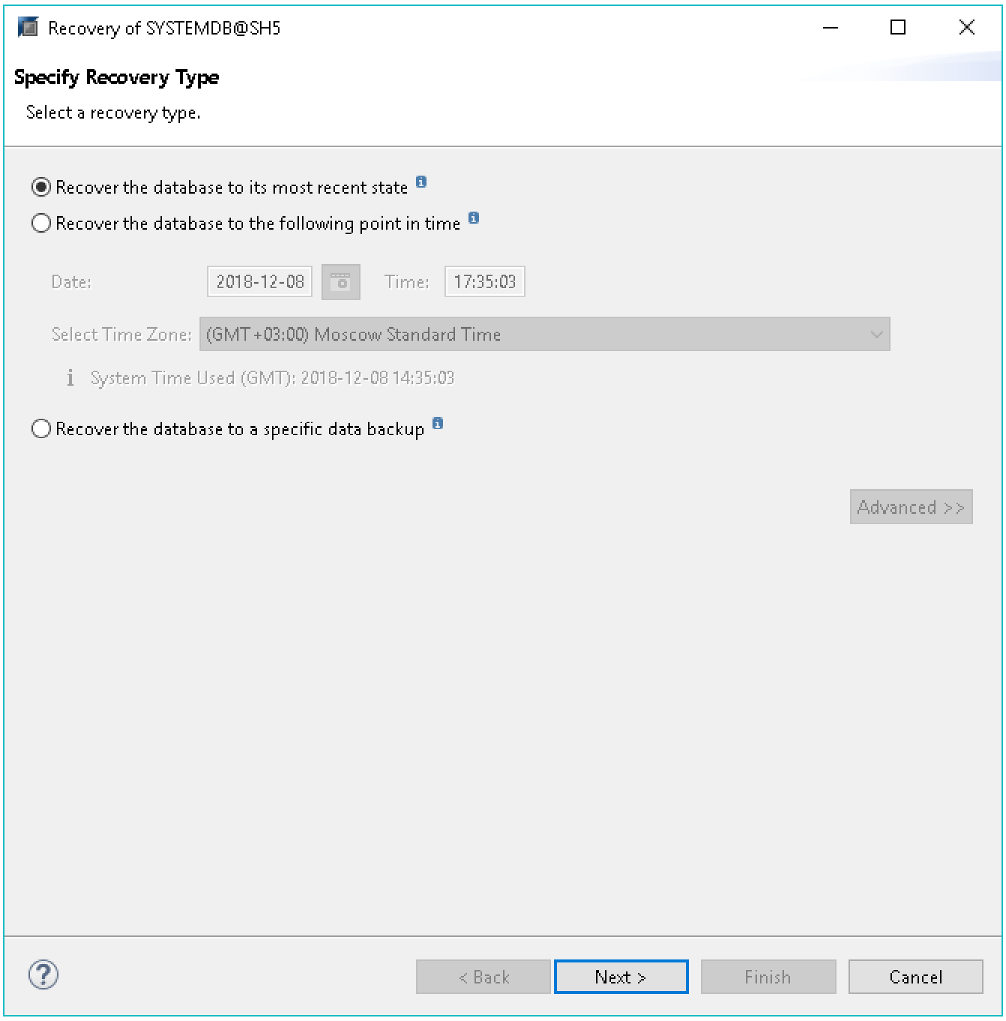
5. Recovery process requires the database to be shut down. In the pop-up window, click **OK** to confirm the database shutdown.



Shut Down System SH5

System must be offline before recovery can start; the system will be shut down now

6. At the **Specify Recovery Type** step of the recovery wizard, select the required restore point or the option to restore the database to the most recent state.



Recovery of SYSTEMDB@SH5

Specify Recovery Type

Select a recovery type.

● Recover the database to its most recent state

○ Recover the database to the following point in time

Date: 2018-12-08 Time: 17:35:03

Select Time Zone: (GMT+03:00) Moscow Standard Time

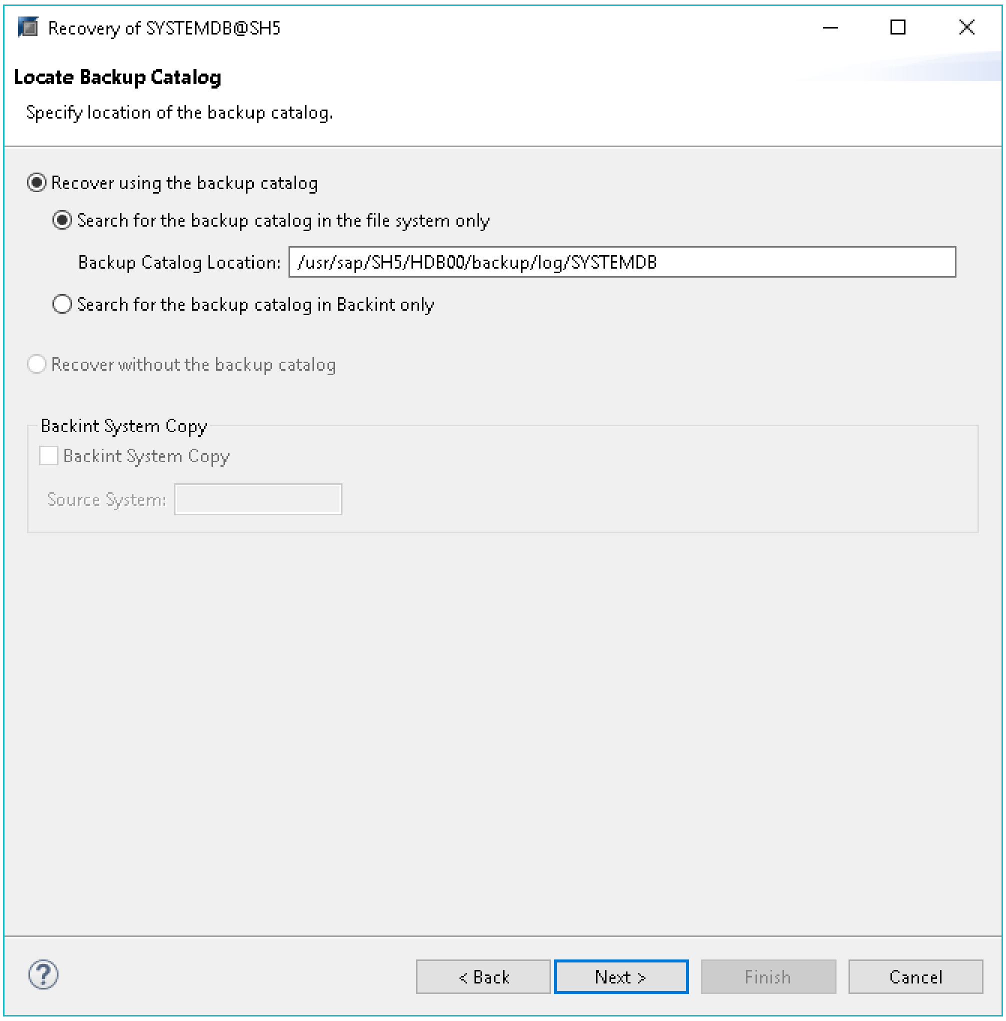
System Time Used (GMT): 2018-12-08 14:35:03

○ Recover the database to a specific data backup

7. At the **Locate Backup Catalog** step of the wizard, select one of the following, depending on where your backup catalogs reside:

   ○ **Search for the backup catalog in the file system only**.

   ○ **Search for the backup catalog in Backint only**.



Recovery of SYSTEMDB@SH5

Locate Backup Catalog

Specify location of the backup catalog.

● Recover using the backup catalog

● Search for the backup catalog in the file system only

Backup Catalog Location: /usr/sap/SH5/HDB00/backup/log/SYSTEMDB

○ Search for the backup catalog in Backint only

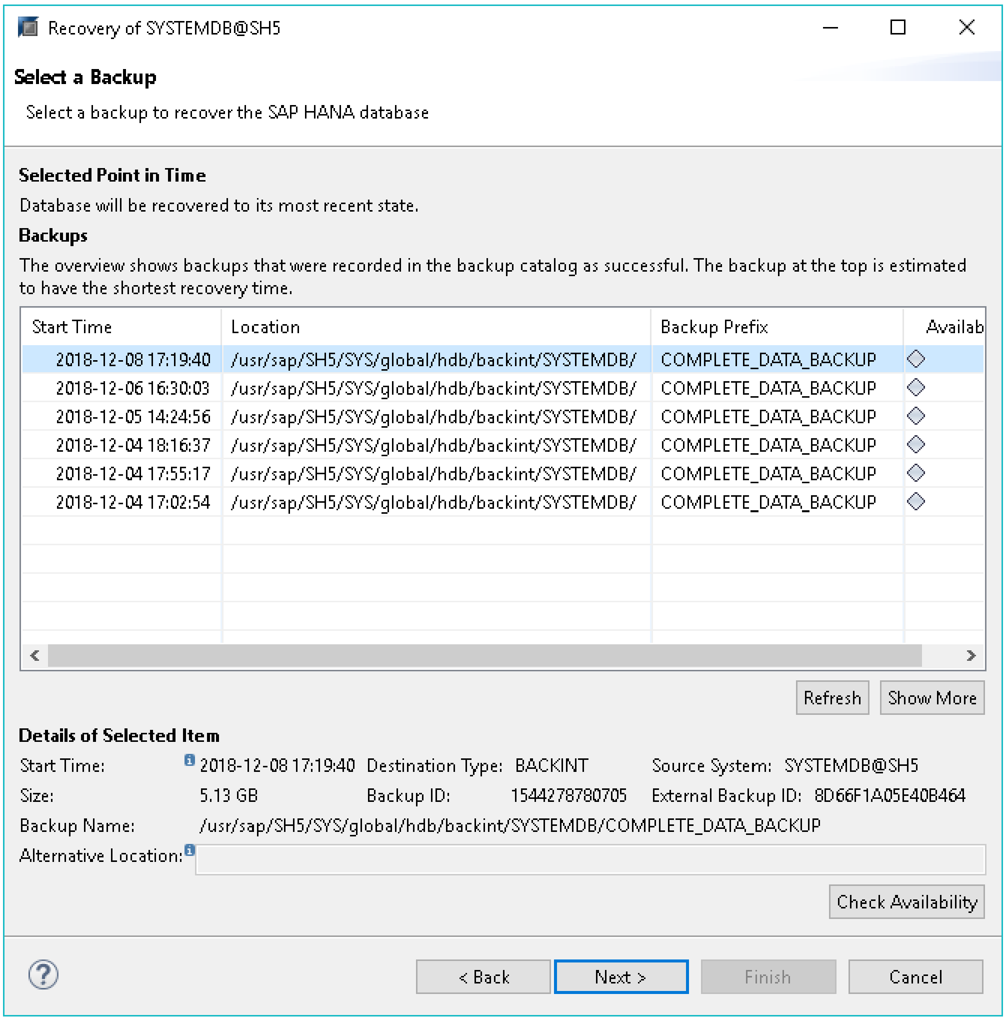
○ Recover without the backup catalog

Backint System Copy

□ Backint System Copy

Source System:

8. Select the required backup to restore.



Recovery of SYSTEMDB@SH5

Select a Backup

Select a backup to recover the SAP HANA database

Selected Point in Time

Database will be recovered to its most recent state.

Backups

The overview shows backups that were recorded in the backup catalog as successful. The backup at the top is estimated to have the shortest recovery time.

Start Time	Location	Backup Prefix	Availab
2018-12-08 17:19:40	/usr/sap/SH5/SYS/global/hdb/backint/SYSTEMDB/	COMPLETE_DATA_BACKUP	◇
2018-12-06 16:30:03	/usr/sap/SH5/SYS/global/hdb/backint/SYSTEMDB/	COMPLETE_DATA_BACKUP	◇
2018-12-05 14:24:56	/usr/sap/SH5/SYS/global/hdb/backint/SYSTEMDB/	COMPLETE_DATA_BACKUP	◇
2018-12-04 18:16:37	/usr/sap/SH5/SYS/global/hdb/backint/SYSTEMDB/	COMPLETE_DATA_BACKUP	◇
2018-12-04 17:55:17	/usr/sap/SH5/SYS/global/hdb/backint/SYSTEMDB/	COMPLETE_DATA_BACKUP	◇
2018-12-04 17:02:54	/usr/sap/SH5/SYS/global/hdb/backint/SYSTEMDB/	COMPLETE_DATA_BACKUP	◇

Details of Selected Item

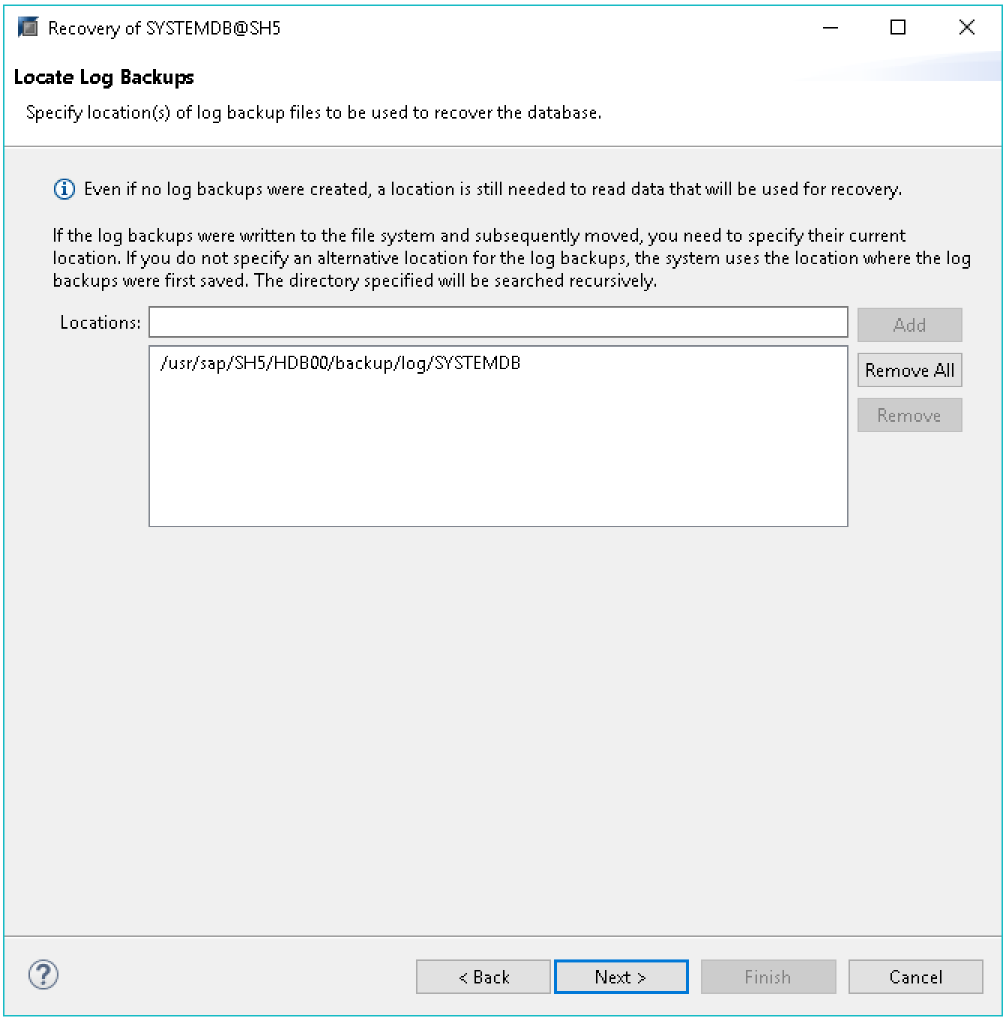
Start Time: 2018-12-08 17:19:40 Destination Type: BACKINT Source System: SYSTEMDB@SH5

Size: 5.13 GB Backup ID: 1544278780705 External Backup ID: 8D66F1A05E40B464

Backup Name: /usr/sap/SH5/SYS/global/hdb/backint/SYSTEMDB/COMPLETE_DATA_BACKUP

Alternative Location:

9. At the **Locate Log Backups** step, click **Next**.



Recovery of SYSTEMDB@SH5

Locate Log Backups

Specify location(s) of log backup files to be used to recover the database.

Even if no log backups were created, a location is still needed to read data that will be used for recovery.

If the log backups were written to the file system and subsequently moved, you need to specify their current location. If you do not specify an alternative location for the log backups, the system uses the location where the log backups were first saved. The directory specified will be searched recursively.

Locations:

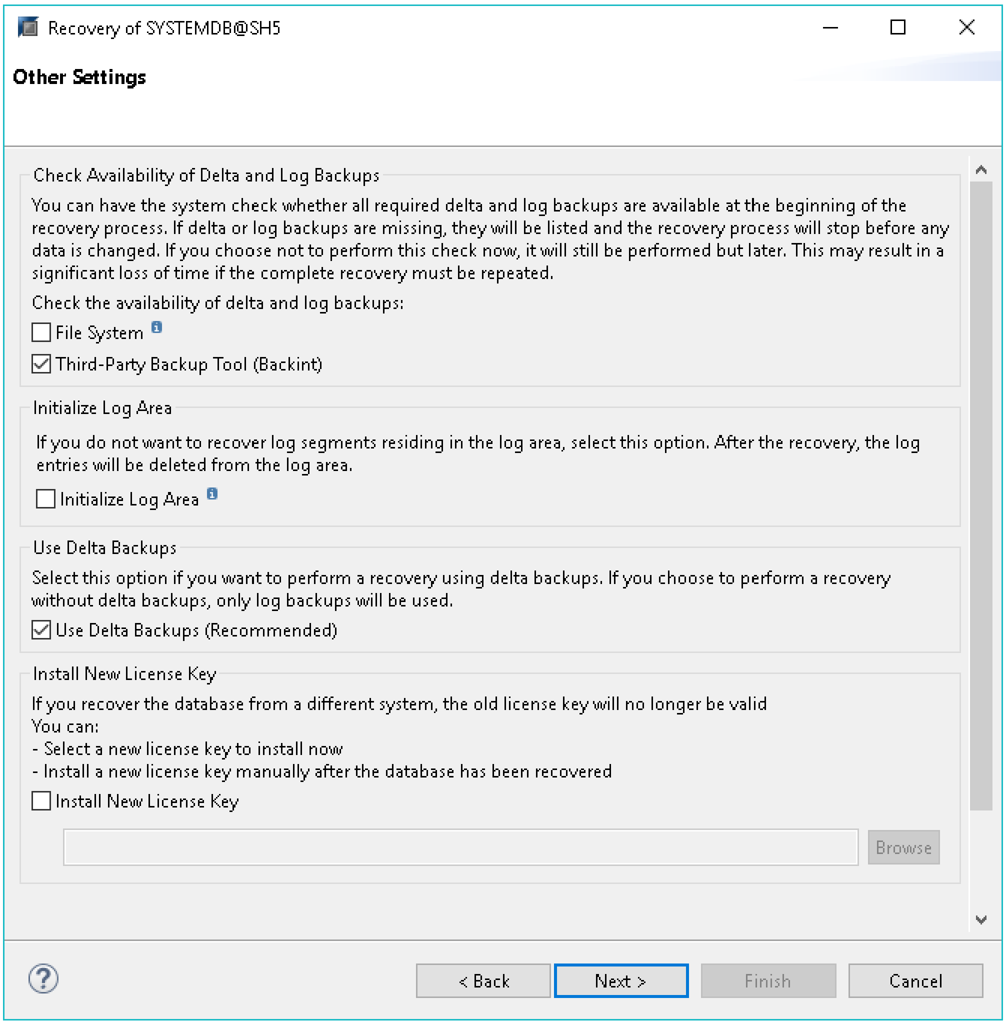
/usr/sap/SH5/HDB00/backup/log/SYSTEMDB

10. At the **Other Settings** step:

    a. Switch on the availability check for the Backint backups.

    b. If you are recovering the database to a database with a new SID or landscape ID, select the **Install New License Key** check box and specify the path to the license file.

    c. Click **Next**.



Recovery of SYSTEMDB@SH5

Other Settings

Check Availability of Delta and Log Backups

You can have the system check whether all required delta and log backups are available at the beginning of the recovery process. If delta or log backups are missing, they will be listed and the recovery process will stop before any data is changed. If you choose not to perform this check now, it will still be performed but later. This may result in a significant loss of time if the complete recovery must be repeated.

Check the availability of delta and log backups:

□ File System

☑ Third-Party Backup Tool (Backint)

Initialize Log Area

If you do not want to recover log segments residing in the log area, select this option. After the recovery, the log entries will be deleted from the log area.

□ Initialize Log Area

Use Delta Backups

Select this option if you want to perform a recovery using delta backups. If you choose to perform a recovery without delta backups, only log backups will be used.

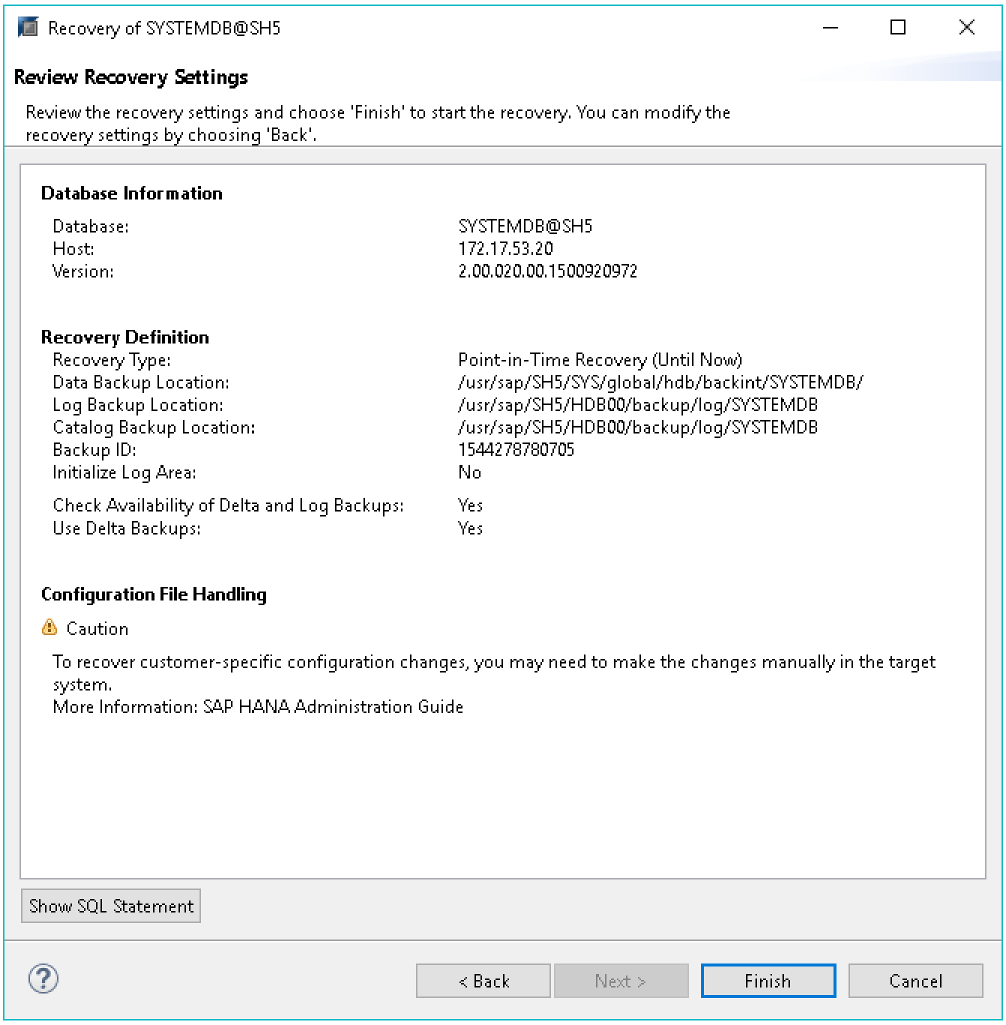
☑ Use Delta Backups (Recommended)

Install New License Key

If you recover the database from a different system, the old license key will no longer be valid
You can:
- Select a new license key to install now
- Install a new license key manually after the database has been recovered

□ Install New License Key

11. At the **Review Recovery Settings** step, click **Finish**.



Recovery of SYSTEMDB@SH5

Review Recovery Settings

Review the recovery settings and choose 'Finish' to start the recovery. You can modify the recovery settings by choosing 'Back'.

Database Information

Database:	SYSTEMDB@SH5
Host:	172.17.53.20
Version:	2.00.020.00.1500920972

Recovery Definition

Recovery Type:	Point-in-Time Recovery (Until Now)
Data Backup Location:	/usr/sap/SH5/SYS/global/hdb/backint/SYSTEMDB/
Log Backup Location:	/usr/sap/SH5/HDB00/backup/log/SYSTEMDB
Catalog Backup Location:	/usr/sap/SH5/HDB00/backup/log/SYSTEMDB
Backup ID:	1544278780705
Initialize Log Area:	No
Check Availability of Delta and Log Backups:	Yes
Use Delta Backups:	Yes

Configuration File Handling

⚠ Caution

To recover customer-specific configuration changes, you may need to make the changes manually in the target system.
More Information: SAP HANA Administration Guide

Restoring SYSTEMDB (SAP HANA Cockpit)

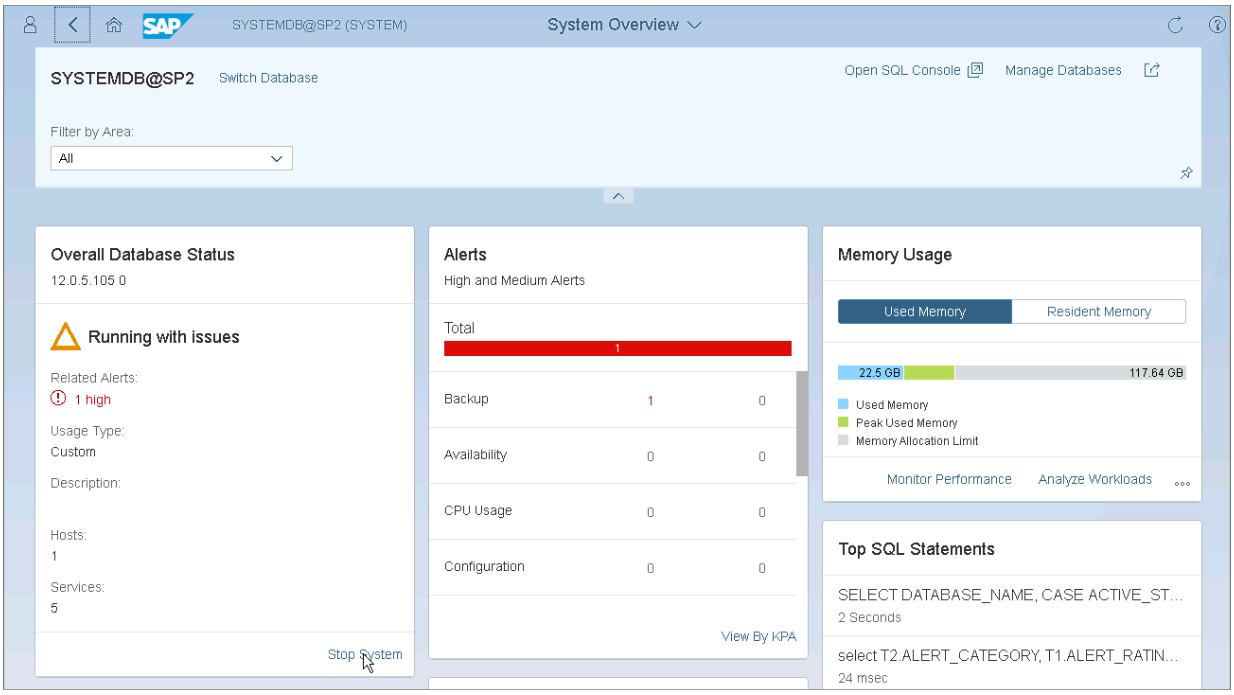
You can restore SAP HANA SYSTEMDB databases from the Veeam Plug-in backups using SAP HANA Cockpit.

The example below is provided for demonstration purposes only. For details on the full restore functionality of SAP HANA Cockpit, see the Recovering an SAP HANA Database section of the SAP HANA Administration Guide.

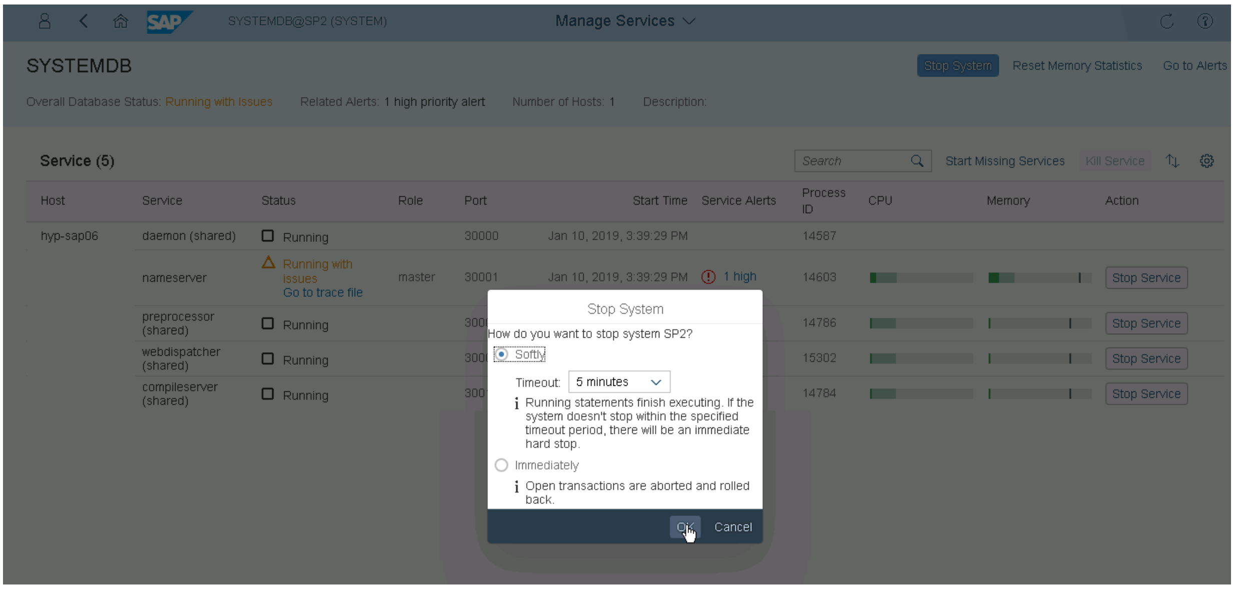
Before You Begin

Before you start the recovery, shut down the database that you want to recover:

1. In the SAP HANA Cockpit console, locate the database that you want to recover.
2. In the **Overall Database Status** block, click **Stop System**.



3. At the **Manage Services** section, click **Stop System** and select the **Softly** option to shut down the database after SAP HANA finishes running statements.



SYSTEMDB@SP2 (SYSTEM) Manage Services

SYSTEMDB

Stop System Reset Memory Statistics Go to Alerts

Overall Database Status: Running with issues Related Alerts: 1 high priority alert Number of Hosts: 1 Description:

Service (5)

Search Start Missing Services Kill Service

Host	Service	Status	Role	Port	Start Time	Service Alerts	Process ID	CPU	Memory	Action
hyp-sap06	daemon (shared)	□ Running		30000	Jan 10, 2019, 3:39:29 PM		14587			
	nameserver	Running with issues Go to trace file	master	30001	Jan 10, 2019, 3:39:29 PM	1 high	14603			Stop Service
	preprocessor (shared)	□ Running		300			14786			Stop Service
	webdispatcher (shared)	□ Running		300			15302			Stop Service
	compileserver (shared)	□ Running		300			14784			Stop Service

Stop System

How do you want to stop system SP2?

● Softly

Timeout: 5 minutes

i Running statements finish executing. If the system doesn't stop within the specified timeout period, there will be an immediate hard stop.

○ Immediately

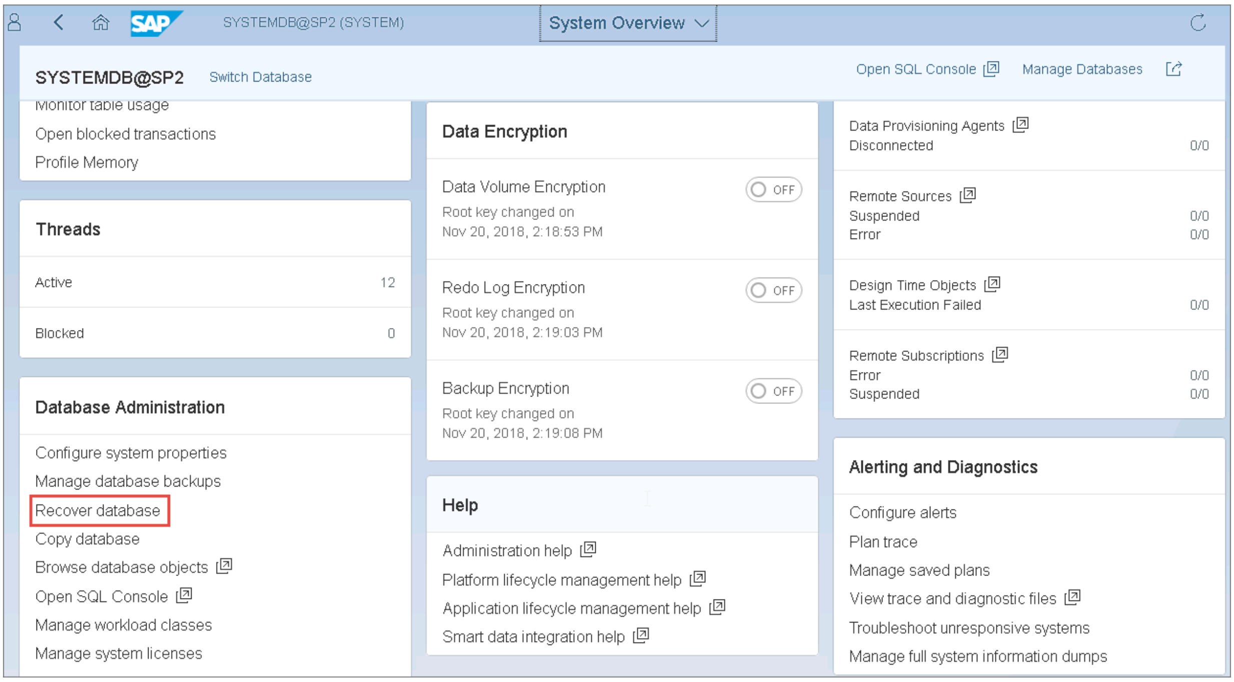
i Open transactions are aborted and rolled back.

OK Cancel

Performing Recovery

To perform a Backint recovery of SYSTEMDB from a Veeam Plug-in backup, do the following:

1. In the **System Overview** block, go to the **Database Administration** section and click **Recover database.**



SYSTEMDB@SP2 (SYSTEM) System Overview

SYSTEMDB@SP2 Switch Database — Open SQL Console — Manage Databases

Monitor table usage
Open blocked transactions
Profile Memory

Threads

Active	12
Blocked	0

Database Administration

Configure system properties
Manage database backups
Recover database
Copy database
Browse database objects
Open SQL Console
Manage workload classes
Manage system licenses

Data Encryption

Data Volume Encryption — OFF
Root key changed on
Nov 20, 2018, 2:18:53 PM

Redo Log Encryption — OFF
Root key changed on
Nov 20, 2018, 2:19:03 PM

Backup Encryption — OFF
Root key changed on
Nov 20, 2018, 2:19:08 PM

Help

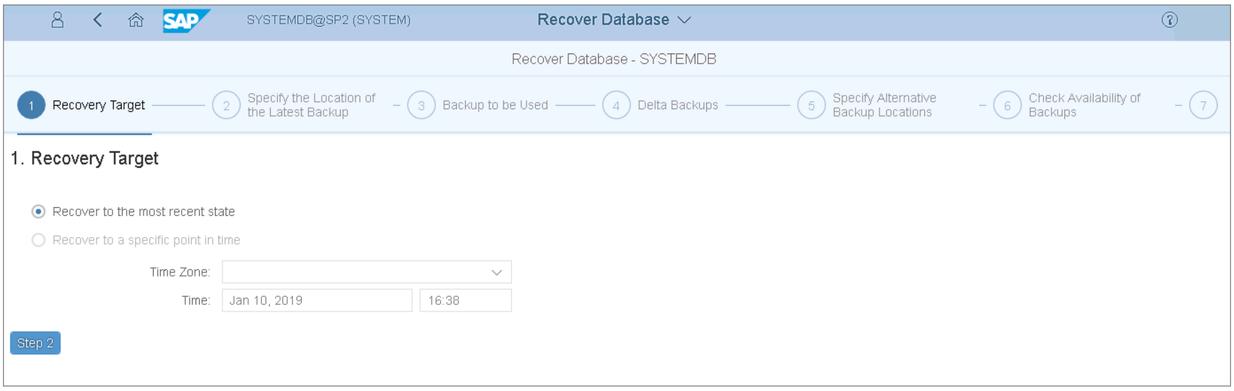
Administration help
Platform lifecycle management help
Application lifecycle management help
Smart data integration help

Data Provisioning Agents	
Disconnected	0/0
Remote Sources	
Suspended	0/0
Error	0/0
Design Time Objects	
Last Execution Failed	0/0
Remote Subscriptions	
Error	0/0
Suspended	0/0

Alerting and Diagnostics

Configure alerts
Plan trace
Manage saved plans
View trace and diagnostic files
Troubleshoot unresponsive systems
Manage full system information dumps

2. At the **Recovery Target** step, select the required restore point or the option to restore the database to the most recent state. Then, click **Step 2.**



SYSTEMDB@SP2 (SYSTEM) Recover Database

Recover Database - SYSTEMDB

1 Recovery Target — 2 Specify the Location of the Latest Backup — 3 Backup to be Used — 4 Delta Backups — 5 Specify Alternative Backup Locations — 6 Check Availability of Backups — 7

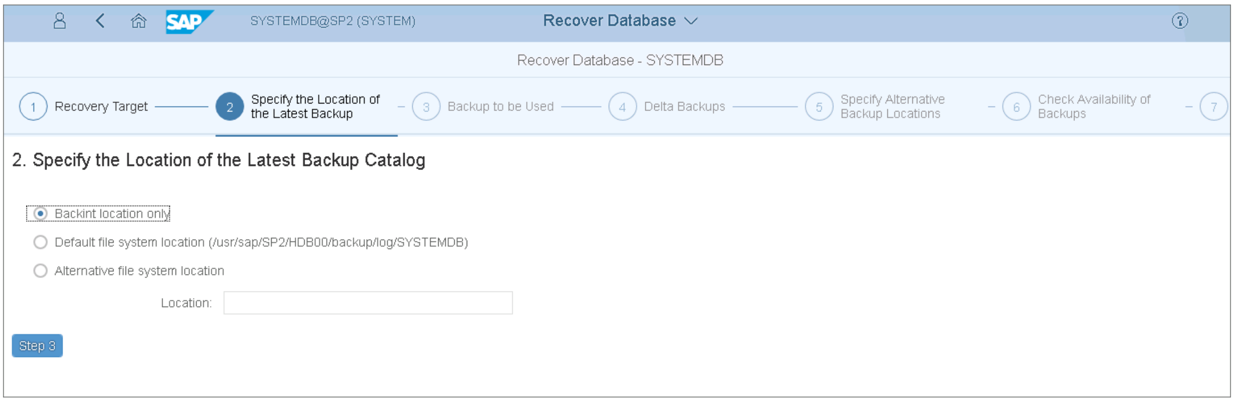
1. Recovery Target

● Recover to the most recent state
○ Recover to a specific point in time

Time Zone:
Time: Jan 10, 2019 16:38

Step 2

3. Specify the location of the latest backup catalog and click **Step 3.**



SYSTEMDB@SP2 (SYSTEM) Recover Database

Recover Database - SYSTEMDB

1 Recovery Target — 2 Specify the Location of the Latest Backup — 3 Backup to be Used — 4 Delta Backups — 5 Specify Alternative Backup Locations — 6 Check Availability of Backups — 7

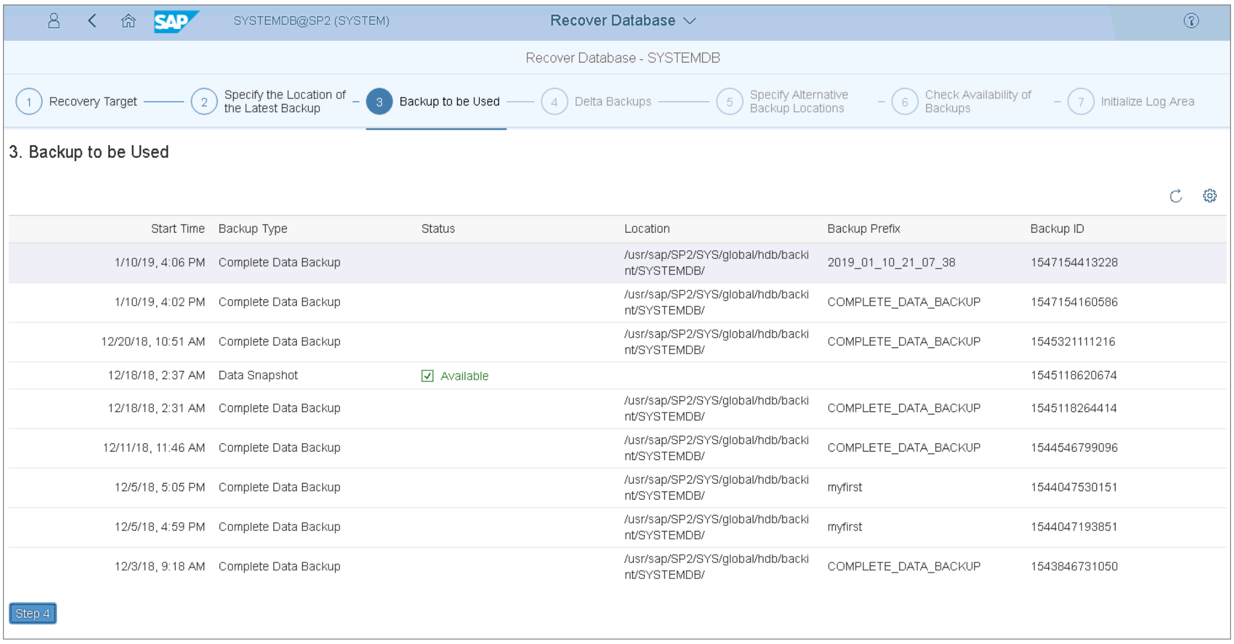
2. Specify the Location of the Latest Backup Catalog

● Backint location only
○ Default file system location (/usr/sap/SP2/HDB00/backup/log/SYSTEMDB)
○ Alternative file system location

Location:

Step 3

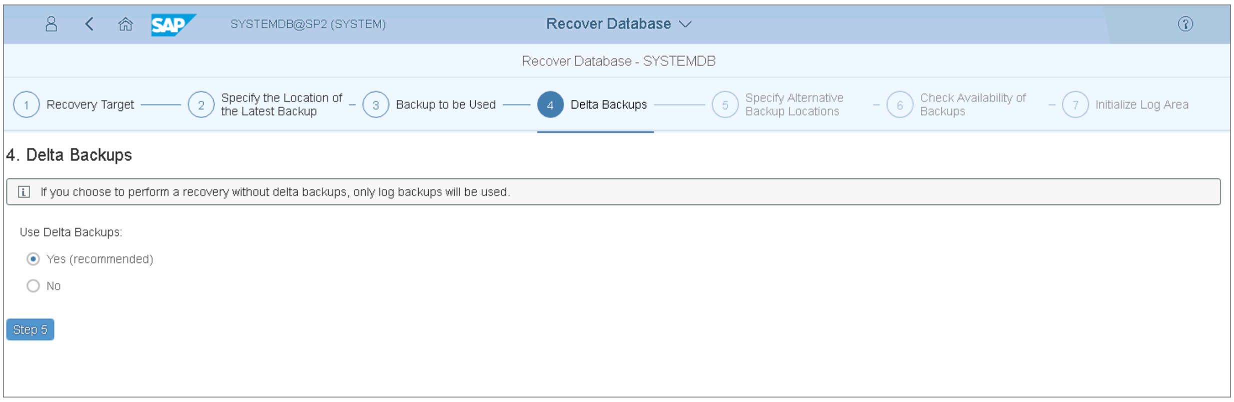
4. At the **Backup to be Used** step, select the backup and click **Step 4**.


SYSTEMDB@SP2 (SYSTEM)
Recover Database
Recover Database - SYSTEMDB
1 Recovery Target
2 Specify the Location of the Latest Backup
3 Backup to be Used
4 Delta Backups
5 Specify Alternative Backup Locations
6 Check Availability of Backups
7 Initialize Log Area

3. Backup to be Used

Start Time	Backup Type	Status	Location	Backup Prefix	Backup ID
1/10/19, 4:06 PM	Complete Data Backup		/usr/sap/SP2/SYS/global/hdb/backint/SYSTEMDB/	2019_01_10_21_07_38	1547154413228
1/10/19, 4:02 PM	Complete Data Backup		/usr/sap/SP2/SYS/global/hdb/backint/SYSTEMDB/	COMPLETE_DATA_BACKUP	1547154160586
12/20/18, 10:51 AM	Complete Data Backup		/usr/sap/SP2/SYS/global/hdb/backint/SYSTEMDB/	COMPLETE_DATA_BACKUP	1545321111216
12/18/18, 2:37 AM	Data Snapshot	☑ Available			1545118620674
12/18/18, 2:31 AM	Complete Data Backup		/usr/sap/SP2/SYS/global/hdb/backint/SYSTEMDB/	COMPLETE_DATA_BACKUP	1545118264414
12/11/18, 11:46 AM	Complete Data Backup		/usr/sap/SP2/SYS/global/hdb/backint/SYSTEMDB/	COMPLETE_DATA_BACKUP	1544546799096
12/5/18, 5:05 PM	Complete Data Backup		/usr/sap/SP2/SYS/global/hdb/backint/SYSTEMDB/	myfirst	1544047530151
12/5/18, 4:59 PM	Complete Data Backup		/usr/sap/SP2/SYS/global/hdb/backint/SYSTEMDB/	myfirst	1544047193851
12/3/18, 9:18 AM	Complete Data Backup		/usr/sap/SP2/SYS/global/hdb/backint/SYSTEMDB/	COMPLETE_DATA_BACKUP	1543846731050

5. At the **Delta Backups** step, select **Yes** to use delta backups.


SYSTEMDB@SP2 (SYSTEM)
Recover Database
Recover Database - SYSTEMDB
1 Recovery Target
2 Specify the Location of the Latest Backup
3 Backup to be Used
4 Delta Backups
5 Specify Alternative Backup Locations
6 Check Availability of Backups
7 Initialize Log Area

4. Delta Backups

If you choose to perform a recovery without delta backups, only log backups will be used.

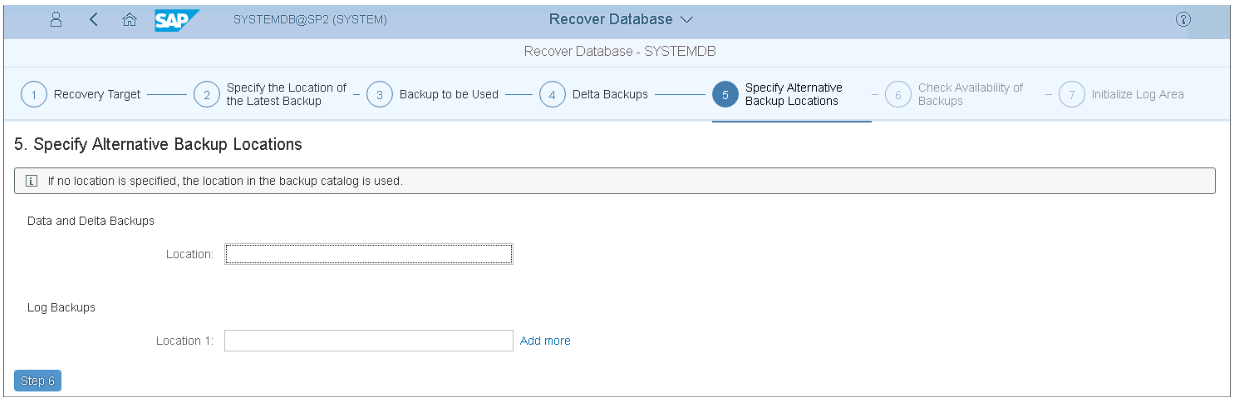
Use Delta Backups:

● Yes (recommended)

○ No

6. At the **Specify Alternative Backup Locations** step, if you want to use backups that are not in the backup catalog, specify their locations. You can also change the location for log backups.

   If you you leave the fields empty, SAP HANA will use the locations specified in the backup catalog.


SYSTEMDB@SP2 (SYSTEM)
Recover Database
Recover Database - SYSTEMDB
1 Recovery Target
2 Specify the Location of the Latest Backup
3 Backup to be Used
4 Delta Backups
5 Specify Alternative Backup Locations
6 Check Availability of Backups
7 Initialize Log Area

5. Specify Alternative Backup Locations

If no location is specified, the location in the backup catalog is used.

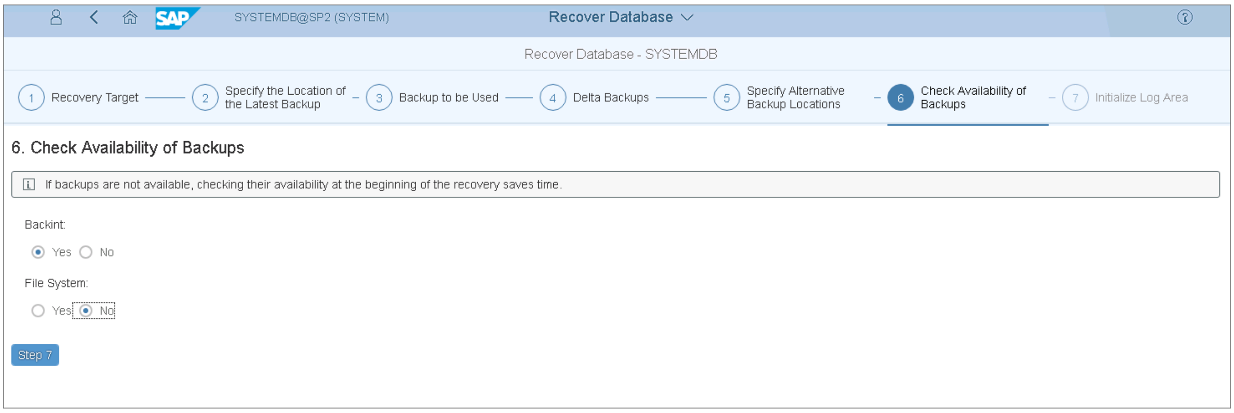
Data and Delta Backups

Location:

Log Backups

Location 1:

7. At the **Check Availability of Backups** step, select **Yes** or **No** options, to check if the backups are available. Note that at this step SAP HANA does not check the integrity of the backup content on the block level.


SYSTEMDB@SP2 (SYSTEM)
Recover Database
Recover Database - SYSTEMDB
1 Recovery Target
2 Specify the Location of the Latest Backup
3 Backup to be Used
4 Delta Backups
5 Specify Alternative Backup Locations
6 Check Availability of Backups
7 Initialize Log Area
Step 7

6. Check Availability of Backups

If backups are not available, checking their availability at the beginning of the recovery saves time.

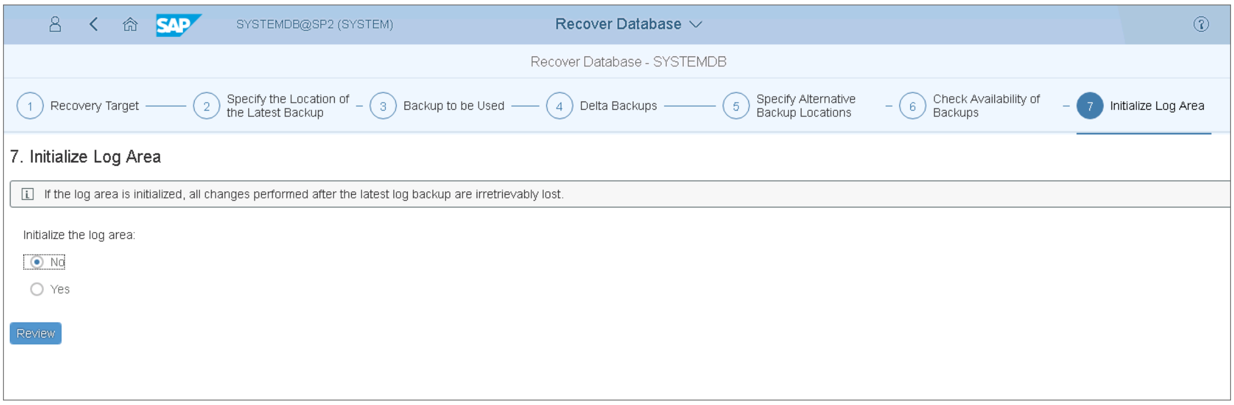
Backint:

● Yes ○ No

File System:

○ Yes ● No

8. At the **Initialize Log Area** step, select **No** to initialize the log area and click **Review**. You must initialize the log area only if the log area is unavailable or if you are recovering the database to a different system.


SYSTEMDB@SP2 (SYSTEM)
Recover Database
Recover Database - SYSTEMDB
1 Recovery Target
2 Specify the Location of the Latest Backup
3 Backup to be Used
4 Delta Backups
5 Specify Alternative Backup Locations
6 Check Availability of Backups
7 Initialize Log Area
Review

7. Initialize Log Area

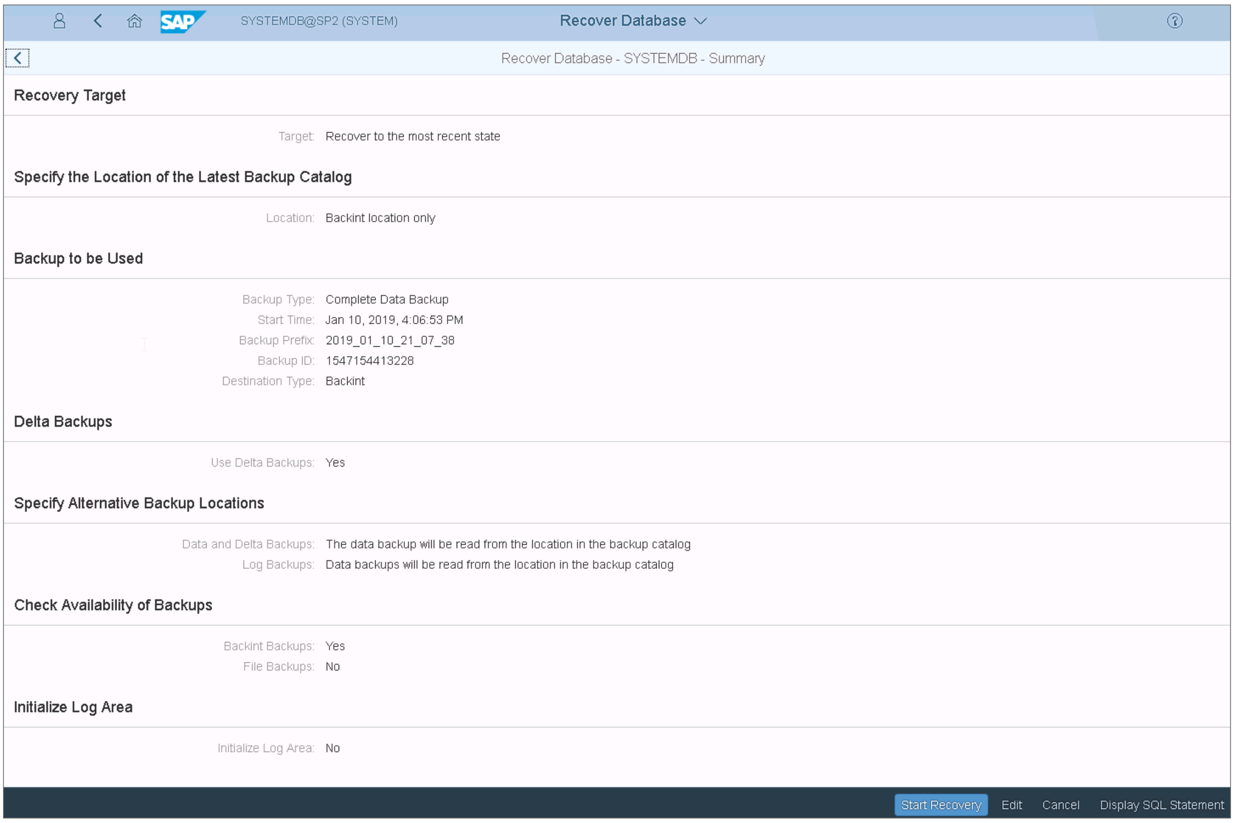
If the log area is initialized, all changes performed after the latest log backup are irretrievably lost.

Initialize the log area:

● No

○ Yes

9. Review the recovery options and click **Start Recovery**.



Recover Database - SYSTEMDB - Summary

Recovery Target

Target: Recover to the most recent state

Specify the Location of the Latest Backup Catalog

Location: Backint location only

Backup to be Used

Backup Type: Complete Data Backup
Start Time: Jan 10, 2019, 4:06:53 PM
Backup Prefix: 2019_01_10_21_07_38
Backup ID: 1547154413228
Destination Type: Backint

Delta Backups

Use Delta Backups: Yes

Specify Alternative Backup Locations

Data and Delta Backups: The data backup will be read from the location in the backup catalog
Log Backups: Data backups will be read from the location in the backup catalog

Check Availability of Backups

Backint Backups: Yes
File Backups: No

Initialize Log Area

Initialize Log Area: No

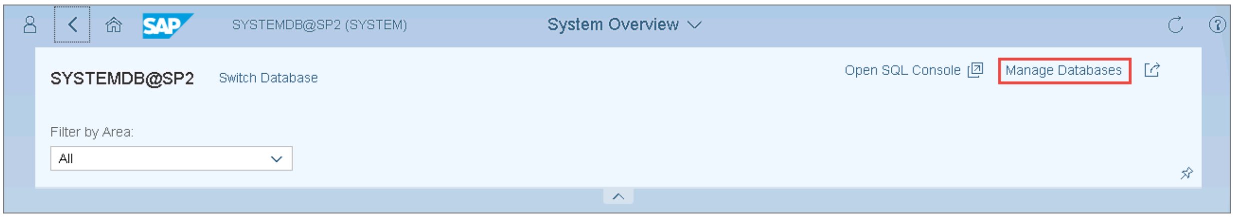
Recovering Tenant Databases with SAP HANA Cockpit

You can restore SAP HANA tenant databases from the Veeam Plug-in backups using SAP HANA Cockpit.

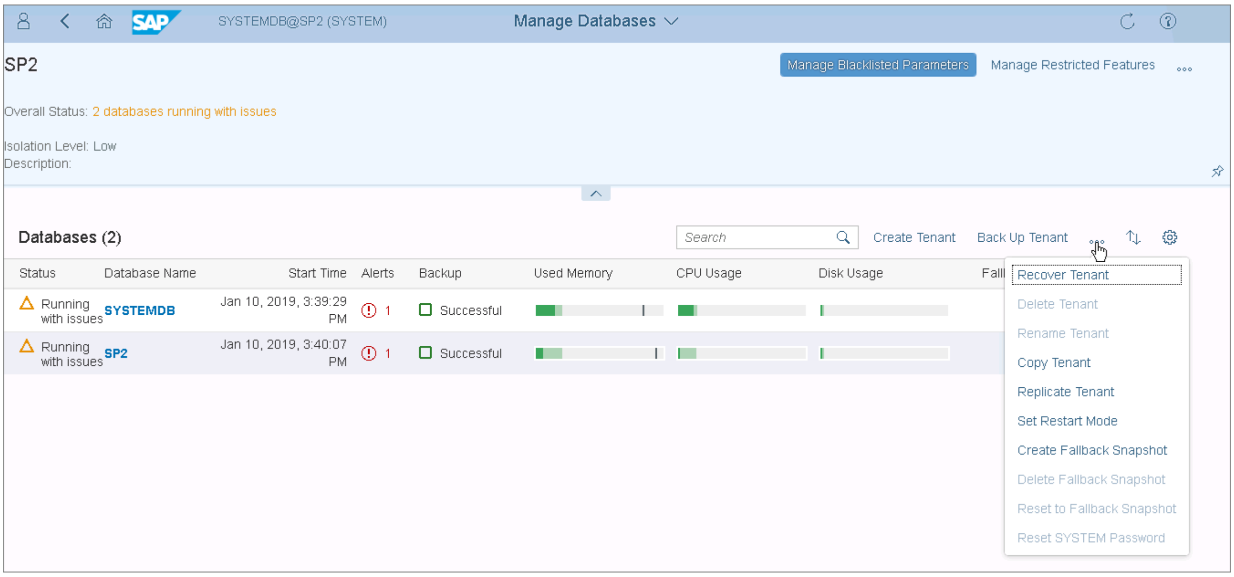
The example below is provided for demonstration purposes only. For details on the full restore functionality of SAP HANA tools, see the Recovering an SAP HANA Database of the SAP HANA Administration Guide.

To perform a Backint recovery of an SAP HANA tenant database from a Veeam Plug-in backup, do the following:

1. In the **System Overview** page of the required system, click **Manage Databases**.



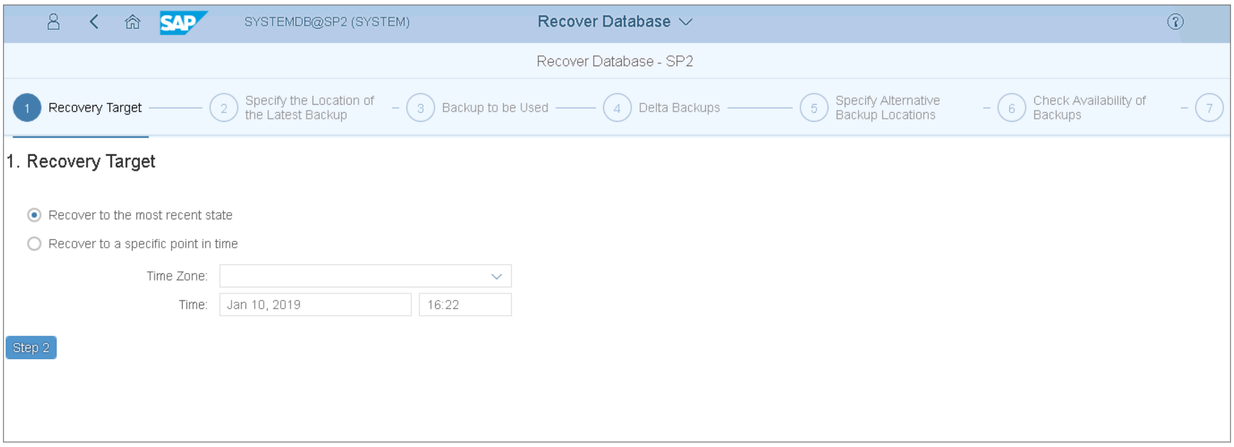
2. In the **Manage Databases** page, expand the toolbar options and select **Recover Tenant**.



Status	Database Name	Start Time	Alerts	Backup	Used Memory	CPU Usage	Disk Usage	Fall
Running with issues	SYSTEMDB	Jan 10, 2019, 3:39:29 PM	1	Successful				
Running with issues	SP2	Jan 10, 2019, 3:40:07 PM	1	Successful				

3. After you launch the recovery wizard, SAP HANA will issue the warning that the database must be stopped for recovery. Click **Stop Tenant** in the warning window.

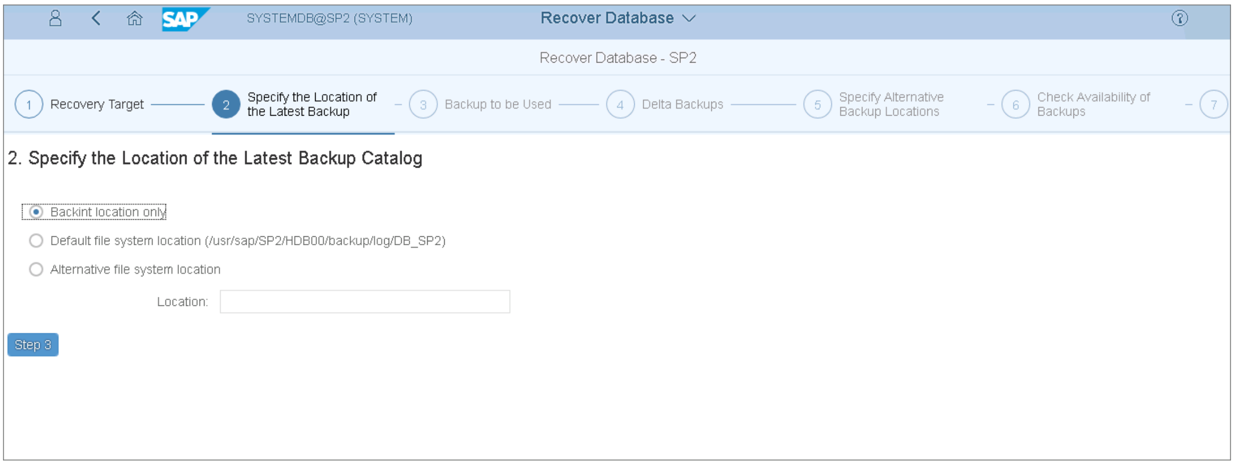
4. At the **Recovery Target** step of the wizard, select the required restore point and click **Step 2**.



● Recover to the most recent state
○ Recover to a specific point in time

Time Zone:
Time: Jan 10, 2019 16:22

5. Specify the location of the latest backup catalog and click **Step 3**.



2. Specify the Location of the Latest Backup Catalog

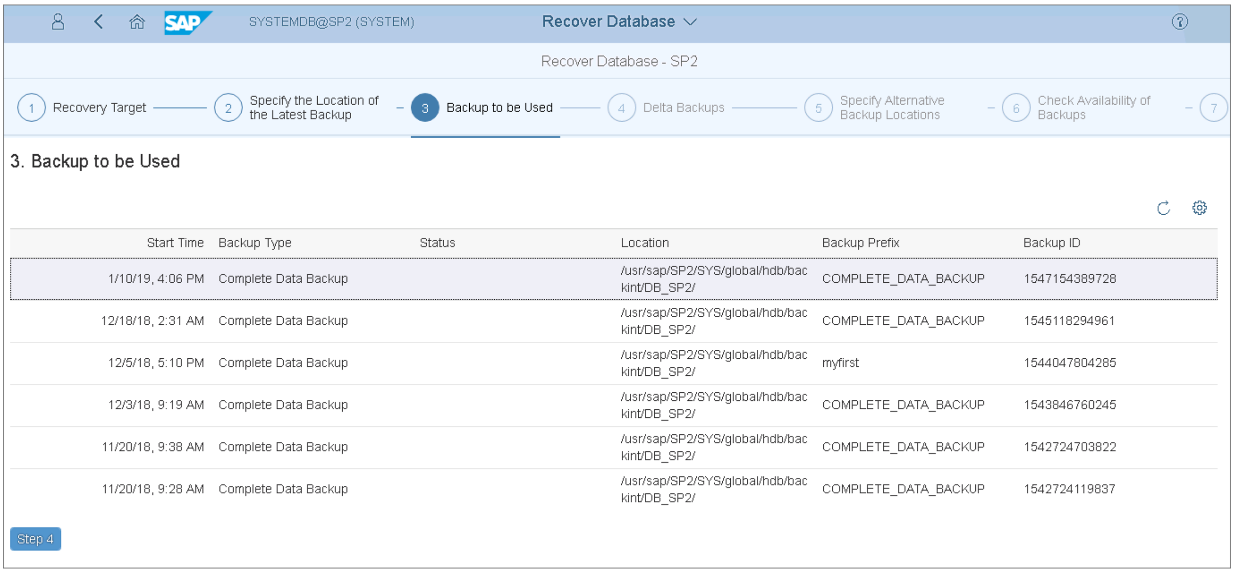
● Backint location only

○ Default file system location (/usr/sap/SP2/HDB00/backup/log/DB_SP2)

○ Alternative file system location

Location:

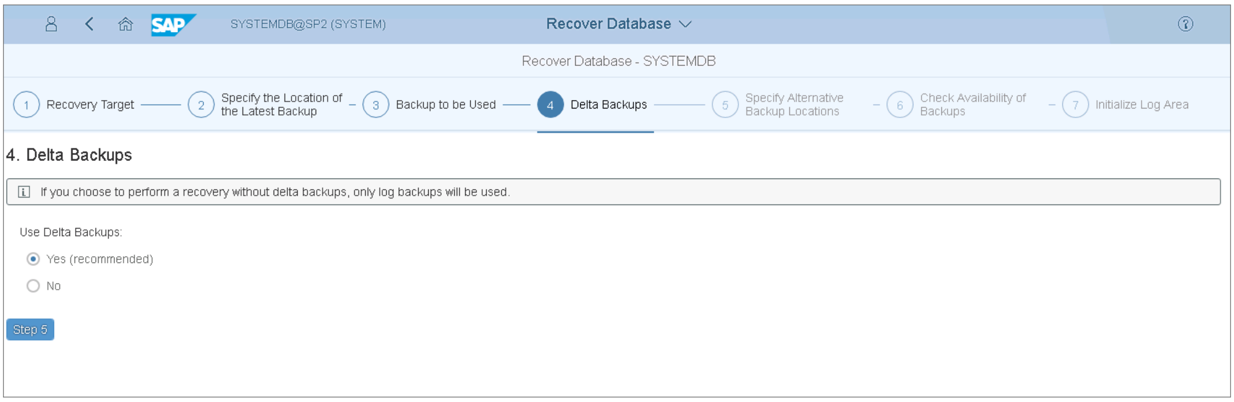
6. At the **Backup to be Used** step, select the backup and click **Step 4**.



3. Backup to be Used

Start Time	Backup Type	Status	Location	Backup Prefix	Backup ID
1/10/19, 4:06 PM	Complete Data Backup		/usr/sap/SP2/SYS/global/hdb/backint/DB_SP2/	COMPLETE_DATA_BACKUP	1547154389728
12/18/18, 2:31 AM	Complete Data Backup		/usr/sap/SP2/SYS/global/hdb/backint/DB_SP2/	COMPLETE_DATA_BACKUP	1545118294961
12/5/18, 5:10 PM	Complete Data Backup		/usr/sap/SP2/SYS/global/hdb/backint/DB_SP2/	myfirst	1544047804285
12/3/18, 9:19 AM	Complete Data Backup		/usr/sap/SP2/SYS/global/hdb/backint/DB_SP2/	COMPLETE_DATA_BACKUP	1543846760245
11/20/18, 9:38 AM	Complete Data Backup		/usr/sap/SP2/SYS/global/hdb/backint/DB_SP2/	COMPLETE_DATA_BACKUP	1542724703822
11/20/18, 9:28 AM	Complete Data Backup		/usr/sap/SP2/SYS/global/hdb/backint/DB_SP2/	COMPLETE_DATA_BACKUP	1542724119837

7. At the **Delta Backups** step, select **Yes** to use delta backups.


SYSTEMDB@SP2 (SYSTEM)
Recover Database
Recover Database - SYSTEMDB
1 Recovery Target
2 Specify the Location of the Latest Backup
3 Backup to be Used
4 Delta Backups
5 Specify Alternative Backup Locations
6 Check Availability of Backups
7 Initialize Log Area
Step 5

4. Delta Backups

If you choose to perform a recovery without delta backups, only log backups will be used.

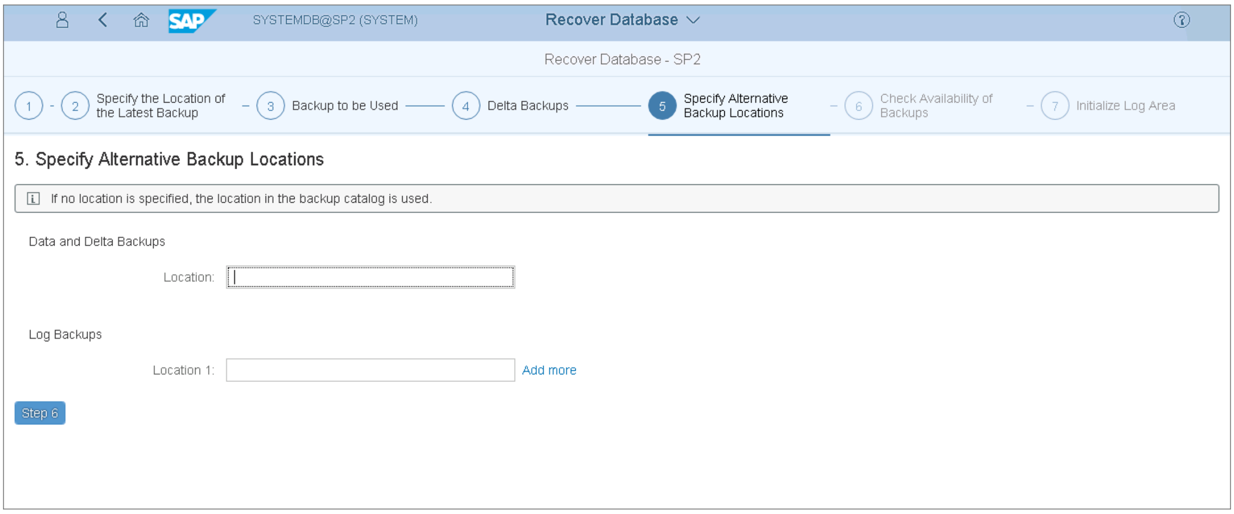
Use Delta Backups:

● Yes (recommended)

○ No

8. At the **Specify Alternative Backup Locations** step, if you want to use backups that are not included in the backup catalog, specify their locations. You can also change the location for log backups.

   If you leave the fields empty, SAP HANA will use the locations specified in the backup catalog.



5. Specify Alternative Backup Locations

If no location is specified, the location in the backup catalog is used.

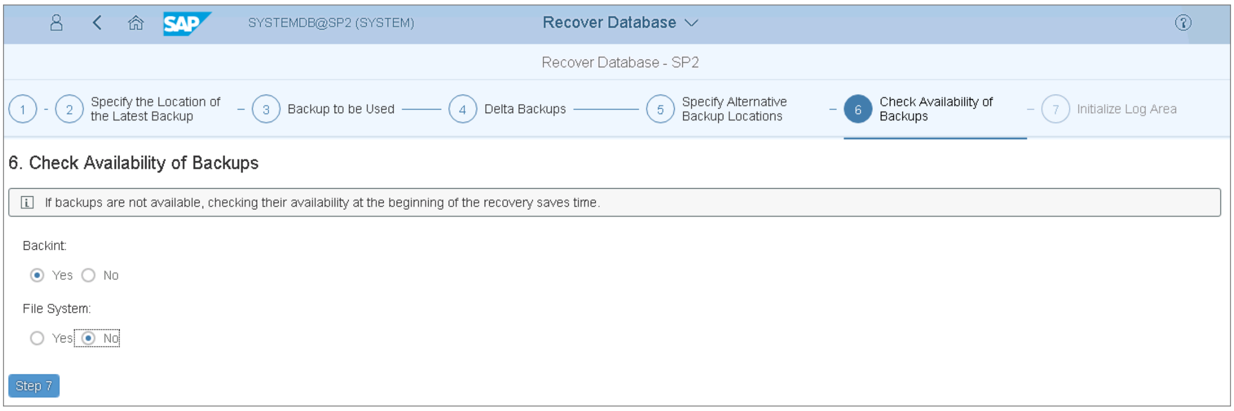
Data and Delta Backups

Location:

Log Backups

Location 1:

9. Select **Yes** or **No**, to check if the backups are available. Note that at this stage SAP HANA does not check the integrity of the backup content on the block level.



6. Check Availability of Backups

If backups are not available, checking their availability at the beginning of the recovery saves time.

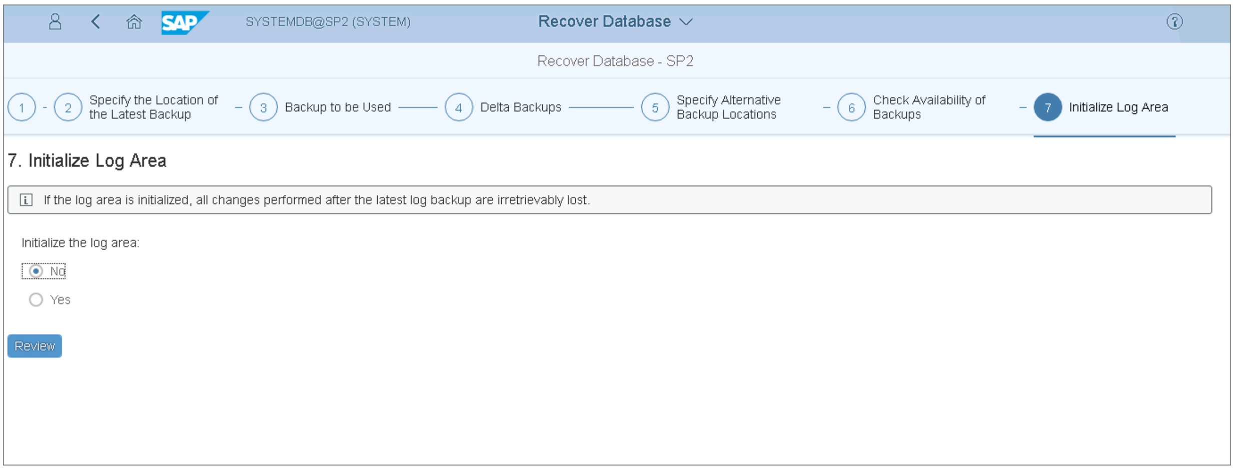
Backint:

● Yes ○ No

File System:

○ Yes ● No

10. Select **No** to initialize the log area and click **Review**. You must initialize the log area only if the log area is unavailable or if you are recovering the database to a different system.



7. Initialize Log Area

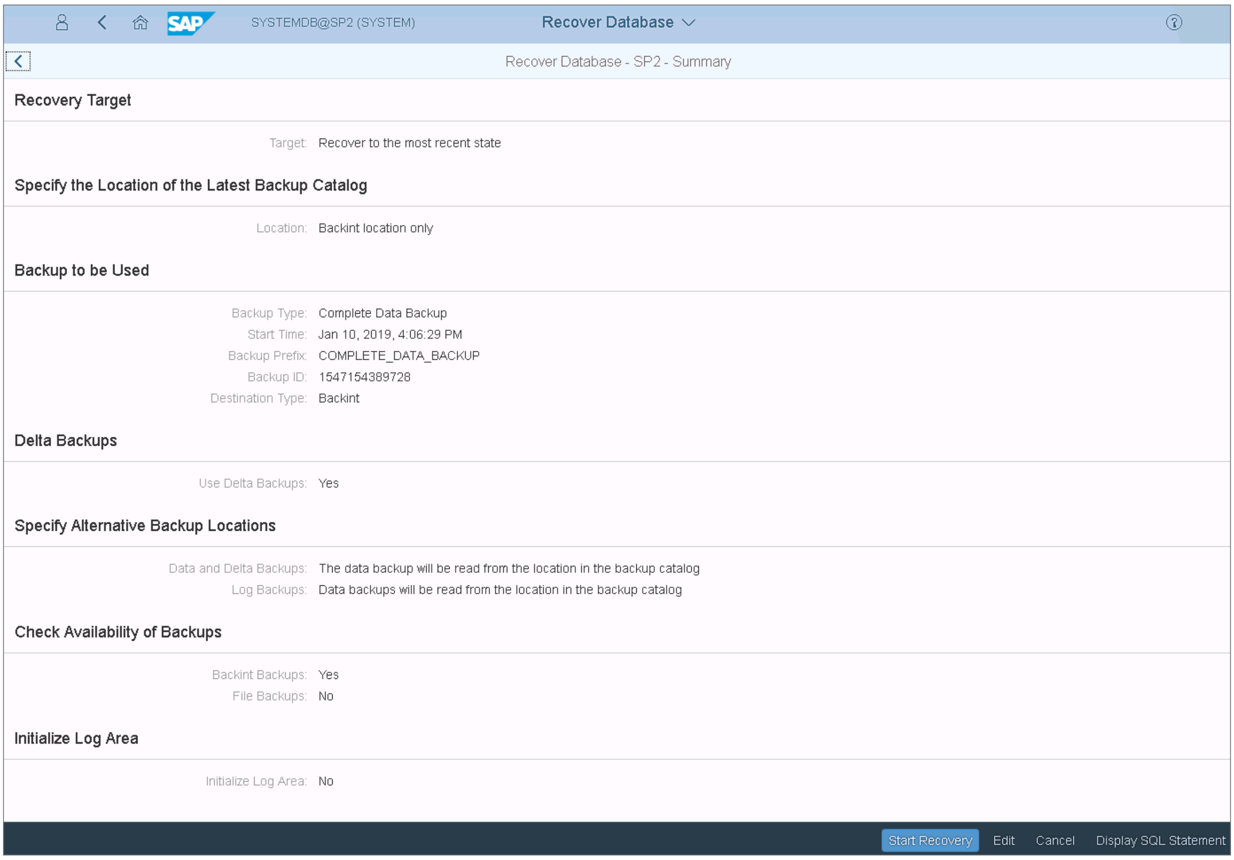
If the log area is initialized, all changes performed after the latest log backup are irretrievably lost.

Initialize the log area:

● No

○ Yes

11. Review the recovery options and click **Start Recovery**.



Recovery Target

Target: Recover to the most recent state

Specify the Location of the Latest Backup Catalog

Location: Backint location only

Backup to be Used

Backup Type: Complete Data Backup
Start Time: Jan 10, 2019, 4:06:29 PM
Backup Prefix: COMPLETE_DATA_BACKUP
Backup ID: 1547154389728
Destination Type: Backint

Delta Backups

Use Delta Backups: Yes

Specify Alternative Backup Locations

Data and Delta Backups: The data backup will be read from the location in the backup catalog
Log Backups: Data backups will be read from the location in the backup catalog

Check Availability of Backups

Backint Backups: Yes
File Backups: No

Initialize Log Area

Initialize Log Area: No

Recovering Databases to Other Servers (System Copy)

You can restore SAP HANA databases from Veeam Plug-in backups to another server. To restore databases to another server, you must reconfigure settings of Veeam Plug-in as shown below.

For security reasons, you can restore databases to another server only in the following condition. The account you use to connect to Veeam Backup & Replication server must be the same account that performed the backup of the source system. If you want to use another account, you can assign the **Veeam Backup Administrator** or **Veeam Restore Operator** roles to the required account. For details on assigning Veeam Backup & Replication roles, see the Users and Roles section of the Veeam Backup & Replication User Guide.

Procedure

To restore databases to another server, you must reconfigure settings of Veeam Plug-in as shown below:

1. Go to `/opt/veeam/VeeamPluginforSAPHANA` and run the following command to select the source server whose backups you want to use during restore.

```
VM2ADM:/opt/veeam/VeeamPluginforSAPHANA> SapBackintConfigTool --set-restor
e-server
Select source SAP HANA plug-in server to be used for system copy restore:
1. SAP-VM1
2. SAP-VM02
Enter server number: 1
```

2. Specify a backup repository where the required backup files are stored.

```
Available backup repositories:
1. serv10_repo
Enter repository number: 1
```

> NOTE
>
> - The account used to connect to Veeam Backup & Replication server must have access permissions on the required repository. Otherwise the repository will not be displayed in the list of available repositories. To learn how to configure access permissions on repositories, see Setting Up User Permissions on Backup Repositories.
> - The wizard does not import existing backups from the repository. To perform a System Copy restore from the imported backup, you must map the backup. For details, see Importing Backups.

3. Perform the SAP HANA System Copy based restore following this SAP KB article.

4. After the restore, you must revert back the restore-server option of the Veeam Plug-in configuration wizard. Otherwise, you will not be able to restore data from the actual server backup file. If you perform only restore to other server, leave this setting enabled. It will not affect the backups of the actual system.

   ```
   VM2ADM:/opt/veeam/VeeamPluginforSAPHANA> SapBackintConfigTool --set-restor
   e-server
   Select source SAP HANA plug-in server to be used for system copy restore:
   1. SAP-VM1
   2. SAP-VM02
   Enter server number: 2
   Available backup repositories:
   1. serv10_repo
   Enter repository number: 1
   ```

NOTE

If you are performing a system copy from another database to a database that was previously backed up by Veeam Plug-in, mind the following.
If the catalog_backup_using_backint parameter is enabled, after performing a system copy, SAP HANA automatically starts a new log chain and sends it to the backint along with a new catalog backup. This new catalog backup overwrites the previous catalog, making it impossible to access pre-restore backups for this database.

If you are planning to restore the older state of this database, you can disable the catalog_backup_using_backint parameter before performing the system copy.

Also, to have access to pre-restore backups, you can store a copy of the old backup catalog outside the default directory and specify this catalog during the restore.

Restore from Backup Copy

You can restore from backups and backup copies. To restore from backup copies, you must enable the **restore from backup copy** option in the Veeam Plug-in wizard.

> IMPORTANT
>
> If the **restore from backup copy** option is enabled, you cannot back up databases using Veeam Plug-in, and you cannot restore from backups created by primary Veeam Plug-in backup jobs. You can restore only from backup copy files until you disable the **restore from backup copy** option.

- Enabling Restore from Backup Copy
- Disabling Restore from Backup Copy

Enabling Restore from Backup Copy

To be able to restore from backup copies, do the following:

1. In the machine where Veeam Plug-in is installed, open the terminal and run the following command:

```
SapBackintConfigTool --configure-restore-from-copy
```

2. Select the number of the backup copy job you want to use:

```
Select secondary job for failover:
0. Disable
1. Plug-ins backup copy job\linuxq01 SAP HANA backup <serv10_repo>
Select secondary job for failover:1
```

> IMPORTANT
>
> The account used to connect to the Veeam Backup & Replication server must have access permissions on the required repository.

Disabling Restore from Backup Copy

To be able to back up with Veeam Plug-in and restore from backups, disable the restore from backup copies (set the parameter back to **0**):

```
SapBackintConfigTool --configure-restore-from-copy
Select secondary job for failover:
0. Disable
1. Plug-ins backup copy job\linuxq01 SAP HANA backup <serv10_repo>
Select secondary job for failover:0
```

Restore from Hardened Repository

As a result of malware activity or unplanned actions, backup job metadata (VACM) files may become unavailable in the hardened repository. In this case, to restore data from the hardened repository, you must re-create the VACM file. To do this, complete the following steps:

1. Run a Veeam Plug-in backup job to create a new Veeam Plug-in backup in a Veeam backup repository. The backup will consist of the VAB, VASM and VACM files.
2. In the backup repository folder, replace the VAB and VASM files created at the step 1 with the VAB and VASM files from the hardened repository.
3. In the Veeam backup console, run the backup repair operation. Veeam Backup & Replication will generate a new VACM file using information from the VASM files. For details, see Repairing Backup.

Once the backup job metadata file is re-created, you can use Veeam Plug-in to restore your data.

Repairing Backup

If you want to restore data from an immutable backup that resides in a hardened repository, you can use the **Repair** operation. During this operation, Veeam Backup & Replication will generate a new backup job metadata (VACM) file using information from the backup metadata (VASM) files.

> IMPORTANT
>
> This operation is intended only for a situation where the backup job metadata file has been lost as a result of malware activity or unplanned actions. Re-creation of the backup job metadata file for other purposes is not supported.

Before you start the repair operation, you must disable the backup job that created the backup. Otherwise, Veeam Backup & Replication will display a message notifying that the job must be disabled.

To repair a backup:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. In the inventory pane, select **Backups**.
3. In the working area, select the necessary backup.
4. Press and hold the **[CTRL]** key, right-click the backup and select **Repair**.

Retention of SAP HANA Backups

In the main scenario, when using Veeam Plug-in for SAP HANA, you must configure the retention policy using native SAP HANA tools. For details the SAP HANA housekeeping options:

- Deleting Backups Using SAP HANA Tools

Also, you can manually delete backups from a backup repository using the Veeam Backup & Replication console and enable the force deletion functionality of Veeam Plug-in. For details, see:

- Deleting Backups Manually Using Veeam Backup & Replication Console
- Configuring Force Deletion of Backups

Deleting Backups Using SAP HANA Tools

To configure retention policies for SAP HANA backups, you can use the SAP HANA housekeeping options:

- Manual Deletion of Backups in SAP HANA Studio
- Configuring Retention Policy in SAP HANA Cockpit
- Deletion of Catalog and Backups Using Scripts

> **IMPORTANT**
>
> If you delete backups from a backup catalog using scripts or SAP HANA Studio and don't select the option to delete backup physically from the backup location, backups will remain in the backup repository. In this case, we recommend to enable the options for physical deletion of backups in used SAP HANA retention tools or you must enable the force deletion feature of Veeam Plug-in for SAP HANA. Otherwise, you will run out of space on the backup repository.

Manual Deletion of Backups in SAP HANA Studio

For details, see the Housekeeping for Backup Catalog and Backup Storage section of the SAP HANA Administration Guide.

To physically delete the backups, you must select the **Catalog and Backup Location** option. Note that if you have physical backups in both the file system and a Veeam backup repository, you can choose to delete data backups in only one location.

Configuring Retention Policy in SAP HANA Cockpit

For details, see the Retention Policy section of the SAP HANA Administration with SAP HANA Cockpit Guide. Note that the retention policy functionality is supported only in SAP HANA 2.0 SPS03 and later versions.

When you configure a retention policy in SAP HANA Cockpit, make sure that you have selected the **Also delete physically from Backint** check box in the **Options for Backup Deletion** section. Otherwise the backups will not be deleted from the repository.

Deletion of Catalog and Backups Using Scripts

Deletion of catalog and backups using scripts. For details see the BACKUP CATALOG DELETE Statement section of the SAP HANA SQL and Views Reference.

To physically delete backups from the backup repository, you must include the **WITH BACKINT and WITH FILE** options in the script.

Deleting Backups Manually

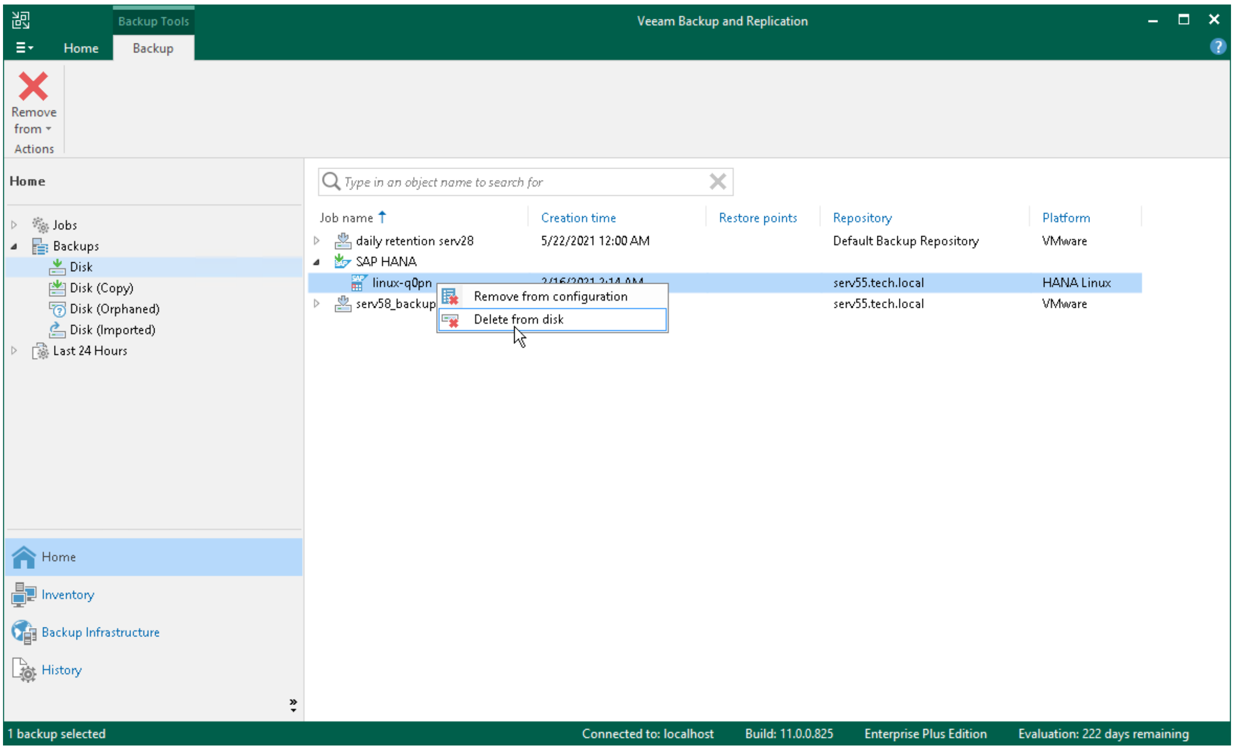
In the main scenario, when using Veeam Plug-in for SAP HANA, you must configure the retention policy using native SAP HANA tools. For details on the SAP HANA housekeeping options, see Deleting Backups Using SAP HANA Tools.

If you have lost the backup catalog, you can delete the backups manually from Veeam backup repositories using the Veeam Backup & Replication console.

> NOTE
>
> If you remove backups from a backup repository manually, the backup catalog will not be updated.

To remove a backup from a backup repository, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. In the **Inventory** pane, select **Backups**.
3. In the working area, right-click the backup job object name and select **Delete from disk**.



Job name	Creation time	Restore points	Repository	Platform
daily retention serv28	5/22/2021 12:00 AM		Default Backup Repository	VMware
SAP HANA				
linux-q0pn	2/16/2021 2:14 AM		serv55.tech.local	HANA Linux
serv58_backup			serv55.tech.local	VMware

1 backup selected | Connected to: localhost | Build: 11.0.0.825 | Enterprise Plus Edition | Evaluation: 222 days remaining

Configuring Force Deletion of Backups

In the main scenario, when using Veeam Plug-in for SAP HANA, you must configure the retention policy using native SAP HANA tools. For details, see Retention of SAP HANA Backups.

Veeam Plug-in for SAP HANA has a functionality that automatically force deletes backup files which are older than specified number of days. For example, you can use it if a backup repository contains backup files that are no longer in the backup catalog.

To enable force deletion of backup files, do the following:

1. On the SAP HANA server, run the following command.

   ```
   SapBackintConfigTool --set-force-delete
   ```

2. Enter the number of days after which Veeam Plug-in will force delete backup files on all configured Veeam backup repositories.

   ```
   Garbage collector automatically deletes backup files older than the specif
   ied number of days.
   Make sure the number of days value exceeds your retention policy.
   To disable this functionality, set the number of days to 0.
   Enter the number of days to delete backups after, between 7 and 999 [0]:
   ```

   By default, the force delete functionality is disabled (set to *0*).

IMPORTANT

- A value for the **number of days** setting must be at least 1 backup generation period longer than the retention period for your SAP HANA backups. Otherwise, Veeam Plug-in will delete earliest backups created within the retention period.
- If a backup repository contains backups older than the specified retention period, Veeam Plug-in removes old backup files only after the next run of the Backint backup.

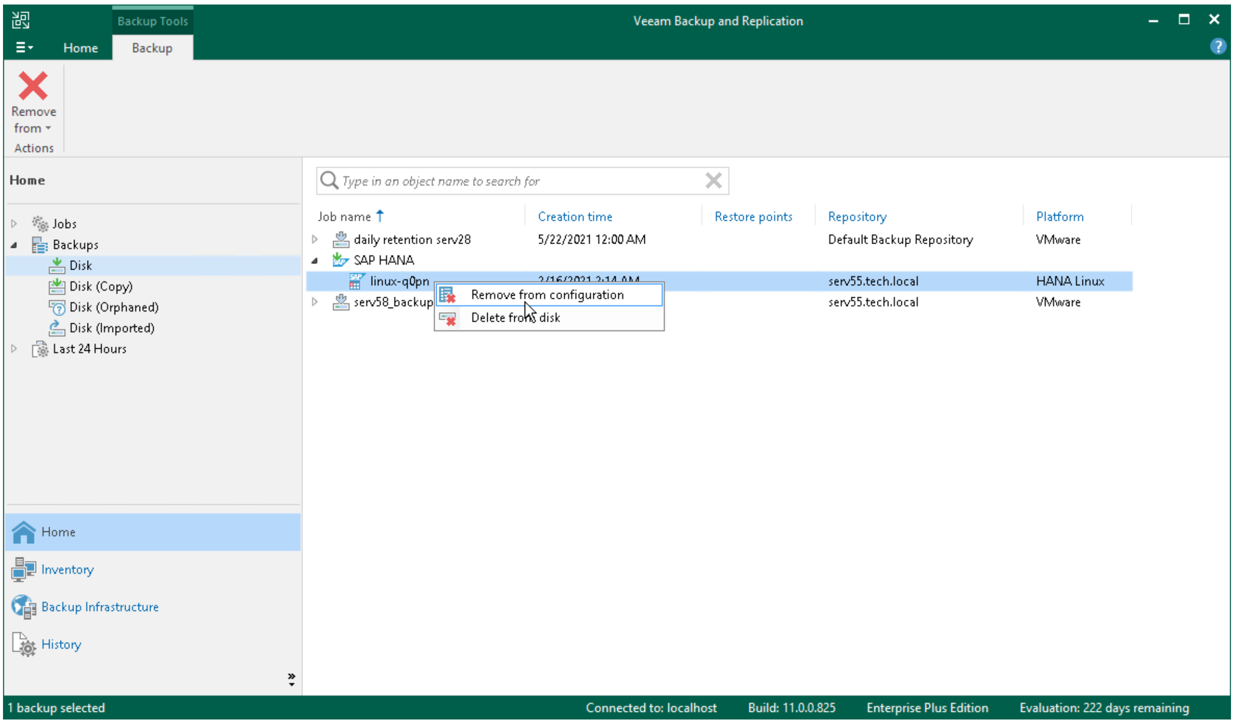
Removing Backups from Configuration

If you want to remove records about backups from the Veeam Backup & Replication console and configuration database, you can use the **Remove from configuration** operation.

When you remove a backup from the configuration, backup files (VAB, VBM) remain on the backup repository. You can import backup files later and restore data from them.

To remove a backup from configuration:

1. Open the **Home** view.
2. In the inventory pane, select **Backups**.
3. In the working area, select the necessary backup.
4. Press and hold the **[CTRL]** key, right-click the backup and select **Remove from configuration**.



Job name	Creation time	Restore points	Repository	Platform
daily retention serv28	5/22/2021 12:00 AM		Default Backup Repository	VMware
SAP HANA				
linux-q0pn	2/16/2021 2:14 AM		serv55.tech.local	HANA Linux
serv58_backup			serv55.tech.local	VMware

Backup Copy for SAP HANA Backups

Having just one backup does not provide the necessary level of safety. The primary backup may get destroyed together with production data, and you will have no backups from which you can restore data.

To build a successful data protection and disaster recovery plan, it is recommended that you follow the 3-2-1 rule:

- 3: You must have at least three copies of your data: the original production data and two backups.
- 2: You must use at least two different types of media to store the copies of your data, for example, local disk and cloud.
- 1: You must keep at least one backup offsite, for example, in the cloud or in a remote site.

Thus, you must have at least two backups and they must be in different locations. If a disaster takes out your production data and local backup, you can still recover from your offsite backup.

In This Section

Creating Backup Copy Job

Veeam Backup & Replication offers the backup copy functionality that allows you to create several instances of the same backup in different locations, whether onsite or offsite. Backup copies have the same format as those created by backup jobs and you can recover your data from them when you need it.

Veeam Backup & Replication fully automates the backup copy process and lets you specify retention settings to maintain the desired number of restore points, as well as full backups for archival purposes. Backup copy is a job-driven process. When enabled, the backup copy job for Veeam Plug-in backups runs continuously. For more details on how it works, see the Backup Copy section of the Veeam Backup & Replication User Guide.

To copy backups to a secondary location, you must configure a backup copy job. The backup copy job defines how, where and when to copy backups. One job can be used to process backups of one or more machines.

You can configure a job and start it immediately or save the job to start it later.

Before creating a job, check prerequisites. Then use the **New Backup Copy Job** wizard to configure a backup copy job.

1. Launch Backup Copy Job wizard.
2. Specify a job name and description.
3. Selects backups to process.
4. Define backup copy target.
5. Specify advanced settings.
6. Define backup copy schedule.
7. Finish working with the wizard.

Before You Begin

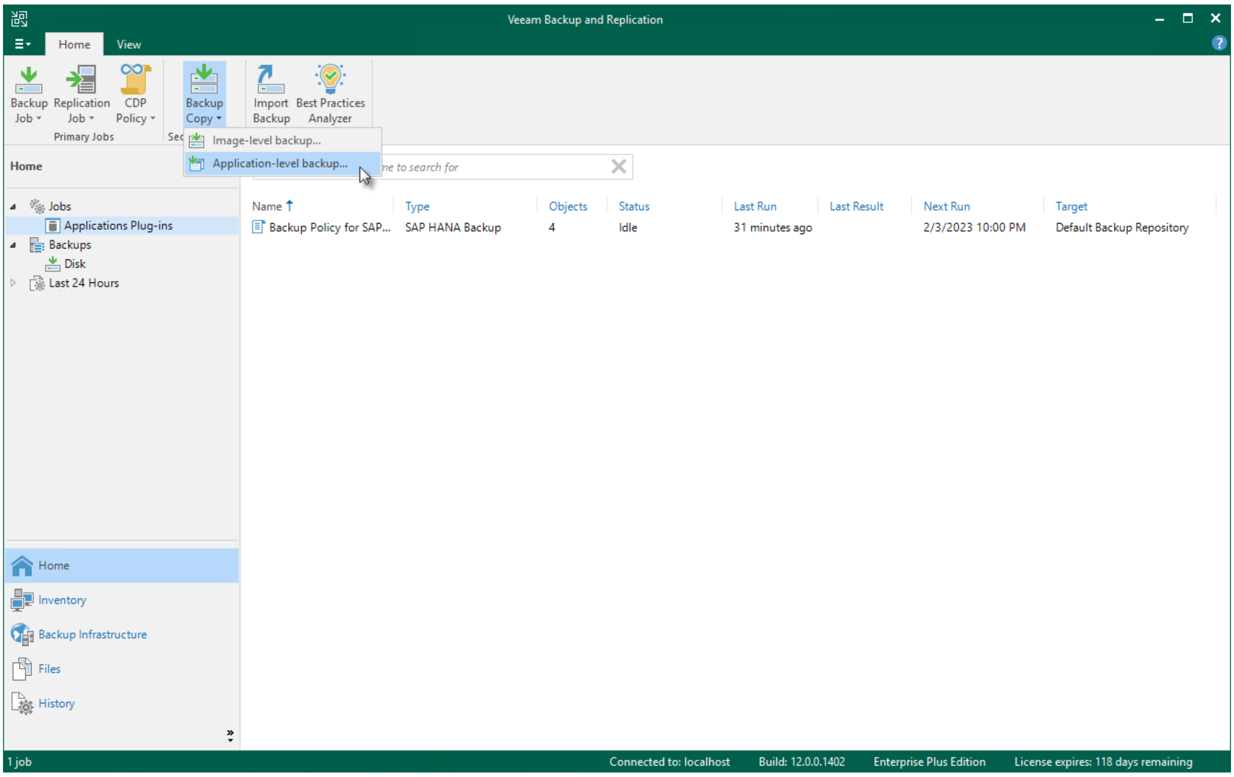
Before you create a backup copy job, check the prerequisites and limitations:

- Backup infrastructure components that will take part in the backup copy process must be added to the backup infrastructure and properly configured. These include source and target backup repositories between which backups must be copied.
- The target backup repository must have enough free space to store copied backups. To receive alerts about low space on the backup repository, configure global notification settings. For more information, see Specifying Other Notification Settings.
- For Veeam Plug-in backup copy jobs, you cannot select a Veeam Cloud Connect repository as a backup copy target.
- If you have upgraded the backup files, make sure that you have upgraded Veeam Plug-in on the source server. If the plug-in is not upgraded to version 12 and you convert backup copy files to backup files, then the next backup job runs will fail.

Step 1. Launch Backup Copy Job Wizard

To create a backup copy job, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Click the **Backup Copy** tab and select **Application-level backup**.

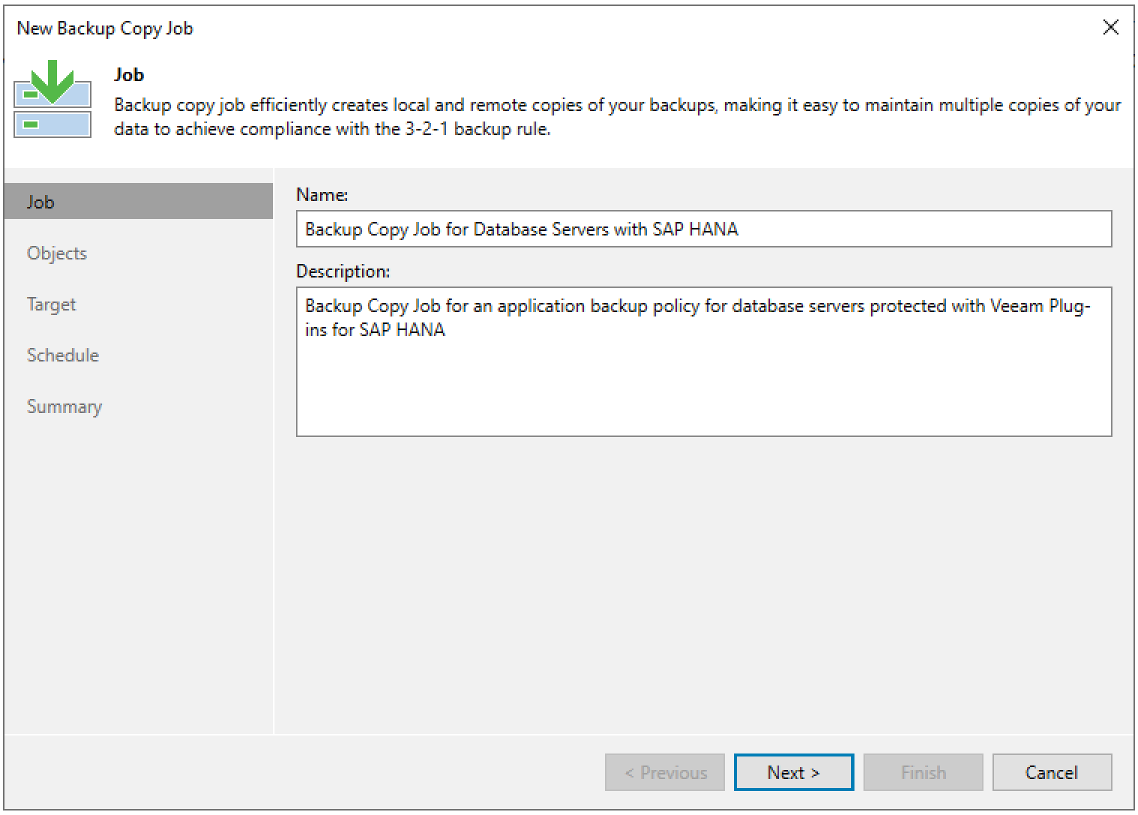


Name ↑	Type	Objects	Status	Last Run	Last Result	Next Run	Target
Backup Policy for SAP...	SAP HANA Backup	4	Idle	31 minutes ago		2/3/2023 10:00 PM	Default Backup Repository

Step 2. Specify Job Name and Description

At the **Job** step of the wizard, specify a name and description for the backup copy job.

1. In the **Name** field, enter a name for the job.
2. In the **Description** field, enter a description for the job. The default description contains information about the user who created the job, date and time when the job was created.



New Backup Copy Job

Job

Backup copy job efficiently creates local and remote copies of your backups, making it easy to maintain multiple copies of your data to achieve compliance with the 3-2-1 backup rule.

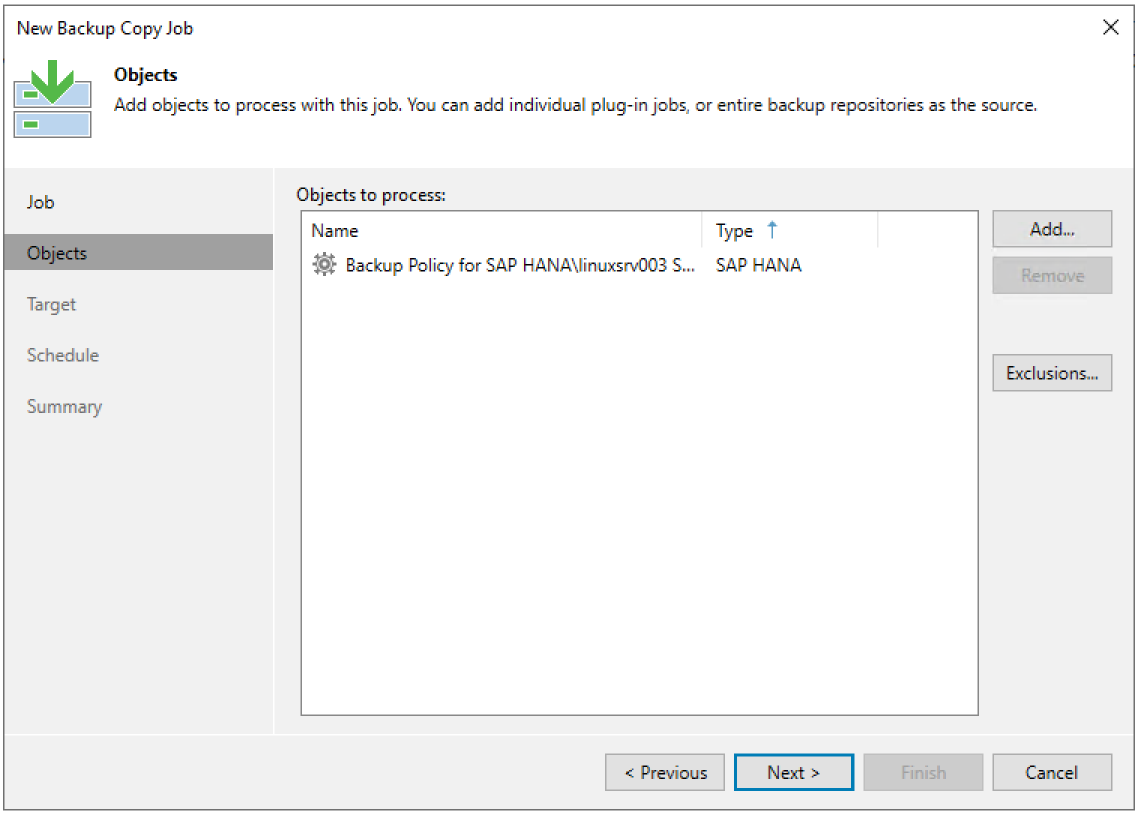
Name: Backup Copy Job for Database Servers with SAP HANA

Description: Backup Copy Job for an application backup policy for database servers protected with Veeam Plug-ins for SAP HANA

Step 3. Select Backups to Process

At the **Object** step of the wizard, select machines whose backups you want to copy to the target repository.

1. Click the **Add** button and select from which entity you want to process the machines.
   - **From jobs**: You can select Veeam Plug-in backup jobs. When a backup copy job runs, Veeam Backup & Replication will search for backup files created by selected jobs.
   - **From repositories**: You can select repositories where Veeam Plug-in backups are stored. When a backup copy job runs, Veeam Backup & Replication will search for backup files created by Veeam Plug-in in selected repositories.
2. Use the **Remove** button if you want to remove selected jobs or repositories from processing.
3. If you have added jobs from a repository and want to exclude from processing some of the backup jobs on the selected repository, click **Exclusions** and select the jobs that you want to exclude.



Objects

Add objects to process with this job. You can add individual plug-in jobs, or entire backup repositories as the source.

Objects to process:

Name	Type
Backup Policy for SAP HANA\linuxsrv003 S...	SAP HANA

Step 4. Define Backup Copy Target

At the **Target** step of the wizard, configure the target repository settings.

1. From the **Backup repository** list, select a backup repository in the target site where copied backups must be stored. When you select a target backup repository, Veeam Backup & Replication automatically checks how much free space is available on it. Make sure that you have enough free space to store copied backups.

   > IMPORTANT
   >
   > For Veeam Plug-in backup copy jobs, you cannot select a Veeam Cloud Connect repository as a backup copy target.

2. If the target repository contains a Veeam Plug-in backup that was excluded from the backup copy job, and if you don't want to transfer duplicate data, you can use the mapping feature.

   After you configure mapping, if some of backup files (VAB) of the source backup are missing in the target backup copy, these files are uploaded to the target backup copy.

   > NOTE
   >
   > Veeam Plug-in backup copy jobs do not use WAN accelerators.

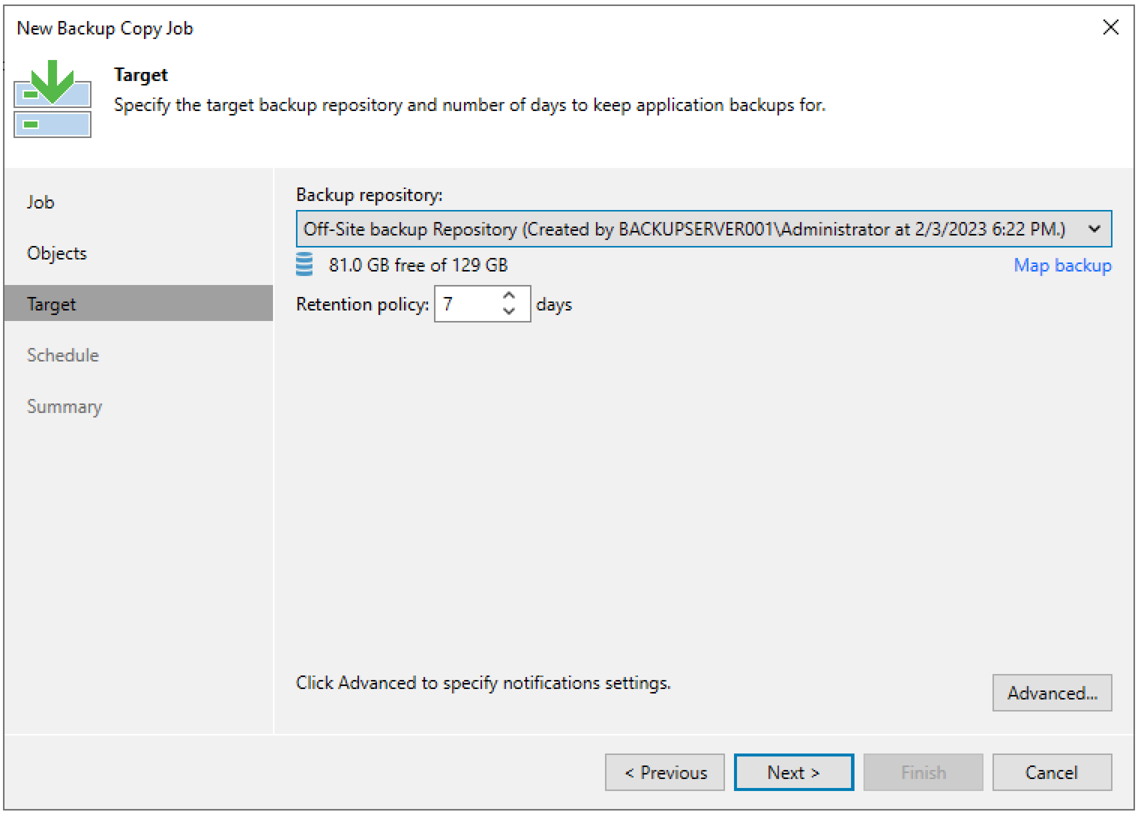
   To map a backup copy job to the backup:

   a. Click the **Map backup** link.

   b. Point the backup copy job to the backup in the target backup repository. Backups in the target backup repository can be easily identified by backup job names. To facilitate search, you can use the search field at the bottom of the window.

   > IMPORTANT
   >
   > - Used account must have access to Veeam backup repositories that you plan to use.
   > - Encryption must be disabled on the repository.
   >
   > Otherwise, the repositories will not be listed as available. To learn how to configure access permissions and encryption settings on repositories, see Access and Encryption Settings on Repositories.

3. You can specify the number of days after which the backup copy will be deleted from the repository. Note that the countdown starts from the moment when source backup has been created.



New Backup Copy Job

Target

Specify the target backup repository and number of days to keep application backups for.

Backup repository: Off-Site backup Repository (Created by BACKUPSERVER001\Administrator at 2/3/2023 6:22 PM.)

81.0 GB free of 129 GB

Retention policy: 7 days

Click Advanced to specify notifications settings.

Step 5. Specify Advanced Settings

At the **Target** step of the wizard, click **Advanced** to configure storage, RPO warning, and notifications settings.

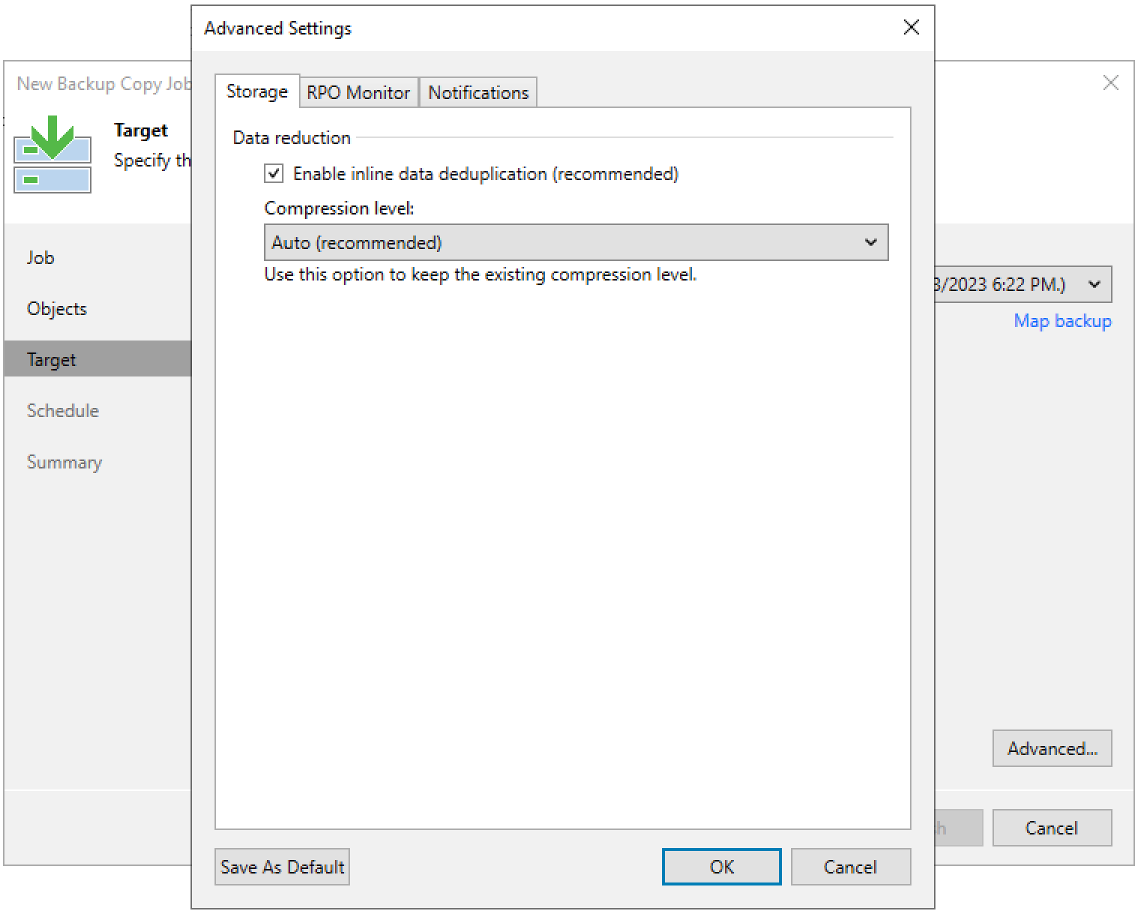
- Storage settings
- RPO warning settings
- Notification settings

Storage Settings

At the **Storage** tab, define compression and deduplication settings.

By default, Veeam Backup & Replication performs deduplication before storing copied data on the target backup repository. Deduplication provides a smaller size of the resulting backup file but may reduce the job performance.

1. You can disable data deduplication. To do this, clear the **Enable inline data deduplication** check box.
2. From the Compression level list, choose a compression level to be used: **Auto**, **None**, **Dedupe-friendly**, **Optimal**, **High** or **Extreme**. The recommended level of compression for backup copy jobs is **Auto**. In this case, Veeam Backup & Replication uses compression settings of the copied backup files. For more information, see Compression and Deduplication.



Data reduction

☑ Enable inline data deduplication (recommended)

Compression level: Auto (recommended)

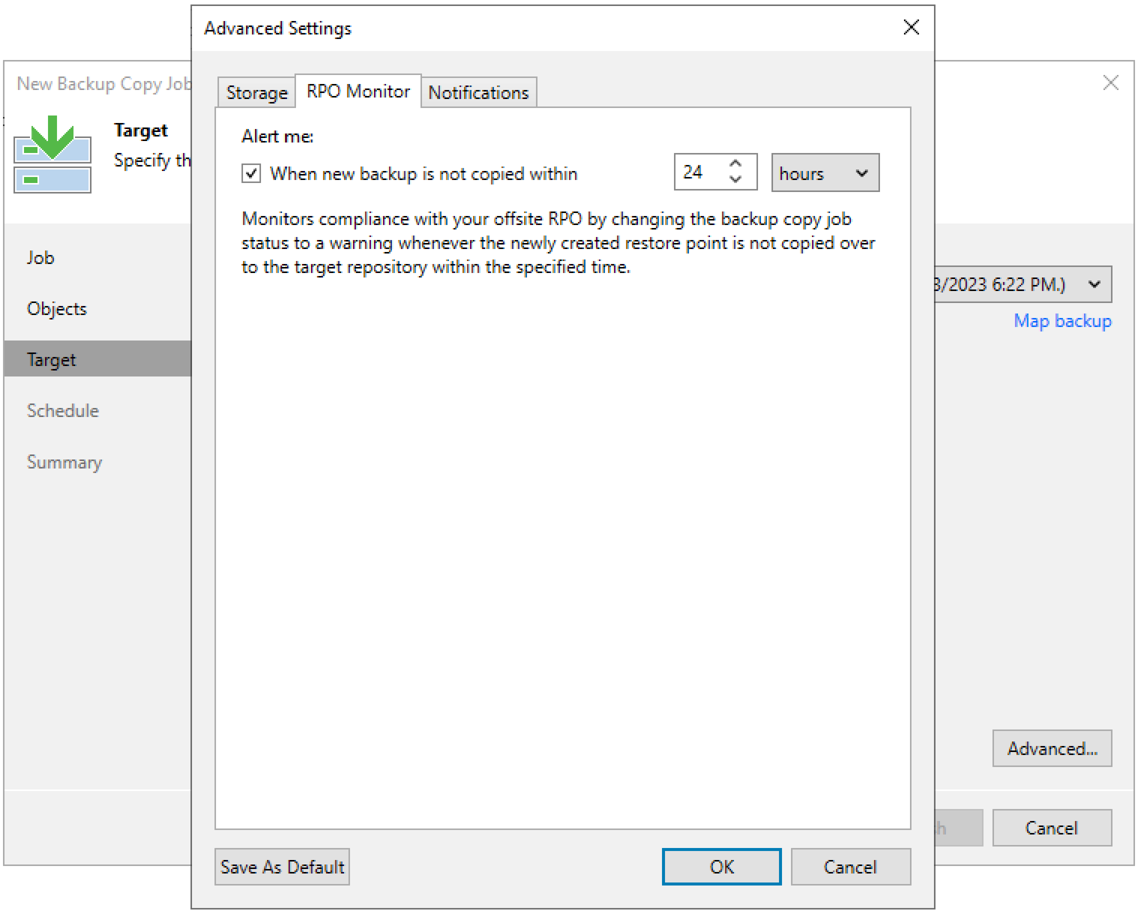
Use this option to keep the existing compression level.

RPO Warning Settings

At the **RPO Monitor** tab, specify RPO warning settings.

Enable the **Warn me if backup is not copied within** check box and specify the time period in **minutes**, **hours**, or **days.**

If the backup copy is not created within the specified time period, the backup copy job will finish with the *Warning* status. The countdown starts from the moment when the required backup is finished and ready to be copied.



Advanced Settings

Alert me:

☑ When new backup is not copied within 24 hours

Monitors compliance with your offsite RPO by changing the backup copy job status to a warning whenever the newly created restore point is not copied over to the target repository within the specified time.

Notification Settings

At the **Notifications** tab, to specify notification settings for the backup copy job:

1. At the **Target** step of the wizard, click **Advanced**.
2. Click the **Notifications** tab.
3. Select the **Send SNMP notifications for this job** check box if you want to receive SNMP traps when the job completes successfully. SNMP traps will be sent if you specify global SNMP settings in Veeam Backup & Replication and configure software on recipient's machine to receive SNMP traps. For more information, see Specifying SNMP Settings.
4. Select the **Send email notifications to the following recipients** check box if you want to receive notifications by email in case of job failure or success. In the field below, specify a recipient's email address. You can enter several addresses separated by a semicolon.

5. Veeam Backup & Replication sends a consolidated email notification once for the specified backup copy interval. Even if the synchronization process is started several times within the interval, for example, due to job retries, only one email notification will be sent.

6. Email notifications will be sent if you configure global email notification settings in Veeam Backup & Replication. For more information, see Configuring Global Email Notification Settings.

7. At the **Send** at field, specify the time when you want to receive notifications. Note that you will receive a notification on the job status once a day.

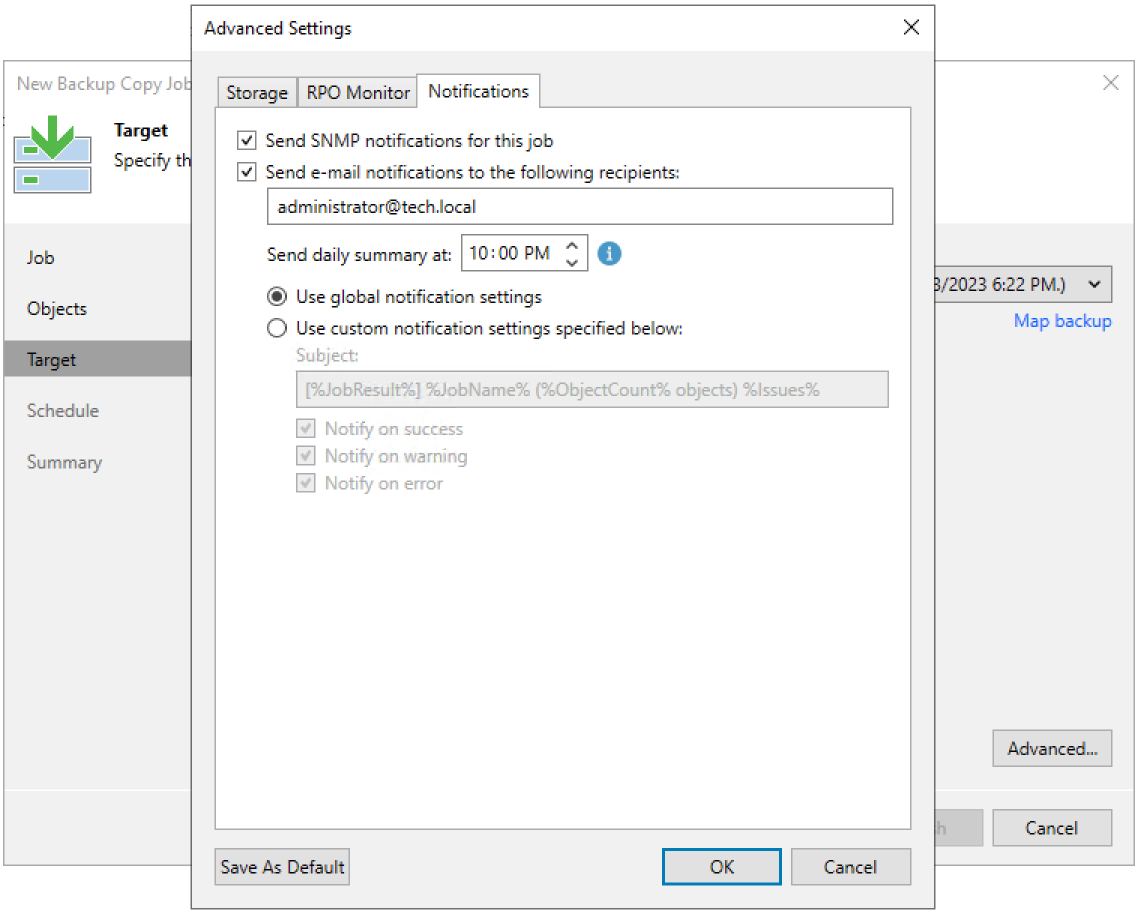
8. You can choose to use global notification settings or specify custom notification settings.

   - To receive a typical notification for the job, select **Use global notification settings**. In this case, Veeam Backup & Replication will apply to the job global email notification settings specified for the backup server. For more information, see Configuring Global Email Notification Settings.

   - To configure a custom notification for a job, select **Use custom notification settings specified below**. You can specify the following notification settings:

     i. In the **Subject** field, specify a notification subject. You can use the following variables in the subject: *%Time%* (completion time), *%JobName%*, *%JobResult%*, *%VmCount%* (number of machines in the job) and *%Issues%* (number of machines in the job that have been processed with the **Warning** or **Failed** status).

     ii. Select the **Notify on success**, **Notify on warning** and **Notify on error** check boxes to receive email notification if data processing within the backup copy interval completes successfully, fails or completes with a warning.



Advanced Settings

Storage | RPO Monitor | Notifications

☑ Send SNMP notifications for this job

☑ Send e-mail notifications to the following recipients:

administrator@tech.local

Send daily summary at: 10:00 PM

● Use global notification settings

○ Use custom notification settings specified below:

Subject:

[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

☑ Notify on success

☑ Notify on warning

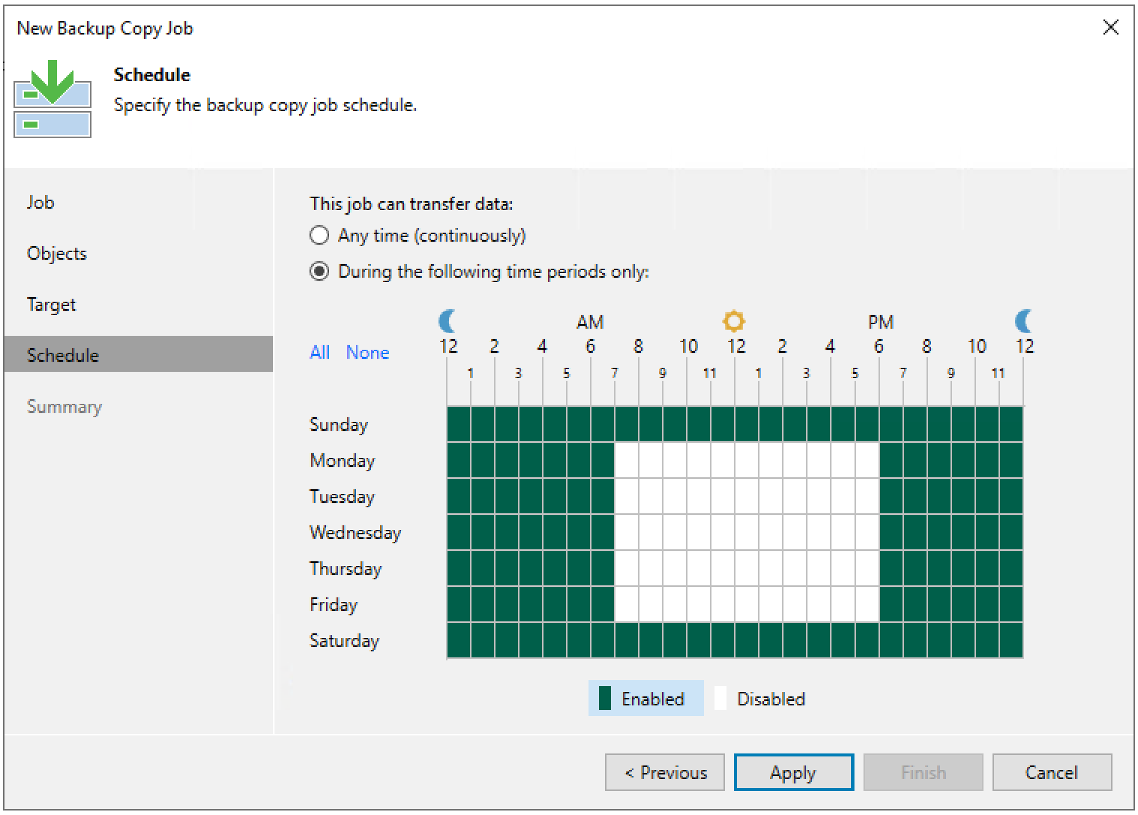
☑ Notify on error

Step 6. Define Backup Copy Schedule

At the **Schedule** step of the wizard, define a time span in which the backup copy job must not transport data between source and target backup repositories. For more information, see Backup Copy Window.

To define a backup window for the backup copy job:

1. Select the **During the following time periods only** option.
2. In the schedule box, select the desired time area.
3. Use the **Enable** and **Disable** options to mark the selected area as allowed or prohibited for the backup copy job.



Schedule

Specify the backup copy job schedule.

This job can transfer data:

○ Any time (continuously)

● During the following time periods only:

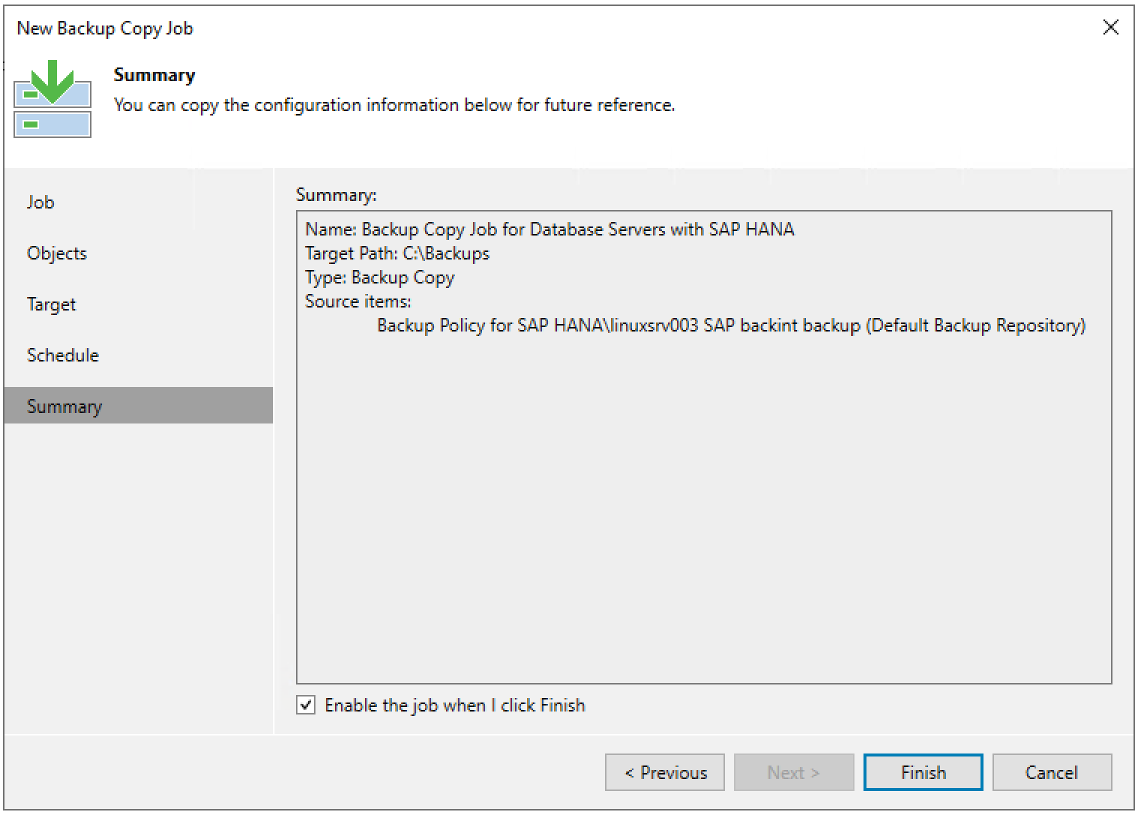
	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11
Sunday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Monday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩
Tuesday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩
Wednesday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩
Thursday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩
Friday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩
Saturday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩

🟩 Enabled ⬜ Disabled

Step 7. Review Backup Copy Job Settings

At the **Summary** step of the wizard, complete the procedure of backup copy job configuration.

1. Review details of the backup copy job.
2. Select the **Enable the job when I click Finish** check box if you want to start the job right after you finish working with the wizard.
3. Click **Finish** to close the wizard.



New Backup Copy Job

Summary

You can copy the configuration information below for future reference.

Summary:

```
Name: Backup Copy Job for Database Servers with SAP HANA
Target Path: C:\Backups
Type: Backup Copy
Source items:
        Backup Policy for SAP HANA\linuxsrv003 SAP backint backup (Default Backup Repository)
```

☑ Enable the job when I click Finish

Converting Backup Copy to Backup

If you have imported Veeam Plug-in backup copies from another server, you can convert them into regular backup files. When you convert a backup copy to a backup, Veeam Plug-in creates a backup job with the converted backup. You can use this backup job to continue a backup chain and use the converted backup as a restore point.

You can convert and unbind Veeam Plug-in backups into regular Veeam Plug-in backup files in the following cases:

- If you have deleted a backup copy job which created the backup copy.
- If you have excluded a backup job from a backup copy job that used multiple backup jobs as a source.
- If you imported a Veeam Plug-in backup copy from another host.

> NOTE
> If you want to restore from a backup copy, you don't need to convert the backup copy to backup. For details, see Restore from Backup Copy.

Converting Backup Copy to Backup for SAP HANA

To convert a backup copy to a primary backup, use the **--promote-backup-copy-to-primary** parameter as shown below:

```
SapBackintConfigTool --promote-backup-copy-to-primary
Backup copies available for promotion to primary backup:
1. Backup Copy Job 1\saprhel01-localdomain SAP backint backup (Default Backup R
epository)
Select backup: 1
Promotion of backup copy to a primary backup will reconfigure the plug-in to us
e a different repository. Continue? (y/N): y
```

> IMPORTANT
>
> [For backups of scale-out clusters and servers with the `customServerName` option] To avoid failure of conversion of backup copies, the cluster name must be the same as the name used in the backup copy.

Logs and Support

If you have any questions or issues with Veeam Plug-in for SAP HANA or Veeam Backup & Replication, you can search for a resolution on Veeam Community Forums or submit a support case on the Veeam Customer Support Portal.

When you submit a support case, we recommend you attach necessary logs related to Veeam Plug-in operations.

To learn how to collect logs, see this Veeam KB.

Veeam Plug-in for Oracle RMAN

Veeam Backup & Replication offers two options to protect Oracle databases:

- Veeam Plug-in for Oracle RMAN: for transactionally-consistent RMAN-based backups of Oracle databases.
- Veeam Backup & Replication or Veeam Agents: for image-level backups of Oracle servers.

You can use both or one of the options depending on your environment specifics and approach to handle Oracle databases.

Veeam Plug-in for Oracle RMAN

Veeam Plug-in uses the backup and restore functionality of Oracle Recovery Manager (RMAN) and transfers backups to Veeam backup repositories.

Use Veeam Plug-in to back up Oracle databases in the following cases:

- If you want the Oracle database administrator to fully control the backup and recovery processes.
- If you want to use existing Oracle RMAN scripts or external schedulers.
- If you use Oracle RAC.
- If you use ASM disks on a physical server.

Veeam Backup & Replication or Veeam Agents

Veeam Backup & Replication (or Veeam Agent) performs image-level/file-level backup and restore of Oracle servers. Use Veeam Backup & Replication or Veeam Agents to back up Oracle servers in the following cases:

- If you do not have Oracle database administrators.
- If you want to control backup and restore processes on the Veeam Backup & Replication side.

If you want to use Veeam Backup & Replication to protect Oracle servers, see the Creating Backup Jobs section of the Veeam Backup & Replication User Guide.

If you want to use Veeam Agents to protect Oracle servers, see one of the following guides: Veeam Agent for Linux, Veeam Agent for Microsoft Windows, Veeam Agent for IBM AIX.

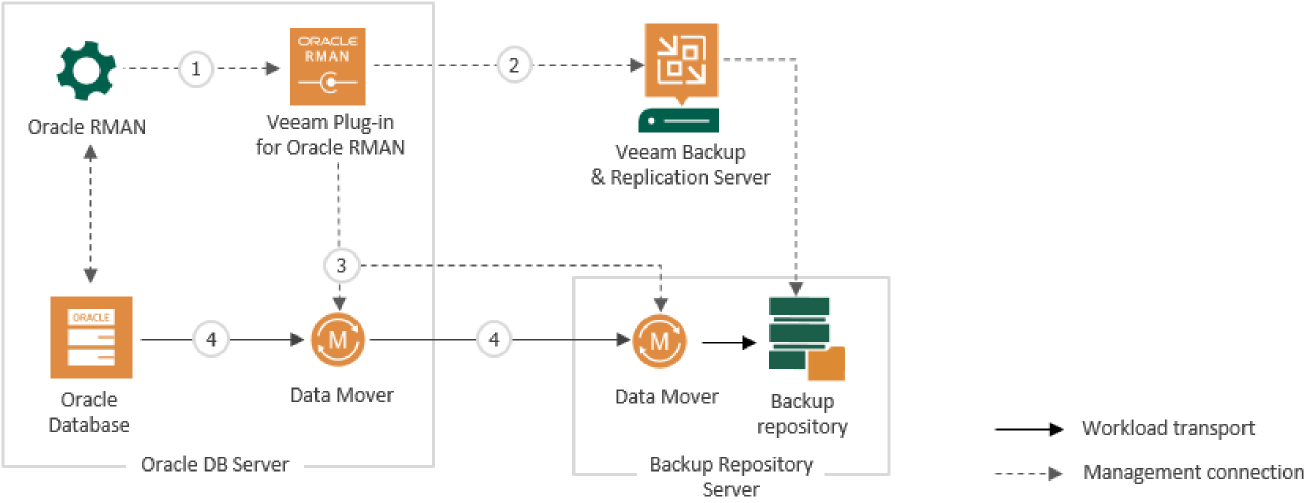
How Veeam Plug-in for Oracle RMAN Works

Veeam Plug-in functions as an agent between Oracle RMAN and Veeam backup repository.

By default, RMAN sends backups to a native RMAN location on disk (`DEFAULT DEVICE TYPE TO DISK`). When you configure the Veeam Plug-in, the default device type is changed to `SBT_TAPE`, which gives control over backup media management to Veeam Plug-in. Thus, after you deploy Veeam Plug-in on an Oracle server, you can perform all backup and restore operations in the Oracle RMAN console. Veeam Plug-in compresses, deduplicates database backups and transfers them to a backup repository connected to Veeam Backup & Replication.

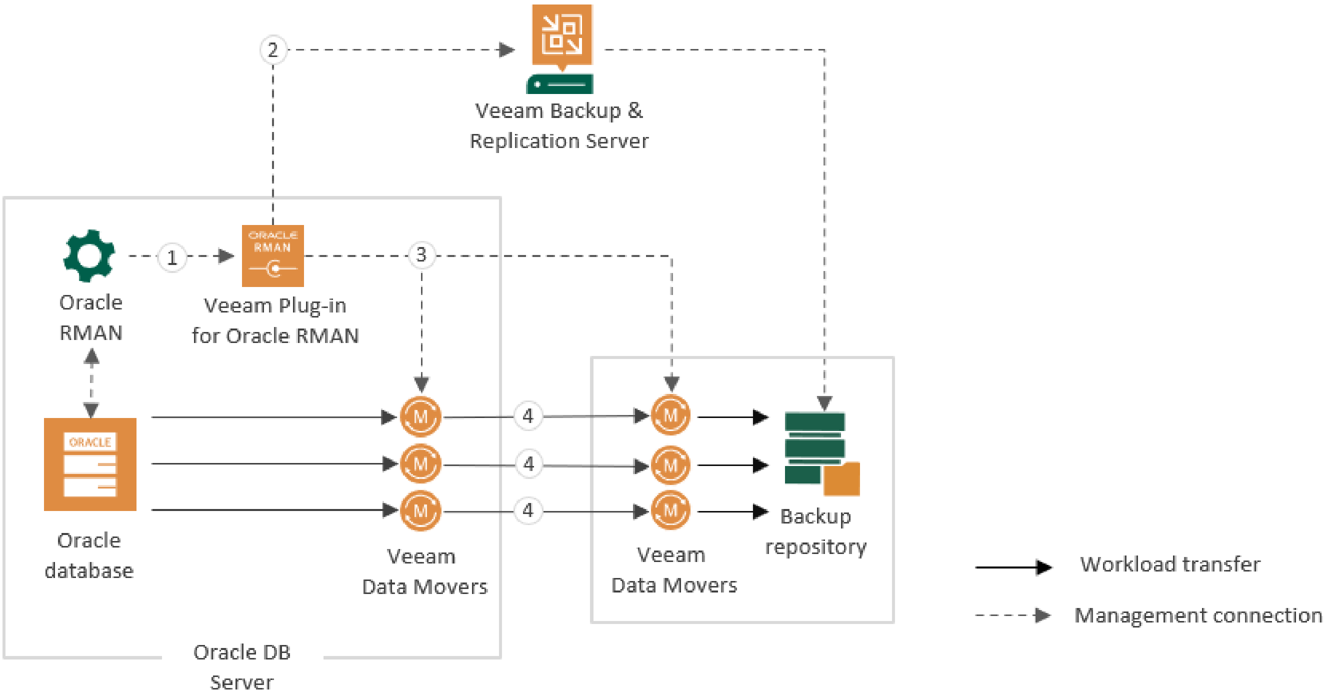
When use Oracle RMAN integrated with Veeam Plug-in, the database backup is performed in the following way:

1. After you launch a database backup process in the Oracle RMAN console, RMAN launches Veeam Plug-in services.
2. Veeam Plug-in connects to the Veeam Backup & Replication server and creates a backup job (if it hasn't been created earlier).
3. Veeam Plug-in starts Veeam Data Movers on the Oracle server and on the Veeam backup repository. Depending on the configured limit of RMAN channels, there will be multiple connections started in parallel.
4. Veeam Data Movers transport the backup data to the backup repository.



Multiple Repositories Deployment

Veeam Plug-in allows you to add up to 4 backup repositories. The backup process can be run in multiple channels. For each channel Veeam Plug-in creates a separate agent process.



Planning and Preparation

Before you start to use Veeam Plug-in for Oracle RMAN, read the environment planning recommendations and make sure that your environment meets system requirements.

- System Requirements
- Required Permissions
- Used Ports
- Licensing
- Oracle Environment Planning
- Veeam Environment Planning
- Veeam Backup Repositories
- Access and Encryption Settings on Repositories

System Requirements

Before you start using Veeam Plug-in for Oracle RMAN, make sure the following requirements are met.

Supported OSes

Veeam Plug-in for Oracle RMAN is supported for the following OSes:

- **Microsoft Windows:**
  - Microsoft Windows Server 2012/2012 R2
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2019
  - Microsoft Windows Server 2022

  > NOTE
  >
  > The Veeam Plug-in for Oracle RMAN installation wizard also installs Microsoft .NET Framework 4.6 if it does not detect this component on the machine during the product installation.

- **Linux:**
  - SUSE Linux Enterprise Server 11, 12, 15 (x86 and x86_64)
  - Red Hat Enterprise Linux 6.4–8.x (x86 and x86_64)
  - Oracle Linux 6.4–8.x (x86 and x86_64)
  - CentOS 6.4–8.x (x86 and x86_64): For non-production environments, as it is not officially supported by Oracle for their databases.
- **Unix:**
  - Oracle Solaris 10, 11 (x86_64, SPARC)
  - IBM AIX 6.1, 7.1, 7.2, 7.3

Oracle Database

Veeam Plug-in for Oracle RMAN supports Oracle Database 11gR2, 12c, 18c, 19c, 21c: Standard and Enterprise Edition (Express Edition is not supported).

Supported Oracle RMAN features

Veeam Plug-in for Oracle RMAN supports the following Oracle RMAN features:

- Veeam Plug-in for Oracle RMAN will be registered as an SBT_TAPE device. All Oracle RMAN functionality that is supported with the SBT_TAPE device type will work. For example, Oracle ASM and Container DBs (CDBs).
- Veeam Plug-in for Oracle RMAN supports Oracle Real Application Clusters (Oracle RAC). Other cluster databases are not supported.

Veeam Backup & Replication

Mind the following compatibility of Veeam Backup & Replication and Veeam Plug-in versions:

- **Veeam Plug-in for Oracle RMAN 12** supports integration only with Veeam Backup & Replication version 12.
- **Veeam Plug-in for Oracle RMAN 11.0.101.1264** supports integration only with Veeam Backup & Replication version 11a Cumulative Patch P20211211 or later.
- **Veeam Plug-in for Oracle RMAN 11.0.100.1261 (11a Cumulative Patch P20211123)** supports integration with Veeam Backup & Replication version 11, 11a.
- **Veeam Plug-in for Oracle RMAN 11** supports integration only with Veeam Backup & Replication version 11.
- **Veeam Plug-in for Oracle RMAN 10.0.1.4854 (10a Cumulative Patch 20201202)** supports integration with Veeam Backup & Replication version 10, 11.
- **Veeam Plug-in for Oracle RMAN 10 (earlier than 10.0.1.4854)** supports integration only with Veeam Backup & Replication version 10.

Note that if you want to use the latest functionality, you must upgrade both Veeam Backup & Replication and Veeam Plug-in to the latest version.

Network

Veeam Plug-in should be able to establish a direct IP connection to the Veeam Backup & Replication server. Thus, Veeam Plug-in cannot work with the Veeam Backup & Replication server that is located behind the NAT gateway.

Permissions

Mind the required permissions for the following user accounts:

- OS User that Configures Veeam Plug-in
- User that Launches Backup/Restore in RMAN
- Veeam Backup Server User

OS User That Configures Veeam Plug-in

The account used for configuring Veeam Plug-in must have the following permissions.

- **For Linux and Unix machines**:

  To configure Veeam Plug-in on a Linux or Unix machine, use an account which is a member of the OSDBA (typically called as "dba") group and has SYSDBA privileges.

- **For Microsoft Windows machines**:

  To configure Veeam Plug-in on a Microsoft Windows machine, use an account which is a member of the ORA_DBA group and has SYSDBA privileges.

User That Launches Backup/Restore in RMAN

The account used for starting Oracle RMAN backup and restore processes Veeam Plug-in must have the following permissions.

- **For Linux and Unix**:

  To launch RMAN backup or restore, you can use any user account that has required set of privileges for backup operations on the Oracle side. Starting from Oracle Database 12c, Oracle recommends to use the SYSBACKUP role. For details, see the Configuring Privilege and Role Authorization section of the Oracle Database Security Guide.

  During the backup process, Veeam Plug-in connects to the database to get DB properties. Thus, Linux/Unix user that started the RMAN client must be a member of the OSDBA (typically called as "dba") group and has SYSDBA privileges.

  > **IMPORTANT**
  >
  > If you use the CONNECT string with the channel allocation command in the Oracle RAC environment, the plug-in manager process will be started by the owner of the Oracle listener, not by the user that started the RMAN client. Thus, if the listener is owned by a cluster service user (`grid`) that is not a member of the OSDBA group and doesn't have SYSDBA privileges, the plug-in manager will not be able to collect database properties and the backup will fail. As a workaround, you can add DBA privileges to the `grid` user.

- **For Microsoft Windows**:

  To launch RMAN backup or restore, you can use any user account that has required set of privileges for backup operations on the Oracle side. Starting from Oracle Database 12c, Oracle recommends to use the SYSBACKUP role. For details, see the Configuring Privilege and Role Authorization section of the Oracle Database Security Guide.

During the backup process, Veeam Plug-in connects to the database to get DB properties. Thus, the Oracle Home user must be a member of the ORA_DBA group and the OS authentication must be enabled for this user.

Veeam Backup Server User

The account which is used to authenticate against Veeam Backup & Replication must have access permissions on required Veeam repository servers. To learn how to configure permissions on repositories, see Granting Access to Repositories.

The Veeam Plug-in for Oracle RMAN uses Windows authentication methods of the Veeam Backup & Replication server to establish a connection to this server and to the backup target. It is recommended to create one user for each Veeam Plug-in server or RAC.

To work with backups created by Veeam Plug-in, you can use only the account used for creating the backup. If you want to use another account, assign the *Veeam Backup Administrator* role or *Veeam Backup Operator* and *Veeam Restore Operator* roles to the account. To learn how to assign Veeam Backup & Replication roles, see the Users and Roles section of the Veeam Backup & Replication Guide.

Ports

To enable proper work of Veeam Plug-ins, make sure that the following ports are open.

Oracle Database Server

The following table describes network ports that must be opened to ensure proper communication of the Oracle server and backup infrastructure components.

From	To	Protocol	Port	Notes
Oracle server where Veeam Plug-in is installed	Veeam Backup & Replication server	TCP	10006	Default port used for communication with the Veeam Backup & Replication server. Note that data between Veeam Plug-ins and backup repositories is transferred directly, bypassing the Veeam Backup & Replication server.
	Backup repository server or gateway server*	TCP	2500 to 3300**	Default range of ports used as data transmission channels. For every TCP connection that a backup process uses, one port from this range is assigned.
	Oracle server (localhost)	TCP	6791+; 2500 to 3300**	Local connections between Veeam Plug-in and source Data Movers.

* For NFS share, SMB share repositories, and Dell Data Domain, HPE StoreOnce deduplication storage appliances, Veeam Backup & Replication uses an auxiliary backup infrastructure component — gateway server. For details, see the Gateway Server section of the Veeam Backup & Replication User Guide.

** This range of ports applies to newly added backup infrastructure components. If you upgrade to Veeam Backup & Replication 10.0 from earlier versions of the product, the range of ports from 2500 to 5000 applies to the already added components.

Backup Repositories and Gateway Servers

Depending on the type of backup repositories that you use for Veeam Plug-in backups, the following ports must be open to allow communication between backup infrastructure components.

From	To	Protocol	Port	Notes
Veeam Backup & Replication server	Backup repository server or gateway server*	TCP	2500 to 3300**	Default range of ports used as data transmission channels. For every TCP connection that a backup process uses, one port from this range is assigned.

From	To	Protocol	Port	Notes
Direct Attached Storage				
Veeam Backup & Replication server	Linux server used as a backup repository or gateway server	TCP	22	Port used as a control channel from the Veeam Plug-in server to the target Linux host.
	Microsoft Windows server used as a backup repository or gateway server	TCP UDP	135, 137 to 139, 445	Ports used as a management channel from the Veeam Plug-in server to the Repository/Gateway server. Also, the ports are used to deploy Veeam components.
		TCP	6160, 6162	Default ports used by the Veeam Installer Service and Veeam Data Mover Service
Network Attached Storage				
Gateway server (specified in the SMB share repository settings)	SMB server	TCP	445	Default port used by SMB transport protocol.
		TCP UDP	135, 137 to 139	SMB/Netbios name resolution for SMB protocol (needed in some cases). For details, see the Used Ports section of the Veeam Backup & Replication User Guide.
Gateway server (specified in the NFS share repository settings)	NFS server	TCP UDP	111, 2049	Standard NFS ports used as a transmission channel from the gateway server to the target NFS share.
Dell Data Domain				
Veeam Backup & Replication server	Dell Data Domain	TCP	111	Port used to assign a random port for the mountd service used by NFS and DDBOOST. Mountd service port can be statically assigned.

From	To	Protocol	Port	Notes
or **Gateway server**	For more information, see this Dell KB article.	TCP	2049	Main port used by NFS. To change the port, you can use the `‘nfs set server-port’` command. Note that the command requires SE mode.
		TCP	2052	Main port used by NFS MOUNTD. To change the port, you can use the `'nfs set mountd-port'` command. Note that the command requires SE mode.
HPE StoreOnce				
Veeam Backup & Replication server or **Gateway server**	HPE StoreOnce	TCP	9387	Default command port used for communication with HPE StoreOnce.
			9388	Default data port used for communication with HPE StoreOnce.
ExaGrid				
Veeam Backup & Replication server	ExaGrid	TCP	22	Default command port used for communication with ExaGrid.
Quantum DXi				
Veeam Backup & Replication server	Quantum DXi	TCP	22	Default command port used for communication with Quantum DXi.

* For NFS share, SMB share repositories, and Dell Data Domain, HPE StoreOnce deduplication storage appliances, Veeam Backup & Replication uses an auxiliary backup infrastructure component — gateway server. For details, see the Gateway Server section of the Veeam Backup & Replication User Guide.

** This range of ports applies to newly added backup infrastructure components. If you upgrade to Veeam Backup & Replication 10.0 from earlier versions of the product, the range of ports from 2500 to 5000 applies to the already added components.

For detailed list of ports used by Veeam Backup & Replication server and backup repositories, see the Used Ports section of the Veeam Backup & Replication User Guide.

Licensing

To use the Veeam Plug-in functionality, you must have a valid Veeam Backup & Replication license. Licenses are installed and managed on the Veeam Backup & Replication server that is connected to the Veeam Plug-in server. If the license is not valid or out of resources, Veeam Plug-in backup jobs fail.

This guide provides information only on specifics of Veeam licenses for Veeam Plug-ins. For terminology and general information about Veeam Licensing, see Veeam Licensing Policy.

In this section:

- Licensed Objects
- Supported License Types and Packages
- Obtaining and Managing Licenses

Licensed Objects

An Oracle server is assumed protected if it has been processed by a Veeam Plug-in backup job in the last 31 days.

If you are using any instance-based (Veeam Universal Licensing) license on your Veeam Backup & Replication, you don't need to install any additional licenses. A protected Oracle server consumes one instance unit from the license. Oracle servers processed by backup copy jobs are not regarded as protected VMs, these types of jobs provide an additional protection level for VMs that are already protected with Veeam Plug-in backup jobs.

A machine protected by both Veeam Plug-in and Veeam Backup & Replication will consume a license only once. For example, you have an Oracle server that you back up using Veeam Plug-in. You also back up this server using image-level backup functionality of Veeam Backup & Replication. In this case, only one license will be consumed.

NOTE

[For Perpetual per-socket licenses] If you are using a legacy perpetual per-socket license, a license is required for each hypervisor CPU socket occupied by protected Oracle servers.

A socket is consumed from the license only if the hypervisor where protected servers reside is added to the Veeam Backup & Replication infrastructure. If the hypervisor is not added to the Veeam Backup & Replication infrastructure, an instance unit will be consumed from the license. To learn how to add a hypervisor to the Veeam Backup & Replication infrastructure, see the Virtualization Servers and Hosts section of the Veeam Backup & Replication User Guide.

IMPORTANT

[For Oracle RAC] The license is required for all cluster nodes, even if Veeam Plug-in is installed only on one of the nodes.

Supported License Types

You can use Veeam Plug-ins with the following license types and packages. Note that this guide contains information on specifics of Veeam license packages only for Veeam Plug-ins. For the full list of license packages, see Pricing and Packaging.

- **For Veeam Universal Licensing**:

  You can use Veeam Plug-ins with all license packages (*Veeam Backup Essentials, Veeam Backup & Replication, Veeam Availability Suite*).

  Note that if you use the *Rental* license type, functionality of Veeam Plug-ins is supported only for the *Enterprise Plus* edition of Veeam Backup & Replication.

- For Perpetual Socket license:

  Functionality of Veeam Plug-ins is supported only for the *Enterprise Plus* edition of Veeam Backup & Replication.

Obtaining and Managing Licenses

To learn how to install a license and monitor licensed objects, see the Licensing section in the Veeam Backup & Replication User Guide.

Oracle Environment Planning

Before you deploy Veeam Plug-in, mind the following requirements and limitations.

Deployment

[For Linux OS and Unix] To install Veeam Plug-in, the `/opt/veeam` directory must be writable.

Oracle Temp Tablespace

Veeam Plug-in runs SQL queries on the Oracle database to collect statistical information about the RMAN job processes. As with any other SQL queries, Oracle can decide based on availability of hardware resources to use Oracle Temp Tablespace for these queries. Make sure that you configure the Temp Tablespace resources to avoid shortage of temporary tablespace.

Scheduling

You can schedule backup processes with all Oracle RMAN relevant scheduling options like Cron, Windows Task Scheduler, UC4 and TWS.

If you use Veeam Backup & Replication or Veeam Agents to create image-level backups of the Oracle server, you can schedule the backup job and run Oracle RMAN backup scripts along with the backup job. For detailed instructions on how to add Oracle RMAN scripts to a backup job, see the one of the following guides:

- For Veeam Backup & Replication: Pre-Freeze and Post-Thaw Scripts section of the Veeam Backup & Replication User Guide.
- For Veeam Agent for Windows: Pre-Freeze and Post-Thaw Scripts section of the Veeam Agent for Windows User Guide.
- For Veeam Agent for Linux: Pre-Freeze and Post-Thaw Scripts section of the Veeam Agent for Linux User Guide.

> NOTE
>
> If you want to use Oracle RMAN scripts within backup jobs of Veeam Backup & Replication or Veeam Agents, mind the following:
>
> - A backup job does not control the workflow of Oracle RMAN scripts. The backup job invokes the script and gets its exit status when the script is finished. Backup job logs show whether the script executed successfully or failed. The script is considered to be executed successfully if "0" is returned. In order to see that the script failed, configure the script to return an exit status different than "0" in case of any errors.
> - The default timeout for a custom script in a backup job is 10 minutes. If it takes longer than 10 minutes to run the script, you can open a support ticket to increase the timeout.

Oracle RAC

Mind the following for Oracle RAC:

- It is recommended to install Veeam Plug-in on each RAC server that is responsible for the backup operations. If the plug-in is not installed on all nodes, the backup process may fail when RMAN selects another node.
- Veeam Plug-in supports parallel execution of all operations supported by Oracle RMAN: backup, restore, crosscheck, remove. This applies to execution of these commands on one or multiple databases residing on one or multiple RAC nodes.
- If you use Veeam Explorer for Oracle to restore a RAC database with different settings, it will not be restored as a cluster database. It will be restored as a standalone database.

Oracle Backup Encryption

The Oracle Secure Backup SBT library is the only interface that supports RMAN encrypted backups. Veeam Plug-in does not support encrypted backups of Oracle databases. If the backup encryption is enabled, Veeam Plug-in backup jobs fail with the following error: `ORA-19919: encrypted backups to tertiary storage require Oracle Secure Backup`. To avoid the error, you must disable the backup encryption on the Oracle side.

Backup File Naming

During backup and restores, Veeam Plug-in uses the `repositoryID` parameter from the plug-in configuration file (`veeam_config.xml`). In the `veeam_config.xml` file, the repository ID is stored in the following format: `repositoryID=“xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”`.

To name backup files, Veeam Plug-in uses the following format by default:

```
CONFIGURE CHANNEL DEVICE TYPE sbt PARMS 'SBT_LIBRARY=/opt/veeam/VeeamPluginforO
racleRMAN/libOracleRMANPlugin.so’ FORMAT 'xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/
RMAN_%I_%d_%T_%U.vab’;
CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE SBT_TAPE TO '%F_RMAN_AU
TOBACKUP.vab’;
```

- If you select multiple Veeam backup repositories and disable RMAN copy processing:

  Backup files will be read by default from the first selected repository. Same naming rules apply as in the single repository scenario.

- If you select multiple Veeam backup repositories and enable RMAN copy processing, you must use the repository ID with the “/” sign as a prefix for the backup file names (see the example above). This allows RMAN to directly access the requested backup file on one of the copy extents.

NOTE

[For Linux, Unix, Windows] In a backup file name, you cannot use symbols reserved by Microsoft Windows: "<" , ">", ":", "/", "\", "|", "?", "*". To learn more about file naming conventions, see Microsoft Documentation.

Backup of Control File and SPFILE

If you set CONFIGURE CONTROLFILE AUTOBACKUP to ON, then RMAN automatically creates a control file and an SPFILE backup after you run the BACKUP command. For details, see the Oracle Documentation.

Controlfile Autobackup File Naming

If you perform the restore with different name and settings using Veeam Explorers for Oracle, you must enable the autobackup of the control file. If you use the Controlfile Autobackup option, the Veeam Plug-in configuration wizard creates the following RMAN configuration entry:

```
CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE SBT_TAPE TO '%F_RMAN_AU
TOBACKUP.vab’;
```

If you enable the control file autobackup after configuring Veeam Plug-in, you can start the configuration wizard again. The control file backup naming option will be set to default.

Parallel Processing

Veeam Plug-in supports parallel backup processing for up to 4 backup repositories or scale-out backup repositories. In the plug-in configuration wizard, if you select more than one repository, the parallelism functionality will be enabled automatically.

Note that your Oracle Enterprise Edition must be able to use RMAN parallel processing.

> **TIP**
>
> If you want to recover the Veeam Plug-in job folder to a specific point in time state, you can use Storage Replication (plus import) or the File Backup to Tape job of Veeam Backup & Replication.

Additional Files to Back up

Veeam Plug-in creates backups of databases and logs. Apart from these files,

Oracle Home

- It is recommended to back up the Oracle home folder in addition to RMAN backups. You can back it up with Veeam Backup & Replication or Veeam Agents.
- If the Oracle home folder is on a shared disk, you can use the file-level backup functionality of Veeam Backup & Replication or Veeam Agent for Linux. Alternatively, you can copy the Oracle home folder to a non-shared disk before the backup.

Oracle Recovery Catalog

You can back up the Oracle Recovery Catalog with Veeam Plug-in on the Recovery Catalog server according to the Oracle procedures. For details, see the Managing a Recovery Catalog section of the Database Backup and Recovery User's Guide.

Veeam Plug-in for RMAN Configuration File

You can back up the Veeam Plug-in configuration file. The file is located in the following directory:

- [Linux or Unix]: `/opt/veeam/VeeamPluginforOracleRMAN/veeam_config.xml`
- [Windows]: `%PROGRAMFILES%\Veeam\VeeamPluginforOracleRMAN\veeam_config.xml`

> **NOTE**
>
> You can also create an image-level backup of the Oracle server using the image-level backup functionality of Veeam Backup & Replication or Veeam Agents.

Disabling Veeam Explorer Processing

You can disable Veeam Explorer based restore for specific Oracle servers. To disable the restore on the Veeam Explorer for Oracle side, do the following:

- [Linux or Unix] On the Oracle server, log in as a user with the Oracle Administrator rights and create an empty file in the following directory: `/etc/veeam/disablerestore`
- [Windows] On the Oracle server, create an empty file in the following directory: `%ProgramData%\Veeam\disablerestore`

Oracle Data Guard

Since version 11, Veeam Plug-in for Oracle RMAN has an official support of Oracle Data Guard.

Database Recovery

If you want to restore a database with a different name and settings using Veeam Explorer for Oracle, the database must use SPFILE. If SPFILE is not used, you will see a warning during a plug-in configuration.

Veeam Environment Planning

Before you deploy Veeam Plug-in, keep in mind the following requirements and limitations.

- RMAN Channels and Resource Consumption
- Veeam Backup Job Name
- Hosting Environments

RMAN Channels and Resource Consumption

Any parallel channel started by RMAN will use one Veeam backup repository task slot. By design, Oracle Standard Edition can work with one channel. Oracle Enterprise Edition has the option to use multiple channels and you can configure them in the Veeam Plug-in configuration wizard or at the ALLOCATE CHANNEL definition in RMAN scripts. It is recommended to carefully plan repository task slots, so that Oracle RMAN can work with multiple channels in parallel when configured.

The following hardware resources are recommended based on tests on Skylake processors:

- **Oracle server**: 1 CPU core and 200 MB of RAM per currently used channel. Note that resource consumption on the Oracle server depends on hardware and Oracle settings.
- **Backup repository server**: 1 CPU core and 1 GB of RAM per 5 currently used channels.

  These resources are recommended only if you use a dedicated backup repository for Veeam Plug-in backups. If you use the same backup repository for Veeam Plug-in backups and VM backups created by Veeam Backup & Replication or Veeam Agents, consider adding the mentioned above hardware resources based on usual load on your backup repository. For details on hardware requirements for a backup repository, see the System Requirements section of the Veeam Backup & Replication User Guide.

  We recommend to contact your Veeam system engineer to optimize the channel settings and resource allocation. Also, consider the following:

  - It is recommended to use a separate backup repository for Veeam Plug-in backups.
  - The control file does not use a repository task slot and will be processed even if there are no free task slots.
- **Veeam Backup & Replication server**: during manual metadata operations such as import of backup files, the Veeam Backup & Replication server needs additional 15 GB of RAM per 1 million files located in the same backup job folder.

Veeam Backup Job Name

- On the Veeam Backup & Replication server, the backup job name will be created automatically based on the server or cluster name and selected repository.
- For environments that use Oracle RMAN copy processing, one job per repository is created.

Backup Files

- A .VAB file stores a compressed copy of an Oracle database. Veeam Plug-in creates .VAB files for both full and incremental backups.
- A .VASM file stores metadata that contain information about the backup. A .VASM file is created for each .VAB file. The .VASM files are used by Veeam Backup & Replication to get data about Veeam Plug-in backups.
- A .VACM file stores metadata of a backup job object.

Hosting Environments

By default, Veeam Plug-in uses the Oracle server hostname to create a Veeam Backup & Replication job object and backup folder. To be able to distinguish individual servers, it is recommended to set the following entry within the Veeam configuration XML file: `<PluginParameters customServerName="hostname.domain.tld" />`

- [Linux or Unix]: `/opt/veeam/VeeamPluginforOracleRMAN/veeam_config.xml`
- [Windows]: `%PROGRAMFILES%\Veeam\VeeamPluginforOracleRMAN\veeam_config.xml`

If your servers that have the same hostname in multiple environments, you must add the following entries in the plug-in configuration file:

```
<PluginParameters useFQDNInServerName="true" />
```

> **IMPORTANT**
>
> For security reasons, it is recommended to use separate repositories for different customers and limit the Veeam Repository Authentication to the specific customer.

Veeam Backup Repositories

Veeam Plug-ins store backup files in repositories added to the Veeam Backup & Replication infrastructure. In this section, you can find the list of supported backup repositories and limitations for Veeam Plug-in backups.

Supported Backup Repositories

Veeam Plug-in for Oracle RMAN supports integration with the following types of repositories added to the Veeam Backup & Replication infrastructure:

- Windows Server
- Linux Server
- CIFS (SMB) Share
- Dell Data Domain Boost
- Quantum DXi
- ExaGrid
- HPE StoreOnce. If you plan to use HPE StoreOnce as a backup repository for Veeam Plug-in backups, the total number of stored files (data and metadata) must not exceed 3,000,000 per Catalyst store. If necessary, multiple Catalyst stores may be created on the same StoreOnce system.
- NFS File Share
- Hardened Repository

You can also use scale-out backup repositories that contain supported repository types.

Backup Repository Limitations

- For Veeam Plug-in backups, the warning which indicates that free space on a storage device has reached a specified threshold is configured in the `veeam_config.xml` file of Veeam Plug-in. The warning settings in the Veeam Backup & Replication console does not affect this setting.

  To configure the warning settings, add the following parameter in the `veeam_config.xml` file.

  ```
  <PluginParameters repositoryFreeSpacePercentWarning="10" />
  ```

- The plug-in configuration wizard will not show repositories where the **Encrypt backups stored in this repository** option is enabled. To learn how to disable the encryption option, see Access and Encryption Settings on Repositories.

  If you want to use the same backup target with the repository-based encryption and Veeam Plug-ins, create a second repository in the subfolder for Veeam Plug-in backups.

- Veeam extract utility cannot extract Veeam Plug-in backup files. By design of Oracle RMAN, these files cannot be imported “as files” to RMAN as they contain additional metadata bound to the used SBT device.

Veeam Scale-Out Backup Repositories

If you want to store Veeam Plug-in backups in scale-out backup repositories, mind the following:

- If you want to add a backup repository as an extent to a scale-out backup repository and Veeam Plug-in backups are present on this backup repository, you must do the following:

  a. In the Veeam Backup & Replication console, select Veeam Plug-in backup files that reside in this backup repository and remove them from configuration. For details, see Removing backups from configuration. Note that this action does not delete the backups from the repository.

  b. In the Veeam Backup & Replication console, delete the Veeam Plug-in backup job. For details, see Deleting Jobs.

  c. Add the repository as an extent to the scale-out repository. For details, see Extending Scale-Out Repositories.

  d. Rescan the scale-out repository. For details, see Rescanning Scale-Out Repositories.

  > NOTE
  >
  > Names of backup files and paths to backup files must contain only allowed characters:
  >
  > - Alphanumeric characters: `a-zA-Z0-9`
  > - Special characters: `_-.+=@^`
  > - Names of backup files and paths to backup files must not contain spaces.

  e. On the Veeam Plug-in server, set the scale-out repository as the target for backups using the following command:

  ```
  OracleRMANConfigTool --set-repositories
  ```

  f. Map the imported backups using the following command:

  ```
  OracleRMANConfigTool --map-backup
  ```

- For Veeam Plug-in backups and backup copies, the *Performance* policy of a scale-out repository functions differently:

  a. Veeam Backup & Replication checks if there are extents without warning on free space insufficiency. If all extents have the warning, Veeam Backup & Replication uses an extent with the largest amount of free space that has a free task slot.

  b. If there are extents without the warning, Veeam Backup & Replication checks if there are incremental extents with free task slots. If there are no incremental extents with free task slots, Veeam Backup & Replication uses a full extent with the least amount of used task slots.

  c. If there are incremental extents with free task slots, Veeam Backup & Replication sends backup files to an incremental extent with the least amount of used task slots. If the amount of used tasks is the same, an extent with the largest amount of free space.

  To learn more about file placement policies of scale-out repositories, see Backup File Placement section of the Veeam Backup & Replication guide.

- If a scale-out repository is configured in the **Data locality** policy, repository extents will be selected according to the amount of free space for each Oracle RMAN connection. If there are two extents with one slot on each extent, the backup will be launched on two streams (one on each extent).

Capacity Tier

You can configure Veeam Backup & Replication to transfer Veeam Plug-in backup files to a capacity tier. Both policies (Move policy, Copy policy) are supported for Veeam Plug-in backups with the following limitations:

- For Veeam Plug-in backup files, capacity tier does not verify whether data that is being moved is unique and has not been offloaded earlier. Thus, it is highly recommended to check the pricing plans of your cloud storage provider to avoid additional costs for offloading and downloading backup data.
- Capacity tier does not track dependencies of full and incremental Veeam Plug-in backup files. Thus, mind the following:
    - [For the Move policy] When backup files are transferred to the capacity tier, Veeam Backup & Replication takes into account only the creation time of backup files. Make sure that the operational restore window is either longer than the whole backup chain cycle period or exceeds that period. Otherwise, you may encounter the scenario when full backup files are transferred to the capacity tier and their increment backup files still remain in the performance tier.
    - The capacity tier immutability expiration date does not have the additional block generation period. The immutability expiration date is based only on the number of days specified in settings of the object storage backup repository.
- If a scale-out repository is down, you cannot restore from the Veeam Plug-in backup files stored on the capacity tier. In this case, you can only import the backup files to Veeam Backup & Replication manually and then perform data recovery operations.
- If you use a capacity tier that has been created in Veeam Backup & Replication version 10, you cannot transfer Veeam Plug-in backup files to a capacity tier. However, if you want to transfer them manually, do the following:
    - If the backup files are created by Veeam Plug-in version 10, upgrade the metadata of backup files as described in Upgrading Metadata Files to New Format.
    - Run the Set-VBRScaleOutBackupRepository PowerShell command with the –`EnablePluginBackupOffload` parameter to offload backup files to the capacity tier.

Hardened Repository

You can configure Veeam Backup & Replication to transfer Veeam Plug-in backup files to a hardened repository. The hardened repository helps to protect Veeam Plug-in backup files from loss as a result of malware activity or unplanned actions. Backup files in the hardened repository become immutable for the time period specified in the backup repository settings. During this period, backup files stored in the repository cannot be modified or deleted.

For Veeam Plug-in for Oracle RMAN backups, immutability works according to the following rules:

- Immutability is applied to backup (VAB) files and backup metadata (VASM) files. Backup job metadata (VACM) files are not immutable.
- Backup files become immutable for the configured time period (minimum 7 days, maximum 9999 days).
- The count of the immutability period starts when the backup metadata (VASM files) has been created during the backup job session.
- The immutability period is not extended for the active backup chain.
- Every 1 hour, the immutability service that runs in the background detects backup files that do not have the immutability flag and sets the immutability flag on the necessary backup files.

Data Restore from Hardened Repository

As a result of malware activity or unplanned actions, backup job metadata (VACM) files may become unavailable in the hardened repository. In this case, to restore data from the hardened repository, you must re-create the VACM file. For more information, see Restore from Hardened Repository.

Access and Encryption Settings on Repositories

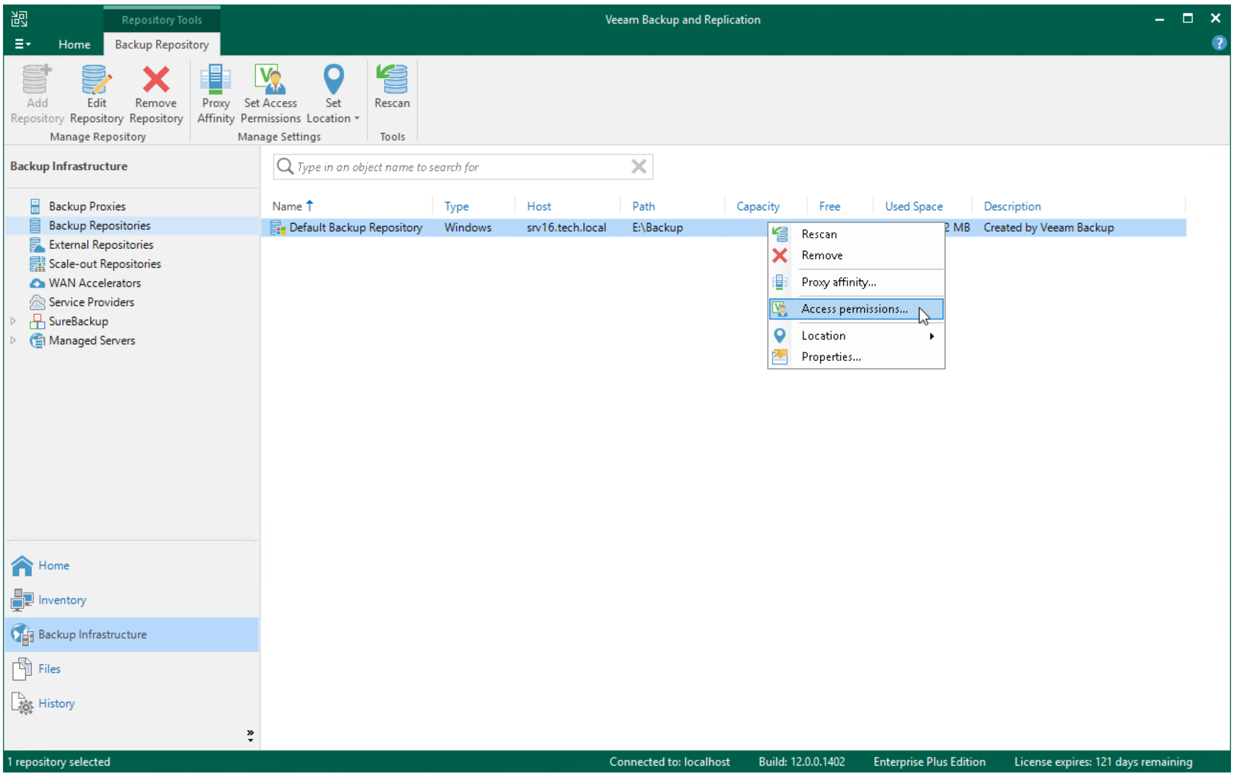
When you configure Veeam Plug-in, you specify an account that must be used to connect to the Veeam Backup & Replication server. To be able to store backups in a backup repository, the specified account must have access permissions on the target backup repository.

To grant access permissions, do the following:

1. In Veeam Backup & Replication, open the **Backup Infrastructure** view.

2. In the inventory pane, click the **Backup Repositories** node or the **Scale-out Repositories** node.

3. In the working area, select the necessary backup repository and click **Set Access Permissions** on the ribbon or right-click the backup repository and select **Access permissions**.



Name	Type	Host	Path	Capacity	Free	Used Space	Description
Default Backup Repository	Windows	srv16.tech.local	E:\Backup			2 MB	Created by Veeam Backup

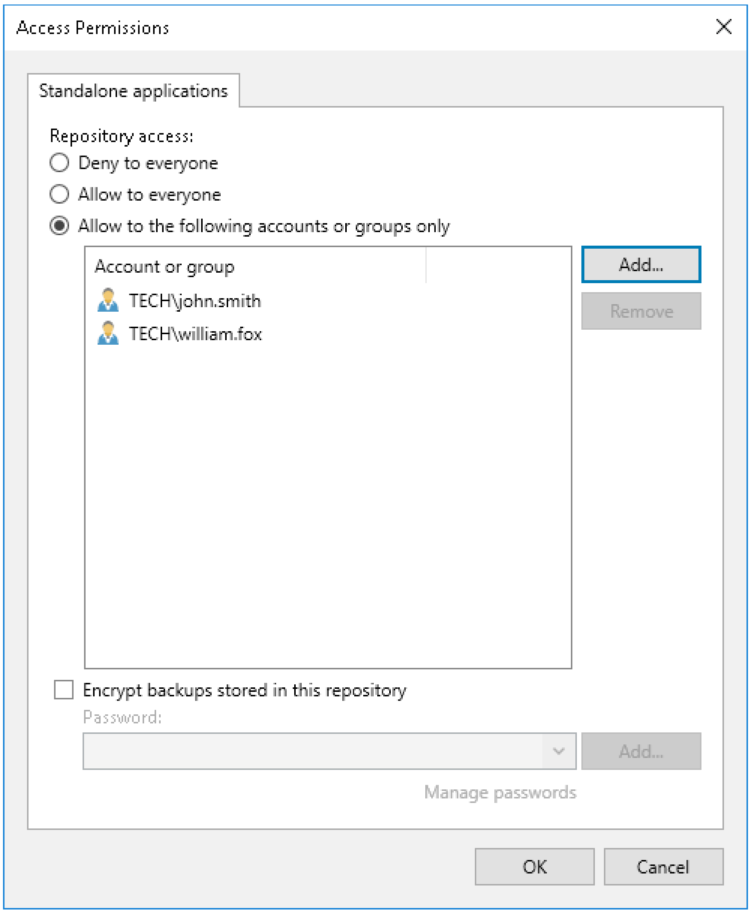
4. In the **Access Permissions** window, on the **Standalone applications** tab specify to whom you want to grant access permissions on this backup repository:

   - *Allow to everyone* — select this option if you want to grant repository access to any user. This option is equal to granting access rights to the *Everyone* group in Microsoft Windows (anonymous users are excluded). For security reasons, the option is not recommended for production environments.

   - *Allow to the following accounts or groups only* — select this option if you want only specific users to be able to store backups in this repository. Click **Add** to add the necessary users and groups to the list.

5. Veeam Plug-ins cannot send backups or backup copies to a backup repository where encryption is enabled. Thus, make sure that the **Encrypt backups stored in this repository** check box is not selected.

6. Click **OK**.



Access Permissions

Standalone applications

Repository access:

○ Deny to everyone

○ Allow to everyone

● Allow to the following accounts or groups only

Account or group
TECH\john.smith
TECH\william.fox

□ Encrypt backups stored in this repository

Password:

Deployment and Configuration

Veeam Plug-in for Oracle RMAN is a feature of Veeam Backup & Replication. This guide gives instructions on how to deploy Veeam Plug-in assuming that you already have deployed Veeam Backup & Replication and configured a backup repository. To learn how to deploy Veeam Backup & Replication, see the Veeam Backup & Replication User Guide for your platform.

To be able to use Veeam Plug-in for Oracle RMAN, you must install the plug-in on the Oracle server and configure the plug-in settings:

- Installing Veeam Plug-in for Oracle RMAN
- Configuring Veeam Plug-in for Oracle RMAN

See Also

- Upgrading Veeam Plug-in for Oracle RMAN
- Importing/Exporting Plug-in Settings
- Importing Backups
- Upgrading Backup Files
- Uninstalling Veeam Plug-in for Oracle RMAN

Installing Veeam Plug-in for Oracle RMAN

See one of the following guides depending on which OS is installed on the target machine.

- Installing Veeam Plug-in on Linux machines
- Installing Veeam Plug-in on Windows machines
- Installing Veeam Plug-in on Oracle Solaris machines
- Installing Veeam Plug-in on IBM AIX machines

Installing Plug-in on Linux

Veeam Plug-in for Oracle RMAN is an additional component of Veeam Backup & Replication, and the installation package of the plug-in is included in the Veeam Backup & Replication installation ISO file.

You can install the plug-in using the `.RPM` package or extract the plug-in files from the `.TAR.GZ` archive. Depending on the type of package suitable for your OS, perform steps in one of the following guides:

- Installing Plug-in from .RPM Package
- Unpacking Plug-in from .TAR.GZ Archive

> **IMPORTANT**
>
> Mind the following:
>
> - Veeam Plug-in for Oracle RMAN must be installed on the Oracle Database server.
> - The `/opt/veeam` directory must be writable.
> - To install the plug-in, use the `sudo` command or a user with root privileges.

Installing Plug-in from .RPM Package

To install Veeam Plug-in on a Linux machine, perform the following steps.

1. Mount the Veeam Backup & Replication installation disk (`VeeamBackup&Replication_12.0.0.1420.iso`).

   If you deploy Veeam backup infrastructure for the first time, you can download the Veeam Backup & Replication installation disk image from the Veeam Backup & Replication: Download page.

2. Open the mounted disk image and go to the `Plugins\Oracle RMAN\Linux` directory.

3. Upload the `VeeamPluginforOracleRMAN-12.0.0.1420-1.x86_64.rpm` package to the Oracle server. If you need the 32-bit version, choose the `i386` package.

4. To install Veeam Plug-in, run the following command:

```
rpm -i VeeamPluginforOracleRMAN-12.0.0.1420-1.x86_64.rpm
```

Unpacking Plug-in from .TAR.GZ Archive

To extract plug-in files from the `.TAR.GZ` archive, perform the following:

1. Mount the Veeam Backup & Replication installation disk (`VeeamBackup&Replication_12.0.0.1420.iso`).

   If you deploy Veeam backup infrastructure for the first time, you can download the Veeam Backup & Replication installation disk image from the Veeam Backup & Replication: Download page.

2. Open the mounted disk image and go to the `Plugins\Oracle RMAN\Linux` directory*.*

3. Upload the `VeeamPluginforOracleRMAN.tar.gz` file to the Oracle server.

4. Create the `/opt/veeam` directory.

   ```
   mkdir /opt/veeam
   ```

5. Unpack the plug-in files from the archive to the `/opt/veeam` directory.

   ```
   tar -xzvf VeeamPluginforOracleRMAN.tar.gz -C /opt/veeam
   ```

Installing Plug-in on Microsoft Windows

You can install Veeam Plug-in for Oracle RMAN on Windows machines using a wizard or in an unattended mode. For instructions, see:

- Installing Veeam Plug-in on Windows machines
- Installing Veeam Plug-in in an unattended mode

> NOTE
>
> When you launch the installation file, it also installs Microsoft .NET Framework 4.5.2 if it does not detect this component on the machine during the product installation. In some cases, installation of .NET Framework requires a reboot of the machine. This can happen, for example, if you have an earlier version of .NET Framework installed on the machine and during the installation process it is used by third-party software.

Installing Plug-in on Windows Machine

Veeam Plug-in for Oracle RMAN is an additional component of Veeam Backup & Replication, and the installation package of the plug-in is included in the Veeam Backup & Replication installation ISO file.

To install Veeam Plug-in for Oracle RMAN on a Windows machine, do the following:

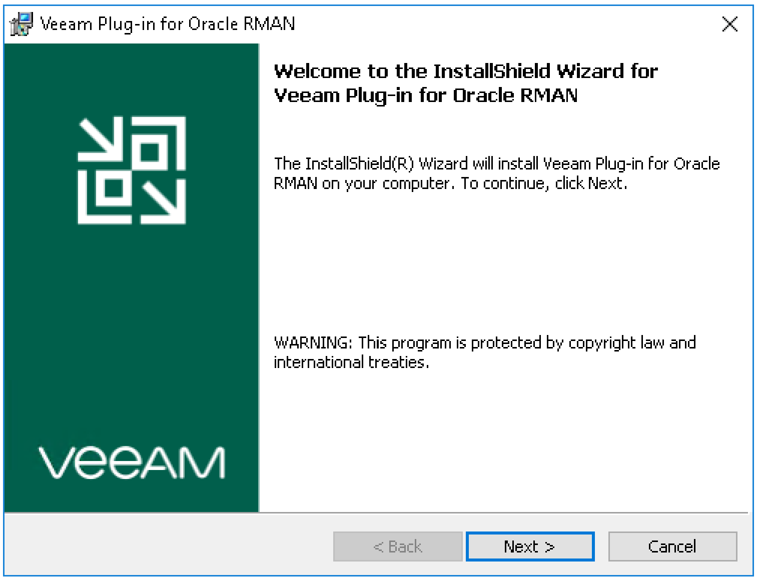
1. Mount the Veeam Backup & Replication installation disk (`VeeamBackup&Replication_12.0.0.1420.iso`).

   If you deploy Veeam backup infrastructure for the first time, you can download the Veeam Backup & Replication installation disk at: https://www.veeam.com/backup-replication-vcp-download.html.

2. In the installation disk folder go to `Plugins\Oracle RMAN\Windows.`

3. To launch the installation wizard, run the `VeeamPluginforOracleRMAN.exe` file.

4. At the welcome screen of the installation wizard, click **Next**.



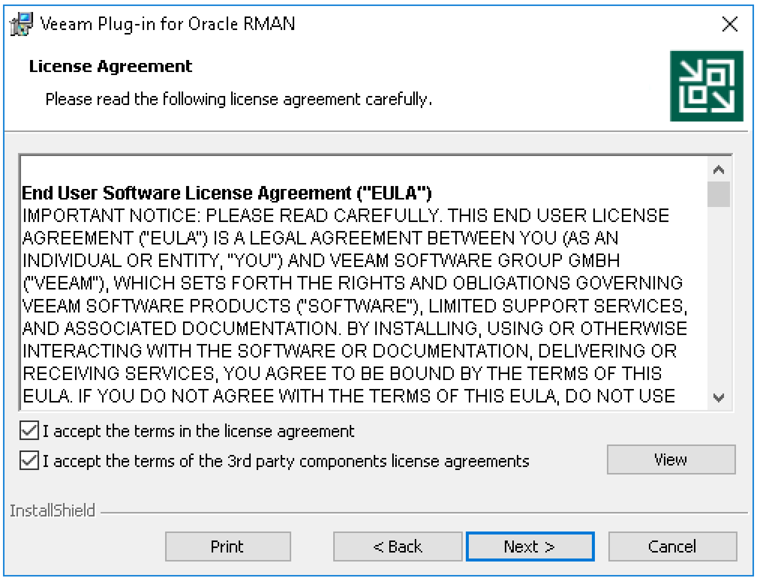
Veeam Plug-in for Oracle RMAN

Welcome to the InstallShield Wizard for Veeam Plug-in for Oracle RMAN

The InstallShield(R) Wizard will install Veeam Plug-in for Oracle RMAN on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

5. At the **License Agreement** step of the wizard, accept the terms of license agreements and click **Next**.



Veeam Plug-in for Oracle RMAN

License Agreement

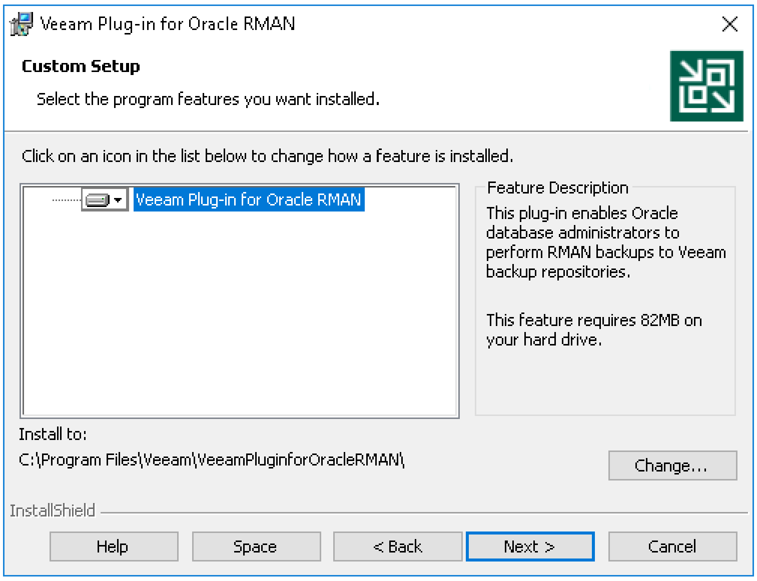
Please read the following license agreement carefully.

End User Software License Agreement ("EULA")
IMPORTANT NOTICE: PLEASE READ CAREFULLY. THIS END USER LICENSE AGREEMENT ("EULA") IS A LEGAL AGREEMENT BETWEEN YOU (AS AN INDIVIDUAL OR ENTITY, "YOU") AND VEEAM SOFTWARE GROUP GMBH ("VEEAM"), WHICH SETS FORTH THE RIGHTS AND OBLIGATIONS GOVERNING VEEAM SOFTWARE PRODUCTS ("SOFTWARE"), LIMITED SUPPORT SERVICES, AND ASSOCIATED DOCUMENTATION. BY INSTALLING, USING OR OTHERWISE INTERACTING WITH THE SOFTWARE OR DOCUMENTATION, DELIVERING OR RECEIVING SERVICES, YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA. IF YOU DO NOT AGREE WITH THE TERMS OF THIS EULA, DO NOT USE

☑ I accept the terms in the license agreement

☑ I accept the terms of the 3rd party components license agreements

6. At the **Custom Setup** step of the wizard, specify the installation path for Veeam Plug-in and click **Next**.



Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

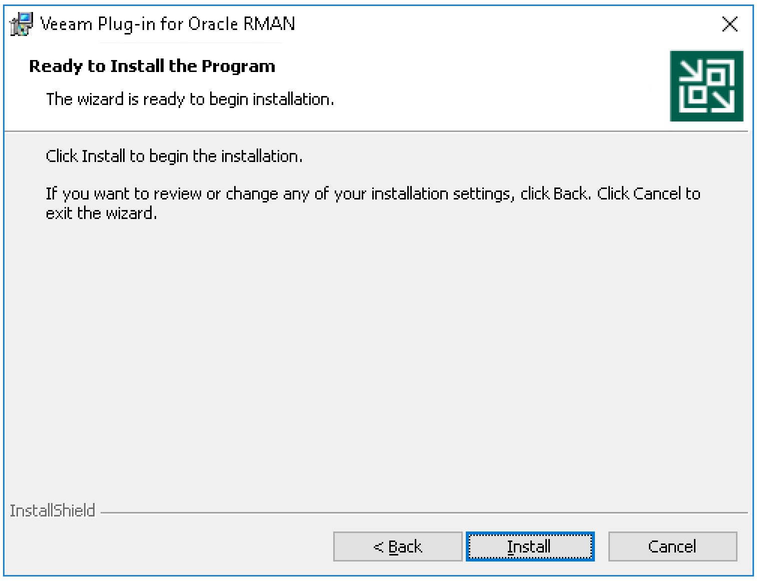
Feature Description

This plug-in enables Oracle database administrators to perform RMAN backups to Veeam backup repositories.

This feature requires 82MB on your hard drive.

Install to:
C:\Program Files\Veeam\VeeamPluginforOracleRMAN\

7. At the **Ready to Install the Program** step of the wizard, click **Install**.



Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

4. Wait for the installation process to complete and click **Finish** to exit the wizard.

Installing the Plug-in in Unattended Mode

You can install Veeam Plug-in for Oracle RMAN on a Windows machine in the unattended mode using the command line. Go to folder where the `VeeamPluginforOracleRMAN.exe` file resides and run the following command:

```
<path_to_exe>\VeeamPluginforOracleRMAN.exe /silent /acceptEula /acceptthirdpart
ylicenses
```

where `<path_to_exe>` is a path to the Veeam Plug-in for Oracle RMAN installation file.

Parameter	Description
/silent	Enables the silent mode.
/accepteula	Accepts EULA terms.
/acceptthirdpartylicenses	Accepts terms of third-party licenses.

Veeam Plug-in for Oracle RMAN uses the following codes to report about the installation results:

- 1000 — Veeam Plug-in for Oracle RMAN has been successfully installed.
- 1001 — prerequisite components required for Veeam Plug-in for Oracle RMAN have been installed on the machine. Veeam Plug-in for Oracle RMAN has not been installed. The machine needs to be rebooted.
- 1002 — Veeam Plug-in for Oracle RMAN installation has failed.
- 1101 — Veeam Plug-in for Oracle RMAN has been installed. The machine needs to be rebooted.

Installing Plug-in on Oracle Solaris

Veeam Plug-in for Oracle RMAN is an additional component of Veeam Backup & Replication, and the installation package of the plug-in is included in the Veeam Backup & Replication installation ISO file.

Veeam Plug-in for Oracle RMAN must be installed on a machine where the target Oracle Database is deployed.

> **NOTE**
>
> To install Veeam Plug-in, the `/opt/veeam` directory must be writable.

To install Veeam Plug-in for Oracle RMAN on a Solaris machine, do the following:

1. Mount the Veeam Backup & Replication installation disk (`VeeamBackup&Replication_12.0.0.1420.iso`).

   If you deploy Veeam backup infrastructure for the first time, you can download the Veeam Backup & Replication installation disk at: https://www.veeam.com/backup-replication-vcp-download.html.

2. In the installation disk folder, go to `Plugins\Oracle RMAN\Solaris`. Select your system: i386 or SPARC.

3. Copy the Veeam Plug-in installation package (`VeeamPluginforOracleRMAN-12.0.0.1420-1.SPARC.pkg`) to Oracle Solaris server.

4. Install the plug-in from package with root privileges. Make sure the root user has privileges to add the PKG file.

   ```
   pkgadd -d /tmp/VeeamPluginforOracleRMAN-12.0.0.1420-1.pkg
   ```

5. Once Veeam Plug-in is installed, you can configure the plug-in settings. For details, see Configuring Plug-in on Linux and Unix Machines.

Installing Plug-in on IBM AIX

Veeam Plug-in for Oracle RMAN is an additional component of Veeam Backup & Replication, and the installation package of the plug-in is included in the Veeam Backup & Replication installation ISO file.

Veeam Plug-in for Oracle RMAN must be installed on a machine where the target Oracle Database is deployed.

> **NOTE**
>
> To install Veeam Plug-in, the `/opt/veeam` directory must be writable.

To install Veeam Plug-in for Oracle RMAN on an IBM AIX machine, do the following:

1. Mount the Veeam Backup & Replication installation disk (`VeeamBackup&Replication_12.0.0.1420.iso`).

   If you deploy Veeam backup infrastructure for the first time, you can download the Veeam Backup & Replication installation disk at: https://www.veeam.com/backup-replication-vcp-download.html.

2. In the installation disk folder, go to `Plugins\Oracle RMAN\AIX\ppc64`.

3. Copy the Veeam Plug-in installation package (`VeeamPluginforOracleRMAN-12.0.0.1420-1.aix6.1.ppc.rpm`) to the AIX server where the target Oracle database is deployed.

4. Install the plug-in from package with root privileges. Make sure the root user has privileges to add the PKG file.

   ```
   rpm -i VeeamPluginforOracleRMAN-12.0.0.1420-1.aix6.1.ppc.rpm
   ```

5. Once Veeam Plug-in is installed, you can configure the plug-in settings. For details, see Configuring Plug-in on Linux and Unix Machines.

Configuring Veeam Plug-in for Oracle RMAN

By default, RMAN sends backups to a native RMAN location on disk (`DEFAULT DEVICE TYPE TO DISK`). When you configure Veeam Plug-in, the default device type is changed to `SBT_TAPE`, which gives control over backup media management to Veeam Plug-in. Thus, after you deploy Veeam Plug-in on an Oracle server, you can perform all backup and restore operations in the Oracle RMAN console. Veeam Plug-in compresses, deduplicates database backups and transfers them to a backup repository connected to Veeam Backup & Replication.

To use Veeam Plug-in you must configure the connection between the Oracle server, Veeam Backup & Replication server and backup repositories where backup files will be stored.

- Configuring Veeam Plug-in for Oracle RMAN on Linux or Unix Machines
- Configuring Veeam Plug-in for Oracle RMAN on Windows Machines

Configuring Plug-in on Linux or Unix

To configure Veeam Plug-in, you can use **OracleRMANConfigTool**. The tool configures Oracle RMAN integration settings and creates the `veeam_config.xml` file which is stored in the installation folder of the plug-in: `/opt/veeam/VeeamPluginforOracleRMAN`.

Note that the Veeam Plug-in configuration tool changes the settings of Oracle RMAN. All original settings of Oracle RMAN are saved in the `/opt/veeam/VeeamPluginforOracleRMAN/RMANParameters.xml` file.

To configure Veeam Plug-in for Oracle RMAN, do the following:

1. Log in to the Oracle server with an account which is a member of the DBA group.
2. Launch the configuration wizard:

   ```
   OracleRMANConfigTool --wizard
   ```

   If you have extracted files form the .TAR.GZ archive, go to the `/opt/veeam/VeeamPluginforOracleRMAN` folder and run the following command:

   ```
   ./OracleRMANConfigTool --wizard
   ```

3. Specify the DNS name or IP address of the Veeam Backup & Replication server.

   ```
   Enter backup server name or IP address: 172.24.164.68
   ```

4. Specify the port which will be used to communicate with the Veeam Backup & Replication server. Default port: *10006*.

   ```
   Enter backup server port number: 10006
   ```

5. Specify credentials to authenticate against the Veeam Backup & Replication server.

```
Enter username: serv17\administrator
Enter password for serv17\administrator:
```

> **IMPORTANT**
>
> Mind the following:
>
> - You can work with backups created by Veeam Plug-in only with the account used for creating the backups. If you want to use another account, assign the *Veeam Backup Administrator* role or *Veeam Backup Operator* and *Veeam Restore Operator* roles to the account.
>
>   To learn how to assign Veeam Backup & Replication roles, see the Users and Roles section of the Veeam Backup & Replication Guide.
> - The account must have access permissions on the required backup repository. To learn how to configure access permissions and encryption settings on repositories, see Access and Encryption Settings on Repositories.

6. Select the backup repository where you want to store the backups. In the wizard dialog, enter the number of the repository from the list of available repositories. If you want to add several repositories, enter the required numbers separated by blank spaces.

   If you want to use the Oracle RMAN Backup Duplexing functionality, you can select up to four repositories. The copies of backups will be sent to all selected repositories. Note that Oracle Database Standard Edition does not allow using more than one RMAN channel. Thus, if you use Standard Edition, you can select only one repository.

```
Available repositories are:
1. serv10_repo
2. serv02_repo
Specify up to 4 Veeam repositories to use as target using whitespace as a
separator: 2
```

> **IMPORTANT**
>
> - The account must have access to backup repositories that you plan to use.
> - Encryption must be disabled on the repository.
>
> Otherwise, the repositories will not be listed as available. To learn how to configure access permissions and encryption settings on repositories, see Access and Encryption Settings on Repositories.

7. Specify the number of parallel data streams for each backup repository. Note that Oracle Database Standard Edition does not allow using more than one RMAN channel. Thus, if you use Standard Edition, you can select only one data stream.

```
Enter the number of data streams (From 1 to 254) to run in parallel for ea
ch repository (RMAN DEVICE PARALLELISM value).
Channel count per device: 4
```

8. If you want to enable Veeam compression of backup files, type **y**. For details, see the Data Compression and Deduplication section of Veeam Backup & Replication User Guide.

```
Do you want to use Veeam compression (Y/n):y
```

9. At the last step of the plug-in wizard, you can export configuration files (the Veeam Plug-in configuration file and RMAN configuration file). You can import these configuration files to other servers to apply the same settings.

```
Save configuration?
1. Apply configuration to the Oracle environment
2. Export configuration into a file for manual setup
3. Cancel without saving
Enter:1
*** Database instance ORCL is configured ***
```

NOTE

When you export the configuration files, Veeam Plug-in automatically enables Oracle's Controlfile Autobackup feature. This feature is required for restoring with different settings using Veeam Explorer for Oracle.

TIP

It is recommended to save the configuration files, so that you can use it as a reference. For example, if you are planning to manually allocate channels for backup and restore operations, you will need the repository UUID. The RMAN configuration file (`rman_config.txt`) contains an example for channel allocation definition for the target repository. You can use this statement in your backup/restore scripts.

Configuration Tool Commands

Apart from running a configuration wizard, you can use the **OracleRMANConfigTool** tool to change a specific parameter in the `veeam_config.xml` file or enable/disable Veeam Plug-in features.

See the list of available commands for **OracleRMANConfigTool**:

Command	Description
--help	Shows the list of parameters of the plug-in configuration tool.
--show-config	Shows configuration parameters.
--wizard	Starts the wizard to configure the plug-in settings. This wizard edits the `veeam_config.xml` file or creates a new one if the configuration file was removed from the `/opt/veeam/VeeamPluginforOracleRMAN` directory.

Command	Description
--set-credentials <"serv\username"> <"password">	Specifies credentials to connect to the Veeam backup server.
--set-host <hostname>	Specifies the host of the Veeam backup server.
--set-port <port_number>	Specifies the host to connect to the Veeam Backup & Replication server.
--set-repositories	Launches a wizard to select a backup repository. A backup repository is selected from repositories which are available in the connected Veeam Backup & Replication instance.
--set-parallelism <number_of_channels>	Configures RMAN parallelism settings.
--compression <y/n>	Enables/disables Veeam proprietary feature which compresses backup files.
--map-backup	Maps the imported backups.
--set-force-delete	Configures the auto-deletion of backup files after specified days.
--configure-restore-from-copy	Enables restore from backup copy. Note that if you enable restore from backup copy, you cannot back up databases with Veeam Plug-in. To revert changes, you must disable restore from backup copy.
--promote-backup-copy-to-primary	Maps the imported backup copy to a regular Veeam Plug-in backup chain.

Example:

To specify credentials that will be used to log in to the Veeam Backup & Replication server, use the plug-in configuration tool with the following command.

```
OracleRMANConfigTool --set-credentials "serv04\joelle" "password"
```

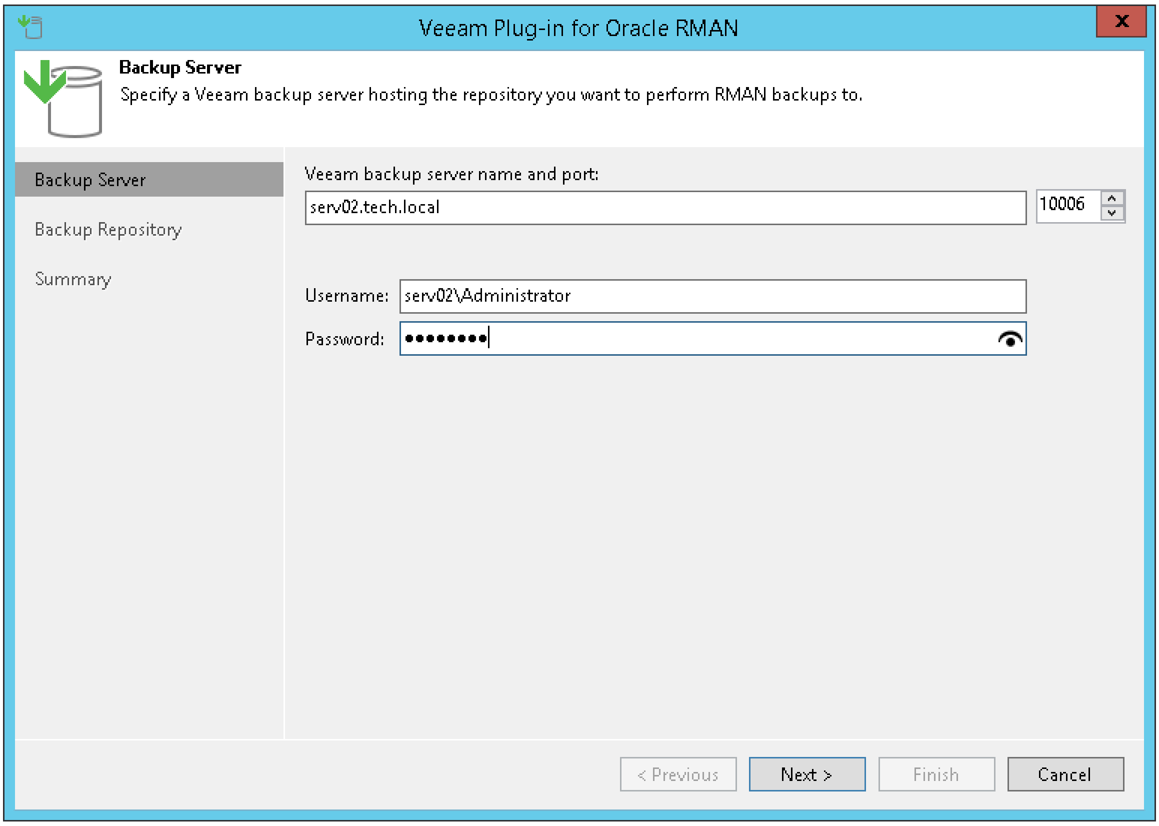
Configuring Plug-in on Windows

To configure backup and restore settings, use the **Veeam Plug-in for Oracle RMAN** configuration wizard. The wizard configures Oracle RMAN settings and creates the `veeam_config.xml` file which is stored in the `%PROGRAMFILES%\Veeam\VeeamPluginforOracleRMAN` folder.

Note that configuration wizard of Veeam Plug-in for Oracle RMAN changes the settings of Oracle RMAN. All original settings of Oracle RMAN are saved in the `%PROGRAMFILES%\Veeam\VeeamPluginforOracleRMAN\RMANParameters.xml` file.

To configure Veeam Plug-in, do the following:

1. On the Oracle server, click launch the Veeam RMAN Configuration Wizard (`%PROGRAMFILES%\Veeam\VeeamPluginforOracleRMAN\Veeam.Backup.RMAN.Configuration.exe`).
2. At the **Backup Server** step of the wizard, specify the DNS name of the Veeam Backup & Replication server and credentials that will be used to connect to the server. The specified account must have the local Administrator permissions on the Veeam Backup & Replication server.



Veeam Plug-in for Oracle RMAN

Backup Server

Specify a Veeam backup server hosting the repository you want to perform RMAN backups to.

Veeam backup server name and port: serv02.tech.local 10006

Username: serv02\Administrator

Password: ●●●●●●●●●

3. At the **Backup Repository** step of the wizard:

   a. Click **Add** and select the required repository. For Oracle Database Standard Edition, you can select only one repository. If you want to use the Oracle RMAN Backup Duplexing functionality, you can select up to four repositories. The copies of backups will be sent to all selected repositories.

      You must allow access to Veeam backup repositories that you plan to use. Also, the encryption on the repository must be disabled. To learn how to configure access and encryption on repositories, see Access and Encryption Settings on Repositories.

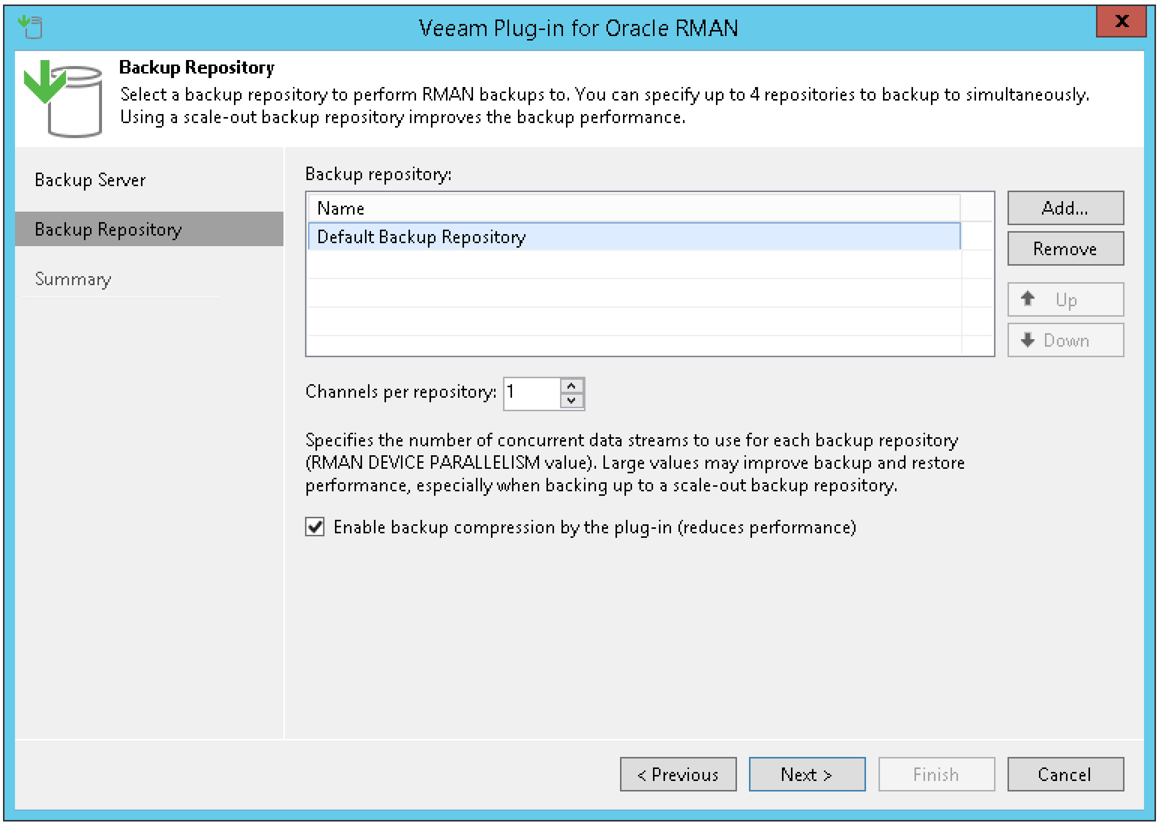
   b. If you want to use another repository, select the repository from the list and click **Remove**. Then, you can add another repository

   c. At the **Channels per repository** field, specify the number of allowed parallel data streams for each repository.

   d. If you want to enable Veeam Plug-in compression, select the **Enable backup compression by the plug-in** check box.

      Note that if you use Veeam Plug-in compression in combination with Oracle RMAN integrated compression (BACKUP AS COMPRESSED commands), it can slow down processing.

   e. Click **Next**.



Veeam Plug-in for Oracle RMAN

Backup Repository

Select a backup repository to perform RMAN backups to. You can specify up to 4 repositories to backup to simultaneously. Using a scale-out backup repository improves the backup performance.

Backup repository:

Name
Default Backup Repository

Channels per repository: 1

Specifies the number of concurrent data streams to use for each backup repository (RMAN DEVICE PARALLELISM value). Large values may improve backup and restore performance, especially when backing up to a scale-out backup repository.

☑ Enable backup compression by the plug-in (reduces performance)

IMPORTANT

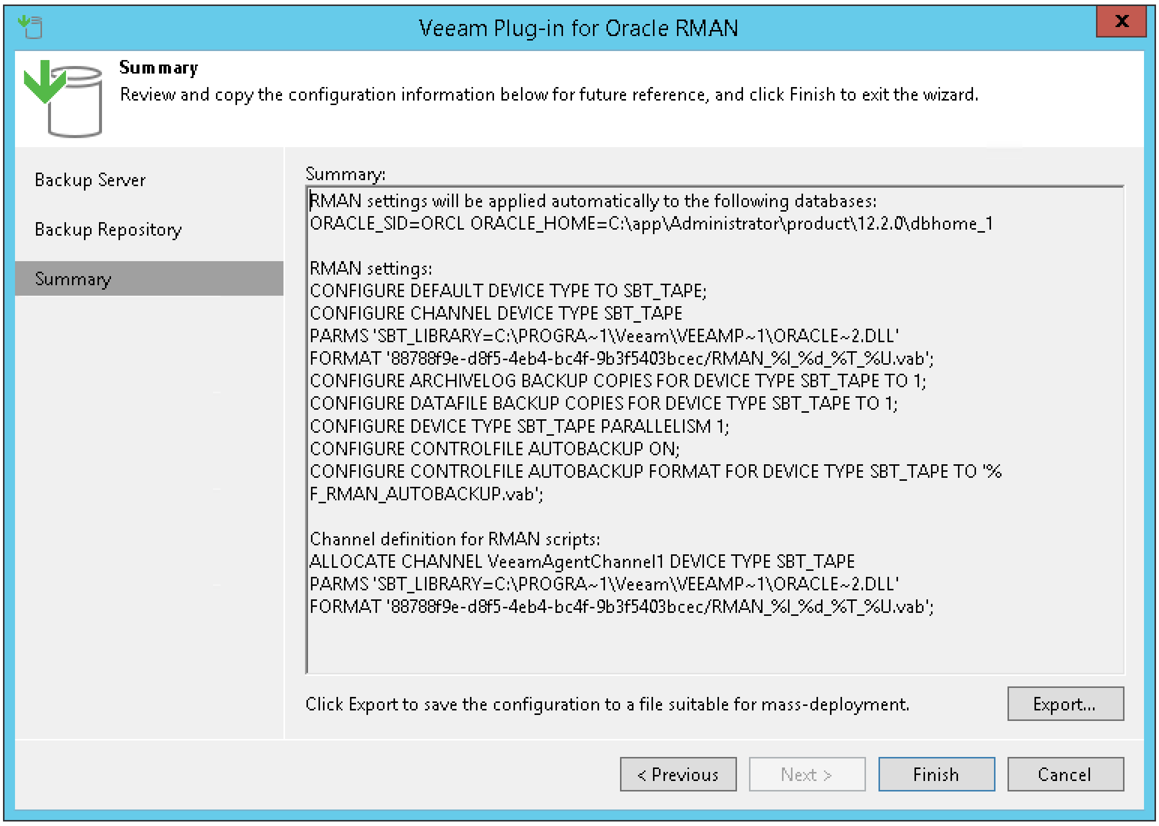
You can work with backups created by Veeam Plug-in only with the account used for creating the backups. If you want to use another account, assign the *Veeam Backup Administrator* role or *Veeam Backup Operator* and *Veeam Restore Operator* roles to the account.

To learn how to assign Veeam Backup & Replication roles, see the Users and Roles section of the Veeam Backup & Replication Guide.

4. At the **Summary** step of the wizard, you can export the plug-in and Oracle RMAN configuration files. You can use the configuration files to apply the plug-in settings on other servers.

   a. To export the `veeam_config.xml` file click **Export** and select **Veeam Config**.

   b. Click **Finish**.


Veeam Plug-in for Oracle RMAN
Summary
Review and copy the configuration information below for future reference, and click Finish to exit the wizard.
Backup Server
Backup Repository
Summary
Summary:
Export...
< Previous
Next >
Finish
Cancel

```
RMAN settings will be applied automatically to the following databases:
ORACLE_SID=ORCL ORACLE_HOME=C:\app\Administrator\product\12.2.0\dbhome_1

RMAN settings:
CONFIGURE DEFAULT DEVICE TYPE TO SBT_TAPE;
CONFIGURE CHANNEL DEVICE TYPE SBT_TAPE
PARMS 'SBT_LIBRARY=C:\PROGRA~1\Veeam\VEEAMP~1\ORACLE~2.DLL'
FORMAT '88788f9e-d8f5-4eb4-bc4f-9b3f5403bcec/RMAN_%I_%d_%T_%U.vab';
CONFIGURE ARCHIVELOG BACKUP COPIES FOR DEVICE TYPE SBT_TAPE TO 1;
CONFIGURE DATAFILE BACKUP COPIES FOR DEVICE TYPE SBT_TAPE TO 1;
CONFIGURE DEVICE TYPE SBT_TAPE PARALLELISM 1;
CONFIGURE CONTROLFILE AUTOBACKUP ON;
CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE SBT_TAPE TO '%
F_RMAN_AUTOBACKUP.vab';

Channel definition for RMAN scripts:
ALLOCATE CHANNEL VeeamAgentChannel1 DEVICE TYPE SBT_TAPE
PARMS 'SBT_LIBRARY=C:\PROGRA~1\Veeam\VEEAMP~1\ORACLE~2.DLL'
FORMAT '88788f9e-d8f5-4eb4-bc4f-9b3f5403bcec/RMAN_%I_%d_%T_%U.vab';
```

Click Export to save the configuration to a file suitable for mass-deployment.

NOTE

When you export the configuration files, Veeam Plug-in automatically enables Oracle's Controlfile Autobackup feature. This feature is required for restoring with different settings using Veeam Explorer for Oracle.

TIP

It is recommended to save the configuration files, so that you can use it as a reference. For example, if you are planning to manually allocate channels for backup and restore operations, you will need the repository UUID. The RMAN configuration file (`rman_config.txt`) contains an example for channel allocation definition for the target repository. You can use this statement in your backup/restore scripts.

Configuration Tool Commands

Apart from running a configuration wizard, you can use the **OracleRMANConfigTool.exe** tool to change a specific parameter in the `veeam_config.xml` file or enable/disable Veeam Plug-in features.

To run a specific command, do the following:

1. On the Oracle server, go to `%PROGRAMFILES%\Veeam\VeeamPluginforOracleRMAN`.
2. Run the required **OracleRMANConfigTool.exe** command from the table below.

   For example, to specify credentials that will be used to log in to the Veeam Backup & Replication server, use the plug-in configuration tool with the following command:

   ```
   OracleRMANConfigTool.exe --set-credentials "serv02\Joelle" "password"
   ```

Command	Description
--help	Shows the list of parameters of the plug-in configuration tool.
--show-config	Shows configuration parameters.
--wizard	Starts the wizard to configure the plug-in settings. This wizard edits the `veeam_config.xml` file or creates a new one if the configuration file was removed from the `/opt/veeam/VeeamPluginforOracleRMAN` directory.
--set-credentials <"serv\username"> <"password">	Specifies credentials to connect to the Veeam Backup & Replication server.
--set-host <hostname>	Specifies the host of the Veeam Backup & Replication server.
--set-port <port_number>	Specifies the host to connect to the Veeam Backup & Replication server.
--set-repositories	Launches a wizard to select a backup repository. A backup repository is selected from repositories which are available in the connected Veeam Backup & Replication instance.
--set-parallelism <number_of_channels>	Configures Oracle RMAN parallelism settings.
--compression <y/n>	Enables/disables Veeam proprietary feature which compresses backup files.
--map-backup	Maps the imported backups.
--set-force-delete	Deletes backup files after specified days.

Command	Description
--configure-restore-from-copy	Enables restore from backup copy. Note that if you enable restore from backup copy, you cannot back up databases with Veeam Plug-in. To revert changes, you must disable restore from backup copy.
--promote-backup-copy-to-primary	Maps the imported backup copy to a regular Veeam Plug-in backup chain.

Upgrading Veeam Plug-in for Oracle RMAN

Periodically, Veeam releases a new version of Veeam Backup & Replication that contains new features and bug fixes. The release package also contains a new version of Veeam Plug-ins.

If you want to upgrade Veeam Plug-in, note that Veeam Backup & Replication must be the same or later that the version of Veeam Plug-in. If you want to use the latest functionality, you must upgrade both Veeam Backup & Replication and Veeam Plug-in to the latest version. After the upgrade, you don't need to to re-run the Veeam Plug-in configuration wizard, the plug-in configuration files will be preserved.

> **IMPORTANT**
>
> The Veeam Backup & Replication version must be the same or later that the Veeam Plug-in version. First, you must upgrade Veeam Backup & Replication, then you can upgrade Veeam Plug-ins. To learn how to upgrade Veeam Backup & Replication, see the Upgrading to Veeam Backup & Replication 12 section of the Veeam Backup & Replication User Guide.

Before You Begin

Veeam Plug-in installation files are included in the installation disk image of Veeam Backup & Replication. You must upload the installation file to the Oracle Database server. To do this, perform the following steps.

1. Mount the Veeam Backup & Replication installation disk (`VeeamBackup&Replication_12.0.0.1420.iso`).
2. Open the mounted disk image and go to the `Plugins\Oracle RMAN\Linux` directory.
3. Select the the Veeam Plug-in installation file suitable for your OS and upload it to the Oracle Database server.

To learn how to upgrade Veeam Plug-in for Oracle RMAN, see the following guides:

- Upgrading Plug-in on Microsoft Windows
- Upgrading Plug-in on Linux (RPM)
- Upgrading Plug-in on Linux (TAR.GZ)
- Upgrading Plug-in on Oracle Solaris
- Upgrading Plug-in on IBM AIX

Upgrading Plug-in on Windows

To upgrade Veeam Plug-in for Oracle RMAN on a Windows machine, upload the `VeeamPluginforOracleRMAN.exe` file of the new version to the Oracle Database server and install it. The old version will be replaced with the new version automatically.

You can upgrade Veeam Plug-in for Oracle RMAN to a later version in the unattended mode using the same command that is used for unattended installation. For details, see Installing Veeam Plug-in on Windows Machine in Unattended Mode.

Upgrading Plug-in on Linux (.RPM)

To upgrade Veeam Plug-in for Oracle RMAN on a Linux machine, do the following:

1. Upload the `VeeamPluginforOracleRMAN-12.0.0.1420-1.x86_64.rpm` package to the Oracle server. If you need the 32-bit version, choose the `i386` package.

2. To upgrade Veeam Plug-in, run the following command. Note that the operation requires *root* privileges.

```
rpm -U VeeamPluginforOracleRMAN-12.0.0.1420-1.x86_64.rpm
```

> **TIP**
>
> To find out which version of Veeam Plug-in is installed on your server, you can use the following command: `rpm -qa | grep VeeamPlugin*`

Upgrading Plug-in on Linux (.TAR.GZ)

To upgrade Veeam Plug-in for Oracle RMAN on a Linux machine from the .TAR.GZ archive, do the following:

1. Upload the `VeeamPluginforOracleRMAN.tar.gz` file to the Oracle server.

2. Unpack the plug-in files from the archive to the `/opt/veeam` directory. Old Veeam Plug-in files will be replaced by new files.

```
tar -xzvf VeeamPluginforOracleRMAN.tar.gz -C /opt/veeam
```

Upgrading Plug-in on Oracle Solaris

To upgrade Veeam Plug-in for Oracle RMAN on an Oracle Solaris machine, do the following:

1. Upload the `VeeamPluginforOracleRMAN-12.0.0.1420-1.SPARC.pkg` package to the Oracle server. If you need the 32-bit version, choose the `i386` package.

2. Make sure the `pkgadd` administration file (`admin_file`) contains the following entry: `"instance=overwrite"`. For details, see the Avoiding User Interaction When Adding Packages section of the Oracle Solaris Administration Guide.

3. To upgrade Veeam Plug-in, run the following command:

```
pkgadd -a admin_file -d /tmp/VeeamPluginforOracleRMAN-12.0.0.1420-1.SPARC.
pkg
```

Upgrading Plug-in on IBM AIX

To upgrade Veeam Plug-in for Oracle RMAN on an IBM AIX machine, do the following:

1. Upload the `VeeamPluginforOracleRMAN-12.0.0.1420-1.aix6.1.ppc.rpm` package to the Oracle server.
2. To upgrade Veeam Plug-in, run the following command. Note that the operation requires *root* privileges.

   ```
   rpm -U VeeamPluginforOracleRMAN-12.0.0.1420-1.aix6.1.ppc.rpm
   ```

Importing/Exporting Plug-in Settings

You can export a Veeam Plug-in configuration file and apply the plug-in settings to other severs.

> **IMPORTANT**
>
> The password included in the configuration file is encrypted. Thus, after you import the configuration file, you must set the credentials manually in the Veeam Plug-in configuration wizard.

To export the configuration file to another Linux server, do the following:

[For Linux and Unix]:

a. On the server where Veeam Plug-in is installed, go to `/opt/veeam/VeeamPluginforOracleRMAN`.

b. Copy the `veeam_config.xml` file to the server where you want to configure the plug-in.

c. Install Veeam Plug-in on the new server and place the copied XML file in the `/opt/veeam/VeeamPluginforOracleRMAN` folder.

d. Set new credentials using the following command:

```
OracleRMANConfigTool --set-credentials "serv\username" "password"
```

[For Windows]:

a. On the server where Veeam Plug-in is installed, go to `%PROGRAMFILES%\Veeam\VeeamPluginforOracleRMAN\`.

b. Copy the `veeam_config.xml` file to the server where you want to configure the plug-in.

c. Install Veeam Plug-in on the new server and place the copied XML file in the `%PROGRAMFILES%\Veeam\VeeamPluginforOracleRMAN\` folder.

d. Set new credentials using the following command:

```
C:\Program Files\Veeam\VeeamPluginforOracleRMAN\OracleRMANConfigTool.exe -
-set-credentials "serv\username" "password"
```

Importing Backup Files

If the Veeam Backup & Replication server has failed and you have restored it in a new location, you can copy the backup files to a new repository and re-map the Veeam Plug-in backup files.

Limitations and Prerequisites

Mind the following limitations:

- If backup files are not imported according to instructions given in this section, Veeam Plug-in backup and restore operations may fail.
- The repository from which you plan to import backups must be added to the Veeam Backup & Replication infrastructure. Otherwise you will not be able to access backup files.
- If you are importing backup files from a scale-out backup repository, the names of backup files and paths to backup files must contain only allowed characters:
  - Alphanumeric characters: `a-zA-Z0-9`
  - Special characters: `_-.+=@^`
  - Names of backup files and paths to backup files must not contain spaces.

How to Import Veeam Plug-in Backup Files

To import Veeam Plug-in backup files, do the following:

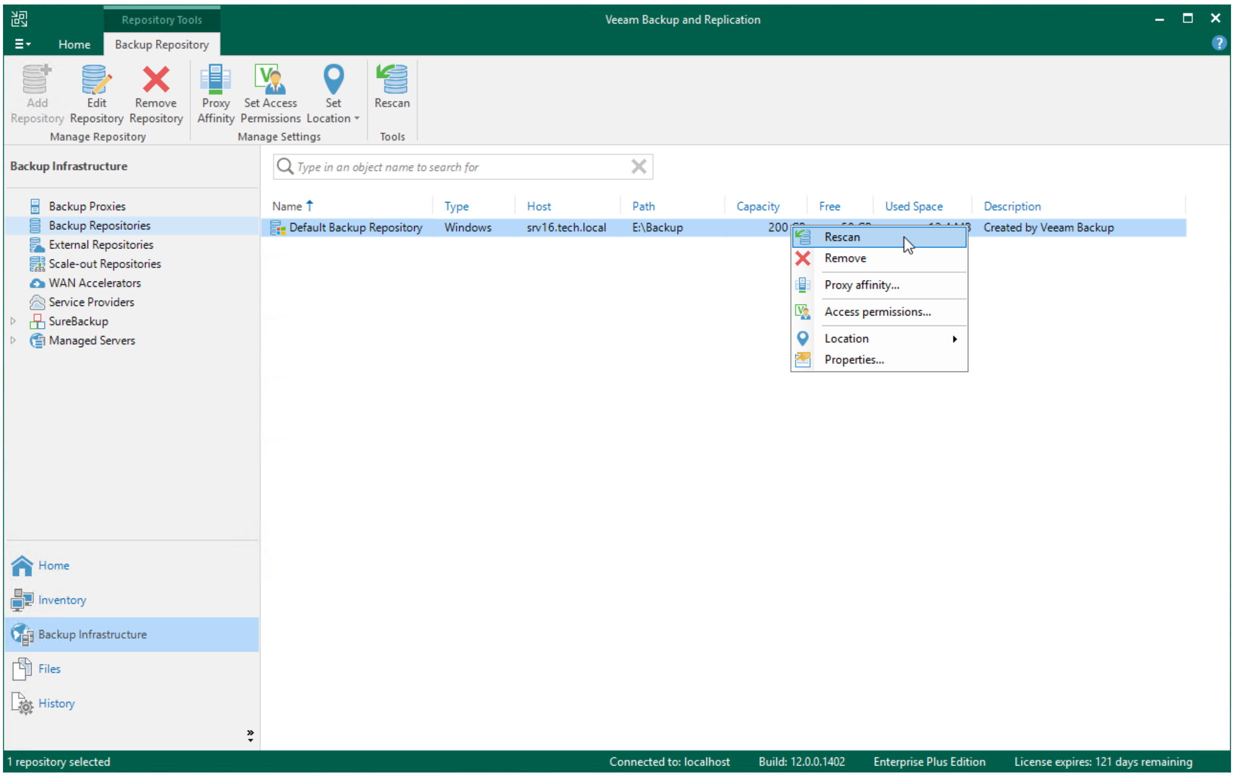
1. Move the folder with the backup file to the required backup repository or create a new backup repository with this folder as a subfolder.

   > **TIP**
   >
   > Each Veeam Plug-in backup file (.vab) has its own metadata file (.vasm). Make sure you import backup files and all related metadata files. Also, you must import the backup job metadata file (.vacm) which is stored in the same folder.

2. In the Veeam Backup & Replication console, open the **Backup Infrastructure** view.
3. In the inventory pane of the **Backup Infrastructure** view, select the **Backup Repositories** node.

4. In the working area, select the required backup repository and click **Rescan** on the ribbon. Alternatively, you can right-click the backup repository and select **Rescan**.

   During the rescan operation, Veeam Backup & Replication gathers information about backups that are currently available in the backup repository and updates the list of backups in the configuration database. After the rescan operation, backups that were not in this configuration database will be shown on the **Home** view in the **Backups > Disk (Imported)** node.



Name	Type	Host	Path	Capacity	Free	Used Space	Description
Default Backup Repository	Windows	srv16.tech.local	E:\Backup	200 [illegible]	[illegible]	[illegible]	Created by Veeam Backup

1 repository selected   Connected to: localhost   Build: 12.0.0.1402   Enterprise Plus Edition   License expires: 121 days remaining

5. On the Oracle server, use the terminal to set the new repository as a target in the Veeam Plug-in settings:

   - **For Windows**:

```
"C:\Program Files\Veeam\VeeamPluginforOracleRMAN\OracleRMANConfigTool"
--set-repositories
Available backup repositories:
1. serv55.tech.local
2. serv07_repo
Enter repository number: 1
```

   - **For Linux and Unix**:

```
OracleRMANConfigTool --set-repositories
Available backup repositories:
1. serv55.tech.local
2. serv07_repo
Enter repository number: 1
```

6. Start the Veeam Plug-in configuration wizard with the `--map-backup` parameter to re-map the plug-in backups:

   - **For Windows**:

     ```
     "C:\Program Files\Veeam\VeeamPluginforOracleRMAN\OracleRMANConfigTool"
     --map-backup
     ```

   - **For Linux and Unix**:

     ```
     OracleRMANConfigTool --map-backup
     ```

Upgrading Backup Files

Since version 11, Veeam Plug-in uses a new format of backup files: instead of one metadata file for all backup files there are separate metadata files (.vasm) for each database backup file (.vab). The new metadata format allows to optimize the productivity of backup and restore operations.

For Veeam Plug-in 11, the backup files upgrade is not obligatory. However, in version 12, backup files created by Veeam Plug-in version 10 will not be supported.

> IMPORTANT
>
> If you do not upgrade backup files, you will get the following warning in the job session logs: *Backup metadata is not up to date. Please upgrade the backup*. If you want to disable the warning, see instructions in this Veeam KB.

Prerequisites

Before upgrading backup files, make sure the following requirements are met.

- Make sure that you have upgraded Veeam Plug-in on the source server. If Veeam Plug-in is not upgraded to version 11 and you upgrade the backup files, then all next backup job runs will fail.
- Make sure that you have disabled the backup job whose backup files you want upgrade. You must also disable the backup copy jobs that use these backup files as a source.
- If the backup files reside on the scale-out backup repository, all repository extents must be available. Also, the extents must not be in the Seal or Maintenance mode.
- If you want to upgrade backup files created by a backup copy job, you must meet the same requirements as for the backup job files.
- During the process of the metadata upgrade, you cannot run the target backup job and you cannot restore from the backup files.

  The upgrade process duration depends on the number of backup files in the backup set, type of the backup repository and workload level on the file system.

  For example, there are backup files of an Oracle server that contains 10 instances and is backed up every 15 minutes with the retention policy set for 2 weeks. The upgrade of backup files can have the following duration on not overloaded file systems:

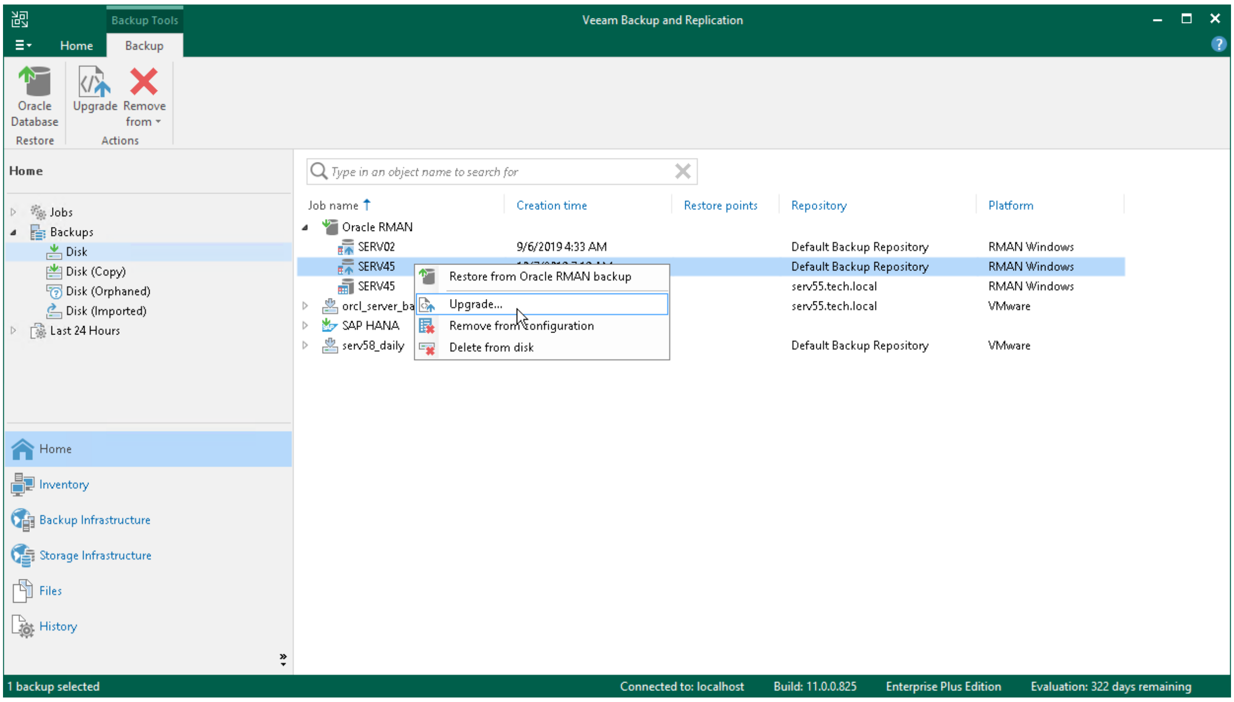
  - Microsoft Windows: 30 minutes
  - Linux: from 30 minutes to 3 hours
  - SMB/NFS: 1.5 hours
  - Data Domain Boost/Quantum DXi/ExaGrid/CIFS (SMB)/NFS file share: 3-4 hours
  - HPE StoreOnce: up to 10 hours (due to specifics of this repository type for processing large number of files)

Upgrading Backup Files in Veeam Backup & Replication Console

To upgrade backup files in the Veeam Backup & Replication console, do the following:

1. Open the **Home** view.
2. In the inventory pane, expand the **Backups** view and select **Disk**.
3. In the working area, right-click the job or the restore point and select **Upgrade**.

   Alternatively, you can select the job or the restore point and click **Upgrade** on the ribbon.



Job name	Creation time	Restore points	Repository	Platform
Oracle RMAN				
SERV02	9/6/2019 4:33 AM		Default Backup Repository	RMAN Windows
SERV45	[illegible]		Default Backup Repository	RMAN Windows
SERV45			serv55.tech.local	RMAN Windows
orcl_server_ba			serv55.tech.local	VMware
SAP HANA				
serv58_daily			Default Backup Repository	VMware

Uninstalling Veeam Plug-in for Oracle RMAN

You can uninstall the Veeam Plug-in and undo the configuration changes made by Veeam Plug-in.

When you configure Veeam Plug-in, original settings of Oracle RMAN are saved in the `/opt/veeam/VeeamPluginforOracleRMAN/RMANParameters.xml` file (or in the `C:\Program Files\Veeam\VeeamPluginforOracleRMAN\RMANParameters.xml` for Windows). If you uninstall Veeam Plug-in for Oracle RMAN, original settings of Oracle RMAN are restored from the `RMANParameters.xml` file.

Uninstalling Veeam Plug-in on Linux or IBM AIX Machines

To uninstall Veeam Plug-in and undo the configuration changes, run the following command. Note that the operation requires *root* privileges.

```
rpm -e VeeamPluginforOracleRMAN
```

Uninstalling Veeam Plug-in on Windows Machines

To uninstall Veeam Plug-in and undo the configuration changes, do the following:

1. Open the **Control Panel** and click **Programs and Features**.
2. In the list of programs, select **Veeam Plug-in for Oracle RMAN** and click **Uninstall**.

Uninstalling Veeam Plug-in on Solaris Machines

To uninstall Veeam Plug-in and undo the configuration changes, run the following command:

```
pkgrm VeeamPluginforOracleRMAN
```

Database Protection

After you configure Veeam Plug-in settings, you can use the Oracle RMAN functionality to back up databases. Veeam Plug-in will automatically transfer the backup files to the Veeam backup repository.

The examples given below are for demonstration purposes only. The backup process is performed on the Oracle RMAN side. Consider configuring required RMAN-specific parameters that may affect the backup process. For details on the backup functionality of Oracle RMAN, see the Backing Up the Database section of the Oracle's Database Backup and Recovery User's Guide.

NOTE

Mind the following:

- In the Veeam Plug-in configuration wizard, you can enable/disable Veeam Plug-in Data Compression and Deduplication. If you enable the Veeam Plug-in compression, do not use Oracle RMAN integrated compression as well. It can slow down the backup and restore processes.
- It is Oracle's best practice to add the `EXIT;` command at the bottom of the script to shut down the RMAN utility. Without the `EXIT;` command in the script, it is up to Oracle RMAN to decide when to close the backup session, which can lead to multiple unclosed RMAN backup sessions.

TIP

If you have configured the retention policy, run the `DELETE OBSOLETE` command after the database backup to delete obsolete backups from the repository.

Oracle RMAN Full Backup

After you configure Veeam Plug-in settings, you can use the Oracle RMAN functionality to back up databases. Veeam Plug-in will automatically transfer the backup files to the Veeam backup repository. You can create a consistent backup of Oracle databases in the ARCHIVELOG mode and in the NOARCHIVELOG mode. For details on the backup process in different modes, see the Choosing Between NOARCHIVELOG and ARCHIVELOG Mode section of the Oracle's Database Administrator's Guide.

> NOTE
>
> The examples given below are for demonstration purposes only. The backup process is performed on the Oracle RMAN side. Consider configuring required RMAN-specific parameters that may affect the backup process. For details on the backup functionality of Oracle RMAN, see the Backing Up the Database section of the Oracle Database Backup and Recovery User's Guide.

Consistent Backup of Oracle Database in ARCHIVELOG Mode

To create a consistent backup of an Oracle database and redo logs in the ARCHIVELOG mode, run the following script. In this example, Oracle RMAN will back up the entire database and available archived redo logs. The current online redo log will be archived to make sure all redo changes are transferred to the archived redo log chain. In the ARCHIVELOG mode, there will be no downtime as you do not have to shut down the database.

```
rman TARGET /
RUN {
BACKUP DATABASE PLUS ARCHIVELOG;
}
EXIT;
```

Consistent Backup of Oracle Database in NOARCHIVELOG Mode

To create a consistent backup of an Oracle database operating in the NOARCHIVELOG mode, start the Oracle RMAN console and run the following script. In this example, the database instance will be started after the backup process is complete. Note that the database will be unavailable during the backup.

```
rman TARGET /
RUN {
SHUTDOWN TRANSACTIONAL;
STARTUP MOUNT;
BACKUP DATABASE;
STARTUP;
}
EXIT;
```

Oracle RMAN Channel Allocation

If you want to manually allocate channels for backup operations, you must specify the Veeam backup repository UUID in the channel parameters. The `ALLOCATE CHANNEL` command must be issued within a RUN block. It allocates a channel only in the block where the command is issued. See the following example.

```
RUN {
     ALLOCATE CHANNEL ch1 DEVICE TYPE SBT_TAPE PARMS 'SBT_LIBRARY=/opt/veeam/Ve
eamPluginforOracleRMAN/libOracleRMANPlugin.so' FORMAT 'd8338780-1aec-4c36-b17c-
e1ea3ea2ca93/RMAN_%I_%d_%T_%U.vab';
     BACKUP DATABASE;
     RELEASE CHANNEL ch1;
}
EXIT;
```

Run the Oracle RMAN script with the following parameters:

1. Use the `ALLOCATE CHANNEL` command to manually allocate a channel or channels between RMAN and the database instance. Specify the following parameters:

   a. Specify the channel ID. For example: `ch1`.

   b. Specify the `SBT_TAPE` option for the `DEVICE TYPE` parameter.

   c. Specify `PARMS` to define other parameters for the `sbt_tape` channel.

   d. Specify which media library must be used for this `sbt_tape` channel. For Linux or Unix, set the path to the `libOracleRMANPlugin.so` file as the `SBT_LIBRARY`. For Windows, set the path to `%PROGRAMFILES%\Veeam\VeeamPluginforOracleRMAN\OracleRMANPlugin.dll`.

   e. Use the Veeam backup repository UUID in the argument for the `FORMAT` parameter. You can find the required backup repository UUID in the `rman_config.txt` file saved during the Veeam Plug-in configuration process or in logs.

   [For Linux] If you have exported Veeam Plug-in configuration files, run the following command to see open the configuration file.

   ```
   cat /tmp/rman_config.txt
   ```

   Alternatively, you can find the repository UUID in logs:

   ```
   grep "received repos" /tmp/veeam_plugin_logs/oracle/OracleRMANConfigToo
   l.log | tail
   ```

   [For Windows] If you have exported Veeam Plug-in configuration files, find the channel allocation definition in the configuration file.

   Alternatively, you can find the repository UUID in logs. Go to the `%\ProgramData\Veeam\Backup\RmanPluginLogs\SERV_NAME` directory and search for "*received repos id*" in the `OracleRMANConfigToolLib.log` file.

2. Use the `BACKUP` command with required parameters to create a database backup.

3. [Optional] Use the `RELEASE CHANNEL` command. By default, RMAN automatically releases all normal channels when the `RUN` command terminates.

Backup Job in Veeam Backup & Replication

After you start a backup process in Oracle RMAN, Veeam Backup & Replication creates a backup job. You can use this job to view the statistics on the backup process, generate backup job reports or you can also disable the backup job.

You cannot start or edit Oracle RMAN backup jobs in the Veeam Backup & Replication console. You can manage backup operations only on the Oracle side using RMAN.

Mind the following regarding the naming of Oracle RMAN backup jobs:

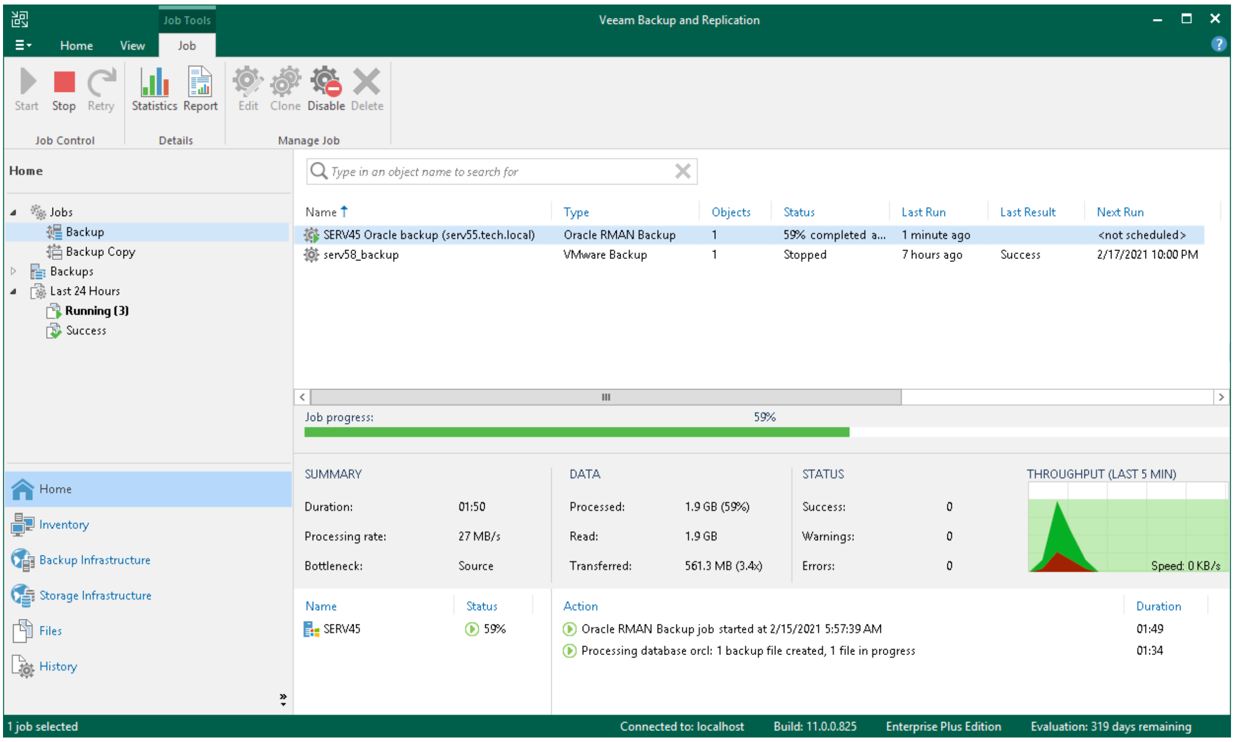
- For a standalone Oracle RMAN server, Veeam Backup & Replication generates the backup job name based on names of the Oracle RMAN server and selected repository.
- For Oracle RAC, Veeam Backup & Replication generates the backup job name based on single client access name (SCAN) of the cluster.

> NOTE
>
> The progress bar of a running Oracle database backup job is available only for backups of standalone Oracle databases. It is not available for Oracle RAC backups.

Viewing Backup Job Statistics

To view details of a backup job process, do the following:

1. Open the Veeam Backup & Replication console.
2. In the **Home** view, expand the **Jobs** node and click **Backup**.
3. In the list of jobs, select the Oracle RMAN backup job to see details of the current backup process or the last backup job session.



Name	Type	Objects	Status	Last Run	Last Result	Next Run
SERV45 Oracle backup (serv55.tech.local)	Oracle RMAN Backup	1	59% completed a...	1 minute ago		<not scheduled>
serv58_backup	VMware Backup	1	Stopped	7 hours ago	Success	2/17/2021 10:00 PM

Job progress: 59%

SUMMARY		DATA		STATUS	
Duration:	01:50	Processed:	1.9 GB (59%)	Success:	0
Processing rate:	27 MB/s	Read:	1.9 GB	Warnings:	0
Bottleneck:	Source	Transferred:	561.3 MB (3.4x)	Errors:	0

Name	Status
SERV45	59%

Action	Duration
Oracle RMAN Backup job started at 2/15/2021 5:57:39 AM	01:49
Processing database orcl: 1 backup file created, 1 file in progress	01:34

1 job selected   Connected to: localhost   Build: 11.0.0.825   Enterprise Plus Edition   Evaluation: 319 days remaining

Generating Backup Job Reports

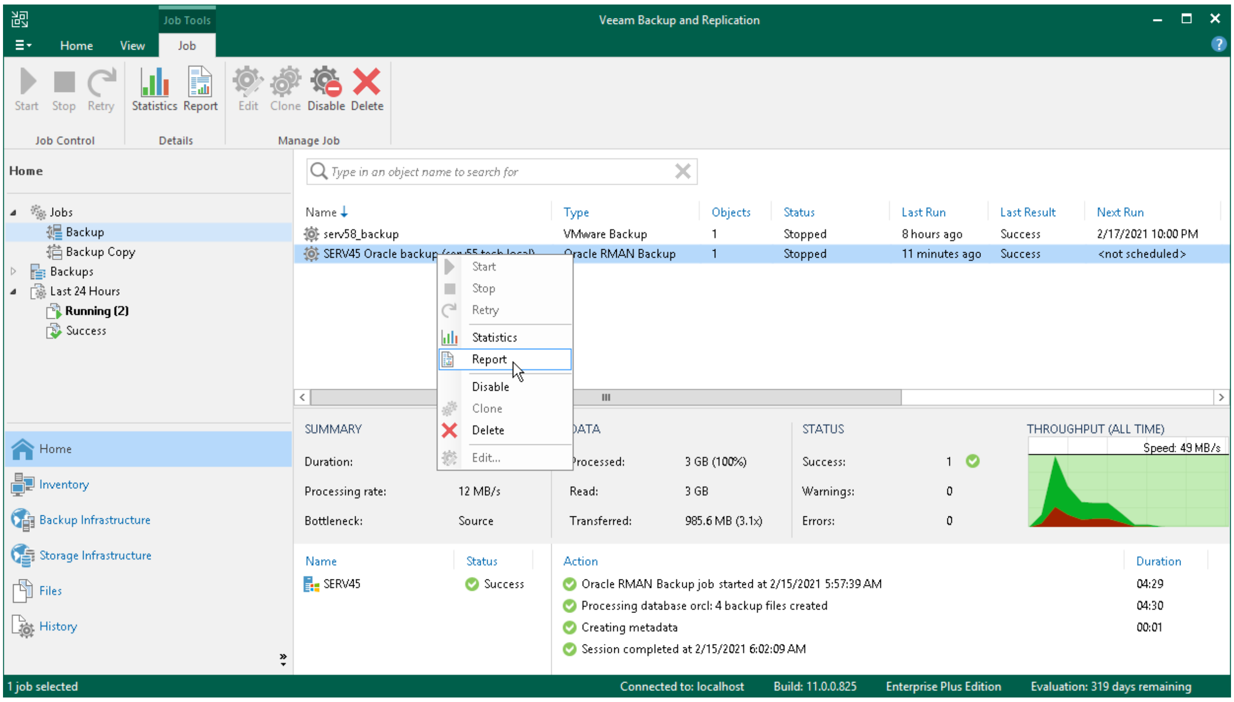
Veeam Backup & Replication can generate reports with details about an Oracle RMAN backup job session performance. The session report contains the following session statistics: session duration details, details of the session performance, amount of read, processed and transferred data, backup size, compression ratio, list of warnings and errors (if any).

To generate a report, do the following:

1. Open the **Home** view.

2. In the inventory pane, select **Jobs**.

3. In the working area, select the necessary job and click **Report** on the ribbon. You can also right-click the job and select **Report**.



Name	Type	Objects	Status	Last Run	Last Result	Next Run
serv58_backup	VMware Backup	1	Stopped	8 hours ago	Success	2/17/2021 10:00 PM
SERV45 Oracle backup	Oracle RMAN Backup	1	Stopped	11 minutes ago	Success	<not scheduled>

SUMMARY		DATA		STATUS	
Duration:		Processed:	3 GB (100%)	Success:	1
Processing rate:	12 MB/s	Read:	3 GB	Warnings:	0
Bottleneck:	Source	Transferred:	985.6 MB (3.1x)	Errors:	0

Name	Status
SERV45	Success

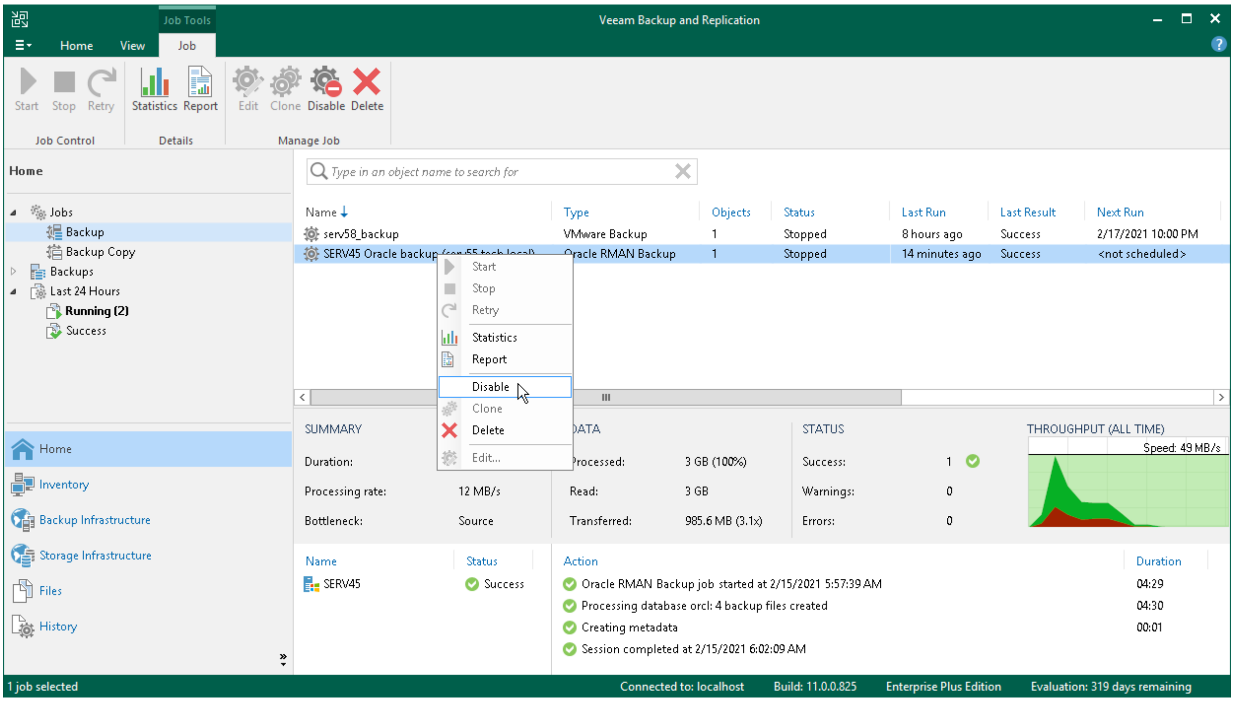
Action	Duration
Oracle RMAN Backup job started at 2/15/2021 5:57:39 AM	04:29
Processing database orcl: 4 backup files created	04:30
Creating metadata	00:01
Session completed at 2/15/2021 6:02:09 AM	

Disabling Backup Job

You can disable Oracle RMAN backup jobs in the Veeam Backup & Replication console. If you disable the job, you will not be able to run RMAN backup commands on the Oracle server.

To disable a backup job, do the following:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the necessary job and click **Disable** on the ribbon. You can also right-click the job and select **Disable**.



Name	Type	Objects	Status	Last Run	Last Result	Next Run
serv58_backup	VMware Backup	1	Stopped	8 hours ago	Success	2/17/2021 10:00 PM
SERV45 Oracle backup	Oracle RMAN Backup	1	Stopped	14 minutes ago	Success	<not scheduled>

SUMMARY

Duration:

Processing rate: 12 MB/s

Bottleneck: Source

DATA

Processed: 3 GB (100%)

Read: 3 GB

Transferred: 985.6 MB (3.1x)

STATUS

Success: 1

Warnings: 0

Errors: 0

Name	Status
SERV45	Success

Action	Duration
Oracle RMAN Backup job started at 2/15/2021 5:57:39 AM	04:29
Processing database orcl: 4 backup files created	04:30
Creating metadata	00:01
Session completed at 2/15/2021 6:02:09 AM	

Database Recovery

With the configured Veeam Plug-in for Oracle RMAN, you can perform all kinds of database restore operations available in Oracle RMAN. You can also restore from database backups in the Veeam Backup & Replication console.

- Restore to Original Server
- Restore to Another Server
- Restore from Backup Copy
- Restore with Veeam Explorer for Oracle
- Restore of Control File from Autobackup
- Restore from Hardened Repository

Restore to Original Server

Veeam Plug-in for Oracle RMAN allows you to restore databases using built-in Oracle RMAN functionality. When you launch a restore, RMAN restores the necessary database from the backup stored in the Veeam backup repository.

If you want to change the repository or channel settings, you must modify the Veeam Plug-in settings. For details, see Configuring Veeam Plug-in for Oracle RMAN.

To restore the Oracle database, you must connect to the database with RMAN and run the restore command. You may need to run additional commands depending on your database infrastructure. Consider configuring required RMAN-specific parameters that may affect the backup process. For details on all restore capabilities of Oracle RMAN, see the Performing Complete Database Recovery section of the Oracle's Database Backup and Recovery User's Guide.

```
rman TARGET /
RUN {
SHUTDOWN IMMEDIATE;
STARTUP MOUNT;
RESTORE DATABASE;
RECOVER DATABASE;
}
EXIT;
```

NOTE

If you use the SEND command on the target server to point to the source server, you can run operations like DUPLICATE. For details, see Restore to Another Server Using RMAN.

Restore to Another Server

If you want to restore Oracle databases from a Veeam Plug-in backup to another server, follow instructions in the Restoring a Database on a New Host section of Oracle's Database Backup and Recovery User's Guide and mind the specifics described in this section.

Restore from Backup to Another Server

After you allocate channels, you must use the SEND command with the `srcSrv=originalServerName` parameter, where `originalServerName` is the hostname of the protected server. In case of RAC, use the cluster SCAN name as `originalServerName`.

> **TIPS**
>
> Mind the following:
>
> - Veeam Plug-in backup job name contains the name of the original server. You can find out what to use as `originalServerName` if you look at the first part of the Veeam Plug-in backup job name.
> - The ALLOCATE CHANNEL and SEND commands must be issued only within a RUN block for a specific restore operation.

Example of a script for restoring the control file and restoring the Oracle database to another server using the SEND command:

```
rman TARGET /
RUN {
ALLOCATE CHANNEL a1 TYPE sbt_tape PARMS "SBT_LIBRARY=/opt/veeam/VeeamPluginforO
racleRMAN/libOracleRMANPlugin.so" SEND "srcSrv=server01";
SET CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE 'SBT_TAPE' TO '%F_RMAN_AUTOBA
CKUP.vab';
RESTORE controlfile FROM 'c-4097408439-20200410-00_RMAN_AUTOBACKUP.vab';
}
EXIT;
```

Use the `ALLOCATE CHANNEL` command to manually allocate a channel or channels between RMAN and the database instance. Specify the following parameters:

1. Assign an ID for the channel. For example: `ch1`.
2. Specify the `SBT_TAPE` option for the `DEVICE TYPE` or `TYPE` parameter.
3. Specify `PARMS` to define other parameters for the `sbt_tape` channel.
4. Specify which media library must be used for this `sbt_tape` channel. For Linux or Unix, set the path to the `libOracleRMANPlugin.so` file as the `SBT_LIBRARY`. For Windows, set the path to `%PROGRAMFILES%\Veeam\VeeamPluginforOracleRMAN\OracleRMANPlugin.dll`.
5. Use the `SEND` command to specify the original server hostname (the `srcSrv` parameter). For example: `"srcSrv=server01"`.

Restore from Backup Copy to Another Server

If you want to restore a database from a backup copy to another server, do the following:

1. On the Oracle server, go to the `\Veeam\VeeamPluginforOracleRMAN` folder (`/opt/veeam/VeeamPluginforOracleRMAN/` for Linux OS).

2. Open the `veeam_config.xml` file with a text editor.

3. Change the `<PluginParameters />` line as follows:

   - For a standalone Oracle Server:

     ```
     <PluginParameters customServerName="original_server_hostname" />
     ```

   - For Oracle RAC:

     ```
     <PluginParameters customServerName="original_cluster_scan_name" />
     ```

   > **IMPORTANT**
   >
   > Mind the following:
   >
   > - Veeam Plug-in for Oracle RMAN must be installed and configured on the target server.
   > - Before you perform any other backup or restore job, revert back the changes in the `veeam_config.xml` file. The default configuration is: `<PluginParameters />`

4. Enable the **restore from backup copy** option, as described in Restore from Backup Copy.

5. Perform the restore.

   ```
   rman TARGET /
   RUN {
   ALLOCATE CHANNEL a1 TYPE sbt_tape PARMS "SBT_LIBRARY=/opt/veeam/VeeamPlugi
   nforOracleRMAN/libOracleRMANPlugin.so";
   RESTORE DATABASE;
   RECOVER DATABASE;
   }
   EXIT;
   ```

Restore from Backup Copy

You can restore from backups and backup copies. To restore from backup copies, you must enable the **restore from backup copy** option in the Veeam Plug-in wizard.

If the **restore from backup copy** option is enabled, you cannot back up databases using Veeam Plug-in, and you cannot restore from backups created by primary Veeam Plug-in backup jobs. You can restore only from backup copy files until you disable the **restore from backup copy** option.

> IMPORTANT
>
> Mind the following:
>
> - You can restore from Veeam Plug-in backups using Veeam Explorer for Oracle, even if the restore from backup copy option is enabled. For details, see Veeam Explorers User Guide.
> - You can restore only from backup copies that are located in repositories with primary backups. If you do not have access to repositories with primary backups, you can convert a backup copy to a primary backup. For details, see Converting Backup Copy to Backup.
> - If you want to restore from a backup copy to another server, see Restore from Backup Copy to Another Server.

Enabling Restore from Backup Copy

To be able to restore from backup copies, do the following.

- **For Linux or Unix OS:**

  a. Open the terminal and launch the following command:

  ```
  OracleRMANConfigTool --configure-restore-from-copy
  ```

  b. Select the number of the required backup copy job:

  ```
  Select secondary job for failover:
  0. Disable
  1. Plug-ins backup copy job\SERV02 Oracle backup <serv10_repo>
  Select secondary job for failover:1
  ```

> IMPORTANT
>
> The account used to connect to the Veeam Backup & Replication server must have access permissions on the required repository.

- **For Windows OS:**

  a. Go to the Veeam Plug-in installation directory (by default, **C:\Program Files\Veeam\VeeamPluginforOracleRMAN\**) and launch the following command:

  ```
  OracleRMANConfigTool.exe --configure-restore-from-copy
  ```

b. Select the number of the required backup copy job:

```
Select secondary job for failover:
0. Disable
1. Plug-ins backup copy job\SERV02 Oracle backup <serv10_repo>
Select secondary job for failover:1
```

Disabling Restore from Backup Copy

To be able to back up with Veeam Plug-in and restore from backups, disable the restore from backup copies:

- **For Linux or Unix OS:**

```
OracleRMANConfigTool --configure-restore-from-copy
Select secondary job for failover:
0. Disable
1. Plug-ins backup copy job\SERV02 Oracle backup <serv10_repo>
Select secondary job for failover:0
```

- **For Windows OS:**

a. Go to the Veeam Plug-in installation directory (by default, `C:\Program Files\Veeam\VeeamPluginforOracleRMAN\`).

b. Run the following command and select *0* as a secondary job for failover:

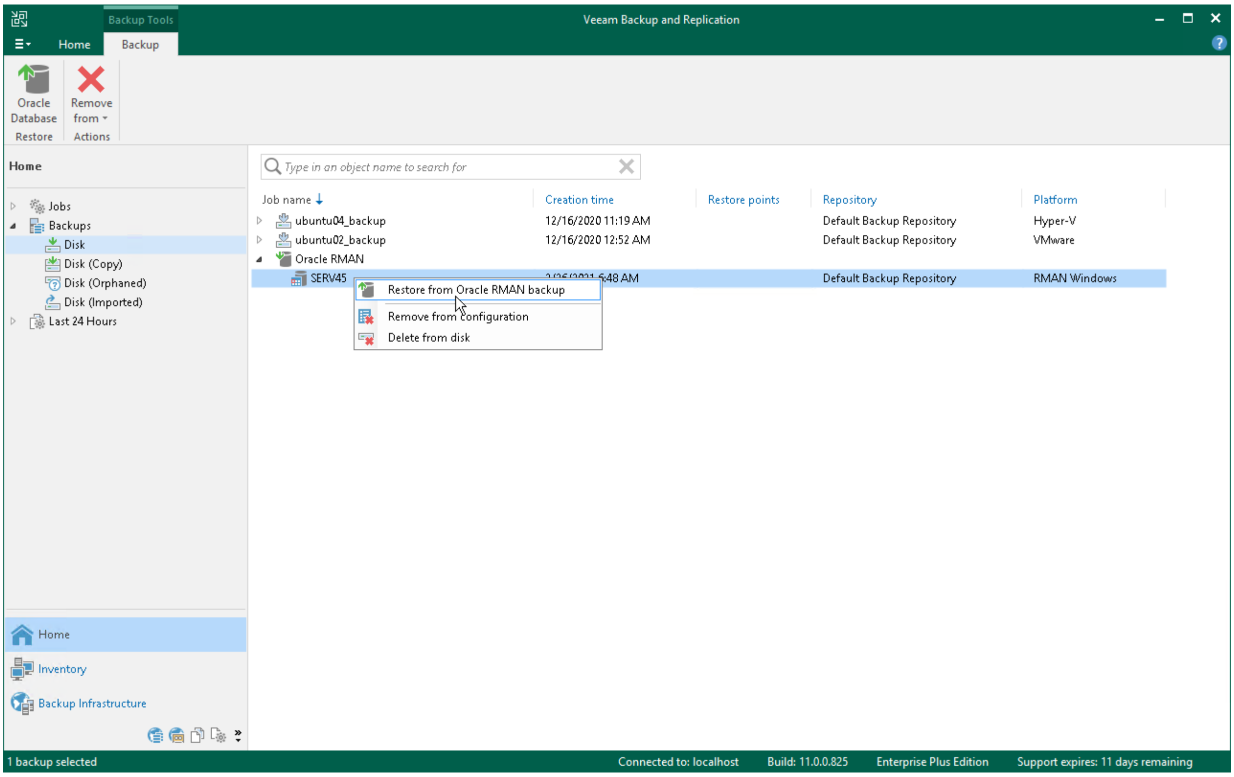
```
OracleRMANConfigTool.exe --configure-restore-from-copy
Select secondary job for failover:
0. Disable
1. Plug-ins backup copy job\SERV02 Oracle backup <serv10_repo>
Select secondary job for failover:0
```

Restore with Veeam Explorer for Oracle

You can restore Oracle databases from Veeam Plug-in backups in the Veeam Backup & Replication console. To restore Oracle databases Veeam Backup & Replication uses Veeam Explorer for Oracle. For details, see the Restoring Oracle RMAN Backups section of the Veeam Explorers User Guide.

> **IMPORTANT**
>
> Mind the following:
>
> - Veeam Explorer for Oracle does not support restore of encrypted Oracle databases.
> - [For Solaris OS and IBM AIX] Veeam Explorer for Oracle does not support restore of Oracle databases deployed on Solaris OS and IBM AIX. You can restore Oracle databases on Solaris OS and IBM AIX only with RMAN. For details, see the Restore with Oracle RMAN section of the Veeam Plug-ins for Enterprise Applications User Guide.

> **TIP**
>
> Mind the following:
>
> - To perform restore from Oracle databases you can also use Veeam Explorer's cmdlets. For details, see the Veeam Explorer for Oracle section of the Veeam Explorers Powershell Reference.
> - For details on Veeam Explorer for Oracle, see the Veeam Explorer for Oracle section of the Veeam Explorers User Guide.



Job name	Creation time	Restore points	Repository	Platform
ubuntu04_backup	12/16/2020 11:19 AM		Default Backup Repository	Hyper-V
ubuntu02_backup	12/16/2020 12:52 AM		Default Backup Repository	VMware
Oracle RMAN				
SERV45	[illegible]:48 AM		Default Backup Repository	RMAN Windows

1 backup selected | Connected to: localhost | Build: 11.0.0.825 | Enterprise Plus Edition | Support expires: 11 days remaining

Restore of Control File from Autobackup

You may need to restore the Oracle database control file in the following cases:

- If you want to restore the database to a new location where the control file does not exist
- If the database control file is lost or corrupted

If you use Veeam Plug-in for Oracle RMAN and want to restore the Oracle database control file from autobackup, the autobackup format must be set to the SBT_TAPE device type.

To check if persistent configuration for the control file autobackup format is set to the SBT_TAPE device type, you can run the SHOW ALL or SHOW CONTROLFILE AUTOBACKUP FORMAT commands in the RMAN console. If the persistent configuration is set, you don't need to set the control file autobackup format before the restore command. If it is not set, you must run the SET CONTROLFILE AUTOBACKUP command before the restore process. See the following examples.

> **NOTE**
>
> To restore the control file from autobackup, the database must be in the NOMOUNT state.

Restoring Control File if Persistent Configuration Setting is NOT Set

If the persistent configuration for the control file autobackup format is NOT set to the SBT_TAPE device type, you must set the autobackup format before running the control file restore.

```
RUN {
ALLOCATE CHANNEL c0 DEVICE TYPE sbt PARMS 'SBT_LIBRARY=/opt/veeam/VeeamPluginfo
rOracleRMAN/libOracleRMANPlugin.so';
SET CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE 'SBT_TAPE' TO '%F_RMAN_AUTOBA
CKUP.vab';
RESTORE controlfile FROM 'c-4097408439-20200410-00_RMAN_AUTOBACKUP.vab';
}
EXIT;
```

Restoring Control File if Persistent Configuration Setting is Set

If persistent configuration for the control file autobackup format is set to the SBT_TAPE device type, you must set the autobackup format before running the control file restore. To restore the control file, run the following script in the RMAN console:

```
RUN {
ALLOCATE CHANNEL c0 DEVICE TYPE sbt PARMS 'SBT_LIBRARY=/opt/veeam/VeeamPluginfo
rOracleRMAN/libOracleRMANPlugin.so';
RESTORE controlfile FROM 'c-4097408439-20200410-00_RMAN_AUTOBACKUP.vab';
}
EXIT;
```

See Also

- For details on restoring the control file, see the RMAN Restore: Restoring Lost Database Files from Backup section of the Database Backup and Recovery Basics guide.
- For details on the control file autobackup format, see the Configuring the Control File Autobackup Format section of the Database Backup and Recovery Basics.

Restore from Hardened Repository

As a result of malware activity or unplanned actions, backup job metadata (VACM) files may become unavailable in the hardened repository. In this case, to restore data from the hardened repository, you must re-create the VACM file. To do this, complete the following steps:

1. Run a Veeam Plug-in backup job to create a new Veeam Plug-in backup in a Veeam backup repository. The backup will consist of the VAB, VASM and VACM files.
2. In the backup repository folder, replace the VAB and VASM files created at the step 1 with the VAB and VASM files from the hardened repository.
3. In the Veeam backup console, run the backup repair operation. Veeam Backup & Replication will generate a new VACM file using information from the VASM files. For details, see Repairing Backup.

Once the backup job metadata file is re-created, you can use Veeam Plug-in to restore your data.

Repairing Backup

If you want to restore data from an immutable backup that resides in a hardened repository, you can use the **Repair** operation. During this operation, Veeam Backup & Replication will generate a new backup job metadata (VACM) file using information from the backup metadata (VASM) files.

> IMPORTANT
>
> This operation is intended only for a situation where the backup job metadata file has been lost as a result of malware activity or unplanned actions. Re-creation of the backup job metadata file for other purposes is not supported.

Before you start the repair operation, you must disable the backup job that created the backup. Otherwise, Veeam Backup & Replication will display a message notifying that the job must be disabled.

To repair a backup:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. In the inventory pane, select **Backups**.
3. In the working area, select the necessary backup.
4. Press and hold the **[CTRL]** key, right-click the backup and select **Repair**.

Retention of RMAN Backups and Archived Logs

In the main scenario, when using Veeam Plug-in for Oracle RMAN, you must configure retention policies for RMAN backups and archived redo logs using native Oracle RMAN functionality:

- Configuring Retention Policy
- Configuring Archived Redo Log Retention

Also, you can manually delete backups from a backup repository using the Veeam Backup & Replication console and enable the force deletion functionality of Veeam Plug-in for Oracle RMAN. For details, see:

- Configuring Force Deletion of Backups
- Deleting Backups Manually
- Deleting Backups from Configuration

Configuring Retention Policy

If you want to edit a retention policy for Oracle RMAN backups, you must connect to the target database in RMAN console and configure one of the following retention policies:

- **Redundancy-Based Retention**: The `redundancy` parameter specifies how many full or level 0 backups of each data file and control file should RMAN keep in the repository. If the number of backups exceeds the specified value, RMAN considers the oldest backups as obsolete. By default, the redundancy parameter is set to 1. To configure a redundancy-based retention policy, run the following command:

  ```
  CONFIGURE RETENTION POLICY TO REDUNDANCY 7;
  ```

- **Recovery Window-Based Retention**: The `recovery window` parameter specifies the number of days between the current time and the earliest point of recoverability. RMAN does not consider any full or level 0 incremental backups as obsolete if it falls within the recovery window. To configure a window-based retention policy, run the following command:

  ```
  CONFIGURE RETENTION POLICY TO RECOVERY WINDOW OF 7 days;
  ```

Deleting Obsolete Backups

To delete obsolete backups, run the following command after each backup:

```
DELETE OBSOLETE;
```

Disabling Retention Policy

To disable retention policy for RMAN backups, run the following command:

```
CONFIGURE RETENTION POLICY TO NONE;
```

For details, see the Configuring the Backup Retention Policy section of the Oracle Database Backup and recovery User's Guide.

Configuring Archived Redo Log Retention

By default, archivelog deletion policy is disabled.

To configure archivelog deletion policy, run the following command. When the number of archived logs exceeds the specified number, RMAN deletes the oldest archived log.

```
CONFIGURE ARCHIVELOG DELETION POLICY TO BACKED UP 3 TIMES TO SBT;
```

To delete obsolete archivelogs, run the following command. If you do not run this command, the archived logs will be deleted from the fast recovery area (FRA) only.

```
DELETE ARCHIVELOG ALL;
```

To disable archivelog deletion policy, run the following command:

```
CONFIGURE ARCHIVELOG DELETION POLICY TO NONE;
```

For details, see the Configuring an Archived Redo Log Deletion Policy section of the Oracle Database Backup and Recovery User's Guide.

Configuring Force Deletion of Backups

In the main scenario, when using Veeam Plug-in for Oracle RMAN, you must configure the retention policy using native Oracle RMAN tools. For details, see Configuring Retention Policy.

Veeam Plug-in for Oracle RMAN has a functionality that automatically force deletes backup files which are older than specified number of days. For example, you can use it if a backup repository contains backup files that are no longer in the backup catalog.

To enable force deletion of backup files, do the following:

1. On the Oracle server, run the following command.

   ○ **For Linux and Unix:**

   ```
   OracleRMANConfigTool --set-force-delete
   ```

   ○ **For Microsoft Windows:**

   ```
   OracleRMANConfigTool.exe --set-force-delete
   ```

   By default, the `OracleRMANConfigTool.exe` file is located in `C:\Program Files\Veeam\VeeamPluginforOracleRMAN`.

2. Enter the number of days after which Veeam Plug-in will force delete backup files on all configured Veeam backup repositories.

   ```
   Garbage collector automatically deletes backup files older than the specif
   ied number of days.
   Make sure the number of days value exceeds your retention policy.
   To disable this functionality, set the number of days to 0.
   Enter the number of days to delete backups after, between 7 and 999 [0]:
   ```

   By default, the force delete functionality is disabled (set to *0*).

IMPORTANT

- A value for the **number of days** setting must be at least 1 backup generation period longer than the retention period for your Oracle Database backups. Otherwise, Veeam Plug-in will delete earliest backups created within the retention period.
- If a backup repository contains backups older than the specified retention period, Veeam Plug-in removes old backup files only after the next run of the RMAN backup.

Deleting Backups Manually

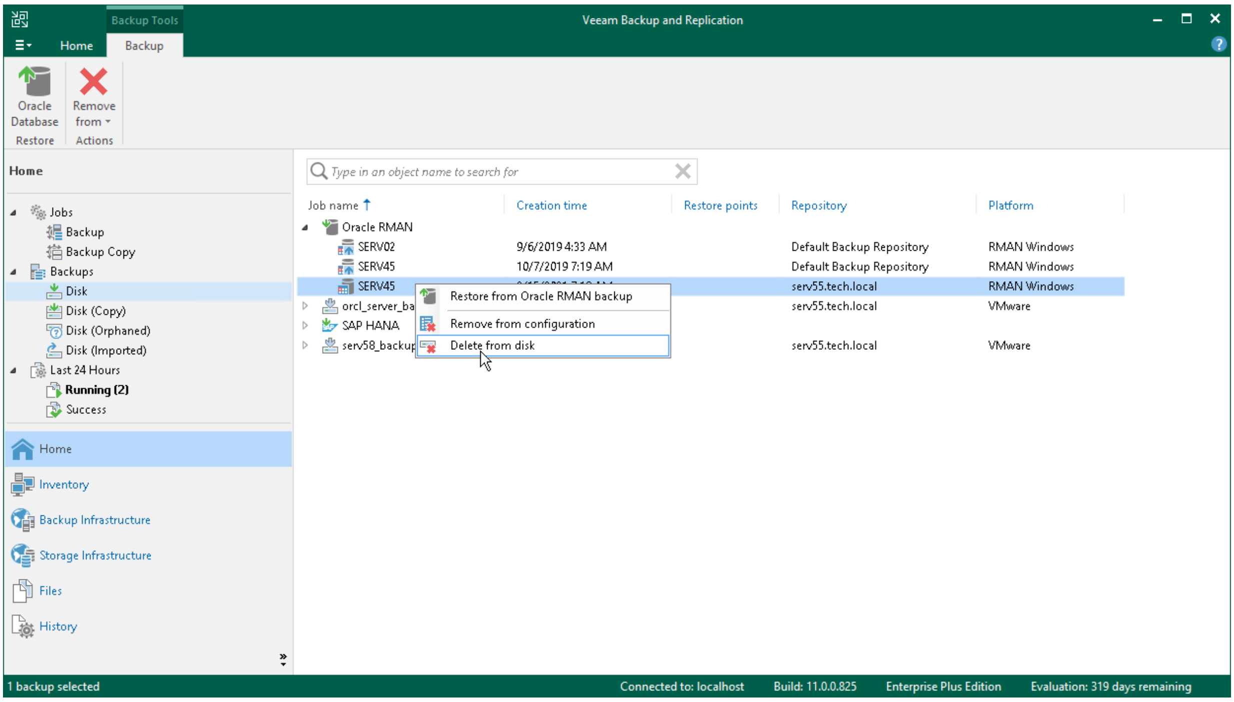
If you want to delete backups files, you can use the Oracle RMAN housekeeping functionality. For details, see the Deleting RMAN Backups and Archived Redo Logs section of the Oracle Database Backup and Recovery User's Guide.

If you have lost the recovery catalog, you can remove the backups manually from a Veeam backup repository.

> **IMPORTANT**
>
> If you remove backups from a Veeam backup repository manually, the metadata about these backups is NOT deleted from the recovery catalog. Thus, if you have a recovery catalog, it is not recommended to manually delete backup files. Otherwise, the recovery catalog will remain in the outdated state.

To remove a backup from Veeam backups repository, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. In the **Inventory** pane, select **Backups**.
3. In the working area, right-click the backup job object name and select **Delete from disk**.



Job name	Creation time	Restore points	Repository	Platform
Oracle RMAN				
SERV02	9/6/2019 4:33 AM		Default Backup Repository	RMAN Windows
SERV45	10/7/2019 7:19 AM		Default Backup Repository	RMAN Windows
SERV45			serv55.tech.local	RMAN Windows
orcl_server_ba			serv55.tech.local	VMware
SAP HANA				
serv58_backup			serv55.tech.local	VMware

1 backup selected   Connected to: localhost   Build: 11.0.0.825   Enterprise Plus Edition   Evaluation: 319 days remaining

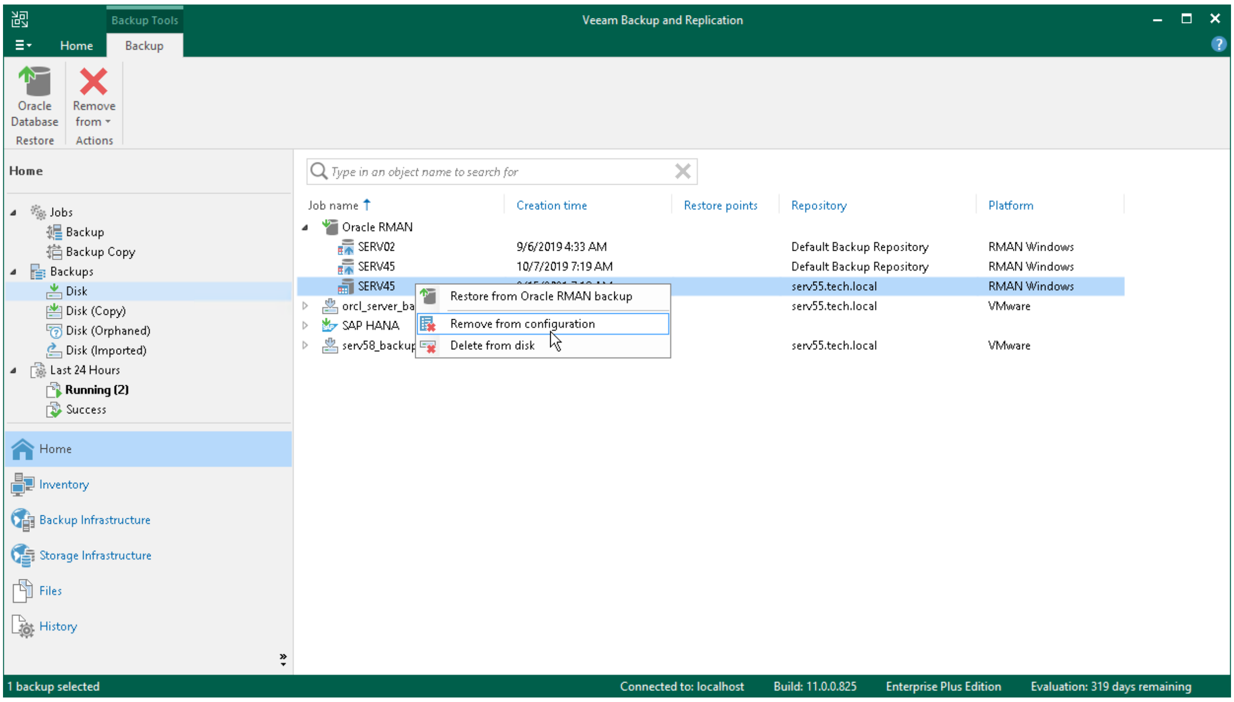
Removing Backups from Configuration

If you want to remove records about backups from the Veeam Backup & Replication console and configuration database, you can use the **Remove from configuration** operation.

When you remove a backup from the configuration, backup files (VAB, VBM) remain on the backup repository. You can import the backup later and restore data from it.

To remove a backup from configuration:

1. Open the **Home** view.
2. In the inventory pane, select **Backups**.
3. In the working area, select the necessary backup.
4. Press and hold the **[CTRL]** key, right-click the backup and select **Remove from configuration**.



Job name	Creation time	Restore points	Repository	Platform
Oracle RMAN				
SERV02	9/6/2019 4:33 AM		Default Backup Repository	RMAN Windows
SERV45	10/7/2019 7:19 AM		Default Backup Repository	RMAN Windows
SERV45	[illegible]		serv55.tech.local	RMAN Windows
orcl_server_ba			serv55.tech.local	VMware
SAP HANA				
serv58_backup			serv55.tech.local	VMware

Backup Copy for Oracle RMAN Backups

Having just one backup does not provide the necessary level of safety. The primary backup may get destroyed together with production data, and you will have no backups from which you can restore data.

To build a successful data protection and disaster recovery plan, it is recommended that you follow the 3-2-1 rule:

- 3: You must have at least three copies of your data: the original production data and two backups.
- 2: You must use at least two different types of media to store the copies of your data, for example, local disk and cloud.
- 1: You must keep at least one backup offsite, for example, in the cloud or in a remote site.

Thus, you must have at least two backups and they must be in different locations. If a disaster takes out your production data and local backup, you can still recover from your offsite backup.

Creating Backup Copy Job

Veeam Backup & Replication offers the backup copy functionality that allows you to create several instances of the same backup in different locations, whether onsite or offsite. Backup copies have the same format as those created by backup jobs and you can recover your data from them when you need it.

Veeam Backup & Replication fully automates the backup copy process and lets you specify retention settings to maintain the desired number of restore points, as well as full backups for archival purposes. Backup copy is a job-driven process. When enabled, the backup copy job for Veeam Plug-in backups runs continuously. For more details on how it works, see the Backup Copy section of the Veeam Backup & Replication User Guide.

To copy backups to a secondary location, you must configure a backup copy job. The backup copy job defines how, where and when to copy backups. One job can be used to process backups of one or more machines.

You can configure a job and start it immediately or save the job to start it later.

Before creating a job, check prerequisites. Then use the **New Backup Copy Job** wizard to configure a backup copy job.

Before You Begin

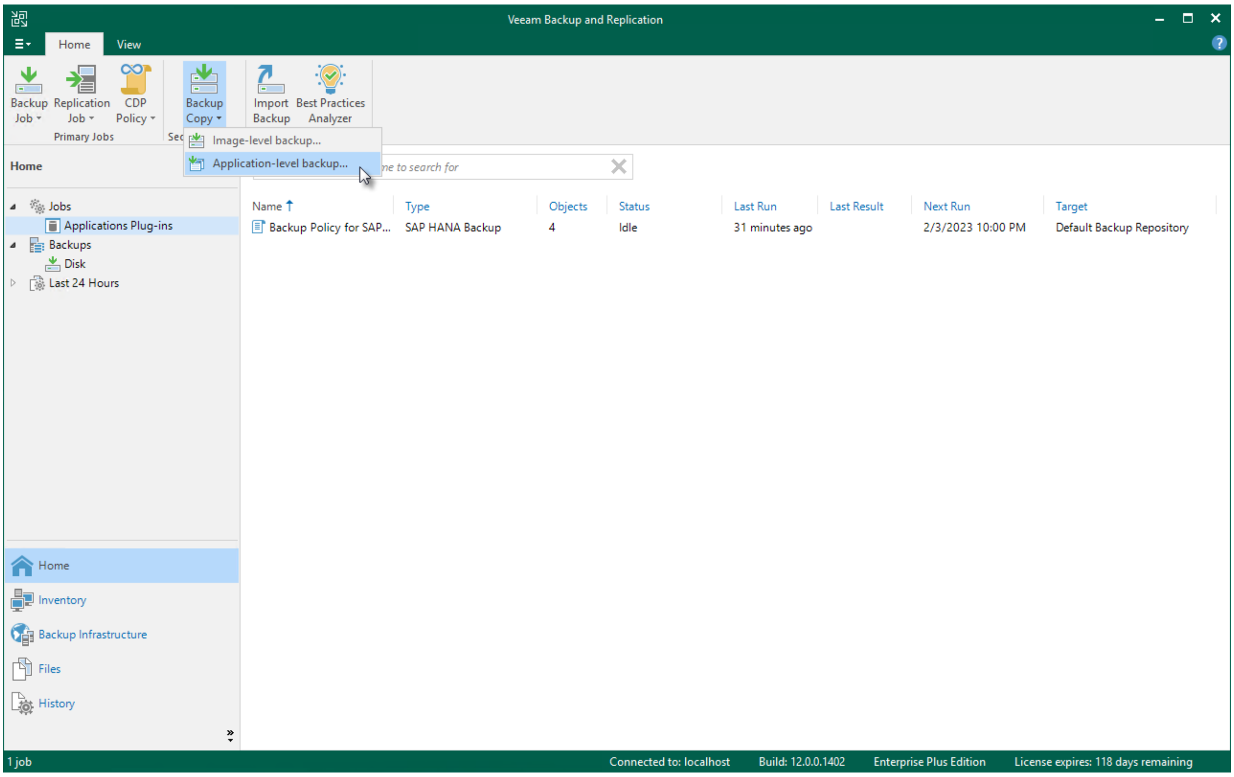
Before you create a backup copy job, check the prerequisites and limitations:

- Backup infrastructure components that will take part in the backup copy process must be added to the backup infrastructure and properly configured. These include source and target backup repositories between which backups must be copied.
- The target backup repository must have enough free space to store copied backups. To receive alerts about low space on the backup repository, configure global notification settings. For more information, see Specifying Other Notification Settings.
- For Veeam Plug-in backup copy jobs, you cannot select a Veeam Cloud Connect repository as a backup copy target.
- If you have upgraded the backup files, make sure that you have upgraded Veeam Plug-in on the source server. If the plug-in is not upgraded to version 12 and you convert backup copy files to backup files, then the next backup job runs will fail.

Step 1. Launch Backup Copy Job Wizard

To create a backup copy job, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Click the **Backup Copy** tab and select **Application-level backup**.



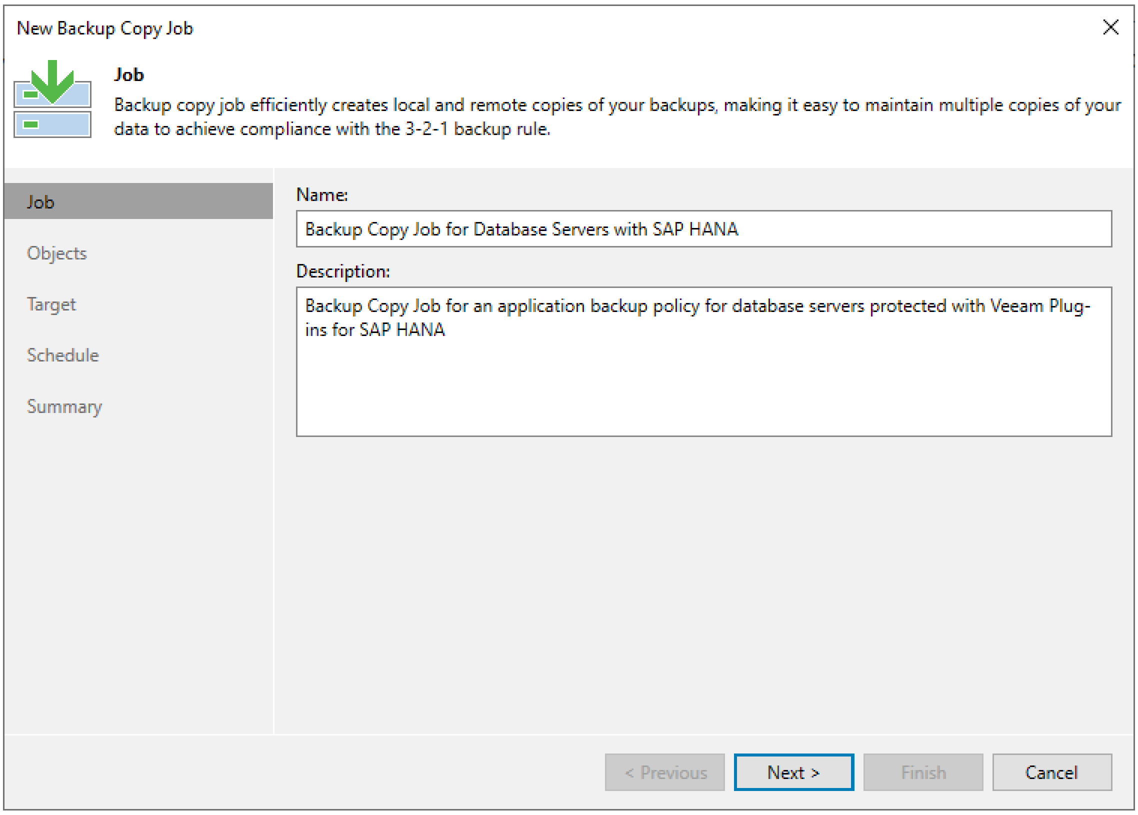
Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target
Backup Policy for SAP...	SAP HANA Backup	4	Idle	31 minutes ago		2/3/2023 10:00 PM	Default Backup Repository

1 job Connected to: localhost Build: 12.0.0.1402 Enterprise Plus Edition License expires: 118 days remaining

Step 2. Specify Job Name and Description

At the **Job** step of the wizard, specify a name and description for the backup copy job.

1. In the **Name** field, enter a name for the job.
2. In the **Description** field, enter a description for the job. The default description contains information about the user who created the job, date and time when the job was created.



Job

Backup copy job efficiently creates local and remote copies of your backups, making it easy to maintain multiple copies of your data to achieve compliance with the 3-2-1 backup rule.

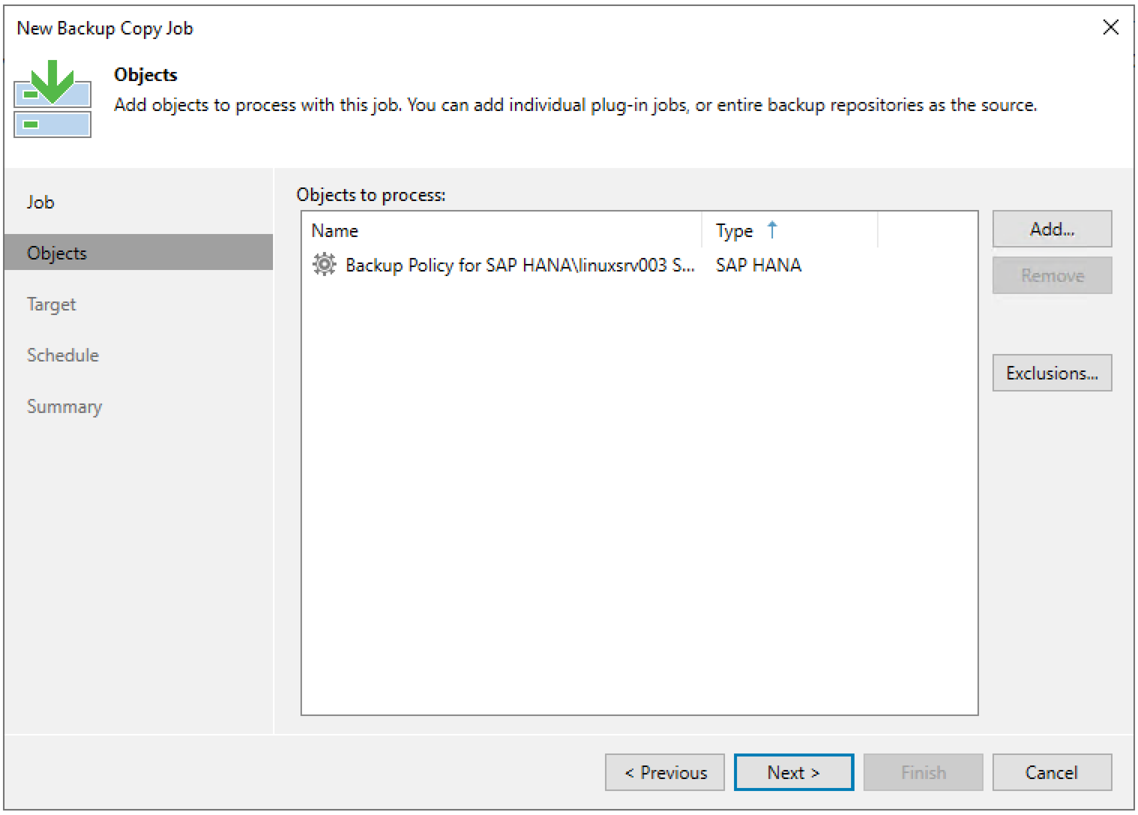
Name: Backup Copy Job for Database Servers with SAP HANA

Description: Backup Copy Job for an application backup policy for database servers protected with Veeam Plug-ins for SAP HANA

Step 3. Select Backups to Process

At the **Object** step of the wizard, select machines whose backups you want to copy to the target repository.

1. Click the **Add** button and select from which entity you want to process the machines.
   - **From jobs**: You can select Veeam Plug-in backup jobs. When a backup copy job runs, Veeam Backup & Replication will search for backup files created by selected jobs.
   - **From repositories**: You can select repositories where Veeam Plug-in backups are stored. When a backup copy job runs, Veeam Backup & Replication will search for backup files created by Veeam Plug-in in selected repositories.
2. Use the **Remove** button if you want to remove selected jobs or repositories from processing.
3. If you have added jobs from a repository and want to exclude from processing some of the backup jobs on the selected repository, click **Exclusions** and select the jobs that you want to exclude.



New Backup Copy Job

Objects

Add objects to process with this job. You can add individual plug-in jobs, or entire backup repositories as the source.

Objects to process:

Name	Type
Backup Policy for SAP HANA\linuxsrv003 S...	SAP HANA

Step 4. Define Backup Copy Target

At the **Target** step of the wizard, configure the target repository settings.

1. From the **Backup repository** list, select a backup repository in the target site where copied backups must be stored. When you select a target backup repository, Veeam Backup & Replication automatically checks how much free space is available on it. Make sure that you have enough free space to store copied backups.

   > IMPORTANT
   >
   > For Veeam Plug-in backup copy jobs, you cannot select a Veeam Cloud Connect repository as a backup copy target.

2. If the target repository contains a Veeam Plug-in backup that was excluded from the backup copy job, and if you don't want to transfer duplicate data, you can use the mapping feature.

   After you configure mapping, if some of backup files (VAB) of the source backup are missing in the target backup copy, these files are uploaded to the target backup copy.

   > NOTE
   >
   > Veeam Plug-in backup copy jobs do not use WAN accelerators.

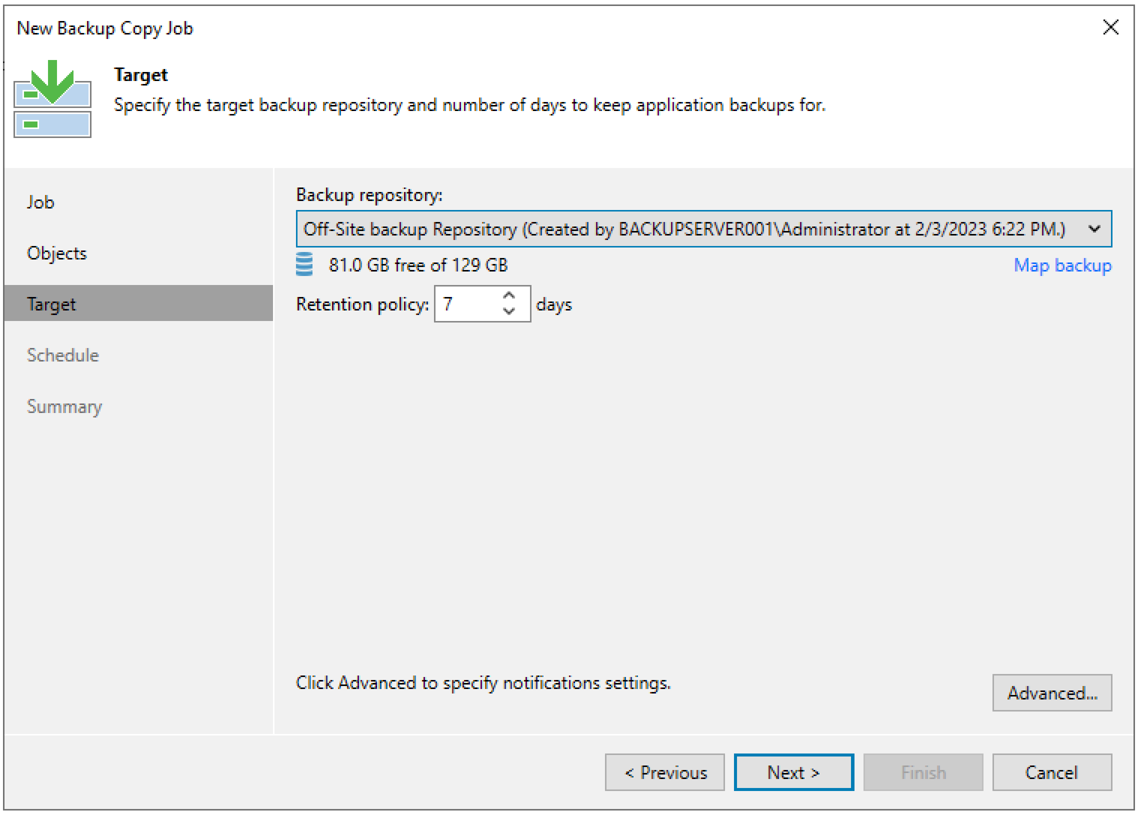
   To map a backup copy job to the backup:

   a. Click the **Map backup** link.

   b. Point the backup copy job to the backup in the target backup repository. Backups in the target backup repository can be easily identified by backup job names. To facilitate search, you can use the search field at the bottom of the window.

   > IMPORTANT
   >
   > - Used account must have access to Veeam backup repositories that you plan to use.
   > - Encryption must be disabled on the repository.
   >
   > Otherwise, the repositories will not be listed as available. To learn how to configure access permissions and encryption settings on repositories, see Access and Encryption Settings on Repositories.

3. You can specify the number of days after which the backup copy will be deleted from the repository. Note that the countdown starts from the moment when source backup has been created.


New Backup Copy Job
Target
Specify the target backup repository and number of days to keep application backups for.
Job
Objects
Target
Schedule
Summary

Backup repository: Off-Site backup Repository (Created by BACKUPSERVER001\Administrator at 2/3/2023 6:22 PM.)

81.0 GB free of 129 GB

Retention policy: 7 days

Click Advanced to specify notifications settings.

Step 5. Specify Advanced Settings

At the **Target** step of the wizard, click **Advanced** to configure storage, RPO warning, and notifications settings.

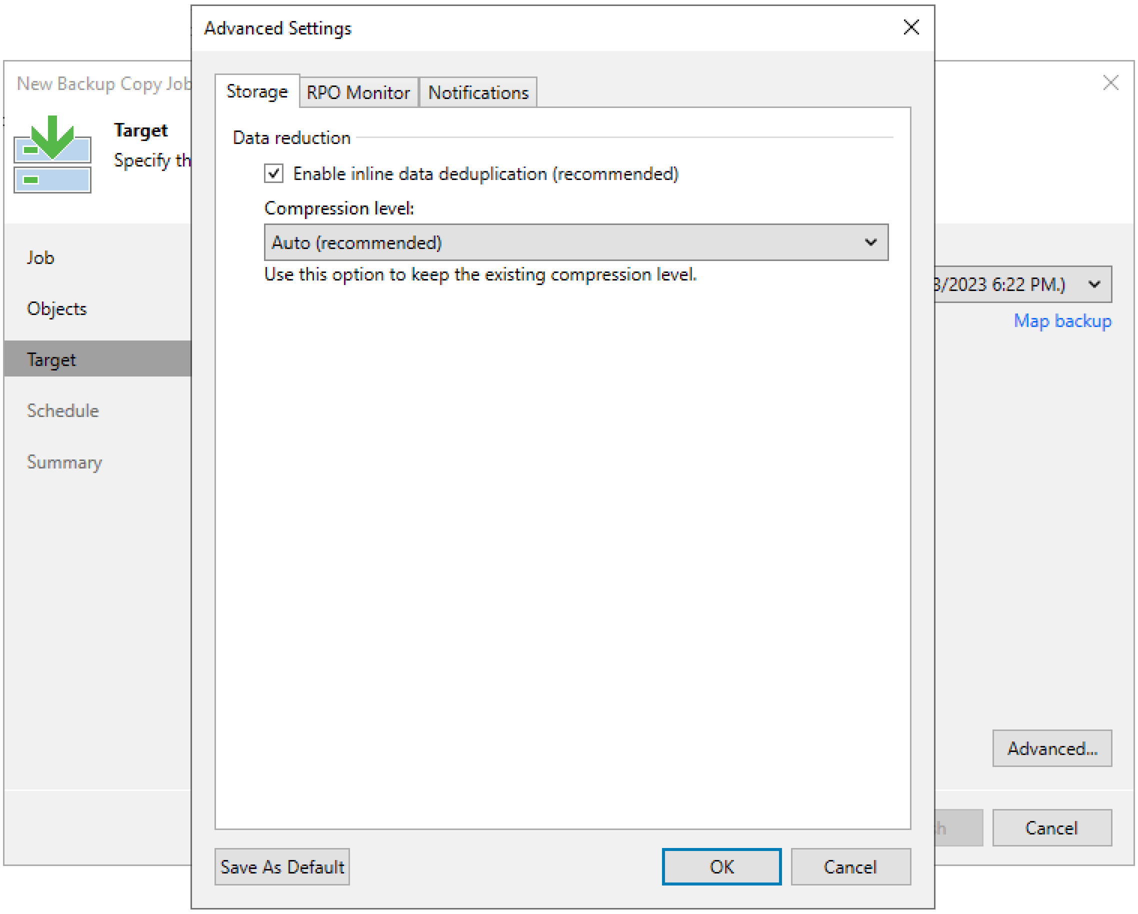
- Storage settings
- RPO warning settings
- Notification settings

Storage Settings

At the **Storage** tab, define compression and deduplication settings.

By default, Veeam Backup & Replication performs deduplication before storing copied data on the target backup repository. Deduplication provides a smaller size of the resulting backup file but may reduce the job performance.

1. You can disable data deduplication. To do this, clear the **Enable inline data deduplication** check box.
2. From the Compression level list, choose a compression level to be used: **Auto**, **None**, **Dedupe-friendly**, **Optimal**, **High** or **Extreme**. The recommended level of compression for backup copy jobs is **Auto**. In this case, Veeam Backup & Replication uses compression settings of the copied backup files. For more information, see Compression and Deduplication.



Advanced Settings

Storage | RPO Monitor | Notifications

Data reduction

☑ Enable inline data deduplication (recommended)

Compression level: Auto (recommended)

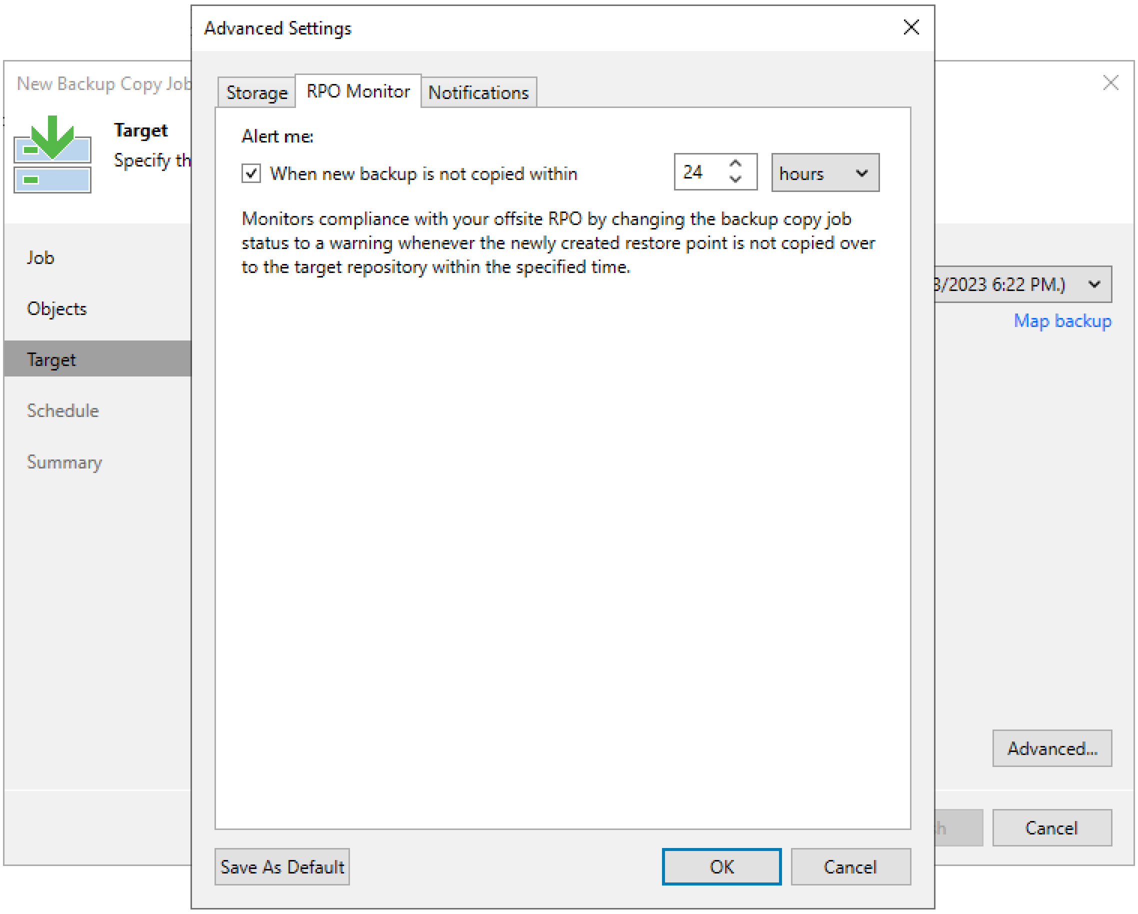
Use this option to keep the existing compression level.

RPO Warning Settings

At the **RPO Monitor** tab, specify RPO warning settings.

Enable the **Warn me if backup is not copied within** check box and specify the time period in **minutes**, **hours**, or **days.**

If the backup copy is not created within the specified time period, the backup copy job will finish with the *Warning* status. The countdown starts from the moment when the required backup is finished and ready to be copied.



Advanced Settings

Alert me:

☑ When new backup is not copied within 24 hours

Monitors compliance with your offsite RPO by changing the backup copy job status to a warning whenever the newly created restore point is not copied over to the target repository within the specified time.

Notification Settings

At the **Notifications** tab, to specify notification settings for the backup copy job:

1. At the **Target** step of the wizard, click **Advanced**.
2. Click the **Notifications** tab.
3. Select the **Send SNMP notifications for this job** check box if you want to receive SNMP traps when the job completes successfully. SNMP traps will be sent if you specify global SNMP settings in Veeam Backup & Replication and configure software on recipient's machine to receive SNMP traps. For more information, see Specifying SNMP Settings.
4. Select the **Send email notifications to the following recipients** check box if you want to receive notifications by email in case of job failure or success. In the field below, specify a recipient's email address. You can enter several addresses separated by a semicolon.

5. Veeam Backup & Replication sends a consolidated email notification once for the specified backup copy interval. Even if the synchronization process is started several times within the interval, for example, due to job retries, only one email notification will be sent.

6. Email notifications will be sent if you configure global email notification settings in Veeam Backup & Replication. For more information, see Configuring Global Email Notification Settings.

7. At the **Send** at field, specify the time when you want to receive notifications. Note that you will receive a notification on the job status once a day.

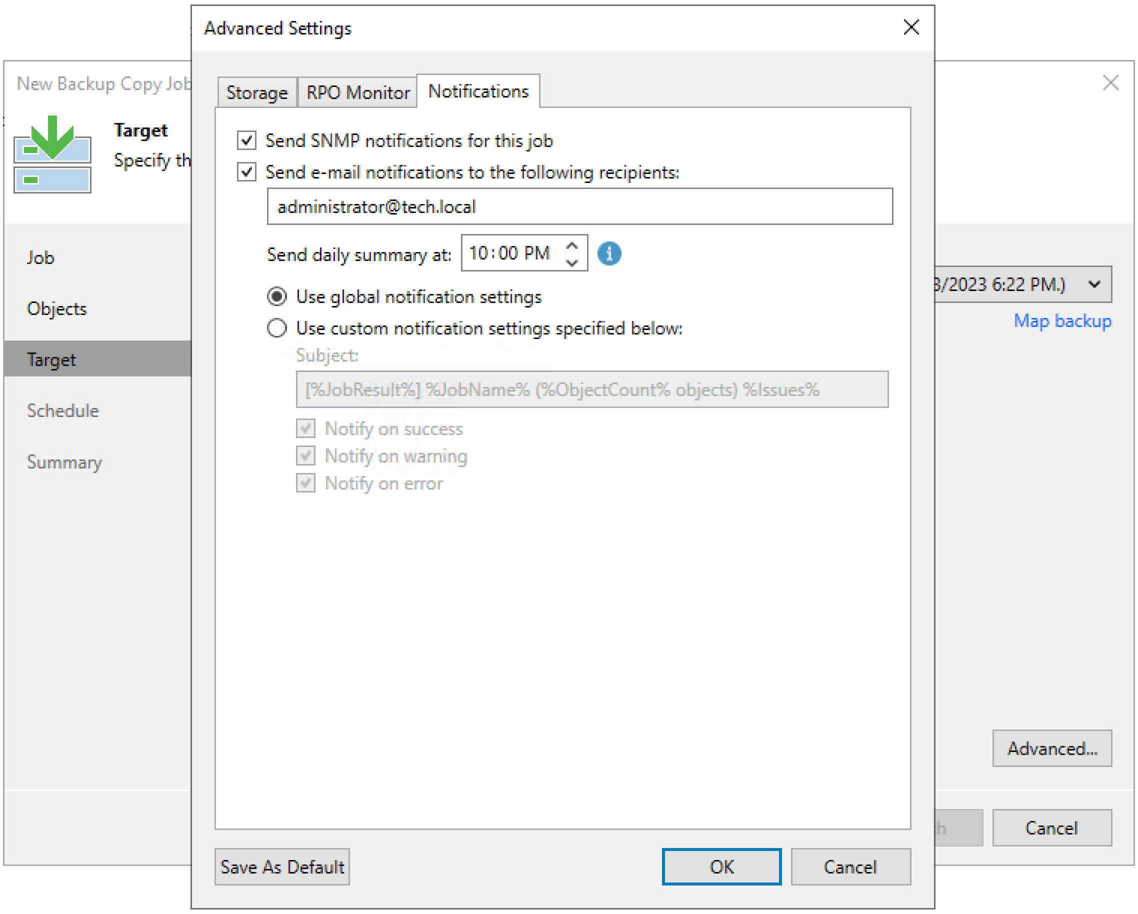
8. You can choose to use global notification settings or specify custom notification settings.

   - To receive a typical notification for the job, select **Use global notification settings**. In this case, Veeam Backup & Replication will apply to the job global email notification settings specified for the backup server. For more information, see Configuring Global Email Notification Settings.

   - To configure a custom notification for a job, select **Use custom notification settings specified below**. You can specify the following notification settings:

     i. In the **Subject** field, specify a notification subject. You can use the following variables in the subject: *%Time%* (completion time), *%JobName%*, *%JobResult%*, *%VmCount%* (number of machines in the job) and *%Issues%* (number of machines in the job that have been processed with the **Warning** or **Failed** status).

     ii. Select the **Notify on success**, **Notify on warning** and **Notify on error** check boxes to receive email notification if data processing within the backup copy interval completes successfully, fails or completes with a warning.



☑ Send SNMP notifications for this job

☑ Send e-mail notifications to the following recipients:

administrator@tech.local

Send daily summary at: 10:00 PM

● Use global notification settings

○ Use custom notification settings specified below:

Subject:

[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

☑ Notify on success

☑ Notify on warning

☑ Notify on error

Step 6. Define Backup Copy Schedule

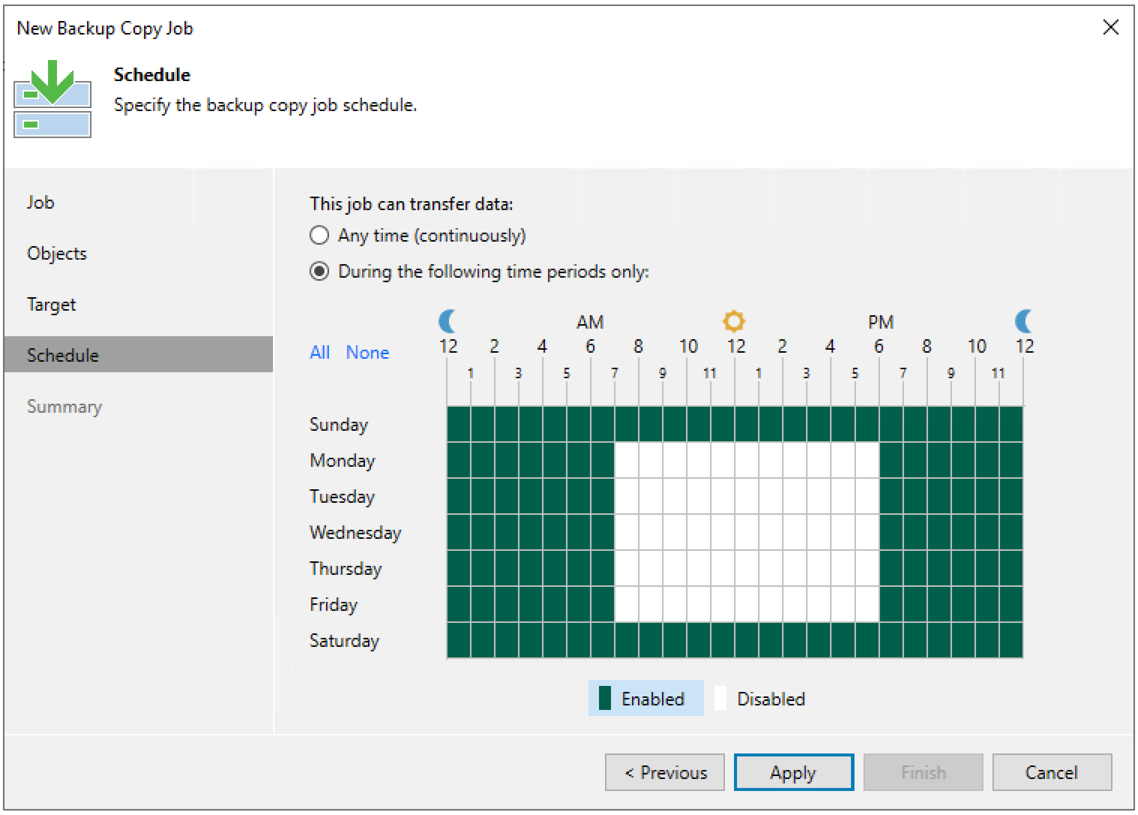
At the **Schedule** step of the wizard, define a time span in which the backup copy job must not transport data between source and target backup repositories. For more information, see Backup Copy Window.

To define a backup window for the backup copy job:

1. Select the **During the following time periods only** option.

2. In the schedule box, select the desired time area.

3. Use the **Enable** and **Disable** options to mark the selected area as allowed or prohibited for the backup copy job.



New Backup Copy Job

Schedule

Specify the backup copy job schedule.

- Job
- Objects
- Target
- Schedule
- Summary

This job can transfer data:

○ Any time (continuously)

● During the following time periods only:

All None

AM / PM

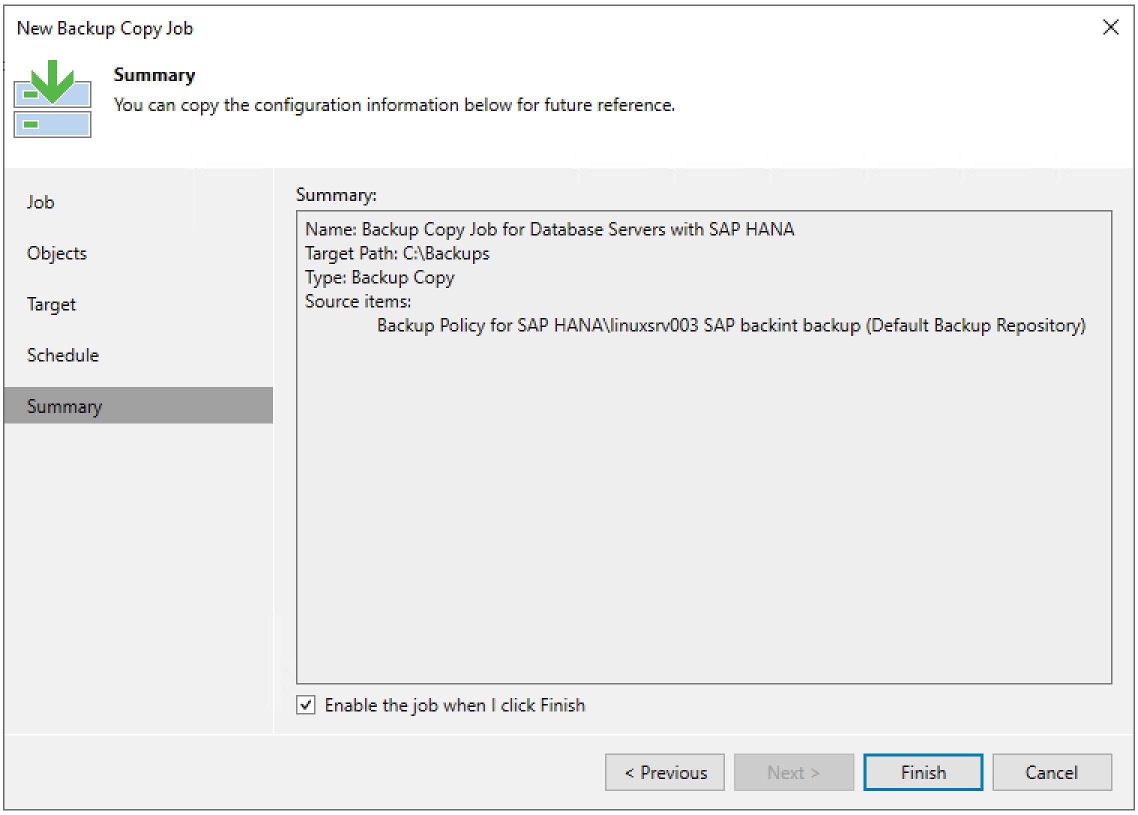
	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11
Sunday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Monday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩
Tuesday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩
Wednesday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩
Thursday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩
Friday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩
Saturday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩

🟩 Enabled ⬜ Disabled

Step 7. Review Backup Copy Job Settings

At the **Summary** step of the wizard, complete the procedure of backup copy job configuration.

1. Review details of the backup copy job.
2. Select the **Enable the job when I click Finish** check box if you want to start the job right after you finish working with the wizard.
3. Click **Finish** to close the wizard.



New Backup Copy Job

Summary

You can copy the configuration information below for future reference.

Summary:

Name: Backup Copy Job for Database Servers with SAP HANA
Target Path: C:\Backups
Type: Backup Copy
Source items:
Backup Policy for SAP HANA\linuxsrv003 SAP backint backup (Default Backup Repository)

☑ Enable the job when I click Finish

Converting Backup Copy to Backup

If you have imported Veeam Plug-in backup copies from another server, you can convert them into regular backup files. When you convert a backup copy to a backup, Veeam Plug-in creates a backup job with the converted backup. You can use this backup job to continue a backup chain and use the converted backup as a restore point.

You can convert and unbind Veeam Plug-in backups into regular Veeam Plug-in backup files in the following cases:

- If you have deleted a backup copy job which created the backup copy.
- If you have excluded a backup job from a backup copy job that used multiple backup jobs as a source.
- If you imported a Veeam Plug-in backup copy from another host.

> **NOTE**
> If you want to restore from a backup copy, you don't need to convert the backup copy to backup. For details, see Restore from Backup Copy.

Procedure

To convert a backup copy to a primary backup, use the **--promote-backup-copy-to-primary** parameter as shown below:

1. Run the **OracleRMANConfigTool** with the **--promote-backup-copy-to-primary** parameter and type a backup copy number from the list of available backup copies.

```
OracleRMANConfigTool --promote-backup-copy-to-primary
Backup copies available for promotion to the primary backup target:
1. Backup Copy Job 1\ORCLSERV01 Oracle backup (Default Backup Repository)
Select a backup copy: 1
Changes to be applied to the RMAN configuration
CONFIGURE CHANNEL DEVICE TYPE SBT_TAPE
PARMS 'SBT_LIBRARY=C:\PROGRA~1\Veeam\VEEAMP~1\ORACLE~2.DLL'
FORMAT '94a7ac5a-2cb5-418b-8395-fb362d3aa182/RMAN_%I_%d_%T_%U.vab';
CONFIGURE CONTROLFILE AUTOBACKUP ON;
CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE SBT_TAPE TO '%F_RM
AN_AUTOBACKUP.vab';
CONFIGURE ARCHIVELOG BACKUP COPIES FOR DEVICE TYPE SBT_TAPE TO 1;
CONFIGURE DATAFILE BACKUP COPIES FOR DEVICE TYPE SBT_TAPE TO 1;
RMAN configuration to be applied:
SQL "alter system set backup_tape_io_slaves=false deferred scope=both";
```

2. Converting a backup copy into regular backup file, requires changes in the RMAN configuration. You can allow the command to change RMAN configuration automatically, or you can change it manually. Select one of the options:

```
Proceed with the action?
1. Promote backup copy destination to the primary backup target and apply
required configuration to RMAN automatically
2. Promote backup copy destination to the primary backup target and export
required RMAN configuration (RMAN will have to be configured manually)
3. Cancel
Enter selection: 1
Promoting backup copy destination
Configuring RMAN
Done
```

Logs and Support

If you have any questions or issues with Veeam Plug-in for Oracle RMAN or Veeam Backup & Replication, you can search for a resolution on Veeam Community Forums or submit a support case on the Veeam Customer Support Portal.

When you submit a support case, we recommend you attach necessary logs related to Veeam Plug-in operations.

To learn how to collect logs, see this Veeam KB.

Veeam Plug-in for SAP on Oracle

Veeam Plug-in for SAP on Oracle is an SAP-certified backup tool for SAP applications running on Oracle Database. Veeam Plug-in integrates with SAP BR*Tools and transfers database and log backups to repositories connected to Veeam Backup & Replication.

> **TIP**
>
> If you want to protect the SAP server itself, you can use the image-level backup functionality of Veeam Backup & Replication or Veeam Agent for Linux.

How Veeam Plug-in for SAP on Oracle Works

Veeam Plug-in for SAP on Oracle functions as an agent between SAP BR*Tools and Veeam backup repositories. After you install and configure Veeam Plug-in, you can perform all backup and restore operations with BR*Tools. Veeam Plug-in compresses, deduplicates database backups and transfers them to a backup repository connected to Veeam Backup & Replication.

Veeam Plug-in for SAP on Oracle supports the following tools:

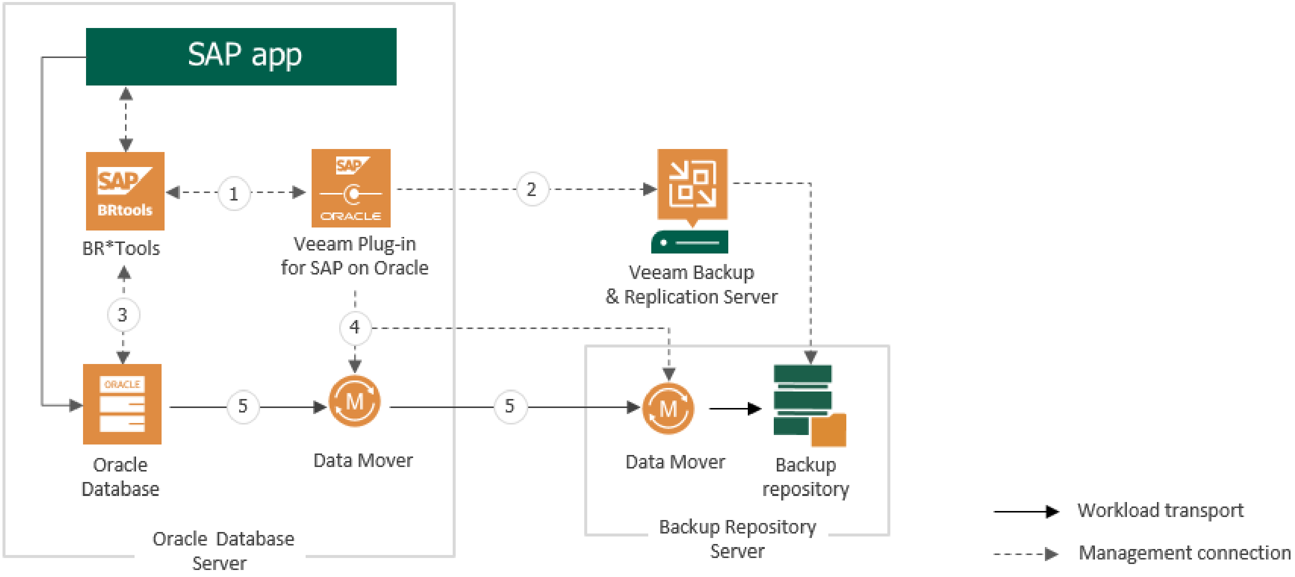
- `brtools`
- `brbackup`
- `brrestore`
- `brarchive`

For details about these tools, see the SAP Database Guide: Oracle.

How Backup Operations Work

After you configure Veeam Plug-in for SAP on Oracle, SAP BR*Tools performs a backup in the following way:

1. When you launch a database backup, BRTOOLS starts the services of Veeam Plug-in.
2. Veeam Plug-in connects to the Veeam Backup & Replication server and creates a backup job object (if it has not been created before). Veeam Backup & Replication administrators can use this backup job object to monitor the backup process, manage backup files and copy the database backup to secondary repositories.
3. BRTOOLS launches the backint BRBACKUP tool that uses the Veeam Plug-in configuration file as an initialization profile.
4. Veeam Plug-in starts Veeam Data Mover on the SAP server and on the backup repository. Veeam Data Movers create communication channels for each backup data stream. Depending on the number of channels specified in Veeam Plug-in settings, there can be 1 or up to 32 parallel channels.
5. Veeam Data Movers transport database backup files to the backup repository.



IMPORTANT

Some backup operations, such as backing up of profiles, log files, control files and performing incremental backups of databases can be performed only with RMAN_UTIL. For details, see the RMAN Backup Strategies.

For detail on how Veeam Plug-in for SAP on Oracle functions along with RMAN see, SAP on Oracle Backup Using RMAN_UTIL.

Planning and Preparation

Before you start to use Veeam Plug-in for SAP on Oracle, read the environment planning recommendations and make sure that your environment meets system requirements.

- System Requirements
- Required Permissions
- Used Ports
- Licensing
- Environment Planning
- Veeam Backup Repositories
- Access and Encryption on Repositories

System Requirements

Before you start using Veeam Plug-in for SAP on Oracle, make sure the following requirements are met.

Supported OSes

Veeam Plug-in for SAP on Oracle is supported for the following OSes:

- SUSE Linux Enterprise Server 11, 12, 15 (x86_64)
- Red Hat Enterprise Linux for SAP Applications 6, 7 (x86_64)
- Oracle Linux 6, 7

BR*Tools

Veeam Plug-in for SAP on Oracle supports BR*Tools 7.20 Patch 42 or later.

Oracle DB

Veeam Plug-in for SAP on Oracle supports Oracle Database 11gR2, 12c, 18c, 19c: Standard and Enterprise Edition (Express Edition is not supported).

Veeam Backup & Replication

The version of Veeam Backup & Replication must be the same or later than version of Veeam Plug-in. Veeam Plug-in for SAP on Oracle version 12 is compatible with Veeam Backup & Replication 12 or later.

Network

Veeam Plug-in should be able to establish a direct IP connection to the Veeam Backup & Replication server. Thus, Veeam Plug-in cannot work with the Veeam Backup & Replication server that is located behind the NAT gateway.

Permissions

User Rights on SAP on Oracle Server

The account used for installing and updating Veeam Plug-in must have root privileges.

User That Starts BR*Tools Operations

The account used to start BR*Tools backup and restore operations must have permissions described in the Starting BR*Tools section of the SAP Database Guide: Oracle.

Veeam Backup Server User

- The account specified in the Veeam Plug-in configuration settings must be able to authenticate against the Veeam Backup & Replication server. For details, see Configuring Veeam Plug-in for SAP on Oracle.
- The account specified in the Veeam Plug-in configuration settings must be granted access rights on the Veeam backup repository where you want to store backups.

  To learn how to grant permissions on Veeam repositories, see Granting Permissions on Repositories.
- You can work with backups created by Veeam Plug-in only with the account used for creating the backups. If you want to use another account, see required permissions in Configuring Veeam Plug-in for SAP on Oracle.

Ports

To enable proper work of Veeam Plug-ins, make sure that the following ports are open.

SAP on Oracle Server

The following table describes network ports that must be opened to ensure proper communication of the SAP on Oracle server and backup infrastructure components.

From	To	Protocol	Port	Notes
SAP on Oracle server where Veeam Plug-in is installed	Veeam Backup & Replication server	TCP	10006	Default port used for communication with the Veeam Backup & Replication server. Note that data between Veeam Plug-ins and backup repositories is transferred directly, bypassing the Veeam Backup & Replication server.
	Backup repository server or gateway server*	TCP	2500 to 3300**	Default range of ports used as data transmission channels. For every TCP connection that a backup process uses, one port from this range is assigned.

* For NFS share, SMB share repositories, and Dell Data Domain, HPE StoreOnce deduplication storage appliances, Veeam Backup & Replication uses an auxiliary backup infrastructure component — gateway server. For details, see the Gateway Server section of the Veeam Backup & Replication User Guide.

** This range of ports applies to newly added backup infrastructure components. If you upgrade to Veeam Backup & Replication 10.0 from earlier versions of the product, the range of ports from 2500 to 5000 applies to the already added components.

Backup Repositories and Gateway Servers

Depending on the type of backup repositories that you use for Veeam Plug-in backups, the following ports must be open to allow communication between backup infrastructure components.

From	To	Protocol	Port	Notes
Veeam Backup & Replication server	Backup repository server or gateway server*	TCP	2500 to 3300**	Default range of ports used as data transmission channels. For every TCP connection that a backup process uses, one port from this range is assigned.
Direct Attached Storage				

From	To	Protocol	Port	Notes
Veeam Backup & Replication server	Linux server used as a backup repository or gateway server	TCP	22	Port used as a control channel from the Veeam Plug-in server to the target Linux host.
	Microsoft Windows server used as a backup repository or gateway server	TCP UDP	135, 137 to 139, 445	Ports used as a management channel from the Veeam Plug-in server to the Repository/Gateway server. Also, the ports are used to deploy Veeam components.
		TCP	6160, 6162	Default ports used by the Veeam Installer Service and Veeam Data Mover Service
Network Attached Storage				
Gateway server (specified in the SMB share repository settings)	SMB server	TCP	445	Default port used by the SMB transport protocol.
		TCP UDP	135, 137 to 139	SMB/Netbios name resolution for the SMB protocol (needed in some cases). For details, see the Used Ports section of the Veeam Backup & Replication User Guide.
Gateway server (specified in the NFS share repository settings)	NFS server	TCP UDP	111, 2049	Standard NFS ports used as a transmission channel from the gateway server to the target NFS share.
Dell Data Domain				
Veeam Backup & Replication server or **Gateway server**	Dell Data Domain For more information, see this Dell KB article.	TCP	111	Port used to assign a random port for the mountd service used by NFS and DDBOOST. Mountd service port can be statically assigned.
		TCP	2049	Main port used by NFS. To change the port, you can use the ‘`nfs set server-port`’ command. Note that the command requires SE mode.

From	To	Protocol	Port	Notes
		TCP	2052	Main port used by NFS MOUNTD. To change the port, you can use the `'nfs set mountd-port'` command. Note that the command requires SE mode.
HPE StoreOnce				
Veeam Backup & Replication server or **Gateway server**	HPE StoreOnce	TCP	9387	Default command port used for communication with HPE StoreOnce.
			9388	Default data port used for communication with HPE StoreOnce.
ExaGrid				
Veeam Backup & Replication server	ExaGrid	TCP	22	Default command port used for communication with ExaGrid.
Quantum DXi				
Veeam Backup & Replication server	Quantum DXi	TCP	22	Default command port used for communication with Quantum DXi.

For detailed list of ports used by Veeam Backup & Replication server and backup repositories, see the Used Ports section of the Veeam Backup & Replication User Guide.

Licensing

To use the Veeam Plug-in functionality, you must have a valid Veeam Backup & Replication license. Licenses are installed and managed on the Veeam Backup & Replication server that is connected to the Veeam Plug-in server. If the license is not valid or out of resources, Veeam Plug-in backup jobs fail.

This guide provides information only on specifics of Veeam licenses for Veeam Plug-ins. For terminology and general information about Veeam Licensing, see Veeam Licensing Policy.

See in this section:

- Licensed Objects
- Supported License Types and Packages
- Obtaining and Managing Licenses

Licensed Objects

An SAP on Oracle server is assumed protected if it has been processed by a Veeam Plug-in backup job in the last 31 days.

If you are using any instance-based (Veeam Universal Licensing) license on your Veeam Backup & Replication, you don't need to install any additional licenses. A protected SAP on Oracle server consumes one instance unit from the license. SAP on Oracle servers processed by backup copy jobs are not regarded as protected VMs, these types of jobs provide an additional protection level for VMs that are already protected with Veeam Plug-in backup jobs.

A machine protected by both Veeam Plug-in and Veeam Backup & Replication will consume a license only once. For example, you have an SAP on Oracle server that you back up using Veeam Plug-in. You also back up this server using image-level backup functionality of Veeam Backup & Replication. In this case, only one license will be consumed.

> NOTE
>
> [For Perpetual per-socket licenses] If you are using a legacy perpetual per-socket license, a license is required for each hypervisor CPU socket occupied by protected SAP on Oracle servers.
>
> A socket is consumed from the license only if the hypervisor where protected servers reside is added to the Veeam Backup & Replication infrastructure. If the hypervisor is not added to the Veeam Backup & Replication infrastructure, an instance unit will be consumed from the license. To learn how to add a hypervisor to the Veeam Backup & Replication infrastructure, see the Virtualization Servers and Hosts section of the Veeam Backup & Replication User Guide.

Supported License Types and Packages

You can use Veeam Plug-ins with the following license types and packages. Note that this guide contains information on specifics of Veeam license packages only for Veeam Plug-ins. For the full list of license packages, see Pricing and Packaging.

- **For Veeam Universal Licensing**:

  You can use Veeam Plug-ins with all license packages (*Veeam Backup Essentials, Veeam Backup & Replication, Veeam Availability Suite*).

  Note that if you use the *Rental* license type, functionality of Veeam Plug-ins is supported only for the *Enterprise Plus* edition of Veeam Backup & Replication.

- **For Perpetual Socket license**:

  Functionality of Veeam Plug-ins is supported only for the *Enterprise Plus* edition of Veeam Backup & Replication.

Obtaining and Managing Licenses

To learn how to install a license and monitor licensed objects, see the Licensing section in the Veeam Backup & Replication User Guide.

Environment Planning

Integration of SAP on Oracle and Veeam Plug-in requires additional environment planning. When you deploy the plug-in, keep in mind the following requirements and limitations.

Scheduling

You can schedule backup processes using `Cron`.

Also, you can schedule and run existing SAP BR*Tools backup scripts within image-level or file-level backup job of Veeam Backup & Replication or Veeam Agent. For details, see the Pre-Freeze and Post-Thaw Scripts section of the Veeam Backup & Replication.

Veeam Backup & Replication Users and Roles

Veeam Plug-in for SAP on Oracle uses the Windows authentication methods of the Veeam Backup & Replication server to establish a connection to this server and to the backup target.

If this user will be later changed manually, the new user must have at least the *Veeam Backup Operator* and *Veeam Restore Operator* rights within the Veeam Backup & Replication user management. To learn how to assign Veeam Backup & Replication roles, see the Users and Roles section of the Veeam Backup & Replication User Guide.

Parallel Data Streams and Backup Repository Task Slots

Any parallel data stream started by SAP Backint will use one backup repository task slot. It is recommended to carefully plan repository task slots, so that SAP Backint can work with multiple channels in parallel.

The following hardware resources are recommended based on tests on Skylake processors:

- **SAP on Oracle server**: 1 CPU core and 200 MB of RAM per currently used channel. Note that resource consumption on the SAP on Oracle server depends on hardware and Oracle settings.
- **Backup repository server**: 1 CPU core and 1 GB of RAM per 5 currently used channels.

  These resources are recommended only if you use a dedicated backup repository for Veeam Plug-in backups. If you use the same backup repository for Veeam Plug-in backups and VM backups created by Veeam Backup & Replication or Veeam Agents, consider adding the hardware resources based on usual load on your backup repository. For details on hardware requirements for a backup repository, see the System Requirements section of the Veeam Backup & Replication User Guide.

  It is recommended to contact your Veeam system engineer to optimize the channel settings and resource allocation.

  It is recommended to use a separate backup repository for Veeam Plug-in backups.
- **Veeam Backup & Replication server**: during manual metadata operations such as import of backup files, the Veeam Backup & Replication server needs additional 15 GB of RAM per 1 million files located in the same backup job folder.

Backup Files

Veeam Plug-in stores backup files in the following formats:

- A .VAB file stores a compressed copy of an Oracle database. Veeam Plug-in creates VAB files for both full and incremental backups.
- A .VASM file stores metadata that contain information about the backup. A .VASM file is created for each .VAB file. The .VASM files are used by Veeam Backup & Replication to get data about Veeam Plug-in backups.
- A .VACM file stores metadata of a backup job object.

Veeam Plug-in generates a name for the .VAB backup file and stores up to 1000 files in backup (FIBs) in one .VAB file. The FIB file names match the external backup IDs (EBID) generated by Veeam Plug-in during the backup.

Also, for each backup file, Veeam Plug-in creates a metadata file that has the same name as the backup file but a different extension (`.VASM`).

Veeam Backup Repositories

Veeam Plug-ins store backup files in repositories added to the Veeam Backup & Replication infrastructure. In this section, you can find the list of supported backup repositories and limitations for Veeam Plug-in backups.

Supported Backup Repositories

Veeam Plug-in for SAP HANA supports integration with the following types of repositories added to the Veeam Backup & Replication infrastructure:

- Windows Server
- Linux Server
- CIFS (SMB) Share
- Dell Data Domain Boost
- Quantum DXi
- ExaGrid
- HPE StoreOnce. If you plan to use HPE StoreOnce as a backup repository for Veeam Plug-in backups, the total number of stored files (data and metadata) must not exceed 3,000,000 per Catalyst store. If necessary, multiple Catalyst stores may be created on the same StoreOnce system.
- NFS File Share
- Hardened Repository

You can also use scale-out backup repositories that contain repositories supported by Veeam Backup & Replication.

Backup Repositories Limitations

- For Veeam Plug-in backups, the warning which indicates that free space on a storage device has reached a specified threshold is configured in the `veeam_config.xml` file of Veeam Plug-in. The warning settings in the Veeam Backup & Replication console does not affect this setting.

  To configure the warning settings, add the following parameter in the `veeam_config.xml` file.

  ```
  <PluginParameters repositoryFreeSpacePercentWarning="10" />
  ```

- The plug-in configuration wizard will not show repositories where the **Encrypt backups stored in this repository** option is enabled. To learn how to disable the encryption option, see Access and Encryption Settings on Repositories.

  If you want to use the same backup target with the repository-based encryption and Veeam Plug-ins, create a second repository in the subfolder for Veeam Plug-in backups.

- Veeam extract utility cannot extract Veeam Plug-in backup files.

Veeam Scale-Out Backup Repositories

If you want to store Veeam Plug-in backups on scale-out backup repositories, mind the following:

- If a scale-out repository is configured in the **Data locality** policy, each time BR*Tools starts a new channel for transferring backup files, Veeam Plug-in checks the free space in the extents and selects a scale-out backup repository extent that has the largest amount of free space. If there are two extents with one slot on each extent, the backup will be launched in two parallel streams (one on each extent).

- For Veeam Plug-in backups and backup copies, the *Performance* policy of a scale-out repository functions differently:

  a. Veeam Backup & Replication checks if there are extents without warning on free space insufficiency. If all extents have the warning, Veeam Backup & Replication uses an extent with the largest amount of free space that has a free task slot.

  b. If there are extents without the warning, Veeam Backup & Replication checks if there are incremental extents with free task slots. If there are no incremental extents with free task slots, Veeam Backup & Replication uses a full extent with the least amount of used task slots.

  c. If there are incremental extents with free task slots, Veeam Backup & Replication will send backup files to an incremental extent with the least amount of used task slots. If the amount of used tasks is the same, an extent with the largest amount of free space.

  To learn more about file placement policies of scale-out repositories, see Backup File Placement section of the Veeam Backup & Replication guide.

- If you want to add a backup repository as an extent to a scale-out backup repository and Veeam Plug-in backups are present on this backup repository, you must do the following:

  a. In the Veeam Backup & Replication console, select Veeam Plug-in backup files that reside in this backup repository and remove them from configuration. For details, see Removing backups from configuration. Note that this action does not delete the backups from the repository.

  b. In the Veeam Backup & Replication console, delete the Veeam Plug-in backup job. For details, see Deleting Jobs.

  c. Add the repository as an extent to the scale-out repository. For details, see Extending Scale-Out Repositories.

  d. Rescan the scale-out repository. For details, see Rescanning Scale-Out Repositories.

  > NOTE
  >
  > Names of backup files and paths to backup files must contain only allowed characters:
  >
  > - Alphanumeric characters: `a-zA-Z0-9`
  > - Special characters: `_-.+=@^`
  > - Names of backup files and paths to backup files must not contain spaces.

  e. On the Veeam Plug-in server, set the scale-out repository as the target for backups using the following command:

  ```
  SapBackintConfigTool --set-repositories
  ```

f. Map the imported backups using the following command:

```
SapBackintConfigTool --map-backup
```

Capacity Tier

You can configure Veeam Backup & Replication to transfer Veeam Plug-in backup files to a capacity tier. Both policies (Move policy, Copy policy) are supported for Veeam Plug-in backups with the following limitations:

- For Veeam Plug-in backup files, capacity tier does not verify whether data that is being moved is unique and has not been offloaded earlier. Thus, it is highly recommended to check the pricing plans of your cloud storage provider to avoid additional costs for offloading and downloading backup data.
- Capacity tier does not track dependencies of full and incremental Veeam Plug-in backup files. Thus, mind the following:
    - [For the Move policy] When backup files are transferred to the capacity tier, Veeam Backup & Replication takes into account only the creation time of backup files. Make sure that the operational restore window is not longer than the whole backup chain cycle period. Otherwise, you may encounter the scenario when full backup files are transferred to the capacity tier and their increment backup files still remain in the performance tier.
    - The capacity tier immutability expiration date does not have the additional block generation period. The immutability expiration date is based only on the number of days specified in settings of the object storage backup repository.
- If a scale-out repository is down, you cannot restore from Veeam Plug-in backup files stored on a capacity tier. In this case, you can only import the backup files manually and then perform data recovery operations.

Hardened Repository

You can configure Veeam Backup & Replication to transfer Veeam Plug-in backup files to a hardened repository. The hardened repository helps to protect Veeam Plug-in backup files from loss as a result of malware activity or unplanned actions. Backup files in the hardened repository become immutable for the time period specified in the backup repository settings. During this period, backup files stored in the repository cannot be modified or deleted.

For Veeam Plug-in for SAP HANA backups, immutability works according to the following rules:

- Immutability is applied to backup (VAB) files and backup metadata (VASM) files. Backup job metadata (VACM) files are not immutable.
- Backup files become immutable for the configured time period (minimum 7 days, maximum 9999 days).
- The count of the immutability period starts when the backup metadata (VASM files) has been created during the backup job session.
- The immutability period is not extended for the active backup chain.
- Every 1 hour, the immutability service that runs in the background detects backup files that do not have the immutability flag and sets the immutability flag on the necessary backup files.

Data Restore from Hardened Repository

As a result of malware activity or unplanned actions, backup job metadata (VACM) files may become unavailable in the hardened repository. In this case, to restore data from the hardened repository, you must re-create the VACM file. For more information, see Restore from Hardened Repository.

Access and Encryption Settings on Repositories

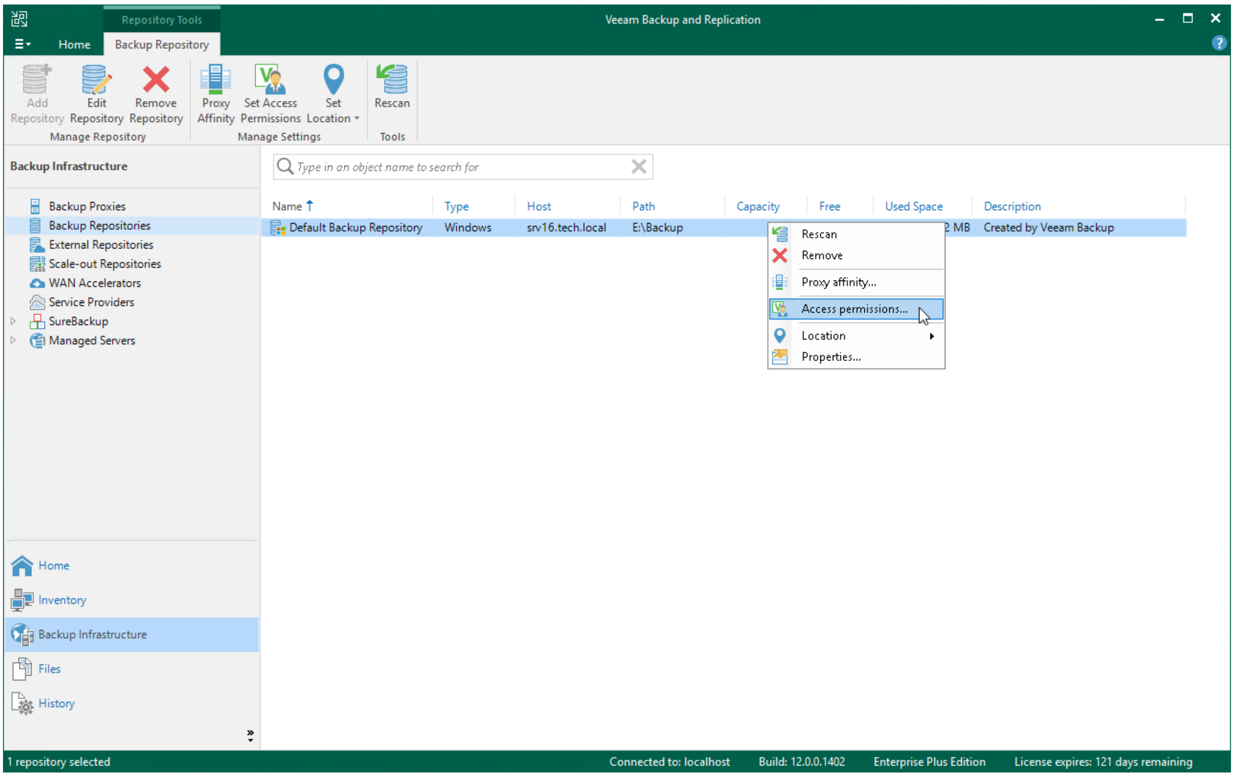
When you configure Veeam Plug-in, you specify an account that must be used to connect to the Veeam Backup & Replication server. To be able to store backups in a backup repository, the specified account must have access permissions on the target backup repository.

To grant access permissions, do the following:

1. In Veeam Backup & Replication, open the **Backup Infrastructure** view.

2. In the inventory pane, click the **Backup Repositories** node or the **Scale-out Repositories** node.

3. In the working area, select the necessary backup repository and click **Set Access Permissions** on the ribbon or right-click the backup repository and select **Access permissions**.



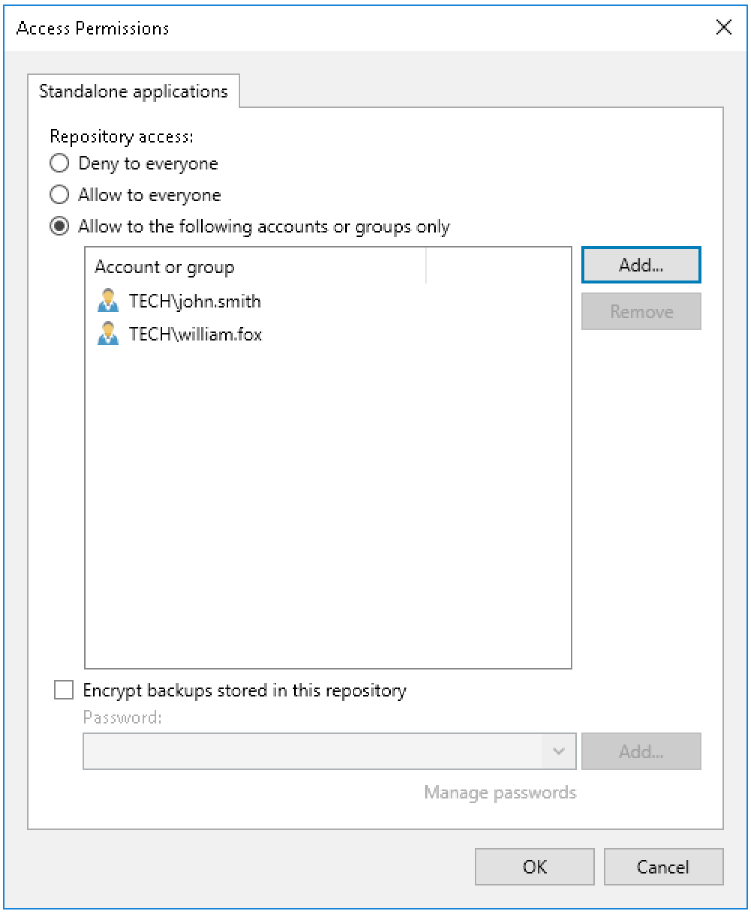
4. In the **Access Permissions** window, on the **Standalone applications** tab specify to whom you want to grant access permissions on this backup repository:

   - *Allow to everyone* — select this option if you want to grant repository access to any user. This option is equal to granting access rights to the *Everyone* group in Microsoft Windows (anonymous users are excluded). For security reasons, the option is not recommended for production environments.

   - *Allow to the following accounts or groups only* — select this option if you want only specific users to be able to store backups in this repository. Click **Add** to add the necessary users and groups to the list.

5. Veeam Plug-ins cannot send backups or backup copies to a backup repository where encryption is enabled. Thus, make sure that the **Encrypt backups stored in this repository** check box is not selected.

6. Click **OK**.



Access Permissions

Standalone applications

Repository access:

○ Deny to everyone

○ Allow to everyone

● Allow to the following accounts or groups only

Account or group
TECH\john.smith
TECH\william.fox

□ Encrypt backups stored in this repository

Password:

Deployment and Configuration

To deploy Veeam Plug-in, you must install the plug-in on a SAP on Oracle server and configure plug-in integration settings. In this section:

- Installing Veeam Plug-in for SAP on Oracle
- Configuring Veeam Plug-in for SAP on Oracle
- Configuring Parallelism for Redo Logs
- Importing Backups
- Uninstalling Veeam Plug-in for SAP on Oracle

This guide gives instructions on how to deploy Veeam Plug-in assuming that you have already deployed a Veeam Backup & Replication server and configured a backup repository. If you need instructions on how to deploy Veeam Backup & Replication, see the Veeam Backup & Replication User Guide for your platform.

Installing Veeam Plug-in for SAP on Oracle

Veeam Plug-in for SAP on Oracle is an additional component of Veeam Backup & Replication, and the installation package of the plug-in is included in the Veeam Backup & Replication installation ISO file. You must install the plug-in on the Oracle Database server.

You can install Veeam Plug-in using the `.RPM` package or extract the plug-in files from the `.TAR.GZ` archive. Depending on the type of package suitable for your OS, perform steps in one of the following guides:

- Installing Plug-in from .RPM Package
- Unpacking Plug-in from .TAR.GZ Archive

> **IMPORTANT**
>
> Mind the following:
>
> - Veeam Plug-in for SAP on Oracle must be installed on the machine where Oracle Database is deployed.
> - The `/opt/veeam` directory must be writable.
> - To install the Veeam Plug-in, use the `sudo` command or a user with root privileges.

Installing Plug-in from .RPM Package

To install Veeam Plug-in using the `.RPM` package, do the following:

1. Mount the Veeam Backup & Replication installation disk (`VeeamBackup&Replication_12.0.0.1420.iso`).

   If you deploy Veeam backup infrastructure for the first time, you can download the Veeam Backup & Replication installation disk image from the Veeam Backup & Replication: Download page.

2. Open the mounted disk image and go to `/Plugins/SAP on Oracle/x64` directory.

3. Upload the `VeeamPluginforSAPOracle-12.0.0.1420-1.x86_64.rpm` file to the Oracle Database server.

4. Run the following command to install the plug-in:

```
rpm -i VeeamPluginforSAPOracle-12.0.0.1420-1.x86_64.rpm
```

Unpacking Plug-in from .TAR.GZ Archive

To extract plug-in files from the `.TAR.GZ` archive, perform the following:

1. Mount the Veeam Backup & Replication installation disk (`VeeamBackup&Replication_12.0.0.1420.iso`).

   If you deploy Veeam backup infrastructure for the first time, you can download the Veeam Backup & Replication installation disk image from the Veeam Backup & Replication: Download page.

2. In the mounted ISO, go to `/Plugins/SAP on Oracle/x64`.

3. Upload the `VeeamPluginforSAPOracle.tar.gz` file to the Oracle Database server.

4. Create the `/opt/veeam` directory.

   ```
   mkdir /opt/veeam
   ```

5. Unpack the plug-in files from the archive to the `/opt/veeam` directory:

   ```
   tar -xzvf -i VeeamPluginforSAPOracle.tar.gz -C /opt/veeam
   ```

Configuring Plug-in for SAP on Oracle

When you configure Veeam Plug-in settings, you set up integration settings between the SAP on Oracle server, Veeam Backup & Replication server and backup repositories where backup files will be stored.

Veeam Plug-in uses the **SapOracleBackintConfigTool** wizard to configure the integration settings. The wizard searches for all SAP on Oracle systems deployed on the server and creates the `veeam_initSID.sap` file for each system. Then, this file is used as an initialization profile for `brbackup`, `brrestore` and `brarchive` tools.

Depending on which version of Oracle Database is used, Veeam Plug-in stores the configuration file in the following directories.

- For Oracle 12 and later, the configuration file is stored at `SAPDATA_HOME/sapprof`.
- For Oracle 11, the configuration file is stored at `ORACLE_HOME/dbs`.

> **IMPORTANT**
>
> In some cases when Oracle Database and SAP central instance are running on different hosts, Veeam Plug-in may not be able to detect SAP instances during the configuration. In this case, you must perform the following:
>
> 1. Complete all the steps of the Veeam Plug-in configuration wizard described in this section. As a result, Veeam Plug-in will create a new `veeam_initSID.sap` initialization profile and save it in the `/tmp/` directory.
> 2. Manually copy all lines from the new initialization profile to the default initialization profile. Or you can specify the path to the `veeam_initSID.sap` file in each BRBACKUP, BRRESTORE and BRARCHIVE command.

Veeam Plug-in Configuration

To configure Veeam Plug-in, do the following. Note that the configuration of Veeam Plug-in must be performed by a user with database administrator rights on the Oracle Database server:

1. Log in to the Oracle Database server as a user with database administrator rights and run the following command to launch the Veeam Plug-in configuration tool. You do not need root privileges if you have configured group access as described in the Required Permissions section.

   ```
   SapOracleBackintConfigTool --wizard
   ```

   If you have extracted files form the .TAR.GZ archive, go to the `/opt/veeam/VeeamPluginforSAPOracle` folder and run the following command:

   ```
   ./SapOracleBackintConfigTool --wizard
   ```

2. Specify the DNS name or IP address of the Veeam Backup & Replication server that you want to use.

   ```
   Enter backup server name or IP address: serv02.tech.local
   ```

3. Specify the port which will be used to communicate with the Veeam Backup & Replication server. Default port: *10006*.

   ```
   Enter backup server port number: 10006
   ```

4. Specify credentials to authenticate against the Veeam Backup & Replication server.

   ```
   Enter username: serv02\administrator
   Enter password for serv02\administrator:
   ```

   > IMPORTANT
   >
   > Mind the following:
   >
   > - You can work with backups created by Veeam Plug-in only with the account used for creating the backups. If you want to use another account, assign the *Veeam Backup Administrator* role or *Veeam Backup Operator* and *Veeam Restore Operator* roles to the account.
   >
   >   To learn how to assign Veeam Backup & Replication roles, see the Users and Roles section of the Veeam Backup & Replication Guide.
   > - The account must have access permissions on the required backup repository. To learn how to configure access permissions and encryption settings on repositories, see Access and Encryption Settings on Repositories.

5. Select a backup repository where you want to store backups.

   In the wizard dialog, you will see a list of available repositories. Enter the number of the target repository from the list.

   ```
   Available backup repositories:
   1. serv10_repo
   2. serv07_repo
   Enter repository number: 1
   ```

   > IMPORTANT
   >
   > Mind the following:
   >
   > - The account used to connect to the Veeam Backup & Replication server must have access to the target backup repositories.
   > - Encryption must be disabled on the target backup repositories.
   >
   > Otherwise, backup repositories will not be listed as available. To learn how to configure access and encryption settings on repositories, see Access and Encryption Settings on Repositories.

6. Specify the number of parallel data streams for each backup repository.

   ```
   Enter number of data streams (From 1 to 32) to run in parallel: 4
   Configuration result:
   An auxiliary initialization profile has been successfully created for SAP
   system "ODB": /oracle/ODB/sapprof/veeam_initODB.sap
   The created profile must be leveraged to perform backup and restore tasks
   by BR*Tools.
   ```

   Note that this parallelism setting applies only to backup and restore of Oracle datafiles. If you want to configure parallel channels for backup and restore of redo logs, see Configuring Parallelism for Redo Logs.

Configuration Tool Commands

Apart from running a configuration wizard, you can use the **SapOracleBackintConfigTool** tool to change a specific parameter in the `veeam_config.xml` file or enable/disable Veeam Plug-in features.

See the list of available commands for **SapOracleBackintConfigTool**:

Command	Description
--help	Shows the list of tool parameters.
--show-config	Shows configuration parameters.
--wizard	Starts the wizard to configure the plug-in settings. This wizard edits the `veeam_config.xml` file or creates a new one if the configuration file was removed from the `/opt/veeam/VeeamPluginforSAPOracle/` directory.
--set-credentials <"serv\username"> <password>	Specifies credentials to log in to the Veeam Backup & Replication server.
--set-host <hostname>	Specifies the IP address or hostname of the Veeam Backup & Replication server.
--set-port <port_number>	Specifies a port number that will be used to communicate with the Veeam Backup & Replication server.
--set-repositories	Launches a wizard to select a backup repository. A backup repository is selected from repositories which are available in the connected Veeam Backup & Replication instance.
--set-restore-server	[for System Copy] Specifies the backup that will be copied.

Command	Description
--set-parallelism <number_of_channels>	Define the number of parallel channels that must be used to transfer Oracle datafiles during the backup and restore operations. You can set up to 32 channels. Note that the parallelism for redo logs is configured separately. For details, see Configuring Parallelism for Redo Logs.
--map-backup	Maps the imported backup.
--set-force-delete	Deletes backup files after specified days.
--configure-restore-from-copy	Enables restore from backup copy. Note that if you enable restore from backup copy, you cannot back up databases with Veeam Plug-in. To revert changes, you must disable restore from backup copy. Note that when you launch the command, the wizard will ask you to reconfigure the catalog backup from backint to disk.
--promote-backup-copy-to-primary	Maps the imported backup copy to a regular Veeam Plug-in backup chain.

Example

The following example shows how to specify credentials that will be used to log in to the Veeam Backup & Replication server.

```
SapOracleBackintConfigTool --set-credentials "serv02\Administrator" "password"
```

Configuring Parallelism for Redo Logs

To configure backup or restore of redo logs through multiple channels, you can change the parallelism parameter in the veeam_config.xml file.

1. In the machine where Veeam Plug-in is installed, go to the /opt/veeam/VeeamPluginforSAPOracle/ directory and open the veeam_config.xml file with a text editor.

2. Set the necessary values for the parallelism values:

   ```
   <PluginParameters Parallelism="4" LogsParallelism="4" />
   ```

   where the LogsParallelism parameter value defines the number of parallel channels for backup and restore of redo logs.

   Note that the first Parallelism value configures the parallelism for backup and restore of Oracle datafiles. This setting is configured in the Veeam Plug-in configuration wizard.

Importing Backup Files

If the Veeam Backup & Replication server has failed and you have restored it in a new location, you can copy the backup files to a new repository and re-map the Veeam Plug-in backup files.

Limitations and Prerequisites

Mind the following limitations:

- If backup files are not imported according to instructions given in this section, Veeam Plug-in backup and restore operations may fail.
- The repository from which you plan to import backups must be added to the Veeam Backup & Replication infrastructure. Otherwise you will not be able to access backup files.
- If you are importing backup files from a scale-out backup repository, the names of backup files and paths to backup files must contain only allowed characters:
  - Alphanumeric characters: `a-zA-Z0-9`
  - Special characters: `_-.+=@^`
  - Names of backup files and paths to backup files must not contain spaces.

How to Import Veeam Plug-in Backup Files

To import Veeam Plug-in backup files, do the following:

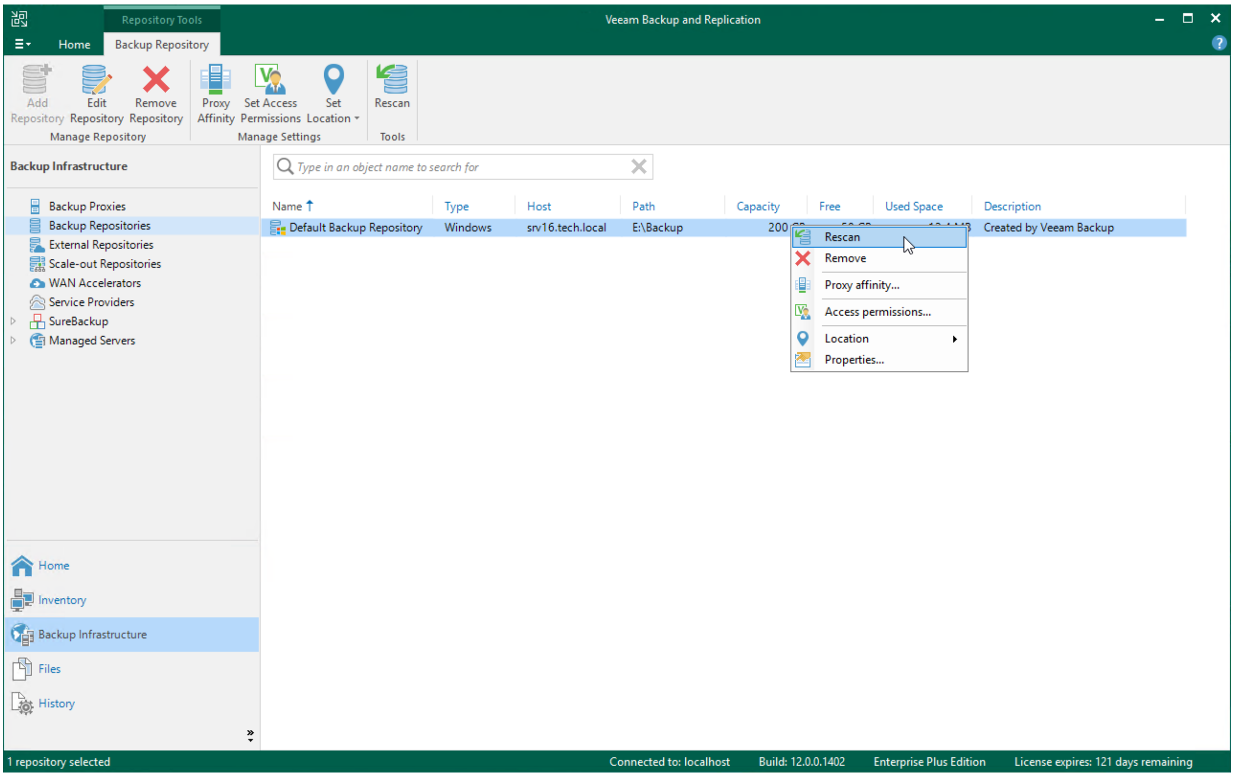
1. Move the folder with the backup file to the required backup repository or create a new backup repository with this folder as a subfolder.

   > **TIP**
   >
   > Each Veeam Plug-in backup file (.vab) has its own metadata file (.vasm). Make sure you import backup files and all related metadata files. Also, you must import the backup job metadata file (.vacm) which is stored in the same folder.

2. Use the Veeam Backup & Replication console to log in to Veeam Backup & Replication.
3. Open the **Backup Infrastructure** view.
4. In the inventory pane of the **Backup Infrastructure** view, select the **Backup Repositories** node.

5. In the working area, select the required backup repository and click **Rescan** on the ribbon. Alternatively, you can right-click the backup repository and select **Rescan**.

   During the rescan operation, Veeam Backup & Replication gathers information about backups that are currently available in the backup repository and updates the list of backups in the configuration database. After the rescan operation, backups that were not in this configuration database will be shown on the **Home** view in the **Backups > Disk (Imported)** node.



6. On the SAP on Oracle server, change the target backup repository in the Veeam Plug-in settings:

```
sudo SapOracleBackintConfigTool --set-repositories
Available backup repositories:
1. serv55.tech.local
2. serv07_repo
Enter repository number: 1
Configuration result:
SID SH2 has been configured
```

7. Run the `--map-backup` command:

```
sudo SapOracleBackintConfigTool --map-backup
```

Upgrading Veeam Plug-in for SAP on Oracle

Periodically, Veeam releases a new version of Veeam Backup & Replication that contains new features and bug fixes. The release package also contains a new version of Veeam Plug-ins.

If you want to upgrade Veeam Plug-in, note that Veeam Backup & Replication must be the same or later that the version of Veeam Plug-in. If you want to use the latest functionality, you must upgrade both Veeam Backup & Replication and to the latest version. After the upgrade, you don't need to to re-run the Veeam Plug-in configuration wizard, the plug-in configuration files will be preserved.

IMPORTANT

Mind the following:

- Version of Veeam Backup & Replication must be the same or later than the version of Veeam Plug-in. First, you must upgrade Veeam Backup & Replication, then you can upgrade Veeam Plug-ins. To learn how to upgrade Veeam Backup & Replication, see the Upgrading to Veeam Backup & Replication 12 section of the Veeam Backup & Replication User Guide.
- Operations in the terminal of the Linux machine require root privileges.

Before You Begin

Veeam Plug-in installation files are included in the installation disk image of Veeam Backup & Replication. You must upload the installation file to the SAP HANA server. To do this, perform the following steps.

1. Mount the Veeam Backup & Replication installation disk (`VeeamBackup&Replication_12.0.0.1420.iso`).
2. Open the mounted disk image and go to the `Plugins\SAP on Oracle\x64` directory.
3. Select the the Veeam Plug-in installation file and upload it to the SAP HANA server.

For instructions on how to upgrade Veeam Plug-in for SAP on Oracle, see the following guides:

- Upgrading Plug-in on Linux (RPM)
- Upgrading Plug-in on Linux (TAR.GZ)

Upgrading Plug-in on Linux (.RPM)

To upgrade Veeam Plug-in for SAP HANA from the `.RPM` package, perform the following:

1. Upload the new `VeeamPluginforSAPOracle-12.0.0.1420-1.x86_64.rpm` package to the SAP HANA server.
2. Run the following command. Note that the operation requires *root* privileges.

```
rpm -U VeeamPluginforSAPOracle-12.0.0.1420-1.x86_64.rpm
```

TIP

To find out which version of Veeam Plug-in is installed on your server, you can use the following command: `rpm -qa | grep VeeamPlugin*`

Upgrading Plug-in on Linux (.TAR.GZ)

To upgrade Veeam Plug-in for SAP on Oracle on a Linux machine from the `.TAR.GZ` archive, do the following:

1. Upload the `VeeamPluginforSAPOracle.tar.gz` file to the Oracle Database server.
2. In the terminal, open the folder that contains the `VeeamPluginforSAPOracle.TAR.GZ` archive.
3. Unpack the plug-in files from the archive to the `/opt/veeam` directory. Old Veeam Plug-in files will be replaced by new files.

   ```
   tar -xzvf VeeamPluginforSAPOracle.tar.gz -C /opt/veeam
   ```

Uninstalling Veeam Plug-in for SAP on Oracle

To uninstall Veeam Plug-in for SAP on Oracle, go to the directory with the Veeam Plug-in installation package and run the following command. Note that the operation requires *root* privileges.

```
rpm -e VeeamPluginforSAPOracle
```

Database Protection

After you configure Veeam Plug-in for SAP on Oracle, you can back up databases using SAP BR*Tools. Veeam Plug-in will automatically transfer backup files to a backup repository and store them in the Veeam proprietary format. The backup process itself is performed by SAP BR*Tools.

Keep in mind that examples in this section are provided only for demonstrating purposes. For details on full backup functionality of SAP BR*Tools, see the BR*Tools for Oracle DBA Guide.

In this section

> **NOTE**
>
> This guide provides examples for SAP BR*Tools commands. Apart from BR*Tools scripts, you can perform backup operations using BRTOOLS interactive wizard and BR*Tools Studio. For details, see the Backing Up the Databases with BR*Tools section of the SAP Database Guide: Oracle.

Limitations and Considerations

Before you start using Veeam Plug-in for SAP on Oracle, mind the following:

- You can make incremental backups only with the `rman_util` parameter. For details, see the RMAN Backup Strategies section of the SAP Database Guide: Oracle. To learn how to perform an incremental backup, see Incremental Backup.
- ASM is supported only with the `rman_util` parameter. If you want to back up ASM instances, see SAP on Oracle Backup Using RMAN_UTIL.
- You cannot back up Oracle RAC databases using the BRBACKUP tool.
- Volume backup (`-d util_vol`, `util_vol_online`) is not supported.
- Backup of directories is not supported.

SAP on Oracle Backup Using Backint

Veeam Plug-in for SAP on Oracle integrates with the BRBACKUP tool and transfers backup files to backup repositories connected to Veeam Backup & Replication. The backup process itself is performed by the BRBACKUP tool. To perform the backup you can use BR*TOOLS or BR*TOOLS Studio.

For details on how the backup is performed, see How Veeam Plug-in for SAP on Oracle Works.

To back up Oracle databases, you can use the interactive wizard of BRTOOLS or you can directly run the backup command using BRBACKUP. When you back up the database using the BRBACKUP tool, you must specify the path to the initialization profile file (`$Oracle_HOME/dbs/veeam_initSID.sap`) as the argument for the `-p` (`-profile`) parameter.

> **NOTE**
>
> You can make incremental backups only with the `rman_util` parameter. For details, see the RMAN Backup Strategies section of the SAP Database Guide: Oracle. To learn how to perform an incremental backup, see Incremental Backup.

Examples

The following examples are only for demonstration purposes. To see the description of all BRBACKUP parameters, see the Backing Up the Database with BR*Tools for Oracle DBA Guide.

- Full Backup
- Redo Logs Backup

Full Backup

If you want to create a full backup Oracle databases, you can use the BRBACKUP tool. When Veeam Plug-in for SAP on Oracle is configured, the plug-in transfers database backup files to a backup repository connected to Veeam Backup & Replication.

Example 1. Performing Full Database Backup in Offline Mode

```
brbackup -p $Oracle_HOME/dbs/veeam_initSID.sap -d util_file -t offline_force -m
all -u <user>/<password>
```

Run the `brbackup` command with the following parameters:

1. Specify the path to the initialization profile file (`$Oracle_HOME/dbs/veeam_initSID.sap`) as the argument for the `-p` (`-profile`) parameter.
2. Specify `util_file` as the argument for the `-d` (`-device`) parameter. This option defines that a file-by-file backup will be performed using Veeam Plug-in.
3. Specify `offline_force` as the argument for the `-t` (`-type`) parameter. With this option, BRBACKUP shuts down the database and performs an offline backup.

4. Specify the argument for the `-m` (`-mode`) parameter. With the `all` argument, BRBACKUP performs backup of files in all tablespaces, but not the control files and online redo log files. For the full list of arguments for the `-mode` parameter, see SAP Documentation.
5. Specify credentials that will be used to connect to the database as the argument for the `-u (-user)` parameter. For details, see SAP Documentation.

Example 2. Performing Full Database Backup in Online Mode

```
brbackup -p $Oracle_HOME/dbs/veeam_initSID.sap -d util_file_online -t online -m
all -u <user>/<password>
```

Run the `brbackup` command with the following parameters:

1. Specify the path to the initialization profile file (`$Oracle_HOME/dbs/veeam_initSID.sap`) as the argument for the `-p` (`-profile`) parameter.
2. Specify `util_file_online` as the argument for the `-d` (`-device`) parameter.
3. Specify the argument for the `-m` (`-mode`) parameter. With the `all` argument, BRBACKUP performs backup of files in all tablespaces, but not the control files and online redo log files. For the full list of arguments for the `-mode` parameter, see SAP Documentation.
4. Specify credentials that will be used to connect to the database as the argument for the `-u (-user)` parameter. For details, see SAP Documentation.

IMPORTANT

When you use BRBACKUP, you must specify the full directory path to the Veeam Plug-in initialization profile file (`-p $Oracle_HOME/dbs/veeam_initSID.sap)`. If the profile file is in the default directory, you can specify only the file name.

Redo Logs Backup

If you want to back up redo log files of Oracle databases, you can use the BRARCHIVE tool. When Veeam Plug-in for SAP on Oracle is configured, the plug-in transfers the redo logs to a backup repository connected to Veeam Backup & Replication.

NOTE

For redo log backup operations, it is recommended to set 4 or less parallel channels. For details on configuring parallel channels, see Configuring Parallelism.

Example: Performing Backup of Archived Redo Logs

To back up redo log files, run the following command.

```
brarchive -p $Oracle_HOME/dbs/veeam_initSID.sap -save -d util_file -u <user>/<p
assword>
```

1. Specify the path to the initialization profile file (`$Oracle_HOME/dbs/veeam_initSID.sap`) as the argument for the `-p` (`-profile`) parameter.
2. Specify the archive function. The `-save` function used in this example archives offline redo log files to a repository.
3. Specify `util_file` as the argument for the `-d` (`-device`) parameter. This option defines that a file-by-file backup will be performed using Veeam Plug-in.
4. Specify credentials that will be used to connect to the database as the argument for the `-u (-user)` parameter. For details, see SAP Documentation.

SAP on Oracle Backup Using RMAN_UTIL

The `rman_util` parameter allows to back up Oracle databases using Oracle RMAN in combination with Veeam Plug-in for Oracle RMAN. BACKINT provides an interface for Veeam Plug-in for Oracle RMAN and is used to back up profiles, log files, control files and to perform incremental backups of databases.

For full description of the `rman_util` parameter, see RMAN Backup with an External Backup Library.

In the Veeam Backup & Replication console, the `rman_util` backup operation will create two backup jobs: Veeam Plug-in for Oracle RMAN backup job for database file backups and another Veeam Plug-in for SAP on Oracle backup job that backups up BR*Tools control data files. Note that if you want to create a backup copy job for SAP on Oracle database, make sure that you have added both jobs to the backup copy job.

Prerequisites

> IMPORTANT
>
> - Before you back up the Oracle database with the rman_util parameter, you must install and configure Veeam Plug-in for Oracle RMAN on the SAP on Oracle server.
> - See Limitations and Considerations.

When you perform the backup using the RMAN_UTIL, RMAN_STAGE or RMAN_DISK parameter, by default, BR*Tools creates one backup set for each log or datafile. This means that every backup piece will contain only one file. This results in a large amount of backup files and significantly slows down backup and restore processes. To avoid this problem, do the following:

1. In the SAP on Oracle server, open the `/oracle/ODB/sapprof/veeam_initSID.sap` file using a text editor.
2. Change the default values for the following parameters:

```
rman_filesperset = 10
rman_filesperset_arch = 100
```

   For example: set the `rman_filesperset` value to 10 for datafiles and the `rman_filesperset_arch` value to 100 for logs.

Also, you must add the SBT_LIBRARY directory to the `rman_parms` setting in the `veeam_initSID.sap` file:

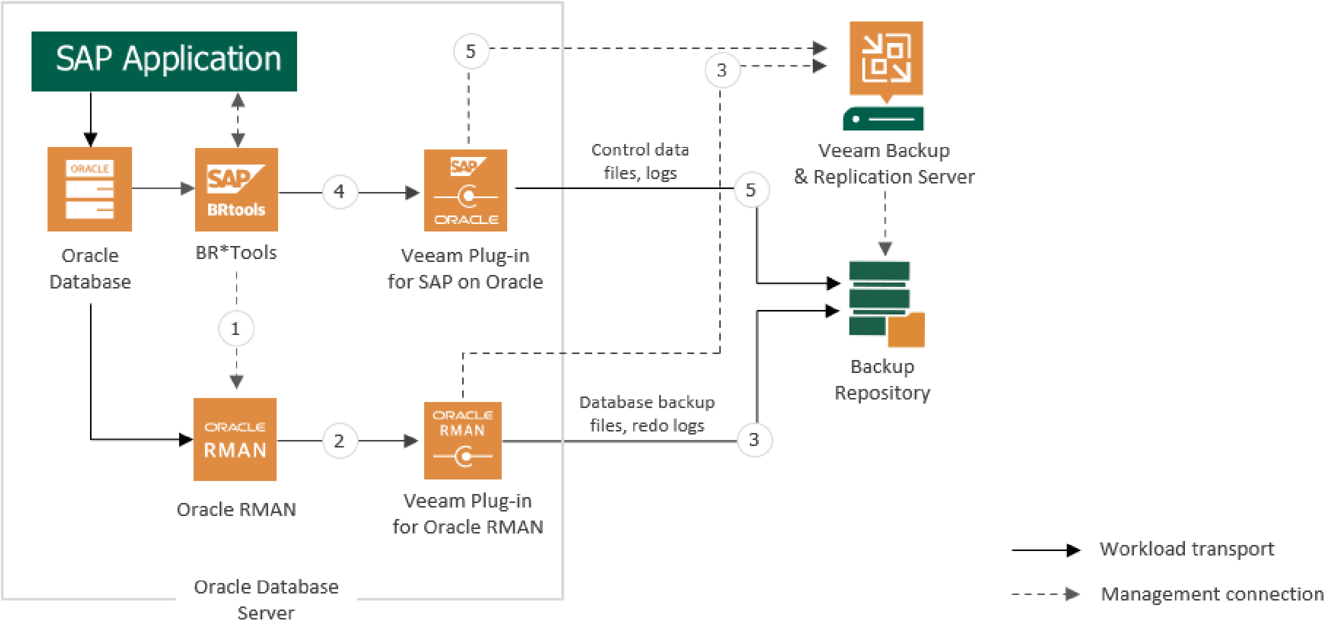
1. In the SAP on Oracle server, open the `/oracle/ODB/sapprof/veeam_initSID.sap` file using a text editor.
2. Add the following line in the `veeam_initSID.sap` file:

```
rman_parms = 'SBT_LIBRARY=/opt/veeam/VeeamPluginforOracleRMAN/libOracleRMA
NPlugin.so'
```

How It Works

When you launch the BRBACKUP or BRARCHIVE tool with the RMAN_UTIL parameter, the following happens:

1. SAP BR*Tools launches the RMAN backup script.
2. Oracle RMAN launches Veeam Plug-in for Oracle RMAN services.
3. Oracle RMAN starts the backup process:
   a. Veeam Plug-in compresses, deduplicates database backup files or redo logs and sends them to the target backup repository through one or multiple channels.
   b. Veeam Plug-in for Oracle RMAN connects to Veeam Backup & Replication and creates a backup job object that shows the job progress and logs.
4. BR*Tools launches the Veeam Plug-in for SAP on Oracle services.
5. BR*Tools start the control data files backup:
   a. Control file, BR*Tools logs are compressed and sent to a backup repository.
   b. Veeam Plug-in for SAP on Oracle connects to Veeam Backup & Replication and creates a backup job object that shows the job progress and logs.



Full Backup

To backup an SAP on Oracle database using RMAN, you must use the `brbackup` tool with the `rman_util` parameter and with the defined directory for SBT library.

```
brbackup -p $Oracle_HOME/dbs/veeam_initSID.sap -t online -d rman_util -m full -
u <user>/<password>
```

1. Specify the path to the initialization profile file (`veeam_initSID.sap`) as the argument for the `-p` (`-profile`) parameter.
2. Specify `rman_util` as the argument for the `-d` (`-device`) parameter. This option defines that the backup will be performed using Oracle RMAN.
3. Specify `online` as the argument for the `-t` (`-type`) parameter. With this option, BRBACKUP performs backup of the database in the online state.
4. Specify `full` as the argument for the `-m` (`-mode`) parameter. With this option, BRBACKUP performs backup of files in all tablespaces, control files and redo log files.
5. Specify credentials that will be used to connect to the database as the argument for the `-u (-user)` parameter. For details, see SAP Documentation.

For the fill list of BRBACKUP parameters, see the Command Options for BRBACKUP section of the SAP Database Guide: Oracle.

Incremental Backup

You can perform an incremental backup by using the BRBACKUP command with the `rman_util` parameter. An incremental backup contains the changed data from the last full backup. Incremental backups use less media and resources than full backups.

Example: Performing Incremental Backup in Online Mode

```
brbackup -p $Oracle_HOME/dbs/veeam_initSID.sap -t online -d rman_util -m incr -
u <user>/<password>
```

Run the `brbackup` command with the following parameters:

1. Specify the path to the initialization profile file (`$Oracle_HOME/dbs/veeam_initSID.sap`) as the argument for the `-p` (`-profile`) parameter.
2. Specify `online_force` as the argument for the `-t` (`-type`) parameter. With this option, BRBACKUP performs backup of the database in the online state.
3. Specify `util_file` as the argument for the `-d` (`-device`) parameter.
4. Set `incr` as the argument for the `-m` (`-mode`) parameter.
5. Specify credentials that will be used to connect to the database as the argument for the `-u (-user)` parameter. For details, see SAP Documentation.

To see all brbackup command options, see the Command Options for BRBACKUP section of the SAP Database Guide: Oracle.

Backup Job in Veeam Backup & Replication

After you start a backup process with BRBACKUP, Veeam Backup & Replication creates a backup job object. You can use this job to view the statistics on the backup process, generate backup job reports or you can also disable the backup job.

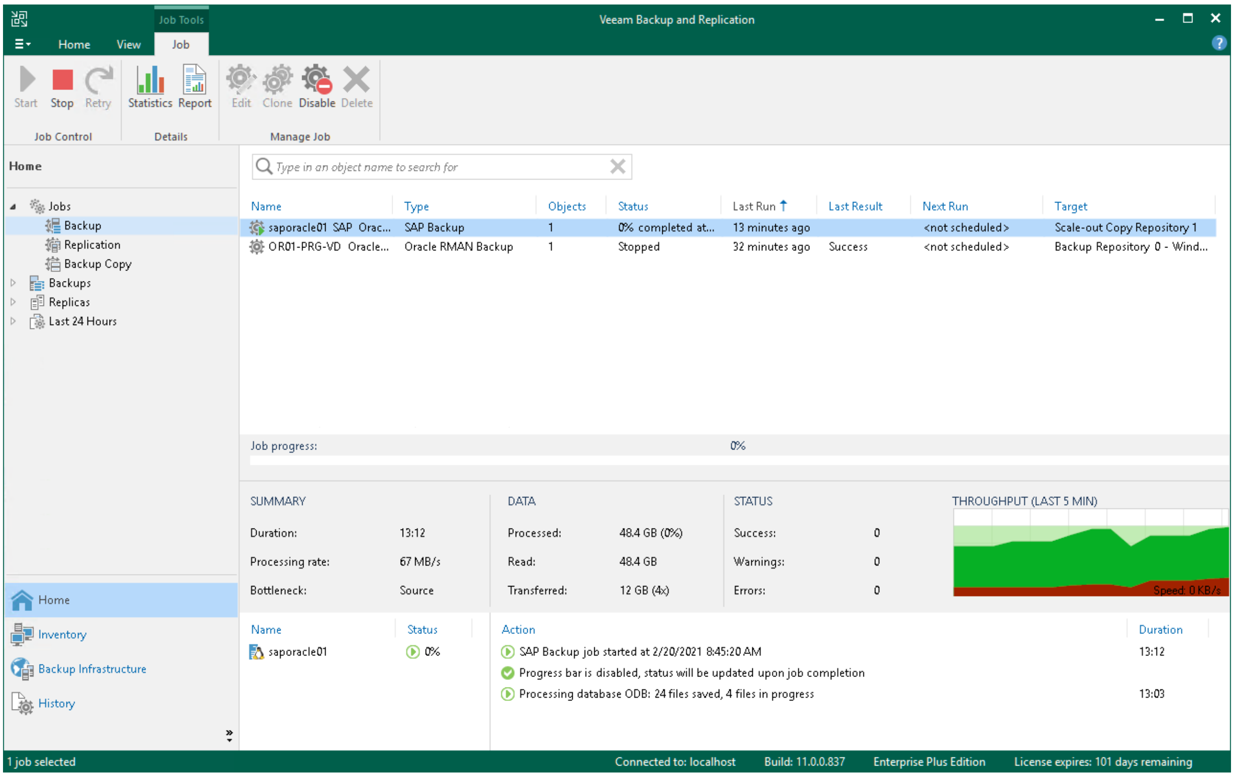
You cannot launch or edit SAP on Oracle backup job objects in the Veeam Backup & Replication console. You can manage backup operations only on the SAP on Oracle side using BR*Tools.

Mind that Veeam Backup & Replication generates the backup job name based on names of the SAP on Oracle server and selected repository.

> **NOTE**
>
> Due to specifics of the SAP on Oracle backup process, the progress bar of a running SAP on Oracle backup job is not available.

To view details of a backup job process, do the following.

1. Open the Veeam Backup & Replication console.
2. In the **Home** view, expand the **Jobs** node and click **Backup**.
3. In the list of jobs, select the BR*Tools backup job to see details of the current backup process or the last backup job session.



Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target
saporacle01 SAP Orac...	SAP Backup	1	0% completed at...	13 minutes ago		<not scheduled>	Scale-out Copy Repository 1
OR01-PRG-VD Oracle...	Oracle RMAN Backup	1	Stopped	32 minutes ago	Success	<not scheduled>	Backup Repository 0 - Wind...

Job progress: 0%

SUMMARY		DATA		STATUS	
Duration:	13:12	Processed:	48.4 GB (0%)	Success:	0
Processing rate:	67 MB/s	Read:	48.4 GB	Warnings:	0
Bottleneck:	Source	Transferred:	12 GB (4x)	Errors:	0

Name	Status
saporacle01	0%

Action	Duration
SAP Backup job started at 2/20/2021 8:45:20 AM	13:12
Progress bar is disabled, status will be updated upon job completion	
Processing database ODB: 24 files saved, 4 files in progress	13:03

1 job selected | Connected to: localhost | Build: 11.0.0.837 | Enterprise Plus Edition | License expires: 101 days remaining

Generating Backup Job Reports

Veeam Backup & Replication can generate reports with details about an BR*Tools backup job session performance. The session report contains the following session statistics: session duration details, details of the session performance, amount of read, processed and transferred data, backup size, compression ratio, list of warnings and errors (if any).

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the necessary job and click **Report** on the ribbon. You can also right-click the job and select **Report**.

Disabling Backup Job

You can disable BR*Tools backup jobs in the Veeam Backup & Replication console. If you disable the job, you will not be able to run BR*Tools backup commands on the SAP on Oracle server.

To disable a backup job:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the necessary job and click **Disable** on the ribbon. You can also right-click the job and select **Disable**.

Database Recovery

With the configured Veeam Plug-in you can restore Oracle databases from the backups that reside on backup repositories. All restore operations are performed on the SAP BR*Tools side.

Keep in mind that examples provided in this section are for demonstration purposes only. To see the full restore functionality of SAP BR*Tools, see the BR*Tools for Oracle DBA Guide.

To learn how to recover Oracle databases from backups created by Veeam Plug-in for SAP on Oracle, see:

- Restoring Oracle Databases
- Restoring Redo Logs
- Recovering Databases to Other Servers (System Copy)
- Restore from Backup Copy
- Restore from Hardened Repository

Oracle Databases Restore

Veeam Plug-in for SAP on Oracle allows to restore databases using the BRRESTORE tool functionality. When you launch the restore, BRRESTORE restores the selected database from backup files stored on the backup repository.

By default, BRRESTORE uses the `initSID.sap` initialization profile. Thus, you must specify the `-p $Oracle_HOME/dbs/veeam_initSID.sap` parameter in the restore commands.

For details on all restore options, see the Command Options for BRRESTORE section of the SAP DATABASE Guide: Oracle.

Example: Performing Full Restore of SAP on Oracle Database

```
brrestore -d util_file -p $Oracle_HOME/dbs/veeam_initSID.sap -b last -m full
```

Run the `brrestore` command with the following parameters:

1. Depending on which backup you want to restore from, use the `util_file` or `rman_util` option as the argument for the `-d` (`-device`) parameter. If the backup was created by Backint, use `util_file`. If the backup was created by RMAN, use `rman_util`.
2. Specify the path to the initialization profile file (`$Oracle_HOME/dbs/veeam_initSID.sap`) as the argument for the `-p` (`-profile`) parameter.
3. Specify `last` as the argument for the `-b` (`-backup`) parameter. With this option, BRRESTORE uses the last successful database backup for the restore.
4. Specify `full` as the argument for the `-m` (`-mode`) parameter. With this option, BRRESTORE performs restore of files in all tablespaces, control files and redo log files.

Redo Logs Restore

If you want to restore redo log files that were backed up with BRARCHIVE, you can use the BRRESTORE tool. For details, see the Names of BRRESTORE Details Logs section of the SAP Database Guide: Oracle.

Example: Performing Restore of SAP on Oracle Redo Logs

```
brrestore -d util_file -p $Oracle_HOME/dbs/veeam_initSID.sap -a 1-100
```

Run the `brrestore` command with the following parameters:

1. Depending on which backup you want to restore from, use the `util_file` or `rman_util` option as the argument for the `-d` (`-device`) parameter. If the backup was created by Backint, use `util_file`. If the backup was created by RMAN, use `rman_util`.

2. Specify the path to the initialization profile file (`$Oracle_HOME/dbs/veeam_initSID.sap`) as the argument for the `-p` (`-profile`) parameter.

3. Specify the log sequence number interval as the argument for the `-a` (`-archive`) parameter. This option defines which log files must be restored.

Database Restore to Another Server (System Copy)

You can restore SAP on Oracle databases from Veeam Plug-in backups to another server. To restore databases to another server, you must reconfigure settings of Veeam Plug-in as shown below.

For security reasons, you can restore databases to another server only in the following condition. The account you use to connect to Veeam Backup & Replication server must be the same account that performed the backup of the source system. If you want to use another account, you can assign the **Veeam Backup Administrator** or **Veeam Restore Operator** roles to the required account. For details on assigning Veeam Backup & Replication roles, see the Users and Roles section of the Veeam Backup & Replication User Guide.

Procedure

To restore databases to another server, you must reconfigure settings of Veeam Plug-in as shown below:

1. Go to `/opt/veeam/VeeamPluginforSAPOracle` and run the following command to select the source server whose backups you want to use during restore.

   ```
   VM2ADM:/opt/veeam/VeeamPluginforSAPOracle> SapOracleBackintConfigTool --set-restore-server
   ```

2. Select the required SAP on Oracle server.

   ```
   Select source SAP on Oracle server to be used as a restore target:
   0. To disable this functionality.
   1. saporacle01
   Enter server number: 1
   ```

3. Specify a backup repository where the required backup files are stored.

   ```
   Available backup repositories:
   1. win_repo02
   2. main_repo
   Enter server number: 2
   ```

   NOTE

   - The account used to connect to Veeam Backup & Replication server must have access permissions on the required repository. Otherwise the repository will not be displayed in the list of available repositories. To learn how to configure access permissions on repositories, see Setting Up User Permissions on Backup Repositories.
   - The wizard does not import existing backups from the repository. To perform a System Copy restore from the imported backup, you must map the backup. For details, see Importing Backups.

4. Perform the restore to another server.

5. After the restore, you must revert back the restore-server option of the Veeam Plug-in configuration wizard. Otherwise, you will not be able to restore data from the actual server backup file. If you perform only restore to other server, leave this setting enabled. It will not affect the backups of the actual system.

   To disable the functionality, run the `--set-restore-server` command and enter *0*.

   ```
   SapOracleBackintConfigTool --set-restore-server
   Select source SAP on Oracle server to be used as a restore target:
   0. To disable this functionality.
   1. saporacle01
   Enter server number: 0
   ```

Restore from Backup Copy

You can restore Oracle databases from backups and backup copies. To restore from backup copies, you must enable the restore from backup copy option in the Veeam Plug-in wizard.

> **IMPORTANT**
>
> If the restore from backup copy option is enabled, you cannot back up databases using Veeam Plug-in, and you cannot restore from backups created by primary Veeam Plug-in backup jobs. You can restore only from backup copy files until you disable the restore from backup copy option.

For instruction on how to enable/disable the restore from backup copy option, see the following guides:

- Enabling Restore from Backup Copy
- Disabling Restore from Backup Copy

Enabling Restore from Backup Copy

To be able to restore from backup copies, do the following:

1. In the machine where Veeam Plug-in is installed, open the terminal and run the following command:

   ```
   SapOracleBackintConfigTool --configure-restore-from-copy
   ```

2. Select the number of the backup copy job you want to use:

   ```
   Select secondary job for failover:
   0. Disable
   1. Plug-ins backup copy job\linuxq01 SAP Oracle backup <serv10_repo>
   Select secondary job for failover:1
   ```

   > **IMPORTANT**
   >
   > The account used to connect to the Veeam Backup & Replication server must have access permissions on the required repository.

Disabling Restore from Backup Copy

To be able to back up with Veeam Plug-in and restore from backups, disable the restore from backup copies (set the parameter back to **0**):

```
SapOracleBackintConfigTool --configure-restore-from-copy
Select secondary job for failover:
0. Disable
1. Plug-ins backup copy job\linuxq01 SAP Oracle backup <serv10_repo>
Select secondary job for failover:0
```

Restore from Hardened Repository

As a result of malware activity or unplanned actions, backup job metadata (VACM) files may become unavailable in the hardened repository. In this case, to restore data from the hardened repository, you must re-create the VACM file. To do this, complete the following steps:

1. Run a Veeam Plug-in backup job to create a new Veeam Plug-in backup in a Veeam backup repository. The backup will consist of the VAB, VASM and VACM files.
2. In the backup repository folder, replace the VAB and VASM files created at the step 1 with the VAB and VASM files from the hardened repository.
3. In the Veeam backup console, run the backup repair operation. Veeam Backup & Replication will generate a new VACM file using information from the VASM files. For details, see Repairing Backup.

Once the backup job metadata file is re-created, you can use Veeam Plug-in to restore your data.

Repairing Backup

If you want to restore data from an immutable backup that resides in a hardened repository, you can use the **Repair** operation. During this operation, Veeam Backup & Replication will generate a new backup job metadata (VACM) file using information from the backup metadata (VASM) files.

> **IMPORTANT**
>
> This operation is intended only for a situation where the backup job metadata file has been lost as a result of malware activity or unplanned actions. Re-creation of the backup job metadata file for other purposes is not supported.

Before you start the repair operation, you must disable the backup job that created the backup. Otherwise, Veeam Backup & Replication will display a message notifying that the job must be disabled.

To repair a backup:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. In the inventory pane, select **Backups**.
3. In the working area, select the necessary backup.
4. Press and hold the **[CTRL]** key, right-click the backup and select **Repair**.

Retention of SAP on Oracle Backups

To set an automatic removal of old backups, you can use the retention policy of Veeam Plug-in for SAP on Oracle. The `--set-force-delete` command of Veeam Plug-in automatically deletes backup files which are older than specified number of days. For details, see Configuring Retention Policy for Backups.

Also, you can manually delete backups from a backup repository using the Veeam Backup & Replication console and. For details, see Deleting Backups Manually Using Veeam Backup & Replication Console.

Configuring Retention Policy for Backups

Veeam Plug-in for SAP on Oracle has a functionality that automatically deletes backup files which are older than specified number of days. For example, you can use it if a backup repository contains backup files that are no longer in the backup catalog.

1. To enable automatic deletion of backup files, run the following command.

```
SapOracleBackintConfigTool --set-force-delete
```

2. Enter the number of days after which Veeam Plug-in will delete backup files on all configured backup repositories.

```
Garbage collector automatically deletes backup files older than the specif
ied number of days.
Make sure the number of days value exceeds your retention policy.
To disable this functionality, set the number of days to 0.
Enter the number of days to delete backups after, between 7 and 999 [0]:
```

By default, the force delete functionality is disabled (set to *0*).

IMPORTANT

A value for the **number of days** setting must be at least 1 backup generation period longer than the retention period for your Oracle Database backups. Otherwise, Veeam Plug-in will delete earliest backups created within the retention period.

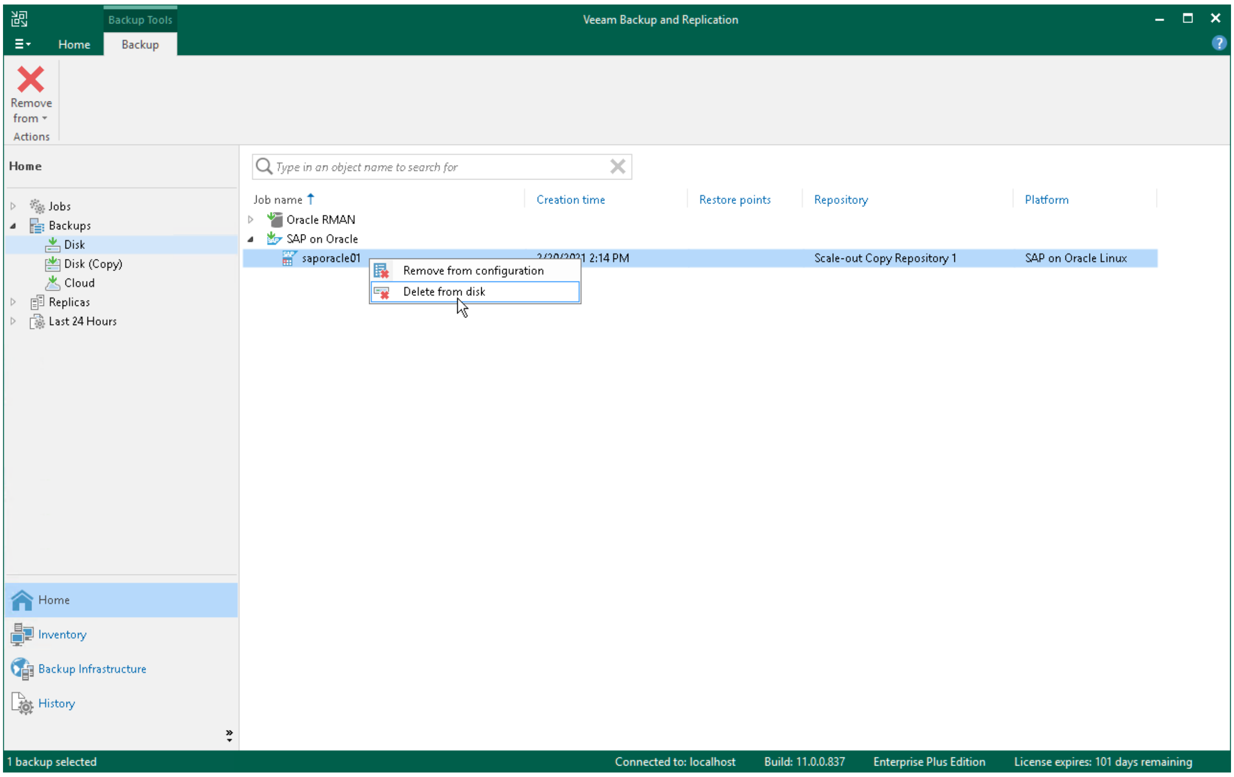
Deleting Backups Manually

Apart from configuring the retention policy, you can delete backups manually from backup repositories using the Veeam Backup & Replication console.

> NOTE
>
> If you remove backups from a backup repository manually, the backup catalog will not be updated.

To remove a backup from a backup repository, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. In the **Inventory** pane, select **Backups**.
3. In the working area, right-click the backup job object name and select **Delete from disk**.



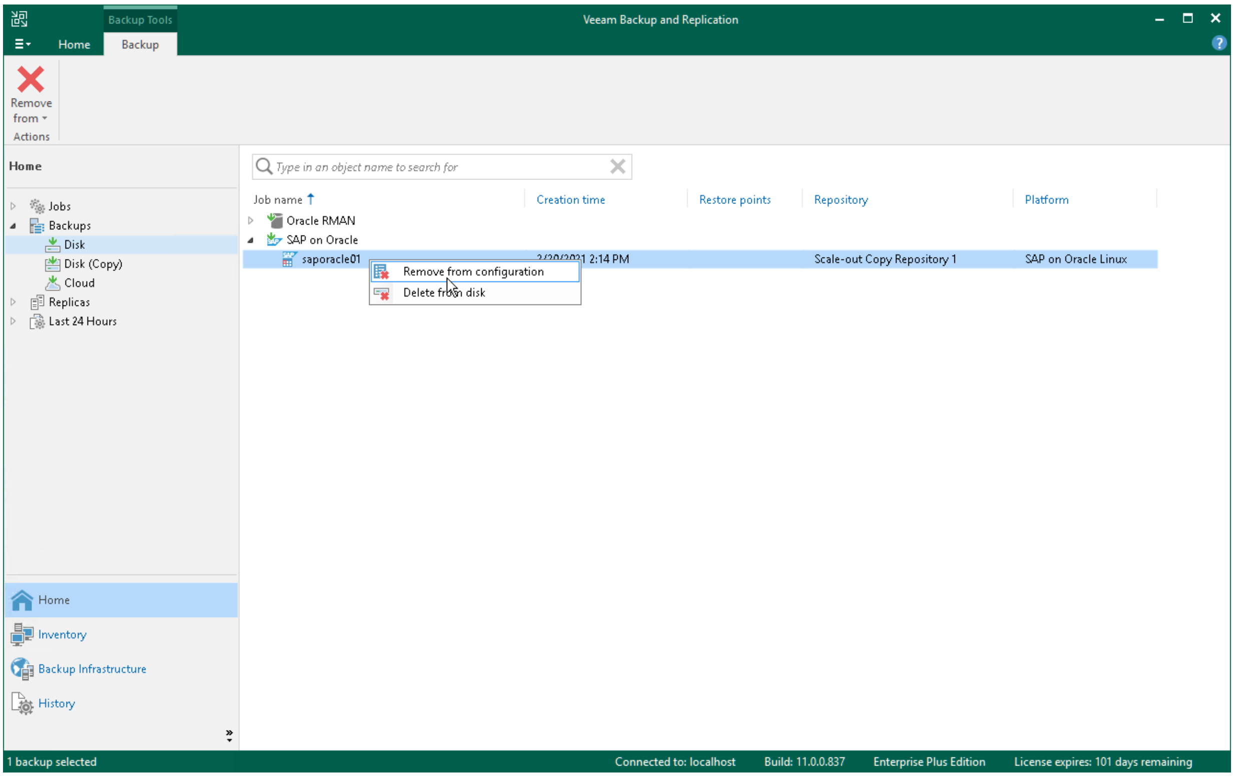
Removing Backups from Configuration

If you want to remove records about backups from the Veeam Backup & Replication console and configuration database, you can use the **Remove from configuration** operation.

When you remove a backup from the configuration, backup files (VAB, VASM) remain on the backup repository. You can import backup files later and restore from them.

To remove a backup from configuration:

1. Open the **Home** view.
2. In the inventory pane, select **Backups**.
3. In the working area, select the necessary backup.
4. Press and hold the **[CTRL]** key, right-click the backup and select **Remove from configuration**.



Backup Copy for SAP on Oracle Backups

Having just one backup does not provide the necessary level of safety. The primary backup may get destroyed together with production data, and you will have no backups from which you can restore data.

To build a successful data protection and disaster recovery plan, it is recommended that you follow the 3-2-1 rule:

- 3: You must have at least three copies of your data: the original production data and two backups.
- 2: You must use at least two different types of media to store the copies of your data, for example, local disk and cloud.
- 1: You must keep at least one backup offsite, for example, in the cloud or in a remote site.

Thus, you must have at least two backups and they must be in different locations. If a disaster takes out your production data and local backup, you can still recover from your offsite backup.

Creating Backup Copy Job

Veeam Backup & Replication offers the backup copy functionality that allows you to create several instances of the same backup in different locations, whether onsite or offsite. Backup copies have the same format as those created by backup jobs and you can recover your data from them when you need it.

Veeam Backup & Replication fully automates the backup copy process and lets you specify retention settings to maintain the desired number of restore points, as well as full backups for archival purposes. Backup copy is a job-driven process. When enabled, the backup copy job for Veeam Plug-in backups runs continuously. For more details on how it works, see the Backup Copy section of the Veeam Backup & Replication User Guide.

To copy backups to a secondary location, you must configure a backup copy job. The backup copy job defines how, where and when to copy backups. One job can be used to process backups of one or more machines.

You can configure a job and start it immediately or save the job to start it later.

Before creating a job, check prerequisites. Then use the **New Backup Copy Job** wizard to configure a backup copy job.

1. Launch Backup Copy Job wizard.
2. Specify a job name and description.
3. Selects backups to process.
4. Define backup copy target.
5. Specify advanced settings.
6. Define backup copy schedule.
7. Finish working with the wizard.

Before You Begin

Before you create a backup copy job, check the prerequisites and limitations:

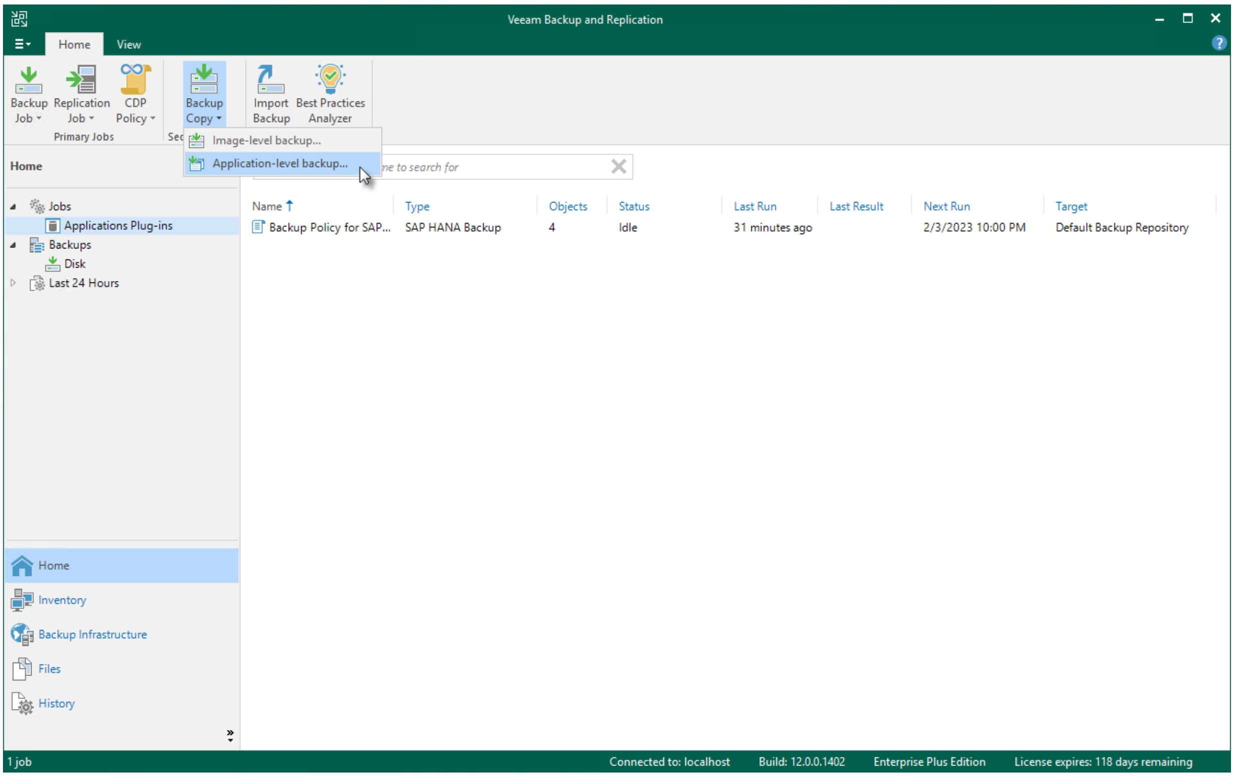
- Backup infrastructure components that will take part in the backup copy process must be added to the backup infrastructure and properly configured. These include source and target backup repositories between which backups must be copied.
- The target backup repository must have enough free space to store copied backups. To receive alerts about low space on the backup repository, configure global notification settings. For more information, see Specifying Other Notification Settings.
- For Veeam Plug-in backup copy jobs, you cannot select a Veeam Cloud Connect repository as a backup copy target.
- If you have upgraded the backup files, make sure that you have upgraded Veeam Plug-in on the source server. If the plug-in is not upgraded to version 12 and you convert backup copy files to backup files, then the next backup job runs will fail.

Step 1. Launch Backup Copy Job Wizard

To create a backup copy job, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.

2. Click the **Backup Copy** tab and select **Application-level backup**.

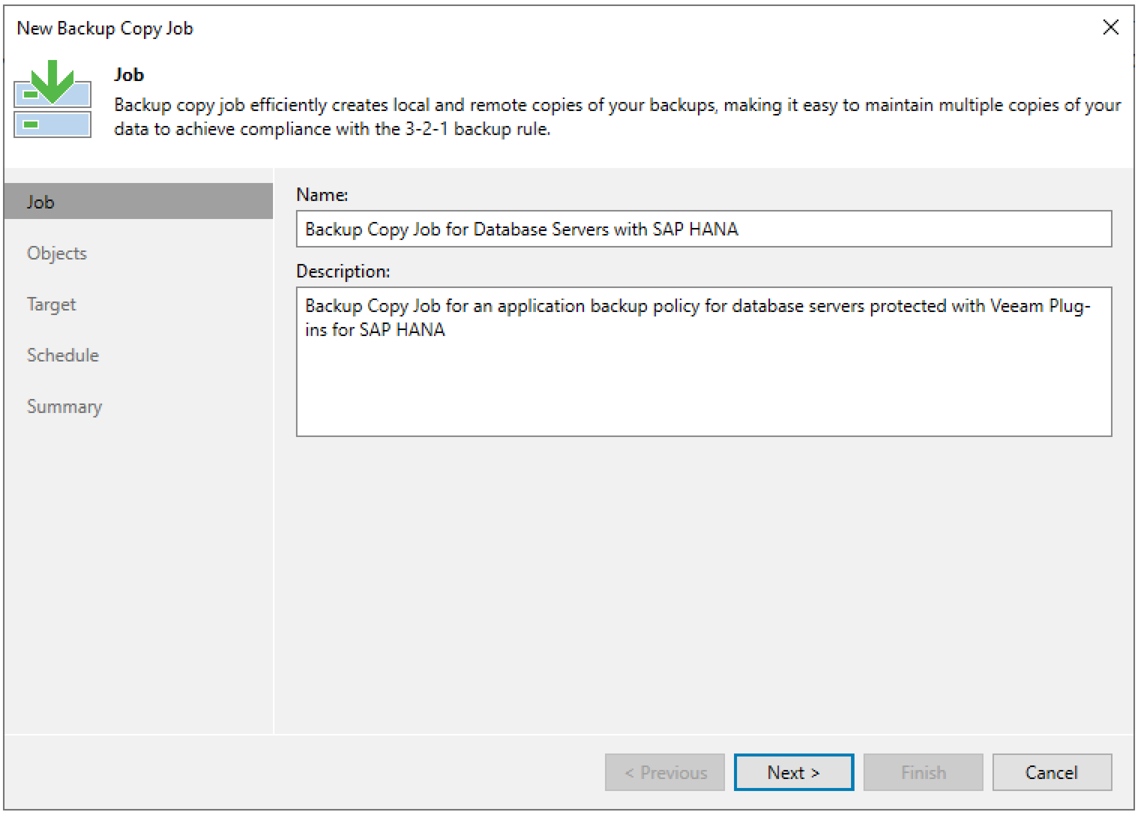


Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target
Backup Policy for SAP...	SAP HANA Backup	4	Idle	31 minutes ago		2/3/2023 10:00 PM	Default Backup Repository

Step 2. Specify Job Name and Description

At the **Job** step of the wizard, specify a name and description for the backup copy job.

1. In the **Name** field, enter a name for the job.
2. In the **Description** field, enter a description for the job. The default description contains information about the user who created the job, date and time when the job was created.



New Backup Copy Job

Job

Backup copy job efficiently creates local and remote copies of your backups, making it easy to maintain multiple copies of your data to achieve compliance with the 3-2-1 backup rule.

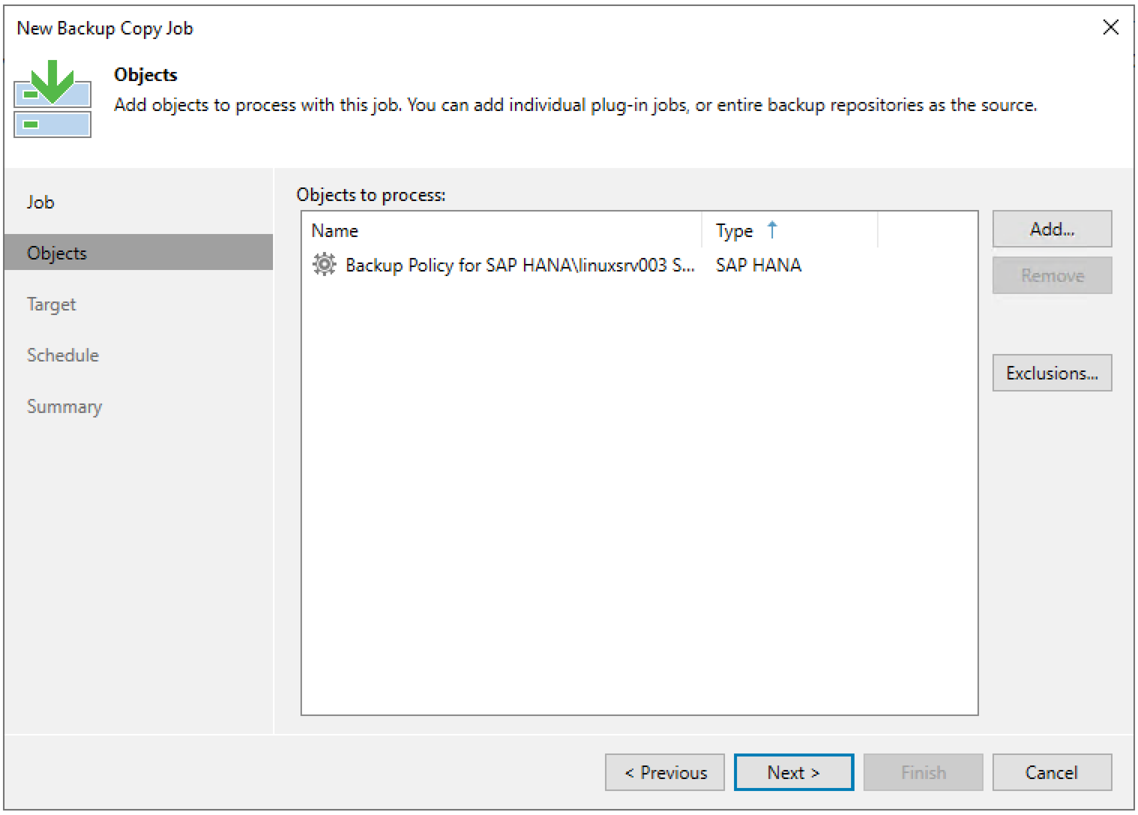
Name: Backup Copy Job for Database Servers with SAP HANA

Description: Backup Copy Job for an application backup policy for database servers protected with Veeam Plug-ins for SAP HANA

Step 3. Select Backups to Process

At the **Object** step of the wizard, select machines whose backups you want to copy to the target repository.

1. Click the **Add** button and select from which entity you want to process the machines.
   - **From jobs**: You can select Veeam Plug-in backup jobs. When a backup copy job runs, Veeam Backup & Replication will search for backup files created by selected jobs.
   - **From repositories**: You can select repositories where Veeam Plug-in backups are stored. When a backup copy job runs, Veeam Backup & Replication will search for backup files created by Veeam Plug-in in selected repositories.
2. Use the **Remove** button if you want to remove selected jobs or repositories from processing.
3. If you have added jobs from a repository and want to exclude from processing some of the backup jobs on the selected repository, click **Exclusions** and select the jobs that you want to exclude.



New Backup Copy Job

Objects

Add objects to process with this job. You can add individual plug-in jobs, or entire backup repositories as the source.

Objects to process:

Name	Type
Backup Policy for SAP HANA\linuxsrv003 S...	SAP HANA

Step 4. Define Backup Copy Target

At the **Target** step of the wizard, configure the target repository settings.

1. From the **Backup repository** list, select a backup repository in the target site where copied backups must be stored. When you select a target backup repository, Veeam Backup & Replication automatically checks how much free space is available on it. Make sure that you have enough free space to store copied backups.

   > IMPORTANT
   >
   > For Veeam Plug-in backup copy jobs, you cannot select a Veeam Cloud Connect repository as a backup copy target.

2. If the target repository contains a Veeam Plug-in backup that was excluded from the backup copy job, and if you don't want to transfer duplicate data, you can use the mapping feature.

   After you configure mapping, if some of backup files (VAB) of the source backup are missing in the target backup copy, these files are uploaded to the target backup copy.

   > NOTE
   >
   > Veeam Plug-in backup copy jobs do not use WAN accelerators.

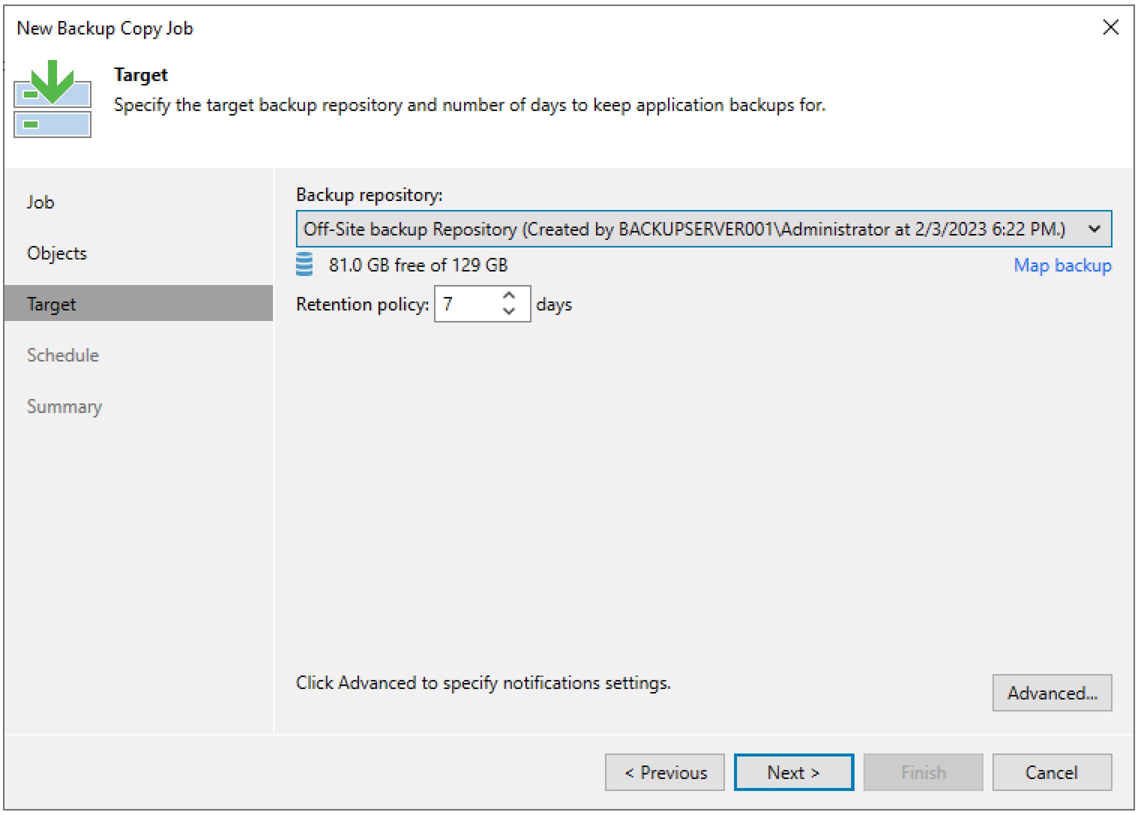
   To map a backup copy job to the backup:

   a. Click the **Map backup** link.

   b. Point the backup copy job to the backup in the target backup repository. Backups in the target backup repository can be easily identified by backup job names. To facilitate search, you can use the search field at the bottom of the window.

   > IMPORTANT
   >
   > - Used account must have access to Veeam backup repositories that you plan to use.
   > - Encryption must be disabled on the repository.
   >
   > Otherwise, the repositories will not be listed as available. To learn how to configure access permissions and encryption settings on repositories, see Access and Encryption Settings on Repositories.

3. You can specify the number of days after which the backup copy will be deleted from the repository. Note that the countdown starts from the moment when source backup has been created.



New Backup Copy Job

Target

Specify the target backup repository and number of days to keep application backups for.

Backup repository: Off-Site backup Repository (Created by BACKUPSERVER001\Administrator at 2/3/2023 6:22 PM.)

81.0 GB free of 129 GB

Retention policy: 7 days

Click Advanced to specify notifications settings.

Step 5. Specify Advanced Settings

At the **Target** step of the wizard, click **Advanced** to configure storage, RPO warning, and notifications settings.

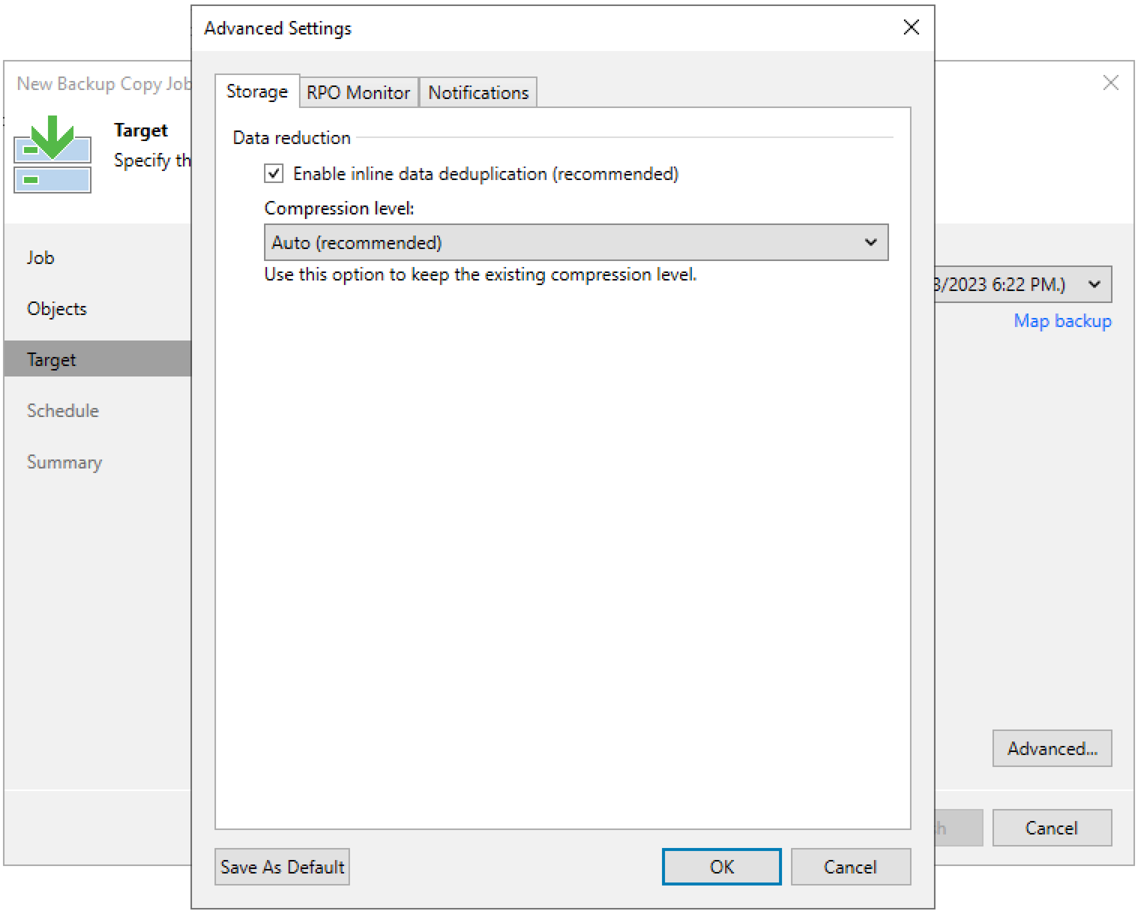
- Storage settings
- RPO warning settings
- Notification settings

Storage Settings

At the **Storage** tab, define compression and deduplication settings.

By default, Veeam Backup & Replication performs deduplication before storing copied data on the target backup repository. Deduplication provides a smaller size of the resulting backup file but may reduce the job performance.

1. You can disable data deduplication. To do this, clear the **Enable inline data deduplication** check box.
2. From the Compression level list, choose a compression level to be used: **Auto**, **None**, **Dedupe-friendly**, **Optimal**, **High** or **Extreme**. The recommended level of compression for backup copy jobs is **Auto**. In this case, Veeam Backup & Replication uses compression settings of the copied backup files. For more information, see Compression and Deduplication.



Advanced Settings

Data reduction

☑ Enable inline data deduplication (recommended)

Compression level: Auto (recommended)

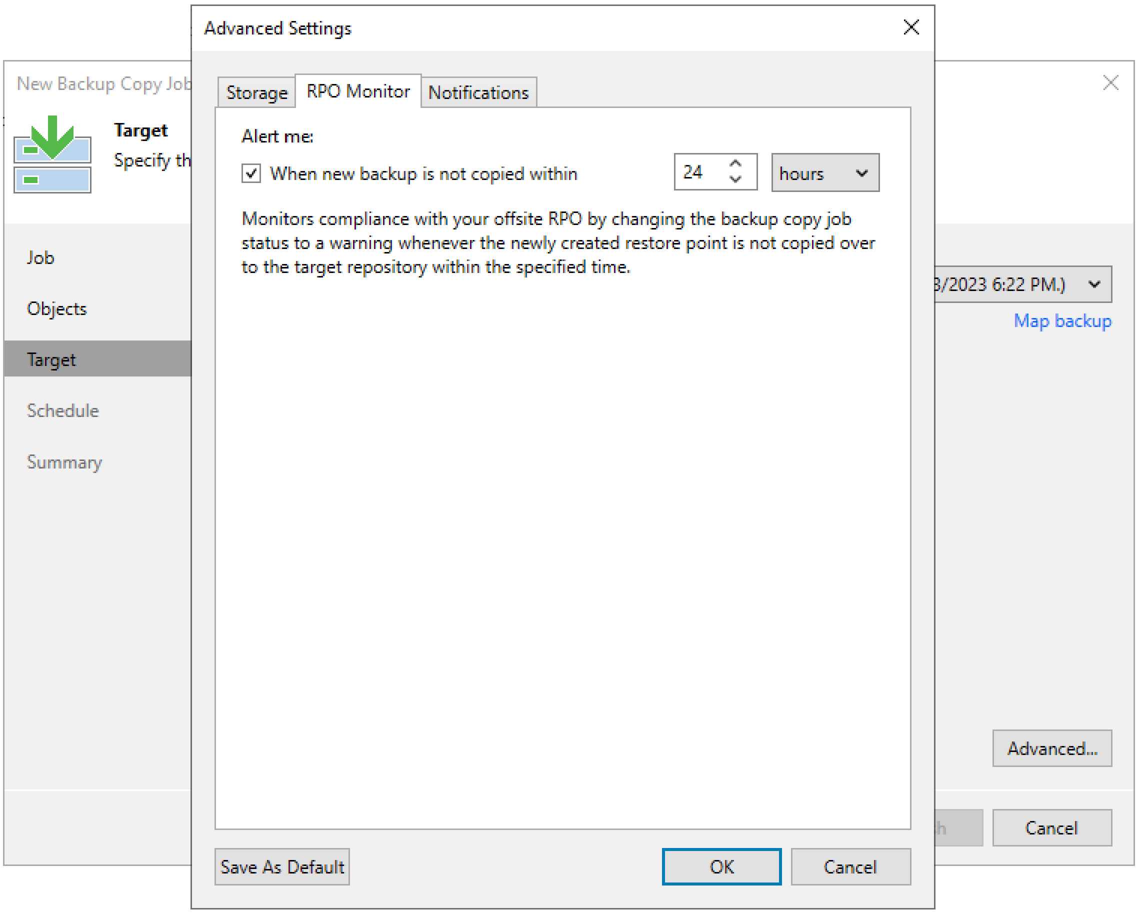
Use this option to keep the existing compression level.

RPO Warning Settings

At the **RPO Monitor** tab, specify RPO warning settings.

Enable the **Warn me if backup is not copied within** check box and specify the time period in **minutes**, **hours**, or **days**.

If the backup copy is not created within the specified time period, the backup copy job will finish with the *Warning* status. The countdown starts from the moment when the required backup is finished and ready to be copied.



Alert me:

☑ When new backup is not copied within 24 hours

Monitors compliance with your offsite RPO by changing the backup copy job status to a warning whenever the newly created restore point is not copied over to the target repository within the specified time.

Notification Settings

At the **Notifications** tab, to specify notification settings for the backup copy job:

1. At the **Target** step of the wizard, click **Advanced**.
2. Click the **Notifications** tab.
3. Select the **Send SNMP notifications for this job** check box if you want to receive SNMP traps when the job completes successfully. SNMP traps will be sent if you specify global SNMP settings in Veeam Backup & Replication and configure software on recipient's machine to receive SNMP traps. For more information, see Specifying SNMP Settings.
4. Select the **Send email notifications to the following recipients** check box if you want to receive notifications by email in case of job failure or success. In the field below, specify a recipient's email address. You can enter several addresses separated by a semicolon.

5. Veeam Backup & Replication sends a consolidated email notification once for the specified backup copy interval. Even if the synchronization process is started several times within the interval, for example, due to job retries, only one email notification will be sent.

6. Email notifications will be sent if you configure global email notification settings in Veeam Backup & Replication. For more information, see Configuring Global Email Notification Settings.

7. At the **Send** at field, specify the time when you want to receive notifications. Note that you will receive a notification on the job status once a day.

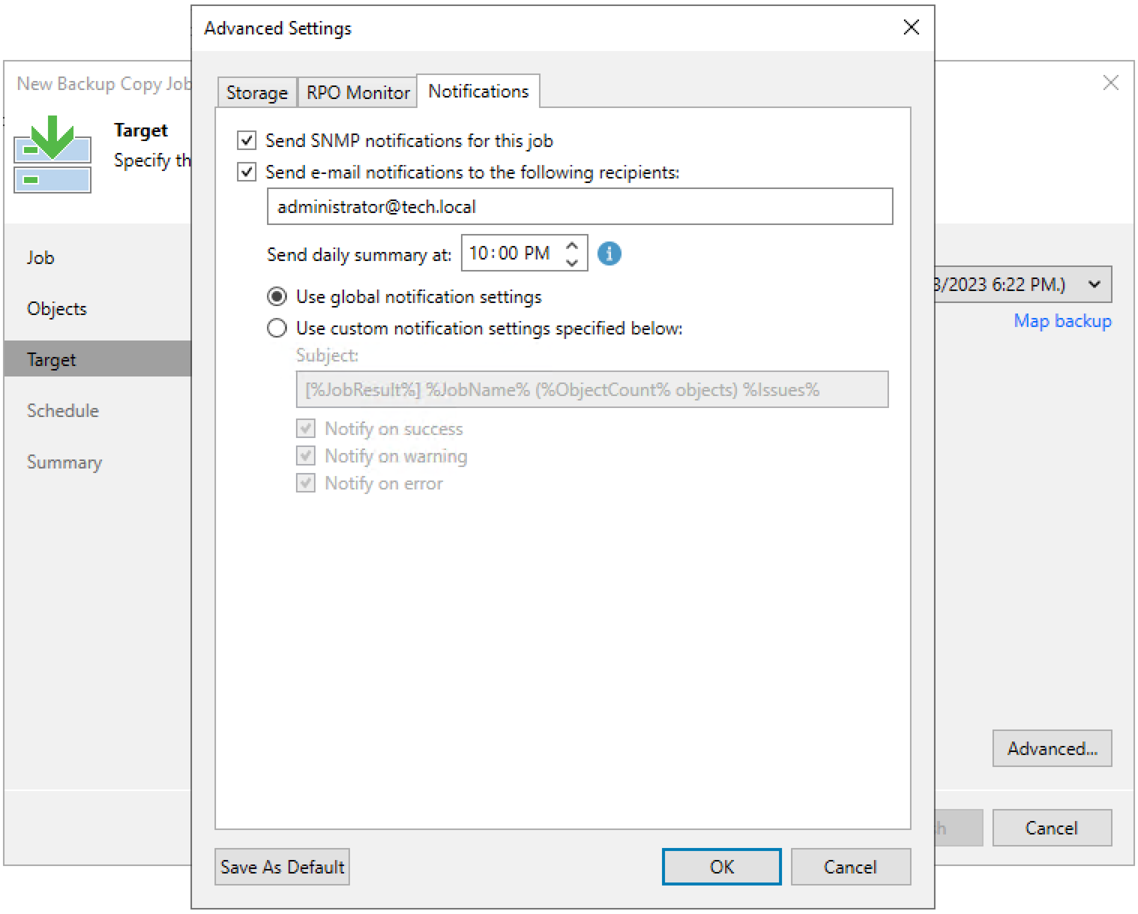
8. You can choose to use global notification settings or specify custom notification settings.

   - To receive a typical notification for the job, select **Use global notification settings**. In this case, Veeam Backup & Replication will apply to the job global email notification settings specified for the backup server. For more information, see Configuring Global Email Notification Settings.

   - To configure a custom notification for a job, select **Use custom notification settings specified below**. You can specify the following notification settings:

     i. In the **Subject** field, specify a notification subject. You can use the following variables in the subject: *%Time%* (completion time), *%JobName%*, *%JobResult%*, *%VmCount%* (number of machines in the job) and *%Issues%* (number of machines in the job that have been processed with the **Warning** or **Failed** status).

     ii. Select the **Notify on success**, **Notify on warning** and **Notify on error** check boxes to receive email notification if data processing within the backup copy interval completes successfully, fails or completes with a warning.



☑ Send SNMP notifications for this job

☑ Send e-mail notifications to the following recipients:

administrator@tech.local

Send daily summary at: 10:00 PM

● Use global notification settings

○ Use custom notification settings specified below:

Subject:

[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

☑ Notify on success

☑ Notify on warning

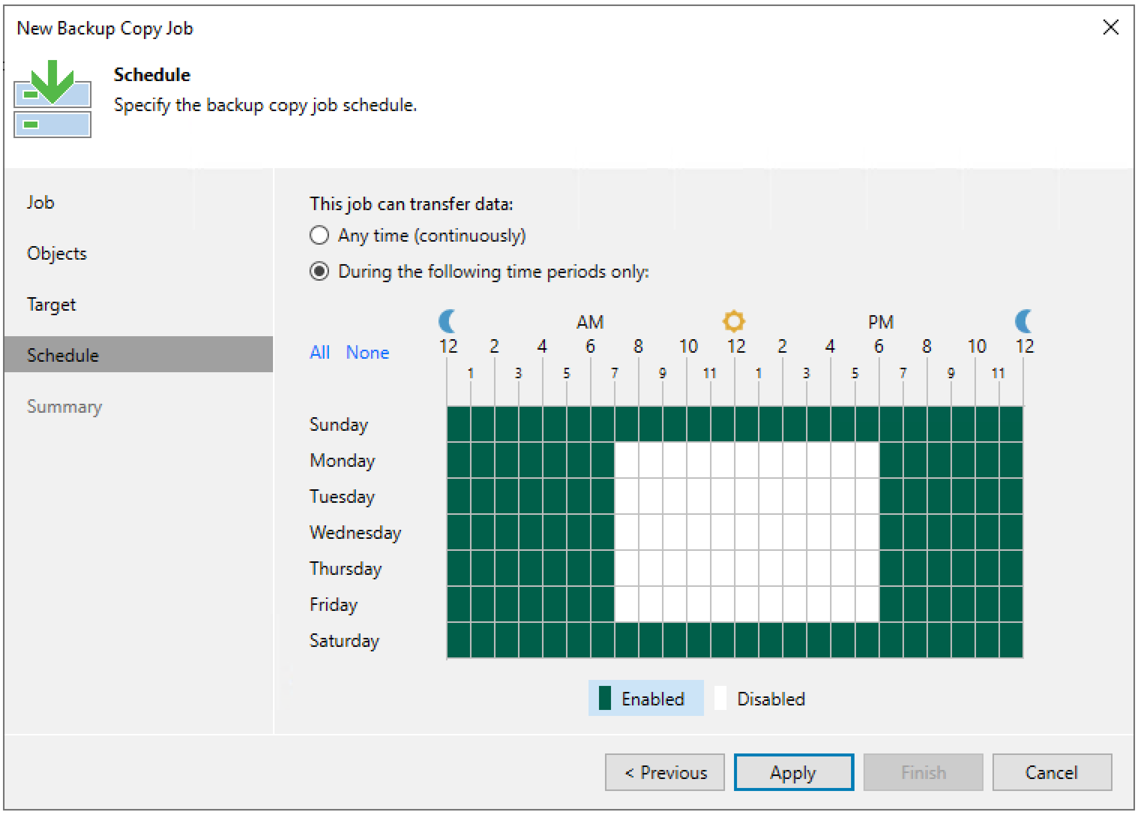
☑ Notify on error

Step 6. Define Backup Copy Schedule

At the **Schedule** step of the wizard, define a time span in which the backup copy job must not transport data between source and target backup repositories. For more information, see Backup Copy Window.

To define a backup window for the backup copy job:

1. Select the **During the following time periods only** option.
2. In the schedule box, select the desired time area.
3. Use the **Enable** and **Disable** options to mark the selected area as allowed or prohibited for the backup copy job.



New Backup Copy Job

Schedule

Specify the backup copy job schedule.

This job can transfer data:

○ Any time (continuously)

● During the following time periods only:

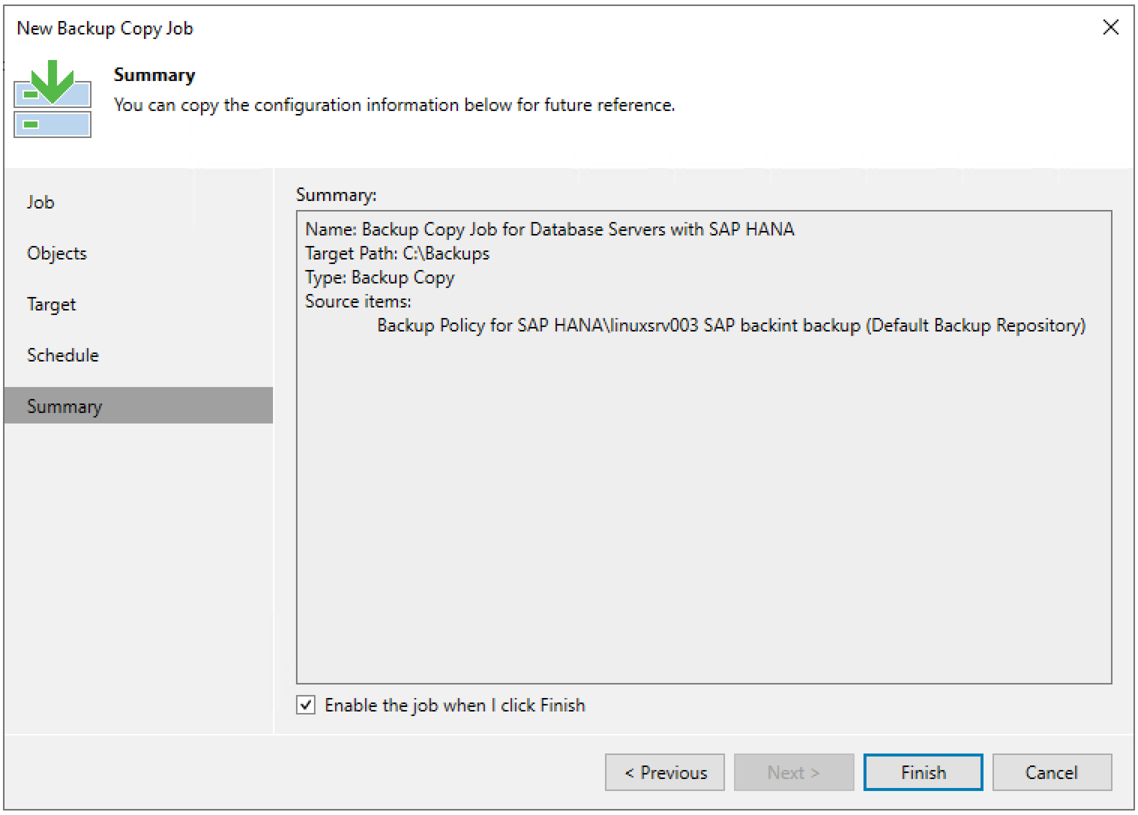
	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11
Sunday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Monday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩
Tuesday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩
Wednesday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩
Thursday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩
Friday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩
Saturday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩

🟩 Enabled ⬜ Disabled

Step 7. Review Backup Copy Job Settings

At the **Summary** step of the wizard, complete the procedure of backup copy job configuration.

1. Review details of the backup copy job.
2. Select the **Enable the job when I click Finish** check box if you want to start the job right after you finish working with the wizard.
3. Click **Finish** to close the wizard.



New Backup Copy Job
Summary
You can copy the configuration information below for future reference.
Job
Objects
Target
Schedule
Summary

Summary:

Name: Backup Copy Job for Database Servers with SAP HANA
Target Path: C:\Backups
Type: Backup Copy
Source items:
    Backup Policy for SAP HANA\linuxsrv003 SAP backint backup (Default Backup Repository)

☑ Enable the job when I click Finish

Converting Backup Copy to Backup

If you have imported backup copy files created by a backup copy job from another repository, you can convert them into regular backup files. When you convert backup copy files to regular backup files, Veeam Plug-in creates a backup job and adds attaches the converted backup files to it. You can use this backup job to continue the backup chain and use converted backup files as a restore point.

If you have imported backups created by a backup copy job from another repository, you can convert them into regular backup files. When you convert backup copy files to regular backup files, Veeam Plug-in creates a backup job and adds attaches the converted backup files to it. You can use this backup job to continue the backup chain and use converted backup files as a restore point.

You can convert imported Veeam Plug-in backups into regular Veeam Plug-in backup files in the following cases:

- If you have deleted a backup copy job which created the backup copy.
- If you have excluded a backup job from a backup copy job that used multiple backup jobs as a source.
- If you have imported a Veeam Plug-in backup copy from another repository.

> NOTE
> If you want to restore from a backup copy, you don't need to convert the backup copy to backup. For details, see Restore from Backup Copy.

Converting Backup Copy to Backup for SAP HANA

To convert a backup copy to a primary backup, use the **--promote-backup-copy-to-primary** parameter as shown below:

```
SapOracleBackintConfigTool --promote-backup-copy-to-primary
Backup copies available for promotion to primary backup:
1. Backup Copy Job 1\saprhel01-localdomain SAP backint backup (Default Backup R
epository)
Select backup: 1
Promotion of backup copy to a primary backup will reconfigure the plug-in to us
e a different repository. Continue? (y/N): y
```

> IMPORTANT
> [For servers with the `customServerName` option] To avoid failure of conversion of backup copies, the server name must be the same as the name used in the backup copy.

Logs and Support

If you have any questions or issues with Veeam Plug-in for SAP on Oracle or Veeam Backup & Replication, you can search for a resolution on Veeam Community Forums or submit a support case on the Veeam Customer Support Portal.

When you submit a support case, we recommend that you attach log files related to Veeam Plug-in operations.

Veeam Plug-in Logs

To export Veeam Plug-in logs, do the following:

1. On the Veeam Backup & Replication server, go to `%PROGRAMDATA%\Veeam\Backup\Plugin`.
2. Copy logs of the required backup or restore process.

SAP Backint Logs

To export SAP Backint logs, on the SAP on Oracle server, go to `/tmp/veeam_plugin_logs/<user_name>/` and copy the following files:

- `SapOracleBackint.log`
- `SapBackintOracleManager.log`
- `Agent.Source.log`

BRTools Logs

The *Detail* and *Summary* logs of BRTools are stored in the `/oracle/SID/sapbackup` and `/oracle/SID/saparch` directories.

For details, see the following sections of the SAP Database Guide: Oracle: BRBACKUP Logs, BRRESTORE Logs, BRARCHIVE Logs, BRRECOVER Logs.

Veeam Plug-in for Microsoft SQL Server

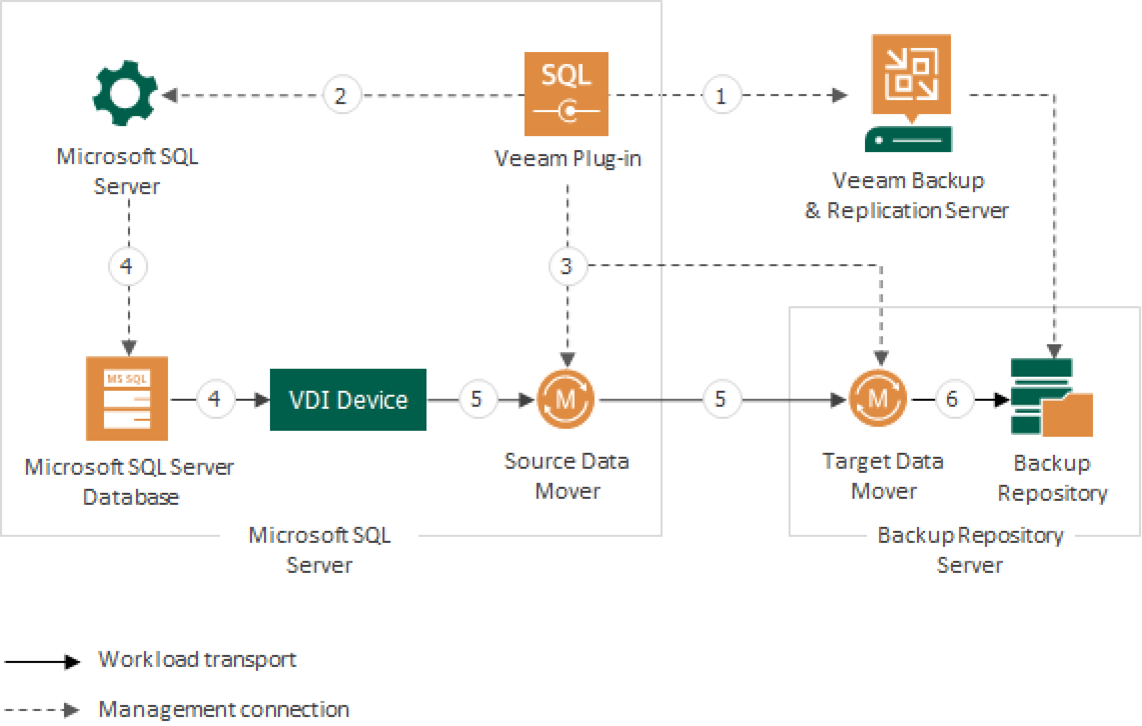
Veeam Plug-in for Microsoft SQL Server is a backup tool for Microsoft SQL Server databases. Veeam Plug-in integrates with Microsoft SQL Server Management Studio and transfers database backups and transaction log backups to backup repositories configured in Veeam Backup & Replication.

Database administrators can use Veeam Plug-in for Microsoft SQL Server to create native application-level backups of Microsoft SQL Server data. Compared to image-level backups created by Veeam Backup & Replication, Veeam Plug-in offers more flexible scenarios for database backup. In particular, Veeam Plug-in users can back up and restore individual Microsoft SQL Server databases, as well as configure independent backup schedule for full, differential and log backups using the SQL Agent Job functionality of Microsoft SQL Server.

How Veeam Plug-in for Microsoft SQL Server Works

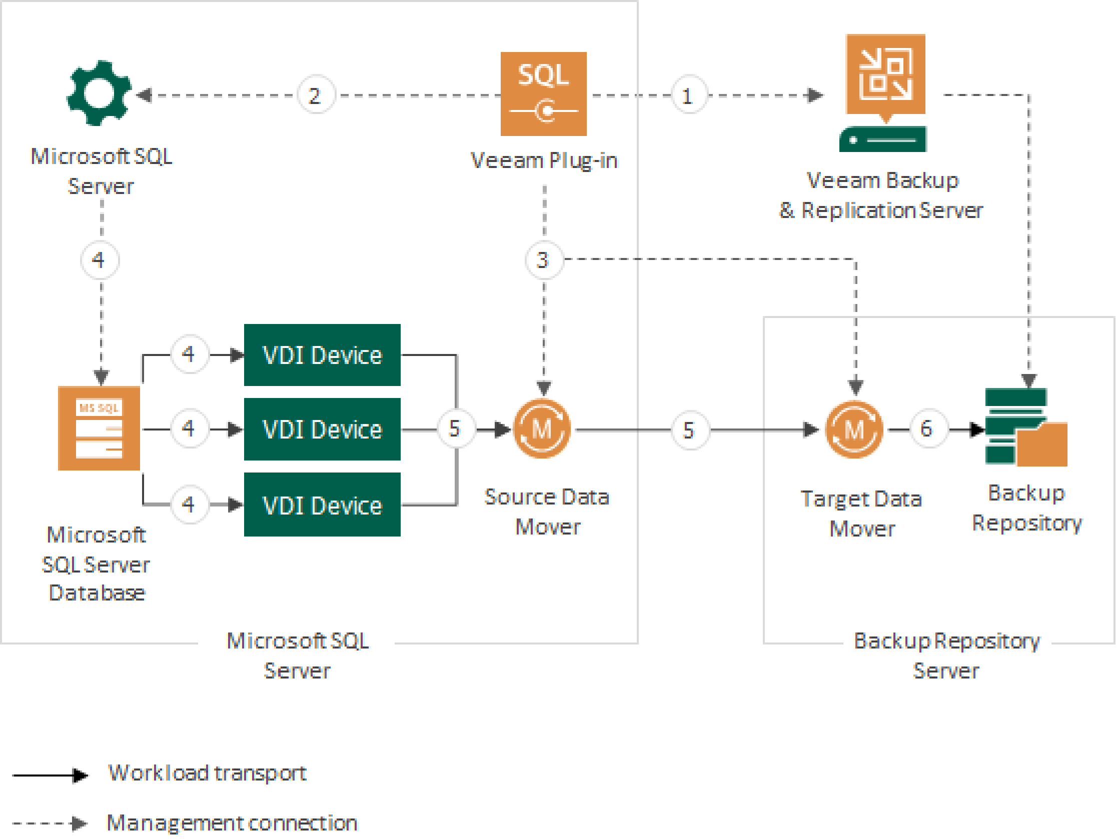
Veeam Plug-in for Microsoft SQL Server performs backup of Microsoft SQL Server databases in the following way:

1. When the backup process is started for the first time, Veeam Plug-in connects to the Veeam Backup & Replication server and creates the backup job.
2. At the backup process start (upon schedule or manually), the *MSSQLRecoveryManager* service of Veeam Plug-in instructs Microsoft SQL Server to back up a database.
3. The *MSSQLRecoveryManager* service starts the source Veeam Data Mover on the Microsoft SQL Server machine, and Veeam Backup Manager in Veeam Backup & Replication starts the target Veeam Data Mover on the Veeam backup repository.
4. Microsoft SQL Server starts the database backup process targeted at a VDI Device — a virtual device that impersonates itself as a backup storage. For each backed-up database, a separate VDI Device is created. The number of VDI Devices also depends on the number of parallel data streams that you specify when configuring backup settings. For more information, see Parallel Database Processing.
5. The source Veeam Data Mover reads the backup data from VDI Devices and transfers it to the target Veeam Data Mover.
6. The target Veeam Data Mover writes the backup data to the backup repository.

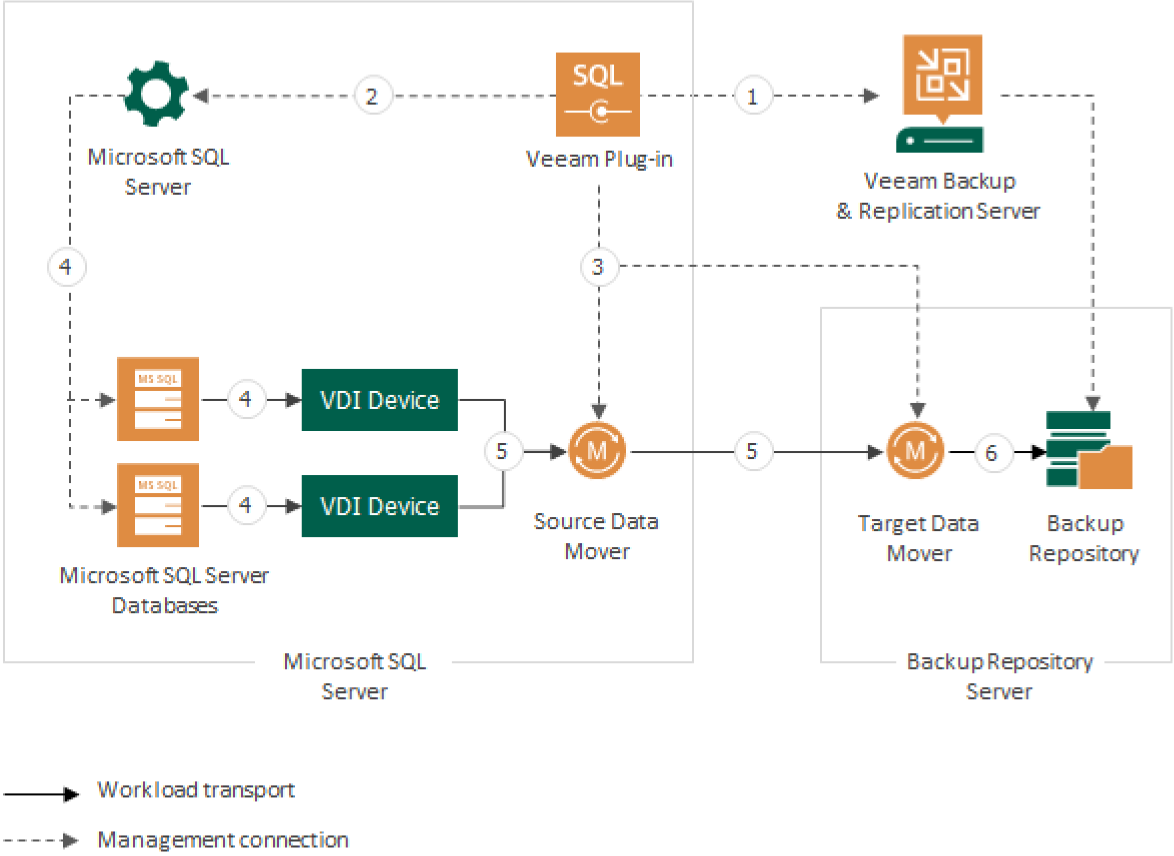


Parallel Database Processing

Veeam Plug-in allows you to back up the same Microsoft SQL Server database in multiple parallel streams. To do this, you must specify the necessary number of data streams when configuring backup settings. For each data stream, a separate VDI Device is created.



If you back up multiple databases simultaneously, a separate VDI Device is created for each backed-up database.



Planning and Preparation

Before you start to use Veeam Plug-in for Microsoft SQL Server, read the environment planning recommendations and make sure that your environment meets system requirements.

- System Requirements
- Permissions
- Ports
- Licensing
- Veeam Environment Planning
- Access and Encryption Settings on Backup Repositories

System Requirements

Before you start using Veeam Plug-in for Microsoft SQL Server, make sure the requirements listed below are met.

Specification	Requirement
OS	64-bit versions of the following operating systems are supported: • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 **Note:** Server Core installations of Microsoft Windows Server OSes are not supported.
Microsoft SQL Server Database	The following Microsoft SQL Server versions are supported: • Microsoft SQL Server 2022 • Microsoft SQL Server 2019 • Microsoft SQL Server 2017 • Microsoft SQL Server 2016 • Microsoft SQL Server 2014 SP3 **Note:** • Standard, Enterprise, Web, Developer editions of Microsoft SQL Server are supported. • Express edition of Microsoft SQL Server is not supported. • Windows Server Failover Clusters are supported, both with shared disks and Cluster Shared Volumes (CSV). • Always On Availability Groups, Always On Clusterless Availability Groups and Always On Failover Cluster Instances are supported. • Distributed Availability Groups are not supported.
Microsoft SQL Server Management Studio	Veeam Plug-in Toolbar requires Microsoft SQL Server Management Studio 18x. **Note:** Remote connections from Microsoft SQL Server Management Studio are not supported.
Veeam Backup & Replication	Veeam Plug-in for Microsoft SQL Server supports integration with Veeam Backup & Replication version 12 or later.
Network	Veeam Plug-in should be able to establish a direct IP connection to the Veeam Backup & Replication server. Thus, Veeam Plug-in cannot work with the Veeam Backup & Replication server that is located behind the NAT gateway.

Permissions

Mind the required permissions for the following user accounts.

User That Performs Veeam Plug-in Installation

The account used for installing and updating Veeam Plug-in must be a member of the local *Administrators* group. Local administrator permissions are required to install and manage Veeam Plug-in Toolbar in Microsoft SQL Server Management Studio.

User That Performs Backup and Restore

To be able to connect to a Microsoft SQL Server instance, the account used for starting Microsoft SQL Server backup and restore processes must be added to the following roles:

- *public*
- *sysadmin*

Veeam Backup & Replication User

The account that is used to authenticate against Veeam Backup & Replication must have access permissions on required Veeam backup repository servers. To learn how to configure permissions on repositories, see Granting Access to Repositories.

Veeam Plug-in for Microsoft SQL Server uses Windows authentication methods of the Veeam Backup & Replication server to establish a connection to this server and to the backup target. It is recommended to create one user for each standalone Microsoft SQL Server or failover cluster with Veeam Plug-in.

To work with backups created by Veeam Plug-in, you can use only the same account that was used for creating the backup. If you want to use another account, assign the *Veeam Backup Administrator* role or *Veeam Backup Operator* and *Veeam Restore Operator* roles to the account. To learn how to assign Veeam Backup & Replication roles, see the Users and Roles section of the Veeam Backup & Replication User Guide.

Ports

To enable proper operation of Veeam Plug-in for Microsoft SQL Server, make sure that the following ports are open.

Microsoft SQL Server

The following table describes network ports that must be opened to ensure proper communication of the Oracle server and backup infrastructure components.

From	To	Protocol	Port	Notes
Microsoft SQL Server where Veeam Plug-in is installed	Veeam Backup & Replication server	TCP	10006	Default port used for communication with the Veeam Backup & Replication server. Note that data between Veeam Plug-ins and backup repositories is transferred directly, bypassing the Veeam Backup & Replication server.
	Backup repository server or gateway server*	TCP	2500 to 3300**	Default range of ports used as data transmission channels. For every TCP connection that a backup process uses, one port from this range is assigned.
	Microsoft SQL Server (localhost)	TCP	6791+; 2500 to 3300**	Local connections between Veeam Plug-in and source Data Movers.

* For NFS share, SMB share repositories, and Dell Data Domain, HPE StoreOnce deduplication storage appliances, Veeam Backup & Replication uses an auxiliary backup infrastructure component — gateway server. For details, see the Gateway Server section of the Veeam Backup & Replication User Guide.

** This range of ports applies to newly added backup infrastructure components. If you upgrade to Veeam Backup & Replication 10.0 from earlier versions of the product, the range of ports from 2500 to 5000 applies to the already added components.

Backup Repositories and Gateway Servers

Depending on the type of backup repositories that you use for Veeam Plug-in backups, the following ports must be open to allow communication between backup infrastructure components.

From	To	Protocol	Port	Notes
Veeam Backup & Replication server	Backup repository server or gateway server*	TCP	2500 to 3300**	Default range of ports used as data transmission channels. For every TCP connection that a backup process uses, one port from this range is assigned.

From	To	Protocol	Port	Notes
Direct Attached Storage				
Veeam Backup & Replication server	Linux server used as a backup repository or gateway server	TCP	22	Port used as a control channel from the Veeam Plug-in server to the target Linux host.
	Microsoft Windows server used as a backup repository or gateway server	TCP UDP	135, 137 to 139, 445	Ports used as a management channel from the Veeam Plug-in server to the Repository/Gateway server. Also, the ports are used to deploy Veeam components.
		TCP	6160, 6162	Default ports used by the Veeam Installer Service and Veeam Data Mover Service
Network Attached Storage				
Gateway server (specified in the SMB share repository settings)	SMB server	TCP	445	Default port used by SMB transport protocol.
		TCP UDP	135, 137 to 139	SMB/Netbios name resolution for SMB protocol (needed in some cases). For details, see the Used Ports section of the Veeam Backup & Replication User Guide.
Gateway server (specified in the NFS share repository settings)	NFS server	TCP UDP	111, 2049	Standard NFS ports used as a transmission channel from the gateway server to the target NFS share.
Dell Data Domain				
Veeam Backup & Replication server	Dell Data Domain	TCP	111	Port used to assign a random port for the mountd service used by NFS and DDBOOST. Mountd service port can be statically assigned.

From	To	Protocol	Port	Notes
or **Gateway server**	For more information, see this Dell KB article.	TCP	2049	Main port used by NFS. To change the port, you can use the ‘`nfs set server-port`’ command. Note that the command requires SE mode.
		TCP	2052	Main port used by NFS MOUNTD. To change the port, you can use the '`nfs set mountd-port`' command. Note that the command requires SE mode.
HPE StoreOnce				
Veeam Backup & Replication server or **Gateway server**	HPE StoreOnce	TCP	9387	Default command port used for communication with HPE StoreOnce.
			9388	Default data port used for communication with HPE StoreOnce.
ExaGrid				
Veeam Backup & Replication server	ExaGrid	TCP	22	Default command port used for communication with ExaGrid.
Quantum DXi				
Veeam Backup & Replication server	Quantum DXi	TCP	22	Default command port used for communication with Quantum DXi.

* For NFS share, SMB share repositories, and Dell Data Domain, HPE StoreOnce deduplication storage appliances, Veeam Backup & Replication uses an auxiliary backup infrastructure component — gateway server. For details, see the Gateway Server section of the Veeam Backup & Replication User Guide.

** This range of ports applies to newly added backup infrastructure components. If you upgrade to Veeam Backup & Replication 10.0 from earlier versions of the product, the range of ports from 2500 to 5000 applies to the already added components.

For detailed list of ports used by Veeam Backup & Replication server and backup repositories, see the Used Ports section of the Veeam Backup & Replication User Guide.

Licensing

To use the Veeam Plug-in functionality, you must have a valid Veeam Backup & Replication license. Licenses are installed and managed on the Veeam Backup & Replication server that is connected to the Veeam Plug-in server. If the license is not valid or out of resources, Veeam Plug-in backup jobs fail.

This guide provides information only on specifics of Veeam licenses for Veeam Plug-ins. For terminology and general information about Veeam Licensing, see Veeam Licensing Policy.

Licensed Objects

A Microsoft SQL Server machine with Veeam Plug-in is assumed protected if it has been processed by a Veeam Plug-in backup job in the last 31 days.

If you use any instance-based (Veeam Universal Licensing) license in Veeam Backup & Replication, you do not need to install any additional licenses. A protected server with Veeam Plug-in consumes one instance unit from the license. Servers processed by backup copy jobs are not regarded as protected machines, these types of jobs provide an additional protection level for machines that are already protected with Veeam Plug-in backup jobs.

A machine protected by both Veeam Plug-in and Veeam Backup & Replication will consume a license only once. For example, you have Microsoft SQL Server that you back up using Veeam Plug-in. You also back up this server using image-level backup functionality of Veeam Backup & Replication. In this case, only one license will be consumed.

> NOTE
>
> [For Perpetual per-socket licenses] If you are using a legacy perpetual per-socket license, a license is required for each hypervisor CPU socket occupied by protected Oracle servers.
>
> A socket is consumed from the license only if the hypervisor where protected servers reside is added to the Veeam Backup & Replication infrastructure. If the hypervisor is not added to the Veeam Backup & Replication infrastructure, an instance unit will be consumed from the license. To learn how to add a hypervisor to the Veeam Backup & Replication infrastructure, see the Virtualization Servers and Hosts section of the Veeam Backup & Replication User Guide.

> IMPORTANT
>
> The license is required for all cluster nodes, even if Veeam Plug-in is installed only on one of the nodes.

Supported License Types

You can use Veeam Plug-ins with the following license types and packages. Note that this guide contains information on specifics of Veeam license packages only for Veeam Plug-ins. For the full list of license packages, see Pricing and Packaging.

- **For Veeam Universal Licensing**:

  You can use Veeam Plug-ins with all license packages (*Veeam Backup Essentials, Veeam Backup & Replication, Veeam Availability Suite*).

  Note that if you use the *Rental* license type, functionality of Veeam Plug-ins is supported only for the *Enterprise Plus* edition of Veeam Backup & Replication.

- **For Perpetual Socket license**:

  Functionality of Veeam Plug-ins is supported only for the *Enterprise Plus* edition of Veeam Backup & Replication.

Obtaining and Managing Licenses

To learn how to install a license and monitor licensed objects, see the Licensing section in the Veeam Backup & Replication User Guide.

Veeam Environment Planning

Before you deploy Veeam Plug-in, keep in mind the following requirements and limitations.

Data Streams and Resource Consumption

Any parallel data stream started by Microsoft SQL Server will use one Veeam backup repository task slot. You can configure the number of backup streams at the **Backup Options** step of the **Back Up Database** wizard. It is recommended to carefully plan repository task slots, so that Microsoft SQL Server can work with multiple streams in parallel when configured.

The following hardware resources are recommended based on tests on Skylake processors:

- **Microsoft SQL Server**: 1 CPU core and 200 MB of RAM per currently used backup stream.
- **Backup repository server**: 1 CPU core and 1 GB of RAM per 5 currently used backup streams.

  These resources are recommended only if you use a dedicated backup repository for Veeam Plug-in backups. If you use the same backup repository for Veeam Plug-in backups and VM backups created by Veeam Backup & Replication or Veeam Agents, consider adding the mentioned above hardware resources based on usual load on your backup repository. For details on hardware requirements for a backup repository, see the System Requirements section of the Veeam Backup & Replication User Guide.

  We recommend to contact your Veeam system engineer to optimize the backup stream settings and resource allocation. Also, note that it is recommended to use a separate backup repository for Veeam Plug-in backups.
- **Veeam Backup & Replication server**: during manual metadata operations such as import of backup files, the Veeam Backup & Replication server needs additional 15 GB of RAM per 1 million files located in the same backup job folder.

Hosting Environments

Veeam Plug-in uses the hostname of the Microsoft SQL Server machine, Microsoft SQL Server failover cluster or Always On availability group to create a Veeam Backup & Replication job object and backup folder.

If you have servers that with the same hostname in multiple environments, you must add the following entries to the plug-in configuration file:

```
<PluginParameters useFQDNInServerName="true" />
```

IMPORTANT

For security reasons, it is recommended to use separate repositories for different customers and limit the Veeam Repository Authentication to the specific customer.

Access and Encryption Settings on Backup Repositories

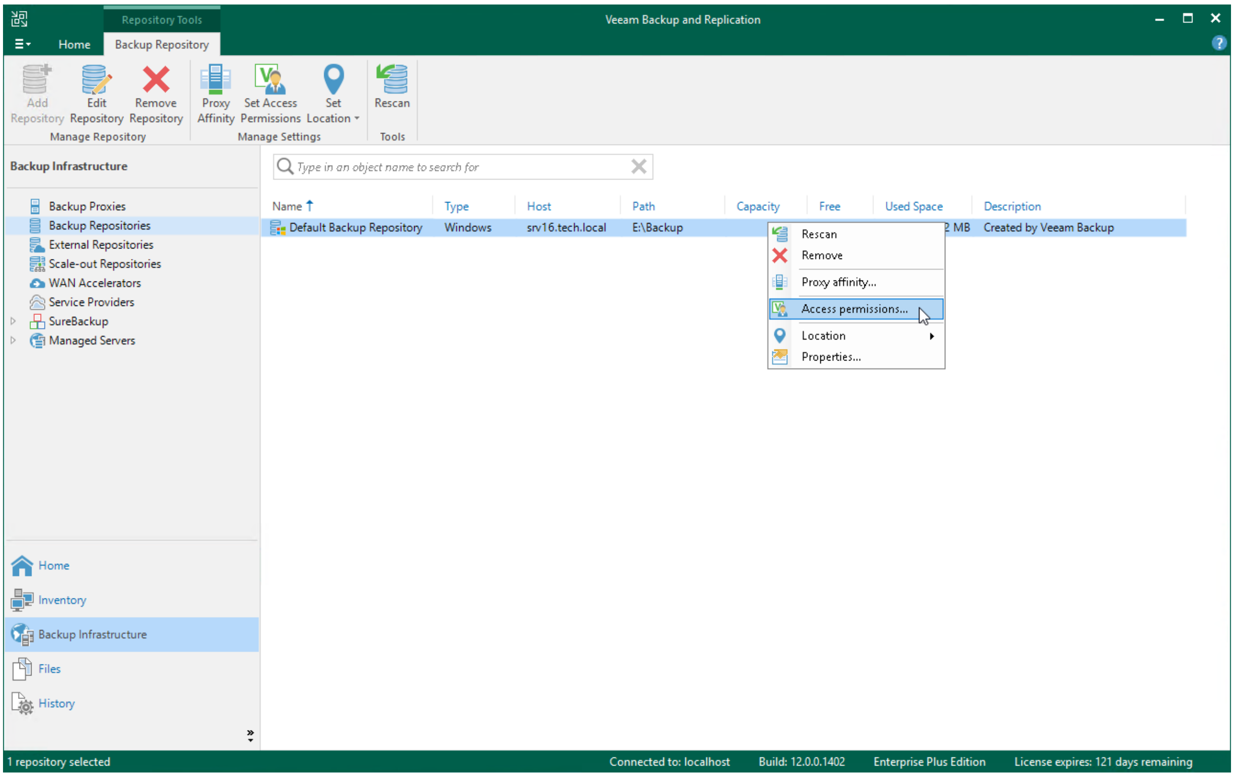
When you configure Veeam Plug-in, you specify an account that must be used to connect to the Veeam Backup & Replication server. To be able to store backups in a backup repository, the specified account must have access permissions on the target backup repository.

To grant access permissions, do the following:

1. In Veeam Backup & Replication, open the **Backup Infrastructure** view.

2. In the inventory pane, click the **Backup Repositories** node or the **Scale-out Repositories** node.

3. In the working area, select the necessary backup repository and click **Set Access Permissions** on the ribbon or right-click the backup repository and select **Access permissions**.



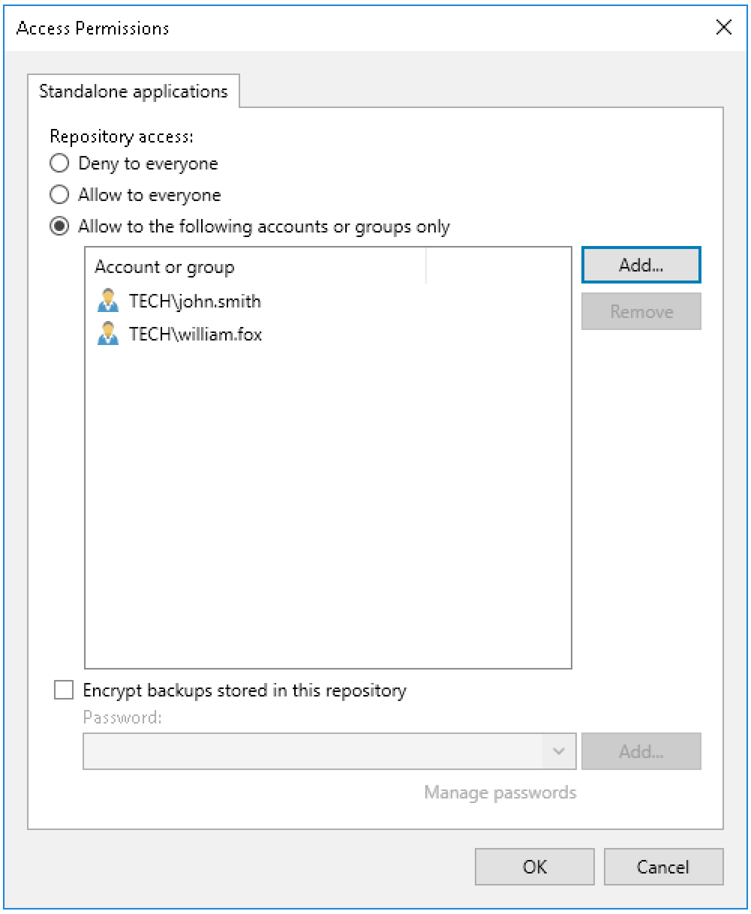
4. In the **Access Permissions** window, on the **Standalone applications** tab specify to whom you want to grant access permissions on this backup repository:

   ○ *Allow to everyone* — select this option if you want to grant repository access to any user. This option is equal to granting access rights to the *Everyone* group in Microsoft Windows (anonymous users are excluded). For security reasons, the option is not recommended for production environments.

   ○ *Allow to the following accounts or groups only* — select this option if you want only specific users to be able to store backups in this repository. Click **Add** to add the necessary users and groups to the list.

5. Veeam Plug-ins cannot send backups or backup copies to a backup repository where encryption is enabled. Thus, make sure that the **Encrypt backups stored in this repository** check box is not selected.

6. Click **OK**.



Access Permissions

Standalone applications

Repository access:

○ Deny to everyone

○ Allow to everyone

● Allow to the following accounts or groups only

Account or group
TECH\john.smith
TECH\william.fox

□ Encrypt backups stored in this repository

Password:

Getting Started

To protect Microsoft SQL Server databases with Veeam Plug-in, perform the following operations:

1. Deploy Veeam Plug-in on the machine that runs Microsoft SQL Server. For more information, see Installing Veeam Plug-in for Microsoft SQL Server.

2. Configure connection between Veeam Plug-in and the backup repository managed by the Veeam Backup & Replication server. For more information, see Configuring Veeam Plug-in for Microsoft SQL Server.

3. Define what data you want to back up and configure backup settings. For more information, see Performing Backup.

4. In case of a disaster, you can restore data from a backup. For more information, see Performing Restore.

Deployment and Configuration

Veeam Plug-in for Microsoft SQL Server is a feature of Veeam Backup & Replication. This guide gives instructions on how to deploy Veeam Plug-in assuming that you already have deployed Veeam Backup & Replication and configured a backup repository. To learn how to deploy Veeam Backup & Replication, see the Veeam Backup & Replication User Guide for your platform.

To be able to use Veeam Plug-in for Microsoft SQL Server, you must complete the following steps:

1. Install the plug-in on the Microsoft SQL Server machine.
2. Configure the plug-in settings.

Installing Veeam Plug-in for Microsoft SQL Server

You can install Veeam Plug-in for Microsoft SQL Server using the installation wizard or in an unattended mode using the command-line interface.

> **NOTE**
>
> When you launch Veeam Plug-in installation, the installation wizard also installs Microsoft .NET Framework 4.5.2 if it does not detect this component on the machine. In some cases, installation of .NET Framework requires a reboot of the machine. This can happen, for example, if you have an earlier version of .NET Framework installed on the machine, and during the installation process it is used by third-party software.

Installing Veeam Plug-in

Veeam Plug-in for Microsoft SQL Server is an additional component of Veeam Backup & Replication, and the installation package of the plug-in is included in the Veeam Backup & Replication installation ISO file.

To install Veeam Plug-in for Microsoft SQL Server, do the following:

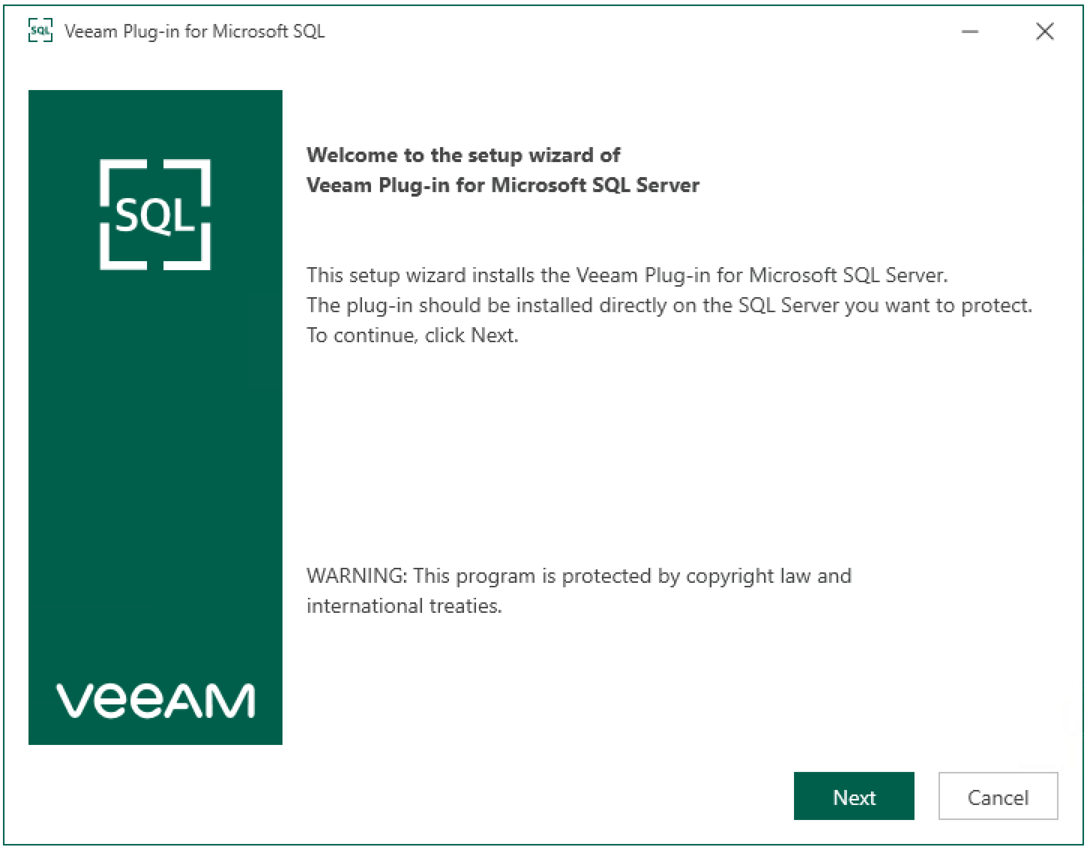
1. Mount the Veeam Backup & Replication installation disk (`VeeamBackup&Replication_12.0.0.1420.iso`).

   If you deploy Veeam backup infrastructure for the first time, you can download the Veeam Backup & Replication installation disk at: https://www.veeam.com/backup-replication-vcp-download.html.

2. In the installation disk folder, navigate to the `Plugins\Microsoft SQL\x64\` folder.

3. To launch the installation wizard, run the `VeeamPluginforMSSQL.exe` file.

4. At the welcome screen of the installation wizard, click **Next**.



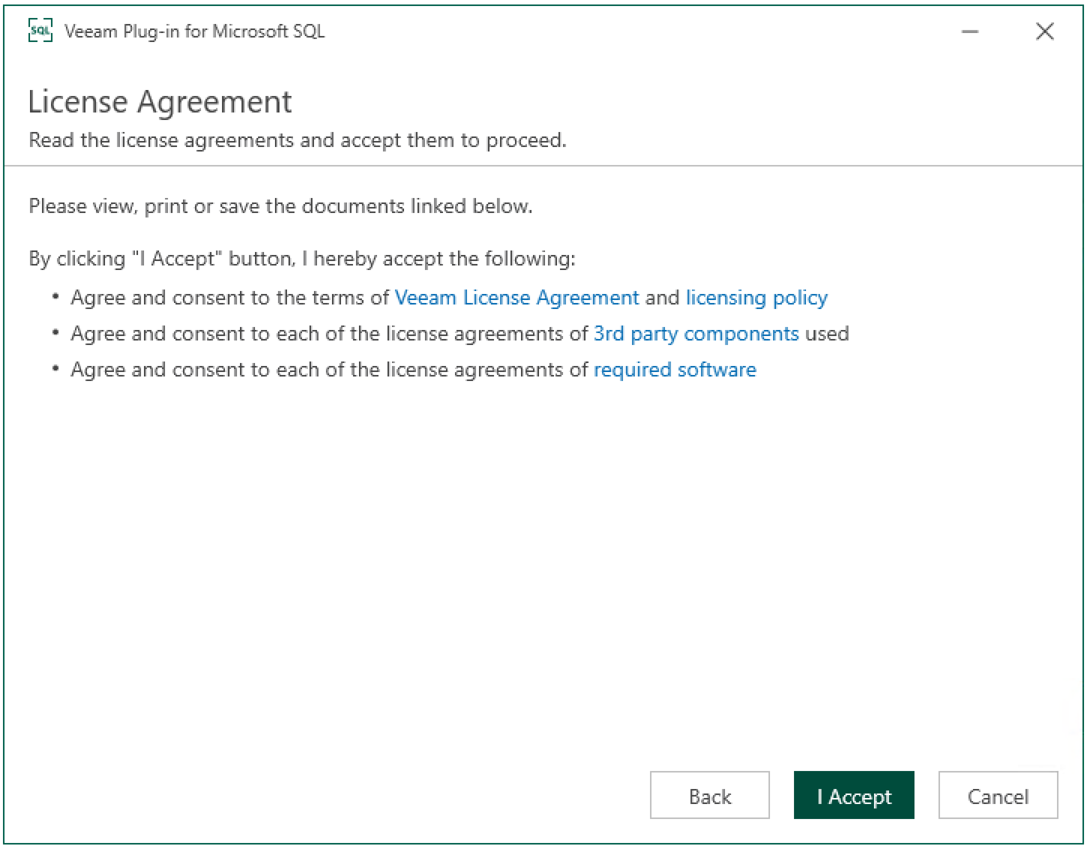
Veeam Plug-in for Microsoft SQL

Welcome to the setup wizard of
Veeam Plug-in for Microsoft SQL Server

This setup wizard installs the Veeam Plug-in for Microsoft SQL Server.
The plug-in should be installed directly on the SQL Server you want to protect.
To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

5. At the **License Agreement** step of the wizard, follow the links to view license agreements and click **I Accept**.



Veeam Plug-in for Microsoft SQL

License Agreement

Read the license agreements and accept them to proceed.

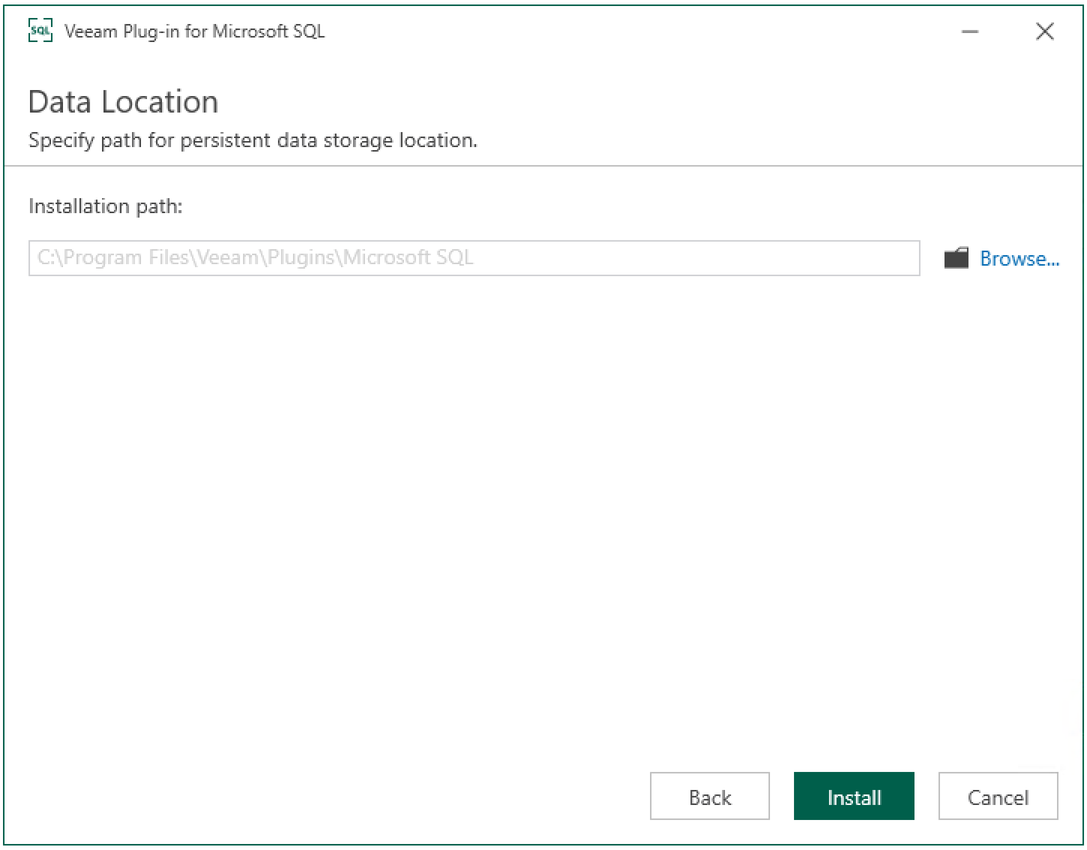
Please view, print or save the documents linked below.

By clicking "I Accept" button, I hereby accept the following:

- Agree and consent to the terms of Veeam License Agreement and licensing policy
- Agree and consent to each of the license agreements of 3rd party components used
- Agree and consent to each of the license agreements of required software

6. At the **Data Location** step of the wizard, specify the installation path for Veeam Plug-in and click **Install**.

   By default, the installation wizard installs the product to the `C:\Program Files\Veeam\Plugins\Microsoft SQL\` folder.

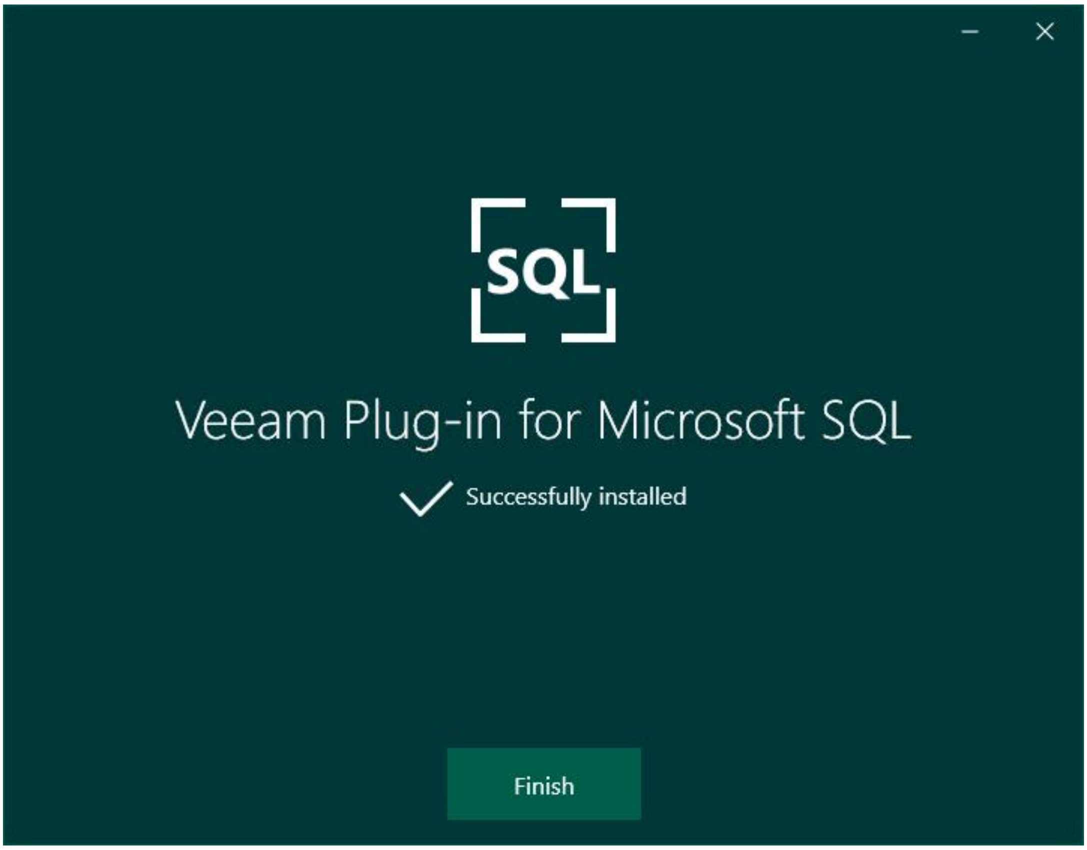


Data Location

Specify path for persistent data storage location.

Installation path: C:\Program Files\Veeam\Plugins\Microsoft SQL

7. Wait for the installation process to complete and click **Finish** to exit the wizard.



Installing Veeam Plug-in in Unattended Mode

You can install Veeam Plug-in for Microsoft SQL Server in the unattended mode using the command line interface. To do this, go to the folder where the `VeeamPluginforMSSQL.exe` file resides and run the following command:

```
<path_to_exe>\VeeamPluginforMSSQL.exe /silent /accepteula /acceptthirdpartylice
nses /acceptrequiredsoftware /acceptlicensingpolicy
```

where `<path_to_exe>` is a path to the Veeam Plug-in for Microsoft SQL Server installation file.

Parameter	Description
`/silent`	Enables the silent mode.
`/accepteula`	Accepts EULA terms.
`/acceptthirdpartylicenses`	Accepts terms of third-party licenses.
`/acceptrequiredsoftware`	Enables installation of the required software (Microsoft .NET Framework 4.5.2) and accepts terms of its license.
`/acceptlicensingpolicy`	Accepts terms of the Veeam licensing policy.

Veeam Plug-in for Microsoft SQL Server uses the following codes to report about the installation results:

- 1000 — Veeam Plug-in for Microsoft SQL Server has been successfully installed.
- 1001 — prerequisite components required for Veeam Plug-in for Microsoft SQL Server have been installed on the machine. Veeam Plug-in for Microsoft SQL Server has not been installed. The machine needs to be rebooted.
- 1002 — Veeam Plug-in for Microsoft SQL Server installation has failed.
- 1101 — Veeam Plug-in for Microsoft SQL Server has been installed. The machine needs to be rebooted.

Configuring Veeam Plug-in for Microsoft SQL Server

To use Veeam Plug-in, you must configure connection between the Microsoft SQL Server machine, Veeam Backup & Replication server and backup repository where backup files will be stored.

To configure connection settings, use the **Configure Plug-in** wizard. The wizard configures Veeam Plug-in settings and saves the settings to the `veeam_config.xml` file. The file is located in the `%PROGRAMFILES%\Veeam\Plugins\Microsoft SQL\` folder on the machine where Veeam Plug-in is installed.

> **TIP**
>
> You can also configure Veeam Plug-in for Microsoft SQL Server using the `MSSQLConfigTool.exe` tool. To learn more, see Configuring Veeam Plug-in with Command-Line Interface.

To configure Veeam Plug-in, do the following:

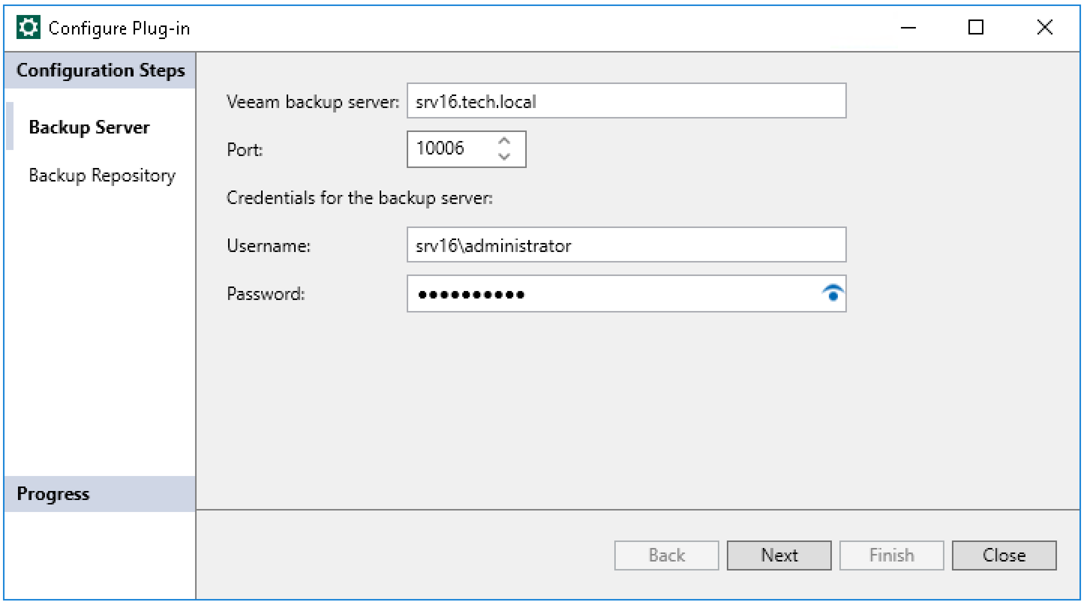
1. On the Microsoft SQL Server machine, launch the **Configure Plug-in** wizard. To do this, do either of the following:
   - Click the **Configure Plug-in** icon on the desktop.
   - From the Microsoft Windows **Start** menu, select **All Programs** > **Veeam** > **Configure Plug-in** or use the Microsoft Windows search to find the **Configure Plug-in** option on your machine.
   - In Microsoft SQL Server Management Studio, click the **Configure Plug-in** button on the toolbar.
   - Launch the `%PROGRAMFILES%\Veeam\Plugins\Microsoft SQL\Veeam.Backup.MSSQLPlugin.UI.Configuration.exe` file.

2. At the **Backup Server** step of the wizard, specify settings to connect to the Veeam Backup & Replication server:

   a. In the **Veeam backup server** field, specify a DNS name of the Veeam Backup & Replication server.

   b. In the **Port** field, specify the port number over which Veeam Plug-in for Microsoft SQL Server will communicate with Veeam Backup & Replication. By default, Veeam Plug-in for Microsoft SQL Server uses port 10006.

   c. In the **Username** and **Password** fields, specify credentials that will be used to connect to the Veeam Backup & Replication server. The specified account must have the local Administrator permissions on the server.



Veeam backup server: srv16.tech.local

Port: 10006

Credentials for the backup server:

Username: srv16\administrator

Password: ●●●●●●●●●●●

3. At the **Backup Repository** step of the wizard, do the following:

   a. From the **Backup repository** drop-down list, select the required repository.

      You must allow access to Veeam backup repositories that you plan to use. Also, the encryption on the backup repository must be disabled. To learn how to configure access and encryption on backup repositories, see Access and Encryption Settings on Repositories.

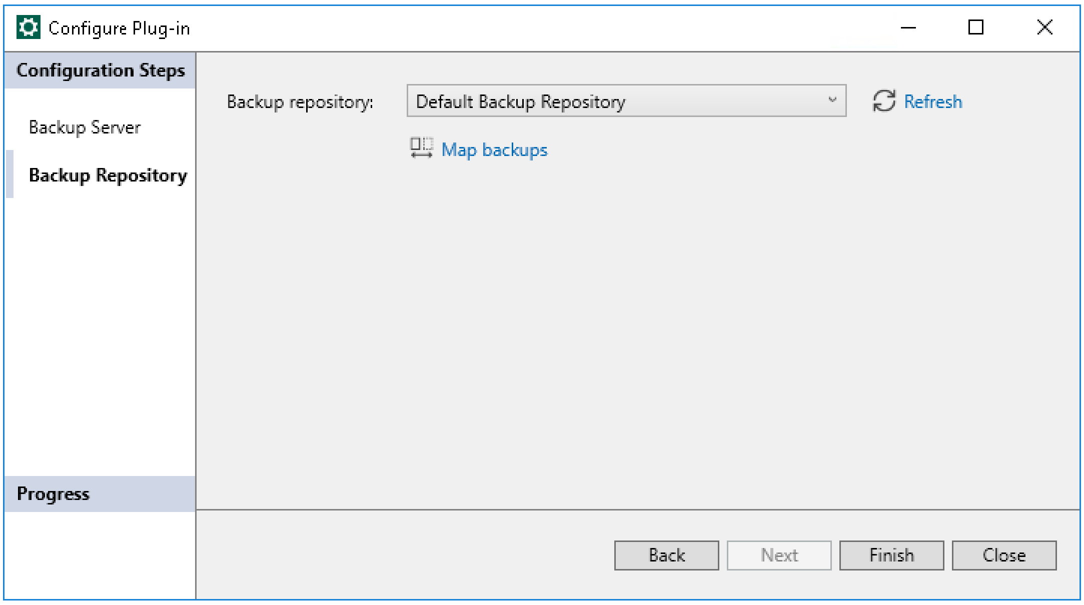
      You can click **Refresh** to update the list of backup repositories. This may be helpful, for example, after you configure access to a backup repository and want to select this repository without the need to re-run the **Configure Plug-in** wizard.

   b. You can map Veeam Plug-in for Microsoft SQL Server backup jobs to backups stored in the backup repository. Backup job mapping can be helpful if you moved backup files to a new backup repository and want to point backup jobs to existing backups in this new backup repository. You can also use backup job mapping if the configuration database got corrupted and you need to reconfigure backup jobs.

      To map Veeam Plug-in for Microsoft SQL Server backup jobs to backups in the backup repository, click the **Map backups** link and select one or more backups in the **Select Backups** window.

      You can map Veeam Plug-in for Microsoft SQL Server backup jobs to multiple backups in the backup repository. This may be helpful, for example, if you want to continue a backup chain for databases that operate as part of a failover cluster or availability group.

3. Click **Finish** to exit the wizard.



Backup repository: Default Backup Repository

> IMPORTANT
>
> You can work with backups created by Veeam Plug-in only under the account that was used for creating these backups. If you want to use another account, assign the *Veeam Backup Administrator* role or *Veeam Backup Operator* and *Veeam Restore Operator* roles to the account.
>
> To learn how to assign Veeam Backup & Replication roles, see the Users and Roles section of the Veeam Backup & Replication Guide.

Configuring Veeam Plug-in with Command-Line Interface

To specify Veeam Plug-in for Microsoft SQL Server settings, you can use the `MSSQLConfigTool.exe` command-line tool. You can use its commands to change a specific parameter in the `veeam_config.xml` file or to enable or disable Veeam Plug-in features.

To specify Veeam Plug-in settings, do the following:

1. On the Microsoft SQL Server machine, navigate to the `%PROGRAMFILES%\Veeam\Plugins\Microsoft SQL\` folder.

2. Run the `MSSQLConfigTool.exe` command with the required parameters. For more information, see Configuration Parameters.

   For example, to specify credentials that will be used to connect to the Veeam Backup & Replication server, use the following command:

   ```
   MSSQLConfigTool.exe --set-credentials "administrator@srv16" "password"
   ```

Configuration Parameters

You can specify the following parameters for the `MSSQLConfigTool.exe` command:

Command	Description
--help	Shows the list of parameters for the plug-in configuration tool.
--show-config	Shows the current Veeam Plug-in for Microsoft SQL Server configuration.
--set-credentials	Specifies credentials to connect to the Veeam Backup & Replication server. Provide a user name in the *username@domain* format and a password in the *password* format. If you do not provide a password as a value for this parameter, Veeam Plug-in will prompt you to specify a password.
--set-host	Specifies the domain name or IP address of the Veeam Backup & Replication server.
--set-port	Specifies the port over which to connect to the Veeam Backup & Replication server.
--set-repository	Specifies the name of the backup repository. If you do not provide the name of the backup repository as a value for this parameter, Veeam Plug-in will prompt you to select a backup repository from the list of repositories managed by the backup server.
--promote-backup-copy-to-primary	Maps the imported backup copy to a regular Veeam Plug-in backup chain.

Exporting and Importing Plug-in Settings

You can export a Veeam Plug-in configuration file and apply the plug-in settings to other severs.

> **IMPORTANT**
>
> The password included in the configuration file is encrypted. Thus, after you import the configuration file, you must set the credentials manually in the Veeam Plug-in configuration wizard or using the `MSSQLConfigTool.exe` command-line tool.

To export the configuration file to another server, do the following:

1. On the server where Veeam Plug-in is installed, navigate to the `%PROGRAMFILES%\Veeam\Plugins\Microsoft SQL\` folder.
2. Copy the `veeam_config.xml` file to the server where you want to configure the plug-in.
3. Install Veeam Plug-in on the new server and place the copied XML file in the `%PROGRAMFILES%\Veeam\Plugins\Microsoft SQL\` folder.
4. Set new credentials to connect to the Veeam Backup & Replication server using the following command:

   ```
   C:\Program Files\Veeam\Plugins\Microsoft SQL\MSSQLConfigTool.exe --set-cre
   dentials "serv\username" "password"
   ```

Importing Backup Files

If the Veeam Backup & Replication server has failed and you have restored it in a new location, you can copy the backup files to a new repository and re-map the Veeam Plug-in backup files.

Limitations and Prerequisites

Mind the following limitations:

- If backup files are not imported according to instructions given in this section, Veeam Plug-in backup and restore operations may fail.
- The repository from which you plan to import backups must be added to the Veeam Backup & Replication infrastructure. Otherwise you will not be able to access backup files.
- If you are importing backup files from a scale-out backup repository, the names of backup files and paths to backup files must contain only allowed characters:
  - Alphanumeric characters: `a-zA-Z0-9`
  - Special characters: `_-.+=@^`
  - Names of backup files and paths to backup files must not contain spaces.

How to Import Veeam Plug-in Backup Files

To import Veeam Plug-in backup files, do the following:

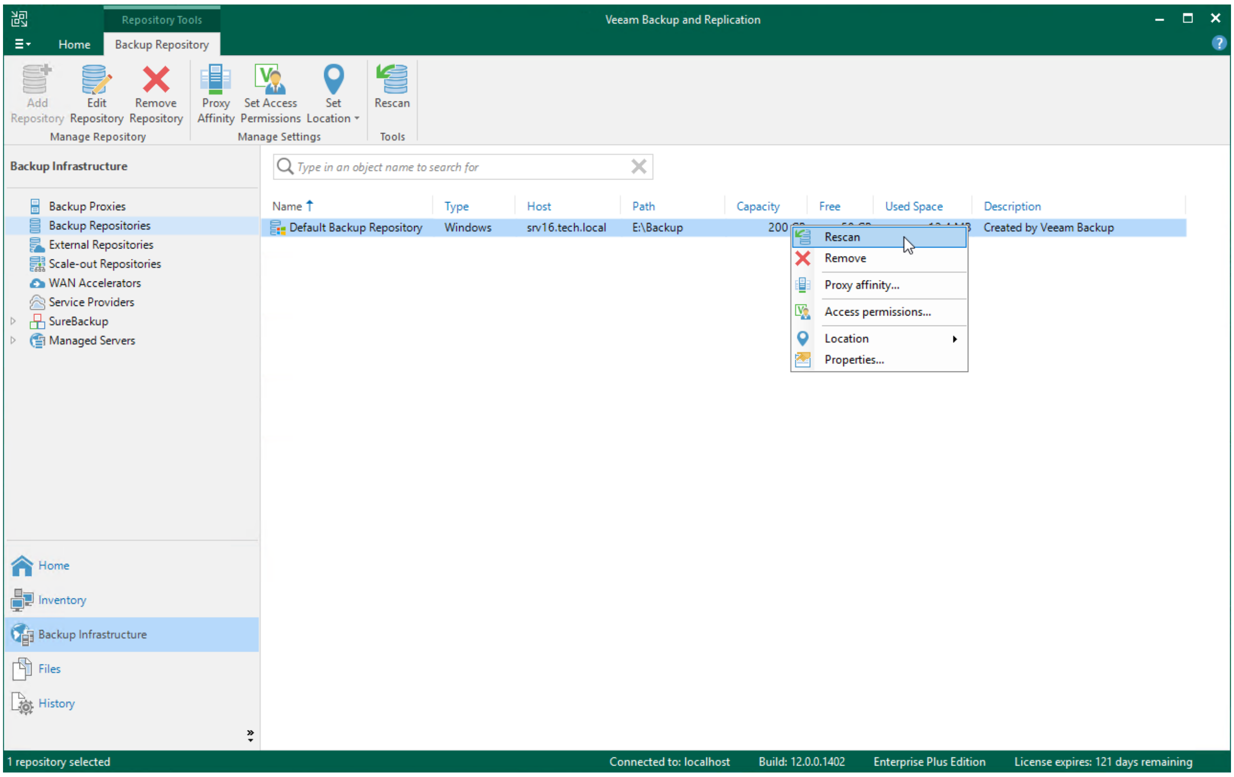
1. Move the folder with the backup file to the required backup repository or create a new backup repository with this folder as a subfolder.

   > **TIP**
   >
   > Each Veeam Plug-in backup file (.vab) has its own metadata file (.vasm). Make sure you import backup files and all related metadata files. You must also import the backup job metadata file (.vacm) which is stored in the same folder.

2. In the Veeam Backup & Replication console, open the **Backup Infrastructure** view.
3. In the inventory pane of the **Backup Infrastructure** view, select the **Backup Repositories** node.

4. In the working area, select the required backup repository and click **Rescan** on the ribbon. Alternatively, you can right-click the backup repository and select **Rescan**.

   During the rescan operation, Veeam Backup & Replication gathers information about backups that are currently available in the backup repository and updates the list of backups in the configuration database. After the rescan operation, backups that were not in this configuration database will be shown on the **Home** view in the **Backups > Disk (Imported)** node.



Name	Type	Host	Path	Capacity	Free	Used Space	Description
Default Backup Repository	Windows	srv16.tech.local	E:\Backup	200 [illegible]	[illegible]	[illegible]	Created by Veeam Backup

1 repository selected   Connected to: localhost   Build: 12.0.0.1402   Enterprise Plus Edition   License expires: 121 days remaining

5. On the Microsoft SQL Server machine, set the new backup repository as a target in the Veeam Plug-in settings and map Veeam Plug-in to backups in the repository. For more information, see Configuring Veeam Plug-in for Microsoft SQL Server.

Uninstalling Veeam Plug-in for Microsoft SQL Server

To uninstall Veeam Plug-in for Microsoft SQL Server, do the following:

1. On the Microsoft SQL Server machine with Veeam Plug-in, open the **Control Panel** and click **Programs and Features**.
2. In the list of programs, select **Veeam Plug-in for Microsoft SQL** and click **Uninstall.**

Performing Backup

After you configure Veeam Plug-in settings, you can use Veeam Plug-in to back up Microsoft SQL Server databases. Veeam Plug-in uses native Microsoft SQL Server mechanisms to create application-level backups of Microsoft SQL Server data.

Veeam Plug-in backs up Microsoft SQL Server databases according to backup settings that you specify. You can specify what databases to back up, the type of database backups you want to create, retention policy for database backups and processing settings for backed-up data. In addition, you can use Microsoft SQL Server Management Studio or a third-party scheduling tool to define schedule for database backup.

About Microsoft SQL Server Backup

Veeam Plug-in uses native Microsoft SQL Server mechanisms to create application-level backups of Microsoft SQL Server data. You can use Veeam Plug-in to create backups of the following types.

- Full backup
- Differential backup
- Log backup
- Copy-only full backup
- Copy-only log backup

For more information about Microsoft SQL Server backup types, see Microsoft Docs.

To create backups of a specific type, you must configure backup settings for Veeam Plug-in and run the backup process. You can run the backup process manually, immediately after you configure backup settings, or you can define schedule according to which Veeam Plug-in will back up Microsoft SQL Server data automatically. For more information, see Backup Settings and Backup Schedule.

Backup Settings

Veeam Plug-in backs up Microsoft SQL Server databases according to backup settings that you specify. You can specify what databases to back up, what type of backups you want to create, retention policy for database backups and processing settings for backed-up data.

To specify backup settings, Veeam Plug-in offers the **Back Up Database** wizard. Alternatively, you can use the `MSSQLRecoveryManager.exe` command-line tool to specify backup settings and start the backup process. For more information, see Configuring Backup Settings and Performing Backup with Command-Line Interface.

In addition, you can use Microsoft SQL Server Management Studio or a third-party scheduling tool to define schedule for database backup.

If you want to perform backups of different types periodically, you must configure backup settings and specify schedule for each backup type. For example, you can specify settings for full backup, settings for differential backup and settings for log backup, save each of these settings as a separate SQL Agent job, and create schedule for these SQL Agent jobs in Microsoft SQL Server Management Studio.

Backup Schedule

Veeam Plug-in for Microsoft SQL Server does not offer its own backup schedule mechanisms. Instead, Veeam Plug-in allows database administrators to use tools of their choice to configure flexible schedule for database backup. For example, you can use native Microsoft SQL Server schedule settings to configure flexible schedule for full, differential or log backups, or use an external scheduling tool.

Veeam Plug-in for Microsoft SQL Server offers two scenarios for backup scheduling:

- Scenario 1. You can configure backup schedule in Microsoft SQL Server. To do this, you must save Veeam Plug-in backup settings as an SQL Agent job. For more information, see Saving Backup Settings as SQL Agent Job.

  After that, you will be able to configure job schedule in the properties of the SQL Agent job in Microsoft SQL Server Management Studio.

- Scenario 2. You can use a third-party scheduling tool to create periodic backups of Microsoft SQL Server data with Veeam Plug-in. To do this, you must configure Veeam Plug-in backup settings and obtain a command that will be used to start the backup process. For more information, see Exporting Backup Settings to Custom Script.

  After that, you will be able to use the resulting command in a custom backup script or with a scheduling tool of your choice.

Backup Chain

A sequence of backups created with Veeam Plug-in for a Microsoft SQL Server database makes up a backup chain. The backup chain can be described at two levels: physical level and logical level.

- At the physical level, the backup chain is a sequence of backup files created by Veeam Plug-in in the backup repository. In contrast to image-level backups created with Veeam Backup & Replication for which a separate backup file is created during each backup session, backup files created with Veeam Plug-in contain data backed up within multiple backup sessions. Thus, instead of a chain of full and incremental backup files, Veeam Plug-in creates its own set of backup files in the backup repository.

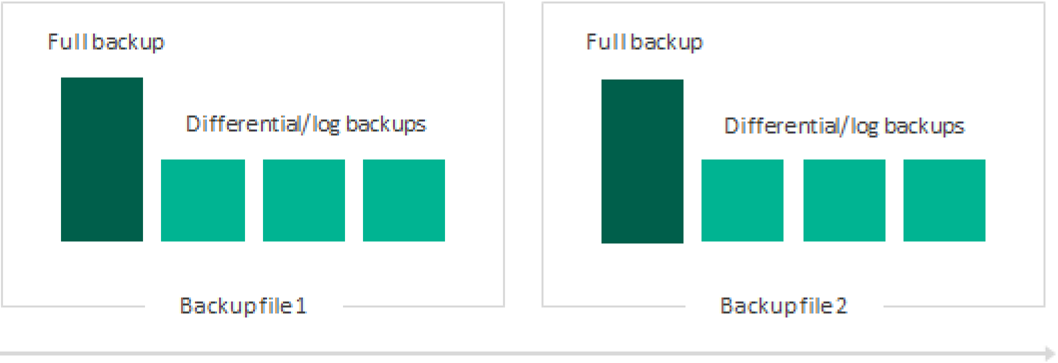
- At the logical level, the backup chain consists of a full backup of a Microsoft SQL Server database and its dependent differential backups and log backups. Backups in the backup chain form a set of restore points. Restore points correspond to the time when the backup was performed and let you recover the database to the necessary state.

  To create a backup chain, Veeam Plug-in implements the forward incremental backup method.

  Full backup, its dependent differential backups and log backups of a Microsoft SQL Server database reside in the same backup file. Depending on what backup settings you specify, the backup chain can also span multiple backup files. This mechanism differs from the one for image-level backups created with Veeam Backup & Replication where one restore point generally corresponds to one backup file.

  The logical sequence of backups is hidden from the user — the user cannot get information about available restore points from a sequence of backup files in the backup repository. The user can view and select restore points when restoring a database. For more information, see Performing Restore.

For information about types of backup files that Veeam Plug-in creates and rules for creating the backup chain, see Backup Files and How Backup Chain Works.



Backup Files

Veeam Plug-in for Microsoft SQL Server creates and maintains the following types of backup files:

- VAB — backup files that store a copy of Microsoft SQL Server data.
- VASM — backup metadata files that store information about the backup. A VASM file is created for each VAB file. The VASM files are used by Veeam Backup & Replication to get information about Veeam Plug-in backups.
- VACM — backup metadata files that store information about the backup job. Veeam Plug-in creates one VACM file for the backup job.

All backup files created by the backup job reside in a dedicated job folder in the backup repository. For example, if the name of the backup job in Veeam Backup & Replication is *SRV01 MSSQL backup (Backup Vol 01)*, Veeam Backup & Replication will create the *SRV01 MSSQL backup (Backup Vol 01)* folder on the target backup repository and store all backup files created by this job in this folder.

How Backup Chain Works

Veeam Plug-in for Microsoft SQL Server creates the backup chain in the following way:

1. During the first backup session, Veeam Plug-in for Microsoft SQL Server creates a new VAB file in the backup repository and writes to this file data of the full backup. This backup becomes a starting point in the backup chain.

   Veeam Plug-in writes data of each backed-up database to a separate backup file. For example, if you back up 2 databases, Veeam Plug-in will create 2 VAB files in the backup repository.

2. During subsequent backup sessions, Veeam Plug-in for Microsoft SQL Server writes the backup data either to the same VAB file or to a new VAB file. A new VAB file is created if one of the following cases:

   - If Veeam Plug-in performs full backup.
   - If the previous backup file created for the database is older than 24 hours.

   > NOTE
   >
   > If the backup is targeted at a scale-out backup repository, Veeam Plug-in selects an extent where to write the backup data according to the placement policy specified for the scale-out backup repository (*Data locality* or *Performance*). After that, Veeam Plug-in applies the same algorithm to choose whether to write the backup data to an existing backup file or new backup file.

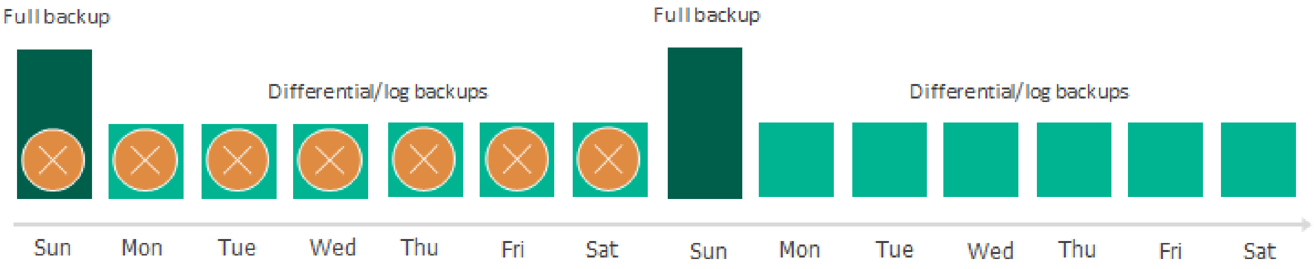
Retention Policy

Veeam Plug-in allows you to configure retention policy for Microsoft SQL Server backups. The retention policy helps maintain the life cycle of restore points and make sure that backup files do not consume the entire space on the backup repository.

Veeam Plug-in for Microsoft SQL Server applies the retention policy at the database level and retains restore points for a number of days defined in the backup settings. After each full backup or differential backup session, Veeam Plug-in checks the time when restore points for the backed-up database were created and removes outdated restore points from the backup chain.

Veeam Plug-in does not remove outdated restore points immediately. Instead, Veeam Plug-in applies the retention policy to the inactive part of the backup chain — that is, the previous full backup and its dependent differential and log backups. Only after the last incremental backup in the chain becomes outdated, Veeam Plug-in will remove the inactive backup chain.

For example, the retention policy is set to 7 days. Veeam Plug-in is set to create full backups each Sunday, and differential backups and log backups are created Monday through Saturday. Although a new full backup is created on Sunday, the previous full backup is not deleted. Without the full backup, the subsequent chain of differential and log backups would be useless. Veeam Plug-in will wait for the time when the last restore point in the inactive backup chain becomes outdated, and only then will delete the entire inactive chain, which will happen next Saturday.



Retention Policy Configuration

To configure the retention policy, select the **Apply retention policy** check box at the **Options** step of the **Back Up Database** wizard and specify the number of days to keep restore points in the backup chain.

In contrast to retention policy for image-level backups in Veeam Backup & Replication, retention policy for backups created with Veeam Plug-in for Microsoft SQL Server is optional. This allows you to easier configure retention policy for different types of Microsoft SQL Server backups.

For example, you want to configure backup settings to create full, differential and log backups for the same database. In this case, you can enable retention policy in the backup settings for full backups only. Differential backups and log backups that depend on the full backup will be processed according to the retention policy specified for the full backup.

Alternatively, if you enable retention policy for multiple types of backups of the same database, you must specify the same number of days to keep restore points in the backup chain for each backup type. Otherwise, Veeam Plug-in will keep restore points according to the lowest number. For example, you set Veeam Plug-in to keep full backups for 7 days and differential backups for 3 days. In this case, Veeam Plug-in will remove inactive backup chains whose restore points are older than 3 days.

If you do not specify the retention policy for any type of Microsoft SQL Server backup, Veeam Plug-in will not remove outdated restore points, and backup files fill remain in the backup repository.

You can also manually delete Veeam Plug-in backups from a backup repository using the Veeam Backup & Replication console. For details, see: Deleting Backup.

Support for SQL Server Failover Clusters

Veeam Plug-in supports backup and restore of Microsoft SQL Server databases that operate as part of a failover cluster. Both Windows Server Failover Clusters with shared disks and Windows Server Failover Clusters with Cluster Shared Volumes (CSV) are supported.

To back up databases that operate as part of a failover cluster, do the following:

1. Install and configure Veeam Plug-in for Microsoft SQL Server on each node of the cluster. For more information, see Installing Veeam Plug-in for Microsoft SQL Server and Configuring Veeam Plug-in for Microsoft SQL Server.
2. Using Failover Cluster Manager, configure backup settings in Veeam Plug-in on the active cluster node. For more information, see Configuring Backup Settings.

   On the passive node, the Microsoft SQL Server instance that operates as part of the cluster is not displayed in the Veeam Plug-in UI.
3. Save backup settings as an SQL Agent job in Microsoft SQL Server Management Studio. For more information, see Saving Backup Settings as SQL Agent Job.

Veeam Plug-in for Microsoft SQL Server will start the backup job on the active cluster node.

To restore a database that operates as part of a failover cluster, you must start the restore process on the active cluster node. On the passive node, the backed-up Microsoft SQL Server instance is not displayed in the Veeam Plug-in UI.

Support for Always On Availability Groups

Veeam Plug-in supports backup and restore of Microsoft SQL Server databases that operate as part of an Always On availability group.

The following types of availability groups are supported:

- Always On Availability Groups
- Always On Clusterless Availability Groups

To back up databases that operate as part of an Always On availability group, do the following:

1. Install and configure Veeam Plug-in for Microsoft SQL Server on each node of the cluster that runs Always On Availability Groups. For more information, see Installing Veeam Plug-in for Microsoft SQL Server and Configuring Veeam Plug-in for Microsoft SQL Server.
2. Configure backup settings in Veeam Plug-in on each node and save backup settings as SQL Agent jobs in Microsoft SQL Server Management Studio. For more information, see Configuring Backup Settings and Saving Backup Settings as SQL Agent Job.
3. In Microsoft SQL Server Management Studio on each node, configure the same schedule settings for SQL Agent jobs so that database backup will start at the same time on each node.

Veeam Plug-in for Microsoft SQL Server performs backup of Always On Availability Groups in the following way:

1. When the SQL Agent job starts, Veeam Plug-in checks backup preferences specified in the properties of the Always On availability group.
2. If the node on which the SQL Agent job is running is the preferred node for backup, Veeam Plug-in performs backup. Otherwise, the backup process stops.

Consider the following:

- Veeam Plug-in does not check backup preferences of the Always On availability group if you start the backup process manually from the Veeam Plug-in UI.
- On secondary replicas, only full copy-only backup and log backup are supported. Differential backup is not supported.
- Veeam Plug-in does not add a restored database to an Always On availability group. You must perform this operation manually after the restore process is completed. For details, see Restore of Always On Availability Groups.

Restore of Always On Availability Groups

To restore a database that operates as part of an Always On availability group, complete the following steps:

1. Restore the database on the primary replica. During the restore process, Veeam Plug-in will remove the original database from the availability group and delete it from Microsoft SQL Server.
2. Perform log backup for the restored database.
3. Remove the original database from the secondary replica.
4. Add the restored database to the availability group.

Veeam Backup Repositories

Veeam Plug-ins store backup files in repositories added to the Veeam Backup & Replication infrastructure. This section lists supported types of backup repositories and limitations for Veeam Plug-in for Microsoft SQL Server backups.

Supported Backup Repositories

Veeam Plug-in for Microsoft SQL Server supports integration with the following types of repositories added to the Veeam Backup & Replication infrastructure:

- Windows Server
- Linux Server
- CIFS (SMB) Share
- Dell Data Domain Boost
- Quantum DXi
- ExaGrid
- HPE StoreOnce. If you plan to use HPE StoreOnce as a backup repository for Veeam Plug-in backups, the total number of stored files (data and metadata) must not exceed 3,000,000 per Catalyst store. If necessary, multiple Catalyst stores may be created on the same StoreOnce system.
- NFS File Share
- Hardened Repository

You can also use scale-out backup repositories that contain supported repository types.

Backup Repository Limitations

- For Veeam Plug-in backups, the warning which indicates that free space on a storage device has reached a specified threshold is configured in the `veeam_config.xml` file of Veeam Plug-in. The warning settings in the Veeam Backup & Replication console does not affect this setting.

  To configure the warning settings, add the following parameter in the `veeam_config.xml` file.

  ```
  <PluginParameters repositoryFreeSpacePercentWarning="10" />
  ```

- The plug-in configuration wizard will not show repositories where the **Encrypt backups stored in this repository** option is enabled. To learn how to disable the encryption option, see Access and Encryption Settings on Repositories.

  If you want to use the same backup target with the repository-based encryption and Veeam Plug-ins, create a second repository in the subfolder for Veeam Plug-in backups.

- Veeam extract utility cannot extract Veeam Plug-in backup files. By design of Microsoft SQL Server, these files cannot be imported “as files” to RMAN as they contain additional metadata bound to the used SBT device.

Veeam Scale-Out Backup Repositories

If you want to store Veeam Plug-in backups in scale-out backup repositories, mind the following:

- If you want to add a backup repository as an extent to a scale-out backup repository and Veeam Plug-in backups are present on this backup repository, you must do the following:

  a. In the Veeam Backup & Replication console, select Veeam Plug-in backup files that reside in this backup repository and remove them from configuration. For details, see Removing Backups from Configuration. Note that this action does not delete the backups from the repository.

  b. In the Veeam Backup & Replication console, delete the Veeam Plug-in backup job. For details, see Deleting Jobs.

  c. Add the repository as an extent to the scale-out repository. For details, see Extending Scale-Out Repositories.

  d. Rescan the scale-out repository. For details, see Rescanning Scale-Out Repositories.

  > NOTE
  >
  > Names of backup files and paths to backup files must contain only allowed characters:
  >
  > - Alphanumeric characters: `a-zA-Z0-9`
  > - Special characters: `_-.+=@^`
  > - Names of backup files and paths to backup files must not contain spaces.

  e. On the Veeam Plug-in server, set the scale-out repository as the target for backups using the following command:

  ```
  MSSQLConfigTool --set-repositories
  ```

f. Map the imported backups using the following command:

```
MSSQLConfigTool --map-backup
```

- For Veeam Plug-in backups and backup copies, the *Performance* policy of a scale-out repository functions differently:

  a. Veeam Backup & Replication checks if there are extents without warning on free space insufficiency. If all extents have the warning, Veeam Backup & Replication uses an extent with the largest amount of free space that has a free task slot.

  b. If there are extents without the warning, Veeam Backup & Replication checks if there are incremental extents with free task slots. If there are no incremental extents with free task slots, Veeam Backup & Replication uses a full extent with the least amount of used task slots.

  c. If there are incremental extents with free task slots, Veeam Backup & Replication sends backup files to an incremental extent with the least amount of used task slots. If the amount of used tasks is the same, an extent with the largest amount of free space.

  To learn more about file placement policies of scale-out repositories, see Backup File Placement section of the Veeam Backup & Replication guide.

- If a scale-out repository is configured in the **Data locality** policy, repository extents will be selected according to the amount of free space for each Microsoft SQL Server connection. If there are two extents with one slot on each extent, the backup will be launched on two streams (one on each extent).

Capacity Tier

You can configure Veeam Backup & Replication to transfer Veeam Plug-in backup files to the capacity tier. Both policies (Move policy, Copy policy) are supported for Veeam Plug-in backups with the following limitations:

- For Veeam Plug-in backup files, capacity tier does not verify whether data that is being moved is unique and has not been offloaded earlier. Thus, it is highly recommended to check the pricing plans of your cloud storage provider to avoid additional costs for offloading and downloading backup data.

- [For the Move policy] For Veeam Plug-in for Microsoft SQL Server backups, capacity tier tracks dependencies of full and differential backup files. Thus, Veeam Backup & Replication tracks inactive backup chains and moves them to the capacity tier. No limitations apply to the operational restore window.

- [For the Copy policy] For Veeam Plug-in for Microsoft SQL Server backups, Veeam Backup & Replication copies to the capacity tier only those backup files for which 24 hours have passed since the backup file was created.

- If a scale-out repository is down, you cannot restore from the Veeam Plug-in backup files stored on the capacity tier. In this case, you can only import the backup files to Veeam Backup & Replication manually and then perform data recovery operations.

- If you use a capacity tier that has been created in Veeam Backup & Replication version 10, you cannot transfer Veeam Plug-in backup files to a capacity tier. However, if you want to transfer them manually, do the following:

  a. If the backup files are created by Veeam Plug-in version 10, upgrade the metadata of backup files as described in Upgrading Metadata Files to New Format.

  b. Run the Set-VBRScaleOutBackupRepository PowerShell command with the –`EnablePluginBackupOffload` parameter to offload backup files to the capacity tier.

Hardened Repository

You can configure Veeam Backup & Replication to transfer Veeam Plug-in backup files to a hardened repository. The hardened repository helps to protect Veeam Plug-in backup files from loss as a result of malware activity or unplanned actions. Backup files in the hardened repository become immutable for the time period specified in the backup repository settings. During this period, backup files stored in the repository cannot be modified or deleted.

For Veeam Plug-in for Microsoft SQL Server backups, immutability works according to the following rules:

- Immutability is applied to backup (VAB) files and backup metadata (VASM) files. Backup job metadata (VACM) files are not immutable.
- Backup files become immutable for the configured time period (minimum 7 days, maximum 9999 days).
- The count of the immutability period starts after 24 hours have passed since the backup file was created. Every 1 hour, the immutability service that runs in the background detects backup files that are older than 24 hours and sets the immutability flag on such backup files.
- The immutability period is automatically extended for backup files that contain restore points of the active chain.

Data Restore from Hardened Repository

As a result of malware activity or unplanned actions, backup job metadata (VACM) files may become unavailable in the hardened repository. In this case, to restore data from the hardened repository, you must re-create the VACM file. To do this, complete the following steps:

1. Run a Veeam Plug-in backup job to create a new Veeam Plug-in backup in a Veeam backup repository. The backup will consist of the VAB, VASM and VACM files.
2. In the backup repository folder, replace the VAB and VASM files created at the step 1 with the VAB and VASM files from the hardened repository.
3. In the Veeam backup console, run the backup repair operation. Veeam Backup & Replication will generate a new VACM file using information from the VASM files. For details, see Repairing Backup.

Once the backup job metadata file is re-created, you can use Veeam Plug-in to restore your data.

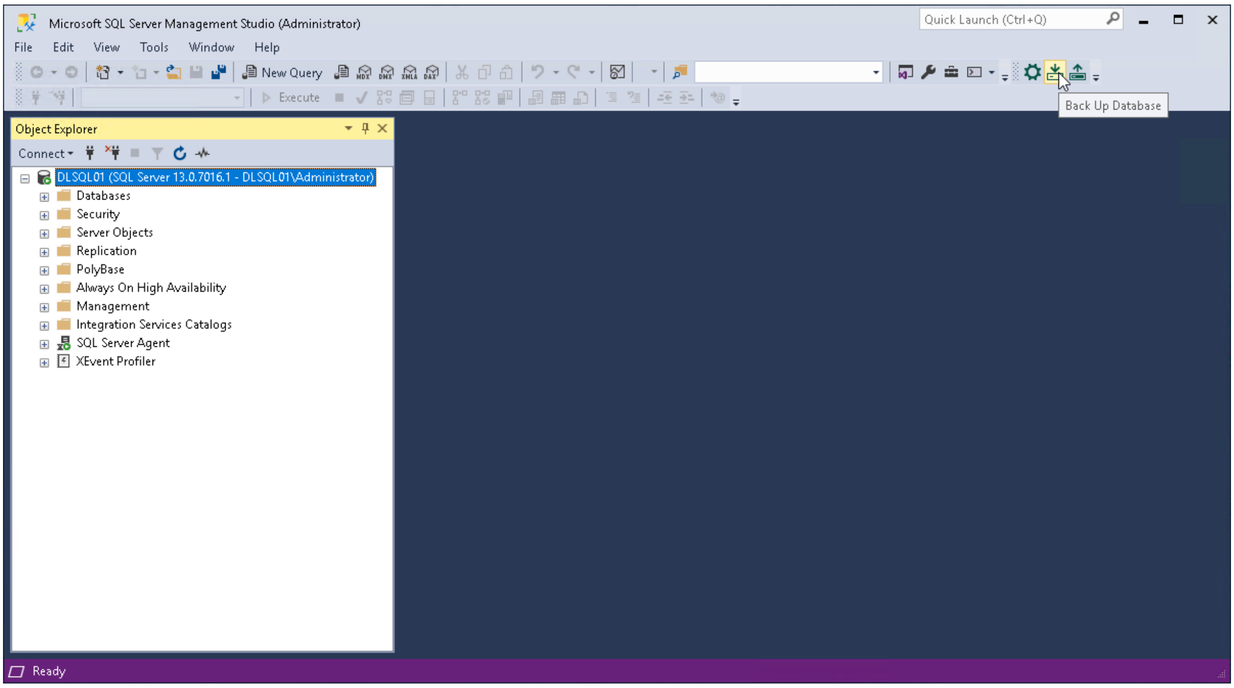
Configuring Backup Settings

To back up Microsoft SQL Server data with Veeam Plug-in, you must configure backup settings. You can select what databases to back up, choose the backup type, specify data retention and data processing settings.

Step 1. Launch Backup Wizard

To launch the **Back Up Database** wizard, on the Microsoft SQL Server machine do either of the following:

- Click the **Back Up Database** icon on the desktop.
- From the Microsoft Windows **Start** menu, select **All Programs** > **Veeam** > **Back Up Database** or use the Microsoft Windows search to find the **Back Up Database** option on your machine.
- In Microsoft SQL Server Management Studio, click the **Back Up Database** button on the toolbar.
- Launch the `%PROGRAMFILES%\Veeam\Plugins\Microsoft SQL\Veeam.Backup.MSSQLPlugin.UI.Backup.exe` file.



Step 2. Select Databases to Back Up

At the **Databases** step of the wizard, select Microsoft SQL Server databases that you want to back up:

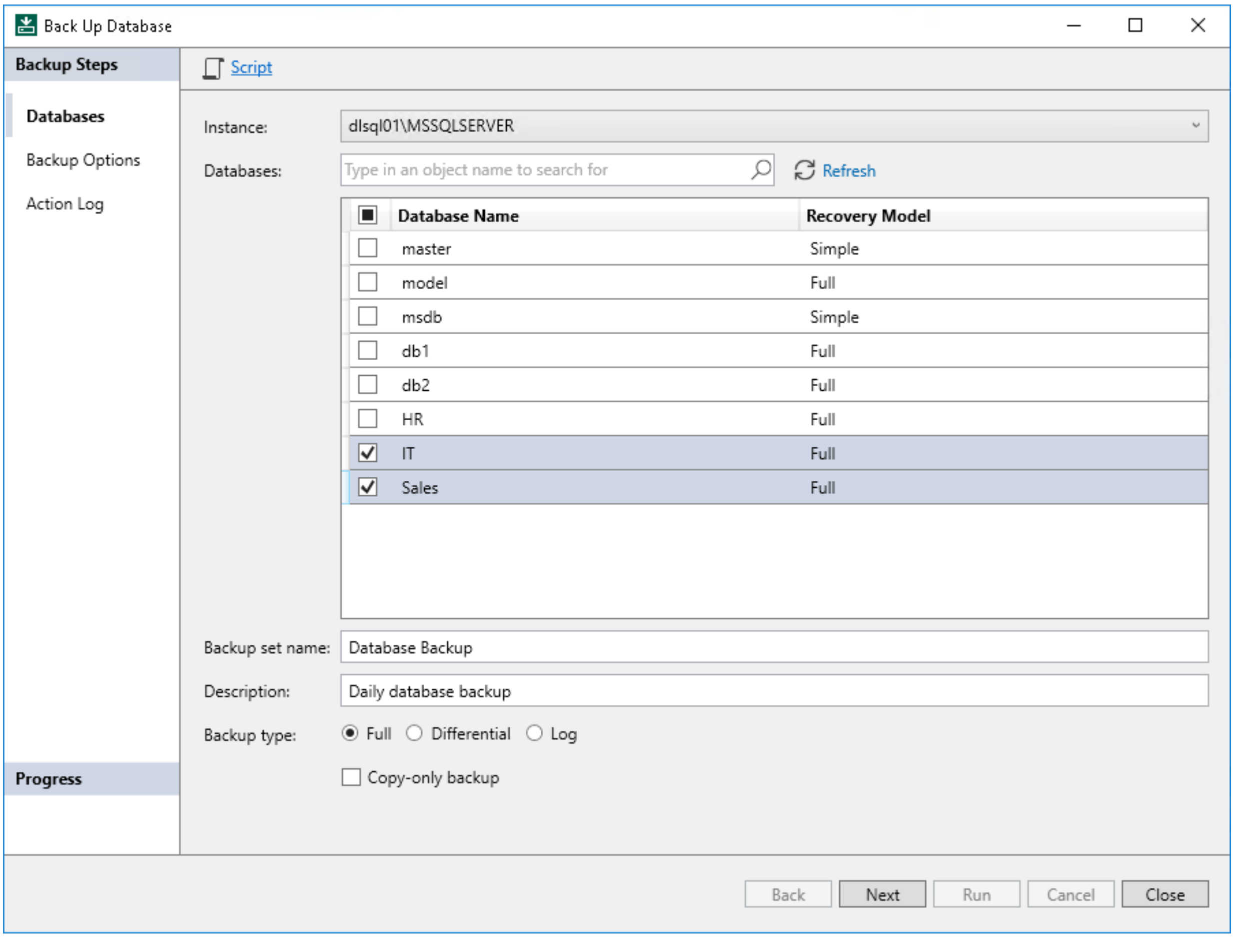
1. From the **Instance** drop-down list, select the Microsoft SQL Server instance whose databases you want to back up.
2. In the **Databases** section, select check boxes next to the necessary databases. Alternatively, if you want to back up all databases of the selected instance, select the check box next to the **Database Name** column name.

   To quickly find the necessary databases, you can type the name of the database in the search field and click the search icon.

   To refresh the list of databases, click **Refresh**. When you refresh the list of databases, Veeam Plug-in will clear check boxes next to the selected databases.
3. In the **Backup set name** field, specify the name for the backup set. This will help you identify databases in case you need to restore a database from the backup.
4. In the **Description** field, specify description for the backup set. The name and description of the backup set will be displayed in the **Restore Database** wizard during restore.
5. In the **Backup type** section, select the type of backup you want to create. You can select from the following native Microsoft SQL Server backup types:
   - **Full** — select this option if you want to create a backup that will contain a full copy of the Microsoft SQL Server database.
   - **Differential** — select this option if you want to create a backup that will contain changes since the previous backup was created.
   - **Log** — select this option if you want to create a backup of Microsoft SQL Server transaction logs.
6. If you selected the **Full** or **Log** option and want to create a copy-only full backup or copy-only log backup, select the **Copy-only backup** check box. For example, you may want to create copy-only log backups if you use a separate solution to process Microsoft SQL Server transaction logs.

TIP

At this step of the wizard, you can also export backup settings to a custom script. You will be able to use this script with a third-party scheduling tool. For details, see Exporting Backup Settings to Custom Script.



Instance: dlsql01\MSSQLSERVER

Databases: Type in an object name to search for

■	Database Name	Recovery Model
□	master	Simple
□	model	Full
□	msdb	Simple
□	db1	Full
□	db2	Full
□	HR	Full
☑	IT	Full
☑	Sales	Full

Backup set name: Database Backup

Description: Daily database backup

Backup type: ● Full ○ Differential ○ Log

□ Copy-only backup

Step 3. Specify Backup Options

At the **Backup Options** step of the wizard, specify data retention settings and data processing settings according to which you want to perform backup, and start the backup process:

1. [Optional] To specify data retention settings, in the **Retention** section, do the following:

   a. Select the **Apply retention policy** check box.

   b. In the **Delete backups older than <N> days** field, specify the number of days for which you want to keep backups in the backup repository. By default, Veeam Plug-in keeps backup files for 7 days.

2. [Optional] To specify settings for data processing during the backup process, in the **Database processing** section, do the following:

   a. In the **Concurrent backup streams** field, specify the number of data streams over which you want to back up Microsoft SQL Server data. For each backup stream, a separate VDI Device is started on the Microsoft SQL Server machine.

   b. If you want to apply Veeam Backup & Replication mechanisms of data compression to the backup, select the **Use compression** check box. To Veeam Plug-in for Microsoft SQL Server backups, the *Optimal* (LZ4) compression level is applied.

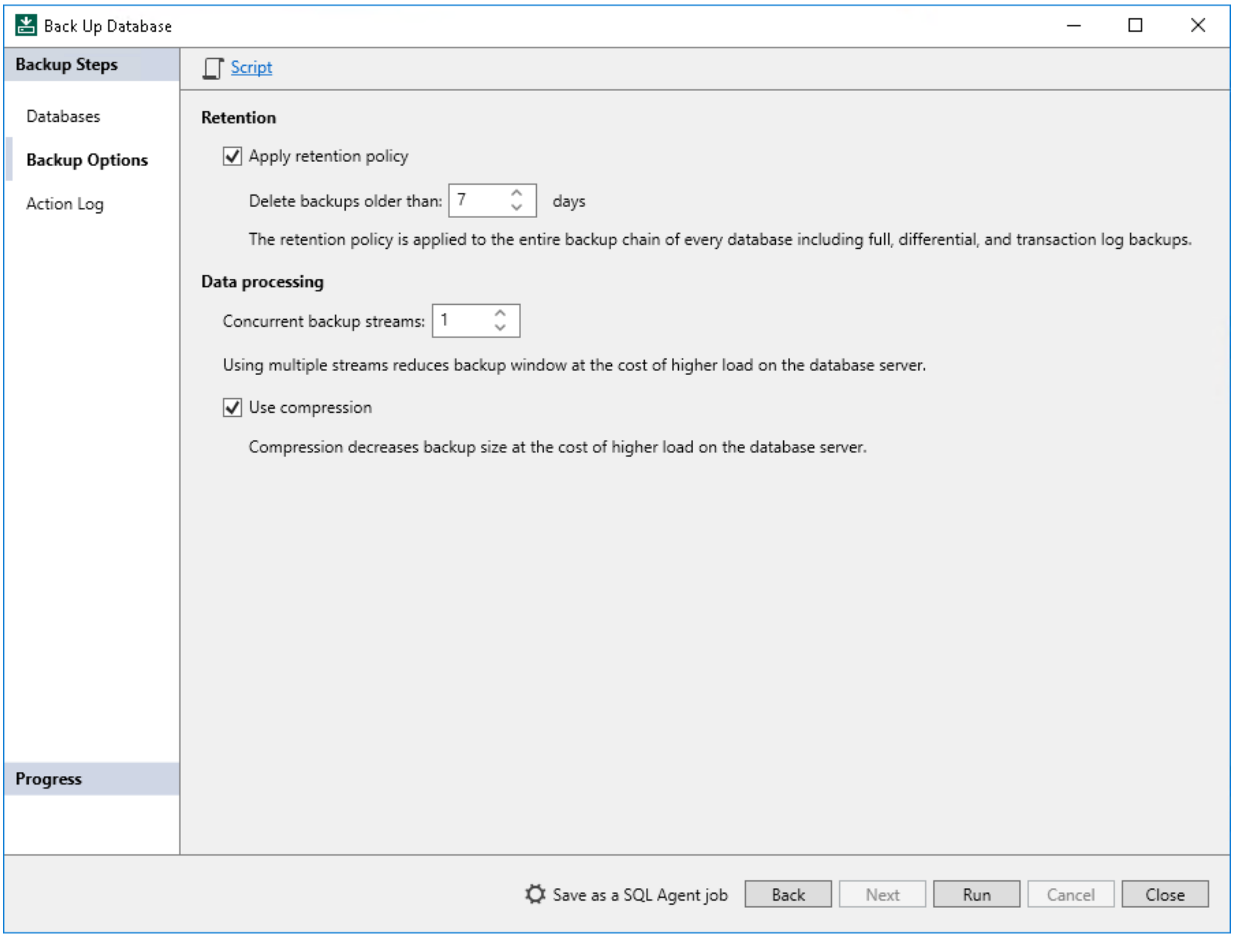
3. Click **Run** to start the backup process.

   You can start the backup process if you want to create a backup immediately or if you want to check that backup process with the specified settings performs successfully.

   If you want Veeam Plug-in to perform backup with the specified settings regularly, you can also perform one of the following operations:

   - If you want to save backup settings as an SQL Agent job to be able to specify schedule for the backup job in Microsoft SQL Server Management Studio, click **Save as a SQL Agent Job**. For details, see Saving Backup Settings as SQL Agent Job.
   - If you want to export backup settings to a custom script and use this script with a third-party scheduling tool, click **Script**. For details, see Exporting Backup Settings to Custom Script.

   If you do not want to start the backup process immediately, click **Close** to exit the wizard.



Back Up Database

Backup Steps: Databases, **Backup Options**, Action Log, Progress

Script

Retention

☑ Apply retention policy

Delete backups older than: 7 days

The retention policy is applied to the entire backup chain of every database including full, differential, and transaction log backups.

Data processing

Concurrent backup streams: 1

Using multiple streams reduces backup window at the cost of higher load on the database server.

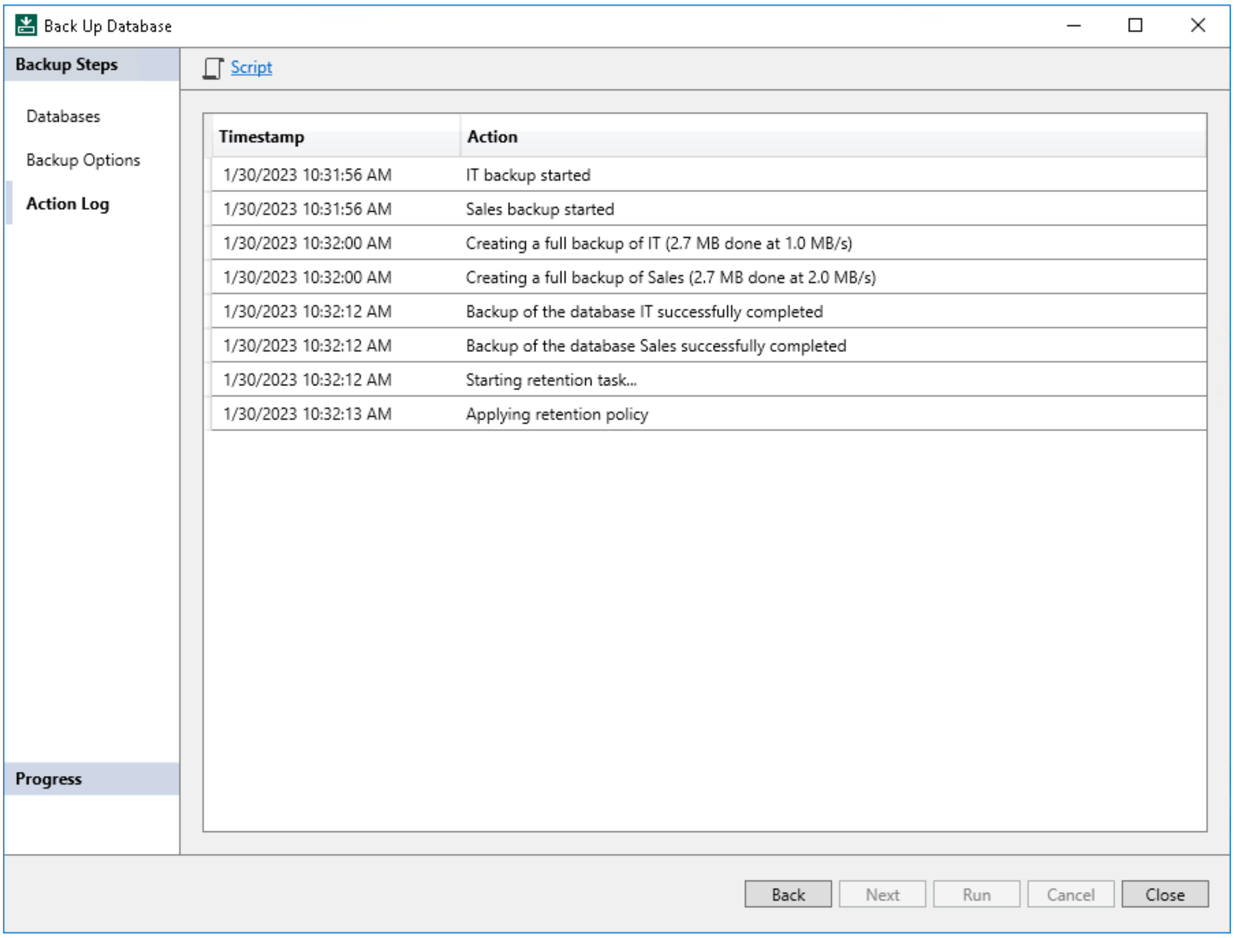
☑ Use compression

Compression decreases backup size at the cost of higher load on the database server.

Step 4. Monitor Backup Process

If you started the backup process at the **Backup Options** step of the wizard, at the **Action Log** step of the wizard review the list of backup operations and click **Close** to exit the wizard.

> TIP
>
> At this step of the wizard, you can also save backup settings as an SQL Agent job. You will be able to specify schedule for the backup job in Microsoft SQL Server Management Studio. For details, see Saving Backup Settings as SQL Agent Job.



Timestamp	Action
1/30/2023 10:31:56 AM	IT backup started
1/30/2023 10:31:56 AM	Sales backup started
1/30/2023 10:32:00 AM	Creating a full backup of IT (2.7 MB done at 1.0 MB/s)
1/30/2023 10:32:00 AM	Creating a full backup of Sales (2.7 MB done at 2.0 MB/s)
1/30/2023 10:32:12 AM	Backup of the database IT successfully completed
1/30/2023 10:32:12 AM	Backup of the database Sales successfully completed
1/30/2023 10:32:12 AM	Starting retention task...
1/30/2023 10:32:13 AM	Applying retention policy

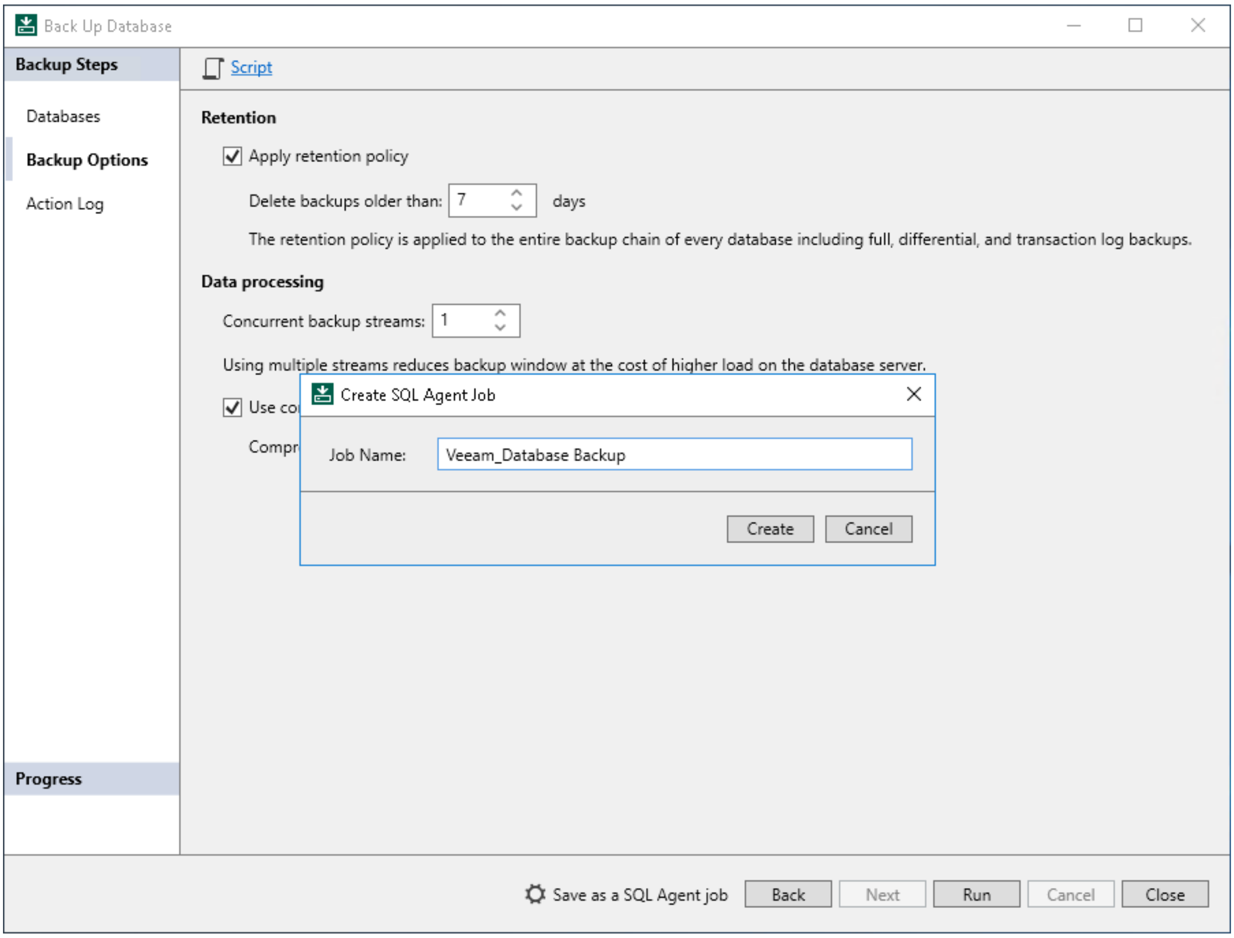
Saving Backup Settings as SQL Agent Job

You can save backup settings specified for Veeam Plug-in for Microsoft SQL Server as an SQL Agent job. This may be helpful if you have Microsoft SQL Server Management Studio in your environment and want to use its functionality to apply schedule to a Microsoft SQL Server backup job.

To save backup settings as an SQL Agent job:

1. At the **Backup Options** step of the **Back Up Database** wizard, click **Save as a SQL Agent Job**.
2. In the **Create SQL Agent Job** window, specify the name for the SQL Agent job and click **Create**.

The SQL Agent job will become available in the **Jobs** node in Microsoft SQL Server Management Studio, and you will be able to specify schedule in the job properties.



Retention

☑ Apply retention policy

Delete backups older than: 7 days

The retention policy is applied to the entire backup chain of every database including full, differential, and transaction log backups.

Data processing

Concurrent backup streams: 1

Using multiple streams reduces backup window at the cost of higher load on the database server.

☑ Use co

Compr

Create SQL Agent Job

Job Name: Veeam_Database Backup

Exporting Backup Settings to Custom Script

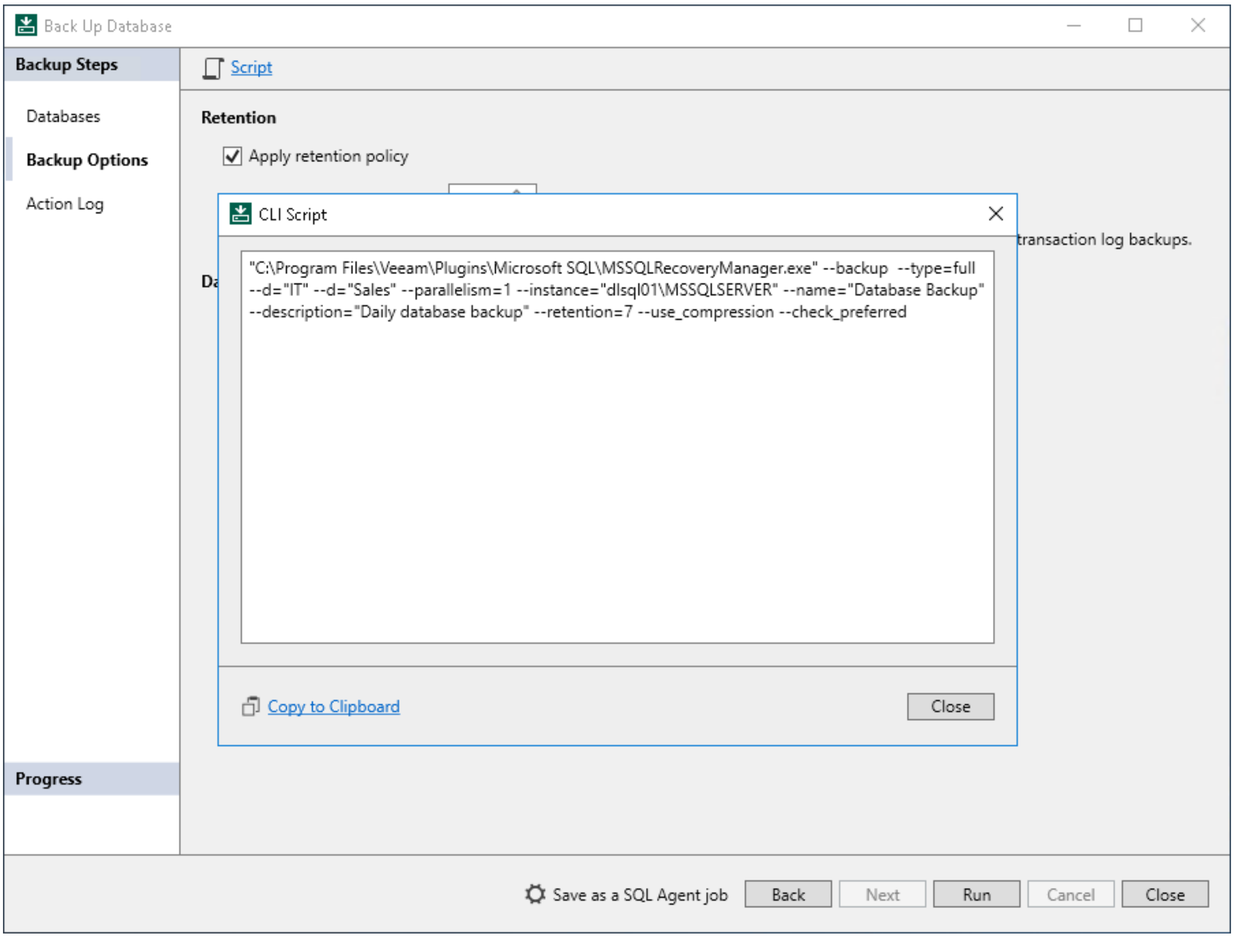
You can export backup settings specified for Veeam Plug-in for Microsoft SQL Server to a custom script. This may be helpful if you want to back up Microsoft SQL Server databases using a third-party scheduling tool.

To export backup settings to a custom script:

1. At the **Databases**, **Backup Options** or **Action Log** step of the **Back Up Database** wizard, click **Script**.
2. In the **CLI Script** window, review the command to back up Microsoft SQL Server data and click **Copy to Clipboard**.

You will be able to use the command in a custom script with an external scheduling tool.

> **TIP**
>
> You can modify parameters of the command used to back up Microsoft SQL Server data if necessary. For information about available backup parameters, see Performing Backup with Command-Line Interface.



```
"C:\Program Files\Veeam\Plugins\Microsoft SQL\MSSQLRecoveryManager.exe" --backup  --type=full
--d="IT" --d="Sales" --parallelism=1 --instance="dlsql01\MSSQLSERVER" --name="Database Backup"
--description="Daily database backup" --retention=7 --use_compression --check_preferred
```

Performing Backup with Command-Line Interface

You can perform backup of Microsoft SQL Server databases with Veeam Plug-in using the command-line interface.

To perform backup, do the following:

1. On the Microsoft SQL Server machine, navigate to the `%PROGRAMFILES%\Veeam\Plugins\Microsoft SQL\` folder.
2. Run the `MSSQLRecoveryManager.exe` command with the required parameters. For more information, see Backup Parameters.

   The following example shows a command to perform full backup of Microsoft SQL Server databases:

   ```
   MSSQLRecoveryManager.exe --backup --name="Database Backup" --description="
   Daily database backup" --type=full --d="IT" --d="Sales" --parallelism=2 --
   instance="dlsql01\MSSQLSERVER" --name="Database Backup" --description="Dai
   ly full database backup" --retention=5 --use_compression --check_preferred
   ```

   > **TIP**
   >
   > You can also use the available backup parameters to modify Veeam Plug-in for Microsoft SQL Server commands used in custom scripts. For information, see Exporting Backup Settings to Custom Script.

Backup Parameters

You can specify the following parameters for backup of Microsoft SQL Server databases with the `MSSQLRecoveryManager.exe` command:

Command	Description
--help	Shows the list of parameters for the `MSSQLRecoveryManager.exe` command.
--backup	Defines the backup operation.
--instance	Specifies the name of the Microsoft SQL Server instance whose databases you want to back up.

Command	Description
--d	Specifies the name of the database to back up. This parameter is optional. If you do not use this parameter, Veeam Plug-in will back up all databases of the specified instance. Alternatively, if you want to back up all databases of the instance except for the specified one, you can use the `--ed` parameter and specify the necessary database as its value.
--ed	Specifies the name of the database that must be excluded from the backup. This parameter is optional. If you do not use this parameter, Veeam Plug-in will back up all databases of the specified instance. Alternatively, if you want to back up a specific database, you can use the `--d` parameter and specify the necessary database as its value.
--name	Specifies the name for the backup set.
--description	Specifies the description for the backup set.
--type	Specifies the backup type. Possible values: • *full* — full backup • *diff* — differential backup • *log* — log backup
--copy-only	Defines the copy-only backup mode. You can use this parameter to create copy-only full backups or copy-only log backups of Microsoft SQL Server databases.
--parallelism	Specifies the number of parallel data streams over which you want to back up Microsoft SQL Server data. For each backup stream, a separate VDI Device is started on the Microsoft SQL Server machine.
--retention	Specifies the number of days to keep backups in the backup repository. This parameter is optional. If you do not use this parameter, Veeam Plug-in will not apply the retention policy to the backup.

Command	Description
--check_preferred	[For backup of Always On Availability Groups] Defines that Veeam Plug-in will check whether the availability replica is the preferred replica for backup.
--use_compression	Defines that Veeam Backup & Replication mechanisms of data compression will be applied to the backup. To Veeam Plug-in for Microsoft SQL Server backups, the Optimal (LZ4) compression level is applied.

Managing Backup Job in Veeam Backup & Replication

After Veeam Plug-in for Microsoft SQL Server starts the backup process, Veeam Backup & Replication creates the backup job. You can use this job to view statistics on the backup process and generate backup job reports. You can also disable the backup job.

You cannot start or edit Microsoft SQL Server backup jobs in the Veeam Backup & Replication console. You can manage backup operations on the Microsoft SQL Server machine only.

Consider the following:

- Veeam Backup & Replication creates one backup job for a standalone Microsoft SQL Server, Microsoft SQL Server failover cluster or Always On availability group. All backup sessions for different databases that reside on this server, cluster or availability group run within this backup job.
- Veeam Backup & Replication generates names for Microsoft SQL Server backup jobs according to the following rules:
  - For standalone Microsoft SQL Server, Veeam Backup & Replication generates the backup job name based on the names of the Microsoft SQL Server machine and backup repository where Veeam Plug-in creates Microsoft SQL Server backups.
  - For Microsoft SQL Server that operates as part of a failover cluster or availability group, Veeam Backup & Replication generates the backup job name based on the name of the cluster or name of the availability group.

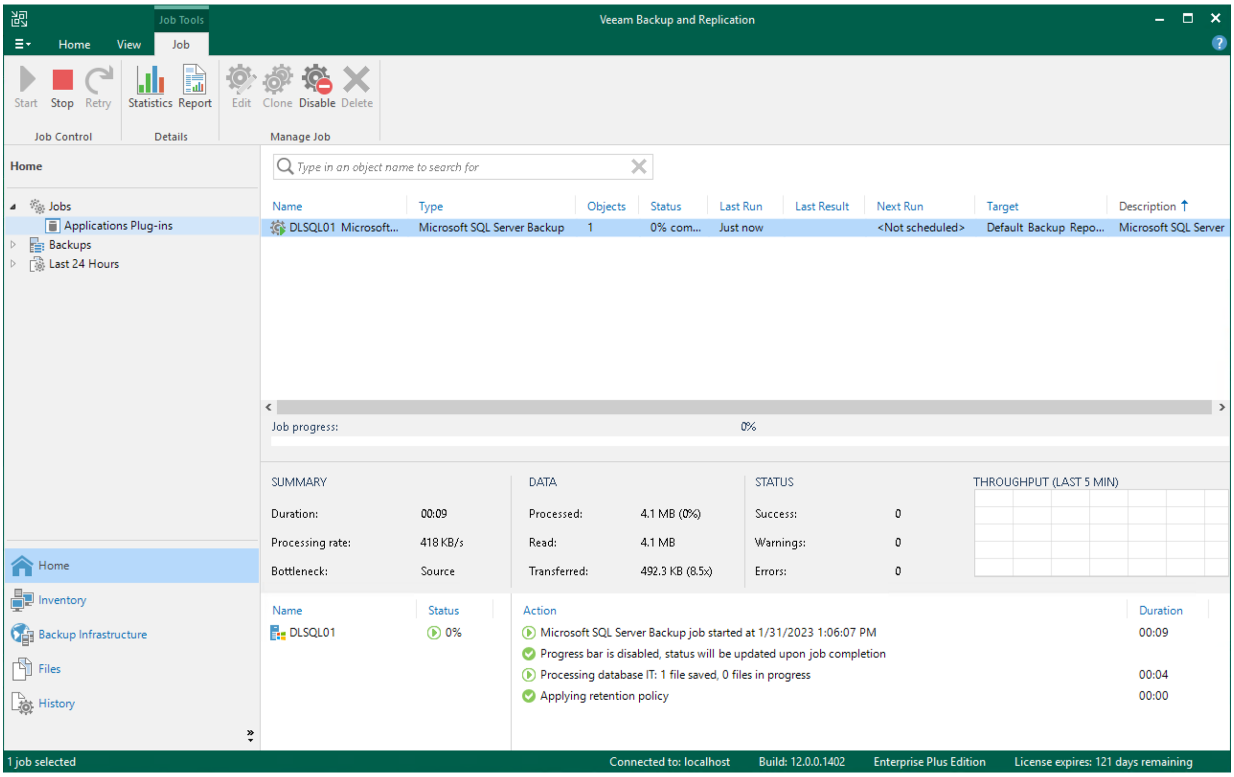
Viewing Backup Job Statistics

To view details of the backup process, do the following:

1. Open the Veeam Backup & Replication console.
2. In the **Home** view, expand the **Jobs** node in the inventory pane and click **Applications Plug-ins**.
3. In the working area, select the Microsoft SQL Server backup job to see details of the current backup process or the last backup job session.

NOTE

Veeam Backup & Replication does not display the progress bar for a running Veeam Plug-in for Microsoft SQL Server backup job. Statistics for backup jobs of this type becomes available after the backup job session is completed.



Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target	Description
DLSQL01 Microsoft...	Microsoft SQL Server Backup	1	0% com...	Just now		<Not scheduled>	Default Backup Repo...	Microsoft SQL Server

Job progress: 0%

SUMMARY		DATA		STATUS	
Duration:	00:09	Processed:	4.1 MB (0%)	Success:	0
Processing rate:	418 KB/s	Read:	4.1 MB	Warnings:	0
Bottleneck:	Source	Transferred:	492.3 KB (8.5x)	Errors:	0

Name	Status
DLSQL01	0%

Action	Duration
Microsoft SQL Server Backup job started at 1/31/2023 1:06:07 PM	00:09
Progress bar is disabled, status will be updated upon job completion	
Processing database IT: 1 file saved, 0 files in progress	00:04
Applying retention policy	00:00

1 job selected

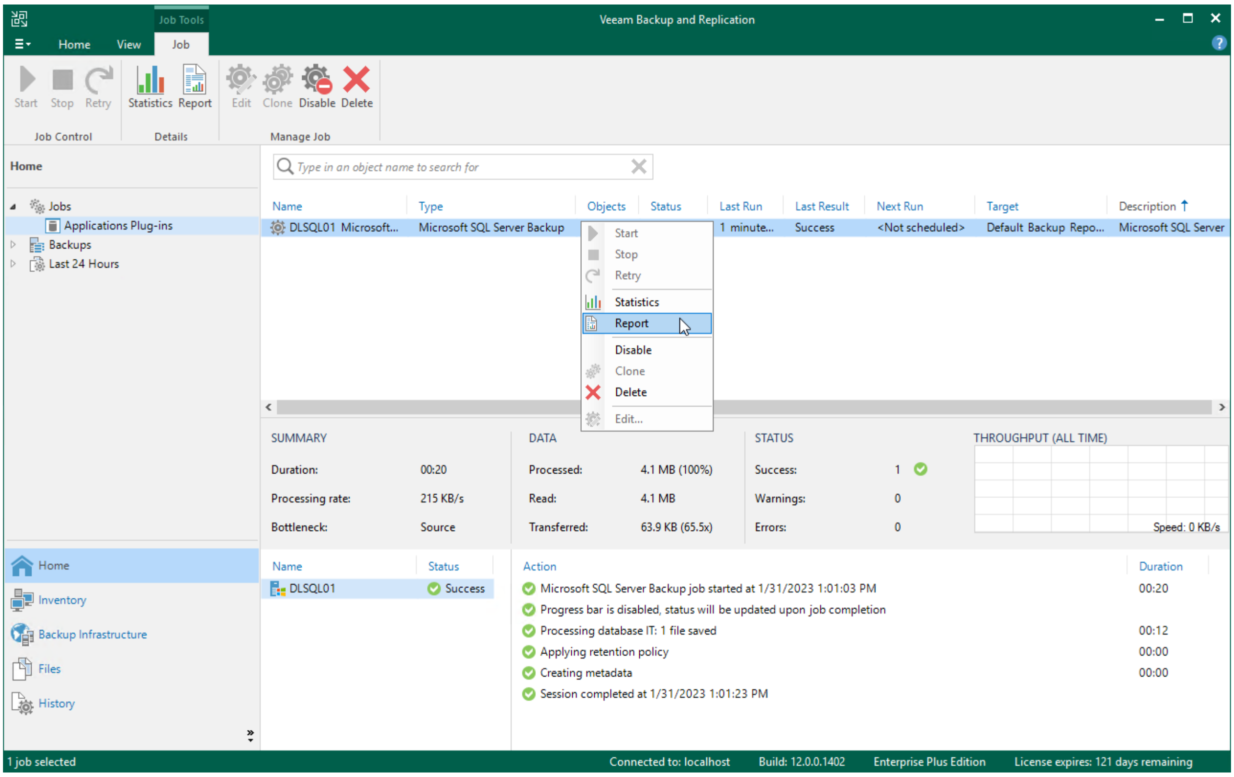
Connected to: localhost Build: 12.0.0.1402 Enterprise Plus Edition License expires: 121 days remaining

Generating Backup Job Reports

Veeam Backup & Replication can generate reports with details about Microsoft SQL Server backup job session performance. The session report contains the following session statistics: session duration details, details of the session performance, amount of read, processed and transferred data, backup size, compression ratio, list of warnings and errors (if any).

To generate a report, do the following:

1. Open the Veeam Backup & Replication console.
2. In the **Home** view, expand the **Jobs** node in the inventory pane and click **Applications Plug-ins**.
3. In the working area, select the necessary job and click **Report** on the ribbon. You can also right-click the job and select **Report**.



Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target	Description
DLSQL01 Microsoft...	Microsoft SQL Server Backup			1 minute...	Success	<Not scheduled>	Default Backup Repo...	Microsoft SQL Server

SUMMARY		DATA		STATUS	
Duration:	00:20	Processed:	4.1 MB (100%)	Success:	1 ✓
Processing rate:	215 KB/s	Read:	4.1 MB	Warnings:	0
Bottleneck:	Source	Transferred:	63.9 KB (65.5x)	Errors:	0

Name	Status
DLSQL01	✓ Success

Action	Duration
✓ Microsoft SQL Server Backup job started at 1/31/2023 1:01:03 PM	00:20
✓ Progress bar is disabled, status will be updated upon job completion	
✓ Processing database IT: 1 file saved	00:12
✓ Applying retention policy	00:00
✓ Creating metadata	00:00
✓ Session completed at 1/31/2023 1:01:23 PM	

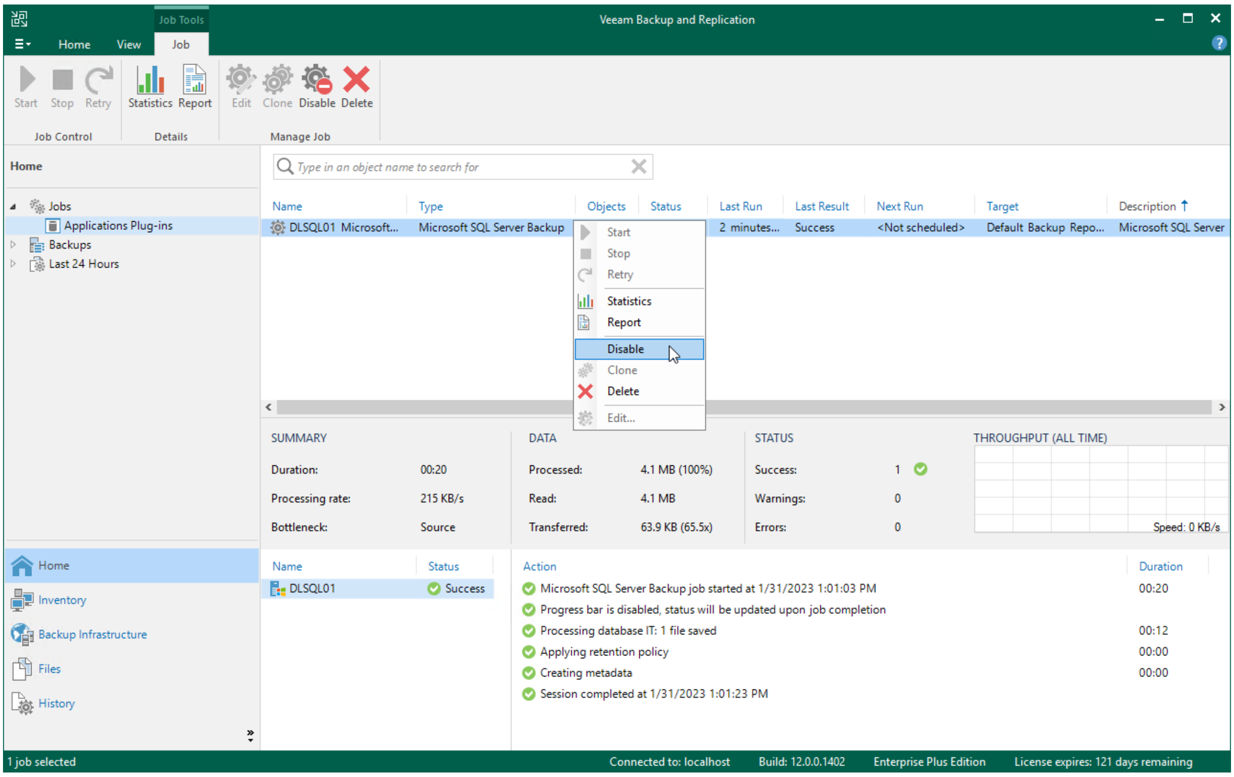
1 job selected — Connected to: localhost — Build: 12.0.0.1402 — Enterprise Plus Edition — License expires: 121 days remaining

Disabling Backup Job

You can disable Microsoft SQL Server backup jobs in the Veeam Backup & Replication console. If you disable the job, you will not be able to run Veeam Plug-in backup commands on the Microsoft SQL Server machine.

To disable a backup job, do the following:

1. Open the Veeam Backup & Replication console.
2. In the **Home** view, expand the **Jobs** node in the inventory pane and click **Applications Plug-ins**.
3. In the working area, select the necessary job and click **Disable** on the ribbon. You can also right-click the job and select **Disable**.



Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target	Description
DLSQL01 Microsoft...	Microsoft SQL Server Backup			2 minutes...	Success	<Not scheduled>	Default Backup Repo...	Microsoft SQL Server

SUMMARY
Duration: 00:20
Processing rate: 215 KB/s
Bottleneck: Source

DATA
Processed: 4.1 MB (100%)
Read: 4.1 MB
Transferred: 63.9 KB (65.5x)

STATUS
Success: 1
Warnings: 0
Errors: 0

THROUGHPUT (ALL TIME)
Speed: 0 KB/s

Name	Status
DLSQL01	Success

Action	Duration
Microsoft SQL Server Backup job started at 1/31/2023 1:01:03 PM	00:20
Progress bar is disabled, status will be updated upon job completion	
Processing database IT: 1 file saved	00:12
Applying retention policy	00:00
Creating metadata	00:00
Session completed at 1/31/2023 1:01:23 PM	

1 job selected   Connected to: localhost   Build: 12.0.0.1402   Enterprise Plus Edition   License expires: 121 days remaining

Managing Veeam Plug-in Backups in Veeam Backup & Replication

In the Veeam Backup & Replication console, backups created by Veeam Plug-ins are displayed in the **Backups** > **Disk** node of the **Home** view. For backups created by Veeam Plug-in for Microsoft SQL Server, consider the following:

- In the working area, backups created by Microsoft SQL Server are listed under the **Microsoft SQL** node.
- In the list of Microsoft SQL Server backups, Veeam Backup & Replication displays one backup for a standalone Microsoft SQL Server, Microsoft SQL Server failover cluster or Always On availability group. This backup contains all restore points created for different databases that reside on this server, cluster or availability group.
- Veeam Backup & Replication generates names for Microsoft SQL Server backups according to the following rules:
    - For standalone Microsoft SQL Server, Veeam Backup & Replication generates the backup name based on name of the Microsoft SQL Server machine.
    - For Microsoft SQL Server that operates as part of a failover cluster or availability group, Veeam Backup & Replication generates the backup name based on the name of the cluster or name of the availability group.

You can use the Veeam Backup & Replication console to perform the following operations with Veeam Plug-in for Microsoft SQL Server backups:

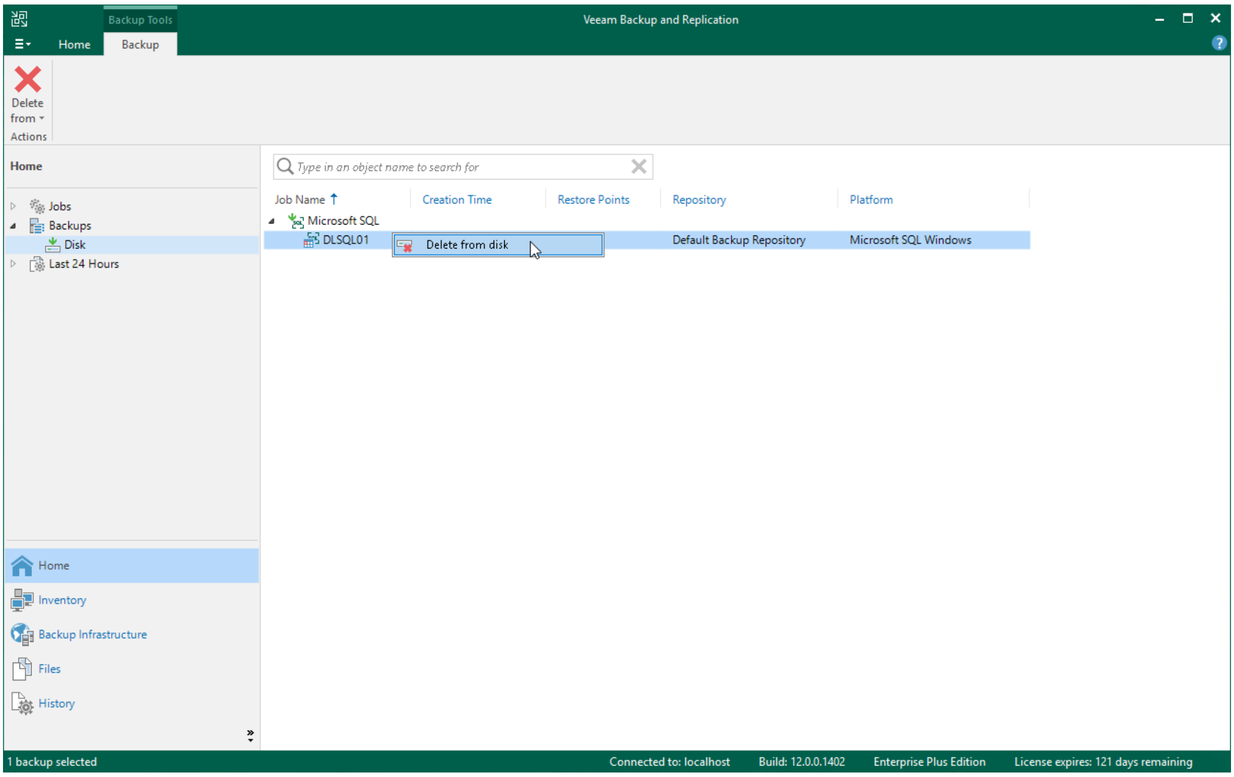
- Delete a backup from the backup repository
- Remove a backup from configuration
- Repair a backup

Deleting Backup

You can use the Veeam Backup & Replication console to delete backups created with Veeam Plug-in for Microsoft SQL Server from a Veeam backup repository.

To delete a backup, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. In the inventory pane, select **Backups**.
3. In the working area, right-click the name of the backed-up object and select **Delete from disk**.



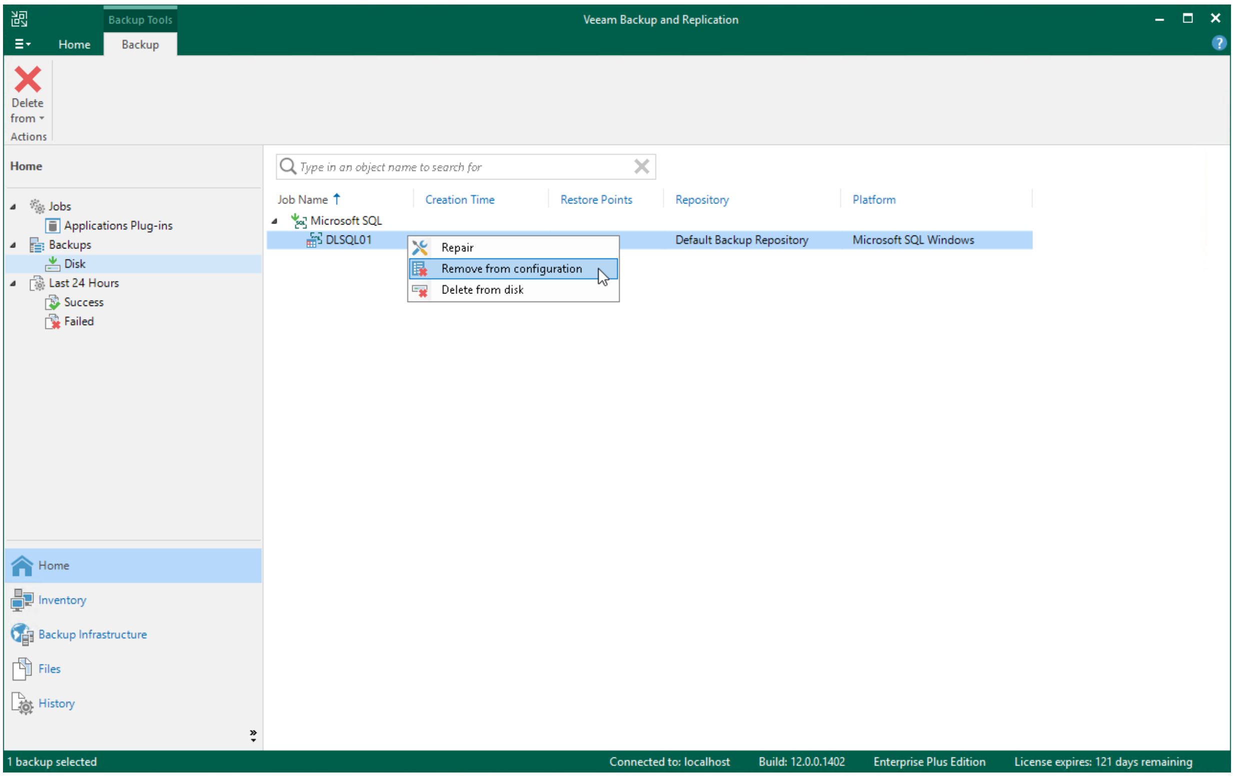
Removing Backup from Configuration

If you want to remove records about backups from the Veeam Backup & Replication console and configuration database, you can use the **Remove from configuration** operation.

When you remove a backup from configuration, backup files (VAB, VASM, VACM) remain in the backup repository. You can import the backup later and restore data from it.

To remove a backup from configuration:

1. Open the **Home** view.
2. In the inventory pane, select **Backups**.
3. In the working area, select the necessary backup.
4. Press and hold the **[CTRL]** key, right-click the backup and select **Remove from configuration**.



Repairing Backup

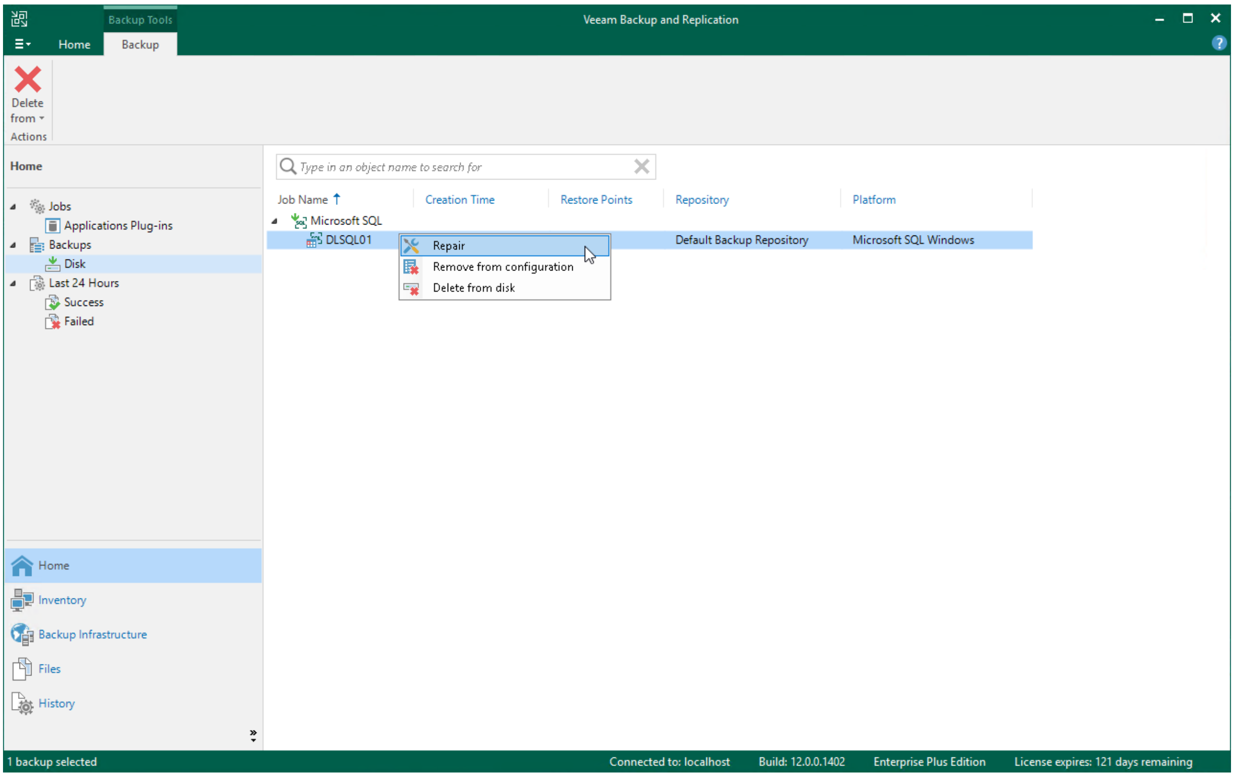
If you want to restore data from an immutable backup that resides in a hardened repository, you can use the **Repair** operation. During this operation, Veeam Backup & Replication will generate a new backup job metadata (VACM) file using information from the backup metadata (VASM) files.

> **IMPORTANT**
>
> This operation is intended only for a situation where the backup job metadata file has been lost as a result of malware activity or unplanned actions. Re-creation of the backup job metadata file for other purposes is not supported.
>
> For more information about data restore from the hardened repository, see Hardened Repository.

Before you start the repair operation, you must disable the backup job that created the backup. Otherwise, Veeam Backup & Replication will display a message notifying that the job must be disabled.

To repair a backup:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. In the inventory pane, select **Backups**.
3. In the working area, select the necessary backup.
4. Press and hold the **[CTRL]** key, right-click the backup and select **Repair**.



Performing Restore

You can restore Microsoft SQL Server databases from backups created with Veeam Plug-in. Veeam Plug-in supports restore of entire databases to the original Microsoft SQL Server machine or to another server.

You can restore a database to the same or different Microsoft SQL Server instance. If you have backup of Microsoft SQL Server transaction logs, you can specify a point in time to which you want to restore the database. Otherwise, Veeam Plug-in will restore the database to the time when the restore point was created.

Before you perform database restore, consider the following:

- The backup job that created the backup must be present in Veeam Backup & Replication.
- For restore to another server under another user account, the account must have the *Restore operator* or *Backup administrator* role on the Veeam backup server.

To restore Microsoft SQL Server databases, you can use the **Restore Database** wizard or the `MSSQLRecoveryManager.exe` command-line tool.

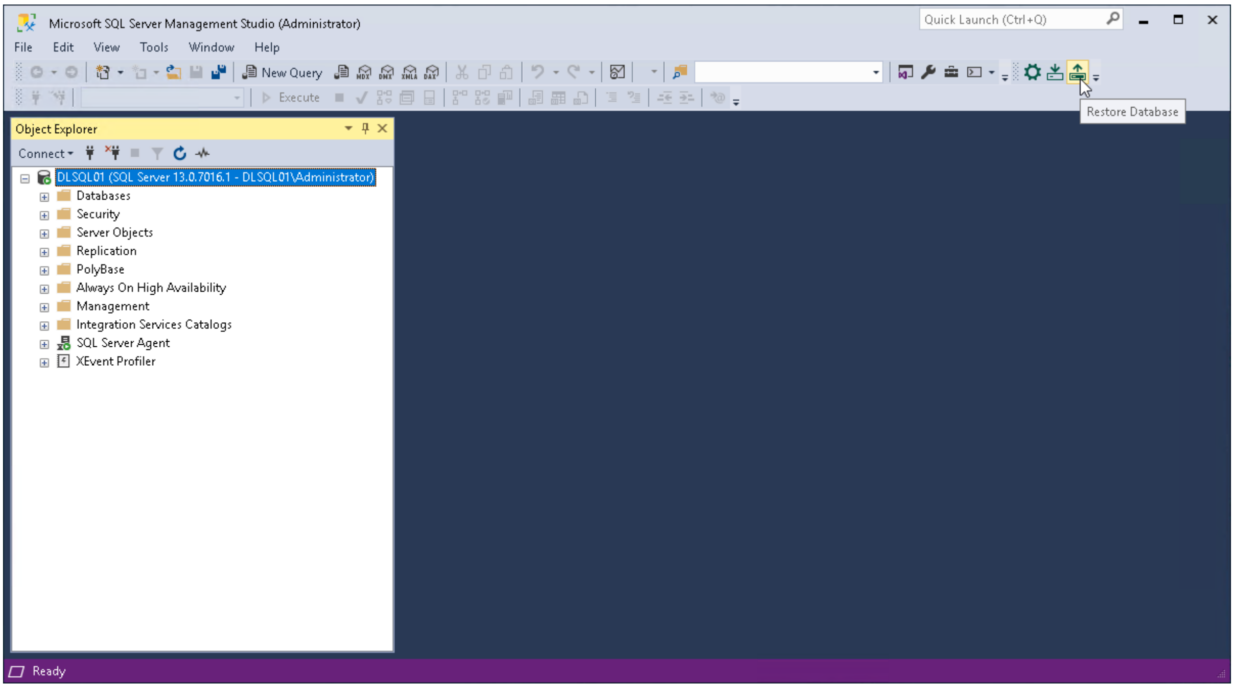
Restore with Restore Database Wizard

You can restore Microsoft SQL Server databases using the **Restore Database** wizard.

Step 1. Launch Restore Wizard

To launch the **Restore Database** wizard, on the Microsoft SQL Server machine do either of the following:

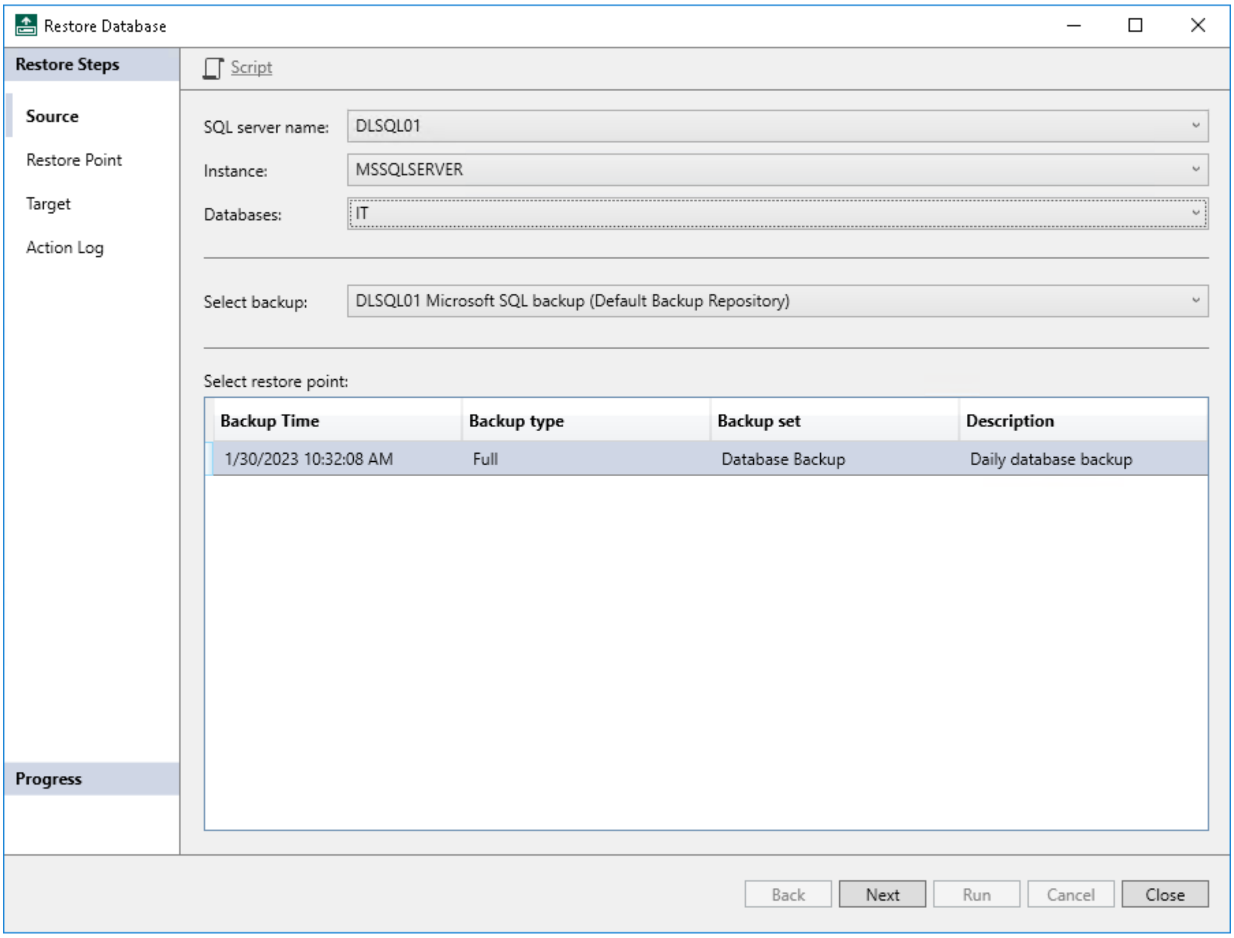
- Click the **Restore Database** icon on the desktop.
- From the Microsoft Windows **Start** menu, select **All Programs** > **Veeam** > **Restore Database** or use the Microsoft Windows search to find the **Restore Database** option on your machine.
- In Microsoft SQL Server Management Studio, click the **Restore Database** button on the toolbar.
- Launch the `%PROGRAMFILES%\Veeam\Plugins\Microsoft SQL\Veeam.Backup.MSSQLPlugin.UI.Restore.exe` file.



Step 2. Select Database to Restore

At the **Source** step of the wizard, select a Microsoft SQL Server database that you want to restore and restore point from which you want to restore the database:

1. From the **SQL Server Name** drop-down list, select the name of the machine that runs Microsoft SQL Server.
2. From the **Instance** drop-down list, select the Microsoft SQL Server instance whose database you want to restore.
3. From the **Databases** drop-down list, select the database that you want to restore.
4. From the **Select backup** drop-down list, select the name of the backup that contains the selected database. If only one backup in the backup repository contains the selected database, Veeam Plug-in will automatically select and display this backup.
5. From the **Select restore point** list, select the name of the restore point from which you want to recover data.



SQL server name: DLSQL01

Instance: MSSQLSERVER

Databases: IT

Select backup: DLSQL01 Microsoft SQL backup (Default Backup Repository)

Select restore point:

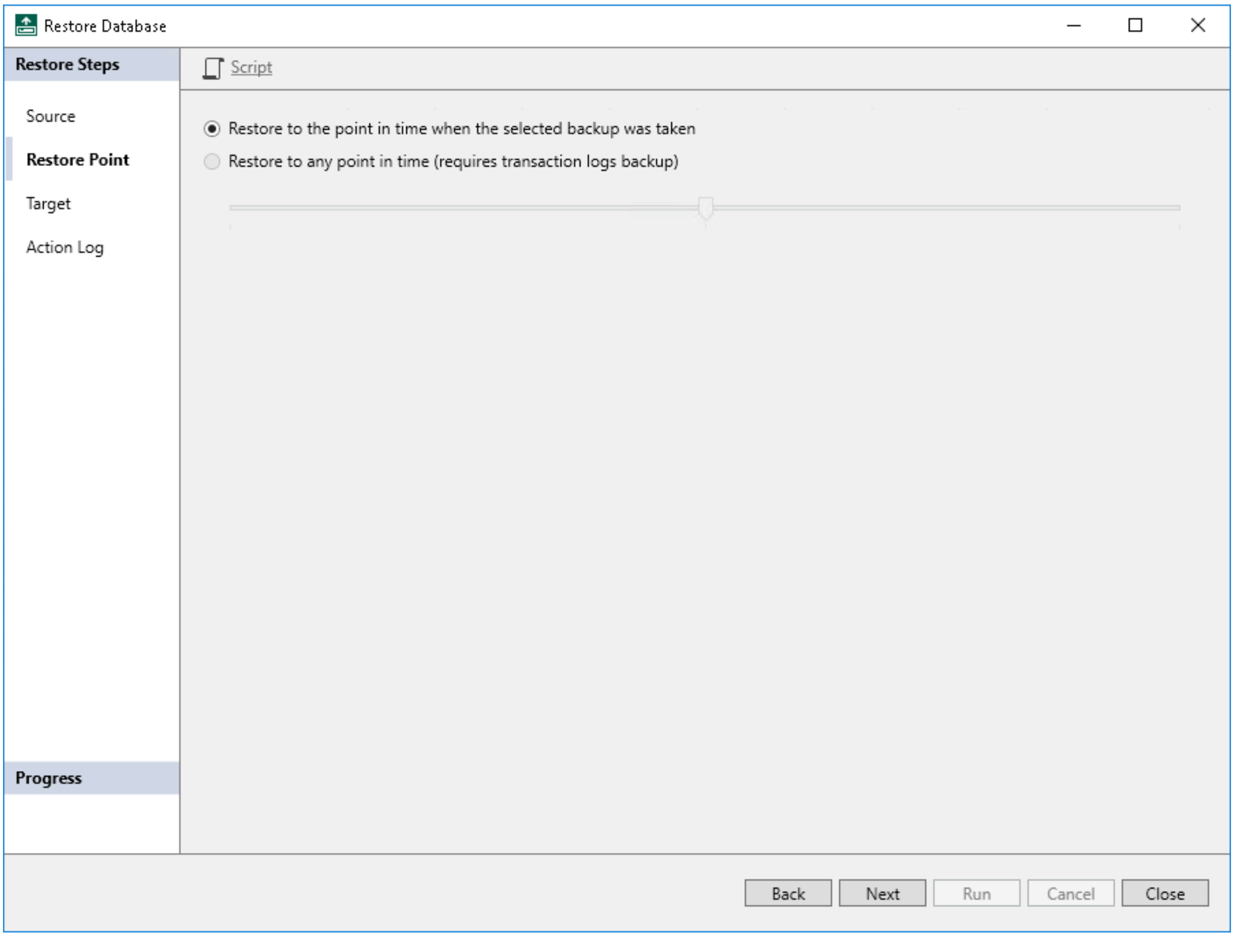
Backup Time	Backup type	Backup set	Description
1/30/2023 10:32:08 AM	Full	Database Backup	Daily database backup

Step 3. Specify Restore Point

At the **Restore Point** step of the wizard, select a point in time to which you want to restore the database:

- Select **Restore to the point in time when the selected backup was taken** if you want to restore the database to the point in time when the restore point that you selected at the **Source** step was created.
- Select **Restore to any point in time** if you want to restore the database to a specific point in time between the selected restore point and a previous restore point. This option is available if you restore data from a backup that contains Microsoft SQL Server transaction logs.

  Use the slider control to choose the point in time you need.



● Restore to the point in time when the selected backup was taken

○ Restore to any point in time (requires transaction logs backup)

Step 4. Specify Restore Target

At the **Target** step of the wizard, specify where and how you want to restore the database:

1. From the **Instance** drop-down list, select the Microsoft SQL Server instance where you want to restore the database.

2. In the **Database** field, specify the name for the restored database or select the name of the target database from the drop-down list. Keep in mind that if you restore a database from the backup to a database that exists in the Microsoft SQL Server instance, the target database will be overwritten.

3. In the **Recovery state** section, select the recovery state:

   - RECOVERY

     Rolls back (*undo*) any uncommitted changes.

   - NORECOVERY

     Skips the *undo* phase so that uncommitted or incomplete transactions are held open.

     This allows further restore stages to carry on from the restore point. When applying this option, the database will be in the *norecovery* state and inaccessible to users.

   - STANDBY

     The database will be in the *standby* state and therefore available for read operations. You can also provide a standby file with uncommitted transactions.

   For more information on recovery modes, see this Microsoft article.

4. Specify the following file locations:

   - Primary database file

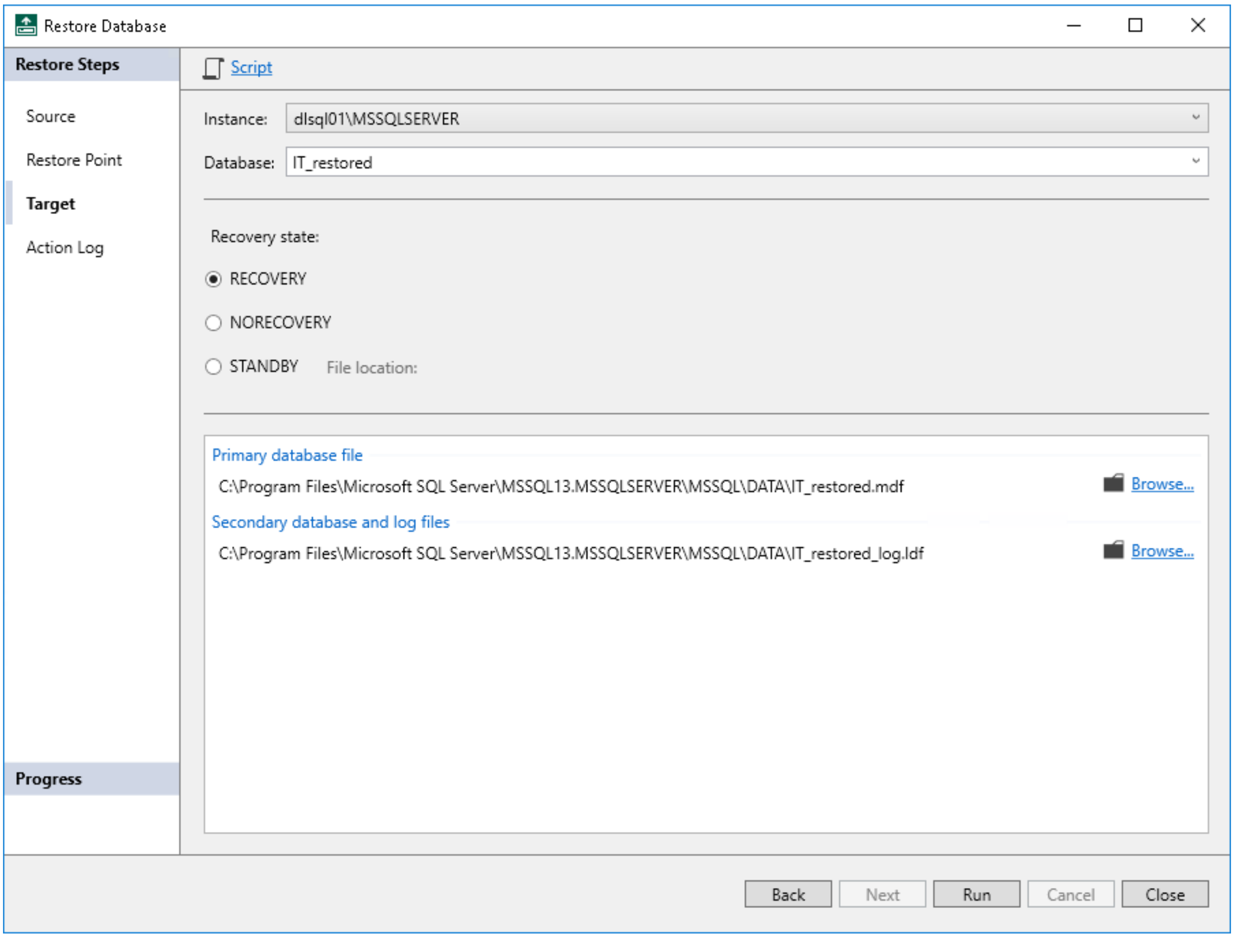
   - Secondary database file and log files

   To specify file locations, do the following:

   a. Click **Browse** next to the necessary database file type.

   b. In the **Browse For Folder** window, browse to the folder where you want to create the restored database files or click **Make New Folder** to create a new folder, and click **OK**.

5. Click **Run** to start the restore process.



Instance: dlsql01\MSSQLSERVER

Database: IT_restored

Recovery state:

● RECOVERY

○ NORECOVERY

○ STANDBY File location:

Primary database file

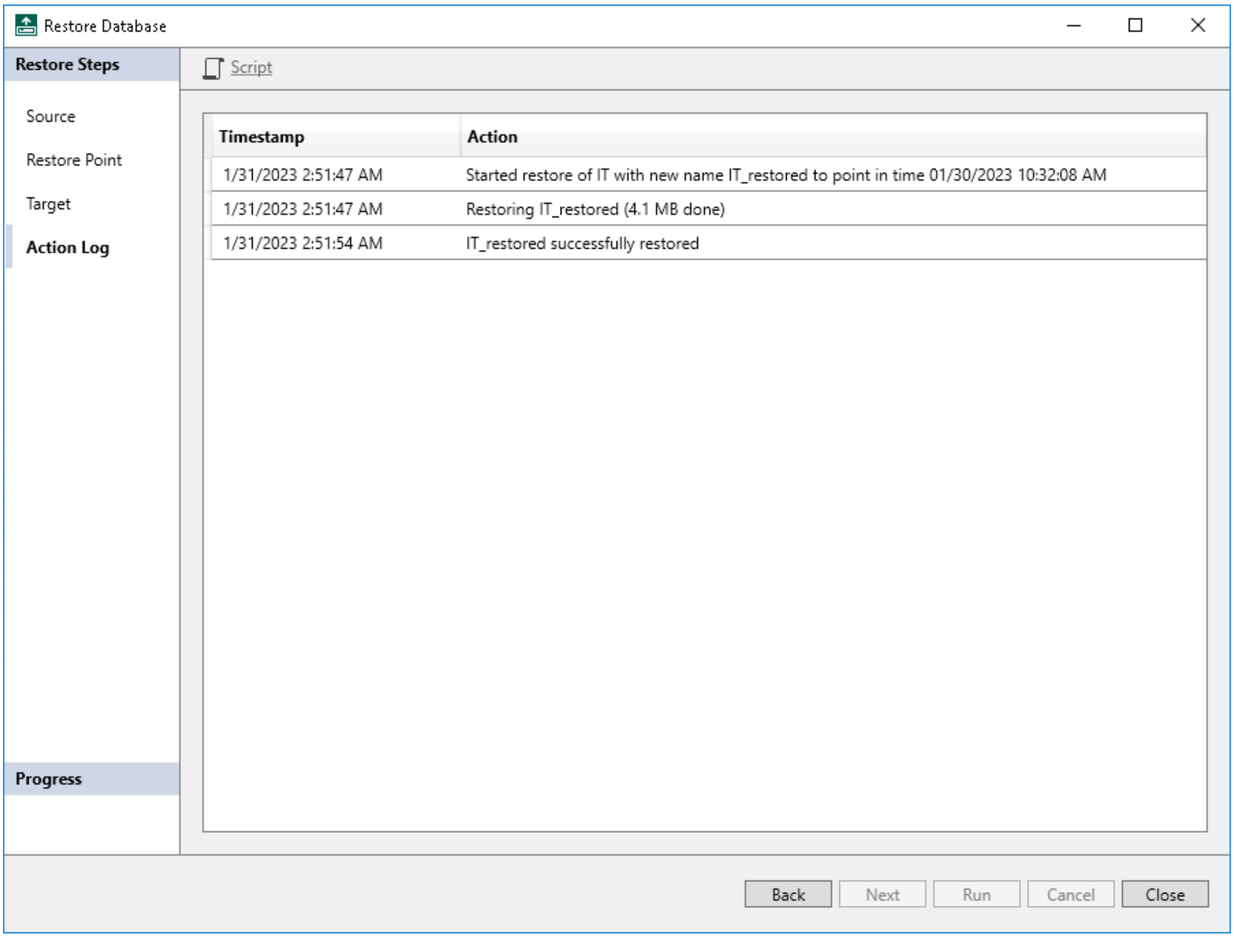
C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\DATA\IT_restored.mdf

Secondary database and log files

C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\DATA\IT_restored_log.ldf

Step 5. Monitor Restore Process

At the **Action Log** step of the wizard, review the list of restore operations and click **Close** to exit the wizard.



Timestamp	Action
1/31/2023 2:51:47 AM	Started restore of IT with new name IT_restored to point in time 01/30/2023 10:32:08 AM
1/31/2023 2:51:47 AM	Restoring IT_restored (4.1 MB done)
1/31/2023 2:51:54 AM	IT_restored successfully restored

Restore with Command-Line Interface

You can restore backup of Microsoft SQL Server databases with Veeam Plug-in using the `MSSQLRecoveryManager.exe` command-line tool.

To perform restore with the command-line interface, do the following:

1. On the Microsoft SQL Server machine, navigate to the `%PROGRAMFILES%\Veeam\Plugins\Microsoft SQL\` folder.

2. Run the `MSSQLRecoveryManager.exe` command with the required parameters. For more information, see Configuration Parameters.

   For example, to restore a Microsoft SQL Server database, use the following command:

   ```
   MSSQLRecoveryManager.exe --restore --src_server="srv16" --src_instance="MS
   SQLSERVER" --src_database="IT" --src_backup "srv16 SQL Backup (Backup Vol
   01)" --date="2022-08-17 09:03:49" --dst_instance="MSSQLSERVER" --dst_datab
   ase="IT_restored" --recovery_state="recovery" --f="'IT'::'DC:\Program File
   s\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\DATA\IT.mdf'" --f="'IT_lo
   g'::C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\DATA\I
   T_log.ldf'"
   ```

Restore Parameters

You can specify the following parameters for database restore with the `MSSQLRecoveryManager.exe` command:

Command	Description
--help	Shows the list of parameters for the `MSSQLRecoveryManager.exe` command.
--restore	Defines the restore operation.
--src_server	Specifies the name of the original server that contained the backed-up database.
--src_instance	Specifies the name of the original Microsoft SQL Server instance that contained the backed-up database.
--src_cluster	Specifies the name of the original Microsoft SQL Server cluster that contained the backed-up database.
--src_aon	Specifies the name of the original Always On availability group that contained the backed-up database.
--src_database	Specifies the name of the database that you want to restore.

Command	Description
--src_backup	Specifies the name of the Veeam Backup & Replication job in that created the backup of the database you want to restore.
--date	Specifies the point in time to which you want to restore the database. This parameter is optional. If you do not use this parameter, Veeam Plug-in will restore the database to the time when the latest restore point was created.
--dst_instance	Specifies the name of the target Microsoft SQL Server instance. This parameter is optional. If you do not use this parameter, Veeam Plug-in will restore the database to the original Microsoft SQL Server instance.
--dst_database	Specifies the name of the restored database. This parameter is optional. If you do not use this parameter, Veeam Plug-in will restore the database with its original name. If you restore the database with its original name to the original location, the original database will be overwritten.
--recovery_state	Specifies the recovery state. Possible values: • *recovery*. Rolls back (*undo*) any uncommitted changes. • *norecovery*. Skips the *undo* phase so that uncommitted or incomplete transactions are held open. This allows further restore stages to carry on from the restore point. When applying this option, the database will be in the *norecovery* state and inaccessible to users. • *standby*. The database will be in the *standby* state and therefore available for read operations. You can also provide a standby file with uncommitted transactions.
--standby_file_path	Specifies the path to a standby file with uncommitted transactions.

Command	Description
--f	Specifies the rules for database file mapping. Provide mapping rules in the following format: `--f="'<DisplayName>'::'<TargetFileLocation>'"`. For example: `--f="'DB'::'D:\SQLServer\Data\DB.mdf'"`. This parameter is optional. If you do not use this parameter, Veeam Plug-in will place database files to the same location as for the original database or the default location.

Backup Copy for Microsoft SQL Server Backups

Having just one backup does not provide the necessary level of safety. The primary backup may get destroyed together with production data, and you will have no backups from which you can restore data.

To build a successful data protection and disaster recovery plan, it is recommended that you follow the 3-2-1 rule:

- 3: You must have at least three copies of your data: the original production data and two backups.
- 2: You must use at least two different types of media to store the copies of your data, for example, local disk and cloud.
- 1: You must keep at least one backup offsite, for example, in the cloud or in a remote site.

Thus, you must have at least two backups and they must be in different locations. If a disaster takes out your production data and local backup, you can still recover from your offsite backup.

To help you adopt the 3-2-1 rule, Veeam Backup & Replication offers the backup copy functionality that allows you to create several instances of the same backup in different locations, whether onsite or offsite. Backup copies have the same format as those created by backup jobs and you can recover your data from them when you need it.

Veeam Backup & Replication fully automates the backup copy process and lets you specify retention settings to maintain the desired number of restore points, as well as full backups for archival purposes. Backup copy is a job-driven process. When enabled, the backup copy job for Veeam Plug-in backups runs continuously.

Creating Backup Copy Job

To copy backups to a secondary location, you must configure a backup copy job. The backup copy job defines how, where and when to copy backups. One job can be used to process backups of one or more machines.

You can configure a job and start it immediately or save the job to start it later.

Before creating a job, check prerequisites. Then use the **New Backup Copy Job** wizard to configure a backup copy job.

1. Launch Backup Copy Job wizard.
2. Specify a job name and description.
3. Select backups to process.
4. Define backup copy target.
5. Specify advanced settings.
6. Define backup copy schedule.
7. Finish working with the wizard.

Before You Begin

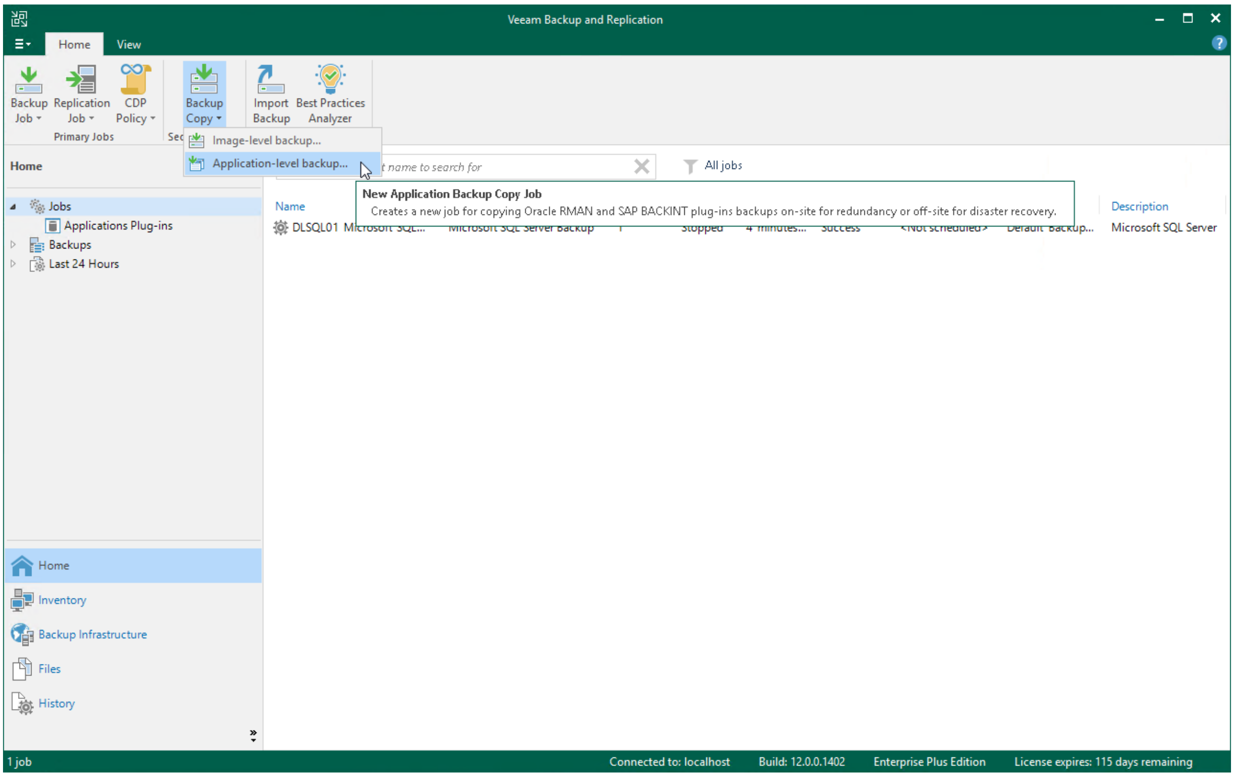
Before you create a backup copy job, check the prerequisites and limitations:

- Backup infrastructure components that will take part in the backup copy process must be added to the backup infrastructure and properly configured. These include source and target backup repositories between which backups must be copied.
- The target backup repository must have enough free space to store copied backups. To receive alerts about low space on the backup repository, configure global notification settings. For more information, see Specifying Other Notification Settings.
- For Veeam Plug-in backup copy jobs, you cannot select a Veeam Cloud Connect repository as a backup copy target.

Step 1. Launch Backup Copy Job Wizard

To create a backup copy job, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Click **Backup Copy** on the ribbon and select **Application-level backup**.



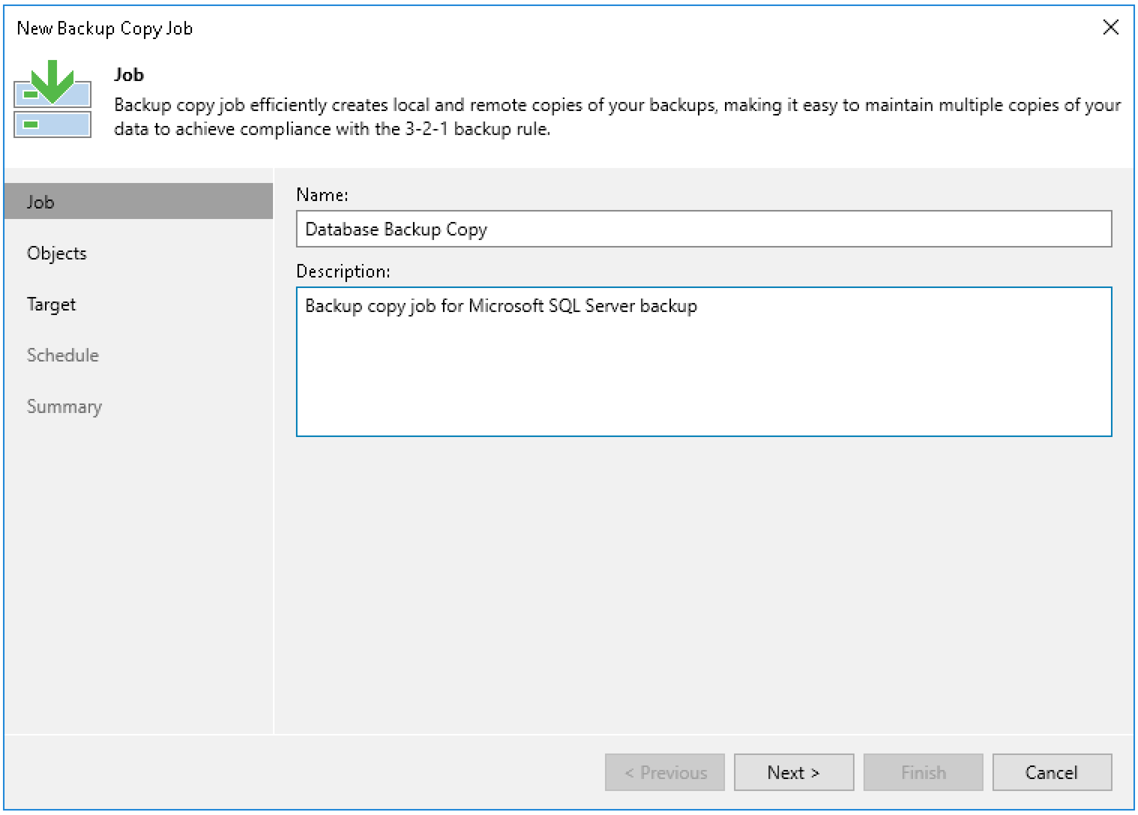
New Application Backup Copy Job

Creates a new job for copying Oracle RMAN and SAP BACKINT plug-ins backups on-site for redundancy or off-site for disaster recovery.

Step 2. Specify Job Name and Description

At the **Job** step of the wizard, specify a name and description for the backup copy job.

1. In the **Name** field, enter a name for the job.
2. In the **Description** field, enter a description for the job. The default description contains information about the user who created the job, date and time when the job was created.



New Backup Copy Job

Job

Backup copy job efficiently creates local and remote copies of your backups, making it easy to maintain multiple copies of your data to achieve compliance with the 3-2-1 backup rule.

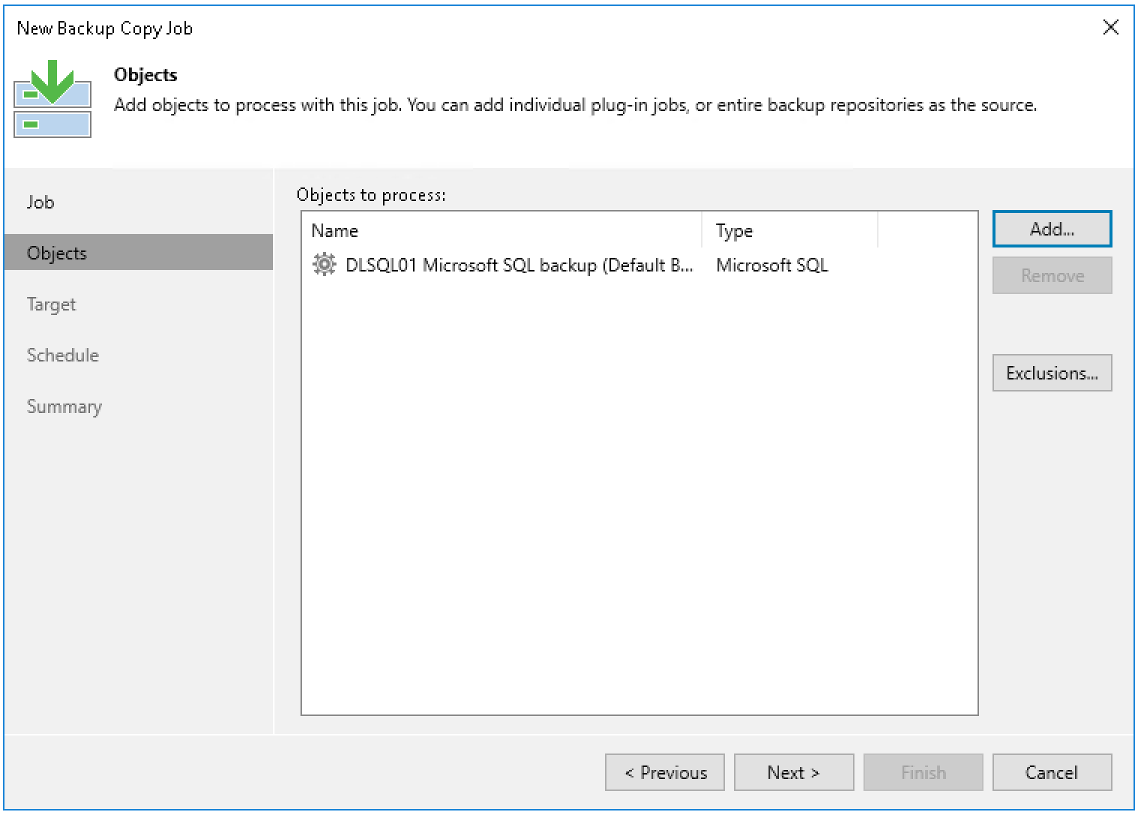
Name: Database Backup Copy

Description: Backup copy job for Microsoft SQL Server backup

Step 3. Select Backups to Process

At the **Object** step of the wizard, select machines whose backups you want to copy to the target repository.

1. Click the **Add** button and select from which entity you want to process the machines.
   - **From jobs**: You can select Veeam Plug-in backup jobs. When a backup copy job runs, Veeam Backup & Replication will search for backup files created by selected jobs.
   - **From repositories**: You can select repositories where Veeam Plug-in backups are stored. When a backup copy job runs, Veeam Backup & Replication will search for backup files created by Veeam Plug-in in selected repositories.
2. Use the **Remove** button if you want to remove selected jobs or repositories from processing.
3. If you have added jobs from a repository and want to exclude from processing some of the backup jobs on the selected repository, click **Exclusions** and select the jobs that you want to exclude.



New Backup Copy Job

Objects

Add objects to process with this job. You can add individual plug-in jobs, or entire backup repositories as the source.

Objects to process:

Name	Type
DLSQL01 Microsoft SQL backup (Default B...	Microsoft SQL

Step 4. Define Backup Copy Target

At the **Target** step of the wizard, configure the target repository settings.

1. From the **Backup repository** list, select a backup repository in the target site where copied backups must be stored. When you select a target backup repository, Veeam Backup & Replication automatically checks how much free space is available on it. Make sure that you have enough free space to store copied backups.

   > IMPORTANT
   >
   > For Veeam Plug-in backup copy jobs, you cannot select a Veeam Cloud Connect repository as a backup copy target.

2. If the target repository contains a Veeam Plug-in backup that was excluded from the backup copy job, and if you don't want to transfer duplicate data, you can use the mapping feature.

   After you configure mapping, if some of backup files (VAB) of the source backup are missing in the target backup copy, these files are uploaded to the target backup copy.

   > NOTE
   >
   > Veeam Plug-in backup copy jobs do not use WAN accelerators.

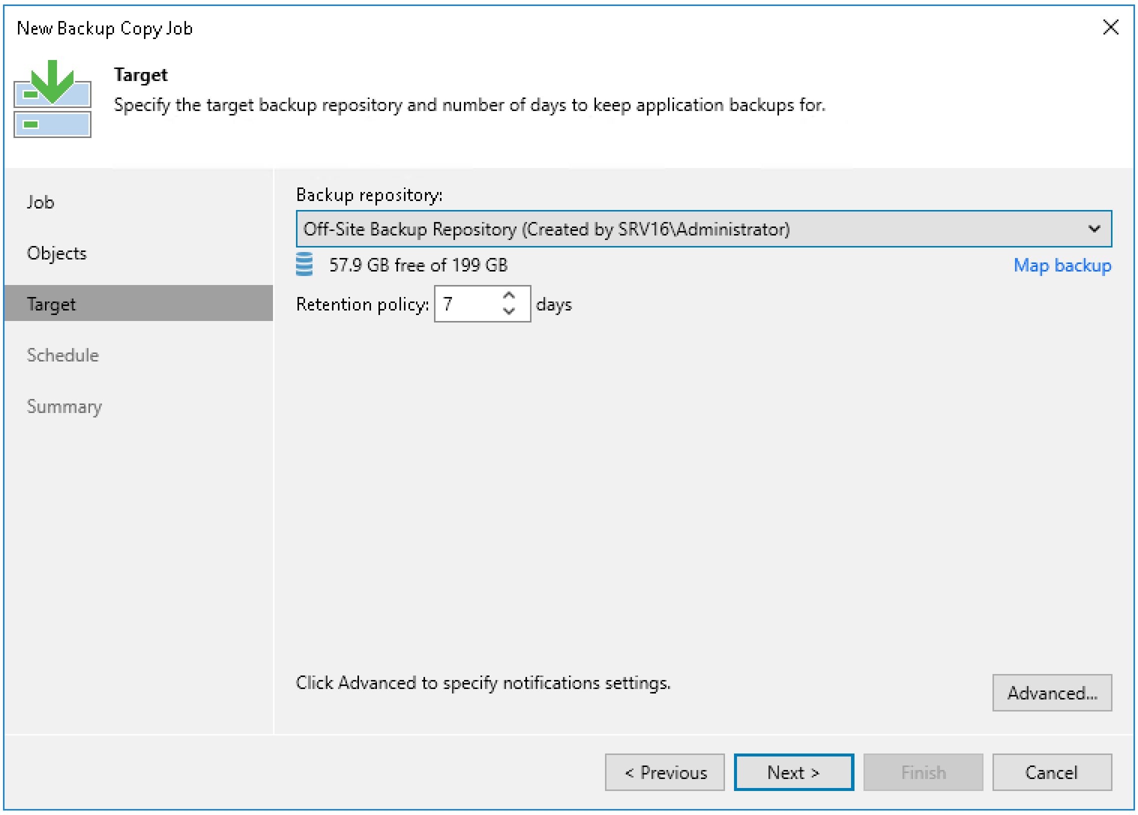
   To map a backup copy job to the backup:

   a. Click the **Map backup** link.

   b. Point the backup copy job to the backup in the target backup repository. Backups in the target backup repository can be easily identified by backup job names. To facilitate search, you can use the search field at the bottom of the window.

   > IMPORTANT
   >
   > - Used account must have access to Veeam backup repositories that you plan to use.
   > - Encryption must be disabled on the repository.
   >
   > Otherwise, the repositories will not be listed as available. To learn how to configure access permissions and encryption settings on repositories, see Access and Encryption Settings on Repositories.

3. You can specify the number of days after which the backup copy will be deleted from the repository. Note that the countdown starts from the moment when source backup has been created.



New Backup Copy Job

Target

Specify the target backup repository and number of days to keep application backups for.

Backup repository: Off-Site Backup Repository (Created by SRV16\Administrator)

57.9 GB free of 199 GB

Retention policy: 7 days

Click Advanced to specify notifications settings.

Step 5. Specify Advanced Settings

At the **Target** step of the wizard, click **Advanced** to configure compression, RPO and notifications settings.

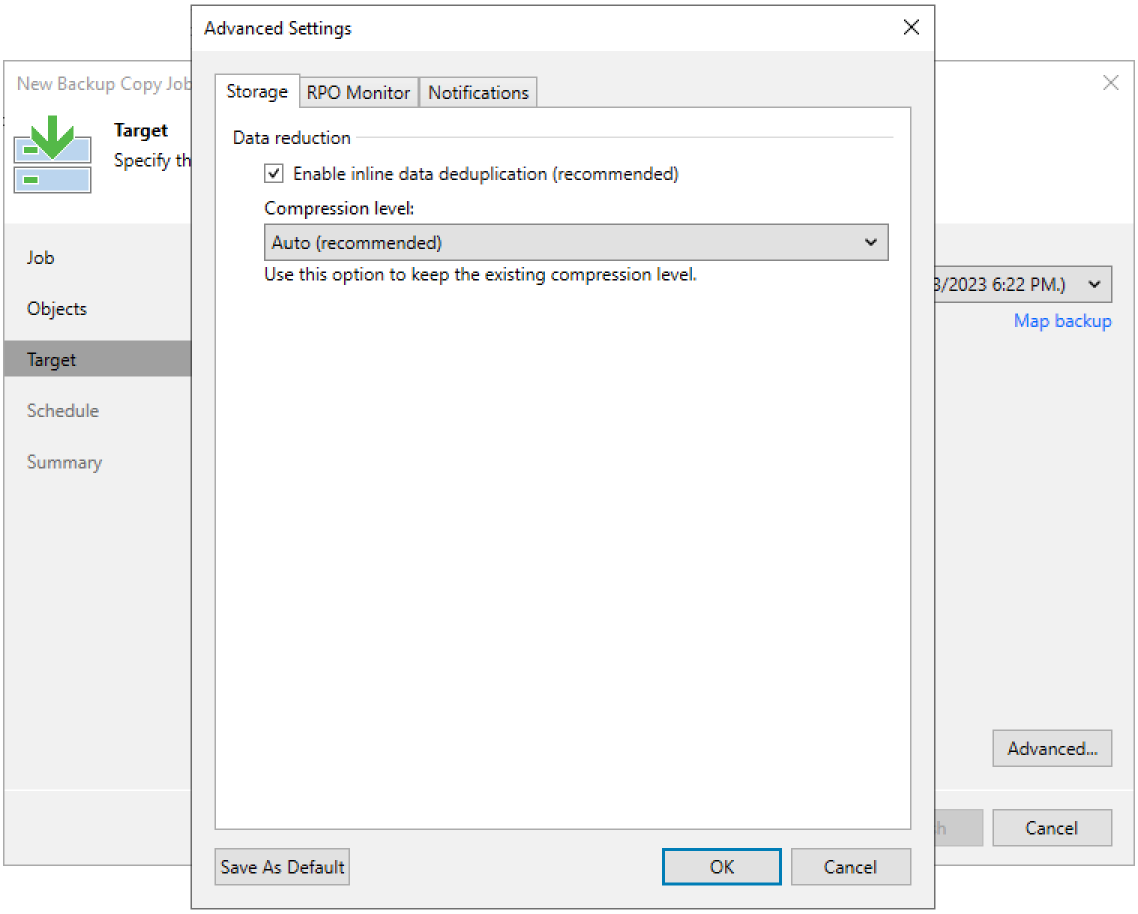
- Compression and Deduplication
- RPO
- Notifications

Compression and Deduplication

At the **Storage** tab, define compression and deduplication settings.

By default, Veeam Backup & Replication performs deduplication before storing copied data on the target backup repository. Deduplication provides a smaller size of the resulting backup file but may reduce the job performance.

1. You can disable data deduplication. To do this, clear the **Enable inline data deduplication** check box.
2. From the Compression level list, choose a compression level to be used: **Auto**, **None**, **Dedupe-friendly**, **Optimal**, **High** or **Extreme**. The recommended level of compression for backup copy jobs is **Auto**. In this case, Veeam Backup & Replication uses compression settings of the copied backup files. For more information, see Compression and Deduplication.



Advanced Settings

Data reduction

☑ Enable inline data deduplication (recommended)

Compression level: Auto (recommended)

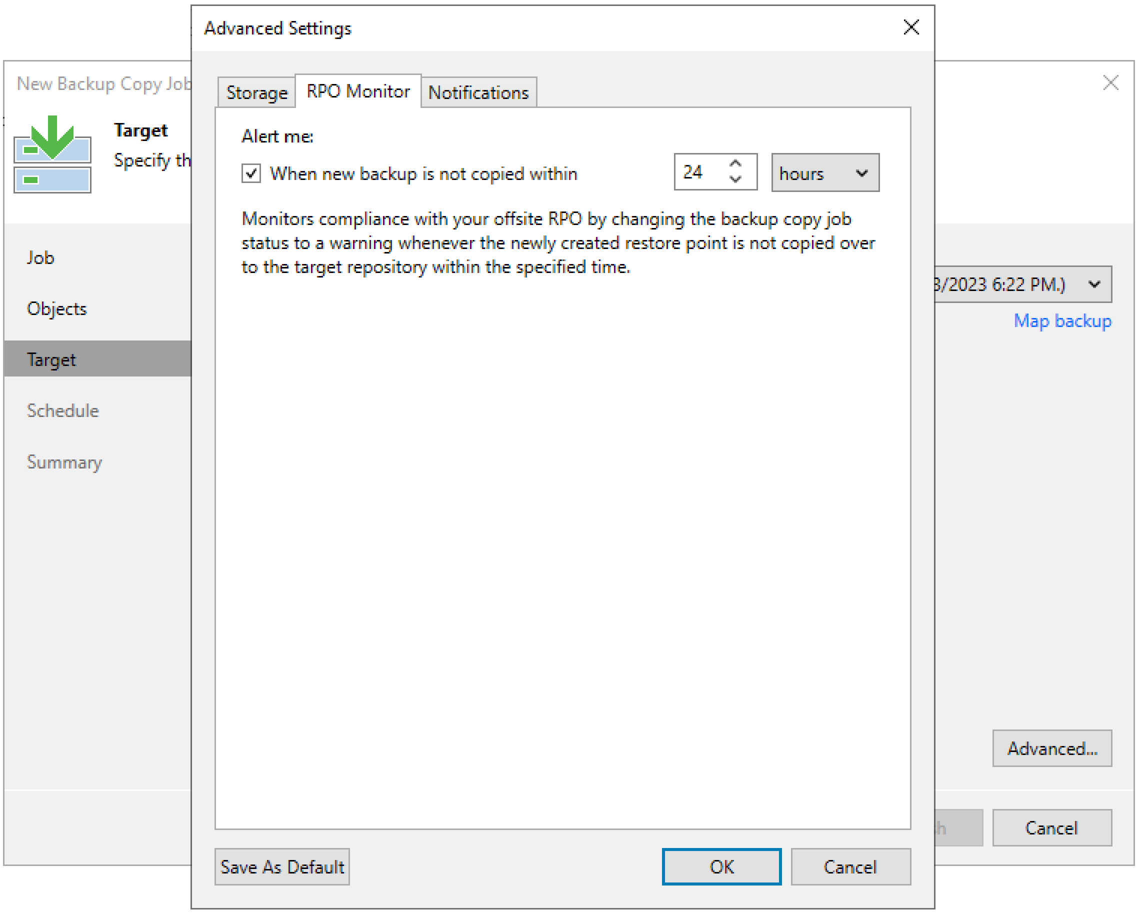
Use this option to keep the existing compression level.

RPO Monitor

At the **RPO Monitor** tab, specify RPO warning settings.

Enable the **Warn me if backup is not copied within** check box and specify the time period in **minutes**, **hours**, or **days**.

If the backup copy is not created within the specified time period, the backup copy job will finish with the *Warning* status. The countdown starts from the moment when the required backup is finished and ready to be copied.



Advanced Settings

Alert me:

☑ When new backup is not copied within 24 hours

Monitors compliance with your offsite RPO by changing the backup copy job status to a warning whenever the newly created restore point is not copied over to the target repository within the specified time.

Notifications

At the **Notifications** tab, to specify notification settings for the backup copy job:

1. At the **Target** step of the wizard, click **Advanced**.
2. Click the **Notifications** tab.
3. Select the **Send SNMP notifications for this job** check box if you want to receive SNMP traps when the job completes successfully. SNMP traps will be sent if you specify global SNMP settings in Veeam Backup & Replication and configure software on recipient's machine to receive SNMP traps. For more information, see Specifying SNMP Settings.
4. Select the **Send email notifications to the following recipients** check box if you want to receive notifications by email in case of job failure or success. In the field below, specify a recipient's email address. You can enter several addresses separated by a semicolon.
5. Veeam Backup & Replication sends a consolidated email notification once for the specified backup copy interval. Even if the synchronization process is started several times within the interval, for example, due to job retries, only one email notification will be sent.
6. Email notifications will be sent if you configure global email notification settings in Veeam Backup & Replication. For more information, see Configuring Global Email Notification Settings.
7. At the **Send** at field, specify the time when you want to receive notifications. Note that you will receive a notification on the job status once a day.

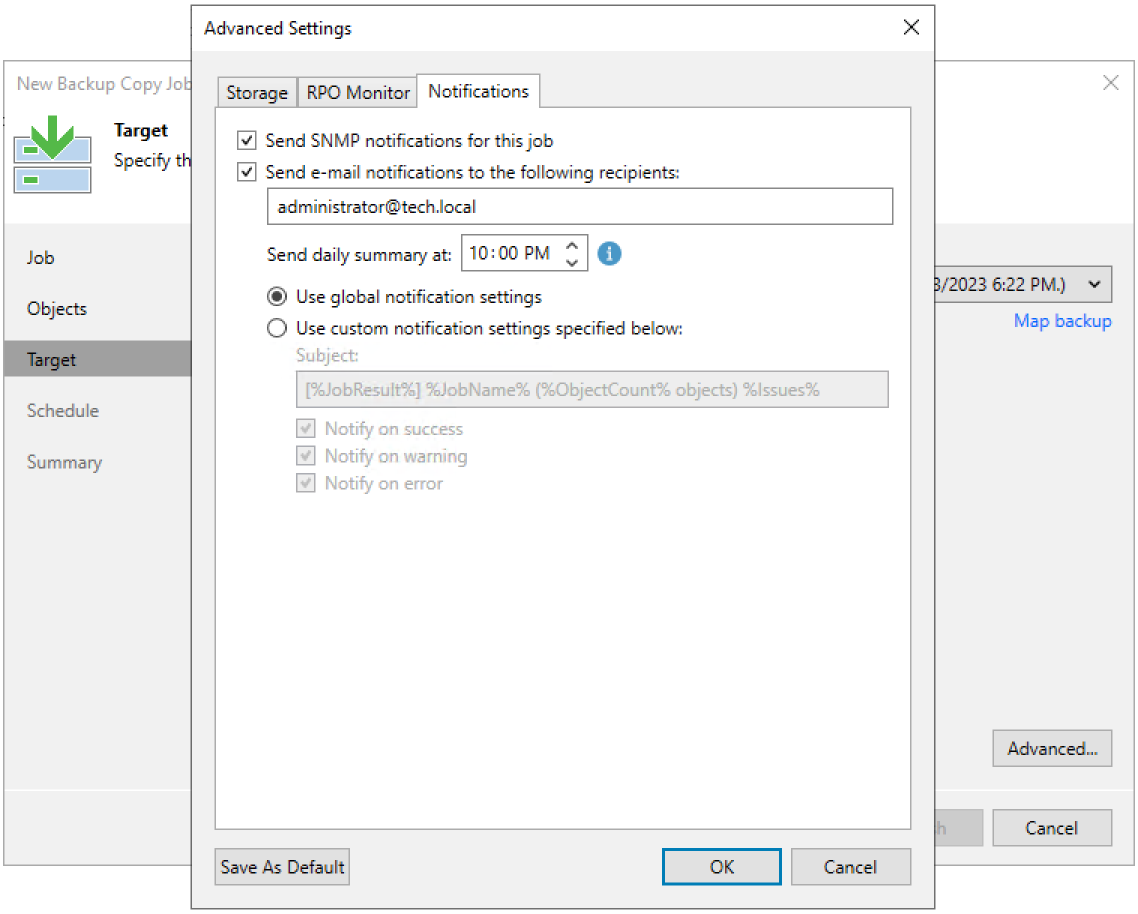
8. You can choose to use global notification settings or specify custom notification settings.

   - To receive a typical notification for the job, select **Use global notification settings**. In this case, Veeam Backup & Replication will apply to the job global email notification settings specified for the backup server. For more information, see Configuring Global Email Notification Settings.

   - To configure a custom notification for a job, select **Use custom notification settings specified below**. You can specify the following notification settings:

     i. In the **Subject** field, specify a notification subject. You can use the following variables in the subject: *%Time%* (completion time), *%JobName%*, *%JobResult%*, *%VmCount%* (number of machines in the job) and *%Issues%* (number of machines in the job that have been processed with the **Warning** or **Failed** status).

     ii. Select the **Notify on success**, **Notify on warning** and **Notify on error** check boxes to receive email notification if data processing within the backup copy interval completes successfully, fails or completes with a warning.



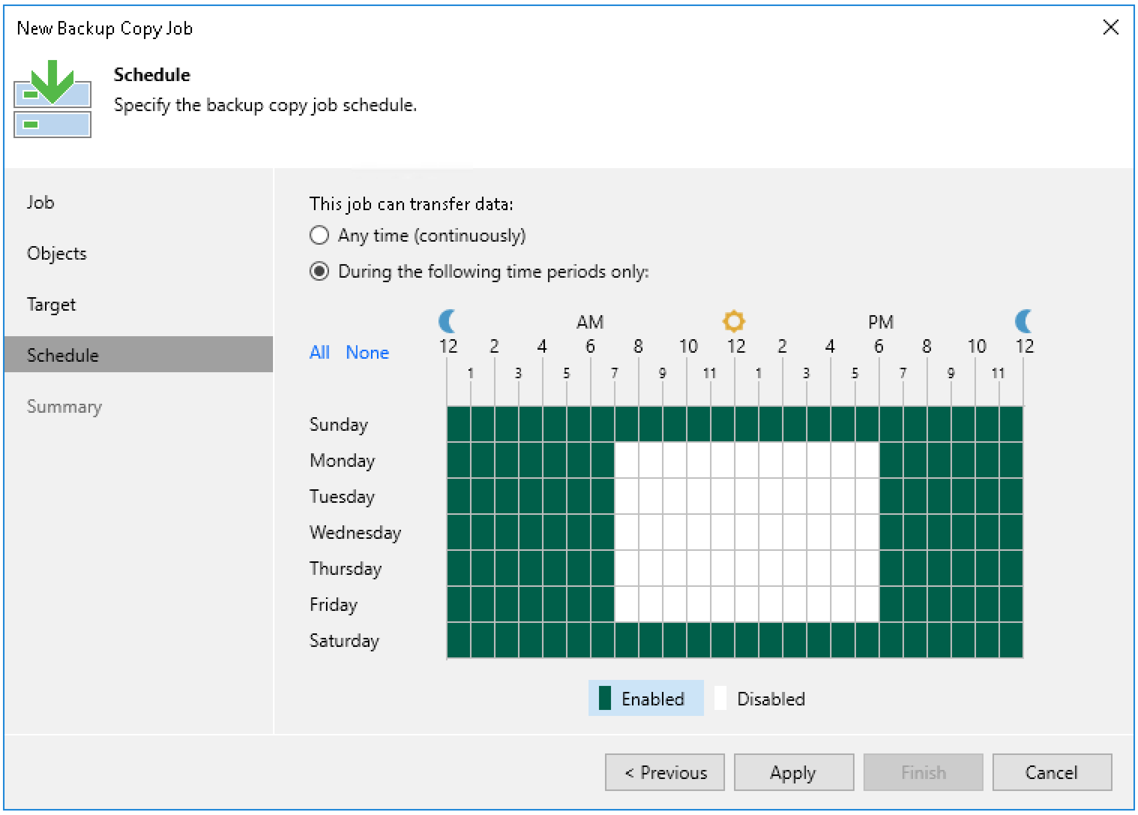
☑ Send SNMP notifications for this job
☑ Send e-mail notifications to the following recipients:
administrator@tech.local
Send daily summary at: 10:00 PM
● Use global notification settings
○ Use custom notification settings specified below:
Subject:
[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%
☑ Notify on success
☑ Notify on warning
☑ Notify on error

Step 6. Define Backup Copy Schedule

At the **Schedule** step of the wizard, define a time span in which the backup copy job must not transport data between source and target backup repositories. For more information, see Backup Copy Window.

To define a backup window for the backup copy job:

1. Select the **During the following time periods only** option.
2. In the schedule box, select the desired time area.
3. Use the **Enable** and **Disable** options to mark the selected area as allowed or prohibited for the backup copy job.



Schedule

Specify the backup copy job schedule.

This job can transfer data:

○ Any time (continuously)

● During the following time periods only:

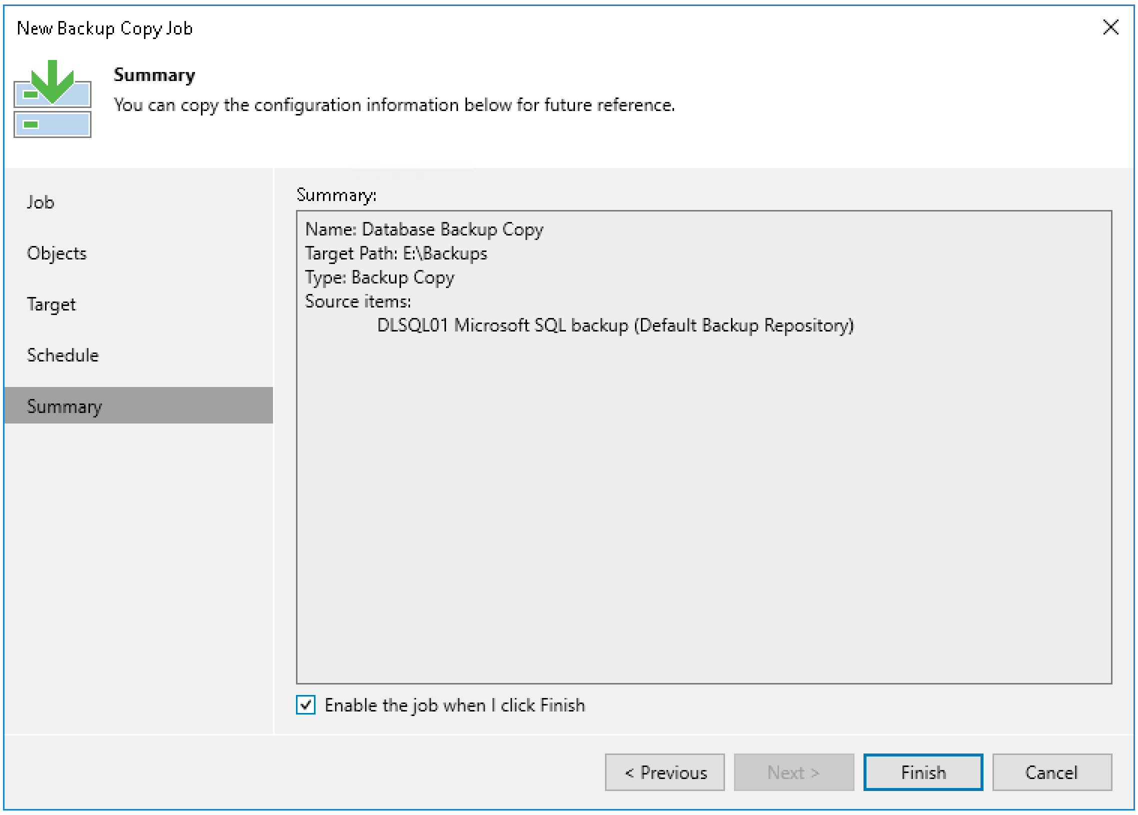
	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11
Sunday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Monday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩
Tuesday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩
Wednesday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩
Thursday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩
Friday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩
Saturday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩

🟩 Enabled ⬜ Disabled

Step 7. Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of backup copy job configuration.

1. Review details of the backup copy job.
2. Select the **Enable the job when I click Finish** check box if you want to start the job right after you finish working with the wizard.
3. Click **Finish** to close the wizard.



Summary:

Name: Database Backup Copy
Target Path: E:\Backups
Type: Backup Copy
Source items:
DLSQL01 Microsoft SQL backup (Default Backup Repository)

☑ Enable the job when I click Finish

Converting Backup Copy to Backup

If you have imported Veeam Plug-in backup copies from another server, you can convert them into regular backup files. When you convert a backup copy to a backup, Veeam Plug-in creates a backup job with the converted backup. You can use this backup job to continue a backup chain and use the converted backup as a restore point.

You can convert and unbind Veeam Plug-in backups into regular Veeam Plug-in backup files in the following cases:

- If you have deleted a backup copy job which created the backup copy.
- If you have excluded a backup job from a backup copy job that used multiple backup jobs as a source.
- If you imported a Veeam Plug-in backup copy from another host.

> **NOTE**
>
> If you want to restore from a backup copy, you do not need to convert the backup copy to the backup.

Procedure

To convert a backup copy to a primary backup, do the following:

1. Run the `MSSQLConfigTool.exe` command-line tool with the `--promote-backup-copy-to-primary` parameter:

   ```
   MSSQLConfigTool.exe --promote-backup-copy-to-primary
   ```

2. Veeam Plug-in will display the list of available backup copies. Type the necessary backup copy number and press **[ENTER]**. Then follow instructions in the command prompt.

   ```
   Backup copies available for promotion to the primary backup target:
   1. Backup Copy Job 1\SERV01 Microsoft SQL backup (Default Backup Repositor
   y)
   Select a backup copy: 1
   Proceed with the action?
   1. Promote backup copy destination to the primary backup target
   2. Cancel
   Enter selection: 1
   Promoting backup copy destination
   Done
   ```

Logs and Support

If you have any questions or issues with Veeam Plug-in for Microsoft SQL Server or Veeam Backup & Replication, you can search for a resolution on Veeam R&D Forums or submit a support case on the Veeam Customer Support Portal.

When you submit a support case, we recommend that you attach logs files related to Veeam Plug-in operations.

To export Veeam Plug-in logs, do the following:

1. On the Microsoft SQL Server machine, navigate to the `%PROGRAMDATA%\Veeam\Backup\MSSQLPluginLogs` directory and copy the contents of the directory.
2. On the Veeam Backup & Replication server, navigate to the `%PROGRAMDATA%\Veeam\Backup\Plugin` directory and copy logs of the required backup or restore process.

Veeam Plug-in Management

Veeam Backup & Replication lets you deploy and manage the following Veeam Plug-ins on computers in your infrastructure:

- Veeam Plug-in for SAP HANA
- Veeam Plug-in for Oracle RMAN
- Veeam Plug-in for SAP on Oracle

> **IMPORTANT**
>
> Veeam Backup & Replication does not support management of computers whose databases are protected with Veeam Plug-in for Microsoft SQL Server.

You do not need to install, set up and operate Veeam Plug-in on every computer whose databases you want to protect. Instead, you can perform the whole set of deployment, administration, data protection, and disaster recovery tasks on computers remotely from the Veeam Backup & Replication console.

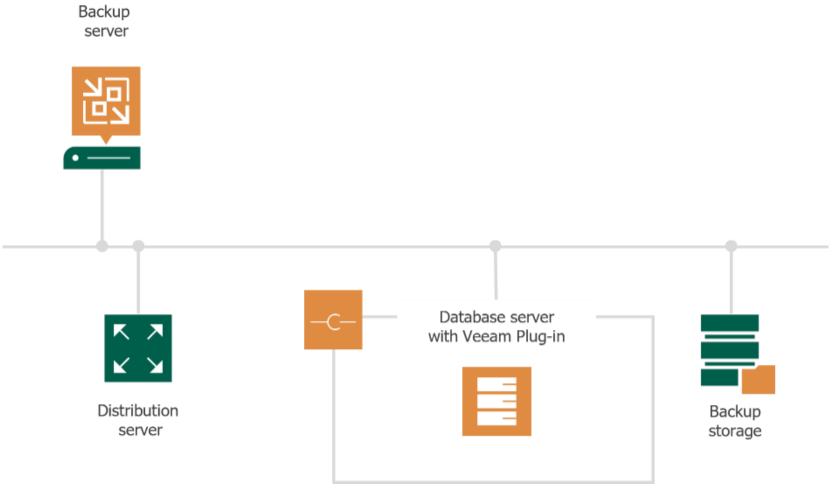
Veeam Backup & Replication offers the following Veeam Agent management capabilities:

- **Automated deployment and management of Veeam Plug-ins.** You can set up Veeam Backup & Replication to automatically discover computers that you want to protect with Veeam Plug-in for SAP HANA, Veeam Plug-in for Oracle RMAN, and Veeam Plug-in for SAP on Oracle and deploy Veeam Plug-ins on these computers. Once Veeam Plug-ins are deployed on protected computers, you can use the Veeam Backup & Replication console to administrate Veeam Plug-ins on multiple computers.
- **Centralized configuration and management of backup policies on protected computers**. You can use the Veeam Backup & Replication console to create and manage backup policies on computers in your infrastructure whose databases you want to protect. You can configure backup policies to apply settings on the computer, database system, or database level.
- **Centralized backup jobs statistics and monitoring.** You can use the Veeam Backup & Replication console to review reports about backup policies performance on computers in your infrastructure whose databases you want to protect.
- **Centralized management of backups created by backup policies**. If you choose to create backups on a backup repository managed by the Veeam backup server, you can use the Veeam Backup & Replication console to restore data from these backups.
- **Secure database restore with recovery tokens.** If you want to restore database from the backup and you are not the owner of this backup, you can ask your *Backup Administrator* to generate a recovery token. Using this recovery token, you can get access to a certain backup on the Veeam backup repository and restore database from this backup.

Veeam Plug-in Management Infrastructure

The Veeam Plug-in management infrastructure comprises the following components:

- Veeam backup server
- Computers with Veeam Plug-ins
- Distribution server



Veeam Backup Server

The Veeam backup server is the core component in the backup infrastructure that fills the role of the "configuration and control center". To use the Veeam Plug-in management functionality offered by Veeam Backup & Replication, you can use the backup server that is already running in your backup infrastructure or deploy a separate backup server.

To learn more, see the Deployment section in the Veeam Backup & Replication User Guide.

Computers with Veeam Plug-ins

To manage Veeam Plug-ins on computers in your infrastructure, you must add computers that you want to protect to the inventory in the Veeam Backup & Replication console and deploy Veeam Plug-ins. In Veeam Backup & Replication, protected computers are organized into protection groups. To learn more, see Protection Groups.

Veeam Backup & Replication lets you manage Veeam Plug-in on computers of the following types:

- Workstations, servers, and failover clusters running a Microsoft Windows OS
- Workstations and servers running a Linux OS

To learn more, see System Requirements.

If you want to manage Veeam Plug-ins installed on protected computers in Veeam Backup & Replication, you must set Veeam Plug-ins in the managed mode. In this mode, all data protection and administration tasks are performed by a backup administrator in Veeam Backup & Replication. In some scenarios, a user can also perform a limited set of backup and disaster recovery tasks directly on a protected computer.

Veeam Backup & Replication is set up to automatically discover computers added to the inventory and deploy Veeam Plug-in and Veeam Plug-in on these computers. To learn more, see Computer Discovery and Veeam Plug-in Deployment.

On every computer added to the inventory, Veeam Backup & Replication installs the Veeam Installer Service. The service performs the following tasks:

- Collects information about the computer and sends it to Veeam Backup & Replication. The collected data includes details on the computer (platform, host name, guest OS, IP address, BIOS UUID), databases (database system name, database hierarchy, names of databases) and Veeam Plug-in (product presence on the computer and version).
- Downloads Veeam Plug-in setup files from the distribution server and installs Veeam Plug-in on the protected computer.

On Microsoft Windows computers, Veeam Backup & Replication connects to a computer using the administrative share (admin$) of the target computer. An account that you plan to use to connect to a computer included in the protection group must have access to the administrative share.

On Linux computers, Veeam Backup & Replication also installs Veeam Deployer Service. For the first time, Veeam Backup & Replication connects to a computer using SSH. Alter the first connection, Veeam Backup & Replication can continue using SSH or start using Veeam Installer Service and Veeam Deployer Service.

Keep in mind that to connect to Linux computer via SSH, this Linux computer must be added to the list of trusted hosts. To learn more, see Configuring Security Settings.

Distribution Server

The distribution server is an architecture component in the Veeam Plug-in management infrastructure used for automated deployment of Veeam Agent setup files to protected computers. When you instruct Veeam Backup & Replication to install Veeam Plug-in on a protected computer, the Veeam backup server communicates to the distribution server, and Veeam Backup & Replication uploads Veeam Plug-in setup files from the distribution server to the target computer.

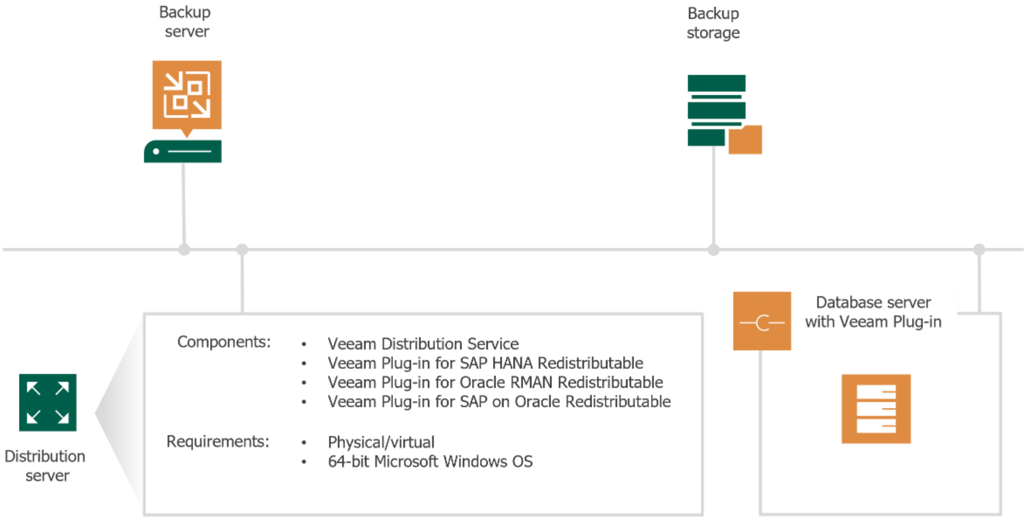
By default, the role of the distribution server is assigned to the backup server. However, you can deploy a dedicated distribution server to reduce workload on the backup server. To deploy a distribution server, you need to add a Windows-based server to Veeam Backup & Replication. To learn more, see the Adding Microsoft Windows Servers section in the Veeam Backup & Replication User Guide. After you assigned the role of distribution server, you need to select this server in the properties of a protection group. To learn more, see Specify Discovery and Deployment Options.

A machine performing the role of the distribution server must meet the following requirements:

- The role of the distribution server can be assigned to a physical or virtual machine.
- The machine must run a 64-bit Microsoft Windows OS.
- You must add the machine to the Veeam Backup & Replication console as a managed server.

The distribution server comprises the following services and components:

- Veeam Distribution Service
- Veeam Plug-in for SAP HANA Redistributable
- Veeam Plug-in for Oracle RMAN Redistributable
- Veeam Plug-in for SAP on Oracle Redistributable


Backup server
Backup storage
Components:
Veeam Distribution Service
Veeam Plug-in for SAP HANA Redistributable
Veeam Plug-in for Oracle RMAN Redistributable
Veeam Plug-in for SAP on Oracle Redistributable
Requirements:
Physical/virtual
64-bit Microsoft Windows OS
Database server with Veeam Plug-in
Distribution server

Computer Discovery and Veeam Plug-in Deployment

Veeam Backup & Replication supports automated and manual deployment of Veeam Plug-ins on computers in your infrastructure.

You can deploy Veeam Plug-in for Oracle RMAN, Veeam Plug-in for SAP HANA, and Veeam Plug-in for SAP on Oracle from the Veeam Backup & Replication console. To deploy Veeam Plug-ins, Veeam Backup & Replication needs to discover computers whose data you want to back up. To enable discovery, you organize your computers into one or more protection groups. Protection group settings define what computers Veeam Backup & Replication will discover and how the discovery process will run. To learn more, see Protection Groups.

You can also disable automated Veeam Plug-in installation when configuring a protection group. In this case, you will need to use the Veeam Backup & Replication console to install Veeam Plug-in on every computer included in the protection group. To learn more, see Installing Veeam Plug-in.

Protection Groups

In Veeam Backup & Replication, computers that you want to protect with Veeam Plug-ins are organized into protection groups. A protection group is a container in the Veeam Backup & Replication inventory aimed to combine protected computers of a specific type. For example, you can use a dedicated protection group for computers of the same type or computers running the same OS type to simplify management of such computers. You can also use a separate protection group for computers that you want to manage in a different way from other computers in your infrastructure.

To start managing Veeam Plug-ins in Veeam Backup & Replication, you need to create a protection group in the inventory and specify computers that you want to protect with Veeam Plug-ins in the protection group settings. You can create one or more protection groups depending on the size and complexity of your infrastructure. Protection groups appear under the **Physical Infrastructure** node in the **Inventory** view of the Veeam Backup & Replication console. To learn more, see Working with Protection Groups.

Protection groups allow you to automate deployment and management of Veeam Plug-ins on computers in your infrastructure. When you configure a protection group, you can specify scheduling options for protected computers discovery and Veeam Plug-in deployment. You do not need to perform administrative tasks individually for every computer that you want to protect with Veeam Plug-in — Veeam Backup & Replication will perform the specified operations automatically upon the defined schedule.

Veeam Backup & Replication connects to discovered computers using credentials of the account specified in the protection group settings. You can specify a master account that Veeam Backup & Replication will use to connect to all computers added to the protection group or specify separate accounts to connect to specific computers in the protection group.

After you create a protection group, Veeam Backup & Replication starts the rescan job to connect to computers added to the protection group and perform the required operations on these computers. To learn more, see Rescan Job.

Protection Group Types

Veeam Backup & Replication offers several methods to specify computers on which you want to install and manage Veeam Plug-ins. You can create protection groups that include the following types of objects:

- **Individual computers**

  You can organize individual computers into a protection group by specifying the necessary computers in the protection group settings. This option is recommended for smaller environments that do not have Microsoft Active Directory deployed.

- **Microsoft Active Directory objects**

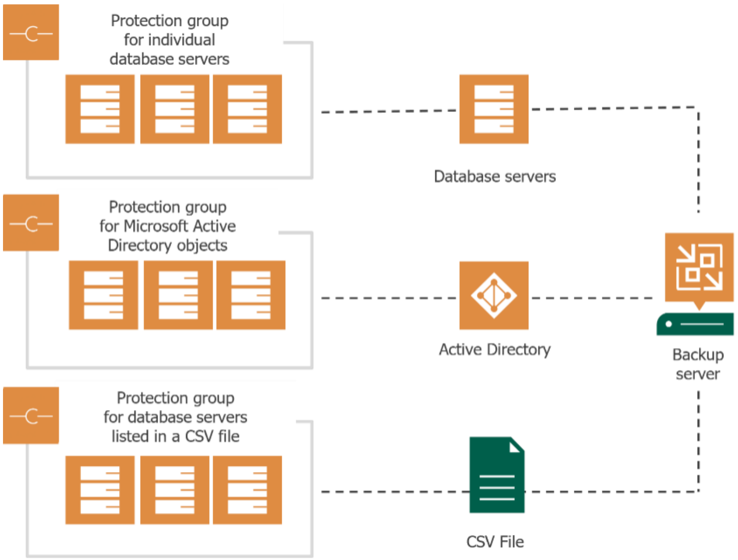
  You can create protection groups that include one or more Microsoft Active Directory objects: entire domain, container, organization unit, group, computer or cluster. This allows you to manage Veeam Plug-ins on computers being part of an Active Directory domain. Protection groups that include Active Directory domain, containers, groups and/or organization units are dynamic in their nature. For example, if a new computer is added to a container, Veeam Backup & Replication will automatically discover this computer and start managing this computer as specified in the protection group settings.

  You can specify a protection scope based on Active Directory objects in one of the following ways:

  - You can select individual Active Directory objects that you want to include in a protection group, for example, selected organization units and/or computers.
  - You can include in the protection group an entire domain or other Active Directory object (such as a container or organization unit) and exclude specific child objects being part of this object, for example, selected organization units and/or computers.

- **Computers listed in a CSV file**

  You can add multiple computers to a protection group by importing a list of computers from a CSV file. Protection groups that include computers listed in a CSV file are also dynamic. If a new computer appears in a CSV file after the protection group is created, during the next protection group rescan session, Veeam Backup & Replication will automatically update the protection group settings to include the added computer.


Protection group for individual database servers
Database servers
Protection group for Microsoft Active Directory objects
Active Directory
Backup server
Protection group for database servers listed in a CSV file
CSV File

Predefined Protection Groups

In addition to protection groups created by a user, the Veeam Backup & Replication inventory may contain one or more predefined protection groups.

Unmanaged

The *Unmanaged* protection group acts as a filter to display computers with unmanaged Veeam Plug-ins, that is, computers that meet the following conditions:

1. Have Veeam Plug-in deployed and configured directly from a computer side.
2. Run a backup job targeted at a backup repository managed by Veeam Backup & Replication.

You cannot perform any operations with the *Unmanaged* protection group, as well as add computers included in this group to an application backup policy. However, you can move such computers to a protection group that you created. To learn more, see Moving Unmanaged Computer to Protection Group.

After you move an unmanaged computer to a protection group, Veeam Backup & Replication will start managing Veeam Plug-in running on this computer according to discovery settings specified in the properties of the protection group. If the protection group is added to an application backup policy, Veeam Backup & Replication will add the new computer to the policy too. You will no longer be able to manage Veeam Plug-in directly on the computer.

Out of Date

The *Out of Date* protection group is displayed when Veeam Backup & Replication discovers protected computers on which an outdated version of Veeam Plug-in is installed. For example, this may happen in a situation where you configure a protection group with Veeam Plug-in deployment options disabled, and Veeam Backup & Replication detects a newer version of Veeam Plug-in on the distribution server during discovery.

The *Out of Date* protection group lets you update Veeam Plug-in on multiple computers at once. To learn more, see Upgrading Plug-in.

Offline

The *Offline* protection group acts as a filter to display computers to which Veeam Backup & Replication could not connect during the latest rescan session.

Untrusted

The *Untrusted* protection group acts as a filter to display Linux-based computers whose fingerprints were not verified in Veeam Backup & Replication. For computers included in this protection group, you need to check and validate SSH fingerprints. To learn more, see Validating SSH Fingerprints.

Rescan Job

For automated discovery of protected computers, Veeam Backup & Replication uses the rescan job that runs on the backup server. Veeam Backup & Replication automatically creates this job once you create the first protection group in the inventory. The rescan job runs upon schedule defined individually for every protection group in the protection group settings. By default, Veeam Backup & Replication is set up to perform discovery at 9:00 PM daily. You can adjust daily schedule in the protection group settings or define periodic schedule.

The rescan job itself is not displayed in the Veeam Backup & Replication console. However, you can start and stop rescan job sessions manually for a specific protection group or individual computer in the inventory. This may be helpful, for example, if new computers appeared in your infrastructure, and you want to discover these computers without waiting for the next scheduled rescan job session start. To learn more, see Rescanning Protection Group and Rescanning Protected Computer.

You can view statistics for currently running and already performed rescan job sessions. To learn more, see Viewing Rescan Job Statistics.

How It Works

When the rescan job is started — either automatically upon schedule or manually — Veeam Backup & Replication performs the following operations:

1. Obtains settings specified for the protection group from the configuration database. The settings include a list of computers to scan, an account for connecting to these computers, and so on.
2. Connects to each computer in the list under the specified account:
   - On Microsoft Windows computers, Veeam Backup & Replication connects to a computer using the administrative share (admin$) of the target computer. An account that you plan to use to connect to a computer included in the protection group must have access to the administrative share.
   - On Linux computers, Veeam Backup & Replication connects to a computer using SSH.

     Keep in mind that to connect to Linux computer via SSH, this Linux computer must be added to the list of trusted hosts. To learn more, see Configuring Security Settings.
3. Deploys Veeam Installer Service on each newly discovered computer.

   In case of Linux-based computers, Veeam Backup & Replication also deploys Veeam Deployer Service.
4. If the automatic Veeam Plug-in deployment option is enabled in the protection group settings, Veeam Backup & Replication deploys Veeam Plug-in on discovered computers. As a part of this process, Veeam Backup & Replication performs the following operations:
   a. Veeam Installer Service running on the computer collects information about the computer and sends it to Veeam Backup & Replication. The collected data includes details on the computer (platform, host name, guest OS, IP address, BIOS UUID) and Veeam Plug-in (product presence on the computer and version).

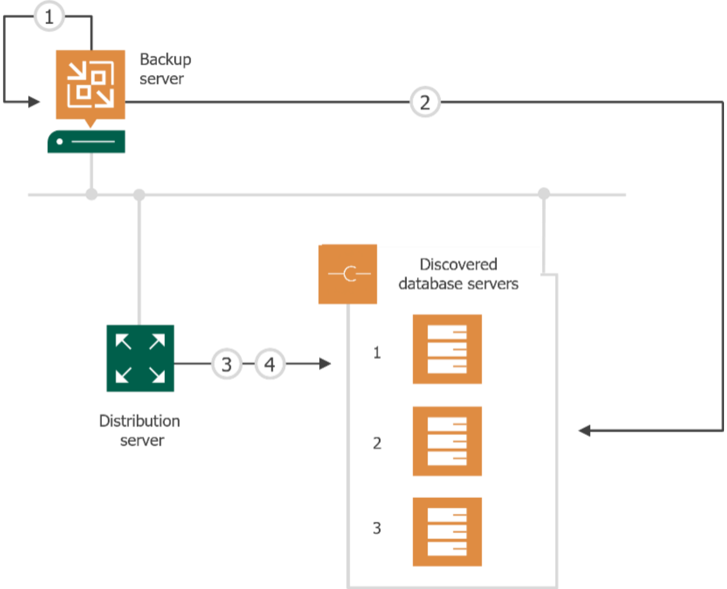
   b. Veeam Backup & Replication uploads the Veeam Plug-in setup file from the distribution server to the discovered computer.

   c. Veeam Installer Service deploys Veeam Plug-in and accompanying product components (for example, Plug-in Manager and Data Mover) on the target computer.

      If Veeam Installer Service detects that Veeam Plug-in is already deployed on the target computer, Veeam Backup & Replication becomes the owner of this Veeam Plug-in. To learn more, see Plug-in Ownership.

d. Veeam Installer Service retrieves the TLS certificate with a public key from the backup server and saves a TLS certificate with a public key in the Veeam Plug-in configuration database on the target computer. Veeam Plug-in will use this certificate to connect to Veeam Backup & Replication.

e. Plug-in Manager running on the target computer collects information about databases available on the target computer. To learn more, see Database Detection.



Plug-in Ownership

To manage Veeam Plug-ins on target computers, you must make Veeam Backup & Replication the owner of these Veeam Plug-ins. To do this, perform one of the following operations from Veeam Backup & Replication console:

- Using protection group, deploy Veeam Plug-ins remotely.
- Add computers with standalone Veeam Plug-ins to a protection group that is configured to deploy Veeam Plug-ins.

  If you add a computer with standalone Veeam Plug-in to a protection group that does not deploy Veeam Plug-ins, Veeam Backup & Replication will not be the owner of this Veeam Plug-in. In this case, you cannot perform any operations with Veeam Plug-in from the Veeam Backup & Replication console. To learn more, see Discovery and Deployment Options.

If Veeam Backup & Replication becomes the owner of Veeam Plug-in, this Veeam Plug-in switches to the managed mode. In the managed mode, a limited set of tasks can be done from the computer side.

You can perform the following tasks from the computer side:

- Create the backup using the backup policy configured in the Veeam Backup & Replication console.
- Restore data from backup to the original and new location.

IMPORTANT

You cannot perform the following tasks from the computer side:

- Create backup of a database that is not added to the backup policy on the Veeam Backup & Replication server. You can still create backup of such database on other targets. For example, local storage or shared folder.
- Edit backup policy settings.

You can run the following commands from the computer side:

- `--showconfig`
- `--help`
- `--set-force-delete`
- `--set-clustername`
- [For Veeam Plug-in for SAP HANA and Veeam Plug-in for SAP on Oracle] `--set-backup-for-restore`
- [For Veeam Plug-in for Oracle RMAN] `--set-auth-data-for-restore`
- [For Veeam Plug-in for Oracle RMAN] `--get-backup-id`

On the computer, you can check the current owner of Veeam Plug-in. If Veeam Plug-in is managed by Veeam Backup & Replication, the following Veeam Backup & Replication connection parameters will be available in the `config.xml` file:

```
<VBRConnectionParams vbrHostName=<hostname> vbrPort=<port_number> vbrUser=<user
name> vbrDomain=<domain> vbrPassword=<password> vbrName=<name> vbrId=<ID> />
```

where:

- `<hostname>` — IP address or hostname of the Veeam Backup & Replication server.
- `<port_number>` — port over which Veeam Plug-in must communicate with Veeam Backup & Replication. The default port used for communication with the Veeam Backup & Replication server is 10006.
- `<username>` — a name of the account that has access to the Veeam Backup & Replication server.
- `<domain>` — a name of the domain in which the account that has access to the Veeam Backup & Replication server is registered.
- `<password>` — password of the account that has access to the Veeam Backup & Replication server.
- `<name>` — name of the Veeam Backup & Replication server.
- `<ID>` — ID of the Veeam Backup & Replication server.

IMPORTANT

A plug-in can be managed by one Veeam Backup & Replication server only. If Veeam Backup & Replication tries to become the owner of Veeam Plug-in that is already managed by another Veeam Backup & Replication, Veeam Backup & Replication will not change the owner and you will get a warning message.

Database Detection

After Veeam Plug-in is installed, Plug-in Manager running on the computer collects information about databases on this computer. Plug-in Manager saves collected information to the XML file and sends to Veeam Backup & Replication. The way Plug-in Manager collects information differs depending on the system installed on the computer:

- Oracle
- SAP HANA
- SAP on Oracle

Oracle

On the Oracle server, Plug-in Manager collects information differently depending on the Oracle deployment way:

- If you install Veeam Plug-in on the standalone Oracle server, the rescan process differs depending on the OS running on the target computer:
  - In case of Oracle server deployed on the Linux computer, Plug-in Manager scans the *oratab* or *orainventory* file. If you use Oracle ASM, Plug-in Manager rescans both files (*oratab* and *orainventory*).
  - In case of Oracle server deployed on the Microsoft Windows computer, Plug-in Manager checks Windows Registry and parses services that are running on the computer.

  As a result, Veeam Backup & Replication gets 3 levels of the database hierarchy (from top to bottom): hostname, Oracle home, Oracle system identifier (SID).

- If you install Veeam Plug-in on Oracle RAC, Plug-in Manager uses the *srvctl* utility. With this utility, Plug-in Manager collects information using the `srvctl config scan` and `srvctl config database` commands.

  As a result, Veeam Backup & Replication gets 3 levels of the database hierarchy (from top to bottom): scanname, Oracle home, Oracle system identifier (SID).

After rescan completes, you can create an application policy and add any level of the database hierarchy to the scope of this policy. For example, you can add a certain Oracle database or Oracle home that contains several databases.

SAP HANA

On the SAP HANA server, Plug-in Manager collects information depending on the SAP HANA deployment way:

- If you install Veeam Plug-in on the standalone SAP HANA server, Plug-in Manager gets path to the *saphostcrl* (SAP Host Agent) utility. With this utility, Plug-in Manager gets the list of database instances.

  As a result, Veeam Backup & Replication gets 3 levels of the database hierarchy (from top to bottom): hostname, SAP system name, database name.

- If you install Plug-in Manager on the SAP HANA scale-out system, Plug-in Manager collects information from the *config.xml* file.

  As a result, Veeam Backup & Replication gets 3 levels of the database hierarchy (from top to bottom): scale-out system name, SAP system name, SAP name.

> **TIP**
>
> During the Veeam Plug-in deployment on the scale-out system nodes, Veeam Backup & Replication sets the scale-out system name using domain name and SAP system name. If you want to set a custom name, use the `set-clustername` command on the computer side. This custom name will be saved in the *config.xml* file.

After rescan completes, you can create an application policy and add any level of the database hierarchy to the scope of this policy. For example, you can add a certain SAP HANA database or a host that contains several SAP HANA databases.

SAP on Oracle

On the SAP on Oracle server, Plug-in Manager gets path to the saphostcrl (SAP Host Agent) utility. With this utility, Plug-in Manager gets the list of database instances.

As a result, Veeam Backup & Replication gets 2 levels of the database hierarchy (from top to bottom): hostname, Oracle system identifier (SID).

> **IMPORTANT**
>
> Veeam Backup & Replication does not support cluster deployment of SAP on Oracle.

After rescan completes, you can create an application policy and add any level of the database hierarchy to the scope of this policy. For example, you can add a certain Oracle database or a host that contains several Oracle databases.

Application Backup Policies

To back up databases on your computers with Veeam Plug-ins, you must configure an application backup policy. An application backup policy is a task that defines what data to back up, how, where and when to back up data.

After you configure the application backup policy on the Veeam Backup & Replication server side, Veeam Plug-ins create transport jobs on your computers. Using these transport jobs, Veeam Backup & Replication orchestrates the backup operations. Transport jobs collect backed-up data and send it from your computers to the backup repository. Each transport job creates an independent backup. For example, if the application backup policy orchestrates 3 transport jobs, a backup repository will store 3 backup files, one file per each transport job.

Backing Up One Computer with Multiple Policies

You can add a database only to one application backup policy. But, you can still configure several application backup policies to back up different databases on the same computer. For example, if you want to back up a staging database and a production database according to different schedules, you must create two application backup policies. In this case, each of these policies will orchestrate its transport job that will produce a backup and send it to a backup repository.

How It Works

After you configure an application backup policy, this backup policy functions in the following way:

1. The backup policy is waiting for the next backup run.

   The backup policy is running continuously. When there is no active backup activities, the backup policy is set to an idle state. This state allows the backup policy to catch warnings and display them in the backup policy statistics.

2. Before starting the next backup run, Veeam Backup & Replication finishes the active session. The backup policy sends a report to Veeam Backup & Replication. The finished session becomes available in the **History** view of the Veeam backup console. To learn more, see Viewing Backup Policy Report and Viewing Backup Policy Statistics.

3. If database log processing is enabled, the backup policy restarts the database log backup run. Database log backup is a separate task that runs in parallel with the database backup.

4. The backup policy creates a list of backup tasks, detects and configure Veeam Plug-ins. Veeam Plug-ins run the backup operations on computers.

5. Transport jobs on computers send backed-up data from computers to the backup repository.

   An application backup policy may consist of several activities. For example, database backup according to the policy schedule, database logs backup according to a separate schedule, and manual database backup. In this case, Veeam Plug-in will store the backed-up data for all activities in the same backup.

6. The backup policy sends a report to Veeam Backup & Replication about backed-up and transported data.

After all backup activities are finished, the backup policy returns to the idle state and waits for the next backup run.

Planning and Preparation

Before you start using the Veeam Plug-in management functionality in Veeam Backup & Replication, make sure that the Veeam backup server and computers that you plan to protect with Veeam Plug-ins meet the system requirements and all required ports are open.

System Requirements

Make sure that components in the plug-in management infrastructure meet system requirements listed below.

Veeam Backup Server

To learn about system requirements for the Veeam backup server and other Veeam Backup & Replication components, see the System Requirements section in the Veeam Backup & Replication User Guide.

Computer with Veeam Plug-in for Oracle RMAN

A computer with databases you want to protect using Veeam Plug-in for Oracle RMAN must meet the following requirements:

Specification	Requirement
OS	The following operating systems are supported: • Microsoft Windows: ○ Microsoft Windows Server 2008 R2 ○ Microsoft Windows Server 2012/2012 R2 ○ Microsoft Windows Server 2016 ○ Microsoft Windows Server 2019 ○ Microsoft Windows Server 2022 • Linux: ○ SUSE Linux Enterprise Server 11, 12, 15 (x86 and x86_64) ○ Red Hat Enterprise Linux 6.4–8.x (x86 and x86_64) ○ Oracle Linux 6.4–8.x (x86 and x86_64) ○ CentOS 6.4–8.x (x86 and x86_64): For non-production environments, as it is not officially supported by Oracle for their databases.
Software	[For Microsoft Windows computers] Microsoft .NET Framework 4.6 is included in the Veeam Plug-in for Oracle RMAN Redistributable. During the deployment process, Veeam Backup & Replication checks whether Microsoft .NET Framework 4.6 is available on the target computer. If Microsoft .NET Framework 4.6 is missing, Veeam Backup & Replication will install missing software automatically.
Database	Oracle database 11gR2, 12c, 18c, 19c, 21c: Standard and Enterprise Edition. Express Edition is not supported.

Specification	Requirement
Oracle RMAN features	The following Oracle RMAN features are supported: • Veeam Plug-in for Oracle RMAN will be registered as an SBT_TAPE device. All Oracle RMAN functionality that is supported with the SBT_TAPE device type will work. For example, Oracle ASM and Container DBs (CDBs). • Veeam Plug-in for Oracle RMAN supports Oracle Real Application Clusters (Oracle RAC). Other cluster databases are not supported. Keep in mind that multiple Oracle homes on Microsoft Windows computers are not supported.

Computer with Veeam Plug-in for SAP HANA

A computer with databases you want to protect using Veeam Plug-in for SAP HANA must meet the following requirements:

Specification	Requirement
OS	The following operating systems are supported: • SLES for SAP Applications 15 (x86_64): GA, SP1, SP2, SP3. • SLES for SAP Applications 12 (x86_64): GA, SP1, SP2, SP3, SP4, SP5. • RHEL for SAP Solutions 8 (x86_64): 8.0, 8.1, 8.2, 8.4, 8.4. • RHEL for SAP Solutions 7 (x86_64): 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.9
Database	SAP HANA 2.0: SPS 02, SPS 03, SPS 04, SPS 05 (only with Backint version 1.0), SPS06. Express Edition is not supported.

Computer with Veeam Plug-in for SAP on Oracle

A computer with databases you want to protect using Veeam Plug-in for SAP on Oracle must meet the following requirements:

Specification	Requirement
OS	The following operating systems are supported: • SUSE Linux Enterprise Server 11, 12, 15 (x86_64) • Red Hat Enterprise Linux for SAP Applications 6, 7 (x86_64)
BR*Tools	BR*Tools 7.20 Patch 42 or later.

Specification	Requirement
Database	Oracle Database 11gR2, 12c, 18c, 19c: Standard and Enterprise Edition. Express Edition is not supported.

Network

Veeam Plug-in should be able to establish a direct IP connection to the Veeam Backup & Replication server. Thus, Veeam Plug-in cannot work with the Veeam Backup & Replication server that is located behind the NAT gateway.

Licensing Requirements

The Veeam Plug-in management functionality is licensed by the number of instances. Instances are units (or tokens) that you can use to protect your computers with Veeam Plug-ins. If the license is not valid or out of resources, Veeam Plug-in backup jobs fail.

The number of instances that you can use depends on the type of license installed in Veeam Backup & Replication:

- For Veeam Universal Licensing (VUL)

  You can use Veeam Plug-ins with all license packages (*Veeam Backup Essentials, Veeam Backup & Replication, Veeam Availability Suite*).

  Keep in mind that if you use the *Rental* license type, functionality of Veeam Plug-ins is supported only for the *Enterprise Plus* edition of Veeam Backup & Replication.

- For Perpetual Socket license

  Functionality of Veeam Plug-ins is supported only for the *Enterprise Plus* edition of Veeam Backup & Replication.

For the full list of license packages, see Pricing and Packaging.

Ports

The following links lead to tables that list network ports that must be opened to ensure proper communication of components in the Veeam Plug-in management infrastructure.

For information about network ports that must be opened to ensure proper communication of the backup server with backup infrastructure components, see the Ports section in the Veeam Backup & Replication User Guide.

In addition to general port requirements applicable to a Veeam backup server, the backup server used in the Veeam Plug-in management scenario must have the following ports opened:

- Veeam Plug-in for Oracle RMAN
- Veeam Plug-in for SAP HANA
- Veeam Plug-in for SAP on Oracle

Getting Started

To start using the Veeam Plug-in management functionality in Veeam Backup & Replication, you must perform the following operations:

1. Deploy Veeam Backup & Replication.

   To learn more, see the Deployment section in the Veeam Backup & Replication User Guide.

2. Configure security settings.

   By default, Veeam Backup & Replication offers the following settings to establish a secure connection between the backup server and protected computers:

   - To establish a secure connection between parties, Veeam Backup & Replication uses the default self-signed certificate.

   - Veeam Backup & Replication allows all new Linux hosts to establish a connection to the backup server.

   You can use the default security settings or change them if needed. To learn more, see Configuring Security Settings.

3. Add computers with databases that you want to protect to the Veeam Backup & Replication inventory.

   In Veeam Backup & Replication, computers with databases that you want to protect are organized into protection groups. You can use the Veeam Backup & Replication console to create one or more protection groups that include individual computers, Microsoft Active Directory objects, or list of computers imported from a CSV file. To learn more, see Creating Protection Groups.

4. Discover computers and deploy Veeam Plug-ins.

   During protection group configuration, you can set Veeam Backup & Replication to automatically discover computers and install Veeam Plug-ins on discovered computers. In this case, these operations are performed immediately after you create a protection group. To learn more, see Discovery and Deployment Options.

   You can also run discovery and deployment operations manually for an individual computer in a protection group. To learn more, see Rescanning Protected Computer.

5. Configure an application backup policy.

   You can configure one or more application backup policies and add to these policies one or more protection groups, Active Directory objects and/or individual computers. In Veeam Backup & Replication, you can configure application backup policies for the following Veeam Plug-ins:

   - Veeam Plug-in for Oracle RMAN

   - Veeam Plug-in for SAP HANA

   - Veeam Plug-in for SAP on Oracle

6. Manage application backup policies.

   You can start, stop, enable and disable application backup policies to administer data protection operations on protected computers. To learn more, see Managing Application Backup Policy.

7. In case of a disaster, you can use created application backups to restore database data.

   To learn more, see Managing Application Backups.

Configuring Security Settings

When you configure the Veeam Plug-in management infrastructure in Veeam Backup & Replication, you can specify what security settings Veeam Backup & Replication will use to establish a secure connection between the backup server and protected computers. By default, Veeam Backup & Replication offers the following security settings:

- To establish a secure connection between parties, Veeam Backup & Replication uses the default self-signed TLS certificate.
- Veeam Backup & Replication allows all computers that run a Linux OS to establish a connection to the backup server using the SSH fingerprint.

Keep in mind that default security settings are only for testing and evaluation purposes. To prevent potential security issues, you can change security settings. For example, you can use a custom TLS certificate and verification of Linux host SSH fingerprints.

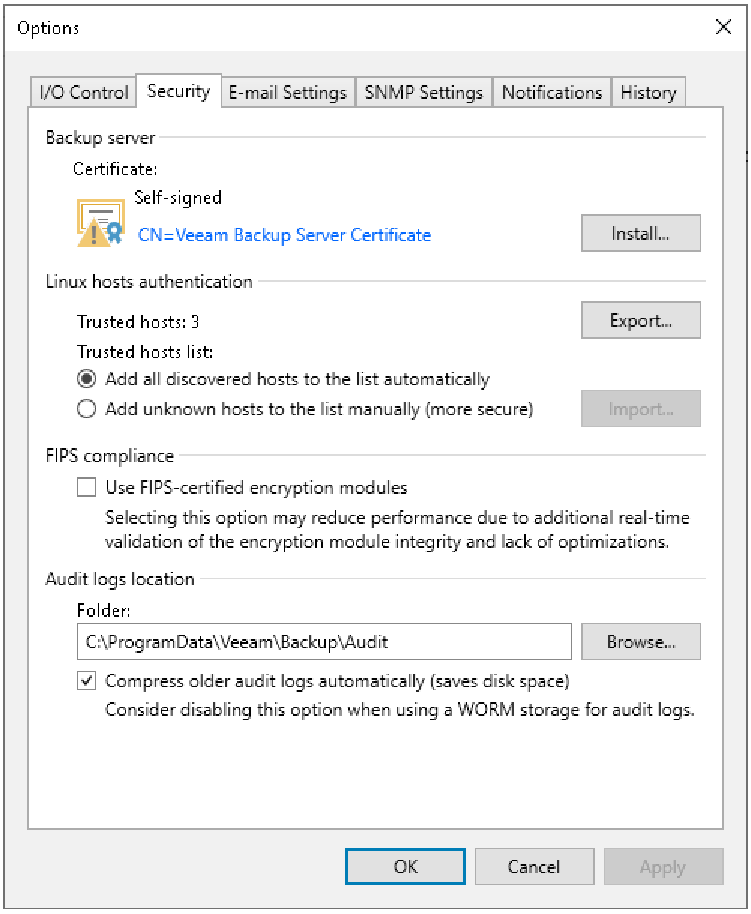
To specify the security settings, do the following:

1. From the main menu, select **General Options**.
2. Click the **Security** tab.
3. In the **Certificate** section, check information about the currently used certificate. By default, Veeam Backup & Replication uses a self-signed TLS certificate generated during the Veeam Backup & Replication installation process. If you want to use a custom certificate, click **Install** and specify a new certificate. To learn more, see Managing TLS Certificates.
4. In the **Linux hosts authentication** section, specify how Veeam Backup & Replication will add Linux-based protected computers to the list of trusted hosts. You can select one of the following options:
   - **Add all discovered hosts to the list automatically** — with this option enabled, Veeam Backup & Replication allows all discovered computers that run a Linux OS to connect to the backup server. This scenario is recommended for demo environments only.
   - **Add unknown hosts to the list manually (more secure)** — with this option enabled, only the following Linux-based computers can connect to the backup server:
     - Protected computers that have already established a connection to the backup server and have their fingerprints stored in the Veeam Backup & Replication database. Veeam Backup & Replication displays the number of such computers in the **Trusted hosts** field. You can export the list of trusted Linux computers to a *known_hosts* file. To do this, click **Export** and specify a path to the folder to save the file.
     - Protected computers specified in the *known_hosts* file imported to Veeam Backup & Replication. To import a *known_hosts* file, click **Import** and specify a path to the folder where the file resides.
     - Protected computers added to the list of trusted hosts in the Veeam Backup & Replication console. To learn more, see Adding Computers to Trusted Hosts List.

   The computers that are not in the list of trusted hosts cannot connect to the Veeam backup server and download Veeam Plug-in installation packages during discovery.
5. Click **OK**.

TIP

To learn more about other security settings available on the **Security** tab, see the Configuring Security Settings section in the Veeam Backup & Replication User Guide.



Backup server

Certificate:

Self-signed

CN=Veeam Backup Server Certificate

Linux hosts authentication

Trusted hosts: 3

Trusted hosts list:

● Add all discovered hosts to the list automatically

○ Add unknown hosts to the list manually (more secure)

FIPS compliance

□ Use FIPS-certified encryption modules

Selecting this option may reduce performance due to additional real-time validation of the encryption module integrity and lack of optimizations.

Audit logs location

Folder:

C:\ProgramData\Veeam\Backup\Audit

☑ Compress older audit logs automatically (saves disk space)

Consider disabling this option when using a WORM storage for audit logs.

Managing TLS Certificates

When you configure the Veeam Plug-in management infrastructure, you can specify what TLS certificate must be used to establish a secure connection between the backup server and protected computers. Veeam Backup & Replication offers the following options for TLS certificates:

- You can choose to keep the default self-signed TLS certificate generated by Veeam Backup & Replication.
- You can use Veeam Backup & Replication to generate a new self-signed TLS certificate. To learn more, see Generating Self-Signed Certificates.
- You can select an existing TLS certificate from the certificates store. To learn more, see Importing Certificates from Certificate Store.
- You can import a TLS certificate from a file in the PFX format. To learn more, see Importing Certificates from PFX Files.

> NOTE
>
> If you plan to use a certificate issued by your own Certificate Authority (CA), make sure that the certificate meets the requirements. To learn more, see Using Certificate Signed by Internal CA.

Generating Self-Signed Certificates

You can use Veeam Backup & Replication to generate a self-signed certificate for authenticating parties in the Veeam Plug-in management infrastructure.

To generate TLS certificates, Veeam Backup & Replication employs the RSA Full cryptographic service provider by Microsoft Windows installed on the Veeam backup server. The created TLS certificate is saved to the *Shared* certificate store. The following types of users can access the generated TLS certificate:

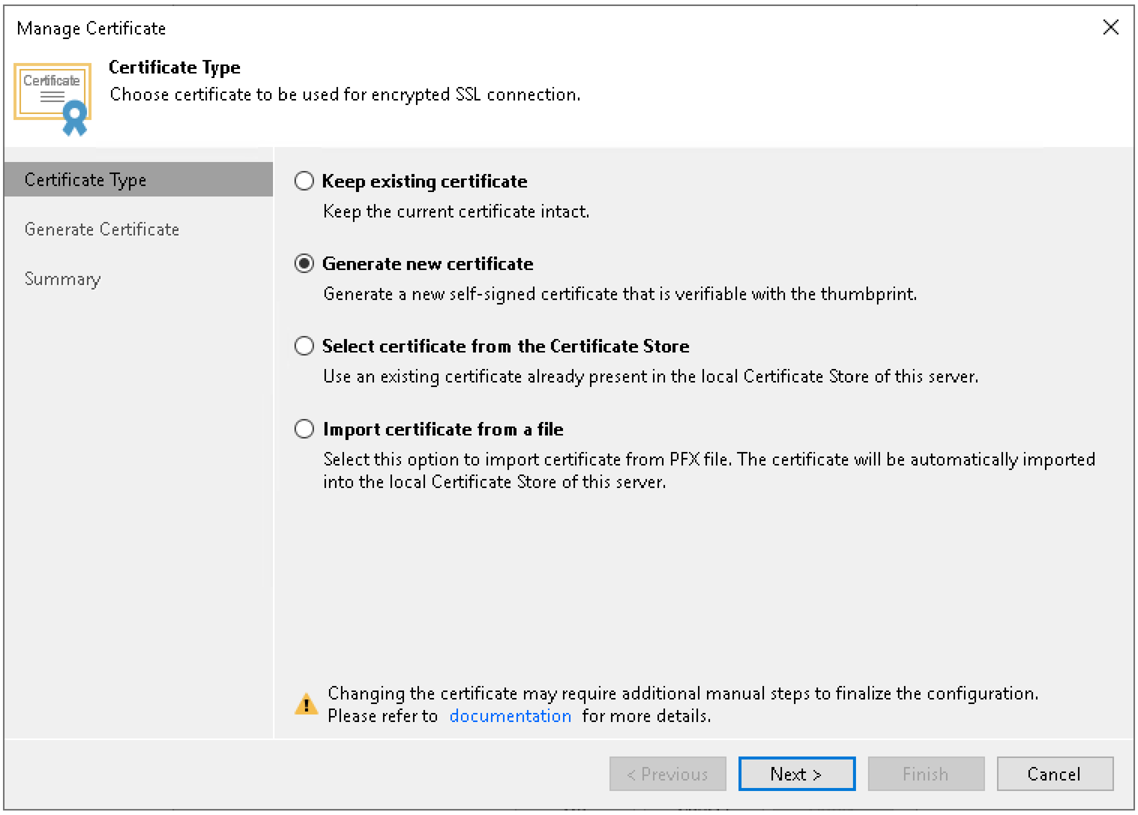
- User who created the TLS certificate
- LocalSystem user account
- Local Administrators group

If you use a self-signed TLS certificate generated by Veeam Backup & Replication, you do not need to take any additional actions to deploy the TLS certificate on a protected computer. When Veeam Backup & Replication discovers a protected computer, a matching TLS certificate with a public key is installed on the protected computer automatically. During discovery, Veeam Installer Service deployed on the protected computer retrieves the TLS certificate with a public key from the backup server and installs a TLS certificate with a public key on the protected computer.

> NOTE
>
> When you generate a self-signed TLS certificate with Veeam Backup & Replication, you cannot include several aliases to the certificate and specify a custom value in the *Subject* field. The *Subject* field value is taken from the Veeam Backup & Replication license installed on the Veeam backup server.

To generate a self-signed TLS certificate:

1. From the main menu, select **General Options**.
2. Click the **Security** tab.
3. In the **Security** tab, click **Install**.
4. At the **Certificate Type** step of the wizard, select **Generate new certificate**.



Manage Certificate

Certificate Type

Choose certificate to be used for encrypted SSL connection.

○ **Keep existing certificate**
Keep the current certificate intact.

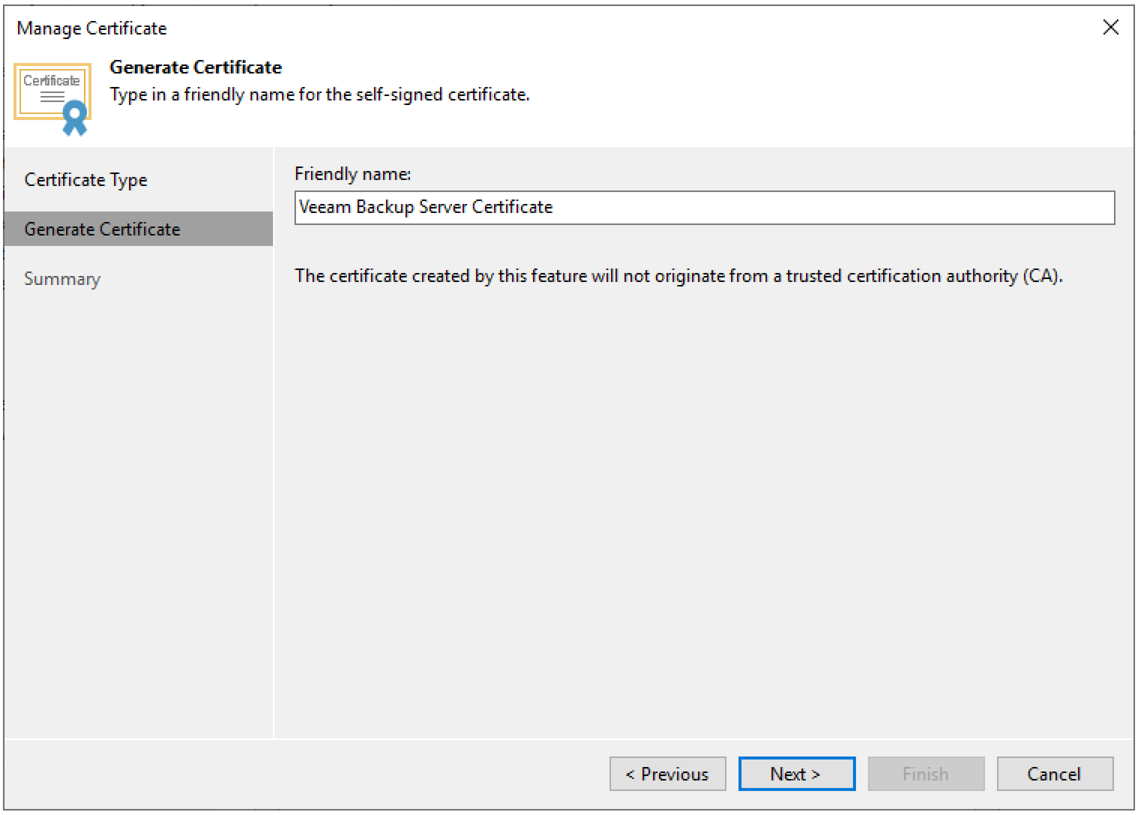
● **Generate new certificate**
Generate a new self-signed certificate that is verifiable with the thumbprint.

○ **Select certificate from the Certificate Store**
Use an existing certificate already present in the local Certificate Store of this server.

○ **Import certificate from a file**
Select this option to import certificate from PFX file. The certificate will be automatically imported into the local Certificate Store of this server.

Changing the certificate may require additional manual steps to finalize the configuration. Please refer to documentation for more details.

5. At the **Generate Certificate** step of the wizard, specify a friendly name for the created self-signed TLS certificate.



Manage Certificate

Generate Certificate

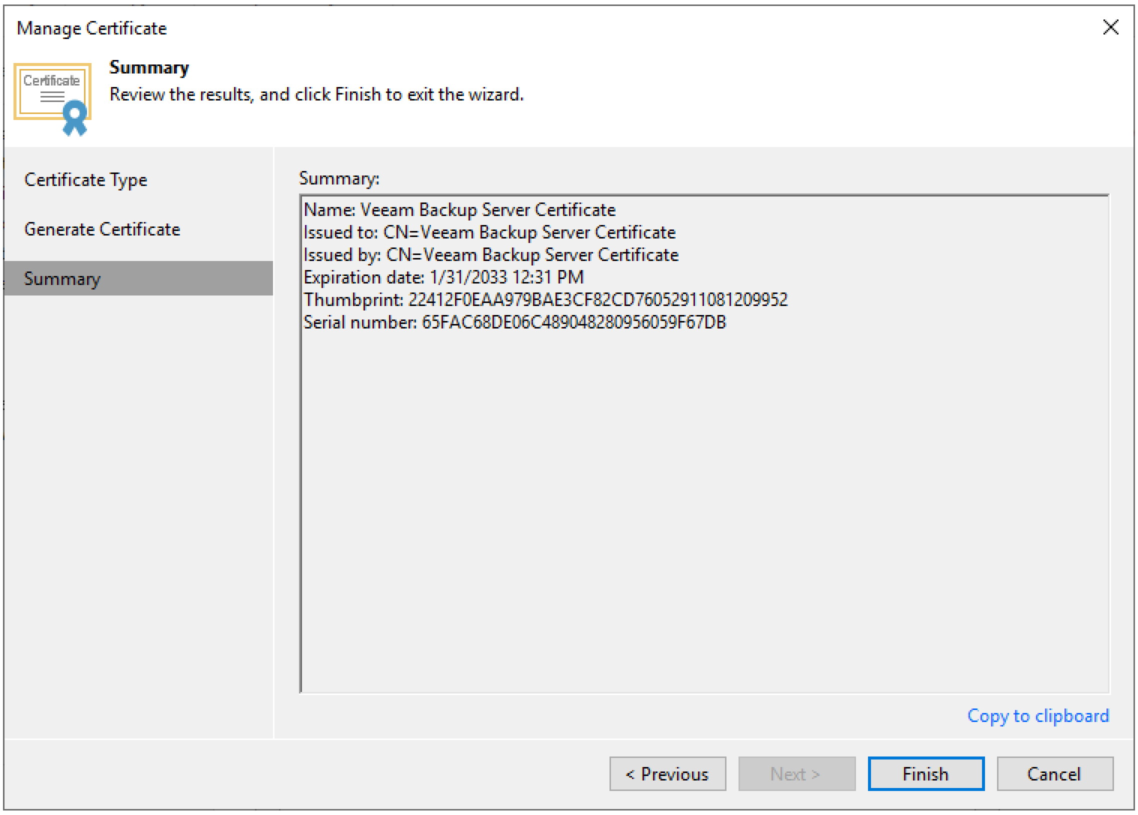
Type in a friendly name for the self-signed certificate.

Friendly name: Veeam Backup Server Certificate

The certificate created by this feature will not originate from a trusted certification authority (CA).

6. At the **Summary** step of the wizard, review the certificate properties. Use the **Copy to clipboard** link to copy and save information about the generated TLS certificate. You will be able to use the copied information to verify the TLS certificate with the certificate thumbprint.

7. Click **Finish**. Veeam Backup & Replication will save the generated certificate in the *Shared* certificate store on the Veeam backup server.



Summary:

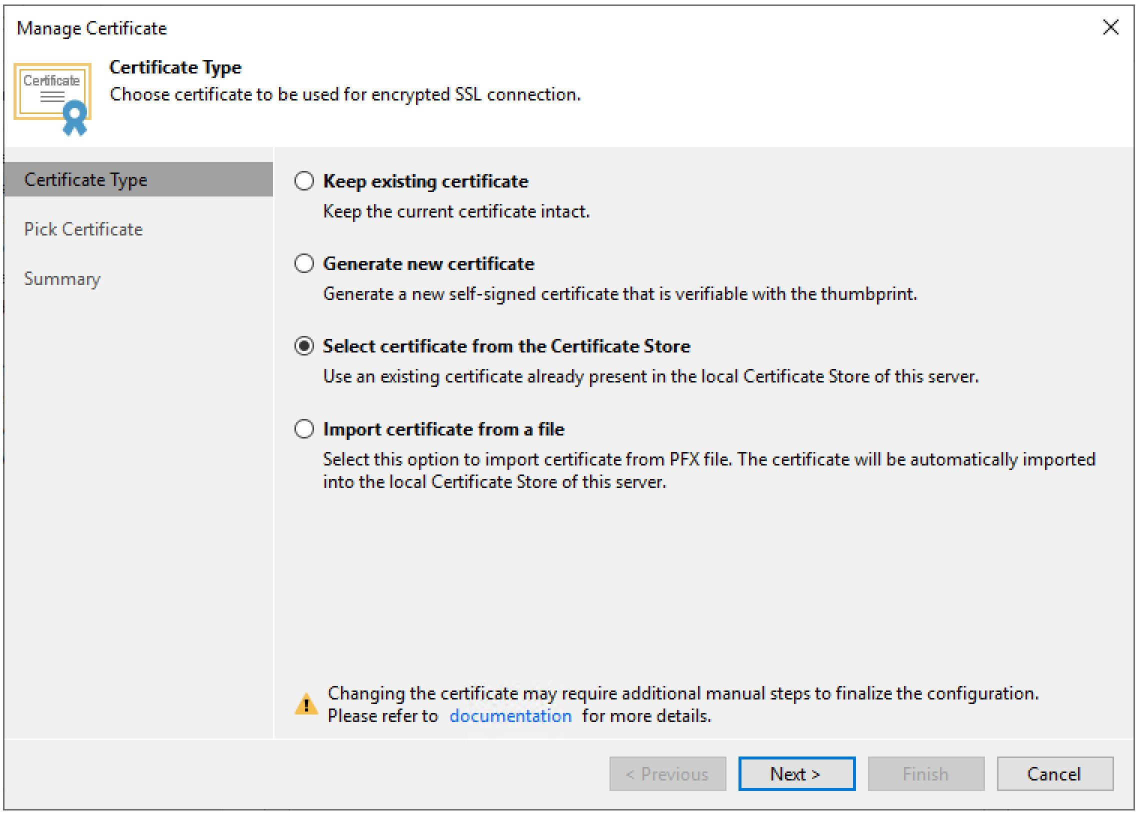
Name: Veeam Backup Server Certificate
Issued to: CN=Veeam Backup Server Certificate
Issued by: CN=Veeam Backup Server Certificate
Expiration date: 1/31/2033 12:31 PM
Thumbprint: 22412F0EAA979BAE3CF82CD76052911081209952
Serial number: 65FAC68DE06C489048280956059F67DB

Importing Certificates from Certificate Store

If your organization has a TLS certificate signed by a CA and the TLS certificate is located in the Microsoft Windows Certificate store, you can use this certificate for authenticating parties in the Veeam Plug-in management infrastructure.

To select a certificate from the Microsoft Windows Certificate store:

1. From the main menu, select **General Options**.
2. Click the **Security** tab.
3. In the **Security** tab, click **Install**.
4. At the **Certificate Type** step of the wizard, choose **Select certificate from the Certificate Store**.



Manage Certificate

Certificate Type

Choose certificate to be used for encrypted SSL connection.

○ **Keep existing certificate**

Keep the current certificate intact.

○ **Generate new certificate**

Generate a new self-signed certificate that is verifiable with the thumbprint.

● **Select certificate from the Certificate Store**

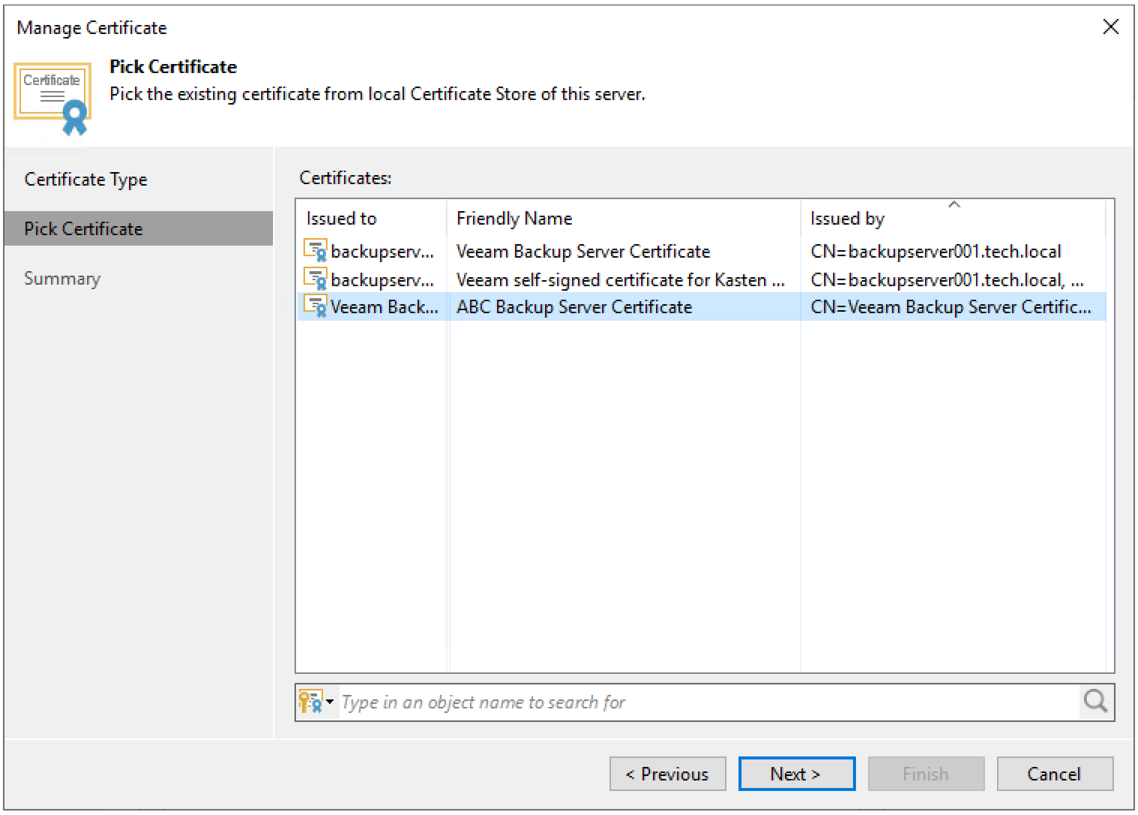
Use an existing certificate already present in the local Certificate Store of this server.

○ **Import certificate from a file**

Select this option to import certificate from PFX file. The certificate will be automatically imported into the local Certificate Store of this server.

Changing the certificate may require additional manual steps to finalize the configuration. Please refer to documentation for more details.

5. At the **Pick Certificate** step of the wizard, select a TLS certificate that you want to use. You can select only certificates that contain both a public key and a private key. Certificates without private keys are not displayed in the list.



Manage Certificate

Pick Certificate

Pick the existing certificate from local Certificate Store of this server.

Certificates:

Issued to	Friendly Name	Issued by
backupserv...	Veeam Backup Server Certificate	CN=backupserver001.tech.local
backupserv...	Veeam self-signed certificate for Kasten ...	CN=backupserver001.tech.local, ...
Veeam Back...	ABC Backup Server Certificate	CN=Veeam Backup Server Certific...

Type in an object name to search for

6. At the **Summary** step of the wizard, review the certificate properties.

7. Click **Finish** to apply the certificate.

Importing Certificates from PFX Files

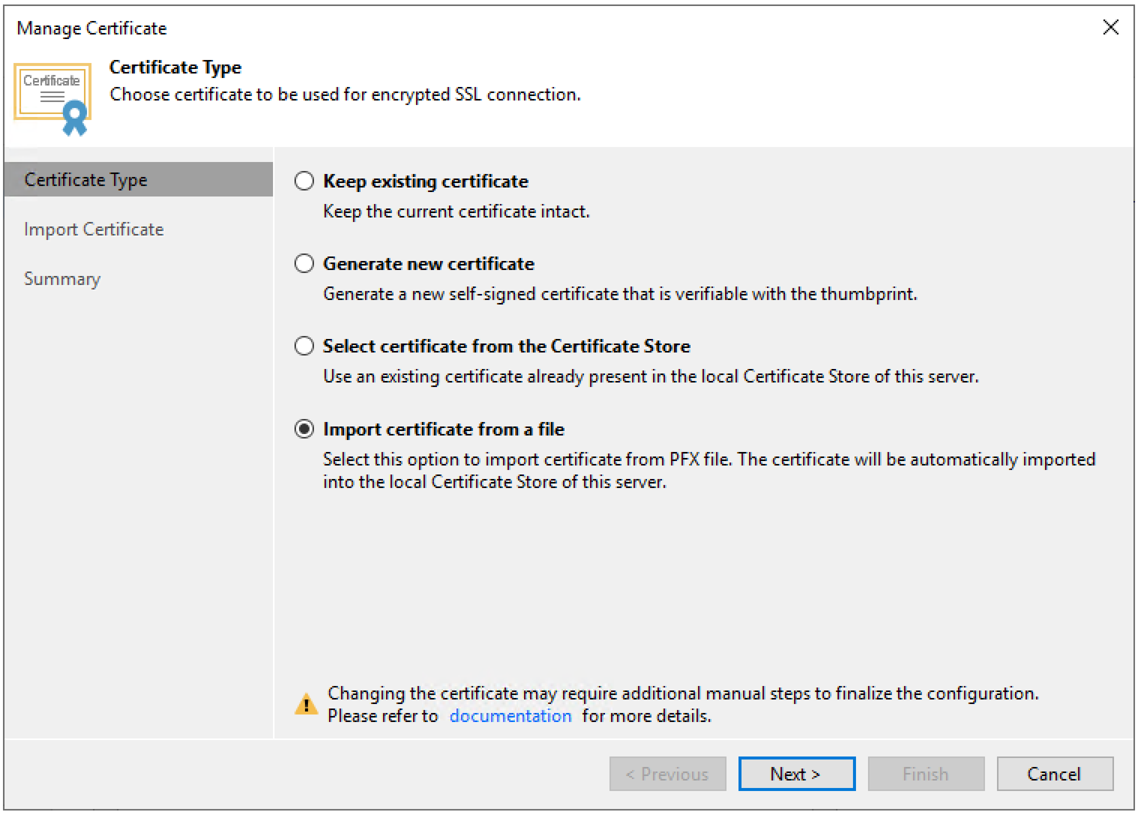
You can import a TLS certificate in the following situations:

- Your organization uses a TLS certificate signed by a CA and you have a copy of this certificate in a file of PFX format.
- You have generated a self-signed TLS certificate in the PFX format with a third-party tool and you want to import it to Veeam Backup & Replication.

> **IMPORTANT**
>
> The TLS certificate must pass validation on the Veeam backup server. In the opposite case, you will not be able to import the TLS certificate.

To import a TLS certificate from a PFX file:

1. From the main menu, select **General Options**.
2. Click the **Security** tab.
3. In the **Security** tab, click **Install**.
4. At the **Certificate Type** step of the wizard, choose **Import certificate from a file**.



Manage Certificate

Certificate Type
Choose certificate to be used for encrypted SSL connection.

○ **Keep existing certificate**
Keep the current certificate intact.

○ **Generate new certificate**
Generate a new self-signed certificate that is verifiable with the thumbprint.

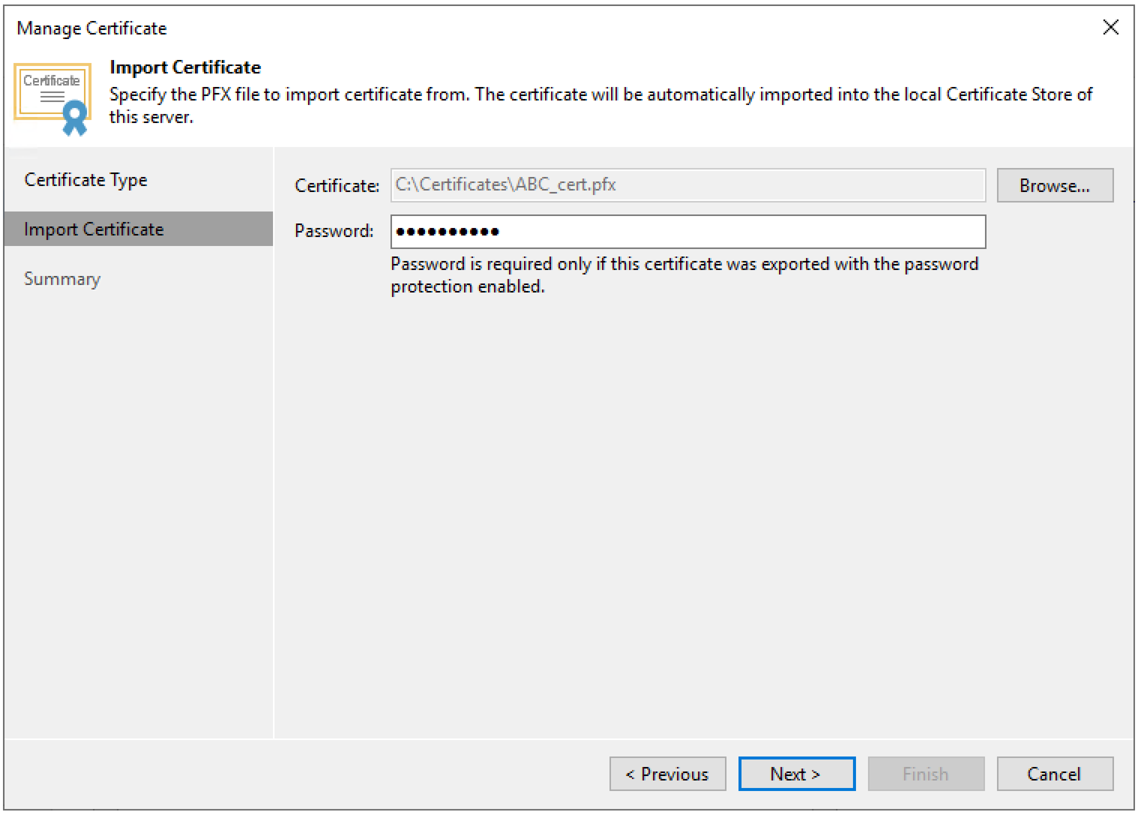
○ **Select certificate from the Certificate Store**
Use an existing certificate already present in the local Certificate Store of this server.

● **Import certificate from a file**
Select this option to import certificate from PFX file. The certificate will be automatically imported into the local Certificate Store of this server.

Changing the certificate may require additional manual steps to finalize the configuration.
Please refer to documentation for more details.

5. At the **Import Certificate** step of the wizard, specify a path to the PXF file.

6. If the PFX file is protected with a password, specify the password in the field below.



Manage Certificate

Import Certificate

Specify the PFX file to import certificate from. The certificate will be automatically imported into the local Certificate Store of this server.

Certificate: C:\Certificates\ABC_cert.pfx

Password: ●●●●●●●●●●●

Password is required only if this certificate was exported with the password protection enabled.

7. At the **Summary** step of the wizard, review the certificate properties. Use the **Copy to clipboard** link to copy and save information about the TLS certificate. You can use the copied information on a protected computer to verify the TLS certificate with the certificate thumbprint.

8. Click **Finish** to apply the certificate.

Using Certificate Signed by Internal CA

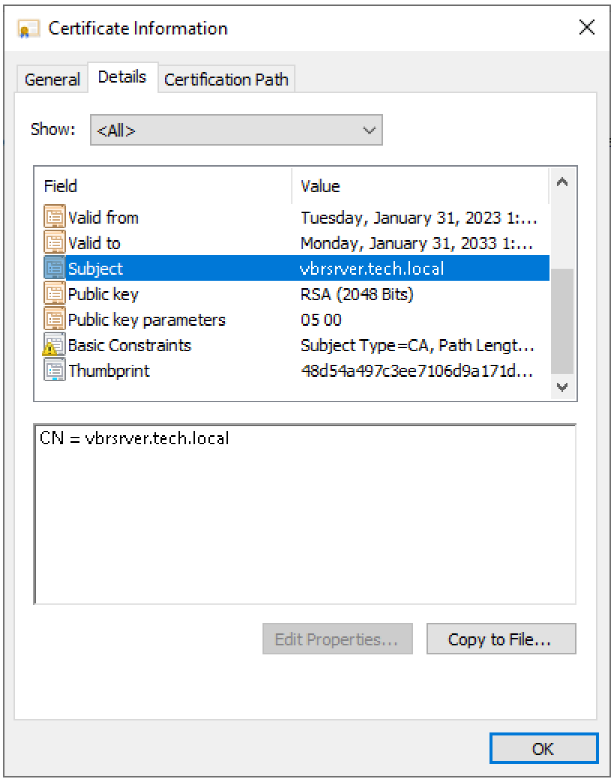
To establish a secure connection between the backup server and protected computers, Veeam Backup & Replication uses a TLS certificate. By default, Veeam Backup & Replication uses a self-signed certificate. Veeam Backup & Replication generates this certificate when you install the product on the Veeam backup server.

If you want to use a certificate signed by your internal Certification Authority (CA), make sure that the following requirements are met:

- Veeam Plug-ins and Veeam Backup & Replication must trust the CA. That is, the Certification Authority certificate must be added to the Trusted Root Certification Authority store on the Veeam backup server and computers with Veeam Plug-ins.
- Certificate Revocation List (CRL) must be accessible from the Veeam backup server and computers with Veeam Plug-ins.
- [For Linux-based computers] OpenSSL version 1.0 or later must be installed on the computer with Veeam Plug-in.

A certificate signed by a CA must meet the following requirements:

1. The certificate subject must be equal to the fully qualified domain name of the Veeam backup server. For example: *vbrserver.tech.local*.



Show: <All>

Field	Value
Valid from	Tuesday, January 31, 2023 1:...
Valid to	Monday, January 31, 2033 1:...
Subject	vbrsrver.tech.local
Public key	RSA (2048 Bits)
Public key parameters	05 00
Basic Constraints	Subject Type=CA, Path Lengt...
Thumbprint	48d54a497c3ee7106d9a171d...

CN = vbrsrver.tech.local

2. The following key usage extensions must be enabled in the certificate to sign and deploy child certificates for computers with Veeam Plug-ins:

   - Digital Signature
   - Certificate Signing
   - Off-line CRL Signing
   - CRL Signing (86)

   If you use Windows Server Certification Authority, it is recommended that you issue a Veeam Backup & Replication certificate based on the built-in "Subordinate Certification Authority" template or templates similar to it.

3. It is highly recommended to add "pathLen=0" to Basic Constraints.

   If you use Windows Server Certification Authority, to do this, enable the **Do not allow subject to issue certificates to other CAs** option in the certificate template.

4. The key type in the certificate must be set to *Exchange*.

   If you create a certificate request using the Windows MMC console, to specify the key type, do the following:

   a. At the **Request Certificates** step of the **Certificate Enrollment** wizard, select a check box next to the necessary certificate template and click **Properties**.

   b. In the **Certificate Properties** window, click the **Private Key** tab.

   c. In the **Key Type** section, select **Exchange**.

To start using the signed certificate, you must select it from the certificates store on the Veeam backup server. To learn more, see Importing Certificates from Certificate Store.

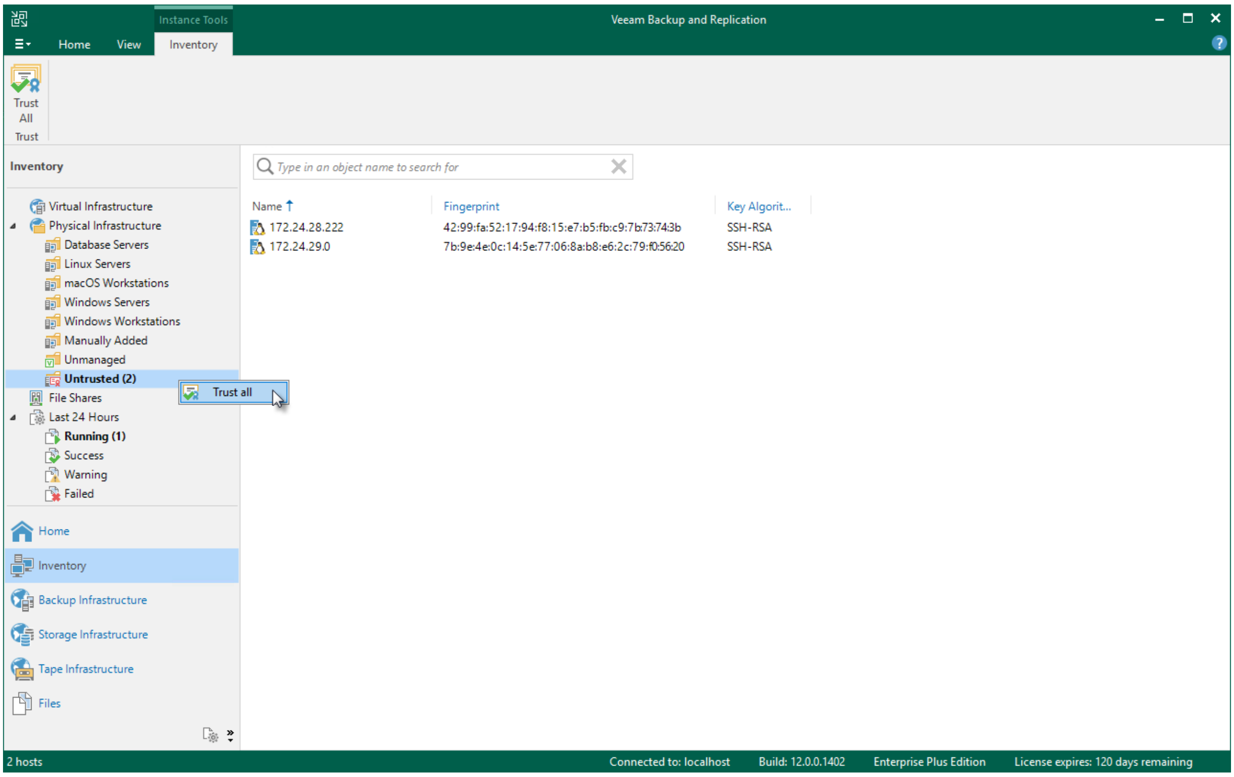
After you specify the signed certificate in Veeam Backup & Replication, during the next application backup policy session Veeam Plug-ins will receive child certificates from the Veeam backup server.

Adding Computers to Trusted Hosts List

After you enable the **Add unknown hosts to the list manually (more secure)** option in Veeam Backup & Replication settings, Linux-based computers whose SSH fingerprints are not stored in the Veeam Backup & Replication database become unable to communicate to the Veeam backup server. During discovery, Veeam Backup & Replication puts such computers to the *Untrusted* protection group. To start managing an untrusted computer, you must manually validate the SSH fingerprint and add the computer to the list of trusted hosts in the Veeam Backup & Replication console.

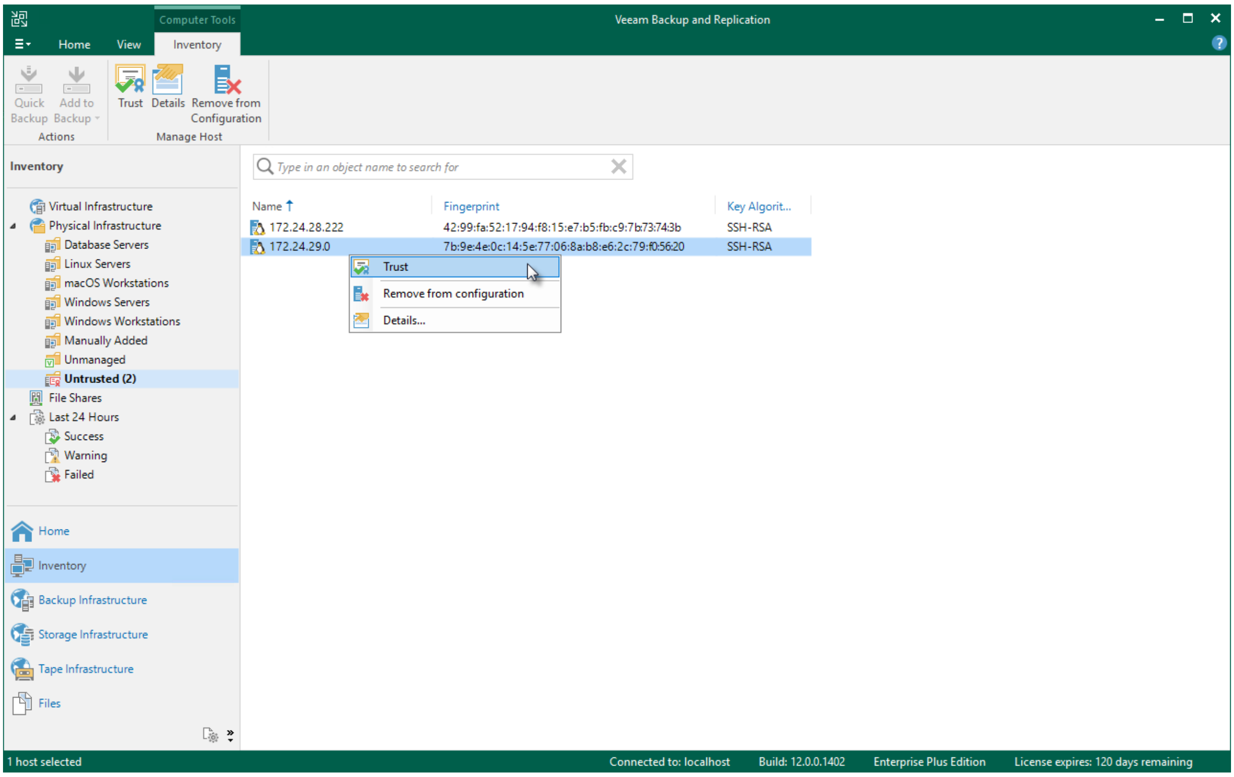
To add a computer to the list of trusted hosts:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and click **Untrusted**.
3. In the working area, Veeam Backup & Replication will display discovered computers that you can add to the list of trusted hosts. Check SSH fingerprints of the computers and add them to the list of trusted hosts in one of the following ways:
   - To add all computers at once to the list of trusted hosts, select the **Untrusted** node in the inventory pane and click **Trust All** on the ribbon or right-click the **Untrusted** node and select **Trust all**.



Name	Fingerprint	Key Algorit...
172.24.28.222	42:99:fa:52:17:94:f8:15:e7:b5:fb:c9:7b:73:74:3b	SSH-RSA
172.24.29.0	7b:9e:4e:0c:14:5e:77:06:8a:b8:e6:2c:79:f0:56:20	SSH-RSA

- To add a specific computer to the list of trusted hosts, select the necessary computer in the working area and click **Trust** on the ribbon or right-click the computer and select **Trust**.



Name	Fingerprint	Key Algorit...
172.24.28.222	42:99:fa:52:17:94:f8:15:e7:b5:fb:c9:7b:73:74:3b	SSH-RSA
172.24.29.0	7b:9e:4e:0c:14:5e:77:06:8a:b8:e6:2c:79:f0:56:20	SSH-RSA

Working with Protection Groups

In Veeam Backup & Replication, computers with Veeam Plug-ins are organized into protection groups. You can perform the following operations with protection groups:

- Create a protection group.
- Edit protection group settings.
- Rescan a protection group.
- Assign location to a protection group.
- Disable a protection group.
- Remove a protection group.

Creating Protection Groups

You must add computers that you plan to protect with Veeam Plug-ins to the inventory in the Veeam Backup & Replication console. In Veeam Backup & Replication, protected computers are organized into protection groups. You can create one or more protection groups that contain computers of different types or offer different discovery and deployment options.

Before You Begin

Before creating a protection group, consider the following prerequisites and limitations:

1. When Veeam Backup & Replication performs discovery of protected computers, Veeam Backup & Replication connects to every computer added to the protection group. If you instruct Veeam Backup & Replication to perform discovery immediately after the protection group is created, make sure that all computers added to the protection group are powered on and may be accessed over the network. Otherwise, Veeam Backup & Replication will be unable to connect to a protected computer and perform the required operations on this computer.
2. A protection group that includes Microsoft Active Directory objects can include objects from one domain only. To add to the inventory computers that reside in another domain, you need to create a separate protection group and include in this protection group the necessary objects from that domain.
3. Veeam Backup & Replication automatically excludes from the protection scope Active Directory objects of the Group type that exist in a parent Active Directory object (organization unit, container or entire domain) specified in the protection group settings. To instruct Veeam Backup & Replication to process a group, you must select this group explicitly in the protection group settings.
4. You cannot add and/or exclude universal and domain local groups to/from protection groups that include Microsoft Active Directory objects. Only global groups are supported.
5. Do not add a computer to a protection group by specifying a dynamic IP address assigned to this computer. If such computer receives another IP address from a DHCP server, Veeam Backup & Replication will be unable to discover the computer and perform on this computer operations defined in the protection group settings.
6. We recommend that you include each object you want to protect in one protection group only. For example, if you have added an Active Directory container to a protection group, it is not recommended to add a computer that exists in this container to another protection group. Adding computers to multiple protection groups with different computer discovery and Veeam Plug-in deployment settings will result in additional load on the backup server.
7. You can add a cluster only to a protection group that includes Microsoft Active Directory objects. You cannot add clusters to protection groups that include individual computers or computers specified in a CSV file.
8. When you configure a protection group for a cluster, do not exclude nodes of this cluster from a protection scope. Otherwise, Veeam Backup & Replication will not have complete information about all clustered servers.

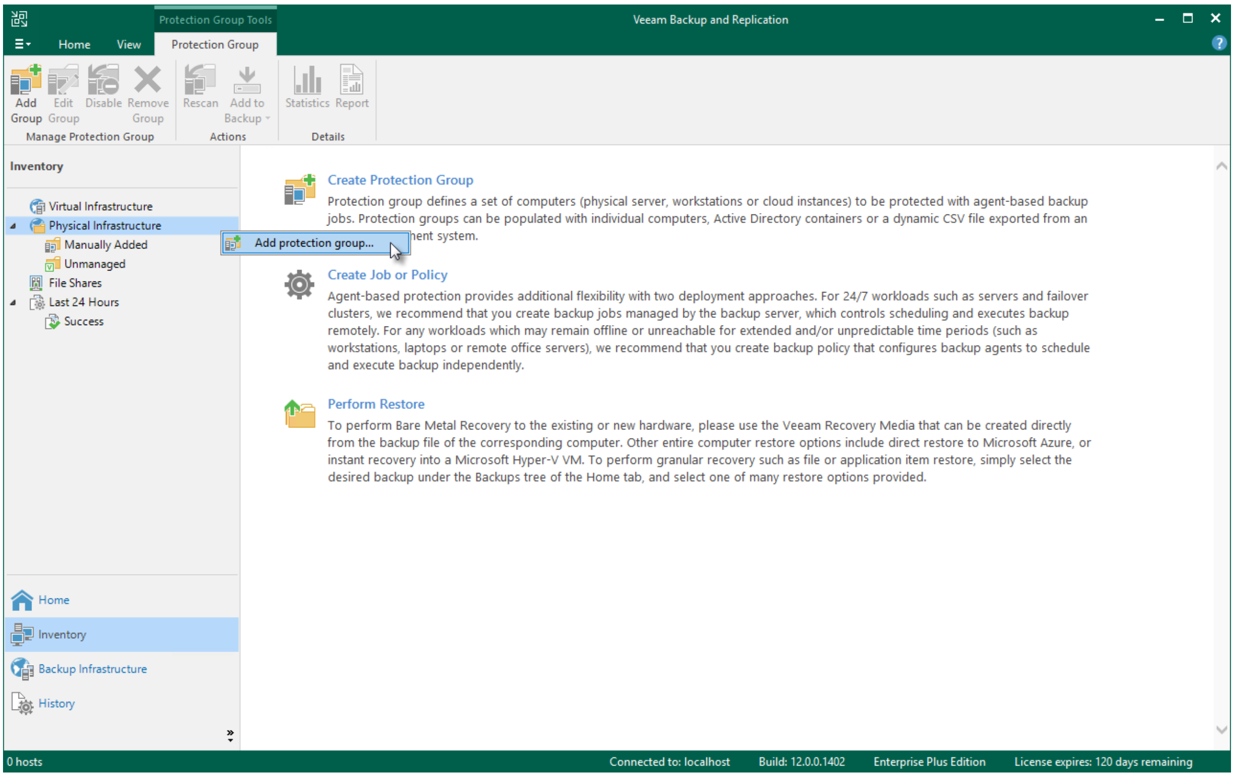
9. To deploy Veeam Installer Service and Veeam Plug-in on a protected computer running Microsoft Windows OS, Veeam Backup & Replication uses the administrative share (admin$) of the target computer. An account that you plan to use to connect to a computer included in the protection group must have access to the administrative share.

   Note that in client Microsoft Windows OSes access to the administrative share is forbidden by default for local accounts. You can enable this option with a registry key. For details, see this Microsoft KB article.

10. Veeam Backup & Replication does not support usage of a Linux account for which system settings modify shell output results to connect to a computer included in the protection group. For example, this includes Linux accounts with the modified *PS1* shell variable.

Step 1. Launch New Protection Group Wizard

To launch the **New Protection Group** wizard, open the **Inventory** view. Right-click the **Physical Infrastructure** node in the inventory pane and select **Add protection group**.



Create Protection Group

Protection group defines a set of computers (physical server, workstations or cloud instances) to be protected with agent-based backup jobs. Protection groups can be populated with individual computers, Active Directory containers or a dynamic CSV file exported from an ent system.

Create Job or Policy

Agent-based protection provides additional flexibility with two deployment approaches. For 24/7 workloads such as servers and failover clusters, we recommend that you create backup jobs managed by the backup server, which controls scheduling and executes backup remotely. For any workloads which may remain offline or unreachable for extended and/or unpredictable time periods (such as workstations, laptops or remote office servers), we recommend that you create backup policy that configures backup agents to schedule and execute backup independently.

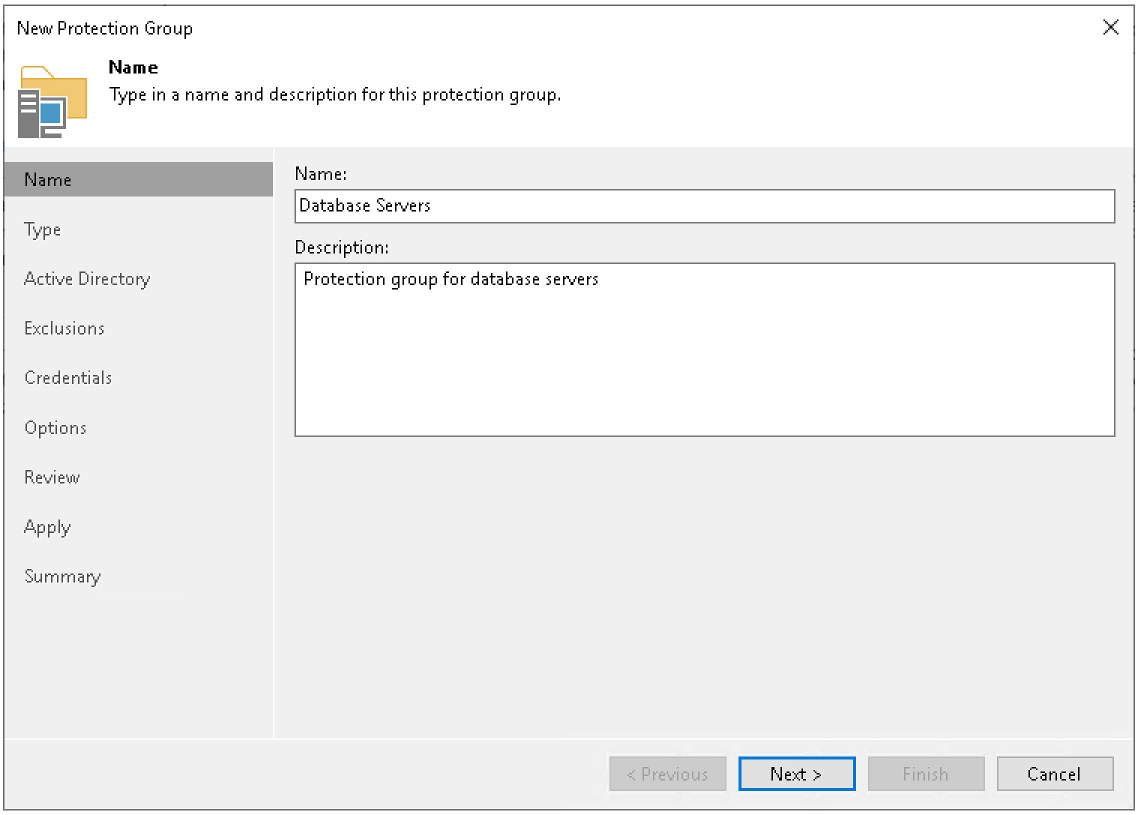
Perform Restore

To perform Bare Metal Recovery to the existing or new hardware, please use the Veeam Recovery Media that can be created directly from the backup file of the corresponding computer. Other entire computer restore options include direct restore to Microsoft Azure, or instant recovery into a Microsoft Hyper-V VM. To perform granular recovery such as file or application item restore, simply select the desired backup under the Backups tree of the Home tab, and select one of many restore options provided.

Step 2. Specify Job Name and Description

At the **Name** step of the wizard, specify a name and description for the protection group.

1. In the **Name** field, specify a name for the protection group.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the protection group, date and time when the protection group was created.



New Protection Group

Name

Type in a name and description for this protection group.

Name:
Database Servers

Description:
Protection group for database servers

Step 3. Select Protection Group Type

At the **Type** step of the wizard, select the type of the protection group.

> IMPORTANT
>
> Veeam Backup & Replication cannot install Veeam Plug-ins on computers added to the protection groups of the following types:
>
> - Computers with pre-installed agents
> - Cloud machines

You can select one of the following types:

- **Individual computers** — select this option if you want to define a static protection scope by adding specific computers to the protection group. This option is recommended for smaller environments that do not have Microsoft Active Directory deployed.

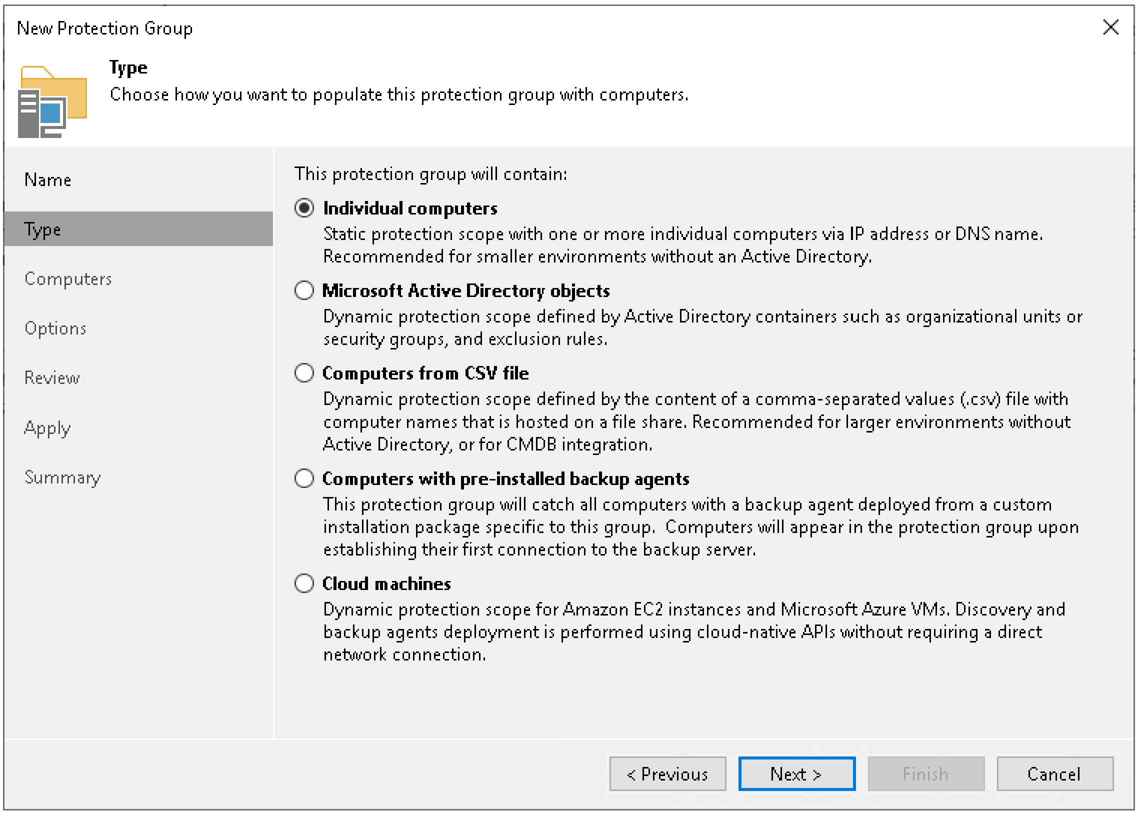
  With this option selected, you will pass to the Computers step of the wizard.

- **Microsoft Active Directory objects** — select this option if you want to add to the protection group one or several Active Directory objects: entire domain, container, organization unit, group, computer or cluster. Protection groups that include Active Directory containers and/or organization units are dynamic in their nature. If a new computer is added to a container or organization unit that you have specified in the protection group settings, during the next rescan session, Veeam Backup & Replication will discover this computer and (optionally) deploy Veeam Plug-in on this computer.

  With this option selected, you will pass to the Active Directory step of the wizard.

- **Computers from CSV file** — select this option if you want to add to the protection scope computers listed in a CSV file that resides in a local folder on the backup server or in a network shared folder. As well as protection groups that include Active Directory containers, protection groups of this type are also dynamic. If a new computer appears in a CSV file after the protection job is created, within the next rescan session, Veeam Backup & Replication will automatically update the protection group settings to include the added computer.

  With this option selected, you will pass to the CSV File step of the wizard.



New Protection Group

Type

Choose how you want to populate this protection group with computers.

This protection group will contain:

● **Individual computers**
Static protection scope with one or more individual computers via IP address or DNS name. Recommended for smaller environments without an Active Directory.

○ **Microsoft Active Directory objects**
Dynamic protection scope defined by Active Directory containers such as organizational units or security groups, and exclusion rules.

○ **Computers from CSV file**
Dynamic protection scope defined by the content of a comma-separated values (.csv) file with computer names that is hosted on a file share. Recommended for larger environments without Active Directory, or for CMDB integration.

○ **Computers with pre-installed backup agents**
This protection group will catch all computers with a backup agent deployed from a custom installation package specific to this group. Computers will appear in the protection group upon establishing their first connection to the backup server.

○ **Cloud machines**
Dynamic protection scope for Amazon EC2 instances and Microsoft Azure VMs. Discovery and backup agents deployment is performed using cloud-native APIs without requiring a direct network connection.

Step 4. Specify Protection Scope

Specify protection scope for the created protection group:

- Specify computers — if you have selected the **Individual computers** option at the Type step of the wizard.
- Specify Microsoft Active Directory objects — if you have selected the **Microsoft Active Directory objects** option at the Type step of the wizard.
- Specify a CSV file — if you have selected the **Computers from CSV file** option at the Type step of the wizard.

Specifying Computers

The **Computers** step of the wizard is available if you have chosen the **Individual computers** option at the Type step of the wizard.

At this step of the wizard, specify computers that you want to add to the protection group.

To add a computer to a protection group:

1. Click **Add**.
2. In the **Add Computer** window, in the **Host name or IP address** field, enter a full DNS name, NetBIOS name or IP address of the computer that you want to add to the protection group.
3. From the **Credentials** list, select a user account that has administrative permissions on the computer that you want to add to the protection group. Veeam Backup & Replication will use this account to connect to the protected computer and perform the necessary operations on the computer: upload and install Veeam Plug-in, and so on.

   If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials. You can select one of the following credentials type:

   - Stored credentials. Select stored credentials if you want Veeam Backup & Replication to use the specified user name and password for each connection to Veeam Agent.
   - [For Linux computers] Single-use credentials. Select single-use credentials if you do not want Veeam Backup & Replication to store credentials in the configuration database. With this option selected, Veeam Backup & Replication will use the specified user name and password only for the first connection to Veeam Plug-in. After that, Veeam Backup & Replication will use Veeam Installer Service and Veeam Deployer Service to communicate with the Veeam Plug-in.

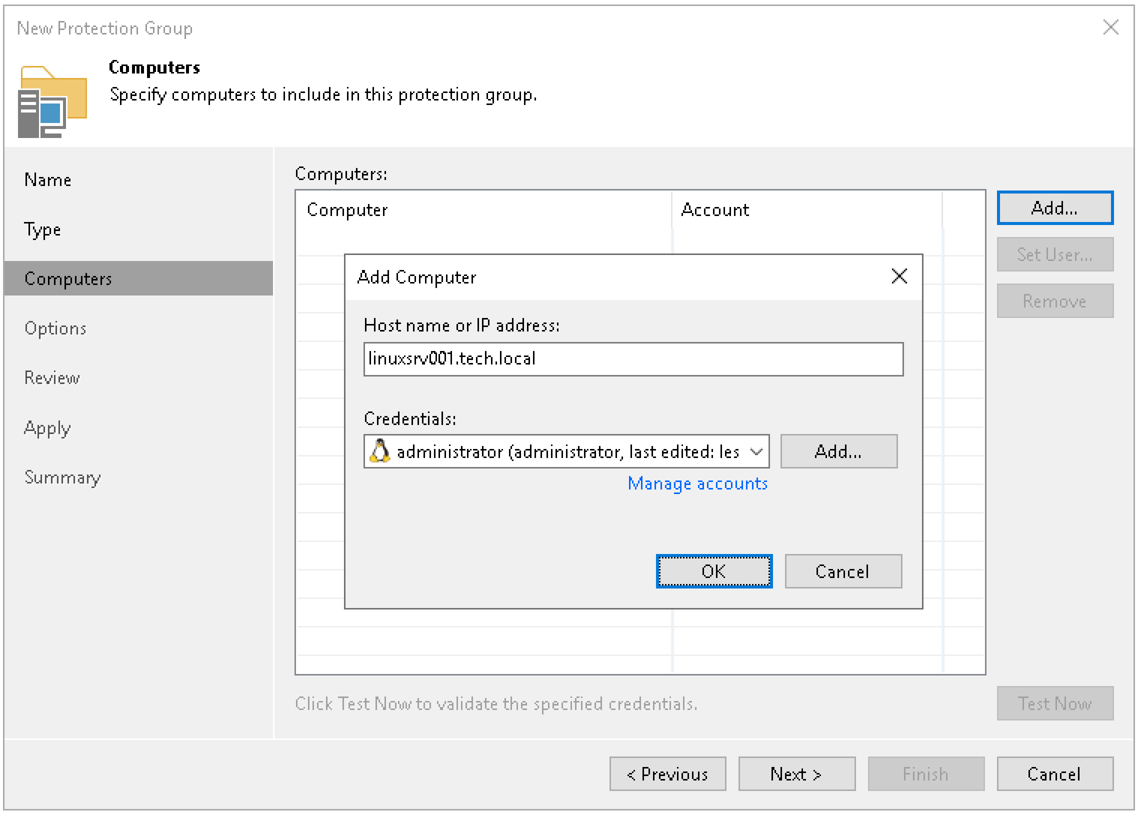
   Keep in mind that the username must be specified in the down-level logon name format. For example, DOMAIN\UserName or HOSTNAME\UserName. Use the full domain or hostname name. Do not replace them with a dot.

   For more information, see the Credentials Manager section in the Veeam Backup & Replication User Guide.

1. Repeat steps 1–3 for every computer that you want to add to the protection group.
2. To check if Veeam Backup & Replication can communicate with computers added to the protection group, click **Test Now**. Veeam Backup & Replication will use the specified credentials to connect to all computers in the list.

NOTE

If you chose to manually add Linux-based computers to the list of trusted hosts in Veeam Backup & Replication, when you test credentials for an unknown Linux-based computer in the protection group settings, the test operation will complete with the *Failed* status. This happens because Veeam Backup & Replication cannot connect to the untrusted computer before you add this computer to the list of trusted hosts. To learn more, see Adding Computers to Trusted Hosts List.



New Protection Group

Computers

Specify computers to include in this protection group.

Computers:

Add Computer

Host name or IP address: linuxsrv001.tech.local

Credentials: administrator (administrator, last edited: les

Click Test Now to validate the specified credentials.

Specifying Active Directory Objects

The **Active Directory** step of the wizard is available if you have chosen the **Microsoft Active Directory objects** option at the Type step of the wizard.

At this step of the wizard, select Active Directory objects that you want to add to the protection group. You can add to a protection group the following types of Active Directory objects: domain, organization unit, container, computer, cluster, or group.

To add Active Directory objects to a protection group:

1. In the **Search for objects in this domain** field, click **Change**.
2. In the **Specify Domain** window, specify settings of the domain whose objects you want to include in the protection group:
   a. In the **Domain controller or domain DNS name** field, type a name of the domain controller or domain whose objects you want to include in the protection group.
   b. In the **Port** field, specify a port number over which Veeam Backup & Replication must communicate with the domain controller. By default, Veeam Backup & Replication uses port 389.

c. From the **Account** list, select a user account that is a member of the *DOMAIN\Administrators* group. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials. For more information, see the Credentials Manager section in the Veeam Backup & Replication User Guide.

d. Click **OK** to close the **Specify Domain** window.

> NOTE
>
> If you want to include a large number of computers in the protection group but do not want to use an account with domain administrator permissions in the protection group settings, consider configuring a protection group based on a list of computers imported from a CSV file. To learn more, see Select Protection Group Type.

3. In the **Selected objects** field, click **Add**.

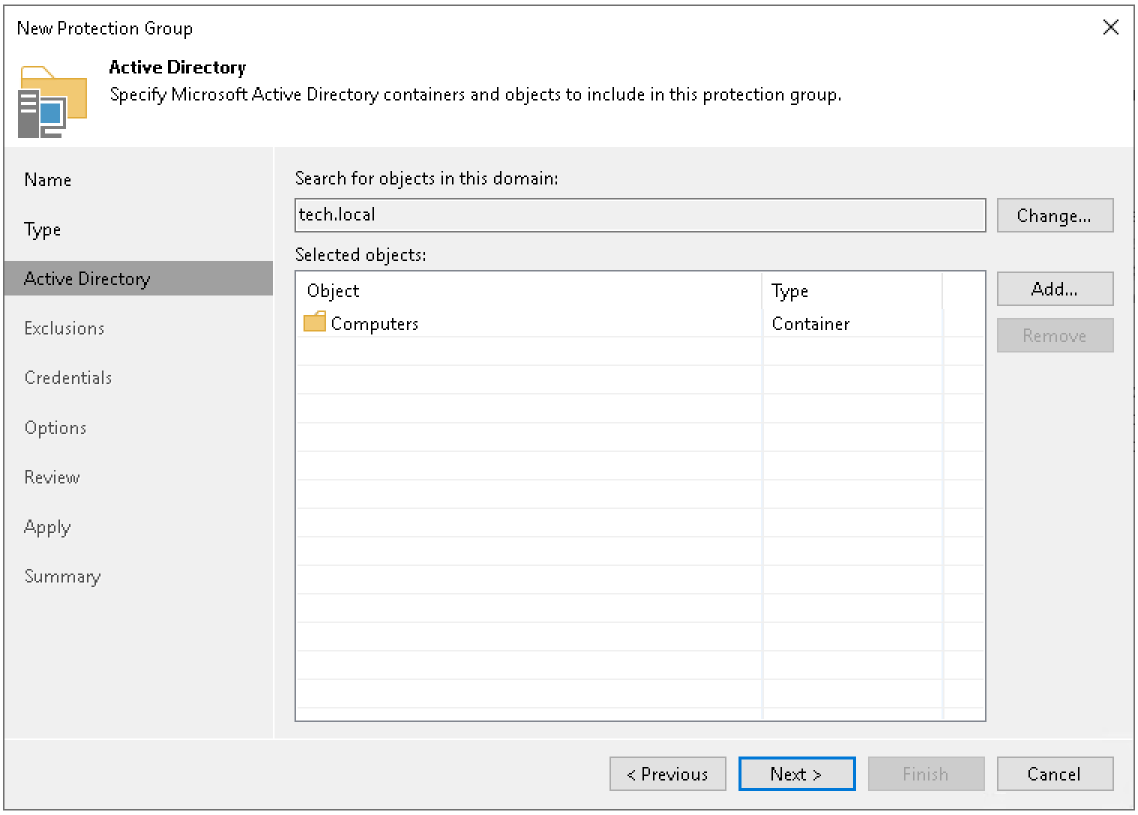
4. In the **Add Objects** window, select the necessary Active Directory object in the tree and click **OK**. You can press and hold **[CTRL]** to select multiple objects at once.

   To quickly find the necessary object, you can use the search field at the bottom of the **Add Objects** window.

   a. Click the button to the left of the search field and select the necessary type of object to search for: *Everything*, *Computer*, *Cluster*, *Organization Unit*, *Container* or *Group*.

   b. Enter the object name or a part of it in the search field.

   c. Click the **Start search** button on the right or press **[ENTER]**.



Active Directory

Specify Microsoft Active Directory containers and objects to include in this protection group.

Search for objects in this domain: tech.local

Selected objects:

Object	Type
Computers	Container

Specifying CSV File

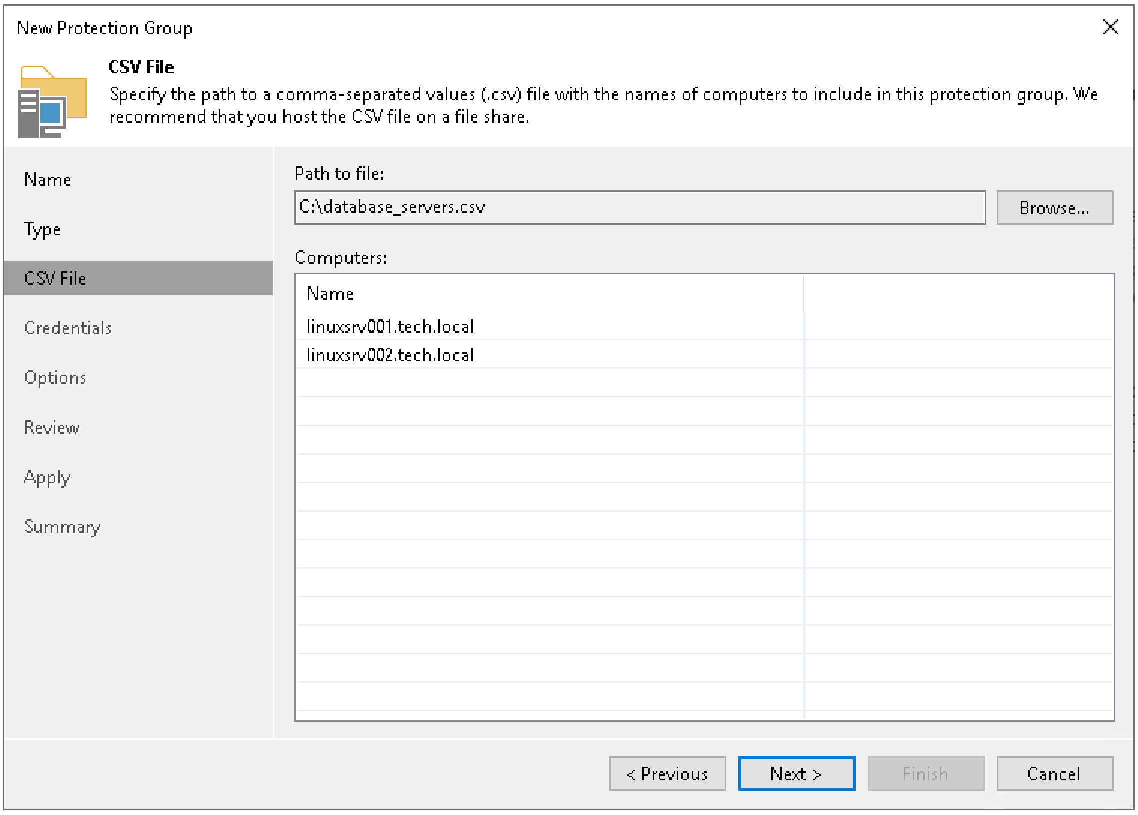
The **CSV File** step of the wizard is available if you have chosen the **Computers from CSV file** option at the Type step of the wizard.

At this step of the wizard, specify a file that defines a list of computers that you want to add to the protection group. You must specify a list of computers in a file of the CSV or TXT format. The file must be created beforehand. To learn more, see Preparing CSV File.

To specify a CSV file:

1. In the **Path to file** field, click **Browse** and specify a path to a CSV file that contains a list of IP addresses or domain names of computers that you want to add to the protection group. The CSV file can reside in a folder on the local drive of the Veeam backup server or in a network shared folder accessible from the backup server.
2. In the **Computers** field, review the list of IP addresses or domain names imported from the CSV file.

> **NOTE**
>
> After you finish configuring the protection group, Veeam Backup & Replication will perform discovery of computers listed in the CSV file upon schedule defined in the protection group settings. If Veeam Backup & Replication is unable to read the CSV file (for example, after the file was moved or deleted from the specified location), the rescan job will use the list of computers imported from the CSV file during the previous rescan job session.



New Protection Group

CSV File

Specify the path to a comma-separated values (.csv) file with the names of computers to include in this protection group. We recommend that you host the CSV file on a file share.

Path to file: C:\database_servers.csv

Computers:

Name
linuxsrv001.tech.local
linuxsrv002.tech.local

Preparing CSV File

To define a dynamic protection scope based on a list of computers, you must create a CSV file with a list of IP addresses or domain names to scan during discovery. Veeam Backup & Replication supports IP addresses of IPv4 and IPv6 formats.

Delimit IP addresses or domain names in the list with commas (',') or semicolons (';'). For example:

```
172.17.53.16,172.17.53.19,172.17.53.31,172.17.53.40
```

Alternatively, you can delimit IP addresses or domain names in the list with the newline character:

```
172.17.53.16
172.17.53.19
172.17.53.31
172.17.53.40
```

Step 5. Exclude Objects from Protection Group

The **Exclusions** step of the wizard is available if you have chosen to define a protection scope that includes Microsoft Active Directory objects.

At this step of the wizard, you can specify which objects you want to exclude from the protection group. You can exclude the following types of objects:

- All virtual machines — all VMs residing in the domain. You can select this option, for example, if you do not want to protect VMs with Veeam Plug-ins and want to back up VM data with Veeam Backup & Replication instead.
- All computers that have been offline for over 30 days — all computers in the domain that have not logged on to Active Directory for more than 30 days.
- Individual objects: computers, clusters, groups, organization units and/or containers.

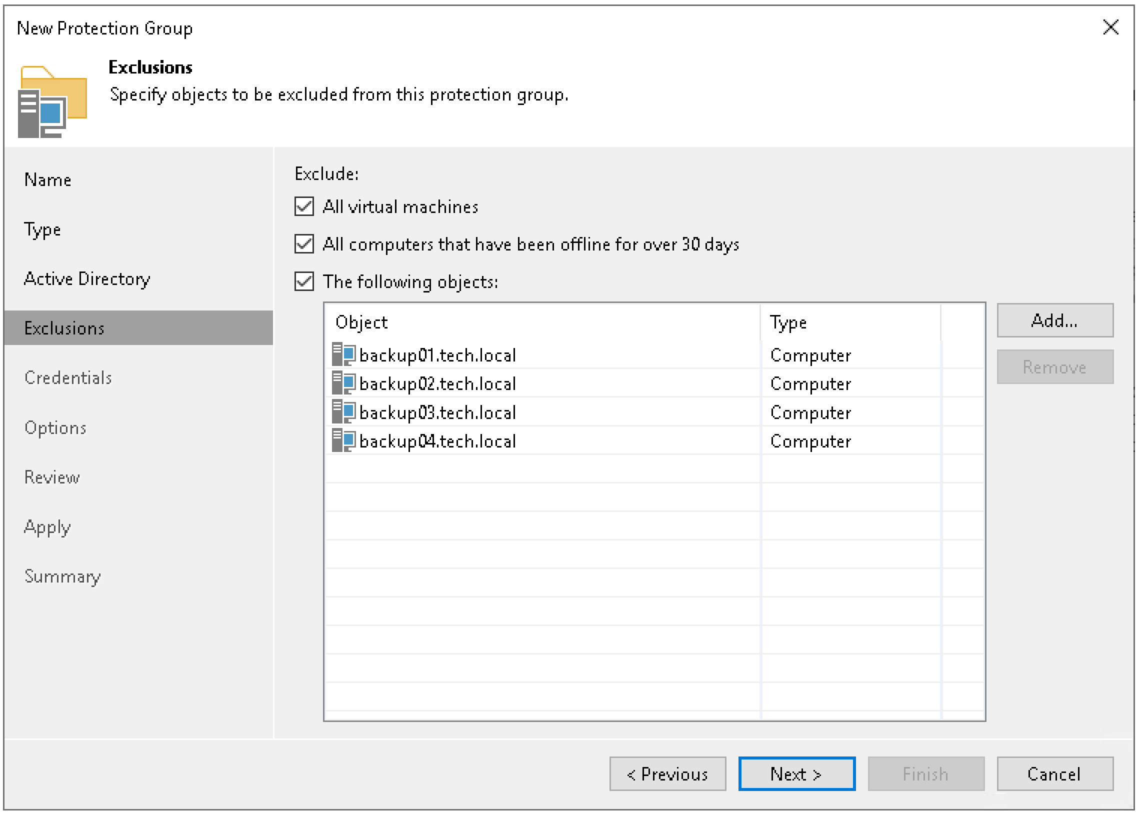
Excluding Individual Active Directory Objects

To exclude Active Directory objects:

1. In the **Exclude** section, select the **The following objects** check box.
2. Click **Add**.
3. In the **Add Objects** window, select the necessary Active Directory object in the tree and click **OK.** You can press and hold **[CTRL]** to select multiple objects at once.

To quickly find the necessary Active Directory object, you can use the search field at the bottom of the **Add Objects** window.

1. Click the button to the left of the search field and select the necessary type of object to search for: *Everything*, *Computer, Cluster, Group, Organization Unit* or *Container*.
2. Enter the object name or a part of it in the search field.
3. Click the **Start search** button on the right or press **[ENTER]**.



New Protection Group

Exclusions

Specify objects to be excluded from this protection group.

Exclude:

☑ All virtual machines

☑ All computers that have been offline for over 30 days

☑ The following objects:

Object	Type
backup01.tech.local	Computer
backup02.tech.local	Computer
backup03.tech.local	Computer
backup04.tech.local	Computer

Step 6. Specify Credentials

The **Credentials** step of the wizard is available if you have chosen to define a protection scope that includes Microsoft Active Directory objects or computers specified in a CSV file.

At this step of the wizard, specify credentials to connect to computers included in the protection group:

1. If you want to use the same credentials for all computers in the protection group, select the necessary user account from the **Master account** list. The account must have local administrator permissions on all computers that you have added to the protection group.

   If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials. For more information, see the Credentials Manager section in the Veeam Backup & Replication User Guide.

2. By default, Veeam Backup & Replication uses credentials specified in the **Master account** field for all computers in the protection group. If some computer requires a different user account, do the following:

   a. Select the **Use custom credentials for the following objects** check box,

   b. Click **Add** next to the list of objects and select the necessary object in the **Add Objects** window:

      - If you configure a protection group that includes Active Directory objects, objects that you have added to the protection group at the **Active Directory** step or the wizard are already displayed in the **Use custom credentials for the following objects** list. In the **Add Objects** window, you can also select child objects for which you want to specify custom credentials. For example, you may want to specify separate credentials for different organization units, containers, groups or individual computers within the entire domain added to the protection group.

      - If you configure a protection group that includes computers specified in a CSV file, you can select in the **Add Objects** window one or more computers listed in a CSV file and add them to the **Use custom credentials for the following objects** list.

   c. In the **Use custom credentials for the following objects** list, select the necessary object, click **Edit** and select custom credentials for the object. Credentials must be specified in the following format:

      - For Active Directory accounts — *DOMAIN\Username*

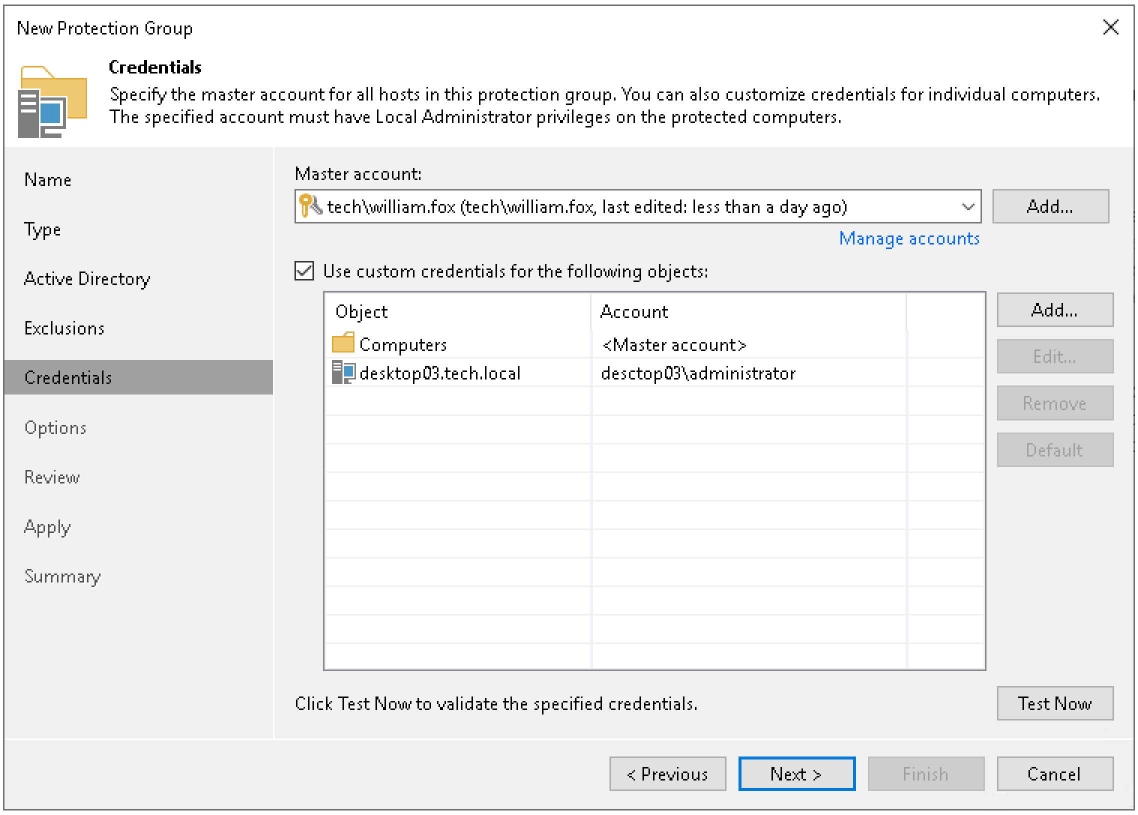
      - For local accounts — *Username* or *HOST\Username*

NOTE

Consider the following:

- Veeam Backup & Replication supports user account names in the SAM-Account-Name format (*DOMAIN\Username*). The User-Principal-Name (UPN) format (*username@domain*) is not supported. If you specify credentials in the UPN format, Veeam Backup & Replication will successfully connect to computers added to the protection group during the *Test Now* operation. However, the subsequent protection group rescan operations will fail.
- The account that you use to connect to a Linux computer must have a home directory on this computer.
- If you configure a protection group that includes dynamic Active Directory objects, such as domain, organization unit, container or group, the master account or custom account specified for an object must be a member of the DOMAIN\Administrators group.
- If you plan to back up Oracle databases that run on Linux computers, the OS account used to connect to the computer must be a member of the group that owns configuration files of the Oracle database (for example, the oinstall group).

To check if Veeam Backup & Replication can connect to computers added to the protection group, click **Test Now**. Veeam Backup & Replication will form a list of computers to connect and use the specified credentials to connect to computers in the list.



New Protection Group

Credentials

Specify the master account for all hosts in this protection group. You can also customize credentials for individual computers. The specified account must have Local Administrator privileges on the protected computers.

Master account: tech\william.fox (tech\william.fox, last edited: less than a day ago)

☑ Use custom credentials for the following objects:

Object	Account
Computers	<Master account>
desktop03.tech.local	desctop03\administrator

Click Test Now to validate the specified credentials.

Step 7. Specify Discovery and Deployment Options

At the **Options** step of the wizard, specify settings for protected computers discovery and Veeam Agent deployment.

Veeam Backup & Replication regularly connects to protected computers according to the schedule defined in the protection group settings. At this step of the wizard, you can define the discovery schedule and specify operations that Veeam Backup & Replication must perform on discovered computers. You can also select which server in your backup infrastructure should act as a distribution server for Veeam Plug-ins.

To specify discovery and deployment options:

1. In the **Discovery** section, define schedule for automatic computer discovery within the scope of the protection group:

    - To run the rescan job at specific time daily, on defined week days or with specific periodicity, select **Daily at this time**. Use the fields on the right to configure the necessary schedule.

    - To run the rescan job repeatedly throughout a day with a specific time interval, select **Periodically every**. In the field on the right, select the necessary time unit: *Hours* or *Minutes*. Click **Schedule** and use the time table to define the permitted time window for the rescan job. In the **Start time within an hour** field, specify the exact time when the job must start.

    - To run the rescan job continuously, select the **Periodically every** option and choose **Continuously** from the list on the right. A new rescan job session will start as soon as the previous rescan job session finishes.

    > NOTE
    >
    > You cannot create a protection group without defining schedule for automatic discovery. However, you can disable automatic discovery for a specific protection group, if needed. To learn more, see Disabling Protection Group.

2. In the **Deployment** section, select the object that will be responsible for the Veeam Plug-ins distribution, select a Microsoft Windows server that you plan to use as a distribution server. Veeam Backup & Replication will use the distribution server to upload Veeam Plug-in setup files to computers added to the protection group. By default, Veeam Backup & Replication assigns the distribution server role to the backup server. To learn more, see Distribution Server.

4. Make sure that the **Install backup agent** check box is clear. Otherwise, Veeam Backup & Replication will install Veeam Agent on the target computer.

    > TIP
    >
    > To learn how to use protection groups to automatically deploy Veeam Agents, see Veeam Agent Management Guide.

3. If you want to instruct Veeam Backup & Replication to automatically deploy Veeam Plug-ins on all discovered computers in the protection group, in the **Deployment** section, make sure that the **Install application plug-ins: configure plug-ins to be installed** check box is selected and click **Configure**. In the **Application Plug-ins** window, select the check boxes next to the plug-ins that you want to install.

NOTE

[For Veeam Plug-in for SAP on Oracle] if you plan to use the `rman_util` parameter, you must install 2 plug-ins on the Oracle server:

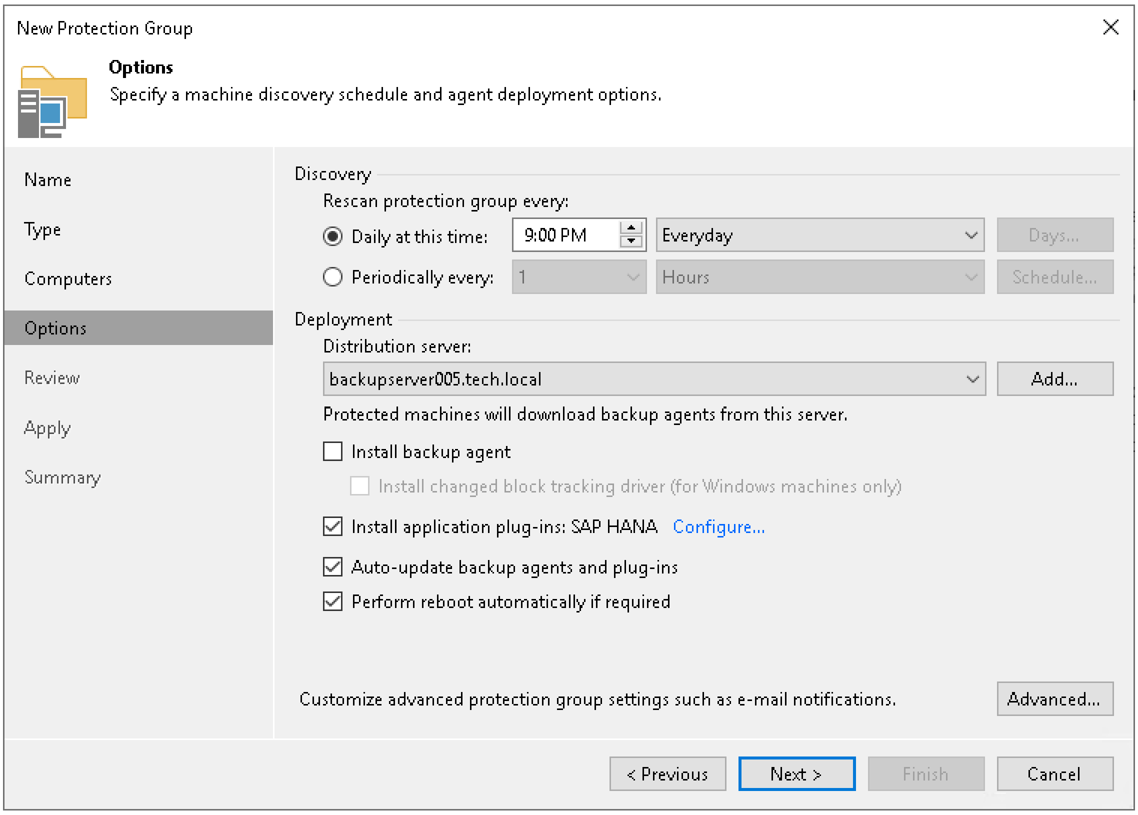
- Veeam Plug-in for Oracle RMAN
- Veeam Plug-in for SAP on Oracle

You can also choose to disable automated Veeam Plug-in installation. To do this, in the **Application Plug-ins** window, clear the check boxes next to the plug-ins that you do not want Veeam Backup & Replication to install. In this case, you will need to install Veeam Plug-in on every computer included in the protection group and discovered by Veeam Backup & Replication. To learn more, see Installing Veeam Plug-in.

4. If you want to instruct Veeam Backup & Replication to automatically upgrade Veeam Plug-ins on discovered computers when a new version of the product appears on the distribution server, in the **Deployment** section, make sure that the **Auto-update backup agents and plug-ins** check box is selected.

5. Select the **Perform reboot automatically if required** check box to allow Veeam Backup & Replication to reboot a protected computer.

6. Click **Advanced** to specify advanced settings for the protection group. To learn more, see Specify Advanced Protection Group Settings.


New Protection Group

Options
Specify a machine discovery schedule and agent deployment options.

Discovery
Rescan protection group every:
● Daily at this time: 9:00 PM | Everyday | Days...
○ Periodically every: 1 | Hours | Schedule...

Deployment
Distribution server:
backupserver005.tech.local | Add...
Protected machines will download backup agents from this server.
☐ Install backup agent
☐ Install changed block tracking driver (for Windows machines only)
☑ Install application plug-ins: SAP HANA Configure...
☑ Auto-update backup agents and plug-ins
☑ Perform reboot automatically if required

Customize advanced protection group settings such as e-mail notifications. Advanced...

Step 8. Specify Advanced Protection Group Settings

You can specify email notification settings for the protection group. If you enable notification settings, Veeam Backup & Replication will send a daily email report with protection group statistics to a specified email address. The report contains cumulative statistics for rescan job sessions performed for the protection group within the last 24-hour period.

> NOTE
>
> Email reports with protection group statistics will be sent only if you configure global email notification settings in Veeam Backup & Replication. For more information, see the Configuring Global Email Notification Settings section in the Veeam Backup & Replication User Guide.
>
> After you enable notification settings for the protection group, in addition to reports sent according to the global email notification settings, Veeam Backup & Replication will send reports with the protection group statistics to email addresses specified in the protection group settings. This allows you to fine-tune email notifications in Veeam Backup & Replication: while one or more backup administrators receive email notifications according to the global settings, other backup administrators can receive reports for specific protection groups only.
>
> If you do not enable global email notification settings in Veeam Backup & Replication, notification settings for the protection group will not be sent even if you enable them in the protection group settings.

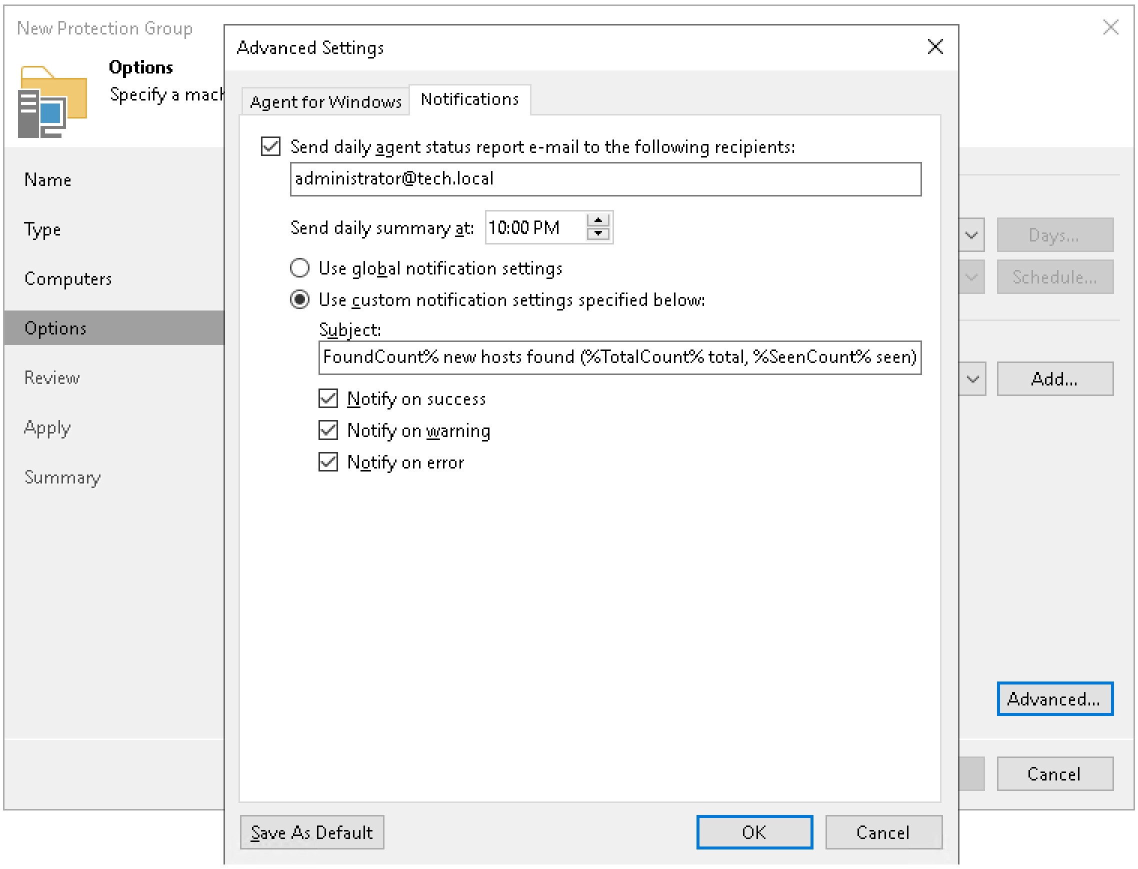
To specify notification settings for the protection group:

1. At the **Options** step of the wizard, click **Advanced**.
2. Click the **Notifications** tab.
3. Select the **Send daily agent status report e-mail to the following recipients** check box and specify a recipient's email address. You can enter several addresses separated by a semicolon.
4. In the **Send daily summary at** field, specify the time when Veeam Backup & Replication must send the daily email report for the protection group.
5. You can choose to use global notification settings or specify custom notification settings.

   To receive a typical notification for the protection group, select **Use global notification settings**. In this case, Veeam Backup & Replication will apply to the protection group global email notification settings specified for the backup server.

To configure a custom notification for the protection group, select **Use custom notification settings specified below**. You can specify the following notification settings:

- In the **Subject** field, specify a notification subject. You can use the following variables in the subject:
  - *%JobResult%* — rescan job result.
  - *%PGName%* — protection group name.
  - *%FoundCount%* — number of new computers discovered within the last 24-hour period.
  - *%TotalCount%* — total number of computers in the protection group.
  - *%SeenCount%* — number of computers in the protection group that were online for the last 24 hours. A computer is considered to be online if Veeam Backup & Replication successfully connected to this computer during the last rescan session.
- Select the **Notify on success**, **Notify on warning** and/or **Notify on error** check boxes to receive email notification if the protection group rescan job completes successfully, completes with a warning or fails.



☑ Send daily agent status report e-mail to the following recipients:

administrator@tech.local

Send daily summary at: 10:00 PM

○ Use global notification settings

● Use custom notification settings specified below:

Subject:

FoundCount% new hosts found (%TotalCount% total, %SeenCount% seen)

☑ Notify on success

☑ Notify on warning

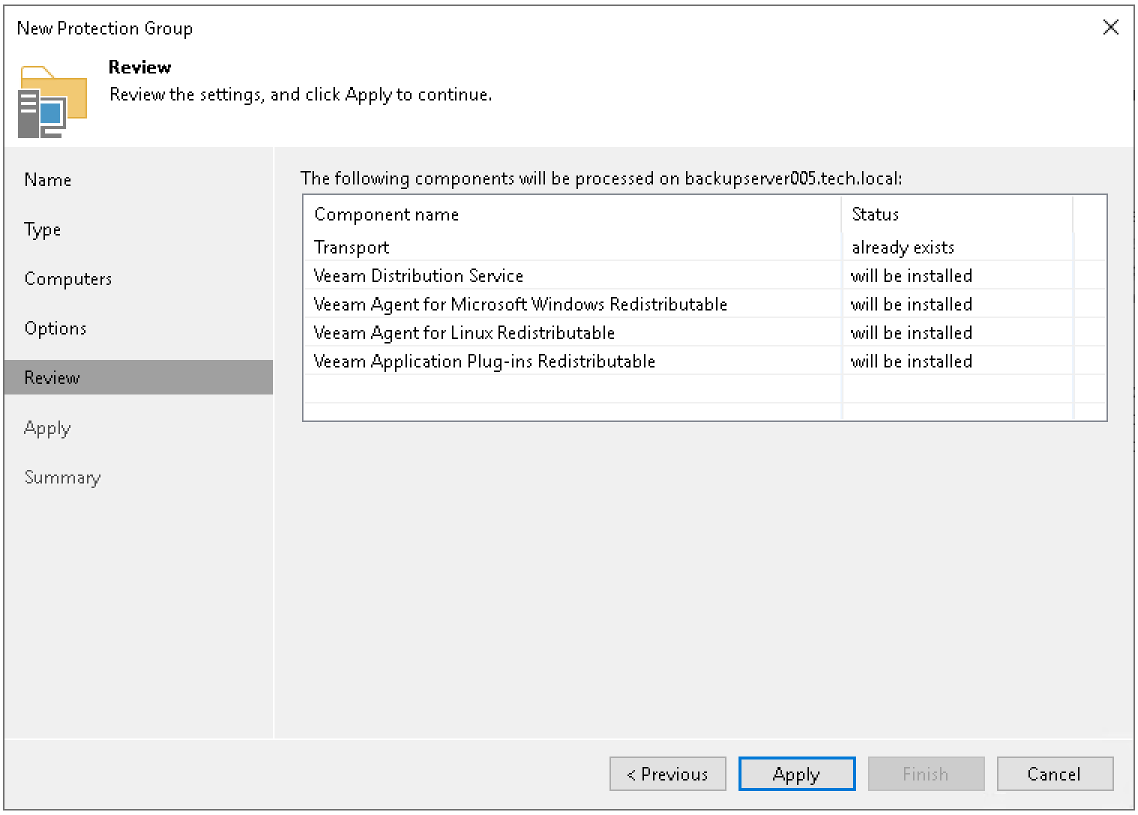
☑ Notify on error

Step 9. Review Components

At the **Review** step of the wizard, review what Veeam Backup & Replication components are already installed on the distribution server specified for the protection group and what components will be installed.

1. Review the components.
2. Click **Apply** to add the configured protection group to the inventory.

> NOTE
>
> Veeam Plug-in and Veeam Agent components are installed on the distribution server even if the **Install application plug-ins** and **Install backup agent** check boxes are clear at the Options step of the wizard.

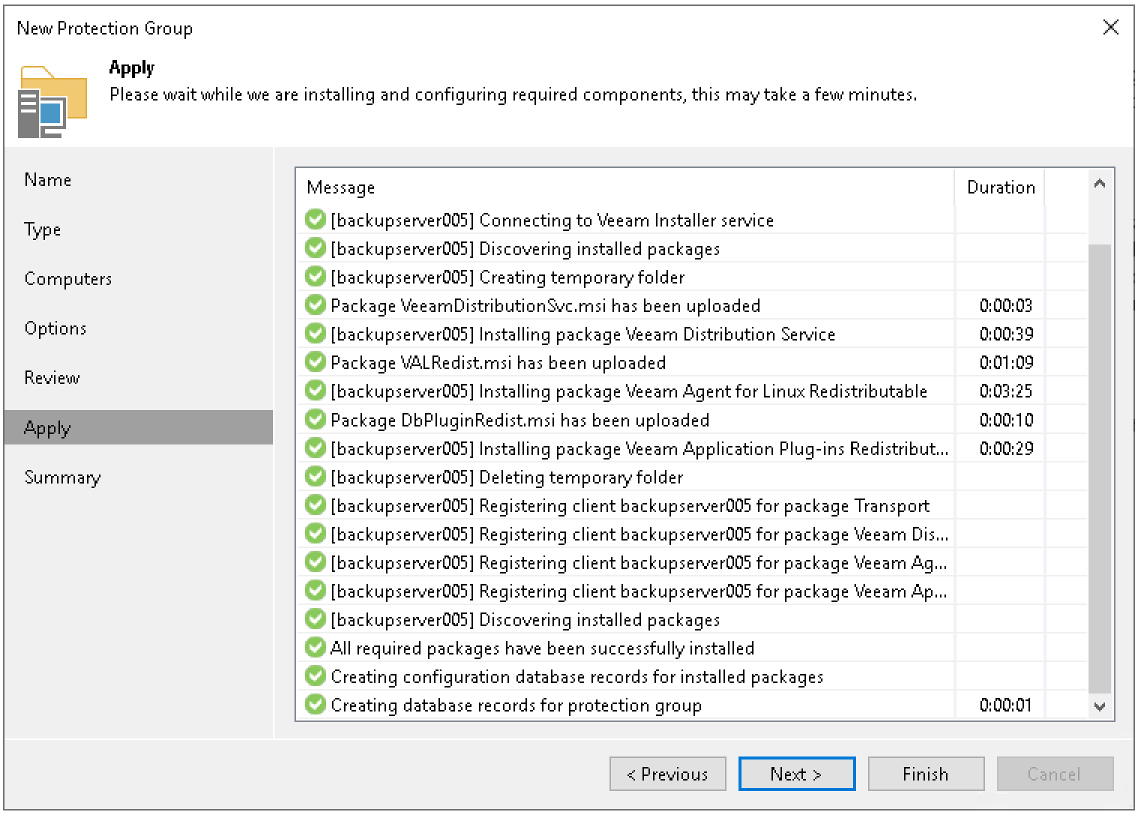


The following components will be processed on backupserver005.tech.local:

Component name	Status
Transport	already exists
Veeam Distribution Service	will be installed
Veeam Agent for Microsoft Windows Redistributable	will be installed
Veeam Agent for Linux Redistributable	will be installed
Veeam Application Plug-ins Redistributable	will be installed

Step 10. Assess Results

At the **Apply** step of the wizard, Veeam Backup & Replication will create the configured protection group. Wait for the operation to complete and click **Next** to continue.



New Protection Group

Apply

Please wait while we are installing and configuring required components, this may take a few minutes.

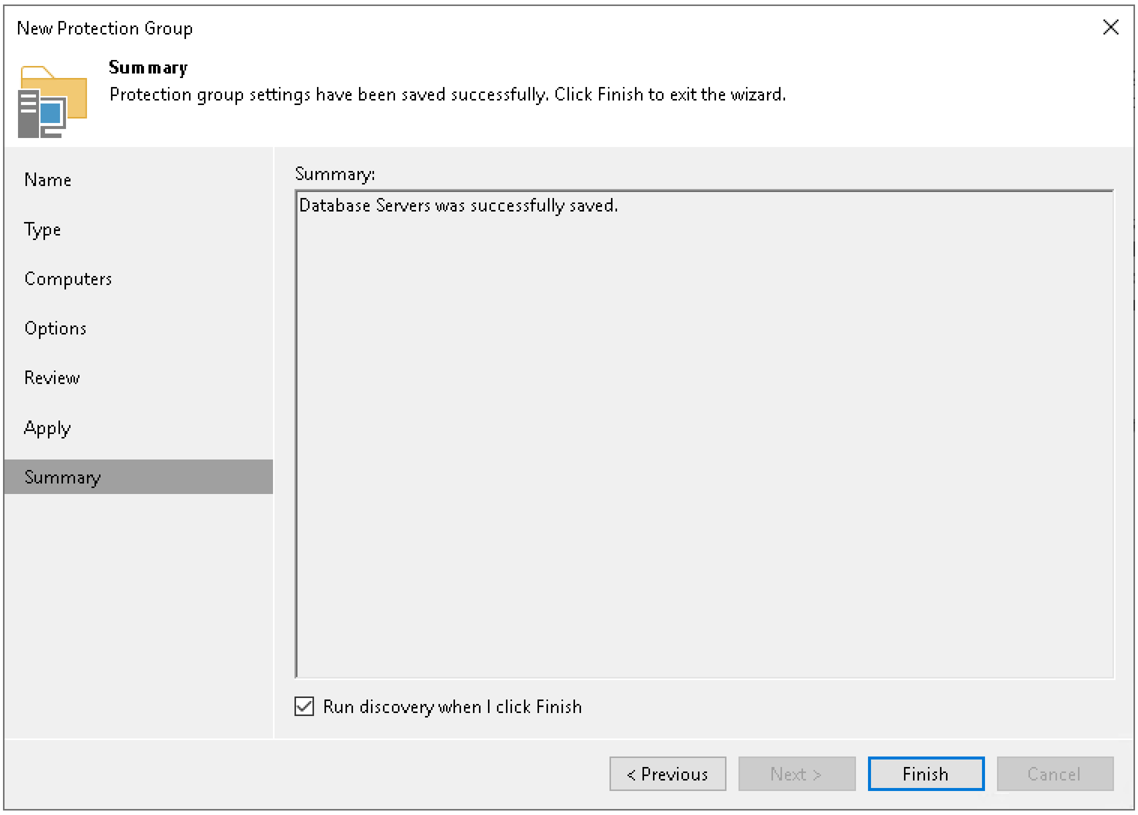
Message	Duration
✓ [backupserver005] Connecting to Veeam Installer service	
✓ [backupserver005] Discovering installed packages	
✓ [backupserver005] Creating temporary folder	
✓ Package VeeamDistributionSvc.msi has been uploaded	0:00:03
✓ [backupserver005] Installing package Veeam Distribution Service	0:00:39
✓ Package VALRedist.msi has been uploaded	0:01:09
✓ [backupserver005] Installing package Veeam Agent for Linux Redistributable	0:03:25
✓ Package DbPluginRedist.msi has been uploaded	0:00:10
✓ [backupserver005] Installing package Veeam Application Plug-ins Redistribut...	0:00:29
✓ [backupserver005] Deleting temporary folder	
✓ [backupserver005] Registering client backupserver005 for package Transport	
✓ [backupserver005] Registering client backupserver005 for package Veeam Dis...	
✓ [backupserver005] Registering client backupserver005 for package Veeam Ag...	
✓ [backupserver005] Registering client backupserver005 for package Veeam Ap...	
✓ [backupserver005] Discovering installed packages	
✓ All required packages have been successfully installed	
✓ Creating configuration database records for installed packages	
✓ Creating database records for protection group	0:00:01

Step 11. Finish Working with Wizard

At the **Summary** step of the wizard, complete the protection group configuration process.

1. Review information about the created protection group.
2. To start the rescan job after you close the wizard, make sure that the **Run discovery when I click Finish** option is selected.

   If you want to perform computer discovery later, you can clear the **Run discovery when I click Finish** check box. In this case, the rescan job will start automatically upon the defined schedule. You can also start the rescan job manually at any time you need. To learn more, see Starting Protection Group Discovery.
3. Click **Finish to close the wizard**.


New Protection Group

Summary

Protection group settings have been saved successfully. Click Finish to exit the wizard.

Summary:

Database Servers was successfully saved.

☑ Run discovery when I click Finish

What You Do Next

After you create a protection group, Veeam Backup & Replication automatically rescans computers that you added to the created protection group and deploys Veeam Plug-ins on these computers. To learn more, see Rescan Job.

After the rescan process completes and Veeam Plug-ins are successfully deployed on target computers, you can create the application backup policy. Application backup policies allow you to protect computers in the protection group. To learn more, see Working with Application Policies.

Editing Protection Group Settings

You can edit settings of a protection group. This operation may be required, for example, if you want to add/remove computers to/from a protection group or change settings for protected computers discovery and Veeam Plug-in deployment defined in the properties of the protection group.

> **NOTE**
>
> Consider the following:
>
> - You cannot change the type of a protection group when editing protection group settings.
> - For the *Manually Added* protection group, you can change only a limited number of settings. In particular, you can edit protected computers discovery and Veeam Plug-in deployment options (except for changing the distribution server for the protection group). You can also remove from this protection group computers that are no longer included in an application backup policy.
> - You cannot edit settings of default protection groups that act as filters used to display protected computers of a specific type: *Unmanaged*, *Out of Date*, *Offline* and *Untrusted*.

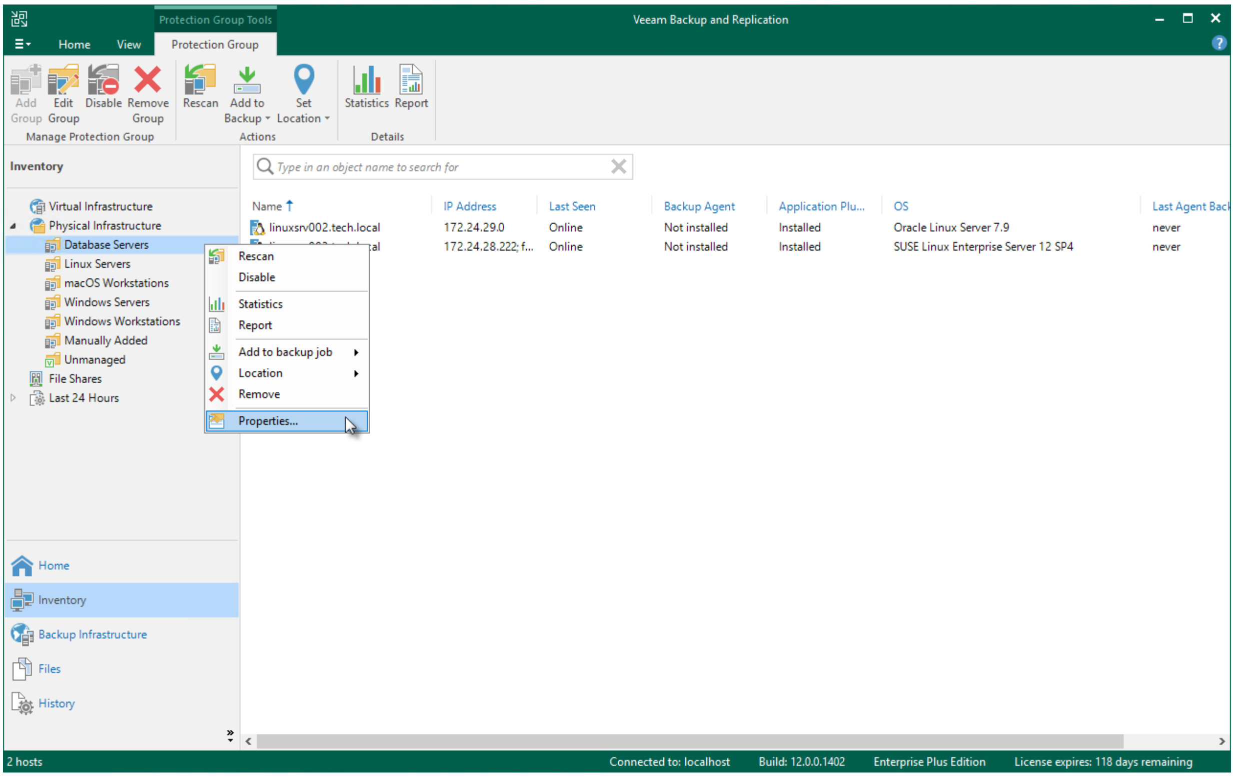
To edit protection group settings:

1. Open the **Inventory** view.

2. In the inventory pane, expand the **Physical Infrastructure** node.

3. In the inventory pane, select the protection group that you want to edit and click **Edit Group** on the ribbon or right-click the protection group that you want to edit and select **Properties**.

4. Edit protection group settings as required.



Name ↑	IP Address	Last Seen	Backup Agent	Application Plu...	OS	Last Agent Back
linuxsrv002.tech.local	172.24.29.0	Online	Not installed	Installed	Oracle Linux Server 7.9	never
[illegible]al	172.24.28.222; f...	Online	Not installed	Installed	SUSE Linux Enterprise Server 12 SP4	never

2 hosts Connected to: localhost Build: 12.0.0.1402 Enterprise Plus Edition License expires: 118 days remaining

Rescanning Protection Group

You can rescan a protection group configured in the inventory. When you perform protection group rescan, you manually start the discovery process for the protection group. This operation may be required, for example, if you want to discover new computers added to the protection group without waiting for the next scheduled start of the rescan job.

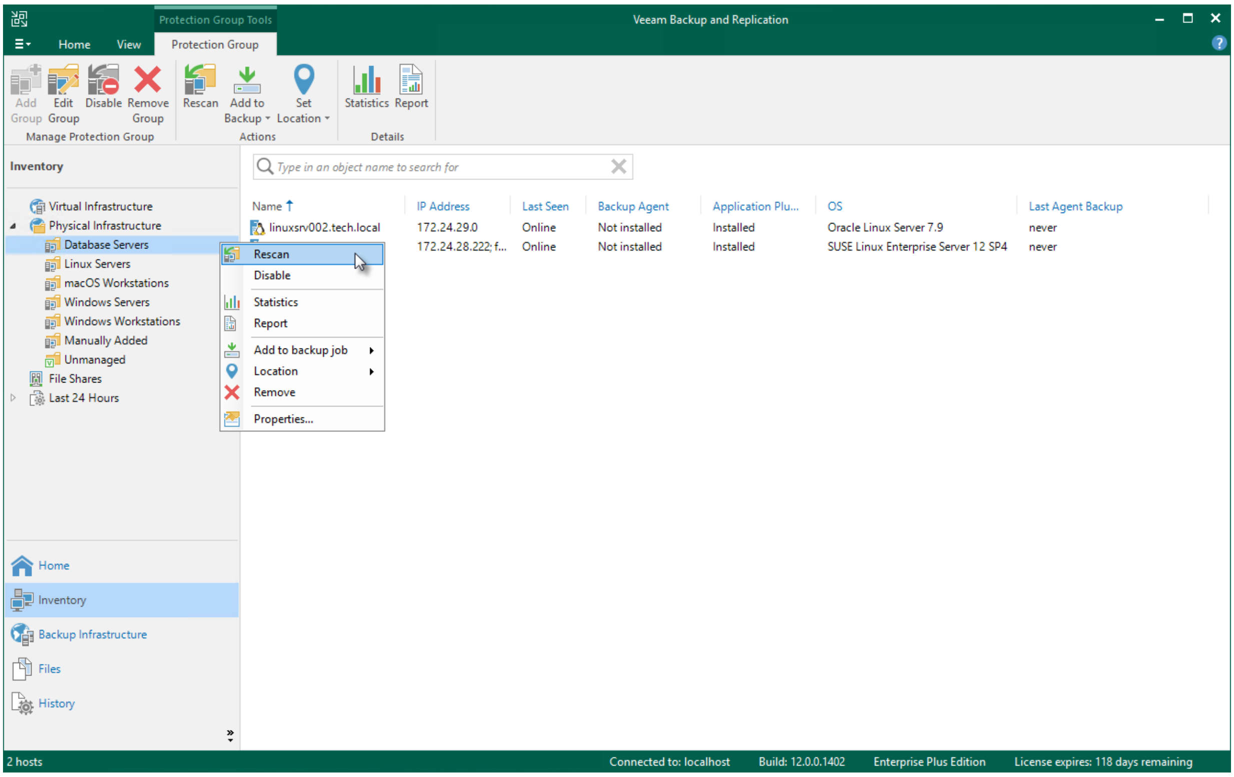
During the rescan operation, Veeam Backup & Replication starts the rescan job in the same way as in case of scheduled discovery. The rescan job connects to computers included in the protection group and performs on these computers operations specified in the protection group settings. For example, if Veeam Backup & Replication is set up to automatically install Veeam Plug-in on protected computers during discovery, you can use the rescan operation to deploy Veeam Plug-in to computers that have appeared in the protection group after the previous scheduled rescan job session finished.

To rescan a protection group:

1. Open the **Inventory** view.

2. In the inventory pane, expand the **Physical Infrastructure** node.

3. In the inventory pane, select the necessary protection group and click **Rescan** on the ribbon or right-click the protection group and select **Rescan**.



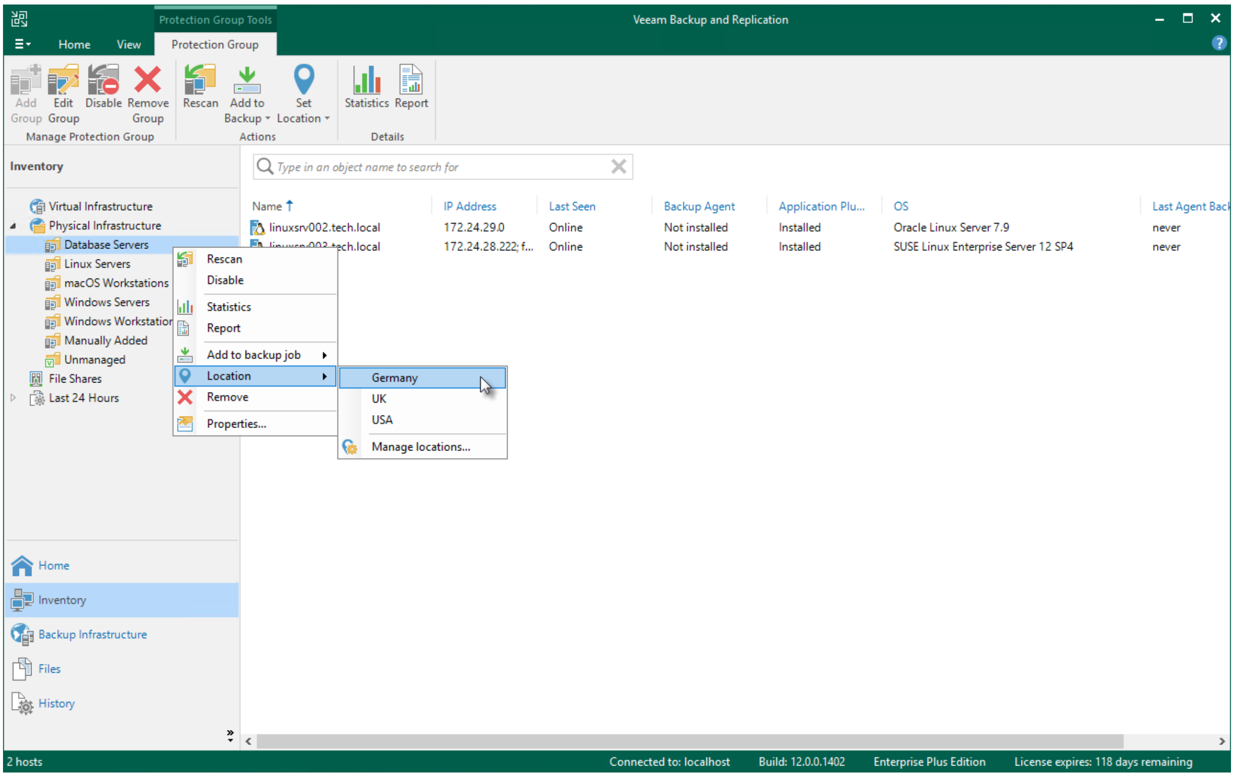
Name	IP Address	Last Seen	Backup Agent	Application Plu...	OS	Last Agent Backup
linuxsrv002.tech.local	172.24.29.0	Online	Not installed	Installed	Oracle Linux Server 7.9	never
	172.24.28.222; f...	Online	Not installed	Installed	SUSE Linux Enterprise Server 12 SP4	never

Assigning Location to Protection Group

You can assign a location to a protection group configured in Veeam Backup & Replication. To assign a location:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node.
3. In the inventory pane, select the necessary protection group and click **Location** > *<Location name>* on the ribbon or right-click the necessary protection group and select **Location** > *<Location name>*.

To learn more about locations, see the Locations section in the Veeam Backup & Replication User Guide.



Name	IP Address	Last Seen	Backup Agent	Application Plu...	OS	Last Agent Back
linuxsrv002.tech.local	172.24.29.0	Online	Not installed	Installed	Oracle Linux Server 7.9	never
...ch.local	172.24.28.222; f...	Online	Not installed	Installed	SUSE Linux Enterprise Server 12 SP4	never

2 hosts
Connected to: localhost
Build: 12.0.0.1402
Enterprise Plus Edition
License expires: 118 days remaining

Disabling Protection Group

You can temporary disable a protection group configured in the inventory. When you disable a protection group, you disable scheduled discovery of protected computers added to this protection group. This may be required, for example, if a new version of Veeam Plug-in appears on a distribution server, and you do not want to deploy Veeam Plug-in to all protected computers at once. Instead, you can disable the protection group, test the deployment process on a specific computer in this group, and then enable the protection group to let Veeam Backup & Replication deploy Veeam Agent to remaining computers.

When you disable a protection group, Veeam Backup & Replication does not start the rescan job upon schedule defined in the protection group settings. However, you can start the discovery process manually if needed. To learn more, see Rescanning Protection Group.

Disabling a protection group does not affect processing of computers included in this protection group. If a protected computer is added to an application policy, and the application policy is scheduled to start at the time when the protection group is in the disabled state, the policy will run as usual.

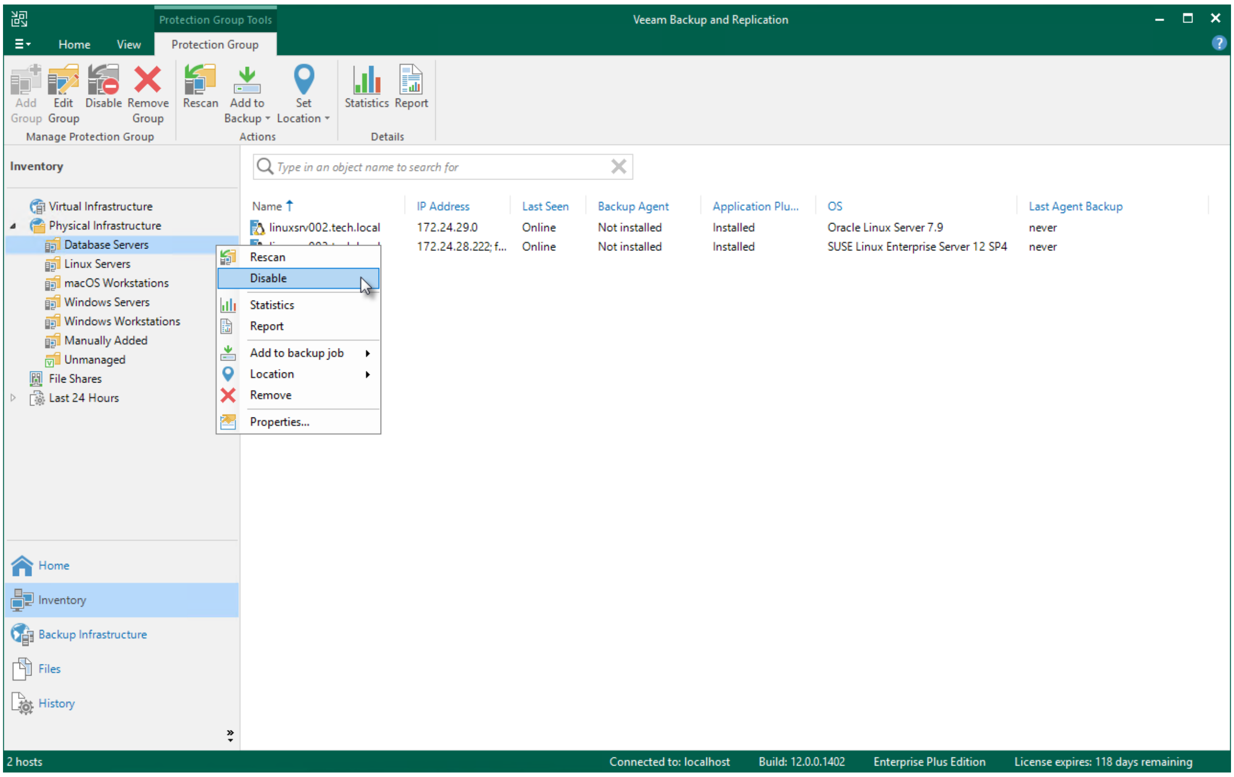
> **NOTE**
>
> You cannot disable default protection groups that act as filters used to display protected computers of a specific type: *Unmanaged*, *Out of Date*, *Offline* and *Untrusted*.

To disable automatic discovery for the protection group:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node.
3. In the inventory pane, select the necessary protection group and click **Disable** on the ribbon or right-click the necessary protection group and select **Disable**.

To enable automatic discovery for the protection group:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node.
3. In the inventory pane, select the necessary protection group and click **Disable** on the ribbon or right-click the necessary protection group and select **Disable**.



Name	IP Address	Last Seen	Backup Agent	Application Plu...	OS	Last Agent Backup
linuxsrv002.tech.local	172.24.29.0	Online	Not installed	Installed	Oracle Linux Server 7.9	never
	172.24.28.222; f...	Online	Not installed	Installed	SUSE Linux Enterprise Server 12 SP4	never

Removing Protection Group

You can remove a protection group that you configured.

When you remove a protection group, you can instruct Veeam Backup & Replication to remove Veeam Plug-ins from all protected computers included in this protection group, too. The protection group is removed permanently. You cannot undo this operation.

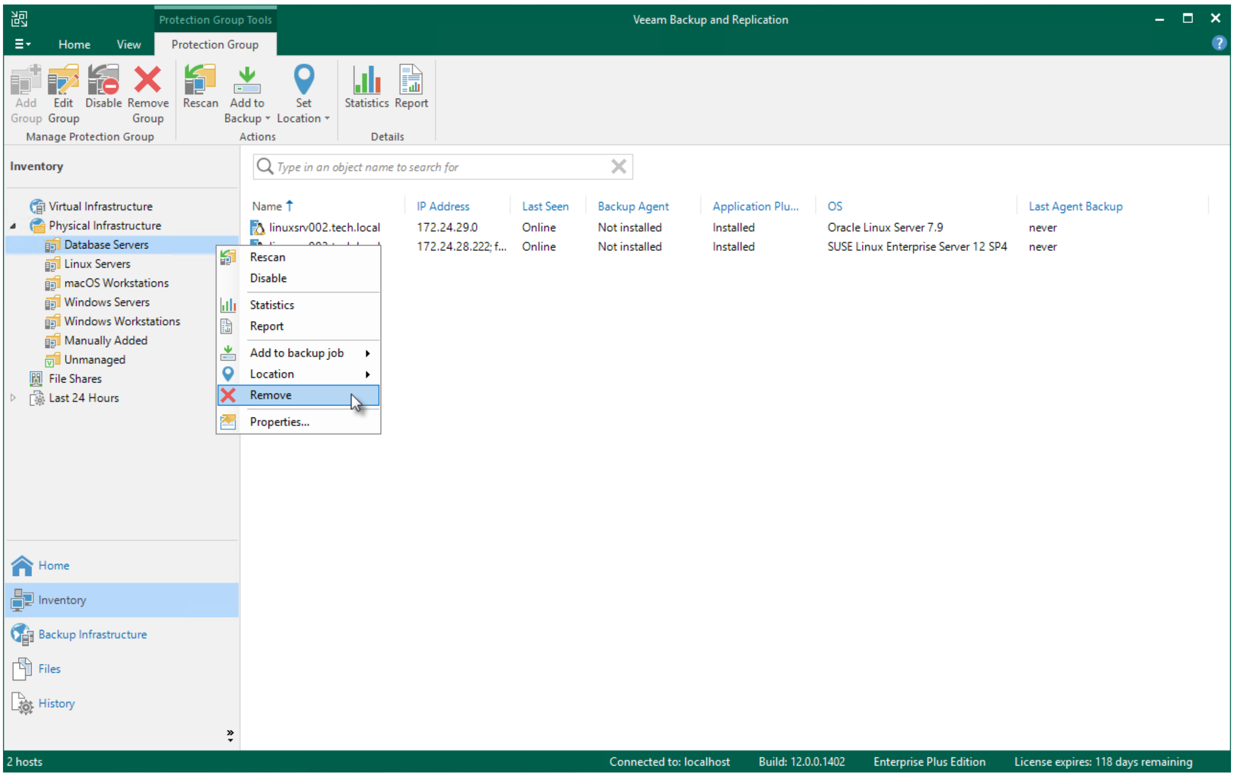
Backups created for computers that were included in the removed protection group remain intact in the backup location. You can delete this backup data manually later if needed.

> NOTE
>
> Consider the following:
>
> - You cannot remove a protection group if the entire protection group or a separate computer included in this protection group is added to an application backup policy.
> - You cannot remove default protection groups, such as *Unmanaged*, *Out of Date* and so on.

> TIP
>
> You can also remove individual computers from protection groups. To learn more, see Removing Computer from Protection Group.

To remove a protection group:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node.
3. In the inventory pane, select the protection group that you want to remove and click **Remove Group** on the ribbon or right-click the protection group and select **Remove**.
4. If you want to remove Veeam Plug-in deployed on protected computers, in the displayed window, select the **Uninstall Everything** check box. With this option selected, Veeam Backup & Replication will remove the protection group from the configuration database and, in addition, uninstall Veeam Plug-ins and Veeam Agents from every computer in the deleted protection group.
5. In the displayed window, click **Yes**.



Name	IP Address	Last Seen	Backup Agent	Application Plu...	OS	Last Agent Backup
linuxsrv002.tech.local	172.24.29.0	Online	Not installed	Installed	Oracle Linux Server 7.9	never
[illegible]	172.24.28.222; f...	Online	Not installed	Installed	SUSE Linux Enterprise Server 12 SP4	never

2 hosts Connected to: localhost Build: 12.0.0.1402 Enterprise Plus Edition License expires: 118 days remaining

Working with Application Policies

Veeam Backup & Replication allows you to create application backup policies for the following Veeam Plug-ins:

- Creating Oracle RMAN Backup Policy
- Creating SAP HANA Backup Policy
- Creating SAP on Oracle Backup Policy

After you configured an application backup policy in Veeam Backup & Replication, you can manage it in Veeam Backup & Replication as well. To learn more, see Managing Application Backup Policy.

Creating Oracle RMAN Backup Policy

To back up databases protected with Veeam Plug-in for Oracle RMAN, you must configure an application backup policy in Veeam Backup & Replication.

Before You Begin

Before you create an application backup policy in the Veeam Backup & Replication console, check the following prerequisites:

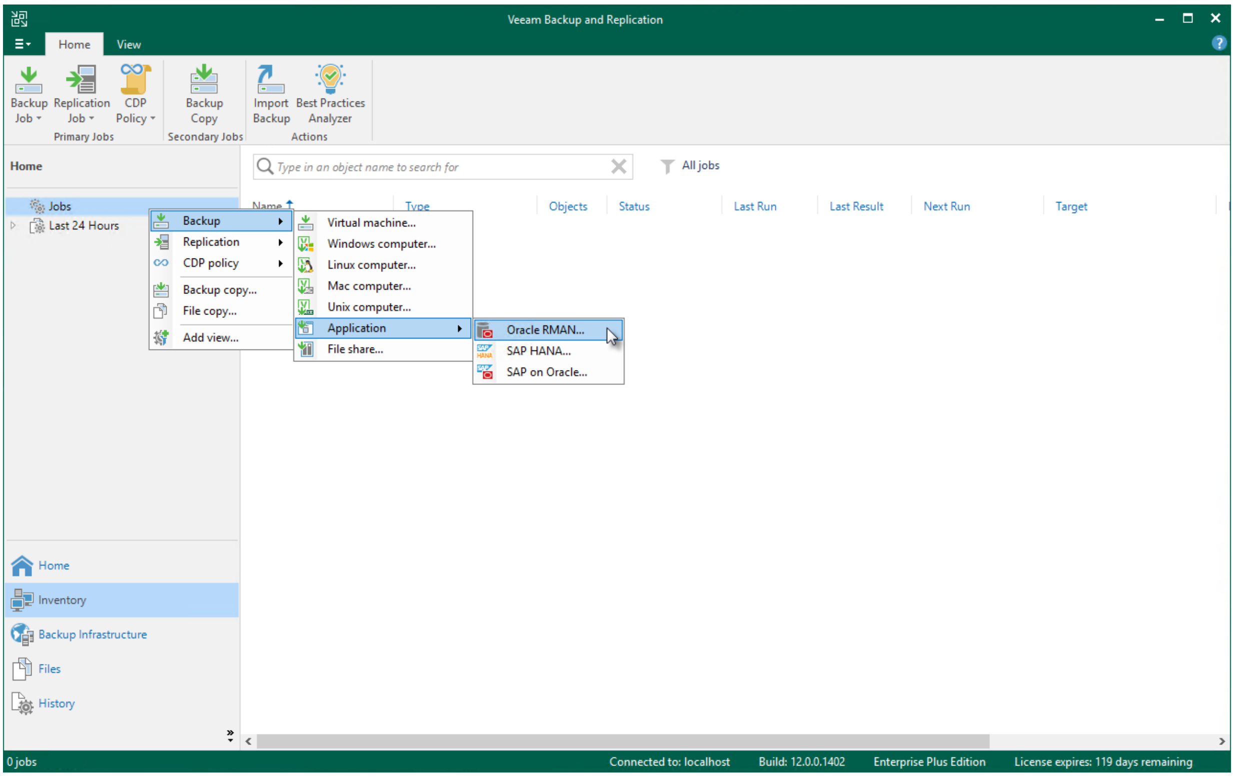
- The Veeam Backup & Replication license must have a sufficient number of instances to process computers that you plan to add to the application backup policy.
- The target location where you plan to store backup files must have enough free space.
- Protection groups that you want to add to the policy must be configured in advance.

Application backup policies have the following limitations:

- One backup object (computer, database system, or database) can be added only to one application backup policy. Otherwise, the application backup policy will fail.
- You can create application backups in a Veeam backup repository. If you want to save backups in other target locations, you must configure backup job on the computer side.
- After you start managing a Veeam Plug-in with Veeam Backup & Replication, data backup for the computer is performed by a backup policy configured in Veeam Backup & Replication. Veeam Plug-in running on the computer starts a new backup chain on a target location specified in the backup policy settings. You cannot continue the existing backup chain that was created by Veeam Plug-in operating in the standalone mode.

Step 1. Launch New Backup Job Wizard

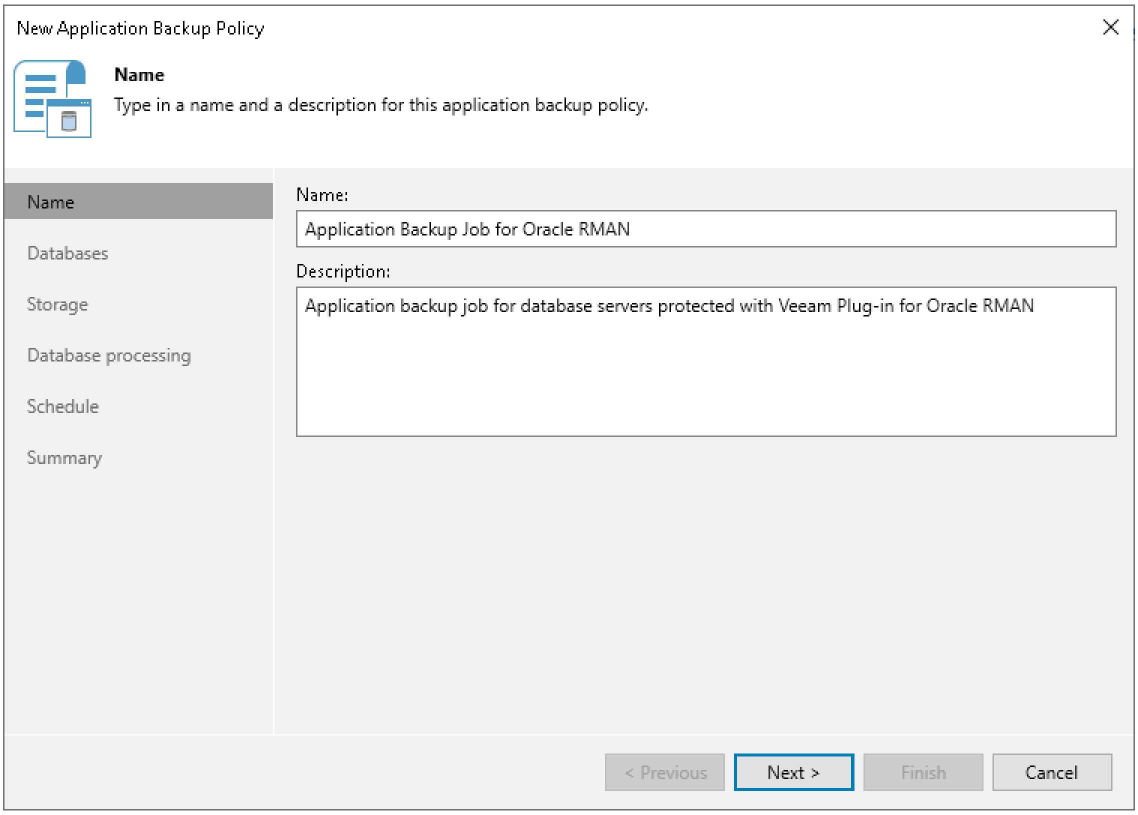
To create an application backup policy for Veeam Plug-in for Oracle RMAN, you must launch the **New Application Backup Policy** wizard. To do this, on the **Home** tab, click **Backup Job** > **Application** > **Oracle RMAN**.



Step 2. Specify Policy Name

At the **Name** step of the wizard, specify a name and description for the application backup policy.

1. In the **Name** field, enter a name for the application backup policy.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who created the policy, date and time when the policy was created.



New Application Backup Policy

Name

Type in a name and a description for this application backup policy.

Name:

Application Backup Job for Oracle RMAN

Description:

Application backup job for database servers protected with Veeam Plug-in for Oracle RMAN

Step 3. Specify Databases

At the **Databases** step of the wizard, select protection groups, computers, database systems or individual databases whose data you want to back up.

You can add to the backup scope one or more objects added to inventory in the Veeam Backup & Replication console.

Application policies with protection groups are dynamic in their nature. If Veeam Backup & Replication discovers a new computer in a protection group after the policy is created, Veeam Backup & Replication will automatically update the policy settings to include the added computer.

Adding Objects from Inventory

To add protection groups, individual computers or databases to the application backup policy:

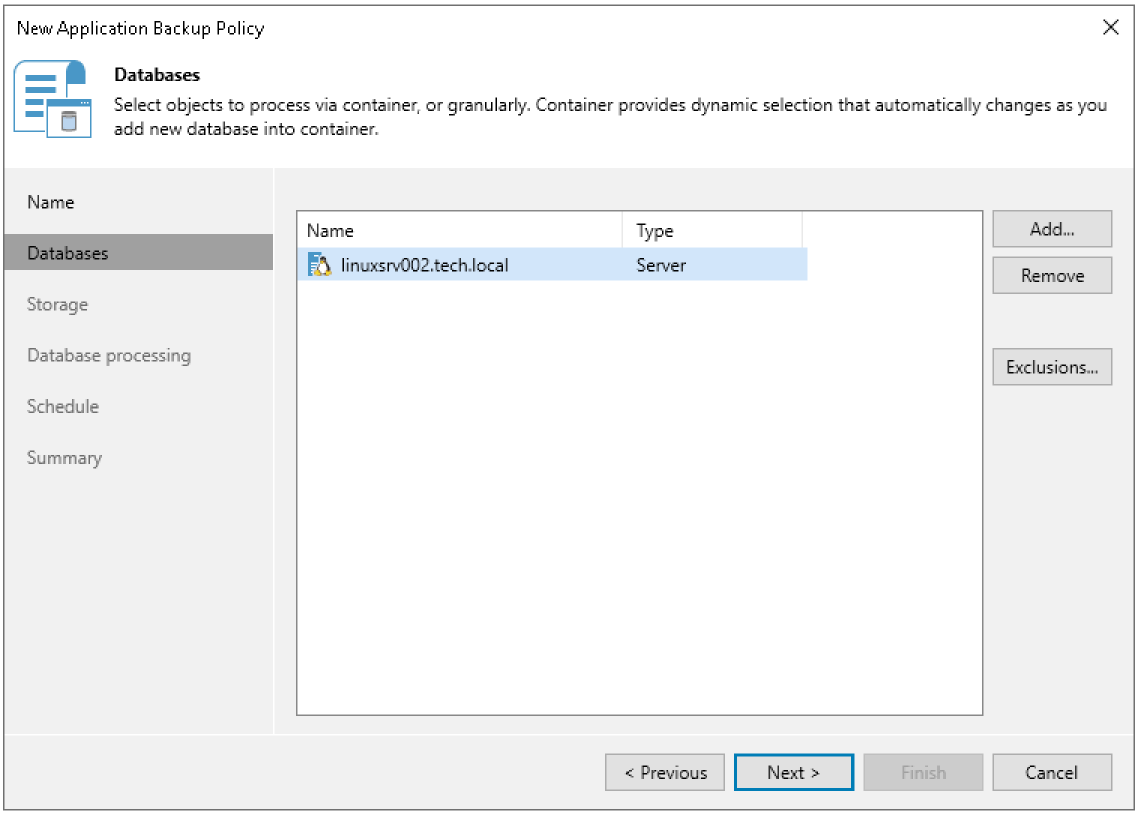
1. Click **Add**.
2. In the **Select Objects** window, select one or more objects in the list and click **OK**. You can select any of the following objects:
   - Protection group
   - Computer
   - Oracle home
   - Oracle database

   You can press and hold **[CTRL]** to select multiple objects at once.

> **NOTE**
>
> In the **Select Objects** window, Veeam Backup & Replication shows only those computers on which Veeam Backup & Replication have detected Oracle database systems during the rescan job. To learn more, see Rescan Job.

To quickly find the necessary object, use the search field at the bottom of the **Select Objects** window.

1. Enter the object name or a part of it in the search field.
2. Click the **Start search** button on the right or press **[ENTER]**.



New Application Backup Policy

Databases

Select objects to process via container, or granularly. Container provides dynamic selection that automatically changes as you add new database into container.

Name	Type
linuxsrv002.tech.local	Server

Excluding Objects

You can exclude protection groups, individual computers or databases from the backup scope of the application backup policy. This may be useful if you want to back up a certain database with another application backup policy.

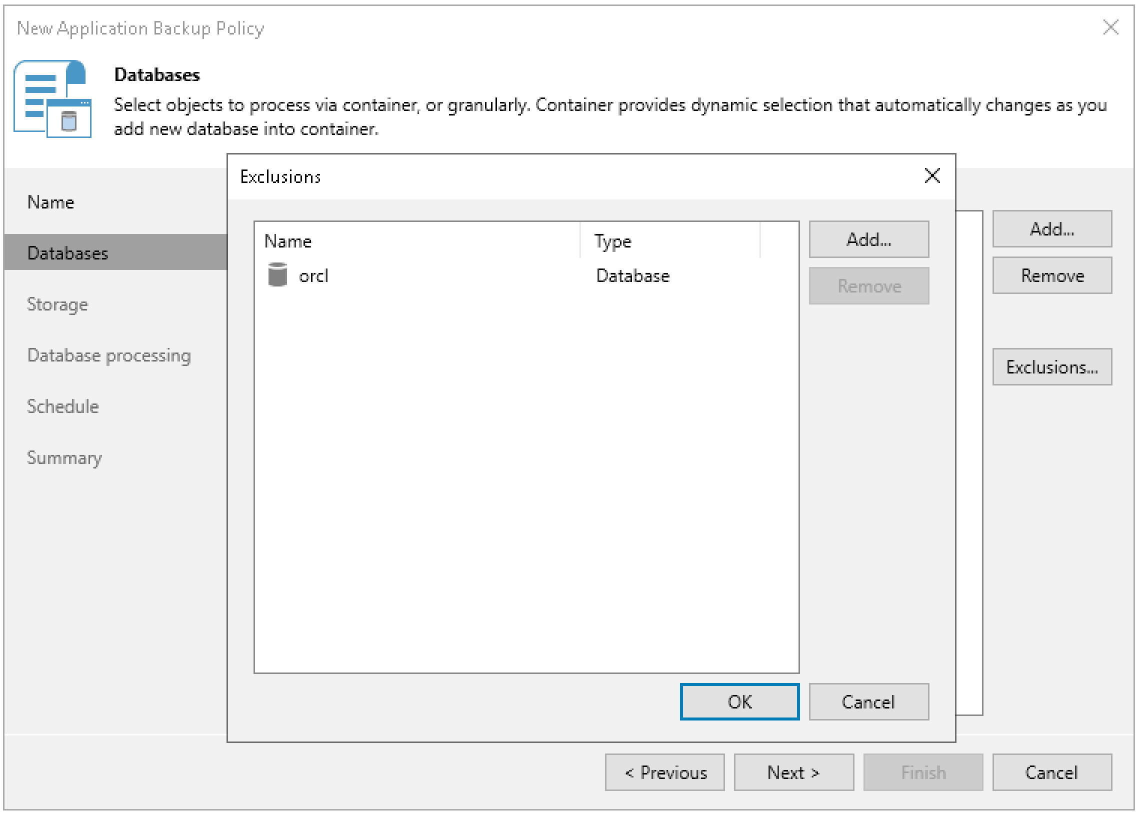
To exclude protection groups, individual computers or databases from the backup scope:

3. Click **Exclusions**.
4. In the **In the Exclusions** window, select one or more objects in the list and click **OK**. You can select any of the following objects:
   - Protection group
   - Computer
   - Oracle home
   - Oracle database

   You can press and hold **[CTRL]** to select multiple objects at once.

NOTE

In the **Exclusions** window, Veeam Backup & Replication shows only those objects which were already added to the backup scope. To learn more, see Adding Objects from Inventory.



New Application Backup Policy

Databases

Select objects to process via container, or granularly. Container provides dynamic selection that automatically changes as you add new database into container.

Name	Type
orcl	Database

Step 4. Specify Storage Settings

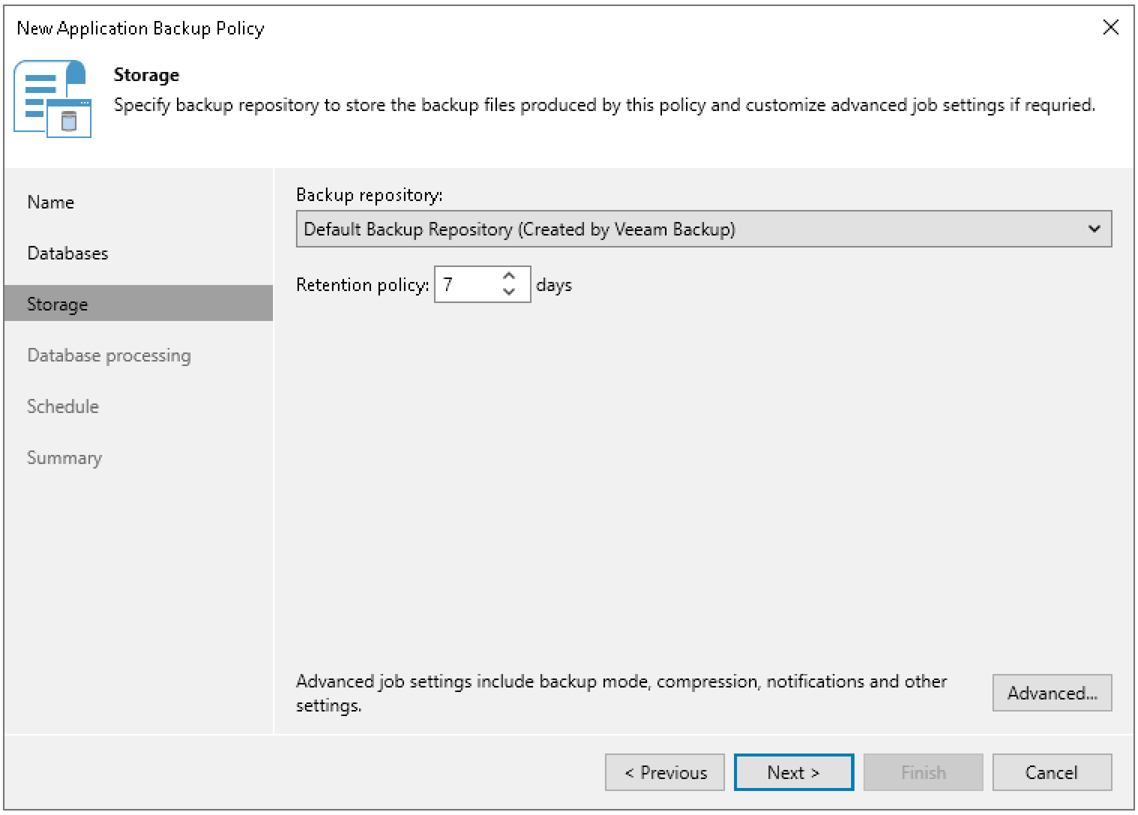
At the **Storage** step of the wizard, specify settings for the target backup repository:

1. From the **Backup repository** list, select a backup repository where you want to store backups. You can select from the Veeam backup repositories configured on the backup server that will manage the created backup policy.

   When you select a backup repository, Veeam Backup & Replication automatically checks how much free space is available on the backup repository.

2. In the **Retention Policy** field, specify the number of days for which you want to store backup files in the target location. By default, Veeam Backup & Replication keeps backup files for 7 days. After this period is over, Veeam Backup & Replication will remove the earliest restore points from the backup chain.

3. Click **Advanced** to specify advanced settings for the backup job. To learn more, see Specify Advanced Backup Settings.



New Application Backup Policy

Storage

Specify backup repository to store the backup files produced by this policy and customize advanced job settings if requried.

Backup repository: Default Backup Repository (Created by Veeam Backup)

Retention policy: 7 days

Advanced job settings include backup mode, compression, notifications and other settings.

Step 5. Specify Advanced Backup Settings

In the **Advanced Settings** window, specify advanced settings for the application backup policy:

- Backup settings
- Storage settings
- Notification settings
- Oracle settings

> **TIP**
>
> After you specify necessary settings for the application backup policy, you can save them as default settings. To do this, click **Save as Default** at the bottom left corner of the **Advanced Settings** window. When you create a new backup job, Veeam Backup & Replication will automatically apply the default settings to the new job.

Backup Settings

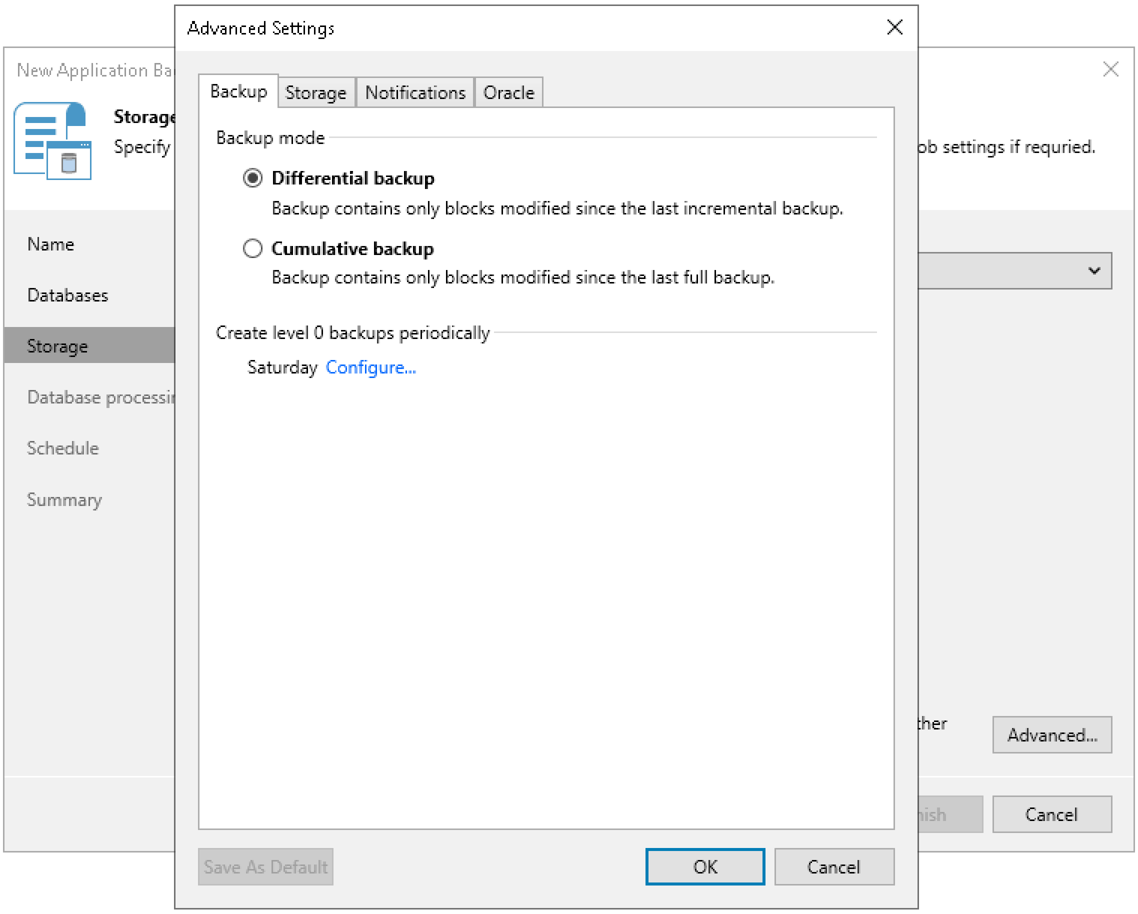
To specify settings for a backup chain created with the backup policy:

1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Backup** tab.
3. In the **Backup mode**, select one of the following modes for incremental backups:
   - Differential backup. In this mode, Veeam Backup & Replication will create a backup of data changed since the last incremental data backup.
   - Cumulative backup. In this mode, Veeam Backup & Replication will create a backup of data changed since the last full data backup.

4. To define the schedule for full backups, click **Configure** and define the schedule in the **Schedule Settings** window:

   - To run the full backup once a month on specific days, select **Monthly on**. Use the fields on the right to configure the necessary schedule.

   - To run the full backup once a week on specific week days, select **Weekly**. Use the fields on the right to select the necessary week days.



Backup mode

● **Differential backup**
Backup contains only blocks modified since the last incremental backup.

○ **Cumulative backup**
Backup contains only blocks modified since the last full backup.

Create level 0 backups periodically

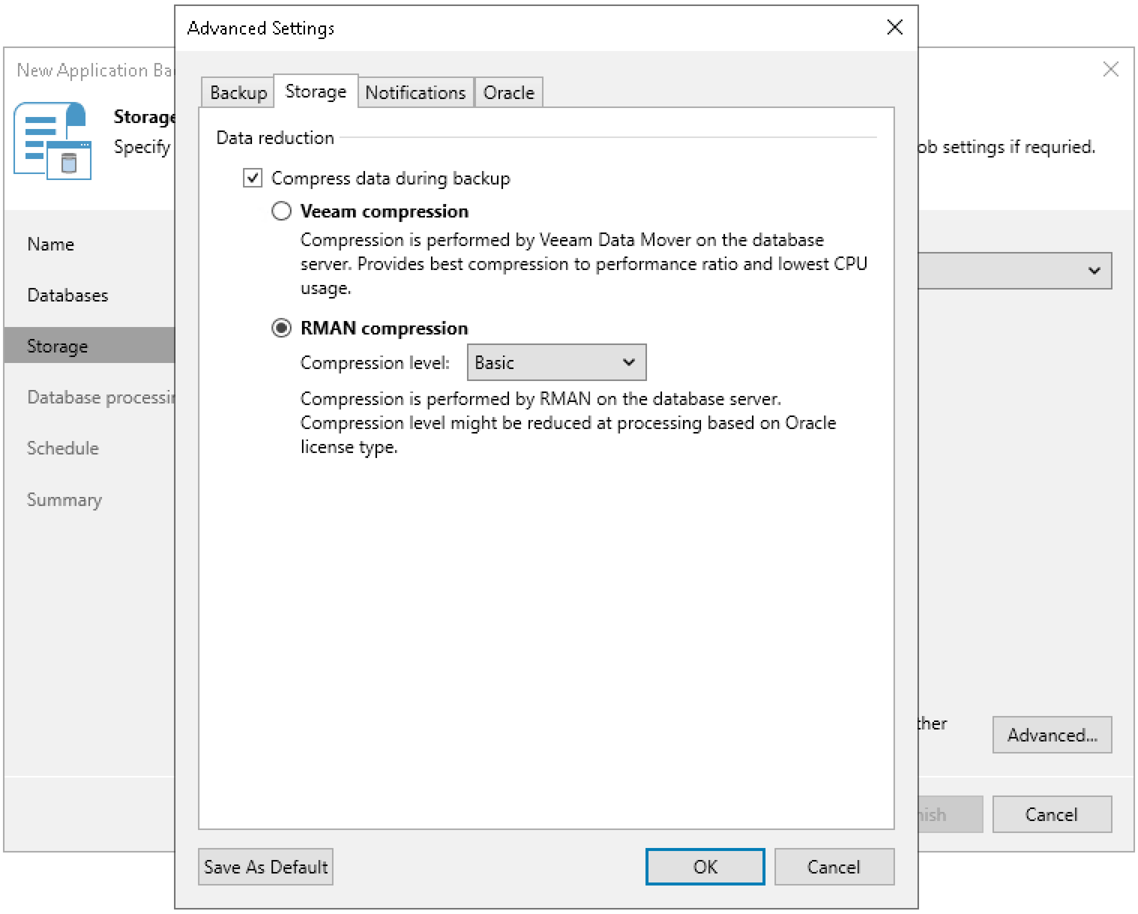
Saturday Configure...

Storage Settings

To specify compression settings for the backup job:

1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Storage** tab.
3. Select the **Compress data during backup** check box and select the way compression is performed:
   - Select **Veeam compression** if you want to perform default data compression with Data Mover by Veeam Software. If this option selected, Data Mover will use the LZ4 compression algorithm.
   - Select **RMAN compression** if you want to perform data compression with Oracle RMAN.

     If you selected the **RMAN compression** option, you can also select the compression level.



Data reduction

☑ Compress data during backup

○ **Veeam compression**

Compression is performed by Veeam Data Mover on the database server. Provides best compression to performance ratio and lowest CPU usage.

● **RMAN compression**

Compression level: Basic

Compression is performed by RMAN on the database server. Compression level might be reduced at processing based on Oracle license type.

Notification Settings

To specify notification settings for the backup policy:

1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Notifications** tab.
3. Select the **Send SNMP notifications for this job** check box if you want to receive SNMP traps when the job completes successfully.

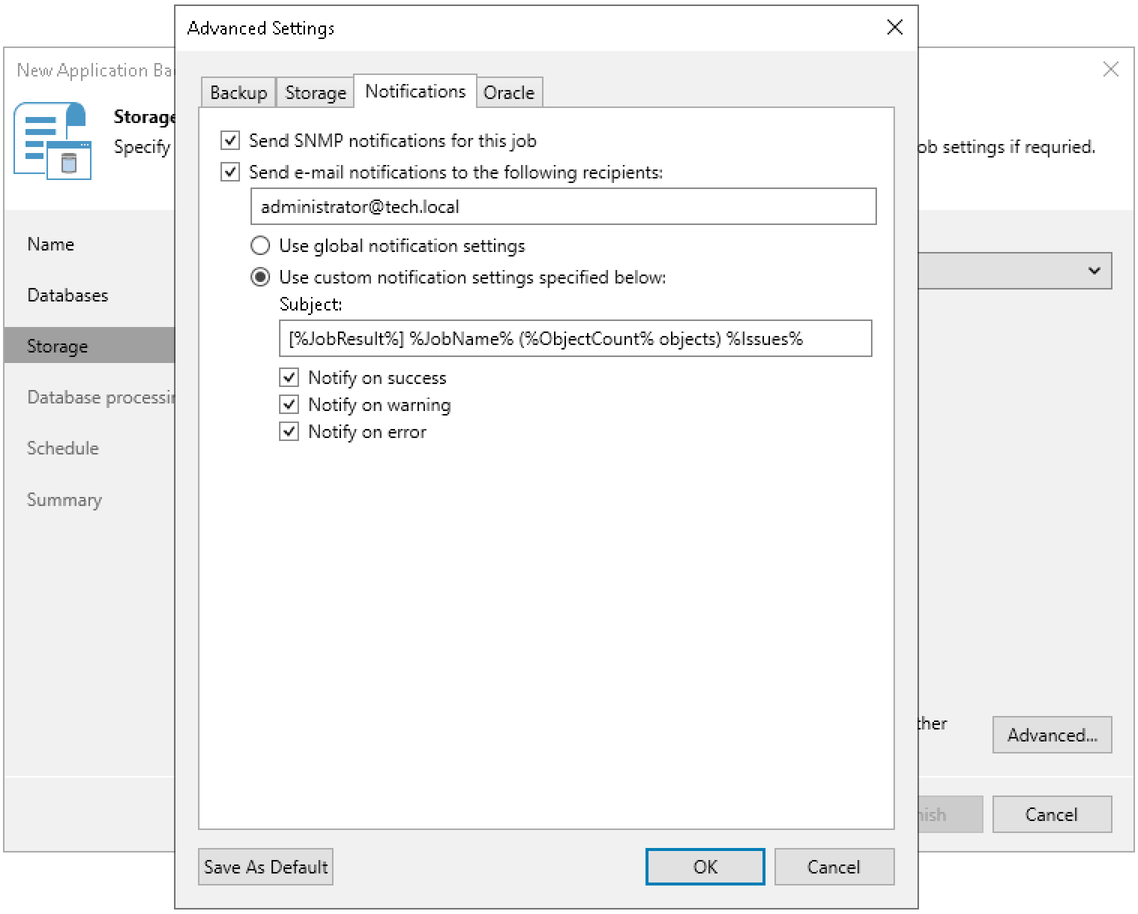
   SNMP traps will be sent if you specify global SNMP settings in Veeam Backup & Replication and configure software on recipient's machine to receive SNMP traps. For more information, see the Specifying SNMP Settings section in the Veeam Backup & Replication User Guide.

4. Select the **Send email notifications to the following recipients** check box if you want to receive notifications about the job completion status by email. In the field below, specify a recipient's email address. You can enter several addresses separated by a semicolon.

   Email notifications will be sent if you configure global email notification settings in Veeam Backup & Replication. For more information, see the Configuring Global Email Notification Settings section in Veeam Backup & Replication User Guide.

5. You can choose to use global notification settings or specify custom notification settings.

   - To receive a typical notification for the policy, select **Use global notification settings**. In this case, Veeam Backup & Replication will apply to the job global email notification settings specified for the backup server.
   - To configure a custom notification for the policy, select **Use custom notification settings specified below**. You can specify the following notification settings:
     - In the **Subject** field, specify a notification subject. You can use the following variables in the subject: *%Time%* (completion time), *%JobName%*, *%JobResult%*, *%ObjectCount%* (number of computers in the policy) and *%Issues%* (number of computers in the policy that have been processed with the *Warning* or *Failed* status).
     - Select the **Notify on success**, **Notify on warning** and/or **Notify on error** check boxes to receive email notification if the policy completes successfully, completes with a warning or fails.
     - Select the **Suppress notifications until the last retry** check box to receive a notification about the final policy status. If you do not enable this option, Veeam Backup & Replication will send one notification per every retry.

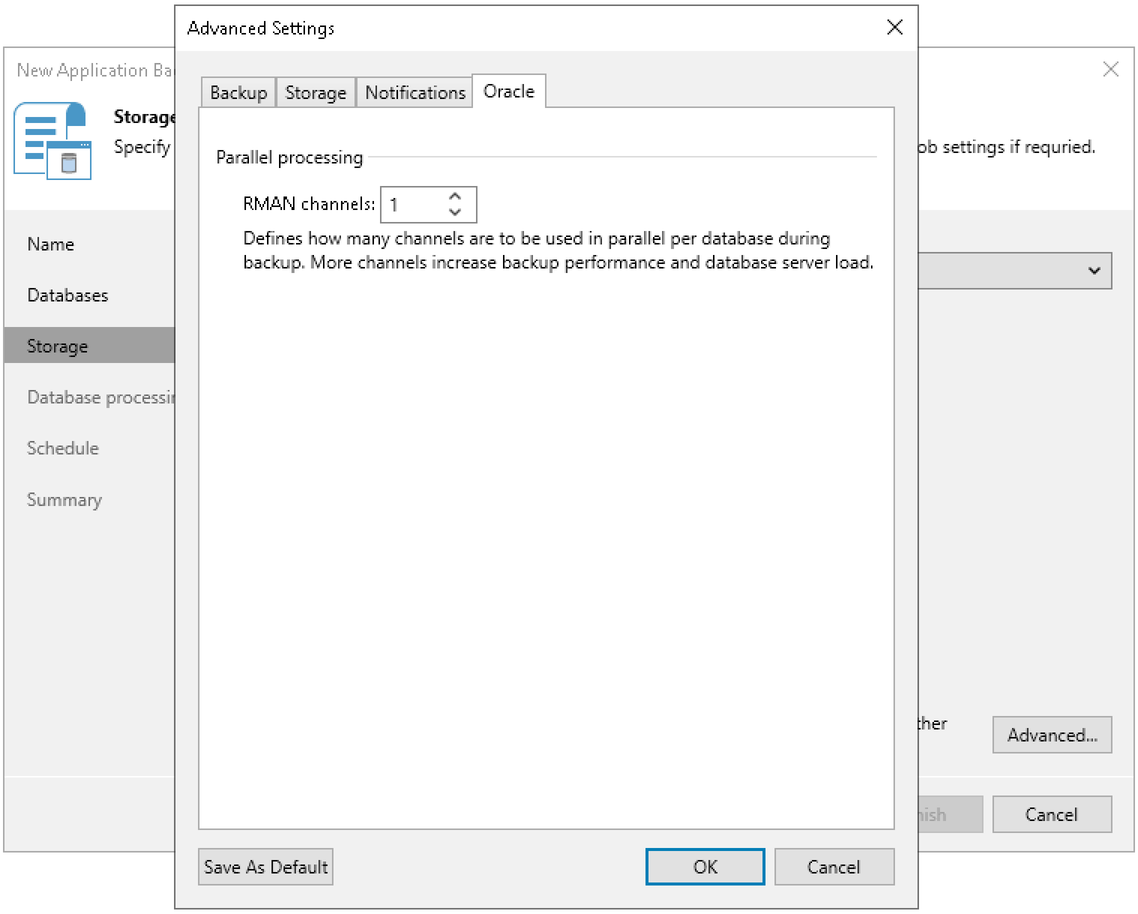


☑ Send SNMP notifications for this job
☑ Send e-mail notifications to the following recipients:
administrator@tech.local
○ Use global notification settings
● Use custom notification settings specified below:
Subject:
[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%
☑ Notify on success
☑ Notify on warning
☑ Notify on error

Oracle Settings

To specify Oracle settings for the backup policy:

1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Oracle** tab.
3. In the **RMAN channels** field, specify the number of data channels that Veeam Plug-in will use in parallel to back up databases.



Advanced Settings

Parallel processing

RMAN channels: 1

Defines how many channels are to be used in parallel per database during backup. More channels increase backup performance and database server load.

Step 6. Specify Database Processing Settings

At the **Settings** step of the wizard, specify database credentials and log processing settings:

1. In the **Credentials** list, select the object and click **Edit**.
2. Specify database credentials and log processing settings for the objects in the list:
   - Processing settings
   - [Only for databases] Pluggable database settings

In the **Credentials** list, Veeam Backup & Replication shows only those objects that you added to the backup scope at the **Databases** step of the wizard. If you added a protection group, but need to specify settings for an individual computer or database in this protection group, you can add such objects to the list. To learn more, see Adding Objects from Backup Scope.

Adding Objects from Backup Scope

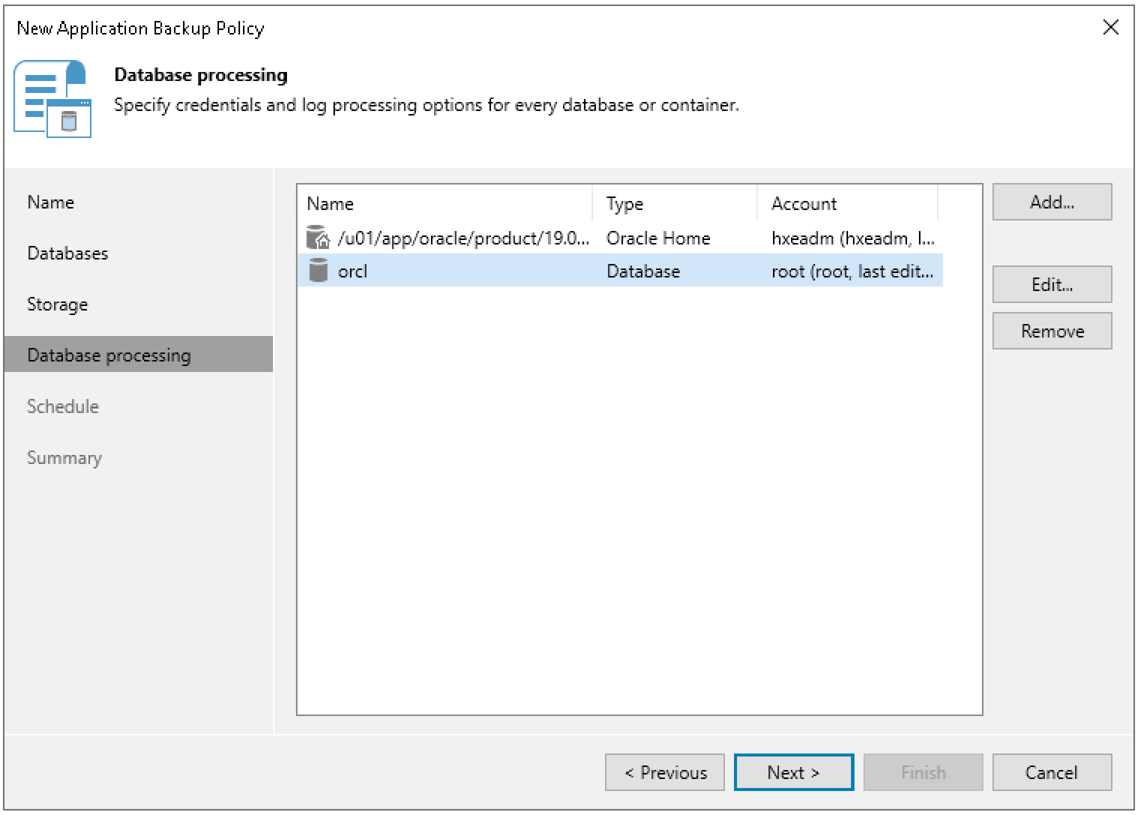
To add protection groups, individual computers or databases to the **Credentials** list:

1. Click **Add**.
2. In the **Select Objects** window, select one or more objects in the list and click **OK**. You can select any of the following objects:
   - Protection group
   - Computer
   - Oracle home
   - Oracle database

   You can press and hold **[CTRL]** to select multiple objects at once.

To quickly find the necessary object, use the search field at the bottom of the **Select Objects** window.

1. Enter the object name or a part of it in the search field.
2. Click the **Start search** button on the right or press **[ENTER]**.



New Application Backup Policy

Database processing

Specify credentials and log processing options for every database or container.

Name	Type	Account
/u01/app/oracle/product/19.0...	Oracle Home	hxeadm (hxeadm, l...
orcl	Database	root (root, last edit...

Processing Settings

To specify processing settings:

1. At the **Database** step of the wizard, select the object in the **Credentials** list and click **Edit**.
2. In the **Processing Settings** window, click the **Processing** tab.
3. To specify a user account that Veeam Plug-in will use to connect to the Oracle database, select from the **Specify Oracle account with SYSDBA privileges** list a user account that has SYSDBA rights on the database. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials.

4. In the **Archived logs** section, specify if Veeam Plug-in must delete archived logs for the Oracle database:

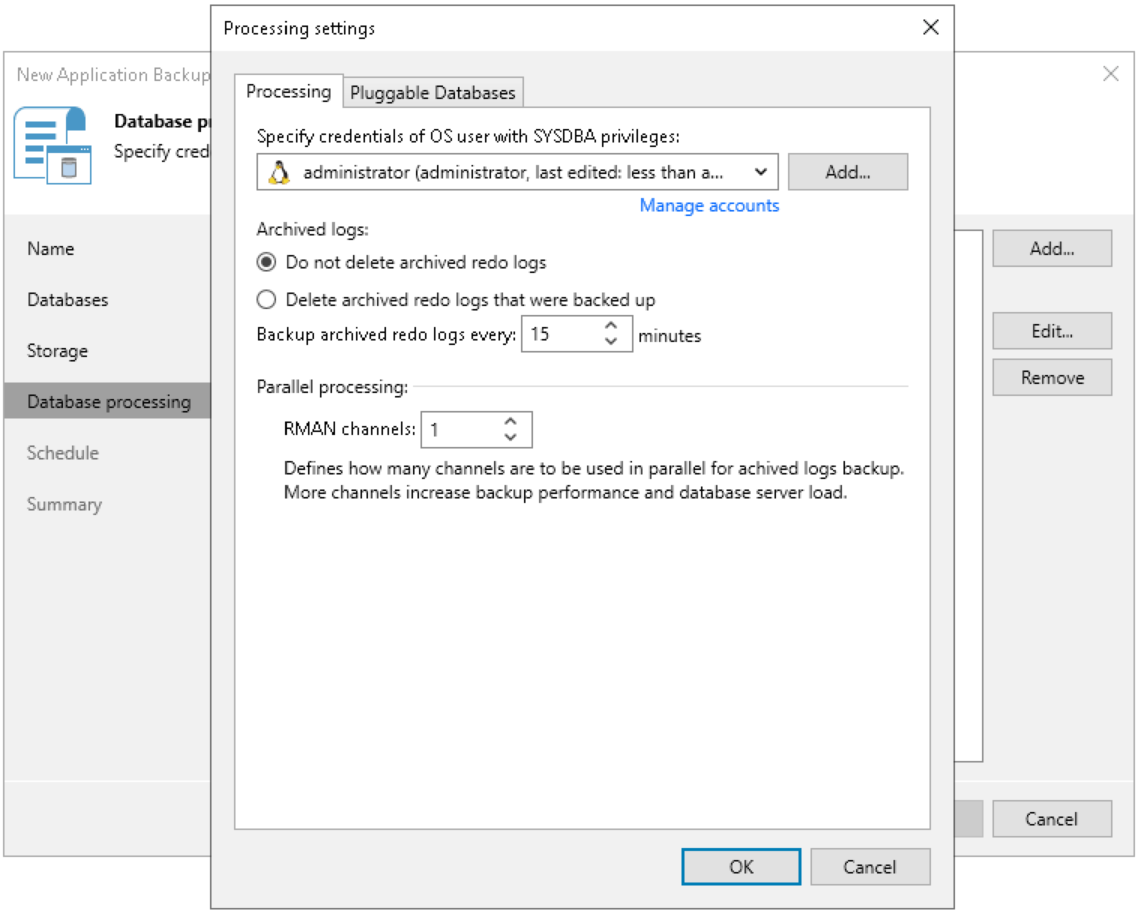
   ○ Select **Do not delete archived redo logs** if you want Veeam Plug-in to preserve archived logs. When the backup job completes, Veeam Plug-in will not delete archived logs.

     It is recommended that you select this option for databases for which the ARCHIVELOG mode is turned off. If the ARCHIVELOG mode is turned on, archived logs may grow large and consume all disk space. In this case, the database administrator must take care of archived logs him-/herself.

   ○ Select **Delete archived redo logs that were backed up** if you want Veeam Plug-in back up logs and delete logs from the database after the backup operation. Veeam Plug-in will wait for the backup job to complete successfully and then trigger archived logs truncation via Oracle Call Interface (OCI). If the backup job fails, the logs will remain untouched until the next successful backup job session.

     In the **Backup archived redo logs every <N> minutes** field, specify the frequency for archived logs backup. By default, archived logs are backed up every 15 minutes. The minimum log backup interval is 5 minutes. The maximum log backup interval is 480 minutes.

5. In the **Parallel processing** section, specify the number of data channels that Veeam Plug-in will use in parallel to back up logs.



Specify credentials of OS user with SYSDBA privileges: administrator (administrator, last edited: less than a...

Archived logs:

● Do not delete archived redo logs

○ Delete archived redo logs that were backed up

Backup archived redo logs every: 15 minutes

Parallel processing:

RMAN channels: 1

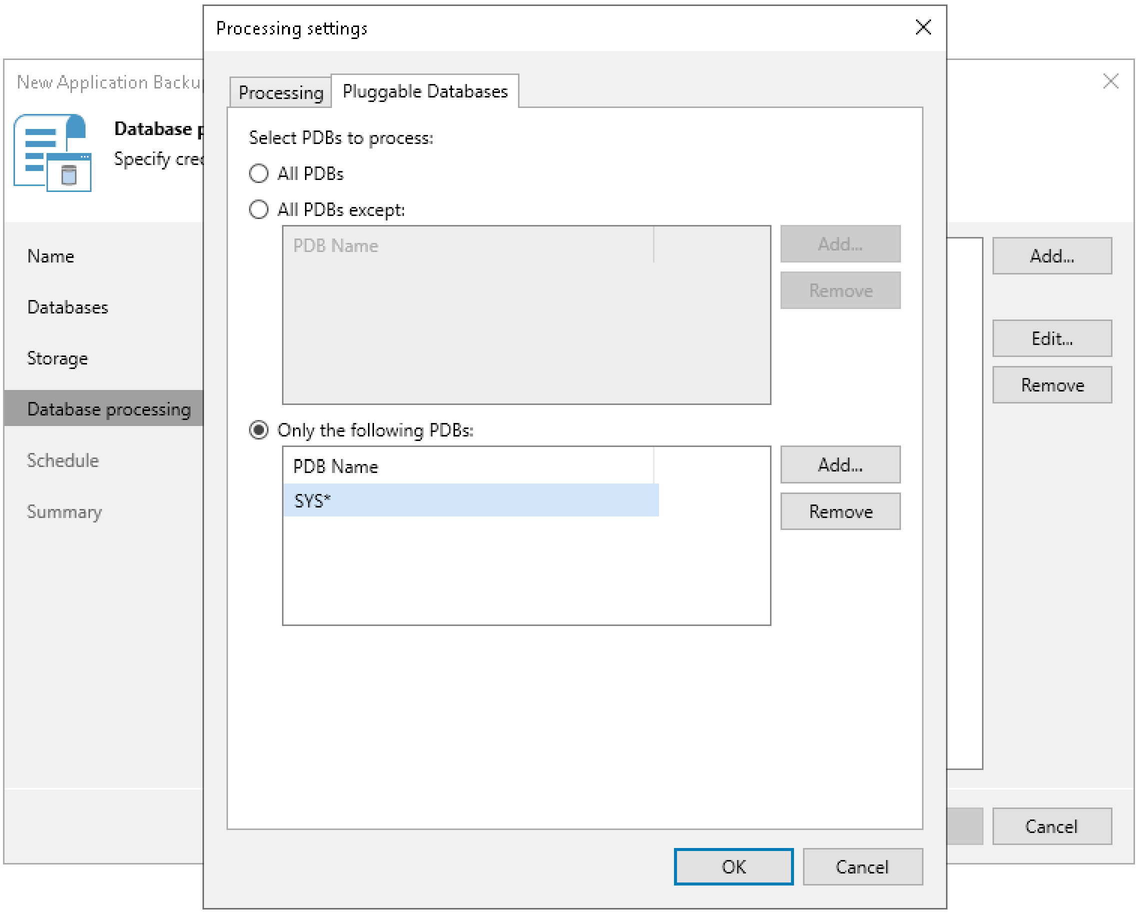
Defines how many channels are to be used in parallel for achived logs backup. More channels increase backup performance and database server load.

Pluggable Database Settings

The **Pluggable Databases** tab is available if you selected an individual database in the **Credentials** list at the **Settings** step of the wizard.

To specify settings for pluggable database (PDB) processing:

1. At the **Database** step of the wizard, select the object in the **Credentials** list and click **Edit**.
2. In the **Processing Settings** window, click the **Pluggable Databases** tab.
3. Select which pluggable databases you want to process:
   - *All PDBs* — select this option if you want to process all detected pluggable databases.
   - *All PDBs except* — select this option if you want to process all detected pluggable databases excluding the databases that you specify. Click Add to add the necessary databases or wildcards to the list.
   - *Only the following PDBs* — select this option if you want to process only those pluggable databases that you specify. Click Add to add the necessary databases or wildcards to the list.



Processing settings

Select PDBs to process:

○ All PDBs

○ All PDBs except:

● Only the following PDBs:

PDB Name
SYS*

Step 7. Specify Policy Schedule

At the **Schedule** step of the wizard, specify the schedule according to which you want to perform backup.

To specify the job schedule:

1. Select the **Run the job automatically** check box. If this check box is not selected, you will have to start the backup job manually to create backup.
2. Define scheduling settings for the job:
   - To run the job at specific time daily, on defined week days or with specific periodicity, select **Daily at this time**. Use the fields on the right to configure the necessary schedule.
   - To run the job once a month on specific days, select **Monthly at this time**. Use the fields on the right to configure the necessary schedule.
   - To run the job repeatedly throughout a day with a specific time interval, select **Periodically every**. In the field on the right, select the necessary time unit: *Hours* or *Minutes*.
   - [For backup job managed by backup server] To define the permitted time window for the job, click **Schedule** and use the time table. In the **Start time within an hour** field, specify the exact time when the job must start.

     A repeatedly run job is started by the following rules:

     - The defined interval always starts at 12:00 AM. For example, if you configure to run a job with a 4-hour interval, the job will start at 12:00 AM, 4:00 AM, 8:00 AM, 12:00 PM, 4:00 PM and so on.
     - If you define permitted hours for the job, after the denied interval is over, the job will start immediately and then run by the defined schedule.

     For example, you have configured a job to run with a 2-hour interval and defined permitted hours from 9:00 AM to 5:00 PM. According to the rules above, the job will first run at 9:00 AM, when the denied period is over. After that, the job will run at 10:00 AM, 12:00 PM, 2:00 PM and 4:00 PM.
   - To run the job continuously, select the **Periodically every** option and choose **Continuously** from the list on the right. A new backup job session will start as soon as the previous backup job session finishes.
   - [For backup job managed by backup server] To chain jobs, use the **After this job** field. In the common practice, jobs start one after another: when job A finishes, job B starts and so on. If you want to create a chain of jobs, you must define the time schedule for the first job in the chain. For the rest of the jobs in the chain, select the **After this job** option and choose the preceding job from the list.

> NOTE
>
> Mind the following:
>
> - The **After this job** option is not available if you have selected the **Managed by agent** option at the **Job Mode** step of the wizard.
> - The **After this job** function will automatically start a job if the first job in the chain is started automatically by schedule. If you start the first job manually, Veeam Backup & Replication will display a notification. You will be able to choose whether Veeam Backup & Replication must start the chained job as well.

3. In the **Automatic retry** section, define whether Veeam Backup & Replication or Veeam Plug-in (depending on the selected job mode) must attempt to run the backup job again if the job fails for some reason. Enter the number of attempts to run the job and define time intervals between them. If you select continuous backup, Veeam Backup & Replication or Veeam Plug-in will retry the job for the defined number of times without any time intervals between the job runs.

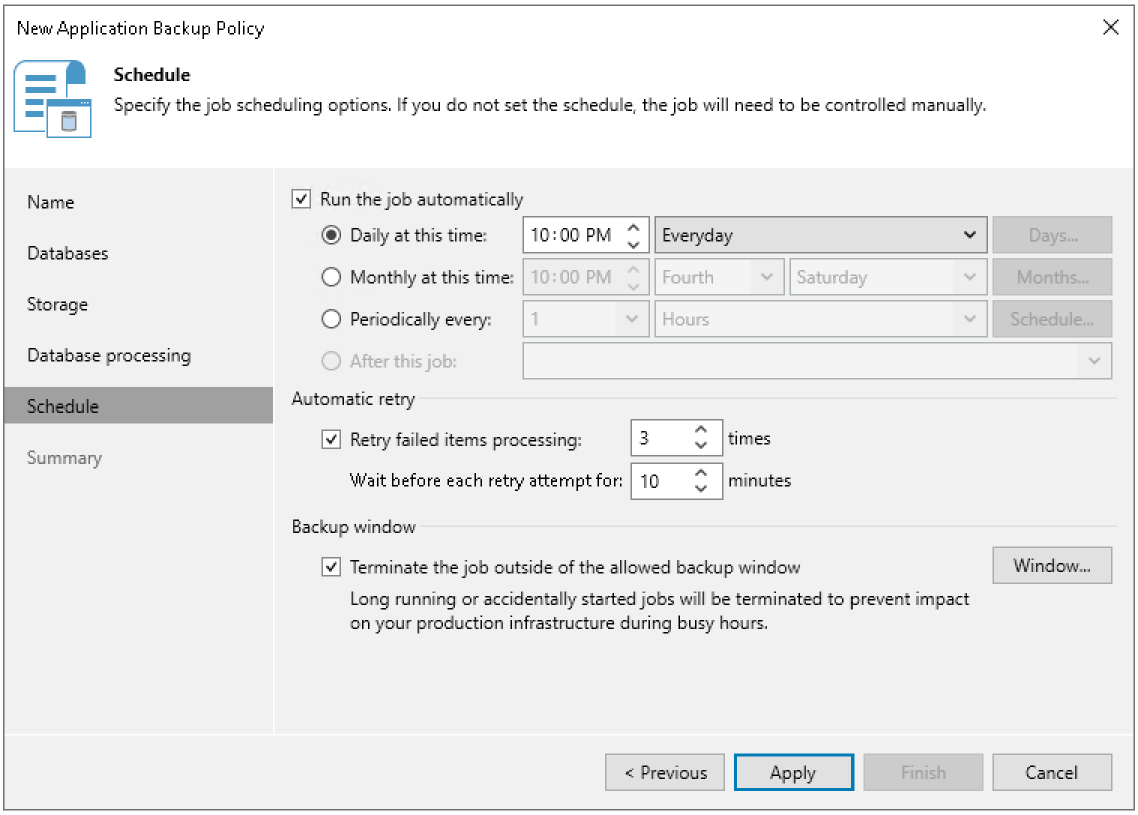
4. [For backup job managed by backup server] In the **Backup window** section, define the time interval within which the backup job must complete. The backup window prevents the job from overlapping with production hours and ensures that the job does not impact performance of your server. To set up a backup window for the job:

   a. Select the **Terminate job if it exceeds allowed backup window** check box and click **Window**.

   b. In the **Time Periods** window, define the allowed hours and prohibited hours for backup. If the job exceeds the allowed window, it will be automatically terminated.

NOTE

If you configure a backup policy, after you click **Apply** at the **Schedule** step of the wizard, Veeam Backup & Replication will immediately apply the backup policy to protected computers.


New Application Backup Policy

Schedule

Specify the job scheduling options. If you do not set the schedule, the job will need to be controlled manually.

☑ Run the job automatically

● Daily at this time: 10:00 PM, Everyday

○ Monthly at this time: 10:00 PM, Fourth, Saturday

○ Periodically every: 1 Hours

○ After this job:

Automatic retry

☑ Retry failed items processing: 3 times

Wait before each retry attempt for: 10 minutes

Backup window

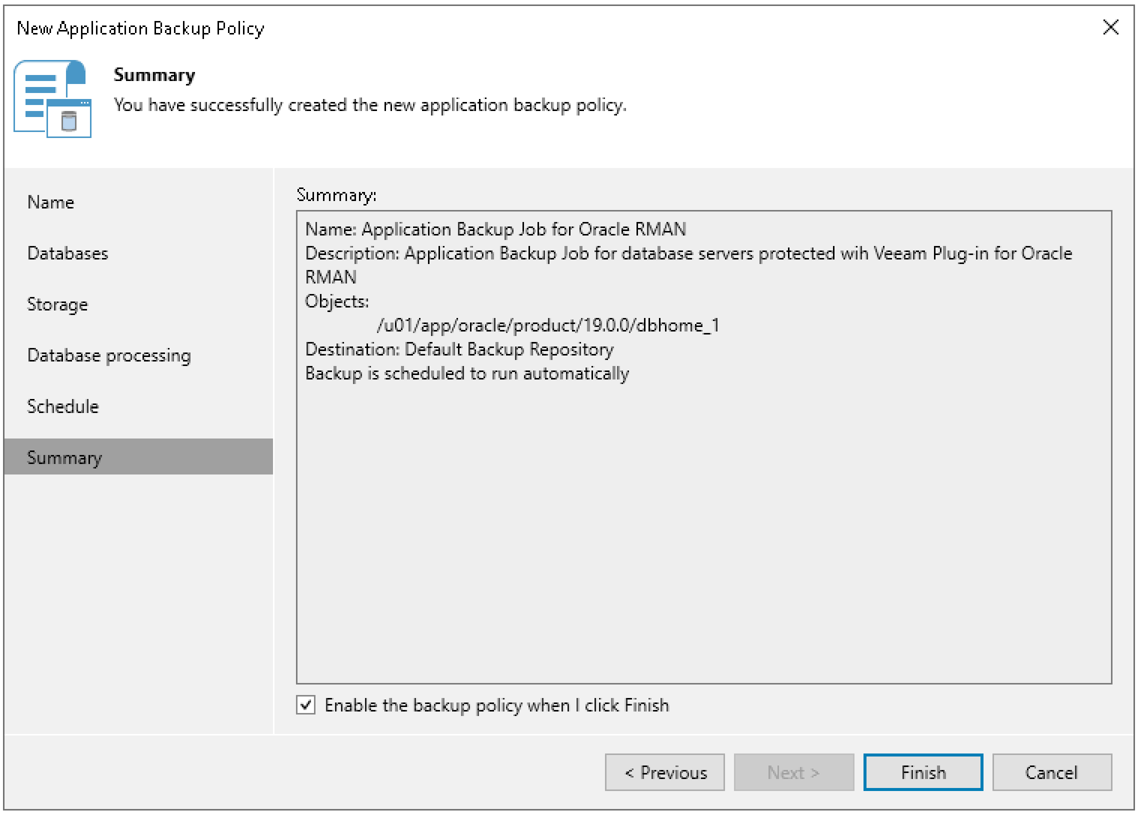
☑ Terminate the job outside of the allowed backup window

Long running or accidentally started jobs will be terminated to prevent impact on your production infrastructure during busy hours.

Step 8. Review Policy Settings

At the **Summary** step of the wizard, complete the configuration process for the application backup policy.

1. Review settings of the configured backup policy.
2. Select the **Run the job when I click Finish** check box if you want to start the policy right after you finish working with the wizard.
3. Click **Finish** to close the wizard.



New Application Backup Policy

Summary

You have successfully created the new application backup policy.

Summary:

```
Name: Application Backup Job for Oracle RMAN
Description: Application Backup Job for database servers protected wih Veeam Plug-in for Oracle
RMAN
Objects:
        /u01/app/oracle/product/19.0.0/dbhome_1
Destination: Default Backup Repository
Backup is scheduled to run automatically
```

☑ Enable the backup policy when I click Finish

Creating SAP HANA Backup Policy

To back up databases protected with Veeam Plug-in for SAP HANA, you must configure an application backup policy in Veeam Backup & Replication.

Before You Begin

Before you create an application backup policy in the Veeam Backup & Replication console, check the following prerequisites:

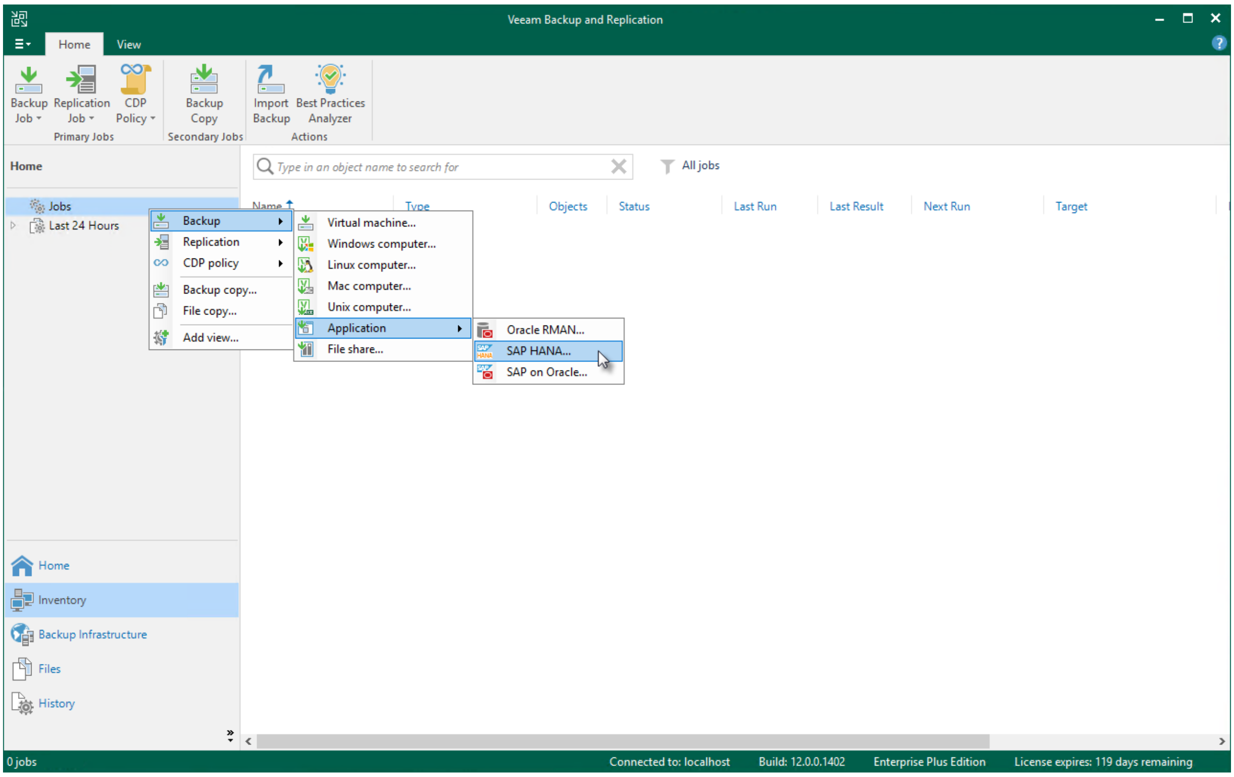
- The Veeam Backup & Replication license must have a sufficient number of instances to process computers that you plan to add to the application backup policy.
- The target location where you plan to store backup files must have enough free space.
- Protection groups that you want to add to the policy must be configured in advance.

Application backup policies have the following limitations:

- One backup object (computer, database system, or database) can be added only to one application backup policy. Otherwise, the application backup policy will fail.
- You can create application backups on a Veeam backup repository. If you want to save backups in other target locations, you must configure backup job on the computer side.
- After you start managing a Veeam Plug-in with Veeam Backup & Replication, data backup for the computer is performed by a backup policy configured in Veeam Backup & Replication. Veeam Plug-in running on the computer starts a new backup chain on a target location specified in the backup policy settings. You cannot continue the existing backup chain that was created by Veeam Plug-in operating in the standalone mode.

Step 1. Launch New Backup Job Wizard

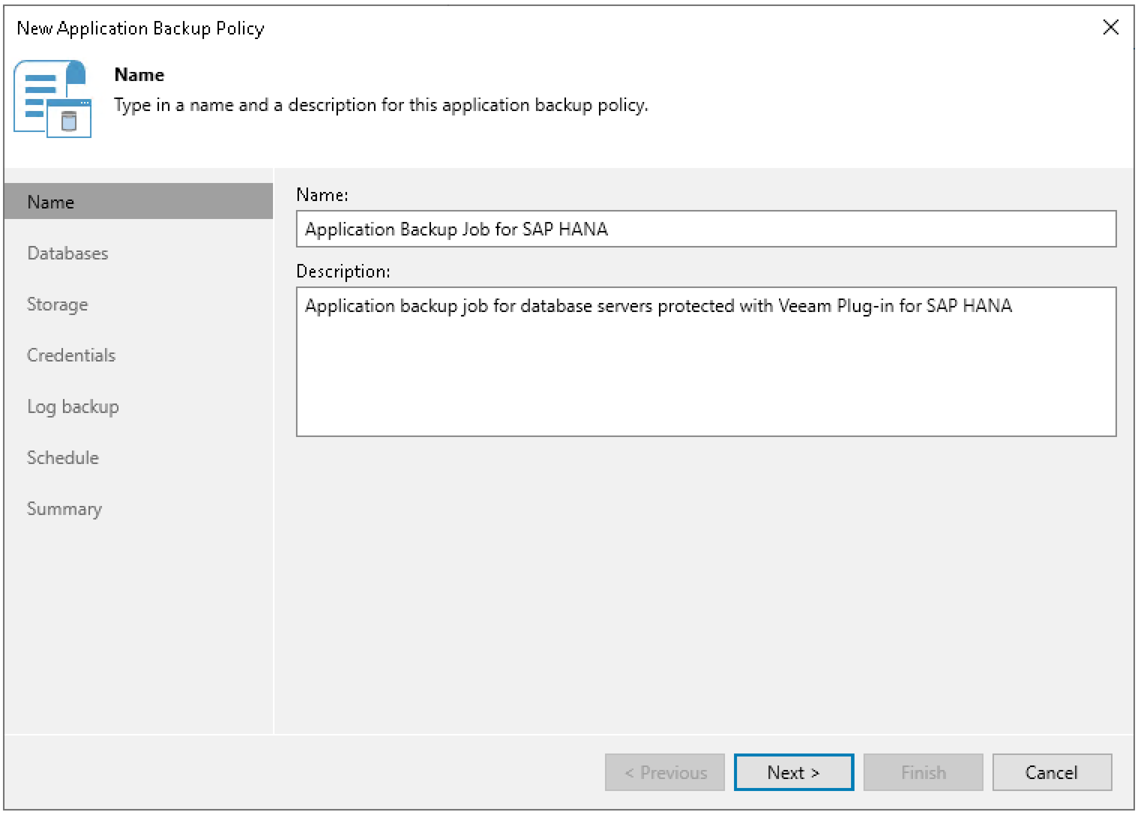
To create an application policy for Veeam Plug-in for SAP HANA, you must launch the **New Application Backup Policy** wizard. To do this, on the **Home** tab, click **Backup Job** > **Application** > **SAP HANA**.



Step 2. Specify Policy Name

At the **Name** step of the wizard, specify a name and description for the application backup policy.

1. In the **Name** field, enter a name for the application backup policy.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who created the job, date and time when the job was created.



New Application Backup Policy

Name

Type in a name and a description for this application backup policy.

Name:

Application Backup Job for SAP HANA

Description:

Application backup job for database servers protected with Veeam Plug-in for SAP HANA

Step 3. Specify Databases

At the **Databases** step of the wizard, select protection groups, computers, database systems or individual databases whose data you want to back up.

You can add to the backup scope one or more objects added to inventory in the Veeam Backup & Replication console.

Application policies with protection groups are dynamic in their nature. If Veeam Backup & Replication discovers a new computer in a protection group after the policy is created, Veeam Backup & Replication will automatically update the policy settings to include the added computer.

Adding Objects from Inventory

To add protection groups, individual computers or databases to the application backup policy:

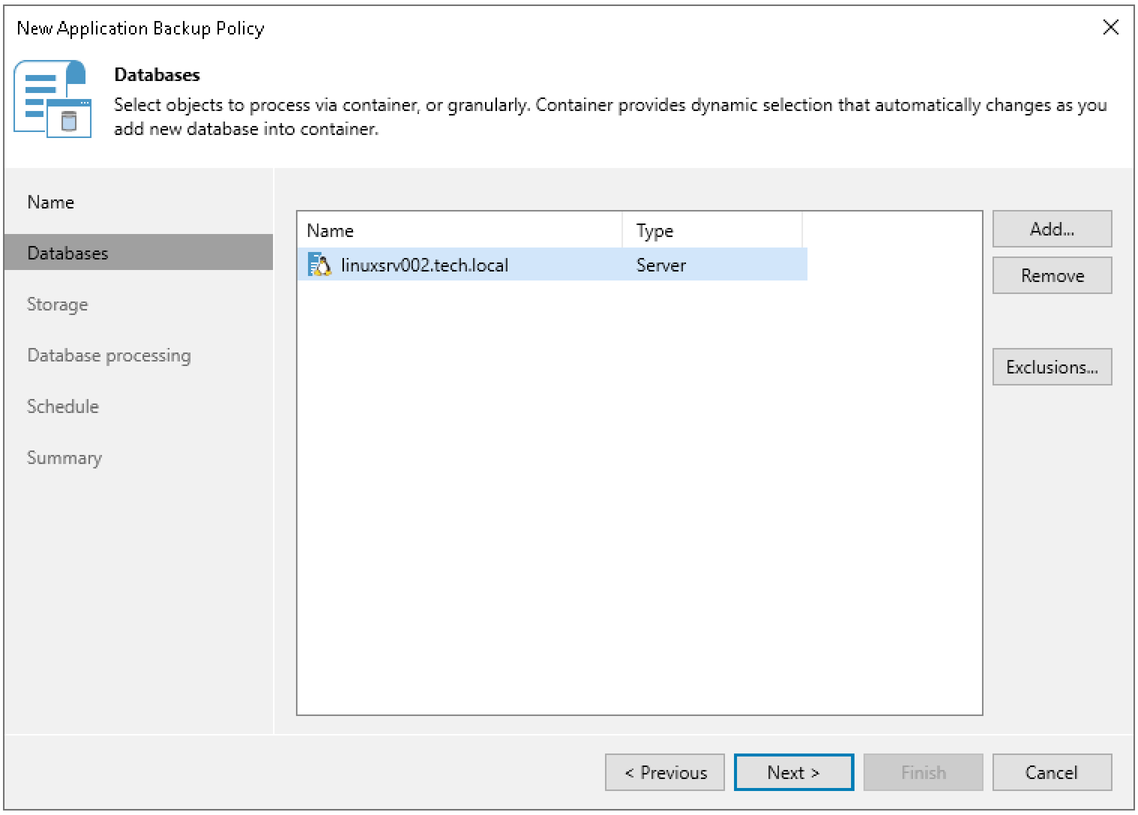
1. Click **Add**.
2. In the **Select Objects** window, select one or more objects in the list and click **OK**. You can select any of the following objects:
   - Protection group
   - Computer
   - SAP system
   - SAP database

   You can press and hold **[CTRL]** to select multiple objects at once.

> **NOTE**
>
> In the **Select Objects** window, Veeam Backup & Replication shows only those computers on which Veeam Backup & Replication have detected SAP systems during the rescan job. To learn more, see Rescan Job.

To quickly find the necessary object, use the search field at the bottom of the **Select Objects** window.

1. Enter the object name or a part of it in the search field.
2. Click the **Start search** button on the right or press **[ENTER]**.



New Application Backup Policy

Databases

Select objects to process via container, or granularly. Container provides dynamic selection that automatically changes as you add new database into container.

Name	Type
linuxsrv002.tech.local	Server

Excluding Objects

You can exclude protection groups, individual computers or databases from the backup scope of the application backup policy. This may be useful if you want to back up a certain database with another application backup policy.

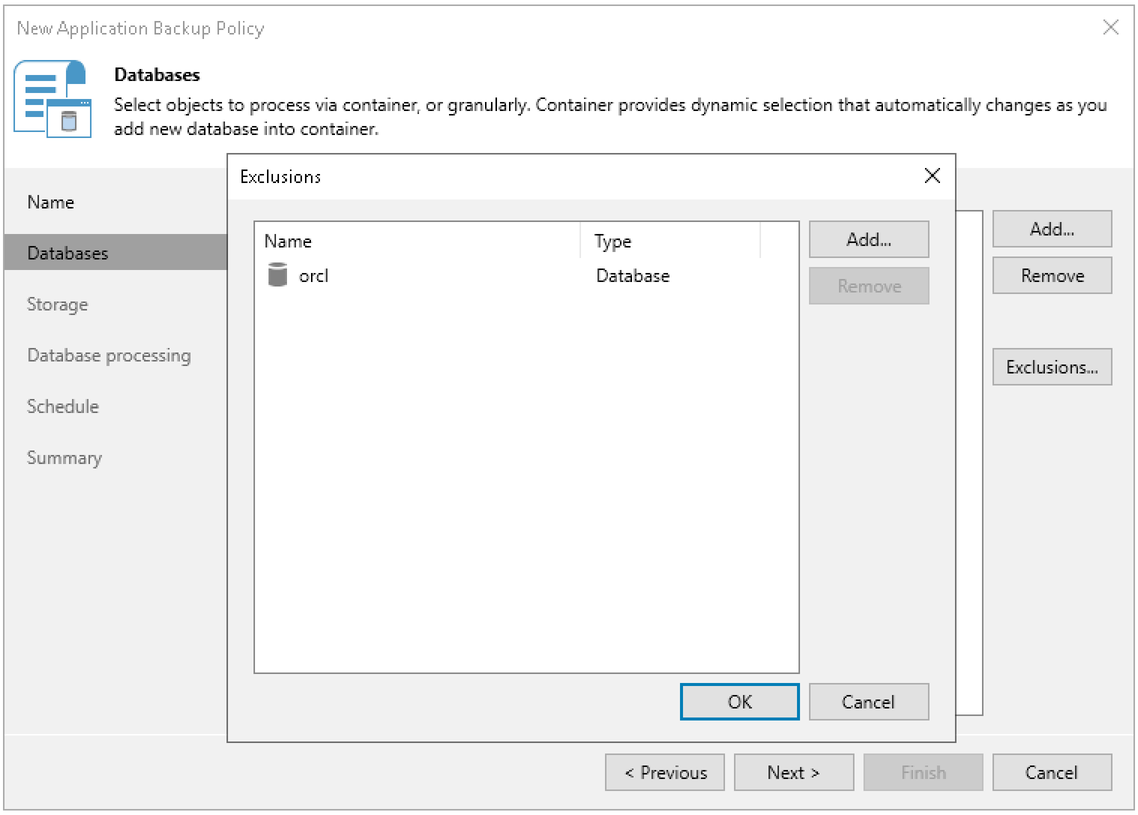
To exclude protection groups, individual computers or databases from the backup scope:

3. Click **Exclusions**.
4. In the **In the Exclusions** window, select one or more objects in the list and click **OK**. You can select any of the following objects:
   - Protection group
   - Computer
   - SAP system
   - SAP database

   You can press and hold **[CTRL]** to select multiple objects at once.

NOTE

In the **Exclusions** window, Veeam Backup & Replication shows only those objects which were already added to the backup scope. To learn more, see Adding Objects from Inventory.



Select objects to process via container, or granularly. Container provides dynamic selection that automatically changes as you add new database into container.

Name	Type
orcl	Database

Step 4. Specify Storage Settings

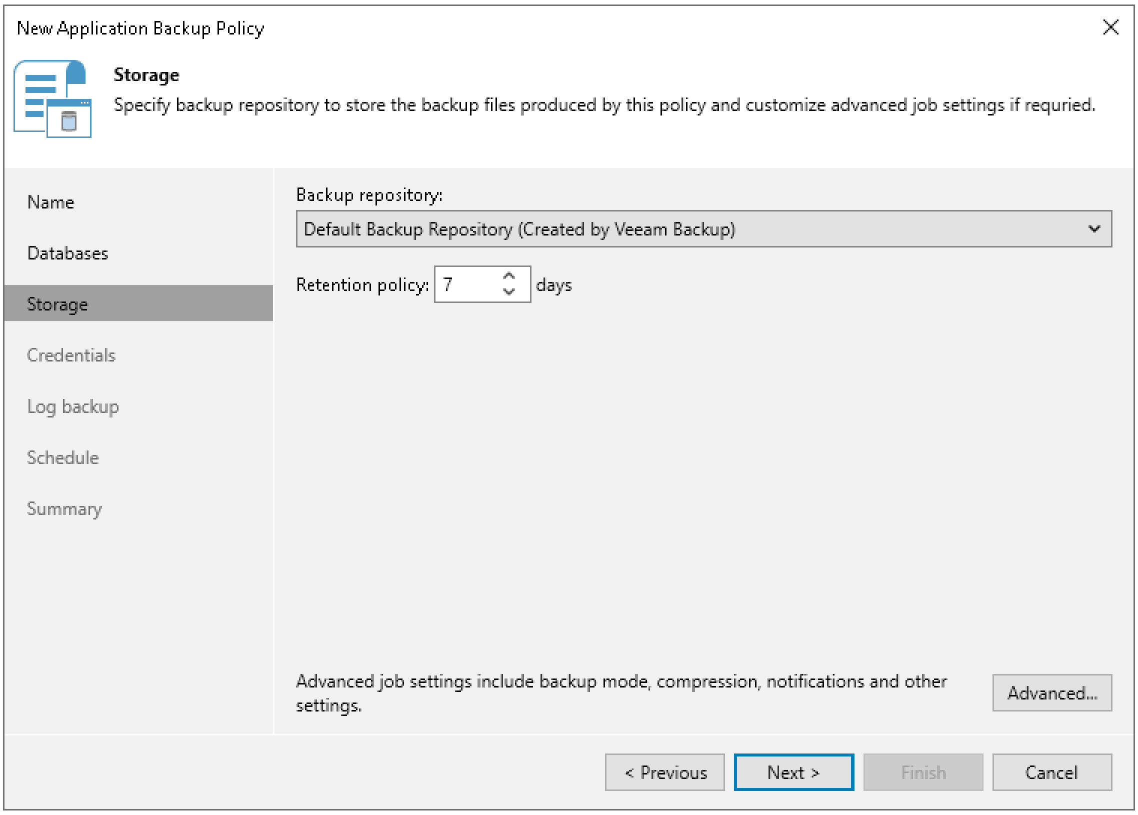
At the **Storage** step of the wizard, specify settings for the target backup repository:

1. From the **Backup repository** list, select a backup repository where you want to store backups. You can select from the Veeam backup repositories configured on the backup server that will manage the created backup policy.

   When you select a backup repository, Veeam Backup & Replication automatically checks how much free space is available on the backup repository.

2. In the **Retention Policy** field, specify the number of days for which you want to store backup files in the target location. By default, Veeam Backup & Replication keeps backup files for 7 days. After this period is over, Veeam Backup & Replication will remove the earliest restore points from the backup chain.

3. Click **Advanced** to specify advanced settings for the backup job. To learn more, see Specify Advanced Backup Settings.


New Application Backup Policy

Storage

Specify backup repository to store the backup files produced by this policy and customize advanced job settings if requried.

Backup repository: Default Backup Repository (Created by Veeam Backup)

Retention policy: 7 days

Advanced job settings include backup mode, compression, notifications and other settings.

Step 5. Specify Advanced Backup Settings

In the **Advanced Settings** window, specify advanced settings for the application backup policy:

- Backup settings
- Notification settings
- SAP HANA settings

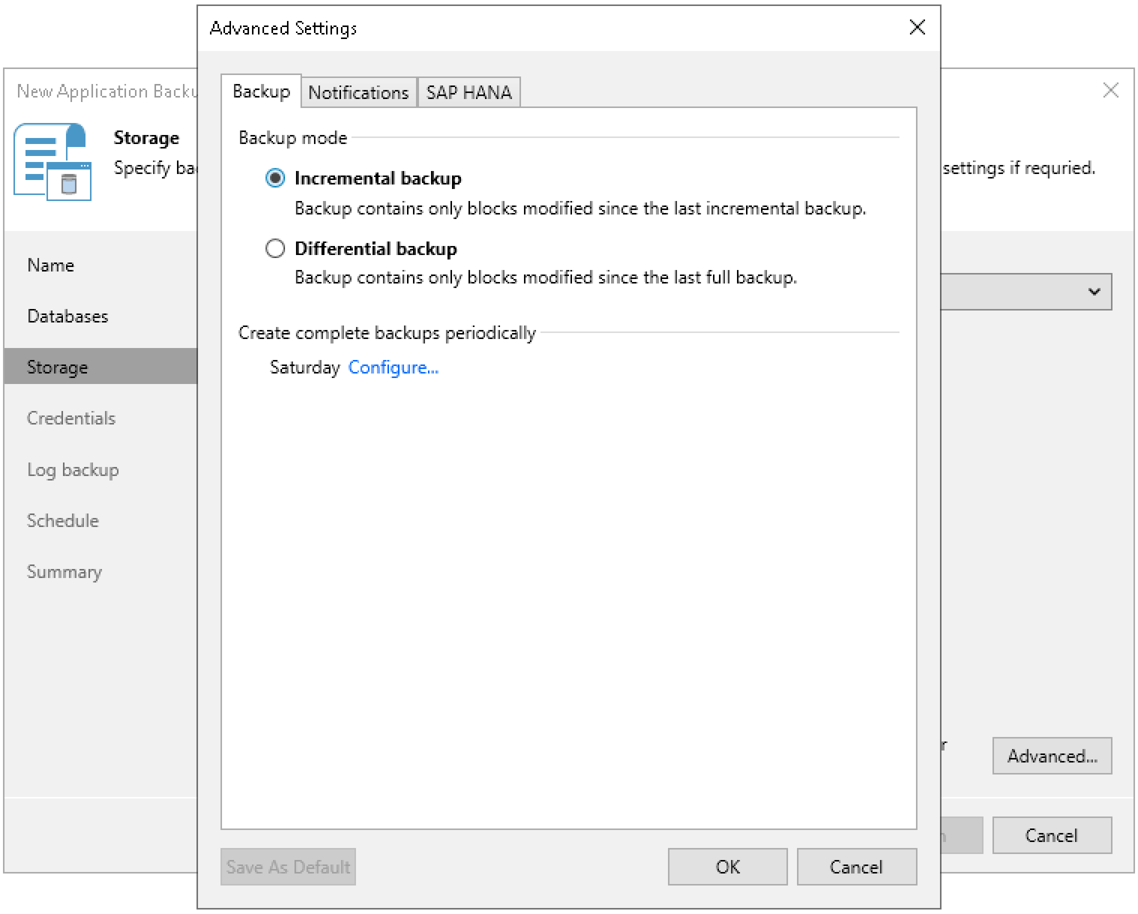
> **TIP**
>
> After you specify necessary settings for the application backup policy, you can save them as default settings. To do this, click **Save as Default** at the bottom left corner of the **Advanced Settings** window. When you create a new backup policy, Veeam Backup & Replication will automatically apply the default settings to the new policy.

Backup Settings

To specify settings for a backup chain created with the backup policy:

1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Backup** tab.
3. In the **Backup mode**, select one of the following modes for incremental backups:
   - Incremental backup. In this mode, Veeam Backup & Replication will create a backup of data changed since the last incremental data backup.
   - Differential backup. In this mode, Veeam Backup & Replication will create a backup of data changed since the last full data backup.

4. To define the schedule for complete backups, click **Configure** and define the schedule in the **Schedule Settings** window:
   - To run the complete backup once a month on specific days, select **Monthly on**. Use the fields on the right to configure the necessary schedule.
   - To run the complete backup once a week on specific week days, select **Weekly**. Use the fields on the right to select the necessary week days.



Advanced Settings

Backup mode

● **Incremental backup**
Backup contains only blocks modified since the last incremental backup.

○ **Differential backup**
Backup contains only blocks modified since the last full backup.

Create complete backups periodically
Saturday Configure...

Notification Settings

To specify notification settings for the backup policy:

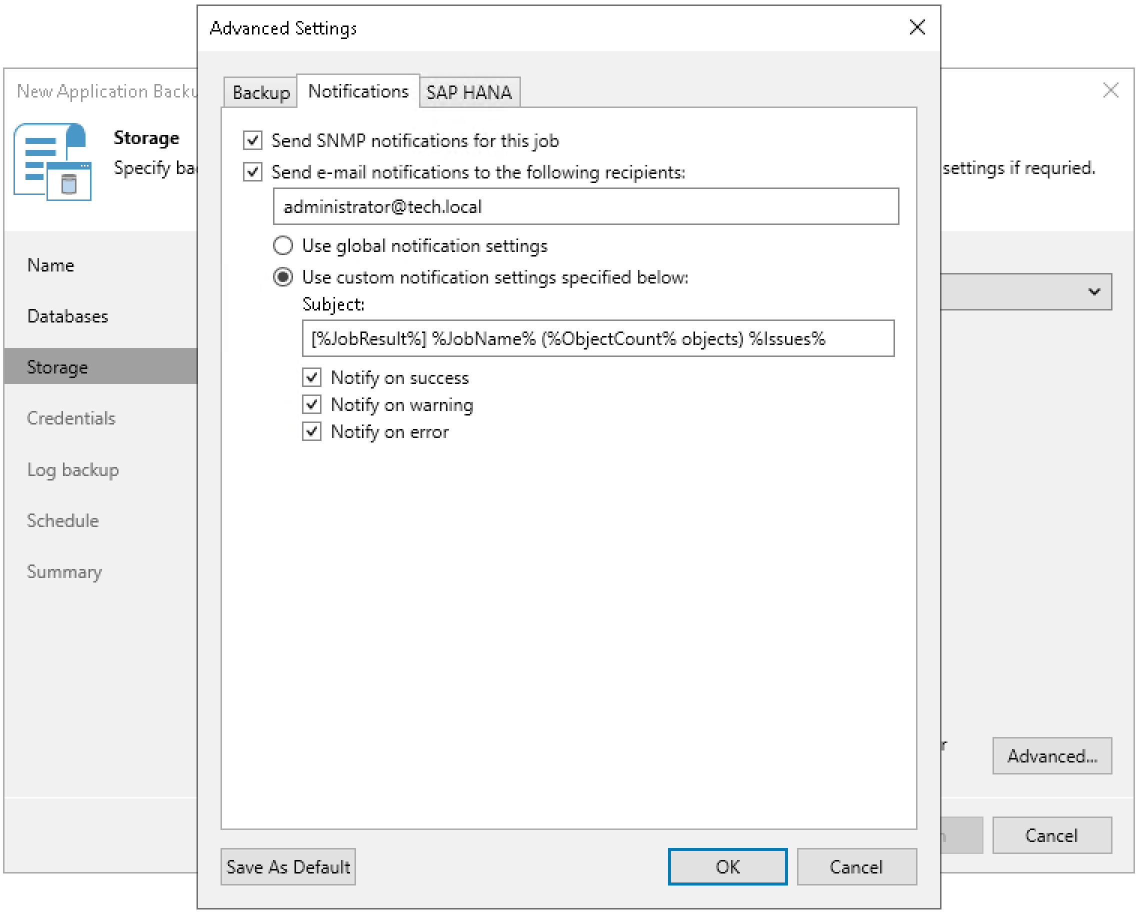
1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Notifications** tab.
3. Select the **Send SNMP notifications for this job** check box if you want to receive SNMP traps when the policy completes successfully.

   SNMP traps will be sent if you specify global SNMP settings in Veeam Backup & Replication and configure software on recipient's machine to receive SNMP traps. For more information, see the Specifying SNMP Settings section in the Veeam Backup & Replication User Guide.
4. Select the **Send email notifications to the following recipients** check box if you want to receive notifications about the policy completion status by email. In the field below, specify a recipient's email address. You can enter several addresses separated by a semicolon.

   Email notifications will be sent if you configure global email notification settings in Veeam Backup & Replication. For more information, see the Configuring Global Email Notification Settings section in Veeam Backup & Replication User Guide.

5. You can choose to use global notification settings or specify custom notification settings.

   - To receive a typical notification for the policy, select **Use global notification settings**. In this case, Veeam Backup & Replication will apply to the policy global email notification settings specified for the backup server.
   - To configure a custom notification for the policy, select **Use custom notification settings specified below**. You can specify the following notification settings:
     - In the **Subject** field, specify a notification subject. You can use the following variables in the subject: *%Time%* (completion time), *%JobName%*, *%JobResult%*, *%ObjectCount%* (number of computers in the policy) and *%Issues%* (number of computers in the policy that have been processed with the *Warning* or *Failed* status).
     - Select the **Notify on success**, **Notify on warning** and/or **Notify on error** check boxes to receive email notification if the policy completes successfully, completes with a warning or fails.
     - Select the **Suppress notifications until the last retry** check box to receive a notification about the final policy status. If you do not enable this option, Veeam Backup & Replication will send one notification per every retry.



Advanced Settings

☑ Send SNMP notifications for this job

☑ Send e-mail notifications to the following recipients:

administrator@tech.local

○ Use global notification settings

● Use custom notification settings specified below:

Subject:

[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

☑ Notify on success

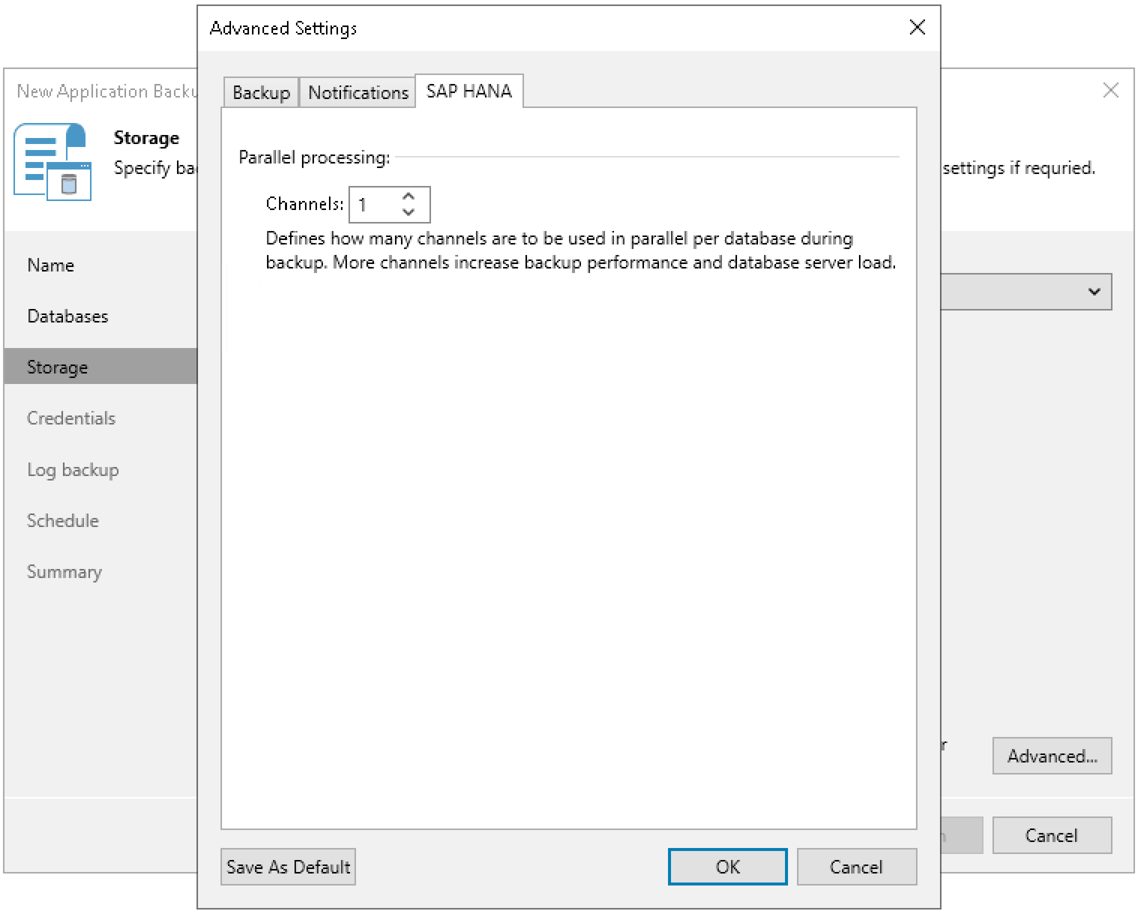
☑ Notify on warning

☑ Notify on error

SAP HANA Settings

To specify Oracle settings for the backup policy:

1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **SAP HANA** tab.
3. In the **Channels** field, specify the number of data channels that Veeam Plug-in will use in parallel to back up databases.



Parallel processing:

Channels: 1

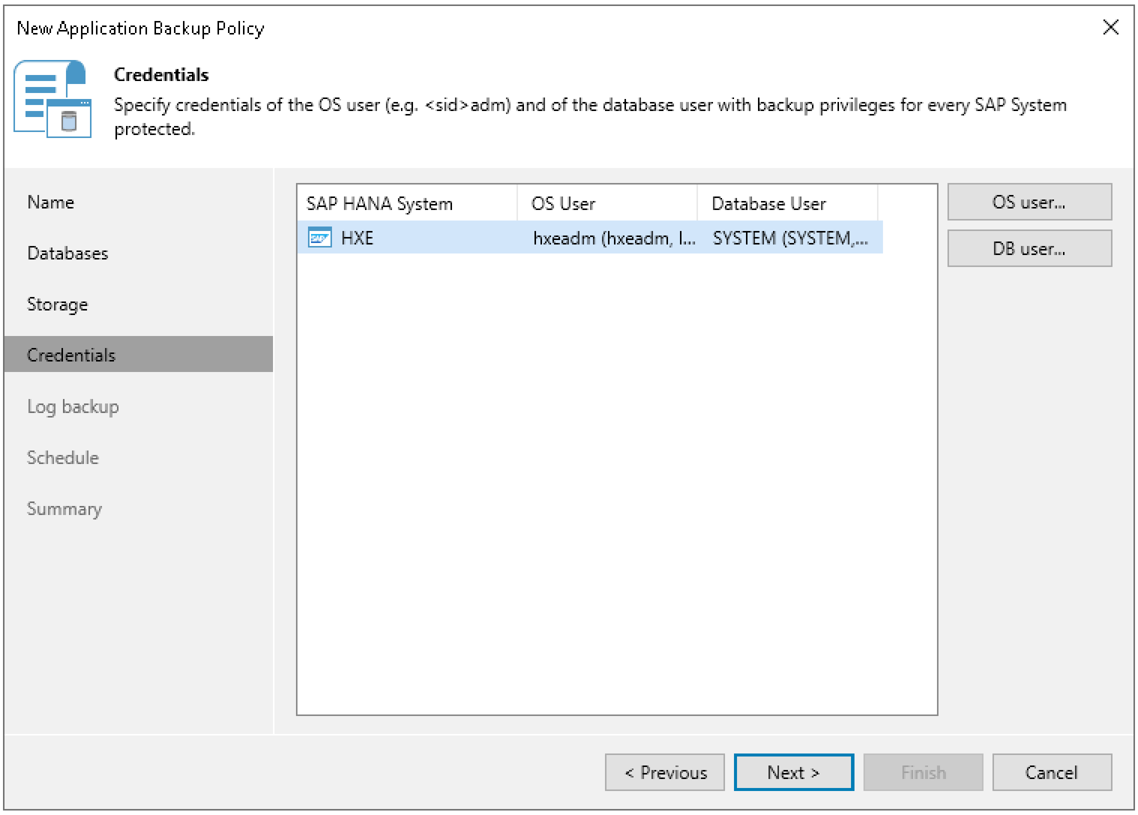
Defines how many channels are to be used in parallel per database during backup. More channels increase backup performance and database server load.

Step 6. Specify Credentials

At the **Credentials** step of the wizard, specify credentials that Veeam Plug-in will use to connect to the database:

1. To specify credentials for the OS user, select the database and click **OS user**. In the **OS user credentials** window, select credentials in the list. If you have not set up credentials beforehand, click **Add** on the right to add credentials.

2. To specify credentials for the database user, select the database and click **Database user**. In the **Database user credentials** window, select credentials in the list. If you have not set up credentials beforehand, click **Add** on the right to add credentials.



New Application Backup Policy

Credentials

Specify credentials of the OS user (e.g. <sid>adm) and of the database user with backup privileges for every SAP System protected.

SAP HANA System	OS User	Database User
HXE	hxeadm (hxeadm, l...	SYSTEM (SYSTEM,...

Step 7. Specify Log Backup Settings

At the **Log Backup** step of the wizard, specify database credentials and log processing settings:

1. In the **Credentials** list, select the object and click **Edit**.
2. Specify database credentials and log processing settings for the objects in the list. To learn more, see Processing settings

In the **Credentials** list, Veeam Backup & Replication shows only those objects that you added to the backup scope at the **Databases** step of the wizard. If you added a protection group, but need to specify settings for an individual computer or database in this protection group, you can add such objects to the list. To learn more, see Adding Objects from Backup Scope.

Adding Objects from Backup Scope

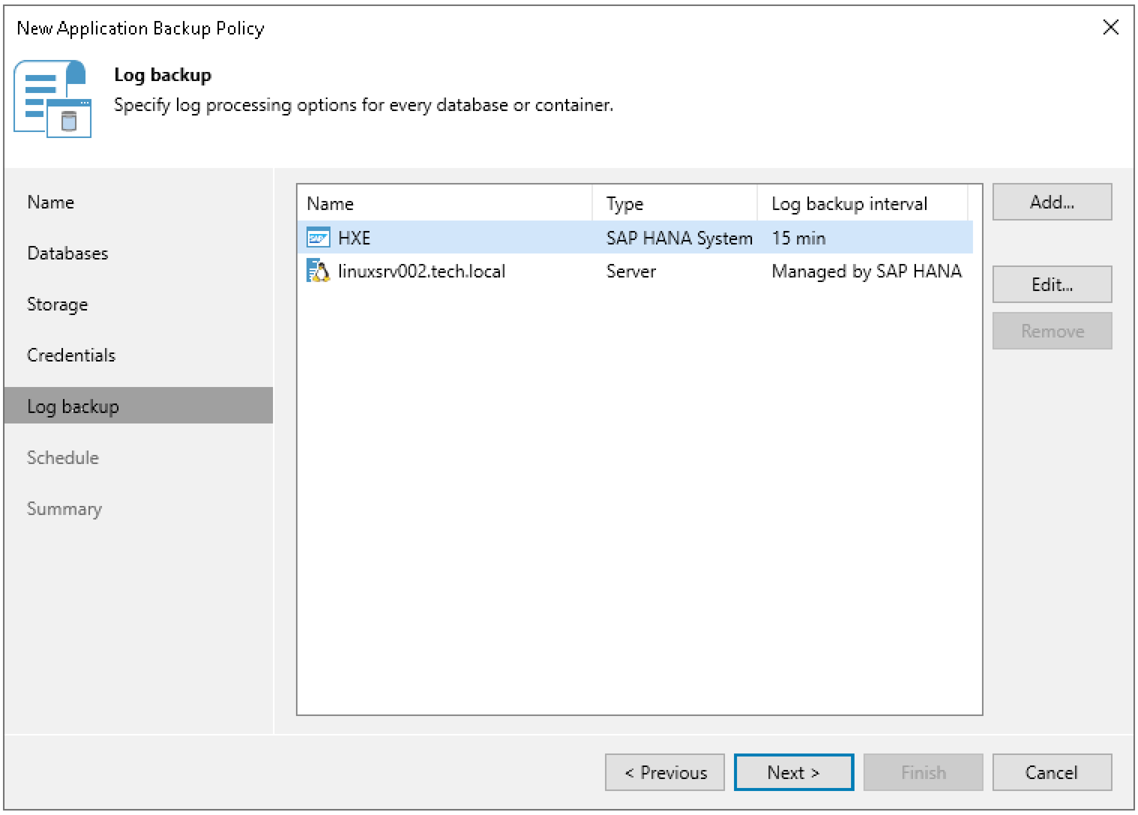
To add protection groups, individual computers or databases to the **Credentials** list:

1. Click **Add**.
2. In the **Select Objects** window, select one or more objects in the list and click **OK**. You can select any of the following objects:
    - Protection group
    - Computer
    - Oracle home
    - Oracle database

   You can press and hold **[CTRL]** to select multiple objects at once.

To quickly find the necessary object, use the search field at the bottom of the **Select Objects** window.

1. Enter the object name or a part of it in the search field.
2. Click the **Start search** button on the right or press **[ENTER]**.



New Application Backup Policy

Log backup

Specify log processing options for every database or container.

Name	Type	Log backup interval
HXE	SAP HANA System	15 min
linuxsrv002.tech.local	Server	Managed by SAP HANA

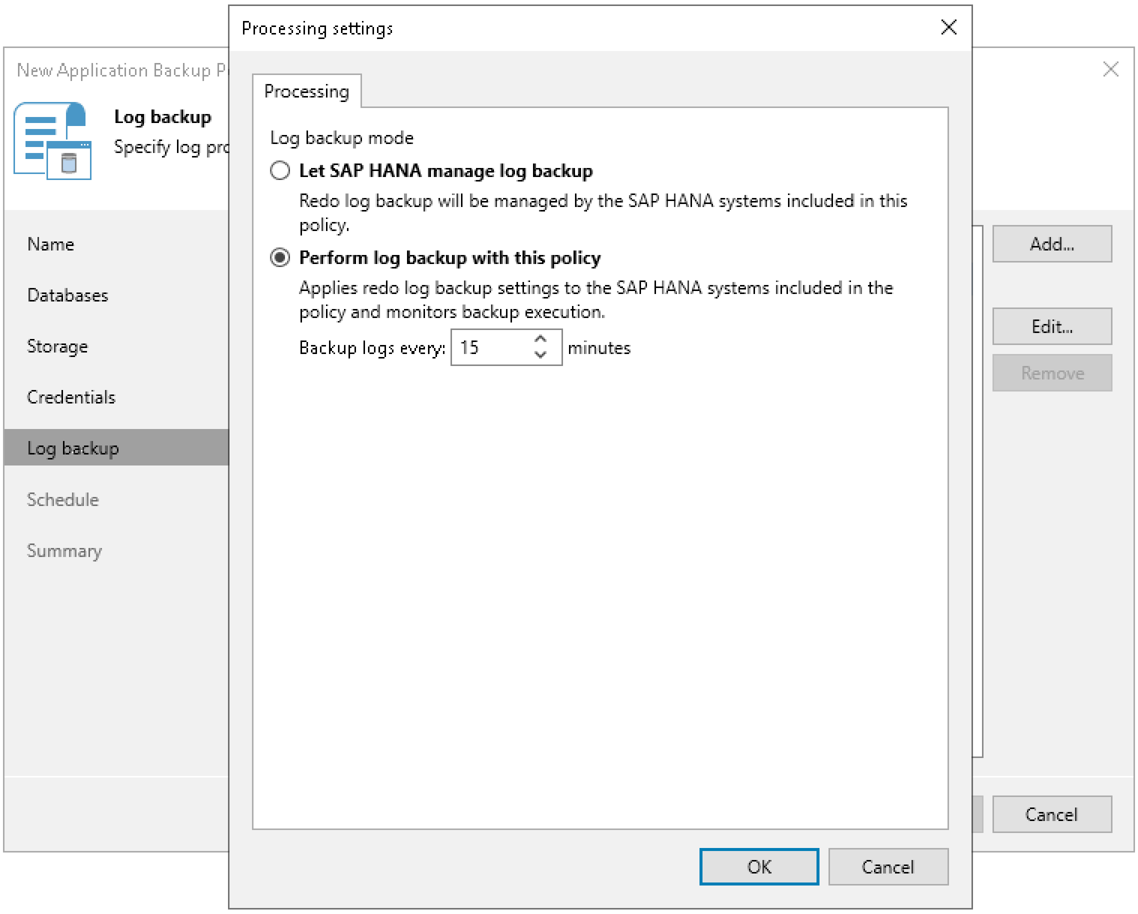
Processing Settings

To specify processing settings for the object:

1. At the **Log Backup** step of the wizard, select the object and click **Edit**.
2. In the **Processing** tab, select the way you want to back up logs:
   - Select **Let SAP HANA manage log backup** if you want to back up logs with SAP HANA tools.

     In this case Veeam Plug-in will not back up logs.
   - Select **Perform log backup with this policy** if you want to back up logs with Veeam Plug-in.

     In the **Backup logs every <N> minutes** field, specify the frequency for logs backup. By default, archived logs are backed up every 15 minutes. The minimum log backup interval is 5 minutes. The maximum log backup interval is 480 minutes.



Log backup mode

○ **Let SAP HANA manage log backup**

Redo log backup will be managed by the SAP HANA systems included in this policy.

● **Perform log backup with this policy**

Applies redo log backup settings to the SAP HANA systems included in the policy and monitors backup execution.

Backup logs every: 15 minutes

Step 8. Specify Policy Schedule

At the **Schedule** step of the wizard, specify the schedule according to which you want to perform backup.

To specify the job schedule:

1. Select the **Run the job automatically** check box. If this check box is not selected, you will have to start the backup job manually to create backup.

2. Define scheduling settings for the job:

    - To run the job at specific time daily, on defined week days or with specific periodicity, select **Daily at this time**. Use the fields on the right to configure the necessary schedule.

    - To run the job once a month on specific days, select **Monthly at this time**. Use the fields on the right to configure the necessary schedule.

- To run the job repeatedly throughout a day with a specific time interval, select **Periodically every**. In the field on the right, select the necessary time unit: *Hours* or *Minutes*.

    - [For backup job managed by backup server] To define the permitted time window for the job, click **Schedule** and use the time table. In the **Start time within an hour** field, specify the exact time when the job must start.

      A repeatedly run job is started by the following rules:

        - The defined interval always starts at 12:00 AM. For example, if you configure to run a job with a 4-hour interval, the job will start at 12:00 AM, 4:00 AM, 8:00 AM, 12:00 PM, 4:00 PM and so on.

        - If you define permitted hours for the job, after the denied interval is over, the job will start immediately and then run by the defined schedule.

      For example, you have configured a job to run with a 2-hour interval and defined permitted hours from 9:00 AM to 5:00 PM. According to the rules above, the job will first run at 9:00 AM, when the denied period is over. After that, the job will run at 10:00 AM, 12:00 PM, 2:00 PM and 4:00 PM.

    - To run the job continuously, select the **Periodically every** option and choose **Continuously** from the list on the right. A new backup job session will start as soon as the previous backup job session finishes.

    - [For backup job managed by backup server] To chain jobs, use the **After this job** field. In the common practice, jobs start one after another: when job A finishes, job B starts and so on. If you want to create a chain of jobs, you must define the time schedule for the first job in the chain. For the rest of the jobs in the chain, select the **After this job** option and choose the preceding job from the list.

> NOTE
>
> Mind the following:
>
> - The **After this job** option is not available if you have selected the **Managed by agent** option at the **Job Mode** step of the wizard.
> - The **After this job** function will automatically start a job if the first job in the chain is started automatically by schedule. If you start the first job manually, Veeam Backup & Replication will display a notification. You will be able to choose whether Veeam Backup & Replication must start the chained job as well.

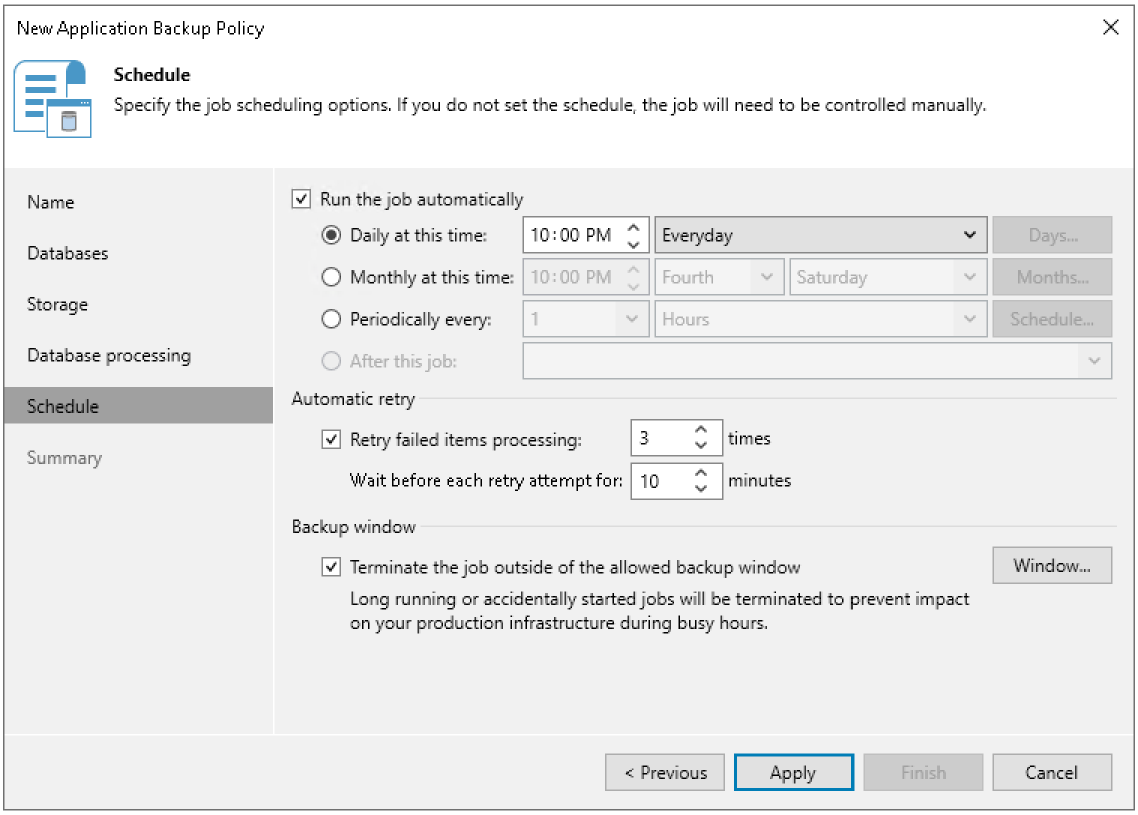
3. In the **Automatic retry** section, define whether Veeam Backup & Replication or Veeam Plug-in (depending on the selected job mode) must attempt to run the backup job again if the job fails for some reason. Enter the number of attempts to run the job and define time intervals between them. If you select continuous backup, Veeam Backup & Replication or Veeam Plug-in will retry the job for the defined number of times without any time intervals between the job runs.

4. [For backup job managed by backup server] In the **Backup window** section, define the time interval within which the backup job must complete. The backup window prevents the job from overlapping with production hours and ensures that the job does not impact performance of your server. To set up a backup window for the job:

   a. Select the **Terminate job if it exceeds allowed backup window** check box and click **Window**.

   b. In the **Time Periods** window, define the allowed hours and prohibited hours for backup. If the job exceeds the allowed window, it will be automatically terminated.

> NOTE
>
> If you configure a backup policy, after you click **Apply** at the **Schedule** step of the wizard, Veeam Backup & Replication will immediately apply the backup policy to protected computers.



New Application Backup Policy

Schedule

Specify the job scheduling options. If you do not set the schedule, the job will need to be controlled manually.

☑ Run the job automatically

● Daily at this time: 10:00 PM Everyday

○ Monthly at this time: 10:00 PM Fourth Saturday

○ Periodically every: 1 Hours

○ After this job:

Automatic retry

☑ Retry failed items processing: 3 times

Wait before each retry attempt for: 10 minutes

Backup window

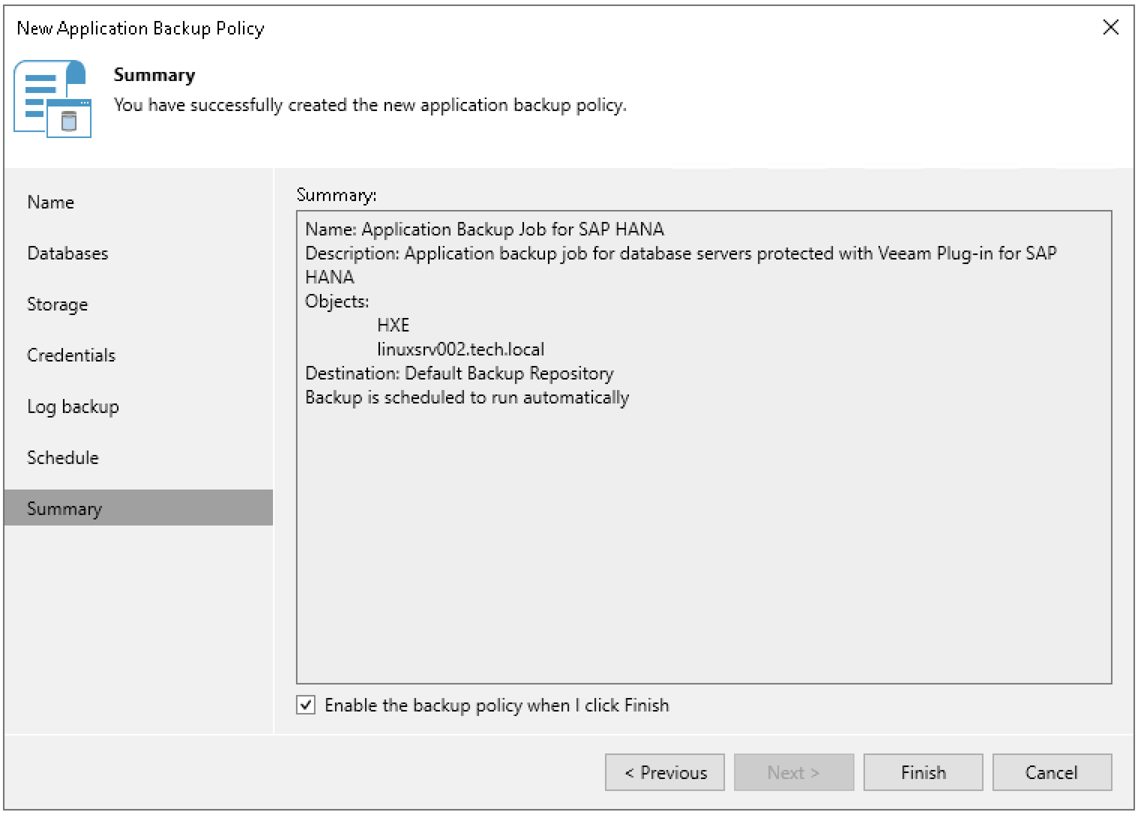
☑ Terminate the job outside of the allowed backup window

Long running or accidentally started jobs will be terminated to prevent impact on your production infrastructure during busy hours.

Step 9. Review Policy Settings

At the **Summary** step of the wizard, complete the configuration process for the application backup policy.

1. Review settings of the configured backup policy.
2. Select the **Run the job when I click Finish** check box if you want to start the policy right after you finish working with the wizard.
3. Click **Finish** to close the wizard.



Summary

You have successfully created the new application backup policy.

Summary:

Name: Application Backup Job for SAP HANA
Description: Application backup job for database servers protected with Veeam Plug-in for SAP HANA
Objects:
HXE
linuxsrv002.tech.local
Destination: Default Backup Repository
Backup is scheduled to run automatically

☑ Enable the backup policy when I click Finish

Creating SAP on Oracle Backup Policy

To back up databases protected with Veeam Plug-in for SAP on Oracle, you must configure an application backup policy in Veeam Backup & Replication.

Before You Begin

Before you create an application backup policy in the Veeam Backup & Replication console, check the following prerequisites:

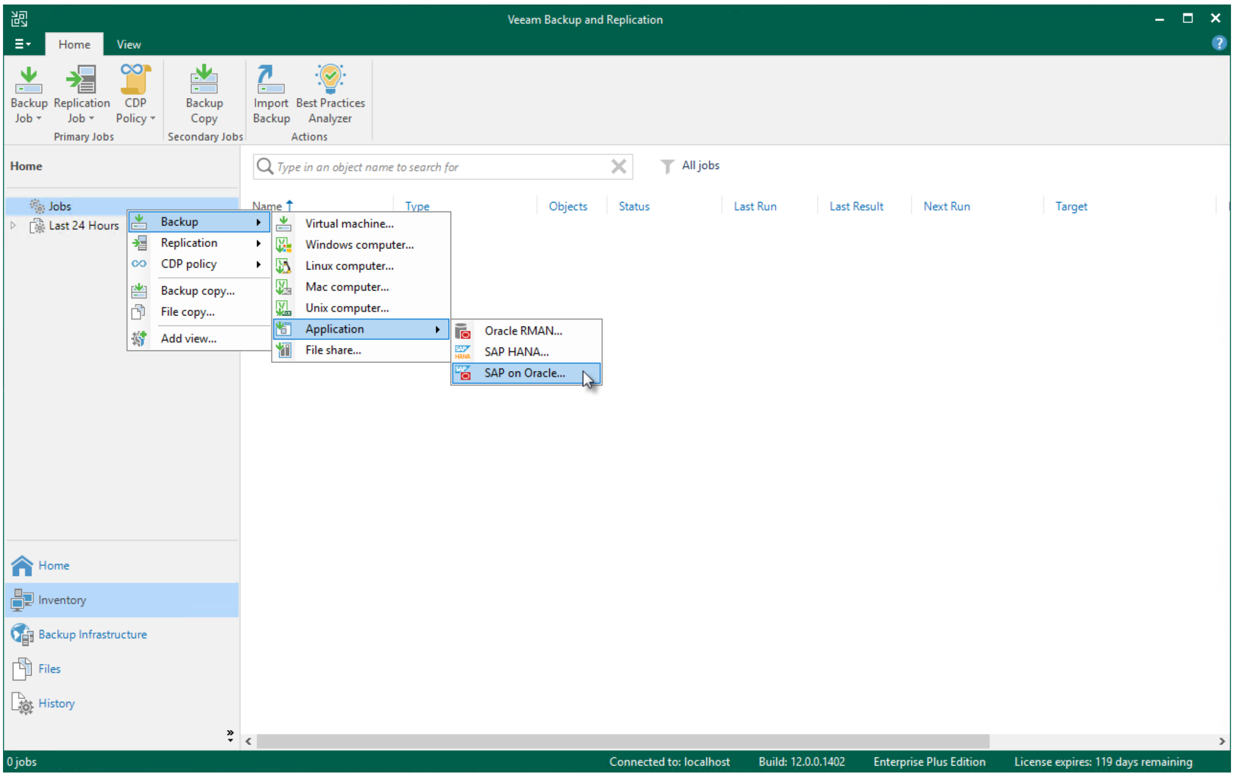
- The Veeam Backup & Replication license must have a sufficient number of instances to process computers that you plan to add to the application backup policy.
- The target location where you plan to store backup files must have enough free space.
- Protection groups that you want to add to the policy must be configured in advance.

Application backup policies have the following limitations:

- One backup object (computer, database system, or database) can be added only to one application backup policy. Otherwise, the application backup policy will fail.
- You can create application backups on a Veeam backup repository. If you want to save backups in other target locations, you must configure backup job on the computer side.
- After you start managing a Veeam Plug-in with Veeam Backup & Replication, data backup for the computer is performed by a backup policy configured in Veeam Backup & Replication. Veeam Plug-in running on the computer starts a new backup chain on a target location specified in the backup policy settings. You cannot continue the existing backup chain that was created by Veeam Plug-in operating in the standalone mode.

Step 1. Launch New Backup Job Wizard

To create an application policy for Veeam Plug-in for SAP on Oracle, you must launch the **New Application Backup Policy** wizard. To do this, on the **Home** tab, click **Backup Job** > **Application** > **SAP on Oracle**.



Step 2. Specify Policy Name

At the **Name** step of the wizard, specify a name and description for the application backup policy.

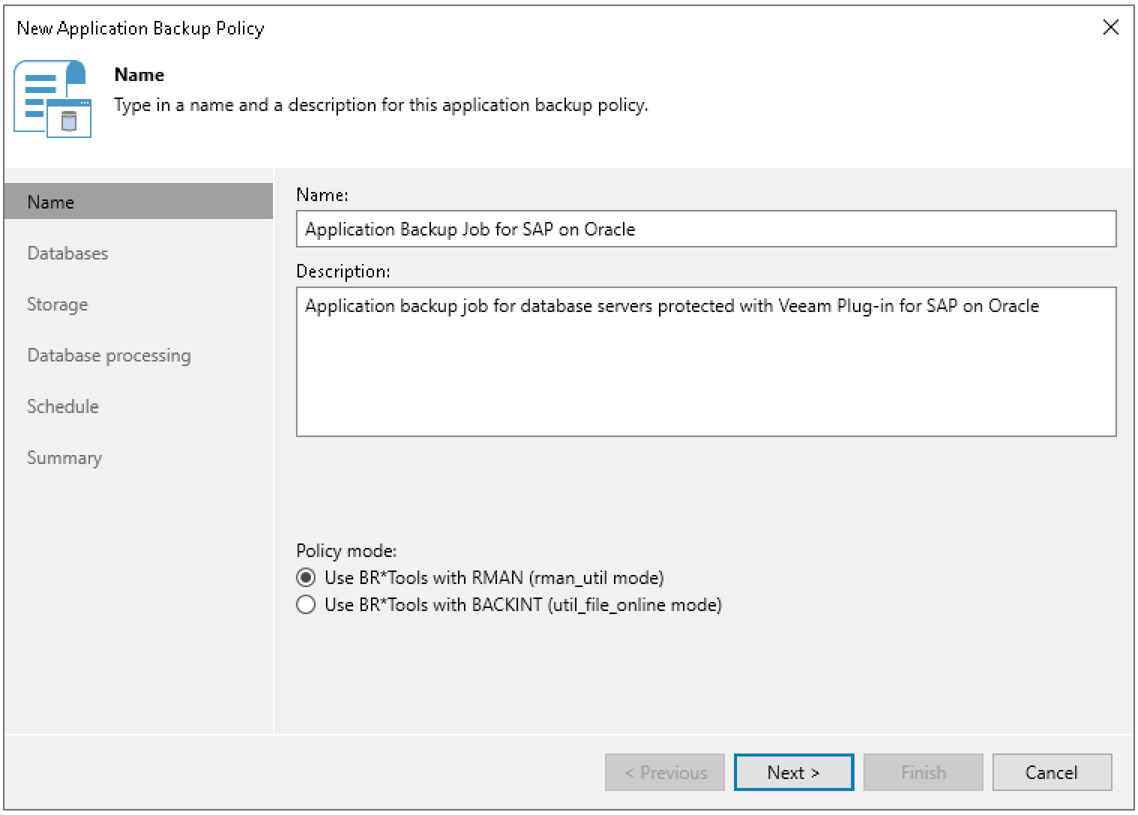
1. In the **Name** field, enter a name for the application backup policy.

2. In the **Description** field, provide a description for future reference. The default description contains information about the user who created the job, date and time when the job was created.

3. In the **Policy mode** field, select the job mode. You can select one of the following modes:

   - Use BR*Tools with RMAN (rman_uril mode)

   - Use BR*Tools with BACKINT (util_file_online mode)



New Application Backup Policy

Name

Type in a name and a description for this application backup policy.

Name:
Application Backup Job for SAP on Oracle

Description:
Application backup job for database servers protected with Veeam Plug-in for SAP on Oracle

Policy mode:
● Use BR*Tools with RMAN (rman_util mode)
○ Use BR*Tools with BACKINT (util_file_online mode)

Step 3. Specify Databases

At the **Databases** step of the wizard, select protection groups, computers, database systems or individual databases whose data you want to back up.

You can add to the backup scope one or more objects added to inventory in the Veeam Backup & Replication console.

Application policies with protection groups are dynamic in their nature. If Veeam Backup & Replication discovers a new computer in a protection group after the policy is created, Veeam Backup & Replication will automatically update the policy settings to include the added computer.

Adding Objects from Inventory

To add protection groups, individual computers or databases to the application backup policy:

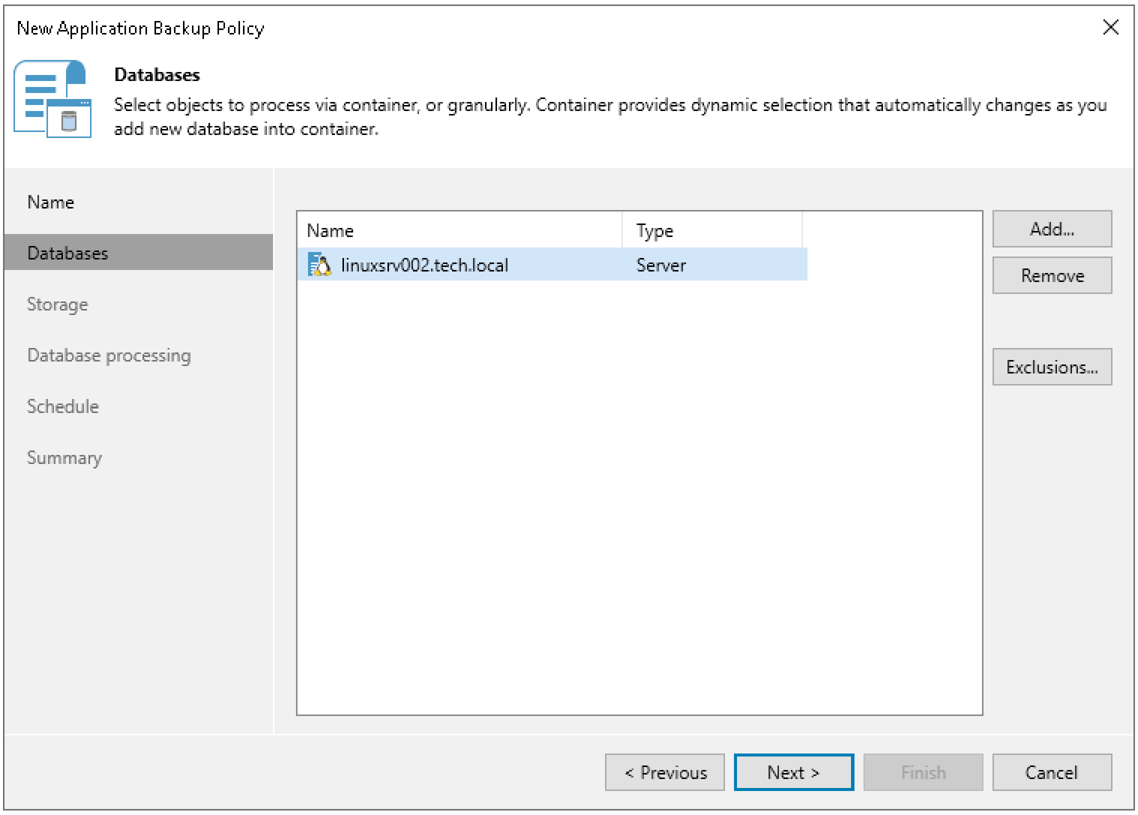
1. Click **Add**.
2. In the **Select Objects** window, select one or more objects in the list and click **OK**. You can select any of the following objects:
   - Protection group
   - Computer
   - Oracle home
   - Oracle database

   You can press and hold **[CTRL]** to select multiple objects at once.

> **NOTE**
>
> In the **Select Objects** window, Veeam Backup & Replication shows only those computers on which Veeam Backup & Replication have detected Oracle database systems during the rescan job. To learn more, see Rescan Job.

To quickly find the necessary object, use the search field at the bottom of the **Select Objects** window.

1. Enter the object name or a part of it in the search field.
2. Click the **Start search** button on the right or press **[ENTER]**.



New Application Backup Policy

Databases

Select objects to process via container, or granularly. Container provides dynamic selection that automatically changes as you add new database into container.

Name	Type
linuxsrv002.tech.local	Server

Excluding Objects

You can exclude protection groups, individual computers or databases from the backup scope of the application backup policy. This may be useful if you want to back up a certain database with another application backup policy.

To exclude protection groups, individual computers or databases from the backup scope:

3. Click **Exclusions**.
4. In the **In the Exclusions** window, select one or more objects in the list and click **OK**. You can select any of the following objects:
   - Protection group
   - Computer
   - Oracle home
   - Oracle database

   You can press and hold **[CTRL]** to select multiple objects at once.

NOTE

In the **Exclusions** window, Veeam Backup & Replication shows only those objects which were already added to the backup scope. To learn more, see Adding Objects from Inventory.

Step 4. Specify Storage Settings

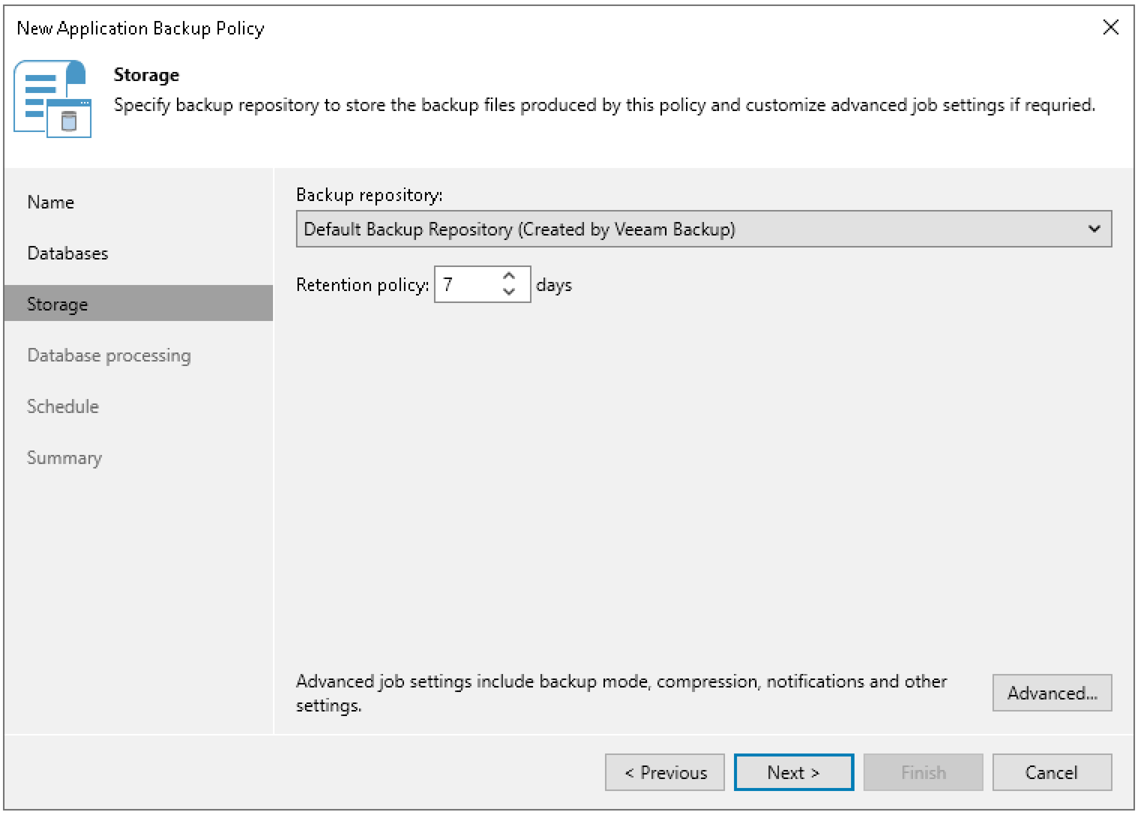
At the **Storage** step of the wizard, specify settings for the target backup repository:

1. From the **Backup repository** list, select a backup repository where you want to store backups. You can select from the Veeam backup repositories configured on the backup server that will manage the created backup policy.

   When you select a backup repository, Veeam Backup & Replication automatically checks how much free space is available on the backup repository.

2. In the **Retention Policy** field, specify the number of days for which you want to store backup files in the target location. By default, Veeam Backup & Replication keeps backup files for 7 days. After this period is over, Veeam Backup & Replication will remove the earliest restore points from the backup chain.

3. Click **Advanced** to specify advanced settings for the backup job. To learn more, see Specify Advanced Backup Settings.


New Application Backup Policy

Storage

Specify backup repository to store the backup files produced by this policy and customize advanced job settings if requried.

Backup repository: Default Backup Repository (Created by Veeam Backup)

Retention policy: 7 days

Advanced job settings include backup mode, compression, notifications and other settings.

Step 5. Specify Advanced Backup Settings

In the **Advanced Settings** window, specify advanced settings for the application backup policy:

- Backup settings
- Storage settings
- Notification settings
- Oracle settings

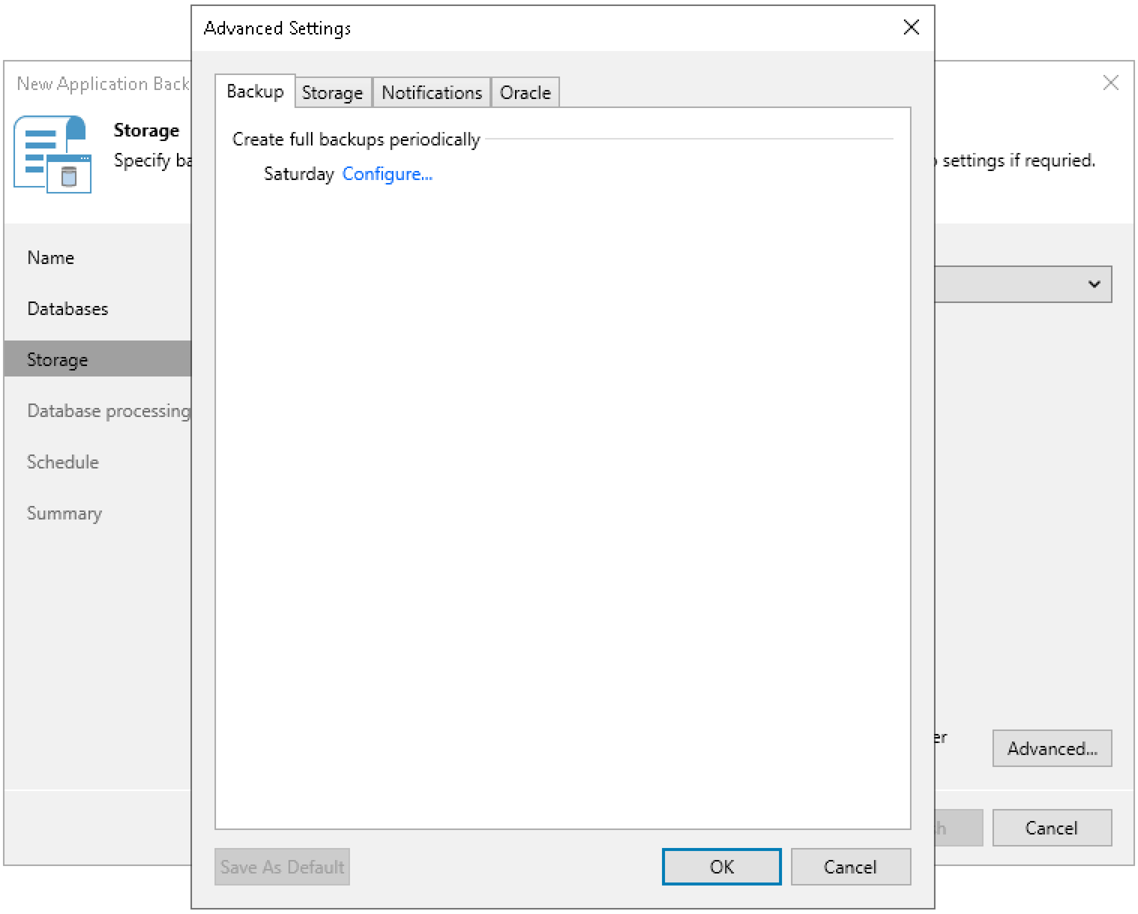
TIP

After you specify necessary settings for the application backup policy, you can save them as default settings. To do this, click **Save as Default** at the bottom left corner of the **Advanced Settings** window. When you create a new backup policy, Veeam Backup & Replication will automatically apply the default settings to the new policy.

Backup Settings

To specify settings for a backup chain created with the backup policy:

1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Backup** tab.
3. To define the schedule for full backups, click **Configure** and define the schedule in the **Schedule Settings** window:
   - To run the job once a month on specific days, select **Monthly on**. Use the fields on the right to configure the necessary schedule.
   - To run the job once a week on specific week days, select **Weekly**. Use the fields on the right to select the necessary week days.



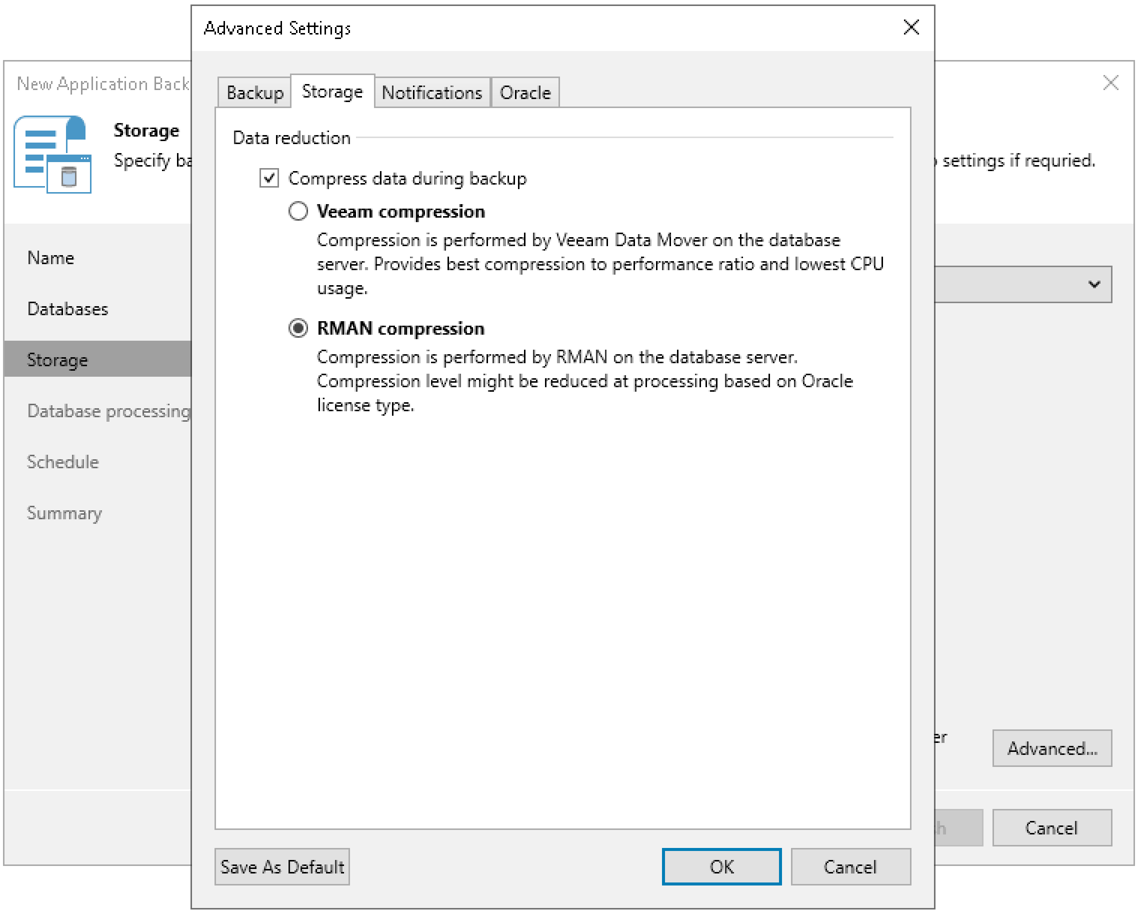
Create full backups periodically

Saturday Configure...

Storage Settings

To specify compression settings for the backup job:

1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Storage** tab.
3. Select the **Compress data during backup** check box and select the way compression is performed:
   - Select **Veeam compression** if you want to perform data compression with Data Mover by Veeam Software.
   - Select **RMAN compression** if you want to perform data compression with Oracle.



Data reduction

☑ Compress data during backup

○ **Veeam compression**
Compression is performed by Veeam Data Mover on the database server. Provides best compression to performance ratio and lowest CPU usage.

● **RMAN compression**
Compression is performed by RMAN on the database server. Compression level might be reduced at processing based on Oracle license type.

Notification Settings

To specify notification settings for the backup job:

1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Notifications** tab.
3. Select the **Send SNMP notifications for this job** check box if you want to receive SNMP traps when the job completes successfully.

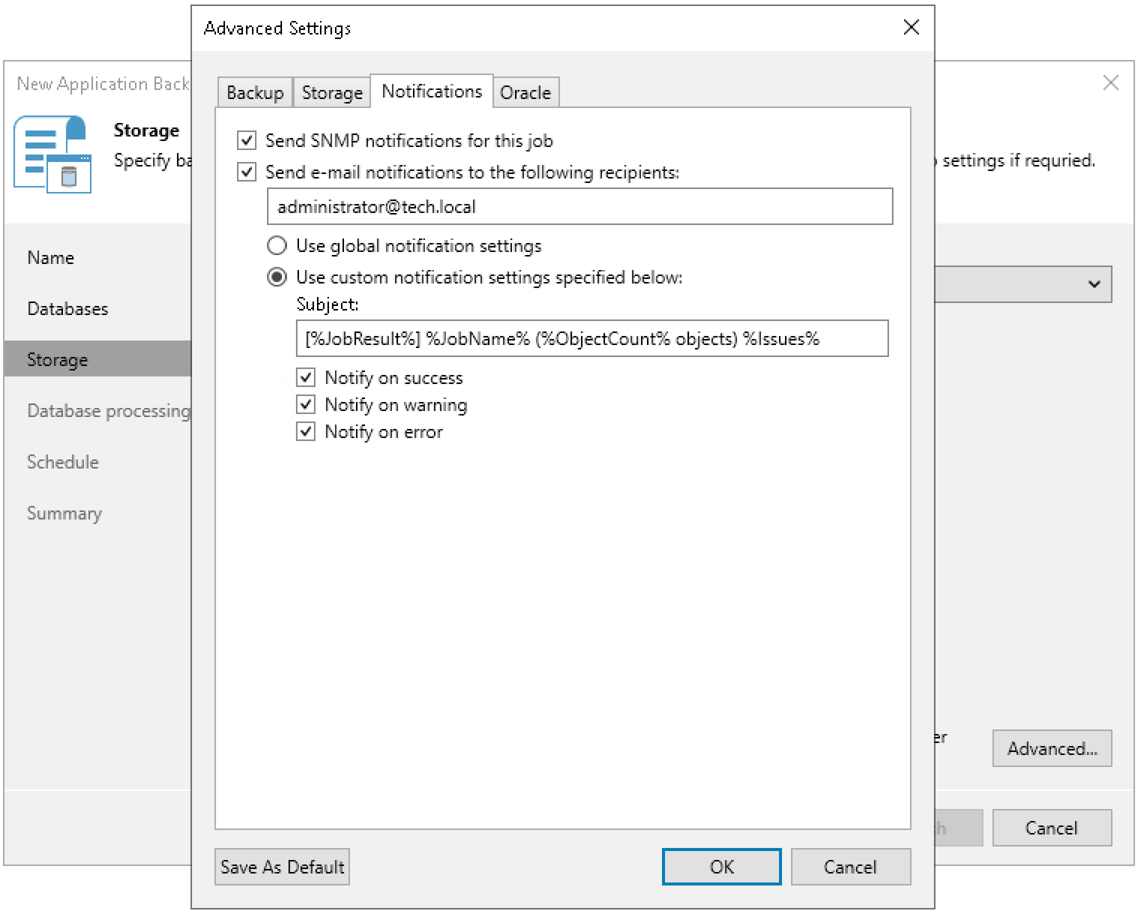
   SNMP traps will be sent if you specify global SNMP settings in Veeam Backup & Replication and configure software on recipient's machine to receive SNMP traps. For more information, see the Specifying SNMP Settings section in the Veeam Backup & Replication User Guide.

4. Select the **Send email notifications to the following recipients** check box if you want to receive notifications about the job completion status by email. In the field below, specify a recipient's email address. You can enter several addresses separated by a semicolon.

   Email notifications will be sent if you configure global email notification settings in Veeam Backup & Replication. For more information, see the Configuring Global Email Notification Settings section in Veeam Backup & Replication User Guide.

5. You can choose to use global notification settings or specify custom notification settings.

   - To receive a typical notification for the job, select **Use global notification settings**. In this case, Veeam Backup & Replication will apply to the job global email notification settings specified for the backup server.
   - To configure a custom notification for the job, select **Use custom notification settings specified below**. You can specify the following notification settings:
     - In the **Subject** field, specify a notification subject. You can use the following variables in the subject: *%Time%* (completion time), *%JobName%*, *%JobResult%*, *%ObjectCount%* (number of machines in the job) and *%Issues%* (number of machines in the job that have been processed with the *Warning* or *Failed* status).
     - Select the **Notify on success**, **Notify on warning** and/or **Notify on error** check boxes to receive email notification if the job completes successfully, completes with a warning or fails.
     - Select the **Suppress notifications until the last retry** check box to receive a notification about the final job status. If you do not enable this option, Veeam Backup & Replication will send one notification per every job retry.



Advanced Settings

Backup | Storage | Notifications | Oracle

☑ Send SNMP notifications for this job

☑ Send e-mail notifications to the following recipients:

administrator@tech.local

○ Use global notification settings

● Use custom notification settings specified below:

Subject:

[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

☑ Notify on success

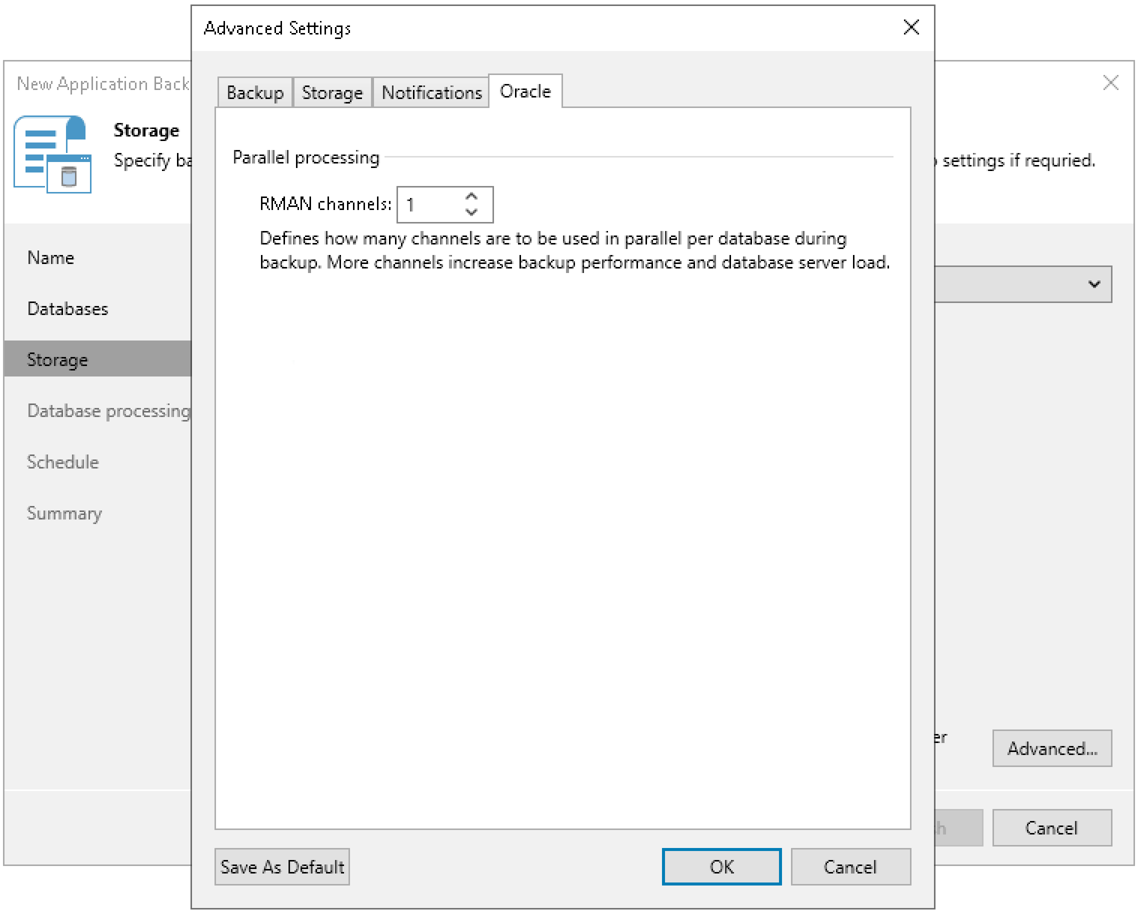
☑ Notify on warning

☑ Notify on error

Oracle Settings

To specify Oracle settings for the backup policy:

1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Oracle** tab.
3. In the **RMAN channels** field, specify the number of data channels that Veeam Plug-in will use to back up databases in parallel.



RMAN channels: 1

Defines how many channels are to be used in parallel per database during backup. More channels increase backup performance and database server load.

Step 6. Specify Database Processing Settings

At the **Database Processing** step of the wizard, specify database credentials and log processing settings:

1. Select the object and click **Edit**.
2. Specify log processing settings for the objects in the list. To learn more, see Processing settings

In the list, Veeam Backup & Replication shows only those objects that you added to the backup scope at the **Databases** step of the wizard. If you added a protection group, but need to specify settings for an individual computer or database in this protection group, you can add such objects to the list. To learn more, see Adding Objects from Backup Scope.

Adding Objects from Backup Scope

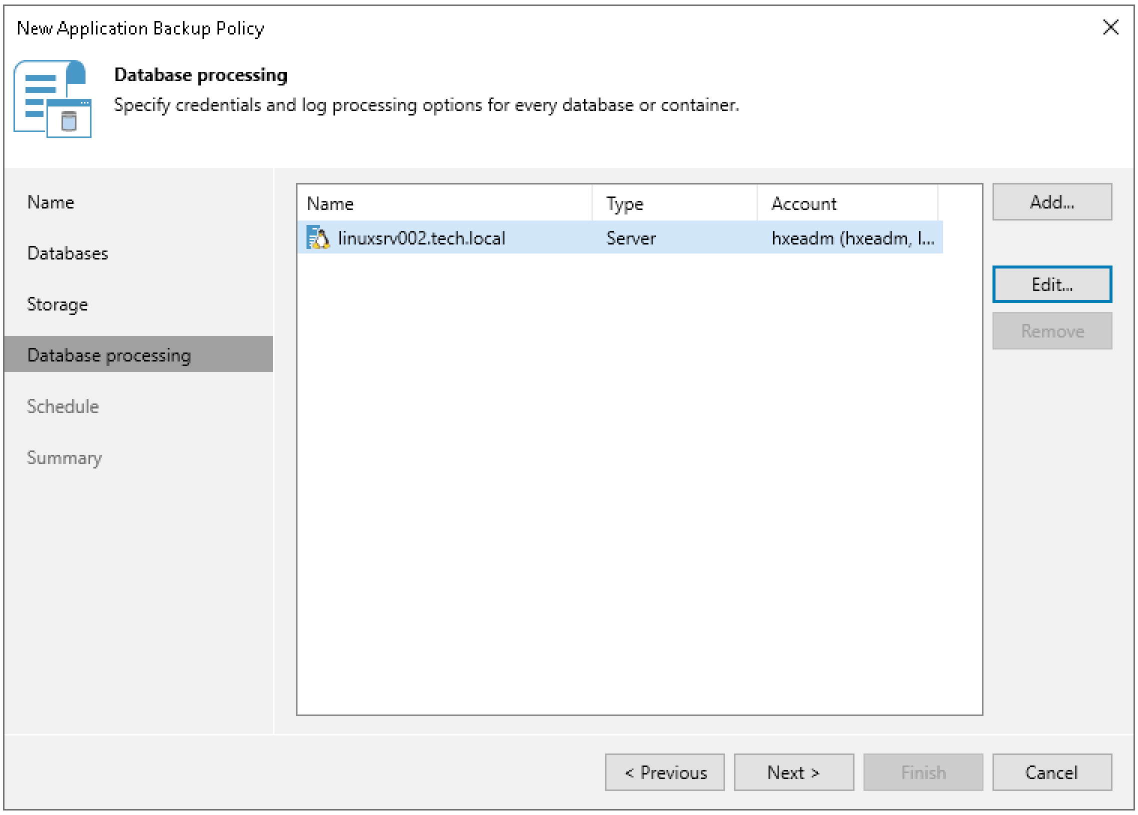
To add protection groups, individual computers or databases to the **Credentials** list:

1. Click **Add**.
2. In the **Select Objects** window, select one or more objects in the list and click **OK**. You can select any of the following objects:
   - Protection group
   - Computer
   - Oracle home
   - Oracle database

   You can press and hold **[CTRL]** to select multiple objects at once.

To quickly find the necessary object, use the search field at the bottom of the **Select Objects** window.

1. Enter the object name or a part of it in the search field.
2. Click the **Start search** button on the right or press **[ENTER]**.



Name	Type	Account
linuxsrv002.tech.local	Server	hxeadm (hxeadm, l...

Processing Settings

To specify processing settings:

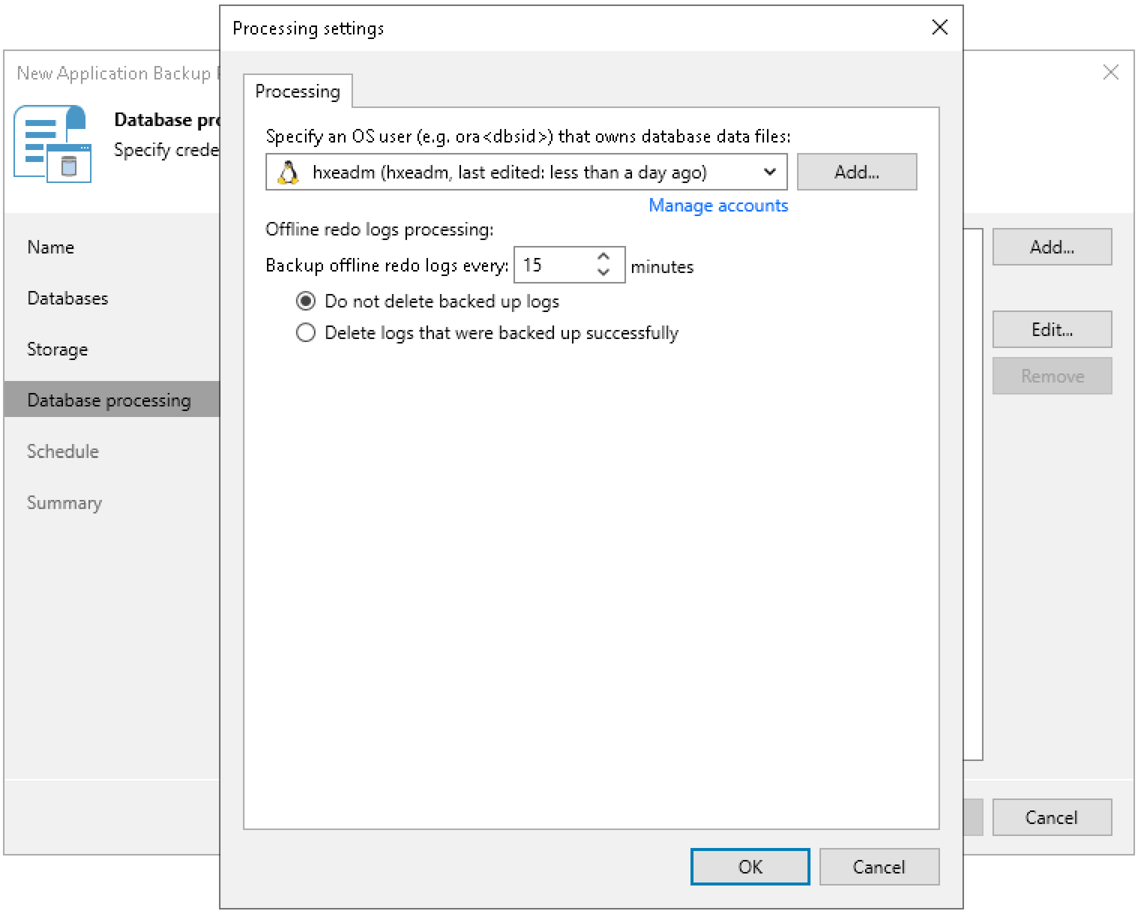
1. At the **Database Processing** step of the wizard, select the object and click **Edit**.
2. In the **Processing Settings** window, click the **Processing** tab.
3. To specify a user account that Veeam Plug-in will use to connect to the Oracle database, select from the **Specify OS user (e.g. ora<dbsid>) who owns data files** of the database list a user account that has SYSDBA rights on the database. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials.
4. In the **Backup archived redo logs every <N> minutes** field, specify the frequency for archived logs backup. By default, archived logs are backed up every 15 minutes. The minimum log backup interval is 5 minutes. The maximum log backup interval is 480 minutes.

5. Specify if Veeam Plug-in must delete archived logs for the Oracle database:

   ○ Select **Do not delete offline redo logs** if you want Veeam Plug-in to preserve archived logs. When the backup job completes, Veeam Plug-in will not delete archived logs.

     It is recommended that you select this option for databases for which the ARCHIVELOG mode is turned off. If the ARCHIVELOG mode is turned on, archived logs may grow large and consume all disk space. In this case, the database administrator must take care of archived logs him-/herself.

   ○ Select **Delete offline redo logs that were backed up** if you want Veeam Plug-in back up logs and delete logs from the database after the backup operation. Veeam Plug-in will wait for the backup job to complete successfully and then trigger archived logs truncation via Oracle Call Interface (OCI). If the backup job fails, the logs will remain untouched until the next successful backup job session.



Processing settings

Processing

Specify an OS user (e.g. ora<dbsid>) that owns database data files: hxeadm (hxeadm, last edited: less than a day ago)

Offline redo logs processing:

Backup offline redo logs every: 15 minutes

● Do not delete backed up logs

○ Delete logs that were backed up successfully

Step 7. Specify Policy Schedule

At the **Schedule** step of the wizard, specify the schedule according to which you want to perform backup.

To specify the job schedule:

1. Select the **Run the job automatically** check box. If this check box is not selected, you will have to start the backup job manually to create backup.

2. Define scheduling settings for the job:

    - To run the job at specific time daily, on defined week days or with specific periodicity, select **Daily at this time**. Use the fields on the right to configure the necessary schedule.

    - To run the job once a month on specific days, select **Monthly at this time**. Use the fields on the right to configure the necessary schedule.

- To run the job repeatedly throughout a day with a specific time interval, select **Periodically every**. In the field on the right, select the necessary time unit: *Hours* or *Minutes*.

    - [For backup job managed by backup server] To define the permitted time window for the job, click **Schedule** and use the time table. In the **Start time within an hour** field, specify the exact time when the job must start.

      A repeatedly run job is started by the following rules:

        - The defined interval always starts at 12:00 AM. For example, if you configure to run a job with a 4-hour interval, the job will start at 12:00 AM, 4:00 AM, 8:00 AM, 12:00 PM, 4:00 PM and so on.

        - If you define permitted hours for the job, after the denied interval is over, the job will start immediately and then run by the defined schedule.

      For example, you have configured a job to run with a 2-hour interval and defined permitted hours from 9:00 AM to 5:00 PM. According to the rules above, the job will first run at 9:00 AM, when the denied period is over. After that, the job will run at 10:00 AM, 12:00 PM, 2:00 PM and 4:00 PM.

    - To run the job continuously, select the **Periodically every** option and choose **Continuously** from the list on the right. A new backup job session will start as soon as the previous backup job session finishes.

    - [For backup job managed by backup server] To chain jobs, use the **After this job** field. In the common practice, jobs start one after another: when job A finishes, job B starts and so on. If you want to create a chain of jobs, you must define the time schedule for the first job in the chain. For the rest of the jobs in the chain, select the **After this job** option and choose the preceding job from the list.

> NOTE
>
> Mind the following:
>
> - The **After this job** option is not available if you have selected the **Managed by agent** option at the **Job Mode** step of the wizard.
> - The **After this job** function will automatically start a job if the first job in the chain is started automatically by schedule. If you start the first job manually, Veeam Backup & Replication will display a notification. You will be able to choose whether Veeam Backup & Replication must start the chained job as well.

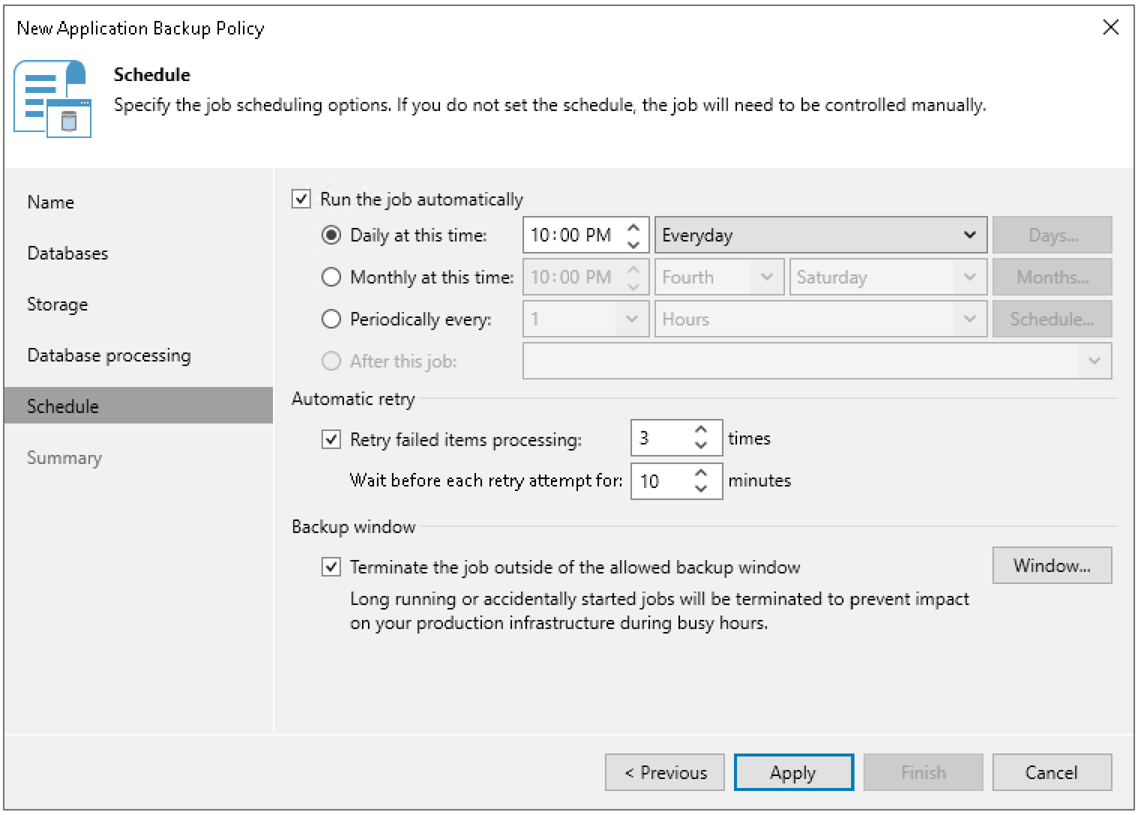
3. In the **Automatic retry** section, define whether Veeam Backup & Replication or Veeam Plug-in (depending on the selected job mode) must attempt to run the backup job again if the job fails for some reason. Enter the number of attempts to run the job and define time intervals between them. If you select continuous backup, Veeam Backup & Replication or Veeam Plug-in will retry the job for the defined number of times without any time intervals between the job runs.

4. [For backup job managed by backup server] In the **Backup window** section, define the time interval within which the backup job must complete. The backup window prevents the job from overlapping with production hours and ensures that the job does not impact performance of your server. To set up a backup window for the job:

   a. Select the **Terminate job if it exceeds allowed backup window** check box and click **Window**.

   b. In the **Time Periods** window, define the allowed hours and prohibited hours for backup. If the job exceeds the allowed window, it will be automatically terminated.

> NOTE
>
> If you configure a backup policy, after you click **Apply** at the **Schedule** step of the wizard, Veeam Backup & Replication will immediately apply the backup policy to protected computers.



Schedule

Specify the job scheduling options. If you do not set the schedule, the job will need to be controlled manually.

☑ Run the job automatically

● Daily at this time: 10:00 PM Everyday Days...

○ Monthly at this time: 10:00 PM Fourth Saturday Months...

○ Periodically every: 1 Hours Schedule...

○ After this job:

Automatic retry

☑ Retry failed items processing: 3 times

Wait before each retry attempt for: 10 minutes

Backup window

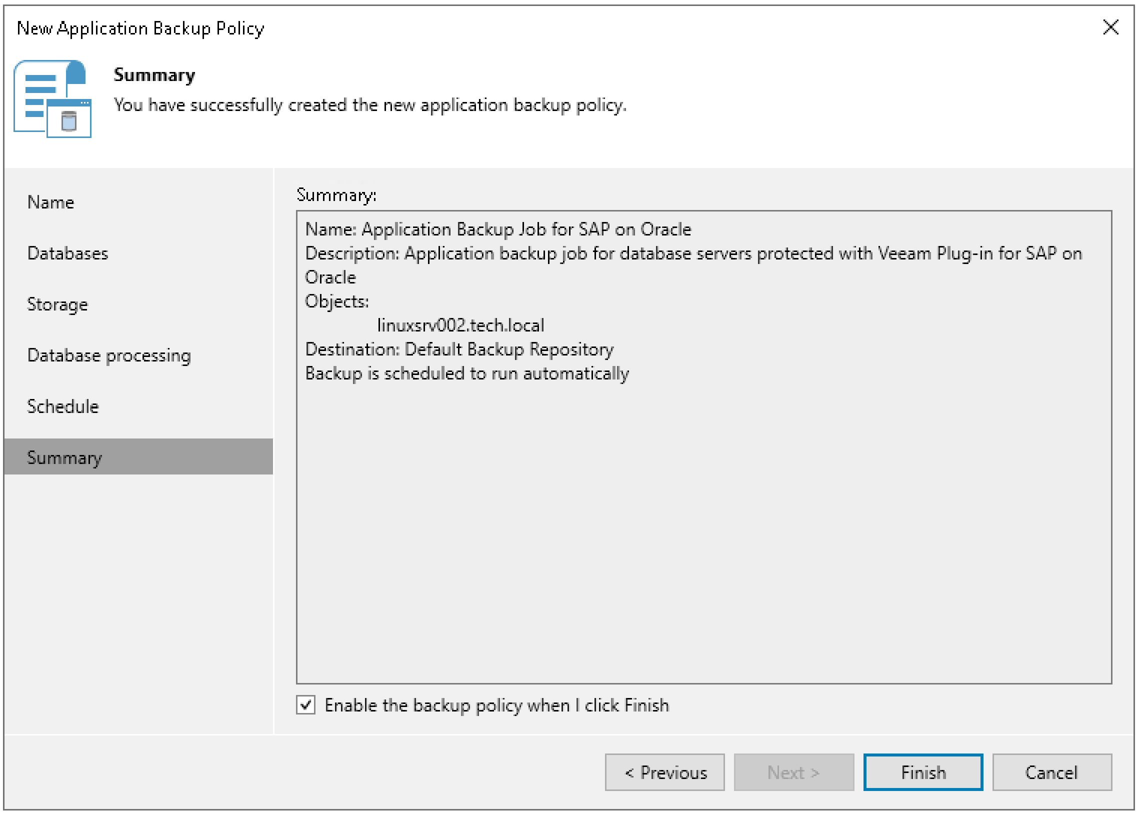
☑ Terminate the job outside of the allowed backup window Window...

Long running or accidentally started jobs will be terminated to prevent impact on your production infrastructure during busy hours.

Step 8. Review Policy Settings

At the **Summary** step of the wizard, complete the configuration process for the application backup policy.

1. Review settings of the configured backup policy.
2. Select the **Run the job when I click Finish** check box if you want to start the policy right after you finish working with the wizard.
3. Click **Finish** to close the wizard.



New Application Backup Policy
Summary
You have successfully created the new application backup policy.
Name
Databases
Storage
Database processing
Schedule
Summary

Summary:

Name: Application Backup Job for SAP on Oracle
Description: Application backup job for database servers protected with Veeam Plug-in for SAP on Oracle
Objects:
linuxsrv002.tech.local
Destination: Default Backup Repository
Backup is scheduled to run automatically

☑ Enable the backup policy when I click Finish

< Previous
Next >
Finish
Cancel

Managing Application Backup Policy

You can use the Veeam Backup & Replication console to perform the following operations with an application backup policy:

- Start and stop backup operations on computers added to the backup policy.
- Perform active full backup on computers added to the backup policy.
- Edit backup policy settings.
- Enable and disable a backup policy.
- Clone a backup policy.
- Delete a backup policy.

Starting and Stopping Backup Policy

You can manually start an application backup policy on computers added to this backup policy. For example, if you want to create an additional restore point in the backup chain and do not want to change the backup schedule. You can also stop the backup process, for example, if processing of a computer is about to take long, and you do not want the backup process to produce workload on the production environment during business hours.

Veeam Backup & Replication does not check whether connection to computers is active at the time when the command is sent. Keep in mind that the start or stop operation will be performed only on those computers that received the command from the backup server.

Starting Backup

To start an application backup policy on computers added to this backup policy:

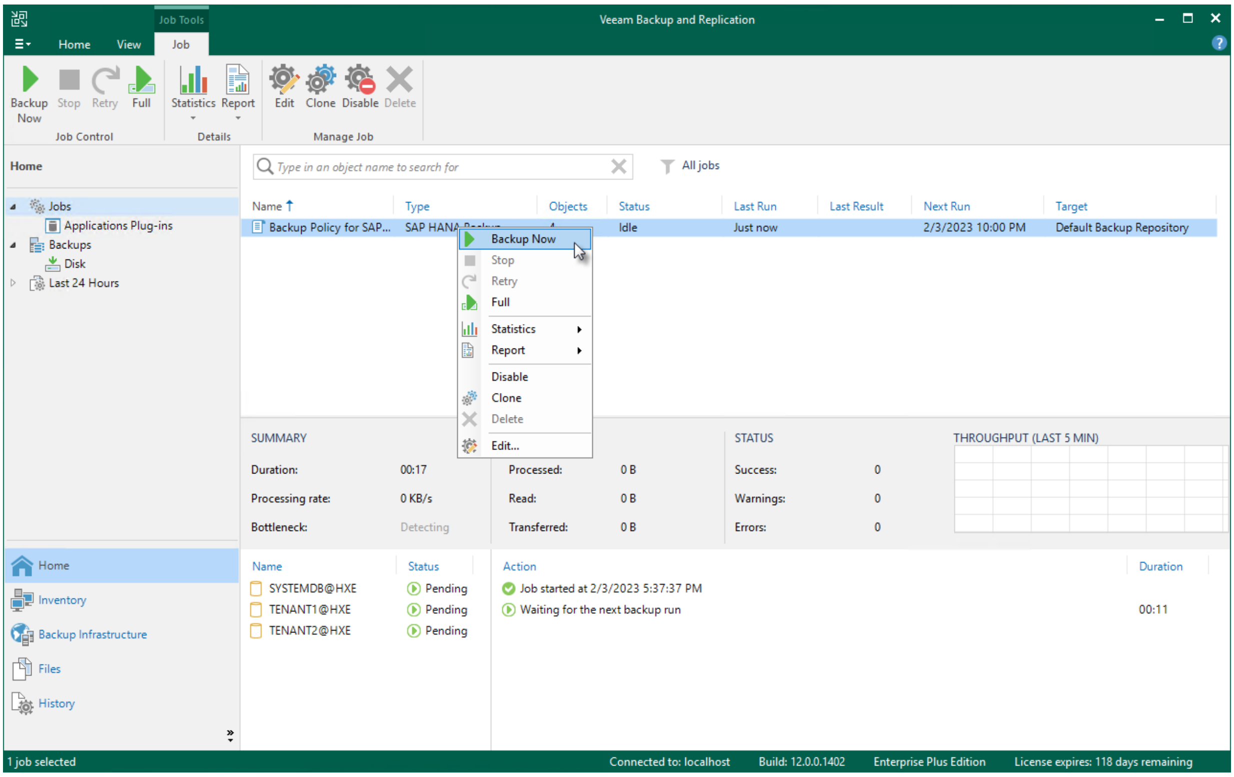
1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the backup policy and click **Backup Now** on the ribbon or right-click the job and select **Backup Now**.

> **TIP**
>
> You can also start an application backup policy directly on a computer from the computer side.

Stopping Backup

To stop application backup policy on computers added to this backup policy:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the backup policy and click **Stop** on the ribbon or right-click the job and select **Stop**. In the displayed window, click **Yes**.



Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target
Backup Policy for SAP...	SAP HANA Backup	4	Idle	Just now		2/3/2023 10:00 PM	Default Backup Repository

SUMMARY

Duration: 00:17
Processing rate: 0 KB/s
Bottleneck: Detecting

Processed: 0 B
Read: 0 B
Transferred: 0 B

STATUS

Success: 0
Warnings: 0
Errors: 0

Name	Status
SYSTEMDB@HXE	Pending
TENANT1@HXE	Pending
TENANT2@HXE	Pending

Action	Duration
Job started at 2/3/2023 5:37:37 PM	
Waiting for the next backup run	00:11

1 job selected   Connected to: localhost   Build: 12.0.0.1402   Enterprise Plus Edition   License expires: 118 days remaining

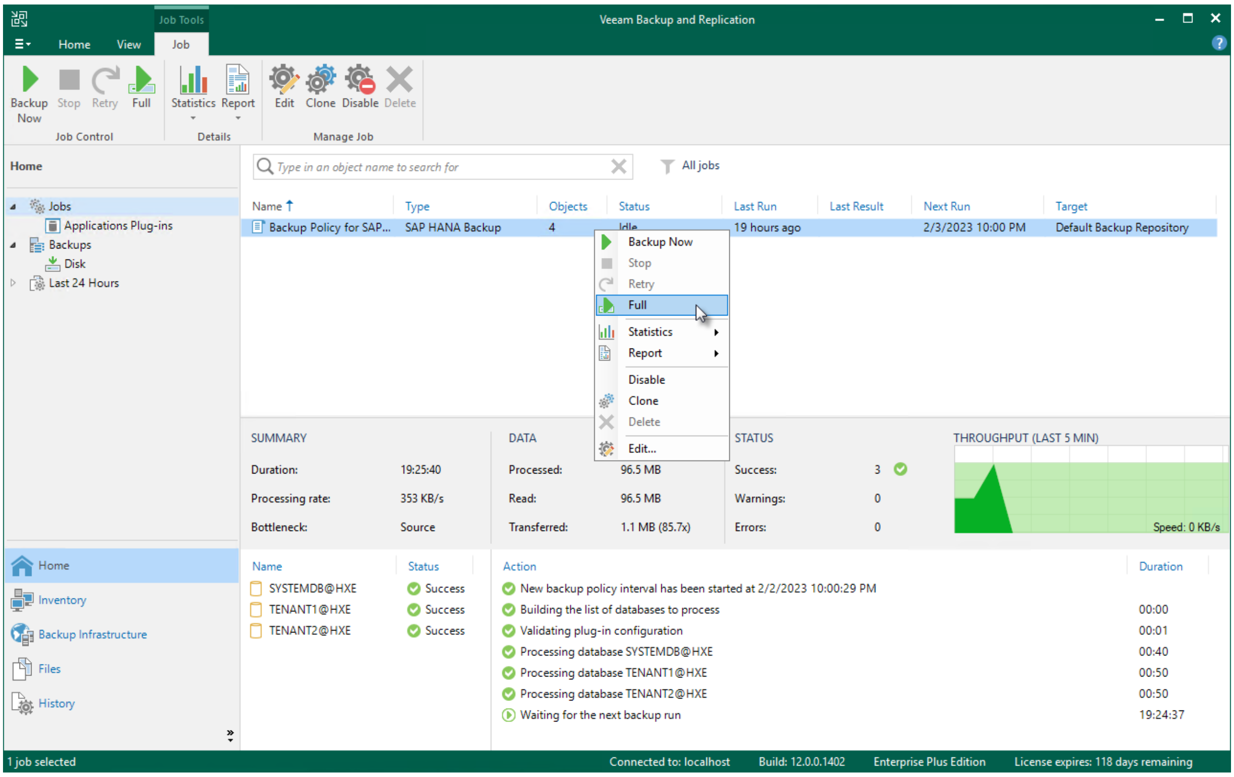
Performing Active Full Backup

You can create an ad-hoc full backup — active full backup, and add it to the backup chain on the backup repository. The active full backup resets the backup chain. All subsequent incremental backups use the active full backup as a starting point. The previously used full backup will remain on the backup repository until it is removed from the backup chain according to the retention policy.

When you start active full backup for a backup policy, Veeam Backup & Replication does not check whether connection to computers is active at the time when the command is sent. Keep in mind that the active full backup operation will be performed only on those computers that received the command from the backup server.

To perform active full backup on computers added to the backup policy:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the backup policy and click **Full** on the ribbon or right-click the job and select **Full**.



Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target
Backup Policy for SAP...	SAP HANA Backup	4	Idle	19 hours ago		2/3/2023 10:00 PM	Default Backup Repository

SUMMARY		DATA		STATUS	
Duration:	19:25:40	Processed:	96.5 MB	Success:	3 ✓
Processing rate:	353 KB/s	Read:	96.5 MB	Warnings:	0
Bottleneck:	Source	Transferred:	1.1 MB (85.7x)	Errors:	0

Name	Status
SYSTEMDB@HXE	Success
TENANT1@HXE	Success
TENANT2@HXE	Success

Action	Duration
New backup policy interval has been started at 2/2/2023 10:00:29 PM	
Building the list of databases to process	00:00
Validating plug-in configuration	00:01
Processing database SYSTEMDB@HXE	00:40
Processing database TENANT1@HXE	00:50
Processing database TENANT2@HXE	00:50
Waiting for the next backup run	19:24:37

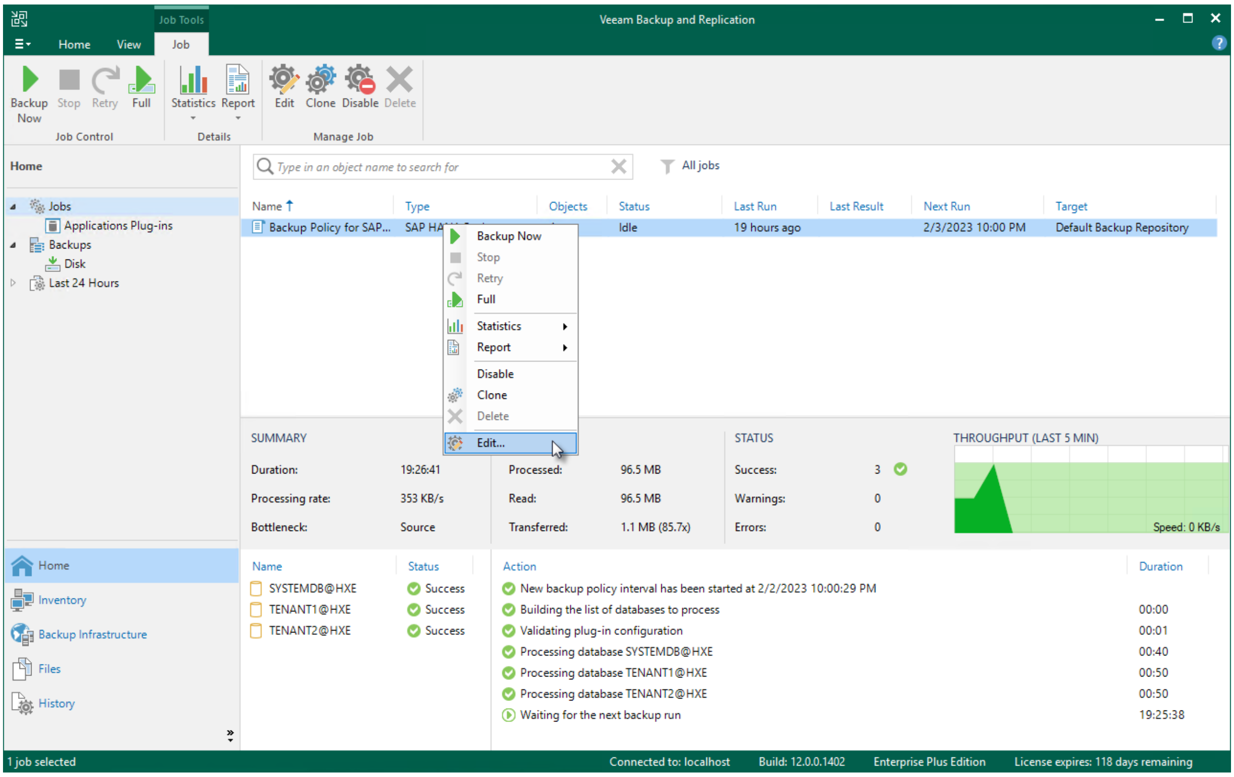
Editing Backup Policy Settings

You can edit settings of an application backup policy at any time. For example, you may want to change the backup scope, target location or scheduling settings for application backup policies running on protected computers.

> NOTE
>
> - You cannot rename an application backup policy.
> - If you want to change a backup repository, you must disable a policy. To learn more, see Enabling and Disabling Backup Policy. In this case during the next run the policy will produce a full backup.

To edit backup policy settings:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the backup policy and click **Edit** on the ribbon or right-click the policy and select **Edit**.
4. Complete the steps of the **Edit Application Backup Policy** wizard to change the job settings as required.



Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target
Backup Policy for SAP...	SAP HA...		Idle	19 hours ago		2/3/2023 10:00 PM	Default Backup Repository

SUMMARY

Duration: 19:26:41
Processing rate: 353 KB/s
Bottleneck: Source

Processed: 96.5 MB
Read: 96.5 MB
Transferred: 1.1 MB (85.7x)

STATUS

Success: 3
Warnings: 0
Errors: 0

THROUGHPUT (LAST 5 MIN)

Speed: 0 KB/s

Name	Status
SYSTEMDB@HXE	Success
TENANT1@HXE	Success
TENANT2@HXE	Success

Action	Duration
New backup policy interval has been started at 2/2/2023 10:00:29 PM	
Building the list of databases to process	00:00
Validating plug-in configuration	00:01
Processing database SYSTEMDB@HXE	00:40
Processing database TENANT1@HXE	00:50
Processing database TENANT2@HXE	00:50
Waiting for the next backup run	19:25:38

1 job selected   Connected to: localhost   Build: 12.0.0.1402   Enterprise Plus Edition   License expires: 118 days remaining

Enabling and Disabling Backup Policy

You can temporary disable application backup policies configured in Veeam Backup & Replication. While a backup policy is in the disabled state, the following operations are not performed in the Veeam Plug-in management infrastructure:

- Veeam Backup & Replication does not apply backup policy settings to computers.
- Veeam Plug-in running on a protected computer does not create backups on the backup repository.

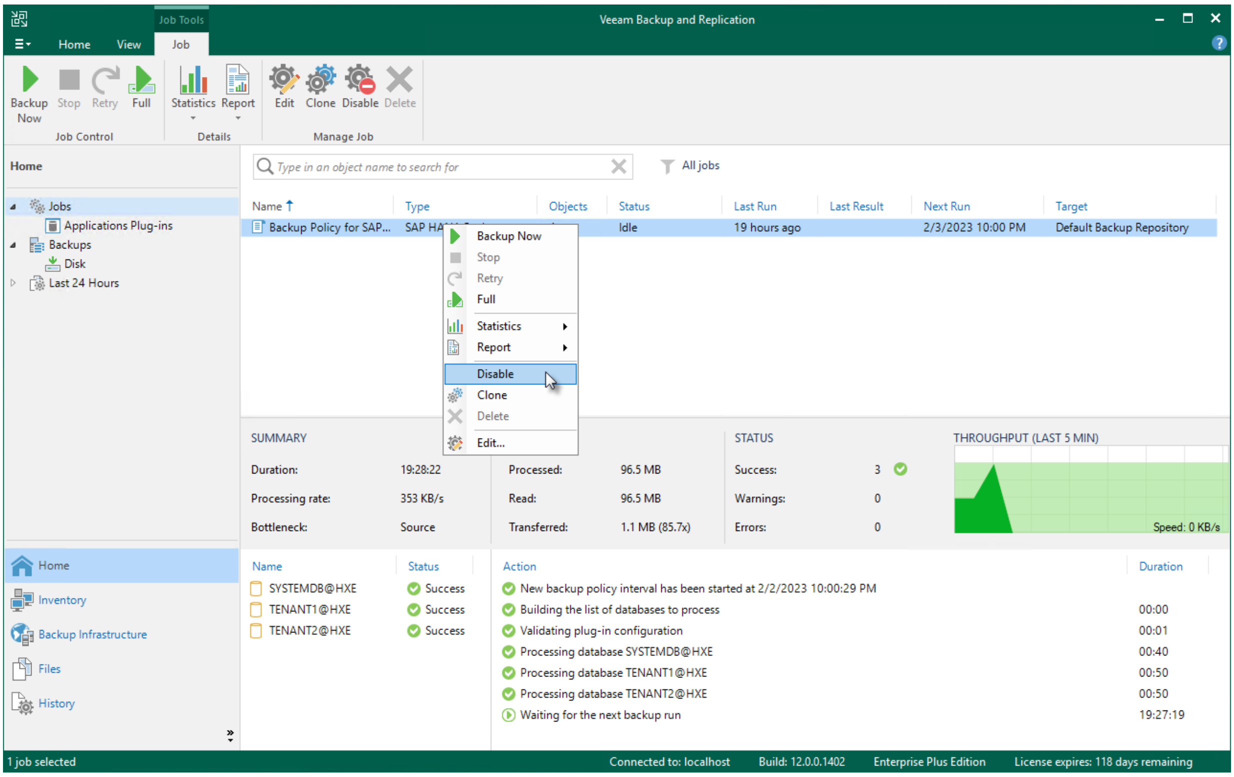
  If a user of a protected computer starts the backup policy manually or if the policy starts by schedule, the job session will fail and report the *"The job has been disabled by the Veeam Backup & Replication administrator"* error.

To disable an application backup policy:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the application backup policy and click **Disable** on the ribbon or right-click the policy and select **Disable**.

   If you disabled a backup policy in the Veeam Backup & Replication console and this backup policy starts a new backup session, this backup session and all automatic retries of this session will fail.

To enable a disabled policy, select it in the list and click **Disable** on the ribbon once again.



Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target
Backup Policy for SAP...	SAP HA...		Idle	19 hours ago		2/3/2023 10:00 PM	Default Backup Repository

SUMMARY

Duration:	19:28:22	Processed:	96.5 MB	Success:	3 ✓
Processing rate:	353 KB/s	Read:	96.5 MB	Warnings:	0
Bottleneck:	Source	Transferred:	1.1 MB (85.7x)	Errors:	0

Name	Status
SYSTEMDB@HXE	✓ Success
TENANT1@HXE	✓ Success
TENANT2@HXE	✓ Success

Action	Duration
✓ New backup policy interval has been started at 2/2/2023 10:00:29 PM	
✓ Building the list of databases to process	00:00
✓ Validating plug-in configuration	00:01
✓ Processing database SYSTEMDB@HXE	00:40
✓ Processing database TENANT1@HXE	00:50
✓ Processing database TENANT2@HXE	00:50
Waiting for the next backup run	19:27:19

1 job selected   Connected to: localhost   Build: 12.0.0.1402   Enterprise Plus Edition   License expires: 118 days remaining

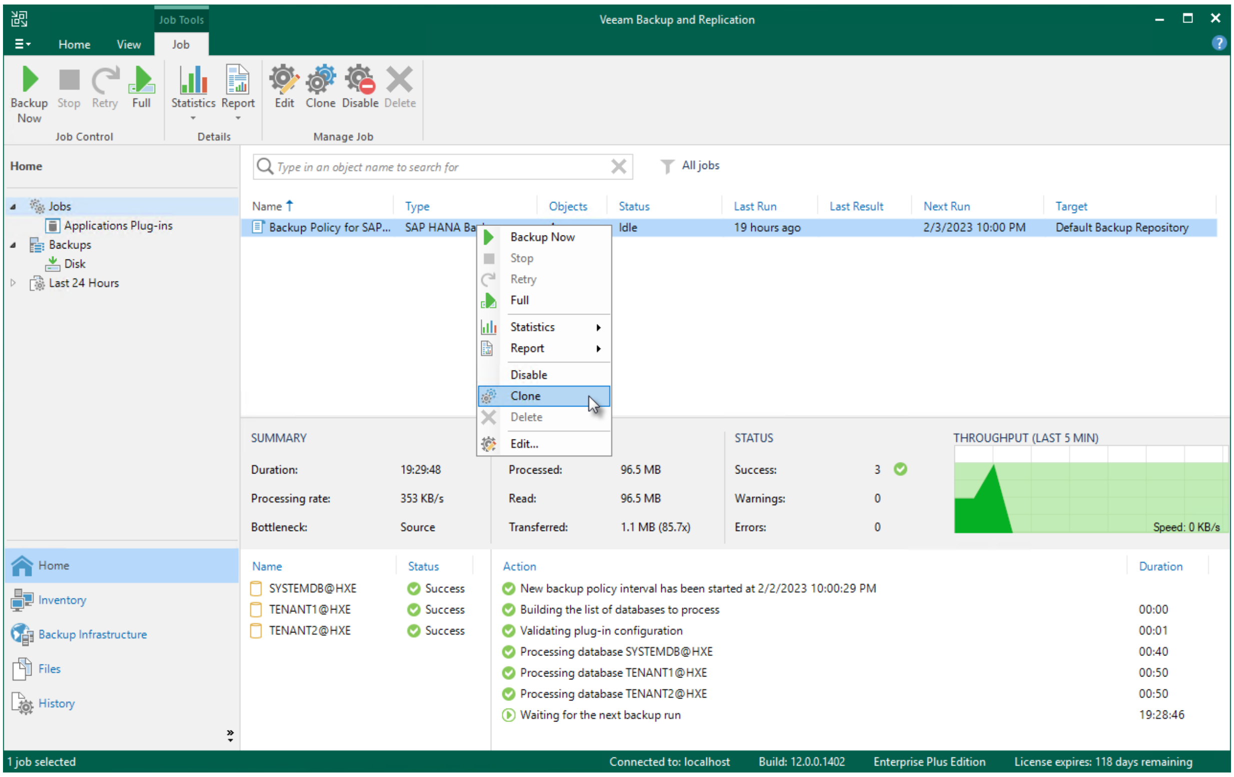
Cloning Backup Policy

You can clone application backup policies configured in Veeam Backup & Replication. For example, you may want to configure a backup policy that will be used as a 'policy template', and use this policy to create multiple policies with similar settings.

To clone a backup policy:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the backup policy and click **Clone** on the ribbon or right-click the backup policy and select **Clone**.
4. After a backup policy is cloned, you can edit all its settings, including the job name.

> **NOTE**
>
> The backup policy cloning functionality is available only in the Enterprise and Enterprise Plus editions of Veeam Backup & Replication.



Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target
Backup Policy for SAP...	SAP HANA Ba...		Idle	19 hours ago		2/3/2023 10:00 PM	Default Backup Repository

SUMMARY

Duration: 19:29:48
Processing rate: 353 KB/s
Bottleneck: Source

Processed: 96.5 MB
Read: 96.5 MB
Transferred: 1.1 MB (85.7x)

STATUS

Success: 3
Warnings: 0
Errors: 0

Name	Status
SYSTEMDB@HXE	Success
TENANT1@HXE	Success
TENANT2@HXE	Success

Action	Duration
New backup policy interval has been started at 2/2/2023 10:00:29 PM	
Building the list of databases to process	00:00
Validating plug-in configuration	00:01
Processing database SYSTEMDB@HXE	00:40
Processing database TENANT1@HXE	00:50
Processing database TENANT2@HXE	00:50
Waiting for the next backup run	19:28:46

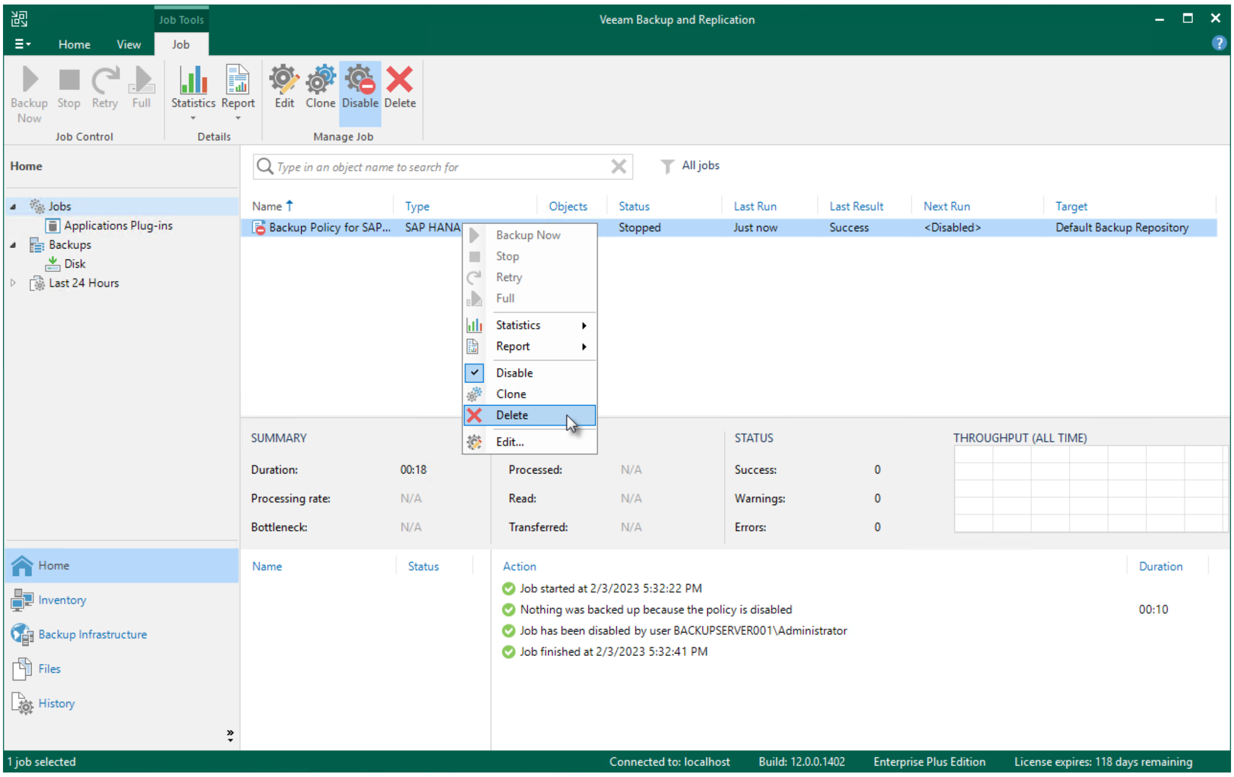
1 job selected   Connected to: localhost   Build: 12.0.0.1402   Enterprise Plus Edition   License expires: 118 days remaining

Deleting Backup Policy

You can permanently remove a disabled application backup policy from Veeam Backup & Replication. Backups created by this backup policy remain on the target location.

To remove an application backup policy:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the application backup policy and click **Disable** on the ribbon or right-click the policy and select **Disable**.
4. Wait for Veeam Backup & Replication to disable the application backup policy, then select the backup policy and click **Delete** on the ribbon or right-click the policy and select **Delete**.



Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target
Backup Policy for SAP...	SAP HANA		Stopped	Just now	Success	<Disabled>	Default Backup Repository

SUMMARY

				STATUS	
Duration:	00:18	Processed:	N/A	Success:	0
Processing rate:	N/A	Read:	N/A	Warnings:	0
Bottleneck:	N/A	Transferred:	N/A	Errors:	0

Name	Status	Action	Duration
		Job started at 2/3/2023 5:32:22 PM	
		Nothing was backed up because the policy is disabled	00:10
		Job has been disabled by user BACKUPSERVER001\Administrator	
		Job finished at 2/3/2023 5:32:41 PM	

1 job selected Connected to: localhost Build: 12.0.0.1402 Enterprise Plus Edition License expires: 118 days remaining

Managing Protected Computers

You can perform the following operations with computers added to the inventory in Veeam Backup & Replication:

- Rescan a protected computer.
- View properties of a protected computer.
- Manage Veeam Plug-in installed on a protected computer:
    - Install Veeam Plug-in on a protected computer.
    - Upgrade Veeam Plug-in on a protected computer.
    - Uninstall Veeam Plug-in on a protected computer.
- Uninstall all Veeam components from a computer.
- Remove a protected computer from a protection group.

Moving Unmanaged Computer to Protection Group

You can quickly move an unmanaged computer to a protection group in the Veeam Backup & Replication inventory. This allows you to start using Veeam Backup & Replication to manage Veeam Plug-in that is already set up to create backups in the Veeam backup repository.

Keep in mind, that you can move an unmanaged computer only to a protection group that includes individual computers.

You can move a computer from the *Unmanaged* protection group to a new protection group or protection group that you have already created.

- When you move an unmanaged computer to a new protection group, Veeam Backup & Replication creates the protection group and adds the computer to this group. In the protection group settings, you can define discovery and deployment options according to which Veeam Backup & Replication will process the added computer.
- When you move an unmanaged computer to an already existing protection group, Veeam Backup & Replication adds this computer to the protection group and starts processing the computer according to discovery and deployment settings defined in the properties of the protection group. Veeam Backup & Replication discovers the added computer, checks whether Veeam Plug-in running on the computer needs upgrade and upgrades Veeam Plug-in if needed.

> NOTE
>
> - After you move a computer to a protection group, data backup for this computer will be performed by a backup job configured in Veeam Backup & Replication. Veeam Plug-in running on the computer will start a new backup chain on a target location specified in the backup job settings. The original backup job configured on the computer will be removed in Veeam Plug-in, and you will not be able to continue the backup chain created with this job.
> - You cannot map an application backup policy configured in Veeam Backup & Replication to a backup chain that was created on a backup repository by Veeam Plug-in operating in the standalone mode.

To move an unmanaged computer to a new protection group:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select the **Unmanaged** node.
3. In the working area, select the necessary computer and click **Move to** > **New protection group** on the ribbon or right click the computer and select **Move to** > **New protection group**.

To move an unmanaged computer to a protection group that is already created in the inventory:

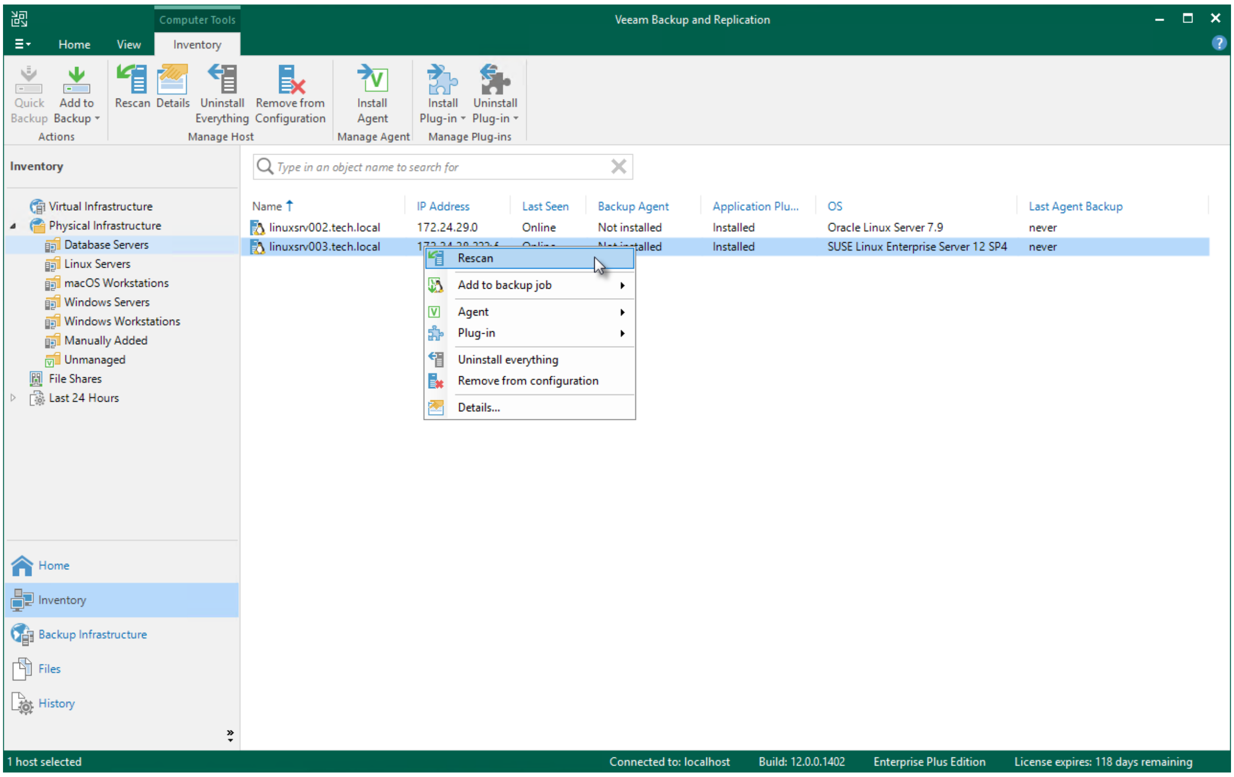
1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select the **Unmanaged** node.
3. In the working area, select the necessary computer and click **Move to** > ***name of the protection group*** on the ribbon or right click the computer and select **Move to** > ***name of the protection group***.

Rescanning Protected Computer

You can rescan protected computers added to the inventory. The rescan operation may be required, for example, if you want to refresh information about the protected computer in the Veeam Backup & Replication database. During the rescan operation, Veeam Backup & Replication communicates to Veeam Installer Service running on the protected computer, retrieves information about the computer and stores this information to the configuration database.

To rescan a protected computer:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select the necessary protection group.
3. In the working area, select the computer and click **Rescan** on the ribbon or right-click the computer and select **Rescan**.



Name	IP Address	Last Seen	Backup Agent	Application Plu...	OS	Last Agent Backup
linuxsrv002.tech.local	172.24.29.0	Online	Not installed	Installed	Oracle Linux Server 7.9	never
linuxsrv003.tech.local	[illegible]	Online	Not installed	Installed	SUSE Linux Enterprise Server 12 SP4	never

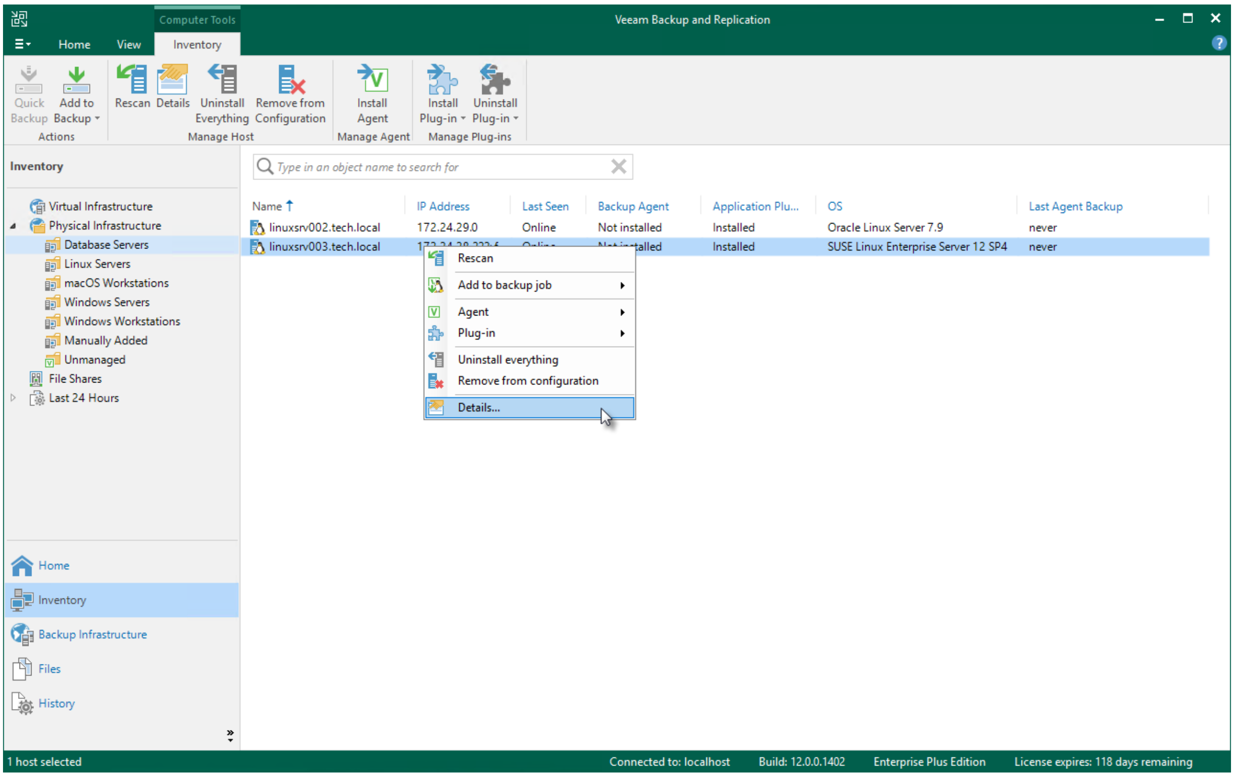
Viewing Properties

You can view detailed information about protected computers. The detailed information provides the following data:

- Host name
- IP address
- Fingerprint (for computers running a Linux OS)
- Key algorithm (for computers running a Linux OS)
- Operating system
- Veeam Plug-in version

To view detailed information about a protected computer:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node.
3. In the working area, select the computer and click **Details** on the ribbon or right-click the computer and select **Details**.



Name	IP Address	Last Seen	Backup Agent	Application Plu...	OS	Last Agent Backup
linuxsrv002.tech.local	172.24.29.0	Online	Not installed	Installed	Oracle Linux Server 7.9	never
linuxsrv003.tech.local	[illegible]	Online	Not installed	Installed	SUSE Linux Enterprise Server 12 SP4	never

1 host selected   Connected to: localhost   Build: 12.0.0.1402   Enterprise Plus Edition   License expires: 118 days remaining

Managing Plug-in

You can use the backup console to manage the following Veeam Plug-ins on a specific computer in the inventory:

- Veeam Plug-in for Oracle RMAN
- Veeam Plug-in for SAP HANA
- Veeam Plug-in for SAP on Oracle

Installing Plug-in

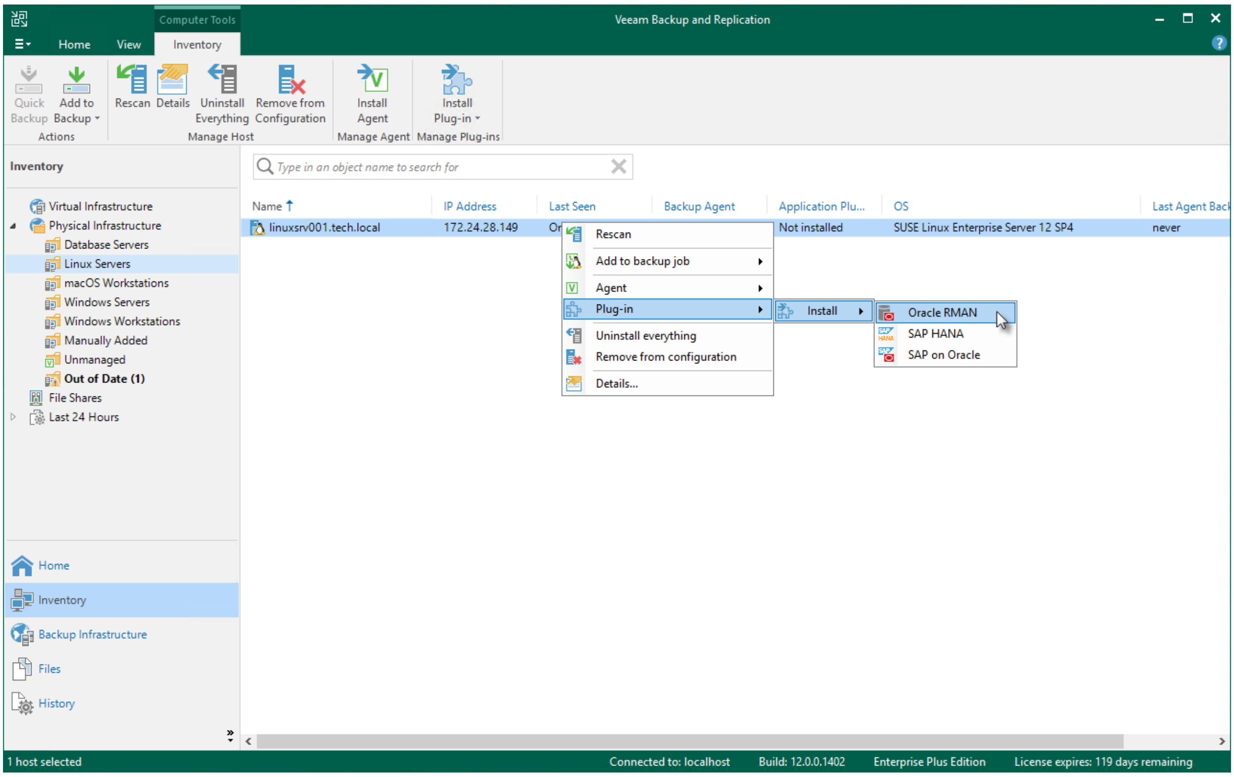
You can install Veeam Plug-in on a specific protected computer in the inventory. This operation may be required, for example, if you want to test the installation process before allowing Veeam Backup & Replication to deploy Veeam Plug-in to all computers included in the protection group.

Before you install Veeam Plug-in, check the following prerequisites:

- The protected computer must be powered on and able to be connected over the network.
- The required version of Veeam Plug-in must be available on the distribution server.

To install Veeam Plug-in on a protected computer:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select the necessary protection group.
3. In the working area, select the necessary computer and click **Install Plug-in** on the ribbon or right-click the computer and select **Plug-in** > **Install and select the plug-in you want to install**.



Name	IP Address	Last Seen	Backup Agent	Application Plu...	OS	Last Agent Back
linuxsrv001.tech.local	172.24.28.149	On		Not installed	SUSE Linux Enterprise Server 12 SP4	never

1 host selected   Connected to: localhost   Build: 12.0.0.1402   Enterprise Plus Edition   License expires: 119 days remaining

Upgrading Plug-in

You can upgrade Veeam Plug-in running on a specific protected computer. This operation may be required, for example, if you did not allow Veeam Backup & Replication to automatically upgrade Veeam Plug-in on computers included in the protection group and want to test the upgrade process on a selected computer first.

Before you upgrade Veeam Plug-in, check the following prerequisites:

- The protected computer must be powered on and able to be connected over the network.
- The required version of Veeam Plug-in must be available on the distribution server.
- There are no running jobs.

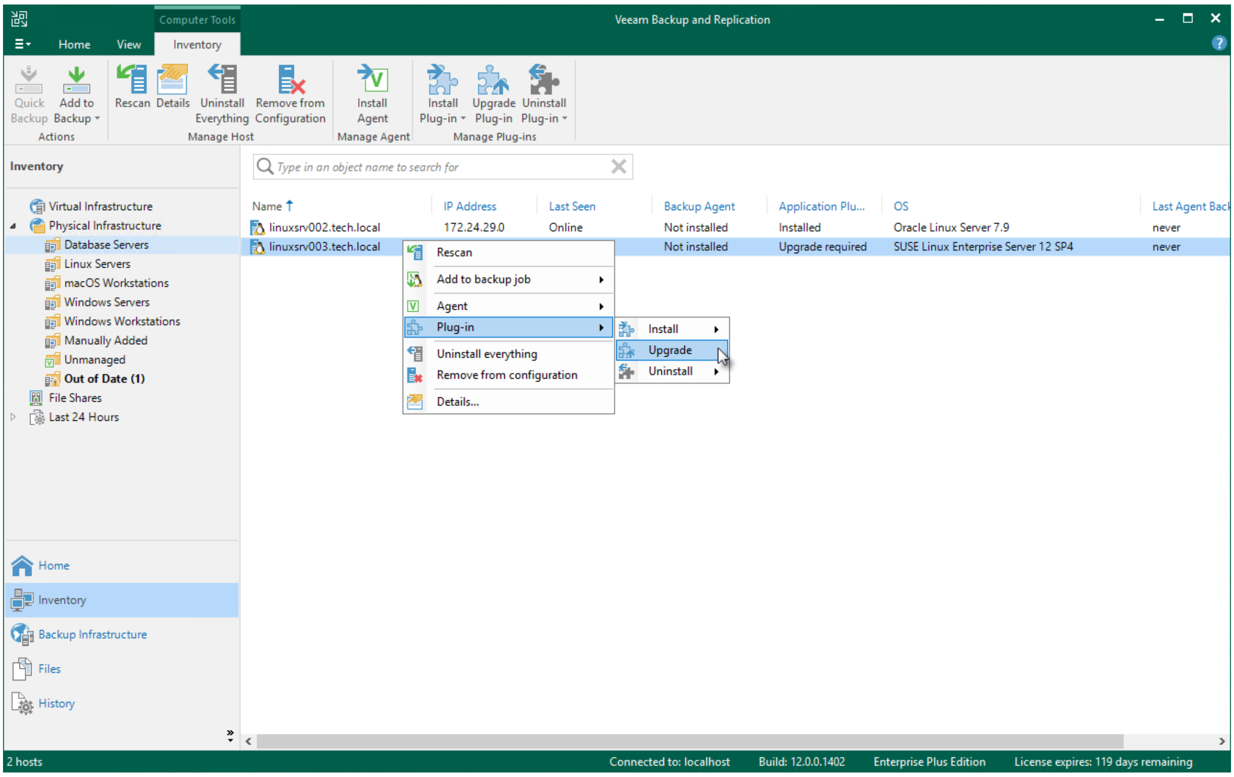
  We recommend that you do not stop running jobs and let them complete successfully. Disable any periodic jobs temporarily to prevent them from starting during the upgrade.

> TIP
>
> During the protected computers discovery process, Veeam Backup & Replication checks the version of Veeam Plug-in running on a protected computer and the version of Veeam Plug-in available on the distribution server. If a newer version of Veeam Plug-in becomes available on the distribution server, and automatic upgrade of Veeam Plug-in is disabled for a protection group, Veeam Backup & Replication puts a computer to the *Upgrade required* state.
>
> In addition, Veeam Backup & Replication includes computers that require upgrade of Veeam Plug-in in the *Out of Date* protection group. You can upgrade Veeam Plug-in on all computers that require upgrade at once. To learn more, see Upgrading Veeam Plug-in on Multiple Computers.

To upgrade Veeam Plug-in on a protected computer:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select the necessary protection group.
3. In the working area, select the necessary computer and click **Upgrade Plug-in** on the ribbon or right-click the computer and select **Plug-in** > **Upgrade**.

> **NOTE**
>
> In some cases, upgrade to the new version of Veeam Plug-in may require computer reboot.



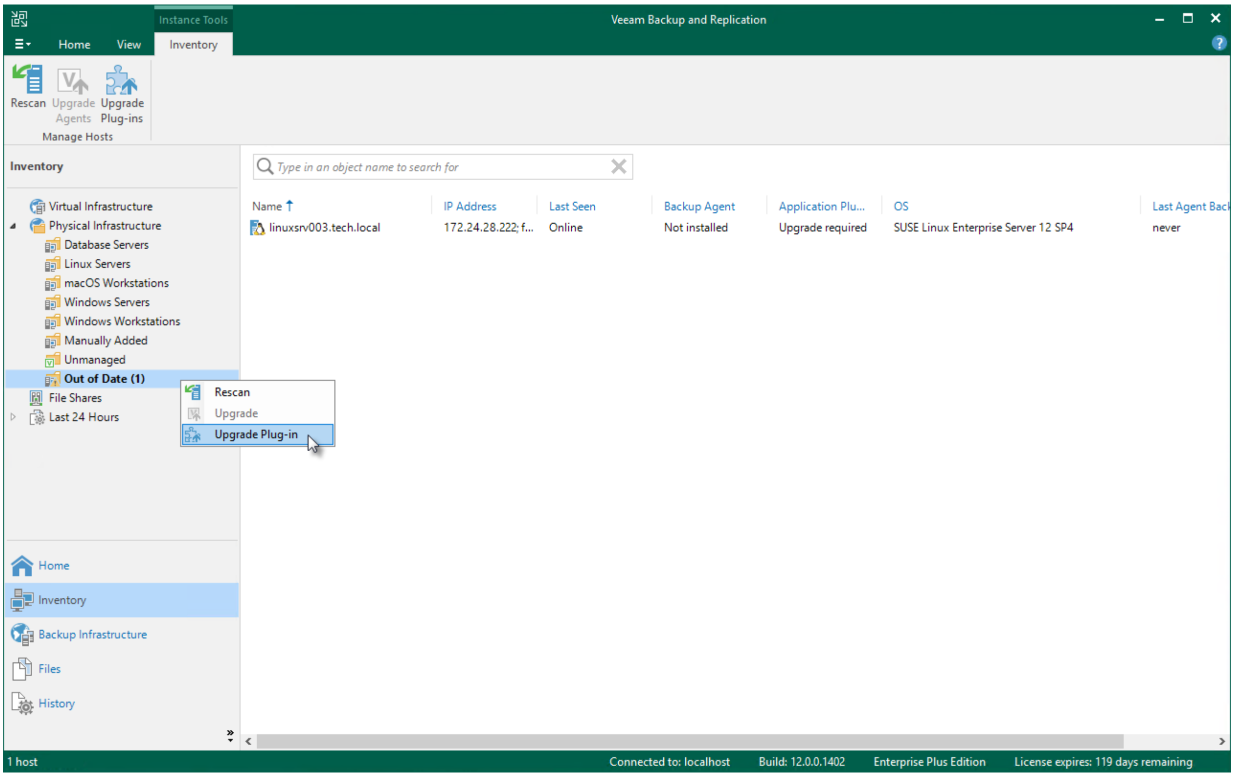
Name	IP Address	Last Seen	Backup Agent	Application Plu...	OS	Last Agent Back
linuxsrv002.tech.local	172.24.29.0	Online	Not installed	Installed	Oracle Linux Server 7.9	never
linuxsrv003.tech.local			Not installed	Upgrade required	SUSE Linux Enterprise Server 12 SP4	never

Upgrading Veeam Plug-in on Multiple Computers

You can upgrade Veeam Plug-in on all computers that require upgrade at once. To upgrade Veeam Plug-in on protected computers:

1. Open the **Inventory** view.
2. In the inventory pane, in the **Physical Infrastructure** node, select the **Out of Date** protection group and click **Upgrade** on the ribbon or right-click the **Out of Date** protection group and select **Upgrade**.

> **NOTE**
>
> In some cases, upgrade to the new version of Veeam Plug-in may require computer reboot.



Name ↑	IP Address	Last Seen	Backup Agent	Application Plu...	OS	Last Agent Back
linuxsrv003.tech.local	172.24.28.222; f...	Online	Not installed	Upgrade required	SUSE Linux Enterprise Server 12 SP4	never

Upgrading from Veeam Plug-in Side

You can also upgrade Veeam Plug-in from the computer side. The process of upgrading differs depending on the Veeam Plug-in:

- Upgrading Veeam Plug-in for Oracle RMAN
- Upgrading Veeam Plug-in for SAP HANA
- Upgrading Veeam Plug-in for SAP on Oracle

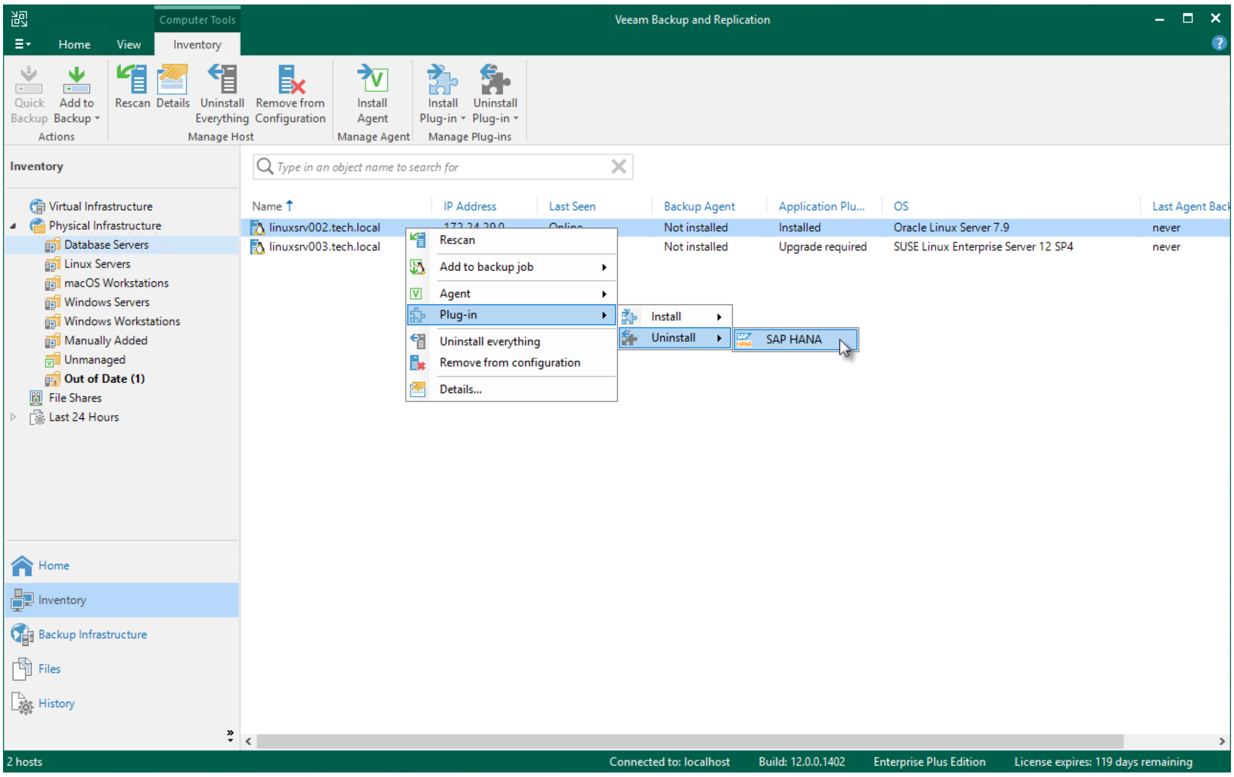
Uninstalling Plug-in

You can remove Veeam Plug-in from a specific protected computer, for example, if you want to reinstall Veeam Plug-in running on the protected computer. When you remove Veeam Plug-in from a protected computer, Veeam Backup & Replication also removes the Veeam Installer Service from this computer.

To uninstall Veeam Plug-in:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select the necessary protection group.
3. In the working area, select the necessary computer and click **Uninstall Plug-in** on the ribbon or right-click the computer and select **Plug-in** > **Uninstall and select Veeam Plug-in you want to uninstall**.
4. In the displayed notification window, click **Yes**.

> NOTE
>
> Mind the following:
>
> - If automatic installation of Veeam Plug-in is enabled in the protection group settings, after you remove Veeam Plug-in from a selected computer, Veeam Backup & Replication will install Veeam Plug-in on this computer during the next rescan job session started by schedule.
> - Prerequisite components installed and used by Veeam Plug-in are not removed during the uninstall process. To remove the remaining components, use the built-in tools directly on this computer (for example, Microsoft Windows Control Panel on the Microsoft Windows computer).



Name	IP Address	Last Seen	Backup Agent	Application Plu...	OS	Last Agent Back
linuxsrv002.tech.local	172.24.29.0	Online	Not installed	Installed	Oracle Linux Server 7.9	never
linuxsrv003.tech.local			Not installed	Upgrade required	SUSE Linux Enterprise Server 12 SP4	never

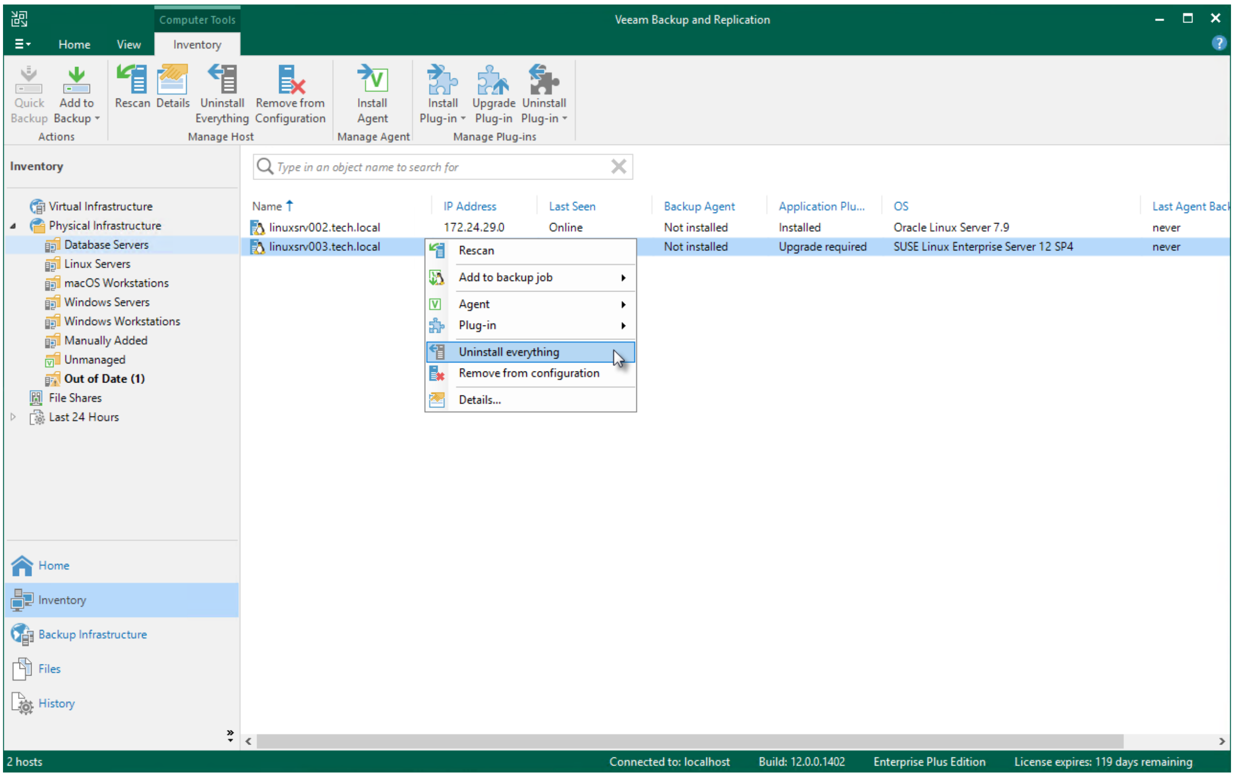
Uninstalling All Veeam Products

You can remove all Veeam components from a specific protected computer, for example, if you want to reinstall Veeam Plug-in running on the protected computer. When you remove Veeam Plug-in from a protected computer, Veeam Backup & Replication also removes the Veeam Installer Service from this computer.

To uninstall Veeam Plug-in:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select the necessary protection group.
3. In the working area, select the necessary computer and click **Uninstall Everything** on the ribbon or right-click the computer and select **Uninstall everything**.
4. In the displayed notification window, click **Yes**.

> NOTE
>
> Mind the following:
>
> - If automatic installation of Veeam Plug-in is enabled in the protection group settings, after you remove Veeam Plug-in from a selected computer, Veeam Backup & Replication will install Veeam Plug-in on this computer during the next rescan job session started by schedule.
> - Prerequisite components installed and used by Veeam Plug-in are not removed during the uninstall process. To remove the remaining components, use the built-in tools directly on this computer (for example, Microsoft Windows Control Panel on the Microsoft Windows computer).



Name	IP Address	Last Seen	Backup Agent	Application Plu...	OS	Last Agent Back
linuxsrv002.tech.local	172.24.29.0	Online	Not installed	Installed	Oracle Linux Server 7.9	never
linuxsrv003.tech.local			Not installed	Upgrade required	SUSE Linux Enterprise Server 12 SP4	never

2 hosts Connected to: localhost Build: 12.0.0.1402 Enterprise Plus Edition License expires: 119 days remaining

Removing Computer from Protection Group

You can remove one or more computers from a protection group, for example, if you do not want to protect these computers with Veeam Plug-in any longer but want to back up data of other computers in the protection group.

When you remove a computer from a protection group, Veeam Backup & Replication removes records about the computer from the Veeam backup console and configuration database but does not uninstall Veeam Plug-in from the computer. You can remove Veeam Plug-in from the computer in advance, before you remove the computer from the protection group. To learn more, see Uninstalling Veeam Plug-in.

Alternatively, you can remove a computer from a protection group, and then uninstall Veeam Plug-in from this computer side. Keep in mind that in this case you will have to uninstall Veeam Plug-in using the built-in tools directly on this computer (for example, Microsoft Windows Control Panel on the Microsoft Windows computer).

> TIP
>
> You can also remove entire protection groups from the Veeam Backup & Replication inventory. When you remove a protection group, you can instruct Veeam Backup & Replication to uninstall Veeam Plug-ins from all protected computers included in this protection group. To learn more, see Removing Protection Group.

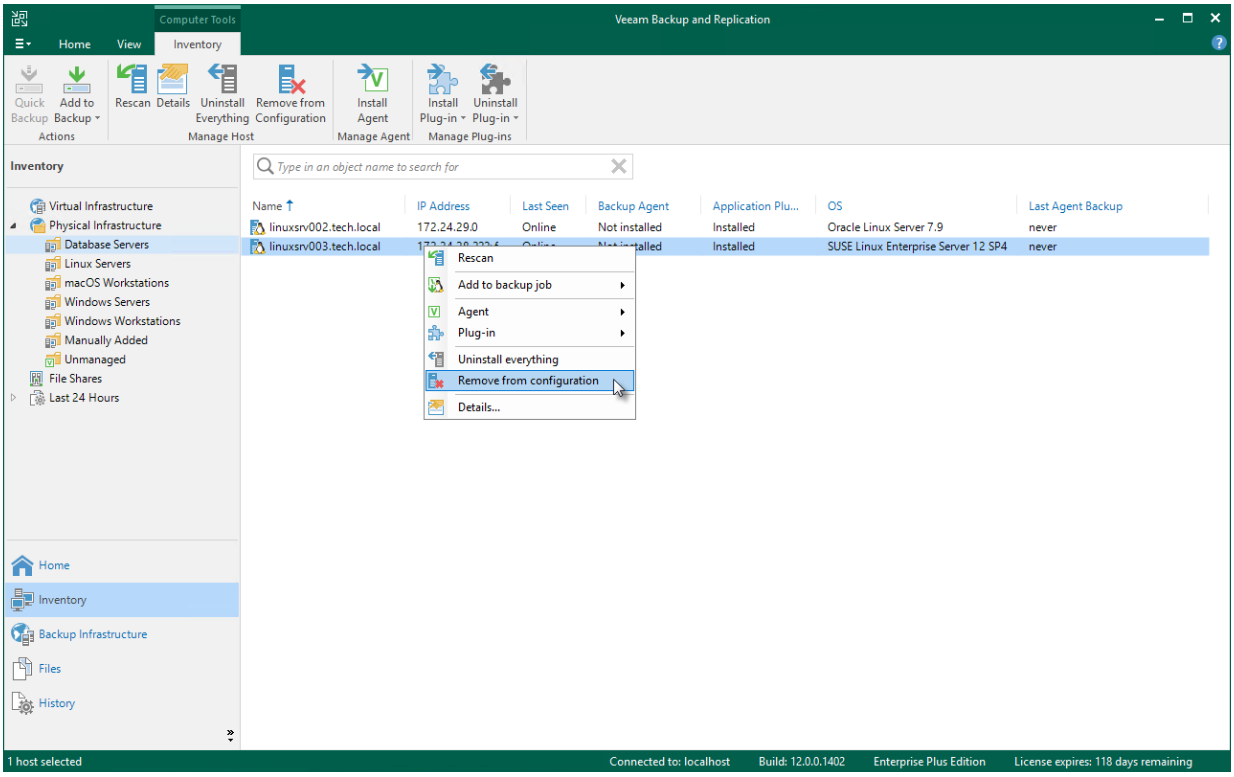
To remove a computer from a protection group:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select the necessary protection group.
3. In the working area, select the necessary computer and click **Remove from configuration** on the ribbon or right-click the computer and select **Remove from configuration**.

Backups created for computers that were removed from a protection group remain intact in the backup location. You can delete this backup data manually later if needed.

NOTE

You cannot remove a computer from the protection group if this computer is a failover cluster node.



Name	IP Address	Last Seen	Backup Agent	Application Plu...	OS	Last Agent Backup
linuxsrv002.tech.local	172.24.29.0	Online	Not installed	Installed	Oracle Linux Server 7.9	never
linuxsrv003.tech.local	[illegible]	Online	Not installed	Installed	SUSE Linux Enterprise Server 12 SP4	never

Alternative Ways to Remove Computer from Protection Group

There are alternative ways to remove computer from protection group that may be suitable for specific situations. Alternative ways of removing computer from protection group differ depending on the type of the protection group that contains the computer you want to remove.

- For a protection group that contains individual computers, edit the protection group and remove the necessary computer at the **Computers** step of the **Edit Protection Group** wizard. To learn more, see Editing Protection Group Settings.

  You can also use this option to remove a computer from the *Manually Added* protection group. This protection group contains computers that you add directly to an application policy. To learn more, see Removing Computer from "Manually Added" Protection Group.

- For a protection group that contains Active Directory objects, edit the protection group and remove the necessary computer account at the **Active Directory** step of the **Edit Protection Group** wizard.

  Alternatively, if the protection group contains a container, organization unit, group or entire domain, you can exclude the computer at the **Exclusions** step of the wizard. To learn more, see Exclude Objects from Protection Group.

- For a protection group that contains computers listed in a CSV file, remove the record about the necessary computer from the CSV file. During subsequent rescan of the protection group, Veeam Backup & Replication will remove the computer from the protection group.

Removing Computer from "Manually Added" Protection Group

Individual computers that you add directly to an application policy are included in the *Manually Added* protection group. When you remove such a computer from the application policy, Veeam Backup & Replication does not remove the computer from the *Manually Added* protection group as well. The computer remains in the *Manually Added* protection group until you remove the computer from this protection group.

To remove a computer from the *Manually Added* protection group, you must edit this protection group and remove the computer at the **Computers** step of the **Edit Protection Group** wizard. To learn more, see Editing Protection Group Settings.

> NOTE
>
> You cannot remove a computer from the *Manually Added* protection group if this computer is added to an application policy.

Managing Application Backups

You can perform administration tasks with backups created on a Veeam backup repository by application backup policies configured in Veeam Backup & Replication. For such backups, Veeam Backup & Replication allows you to perform the same set of operations as for backups created with application policies configured directly on a protected computer. You can perform the following tasks:

- Create a recovery token for a computer.
- Repair a backup.
- Delete an application backup from configuration.
- Delete an application backup from disk.
- Create a backup copy.

Creating Recovery Token

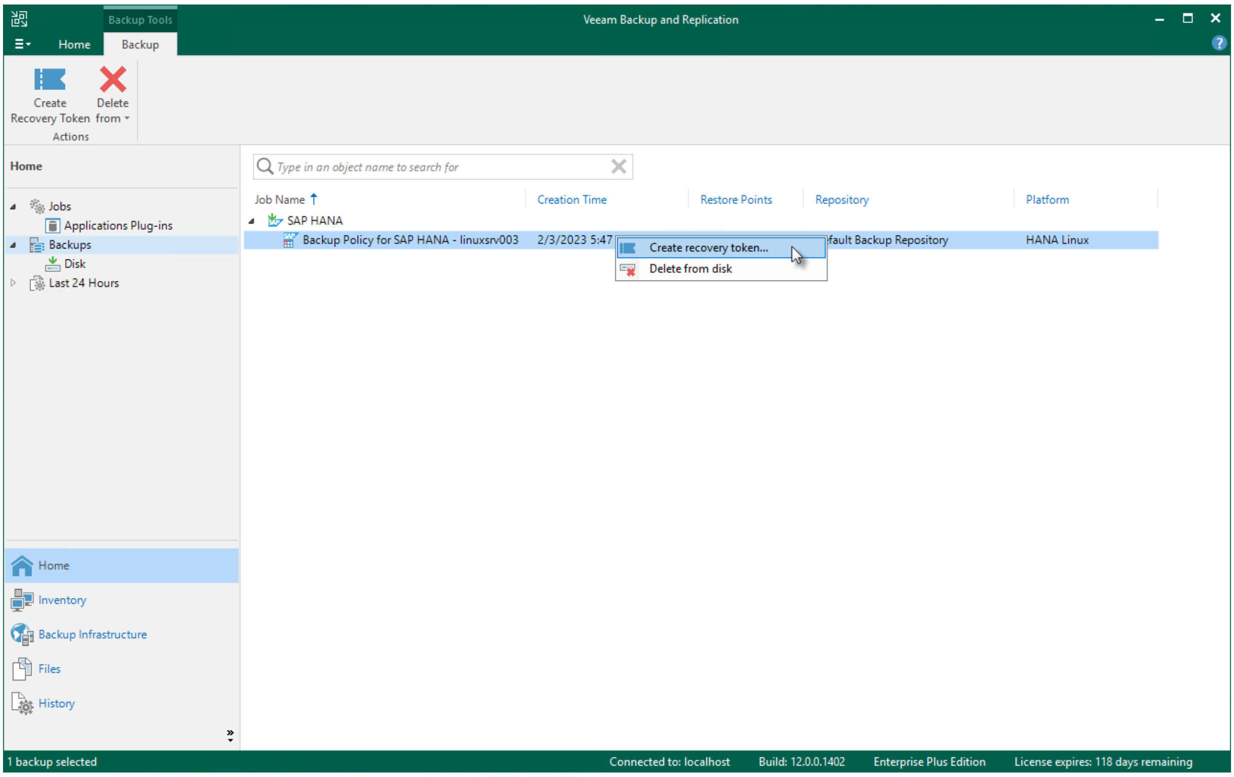
If you want to recover database, you can use the **Create recovery token** operation.

You can generate the recovery token on the Veeam Backup & Replication side. Then, on the computer side, with this recovery token get access to the backup and recover the database that is stored in the backup.

> **TIP**
>
> If you created recovery token for Veeam Agent

To create a recovery token on the Veeam Backup & Replication side:

1. Open the **Home** view.
2. In the inventory pane, click **Backups**.
3. In the working area, right-click the backup and select **Create recovery token**.



To access backup using a recovery token on the Veeam Plug-in side:

1. Set authentication to use the recovery token and enter the token using one of the following commands:
   - [For Veeam Plug-in for SAP HANA and Veeam Plug-in for SAP on Oracle] `--set-backup-for-restore`
   - [For Veeam Plug-in for Oracle RMAN] `--set-auth-data-for-restore`

> TIP
>
> Alternatively, you can get access to the backup using user credentials.

2. Select the backup.

   If you plan to recover database with Veeam Plug-in for Oracle RMAN, use the following command to get the list of backups: `--get-backup-id`.

3. Recover database from the selected backup.

Limitations

Database recovery with recovery token has the following limitations:

- Recovery tokens stay valid for 24 hours.
- You can recover database from the selected backup only.
- Parallel restore from several backups is supported only by Veeam Plug-in for Oracle RMAN.
- During recovery, Veeam Backup & Replication does not stop backup operations.

Repairing Backup

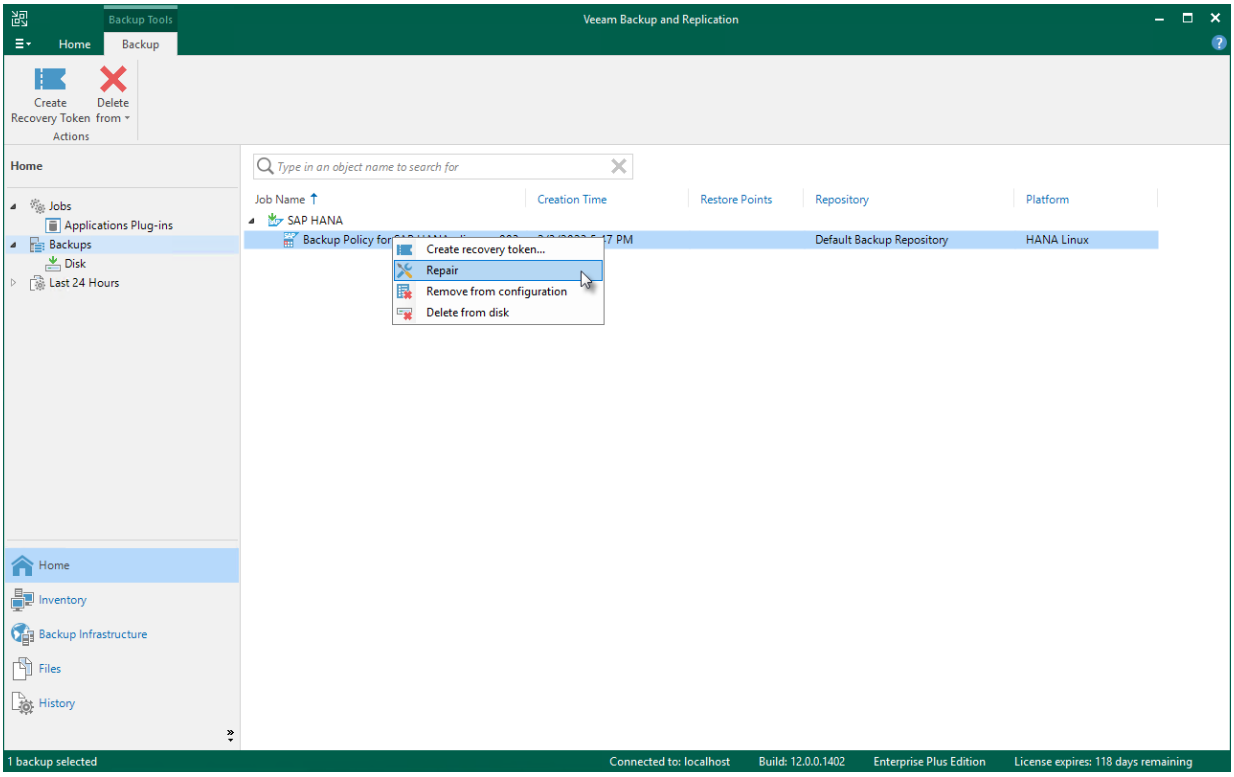
If you want to restore data from an immutable backup that resides in a hardened repository, you can use the **Repair** operation. During this operation, Veeam Backup & Replication will generate a new backup job metadata (VACM) file using information from the backup metadata (VASM) files.

> IMPORTANT
>
> This operation is intended only for a situation where the backup job metadata file has been lost as a result of malware activity or unplanned actions. Re-creation of the backup job metadata file for other purposes is not supported.

Before you start the repair operation, you must disable the backup job that created the backup. Otherwise, Veeam Backup & Replication will display a message notifying that the job must be disabled.

To repair a backup:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. In the inventory pane, select **Backups**.
3. In the working area, select the necessary backup.
4. Press and hold the **[CTRL]** key, right-click the backup and select **Repair**.



Removing Backup from Configuration

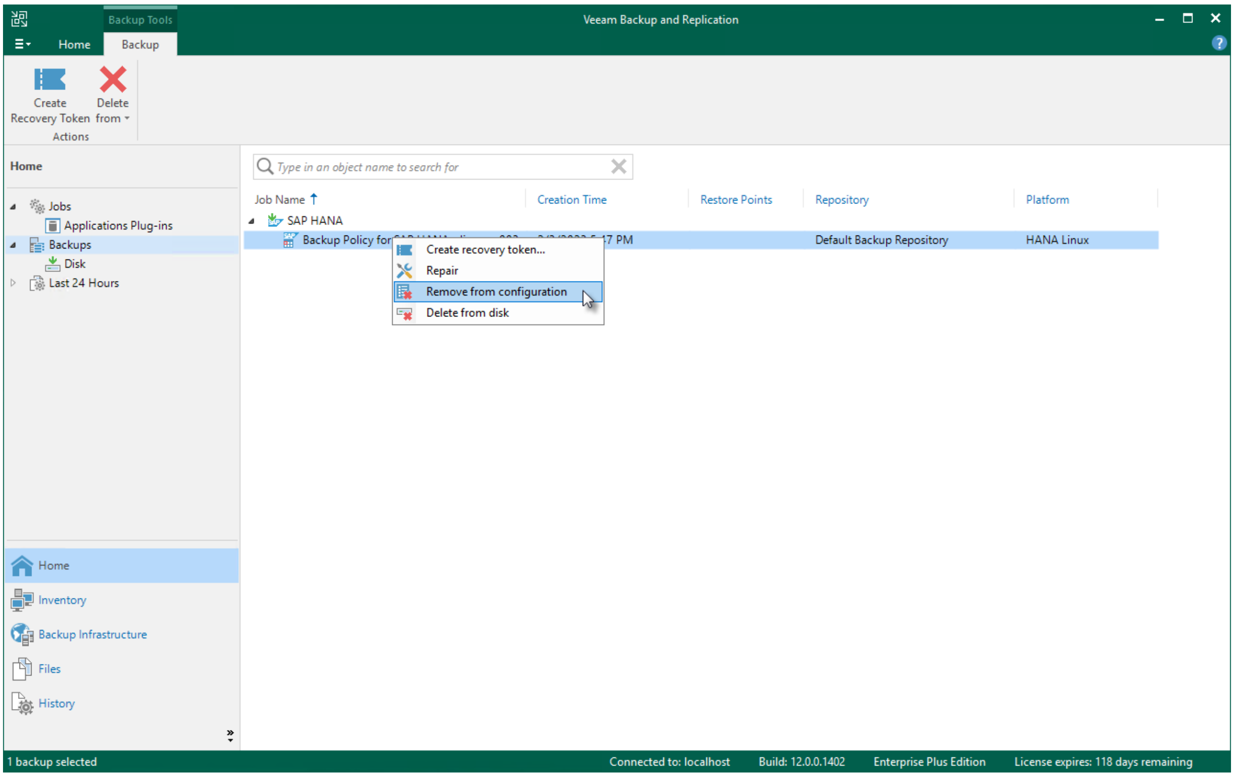
If you want to remove records about Veeam Plug-in backups from the Veeam Backup & Replication console and configuration database, you can use the **Remove from configuration** operation. When you remove a Veeam Plug-in backup from configuration, the actual backup files remain on the backup repository. You can import the backup to the Veeam Backup & Replication at any time later and restore data from it.

> NOTE
>
> Mind the following:
>
> - You can use the Veeam Backup & Replication console to remove backups created by application backup policies in the Veeam backup repository. Backups created on a local drive of a protected computer or in a network shared folder are not displayed in the Veeam backup console.
> - If you remove from configuration a backup of a failover cluster node, all backups of this failover cluster will be removed.

You can remove an entire backup related to an application backup policy or remove specific child backups — backups related to individual computers in the backup.

To remove a Veeam Plug-in backup from configuration:

1. Open the **Home** view.
2. In the inventory pane, click **Backups**.
3. In the working area select and remove the necessary backup:
   - To remove the entire backup related to the application backup policy, select the backup, press and hold the **[CTRL]** key, right-click the backup and select **Remove from configuration**.
   - To remove a backup of a specific computer in the application backup policy, expand the parent backup, select the necessary computer, press and hold the **[CTRL]** key, right-click the backup and select **Remove from configuration**.



Deleting Backup from Disk

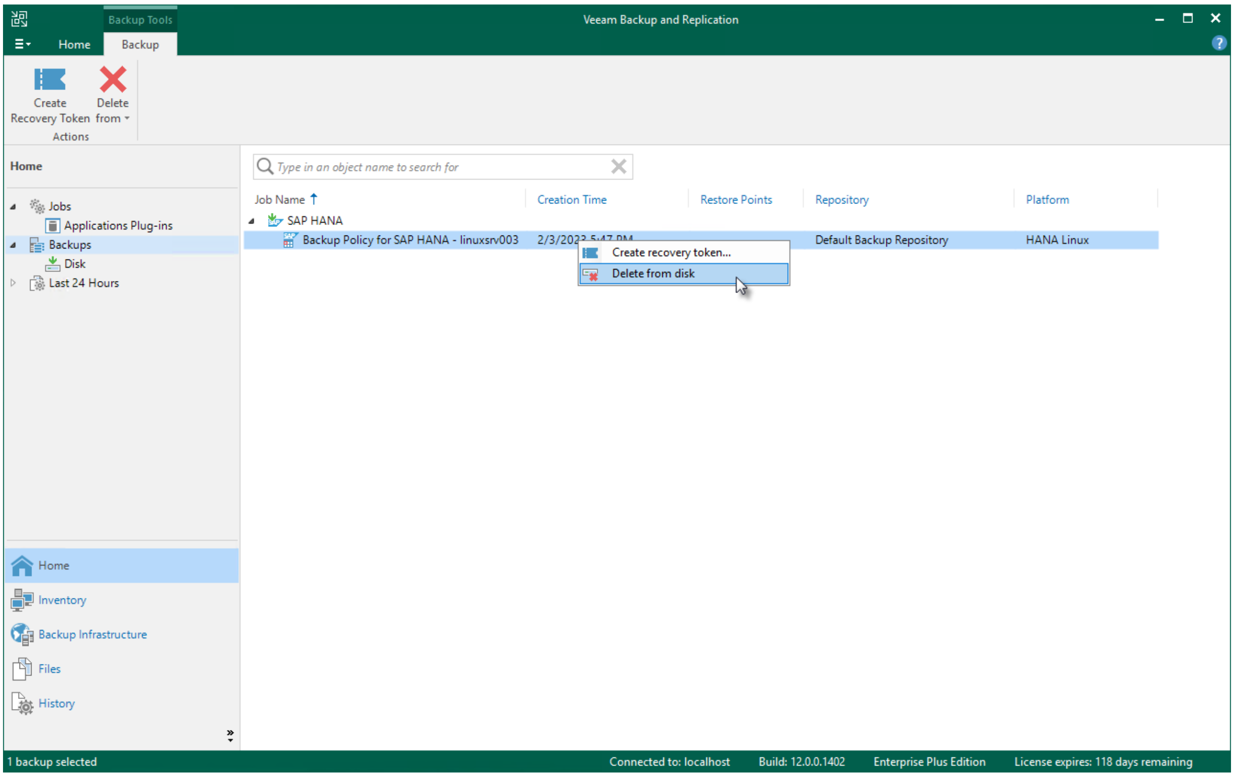
If you want to delete records about backups from the Veeam Backup & Replication console and configuration database and, additionally, delete backup files from the backup repository, you can use the **Delete from disk** operation.

> NOTE
>
> You can use the Veeam Backup & Replication console to remove backups created by application policies on the Veeam backup repository. Backups created on a local drive of a protected computer or in a network shared folder are not displayed in the Veeam Backup & Replication console.

You can remove an entire backup related to an application policy or remove specific child backups — backups related to individual computers in the backup.

To remove an application backup from the backup repository:

1. Open the **Home** view.
2. In the inventory pane, click **Backups**.
3. In the working area, select the backup and click **Delete from** > **Disk** on the ribbon or right-click the backup and select **Delete from disk**.



Job Name	Creation Time	Restore Points	Repository	Platform
SAP HANA				
Backup Policy for SAP HANA - linuxsrv003	2/3/2023 5:47 PM		Default Backup Repository	HANA Linux

1 backup selected   Connected to: localhost   Build: 12.0.0.1402   Enterprise Plus Edition   License expires: 118 days remaining

Creating Backup Copy Job

Veeam Backup & Replication offers the backup copy functionality that allows you to create several instances of the same backup in different locations, whether onsite or offsite. Backup copies have the same format as those created by backup jobs and you can recover your data from them when you need it.

Veeam Backup & Replication fully automates the backup copy process and lets you specify retention settings to maintain the desired number of restore points, as well as full backups for archival purposes. Backup copy is a job-driven process. When enabled, the backup copy job for Veeam Plug-in backups runs continuously. For more details on how it works, see the Backup Copy section of the Veeam Backup & Replication User Guide.

To copy backups to a secondary location, you must configure a backup copy job. The backup copy job defines how, where and when to copy backups. One job can be used to process backups of one or more machines.

You can configure a job and start it immediately or save the job to start it later.

Before creating a job, check prerequisites. Then use the **New Backup Copy Job** wizard to configure a backup copy job.

1. Launch Backup Copy Job wizard.
2. Specify a job name and description.
3. Select backups to process.
4. Define backup copy target.
5. Specify advanced settings.
6. Define backup copy schedule.
7. Finish working with the wizard.

Before You Begin

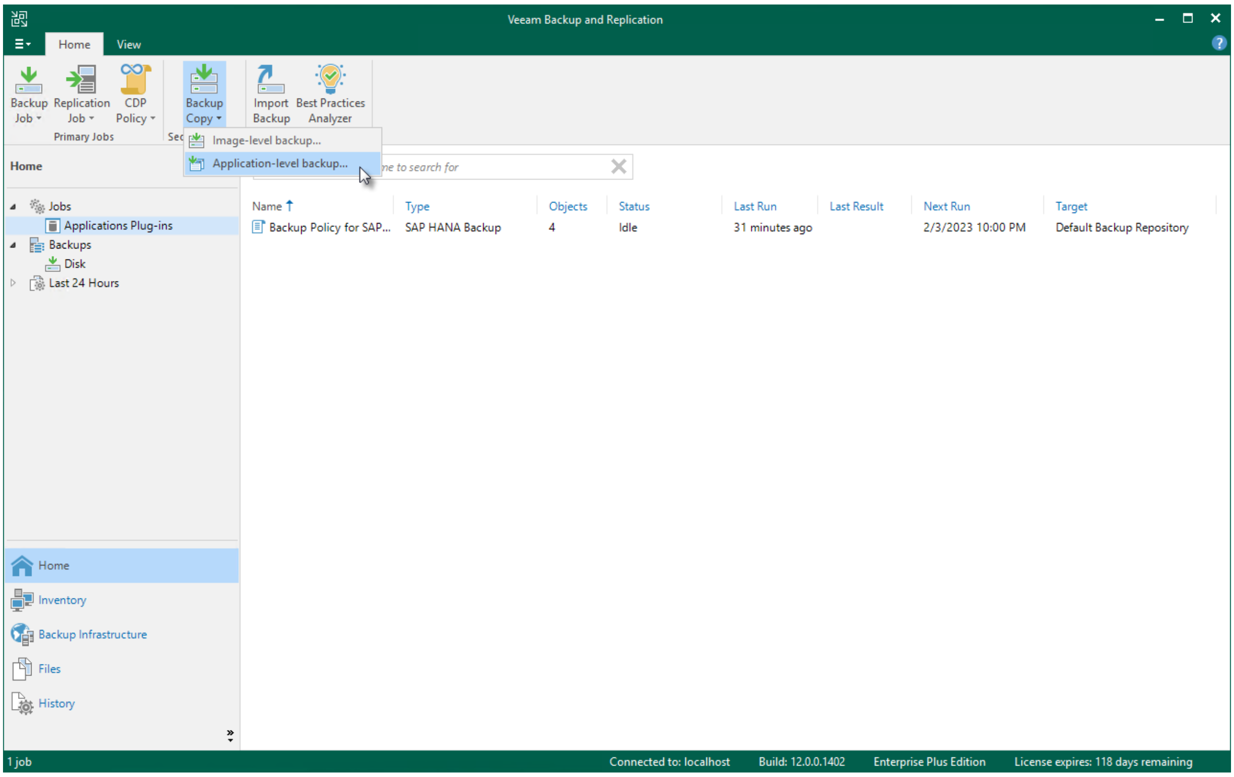
Before you create a backup copy job, check the prerequisites and limitations:

- Backup infrastructure components that will take part in the backup copy process must be added to the backup infrastructure and properly configured. These include source and target backup repositories between which backups must be copied.
- The target backup repository must have enough free space to store copied backups. To receive alerts about low space on the backup repository, configure global notification settings. For more information, see Specifying Other Notification Settings.
- For Veeam Plug-in backup copy jobs, you cannot select a Veeam Cloud Connect repository as a backup copy target.
- If you have upgraded the backup files, make sure that you have upgraded Veeam Plug-in on the source server. If the plug-in is not upgraded to version 12 and you convert backup copy files to backup files, then the next backup job runs will fail.

Step 1. Launch Backup Copy Job Wizard

To create a backup copy job, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. Click the **Backup Copy** tab and select **Application-level backup**.

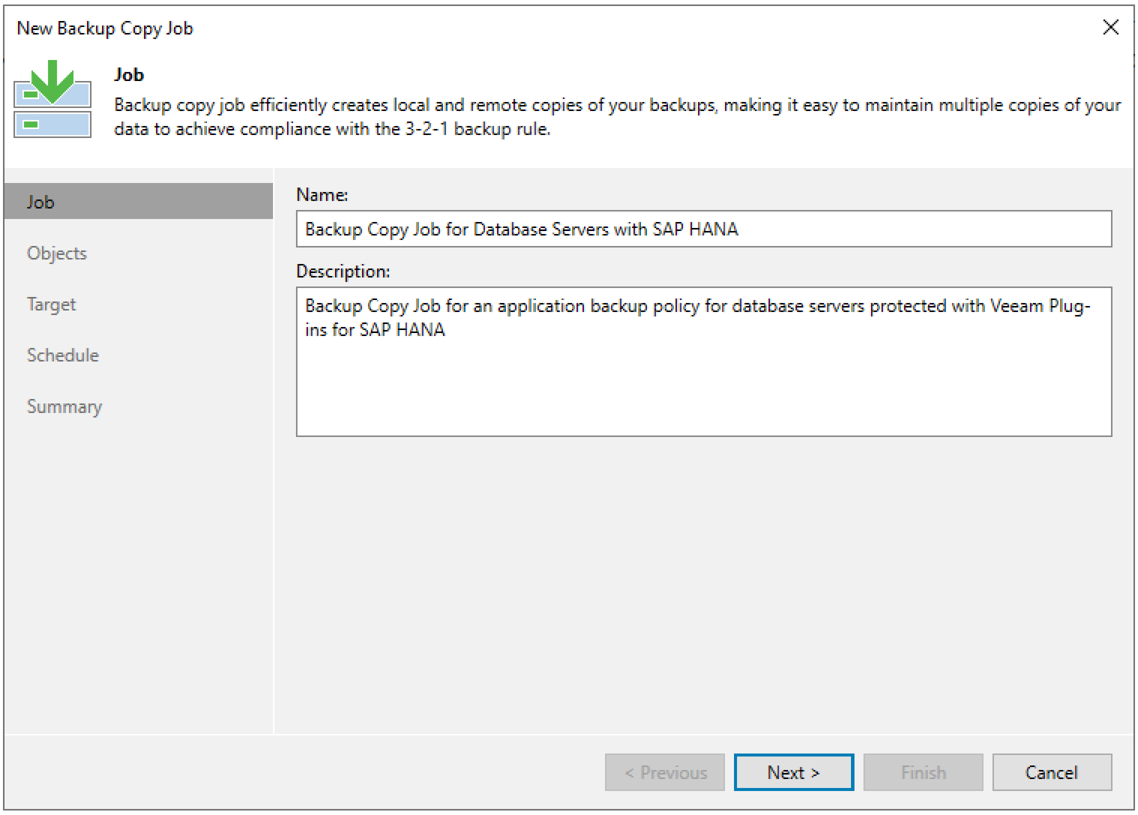


Name ↑	Type	Objects	Status	Last Run	Last Result	Next Run	Target
Backup Policy for SAP...	SAP HANA Backup	4	Idle	31 minutes ago		2/3/2023 10:00 PM	Default Backup Repository

Step 2. Specify Job Name and Description

At the **Job** step of the wizard, specify a name and description for the backup copy job.

1. In the **Name** field, enter a name for the job.
2. In the **Description** field, enter a description for the job. The default description contains information about the user who created the job, date and time when the job was created.



Job

Backup copy job efficiently creates local and remote copies of your backups, making it easy to maintain multiple copies of your data to achieve compliance with the 3-2-1 backup rule.

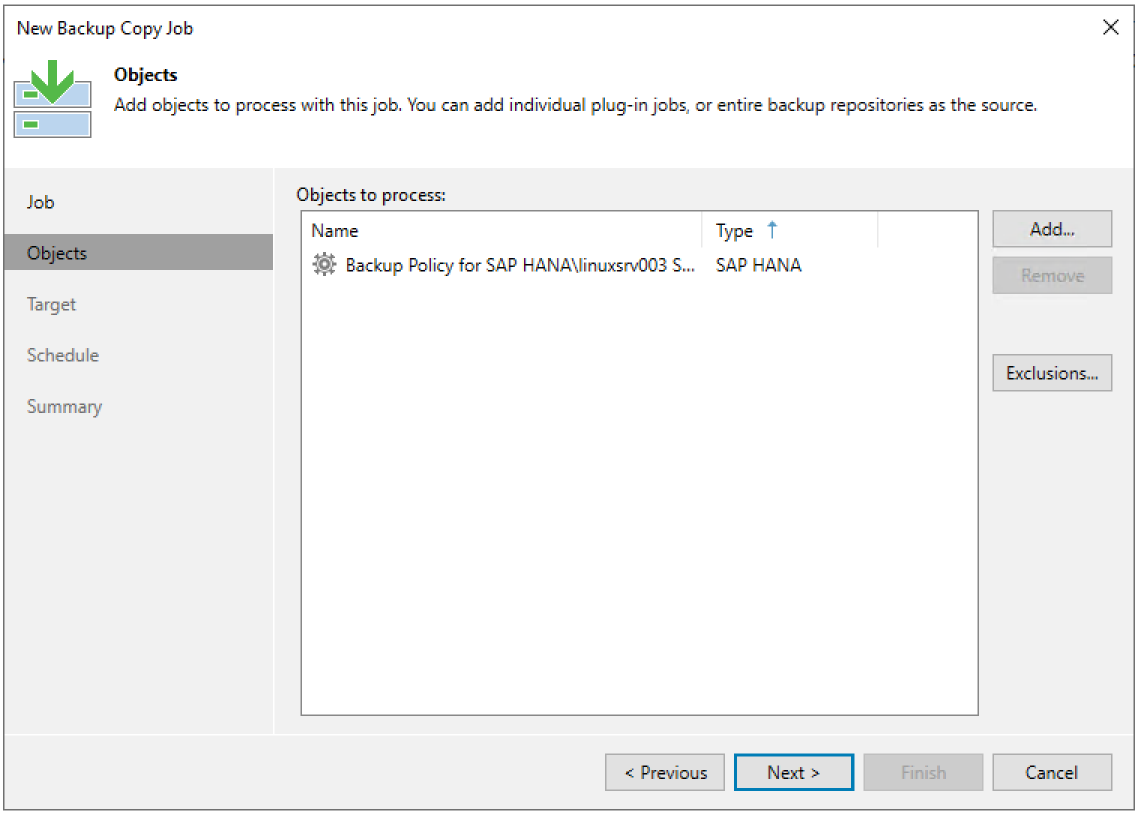
Name: Backup Copy Job for Database Servers with SAP HANA

Description: Backup Copy Job for an application backup policy for database servers protected with Veeam Plug-ins for SAP HANA

Step 3. Select Backups to Process

At the **Object** step of the wizard, select machines whose backups you want to copy to the target repository.

1. Click the **Add** button and select from which entity you want to process the machines.
    - **From jobs**: You can select Veeam Plug-in backup jobs. When a backup copy job runs, Veeam Backup & Replication will search for backup files created by selected jobs.
    - **From repositories**: You can select repositories where Veeam Plug-in backups are stored. When a backup copy job runs, Veeam Backup & Replication will search for backup files created by Veeam Plug-in in selected repositories.
2. Use the **Remove** button if you want to remove selected jobs or repositories from processing.
3. If you have added jobs from a repository and want to exclude from processing some of the backup jobs on the selected repository, click **Exclusions** and select the jobs that you want to exclude.



New Backup Copy Job

Objects

Add objects to process with this job. You can add individual plug-in jobs, or entire backup repositories as the source.

Objects to process:

Name	Type
Backup Policy for SAP HANA\linuxsrv003 S...	SAP HANA

Step 4. Define Backup Copy Target

At the **Target** step of the wizard, configure the target repository settings.

1. From the **Backup repository** list, select a backup repository in the target site where copied backups must be stored. When you select a target backup repository, Veeam Backup & Replication automatically checks how much free space is available on it. Make sure that you have enough free space to store copied backups.

   > IMPORTANT
   >
   > For Veeam Plug-in backup copy jobs, you cannot select a Veeam Cloud Connect repository as a backup copy target.

2. If the target repository contains a Veeam Plug-in backup that was excluded from the backup copy job, and if you don't want to transfer duplicate data, you can use the mapping feature.

   After you configure mapping, if some of backup files (VAB) of the source backup are missing in the target backup copy, these files are uploaded to the target backup copy.

   > NOTE
   >
   > Veeam Plug-in backup copy jobs do not use WAN accelerators.

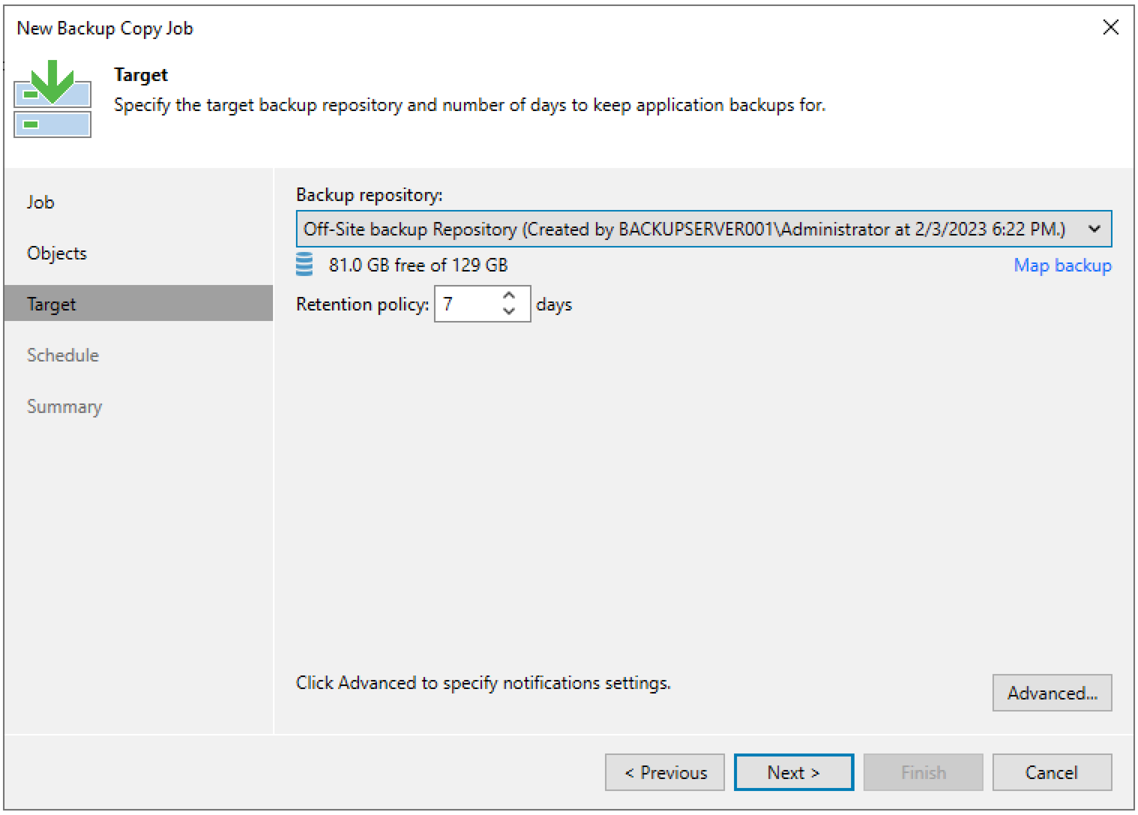
   To map a backup copy job to the backup:

   a. Click the **Map backup** link.

   b. Point the backup copy job to the backup in the target backup repository. Backups in the target backup repository can be easily identified by backup job names. To facilitate search, you can use the search field at the bottom of the window.

   > IMPORTANT
   >
   > - Used account must have access to Veeam backup repositories that you plan to use.
   > - Encryption must be disabled on the repository.
   >
   > Otherwise, the repositories will not be listed as available. To learn how to configure access permissions and encryption settings on repositories, see Access and Encryption Settings on Repositories.

3. You can specify the number of days after which the backup copy will be deleted from the repository. Note that the countdown starts from the moment when source backup has been created.



New Backup Copy Job

Target

Specify the target backup repository and number of days to keep application backups for.

Backup repository: Off-Site backup Repository (Created by BACKUPSERVER001\Administrator at 2/3/2023 6:22 PM.)

81.0 GB free of 129 GB

Retention policy: 7 days

Click Advanced to specify notifications settings.

Step 5. Specify Advanced Settings

At the **Target** step of the wizard, click **Advanced** to configure storage, RPO warning, and notifications settings.

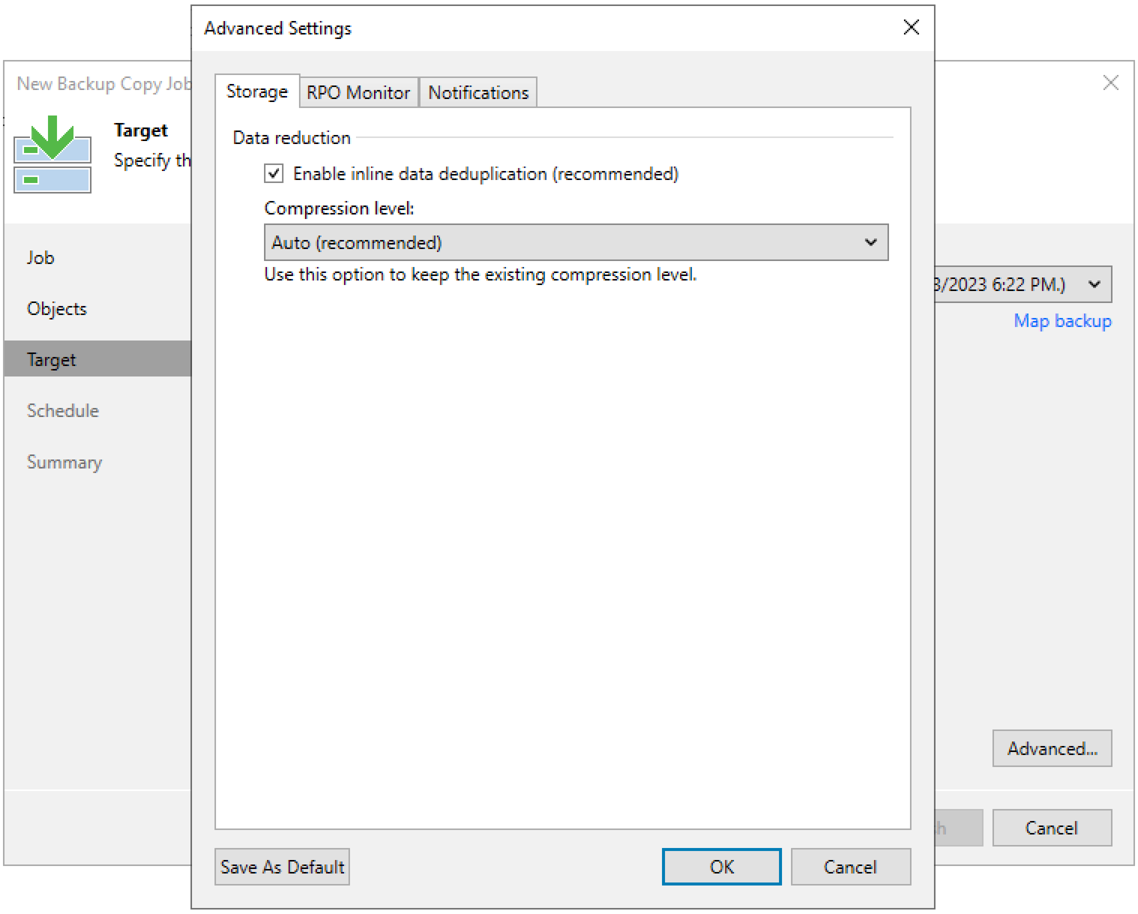
- Storage settings
- RPO warning settings
- Notification settings

Storage Settings

At the **Storage** tab, define compression and deduplication settings.

By default, Veeam Backup & Replication performs deduplication before storing copied data on the target backup repository. Deduplication provides a smaller size of the resulting backup file but may reduce the job performance.

1. You can disable data deduplication. To do this, clear the **Enable inline data deduplication** check box.
2. From the Compression level list, choose a compression level to be used: **Auto**, **None**, **Dedupe-friendly**, **Optimal**, **High** or **Extreme**. The recommended level of compression for backup copy jobs is **Auto**. In this case, Veeam Backup & Replication uses compression settings of the copied backup files. For more information, see Compression and Deduplication.



Advanced Settings

Data reduction

☑ Enable inline data deduplication (recommended)

Compression level:

Auto (recommended)

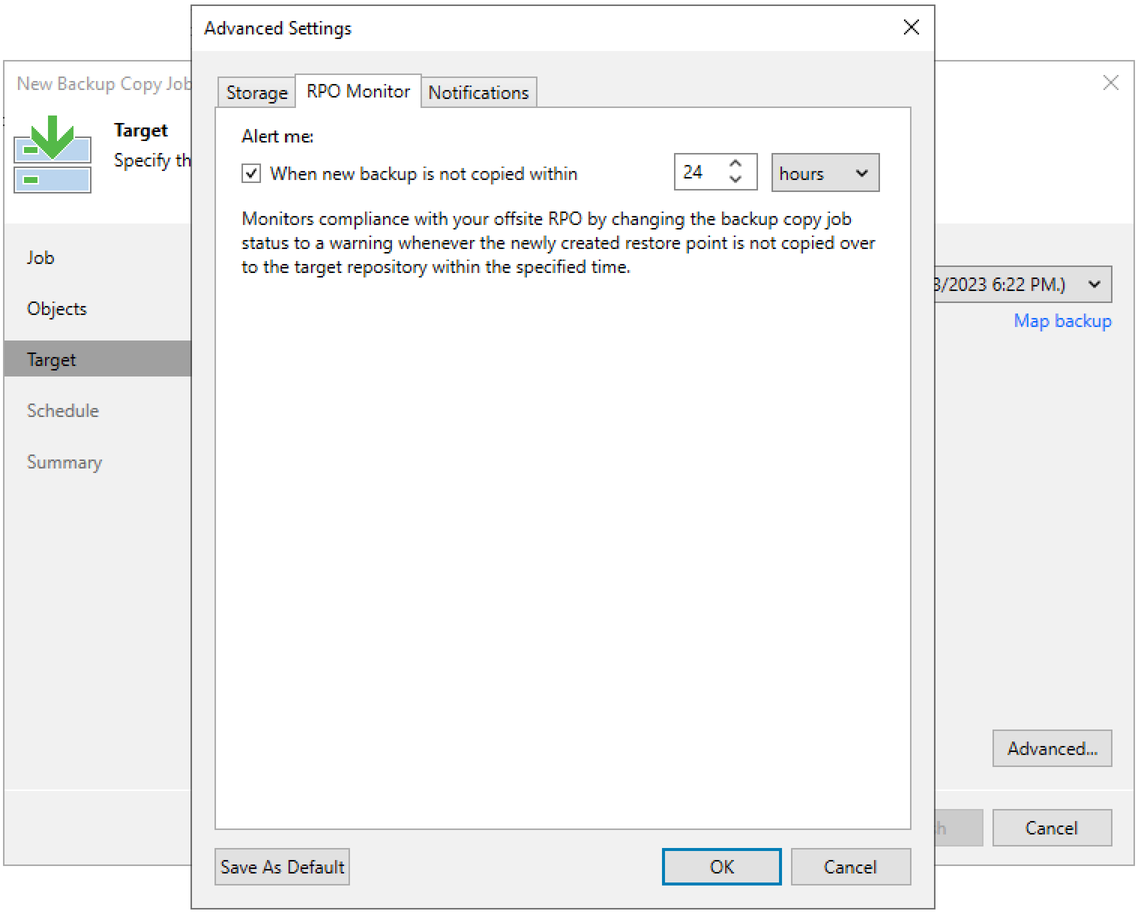
Use this option to keep the existing compression level.

RPO Warning Settings

At the **RPO Monitor** tab, specify RPO warning settings.

Enable the **Warn me if backup is not copied within** check box and specify the time period in **minutes**, **hours**, or **days**.

If the backup copy is not created within the specified time period, the backup copy job will finish with the *Warning* status. The countdown starts from the moment when the required backup is finished and ready to be copied.



Alert me:

☑ When new backup is not copied within 24 hours

Monitors compliance with your offsite RPO by changing the backup copy job status to a warning whenever the newly created restore point is not copied over to the target repository within the specified time.

Notification Settings

At the **Notifications** tab, to specify notification settings for the backup copy job:

1. At the **Target** step of the wizard, click **Advanced**.
2. Click the **Notifications** tab.
3. Select the **Send SNMP notifications for this job** check box if you want to receive SNMP traps when the job completes successfully. SNMP traps will be sent if you specify global SNMP settings in Veeam Backup & Replication and configure software on recipient's machine to receive SNMP traps. For more information, see Specifying SNMP Settings.
4. Select the **Send email notifications to the following recipients** check box if you want to receive notifications by email in case of job failure or success. In the field below, specify a recipient's email address. You can enter several addresses separated by a semicolon.

5. Veeam Backup & Replication sends a consolidated email notification once for the specified backup copy interval. Even if the synchronization process is started several times within the interval, for example, due to job retries, only one email notification will be sent.

6. Email notifications will be sent if you configure global email notification settings in Veeam Backup & Replication. For more information, see Configuring Global Email Notification Settings.

7. At the **Send** at field, specify the time when you want to receive notifications. Note that you will receive a notification on the job status once a day.

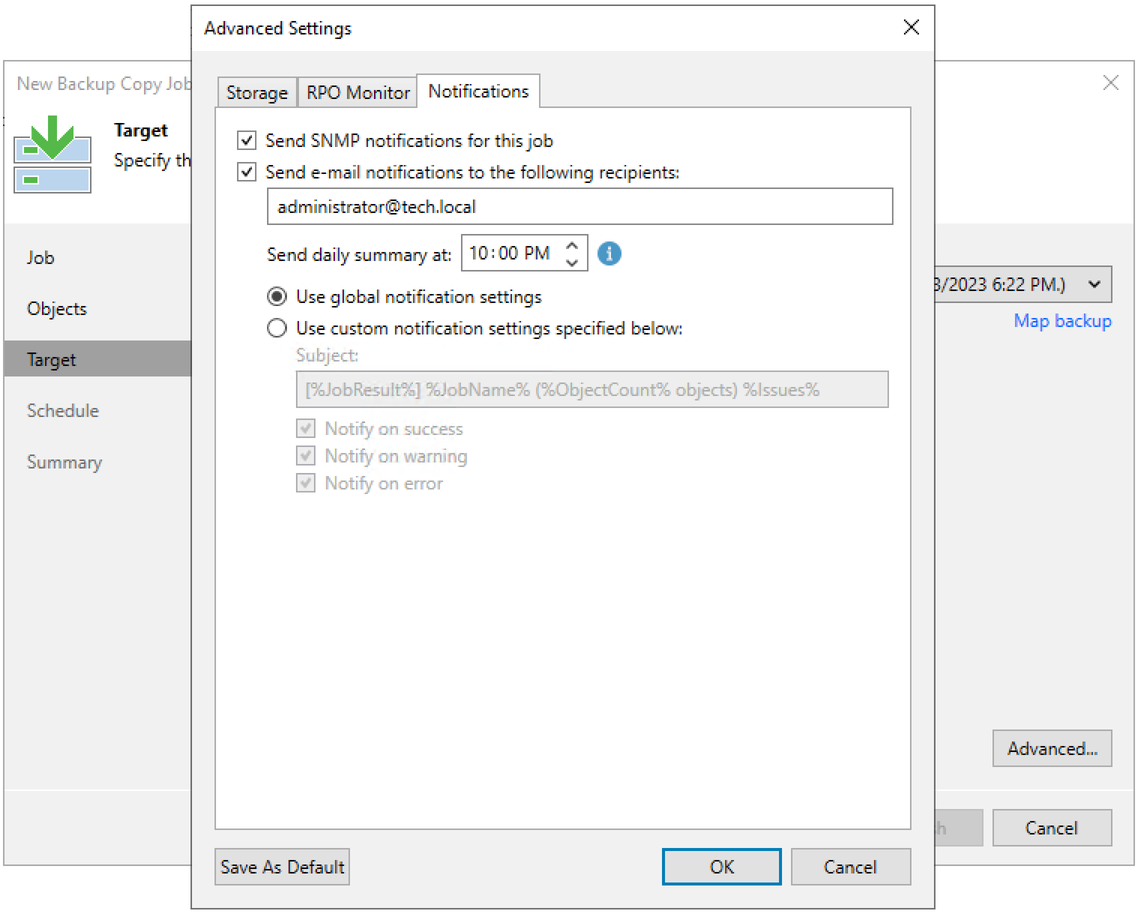
8. You can choose to use global notification settings or specify custom notification settings.

   - To receive a typical notification for the job, select **Use global notification settings**. In this case, Veeam Backup & Replication will apply to the job global email notification settings specified for the backup server. For more information, see Configuring Global Email Notification Settings.

   - To configure a custom notification for a job, select **Use custom notification settings specified below**. You can specify the following notification settings:

     i. In the **Subject** field, specify a notification subject. You can use the following variables in the subject: *%Time%* (completion time), *%JobName%*, *%JobResult%*, *%VmCount%* (number of machines in the job) and *%Issues%* (number of machines in the job that have been processed with the **Warning** or **Failed** status).

     ii. Select the **Notify on success**, **Notify on warning** and **Notify on error** check boxes to receive email notification if data processing within the backup copy interval completes successfully, fails or completes with a warning.



☑ Send SNMP notifications for this job

☑ Send e-mail notifications to the following recipients:

administrator@tech.local

Send daily summary at: 10:00 PM

● Use global notification settings

○ Use custom notification settings specified below:

Subject:

[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

☑ Notify on success

☑ Notify on warning

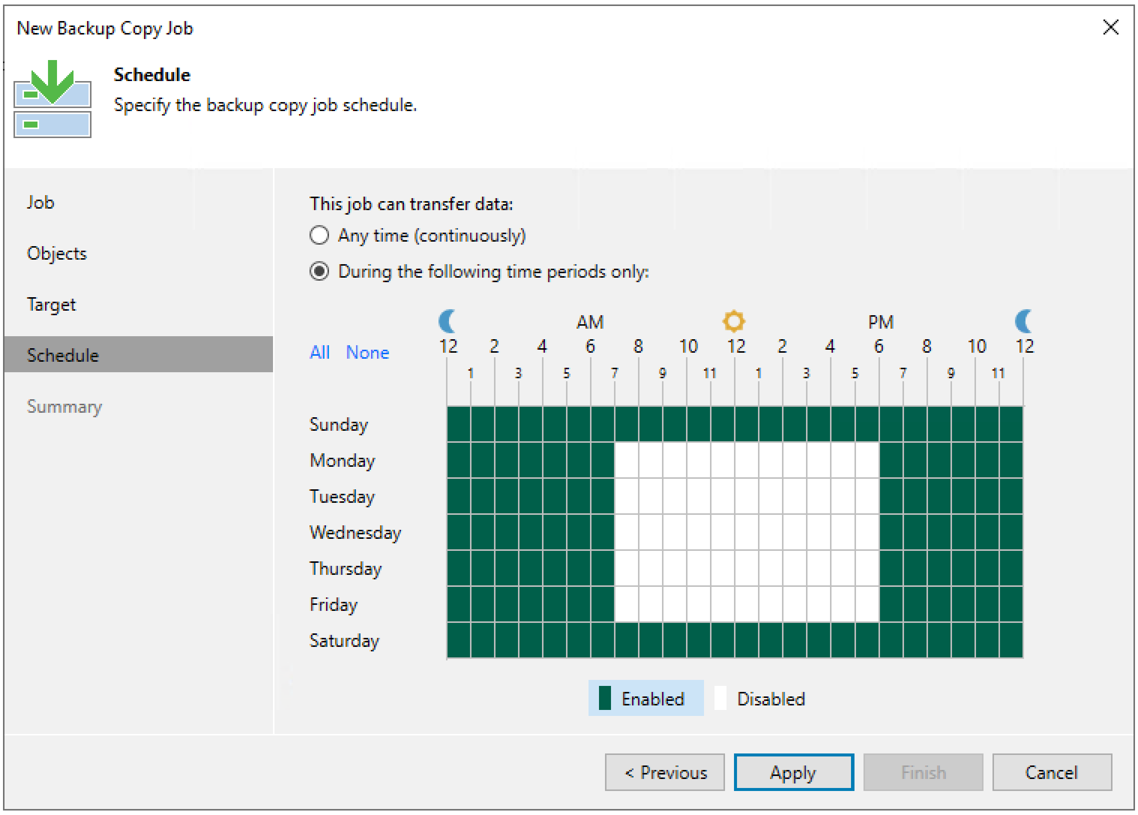
☑ Notify on error

Step 6. Define Backup Copy Schedule

At the **Schedule** step of the wizard, define a time span in which the backup copy job must not transport data between source and target backup repositories. For more information, see Backup Copy Window.

To define a backup window for the backup copy job:

1. Select the **During the following time periods only** option.
2. In the schedule box, select the desired time area.
3. Use the **Enable** and **Disable** options to mark the selected area as allowed or prohibited for the backup copy job.



Schedule

Specify the backup copy job schedule.

This job can transfer data:

○ Any time (continuously)

● During the following time periods only:

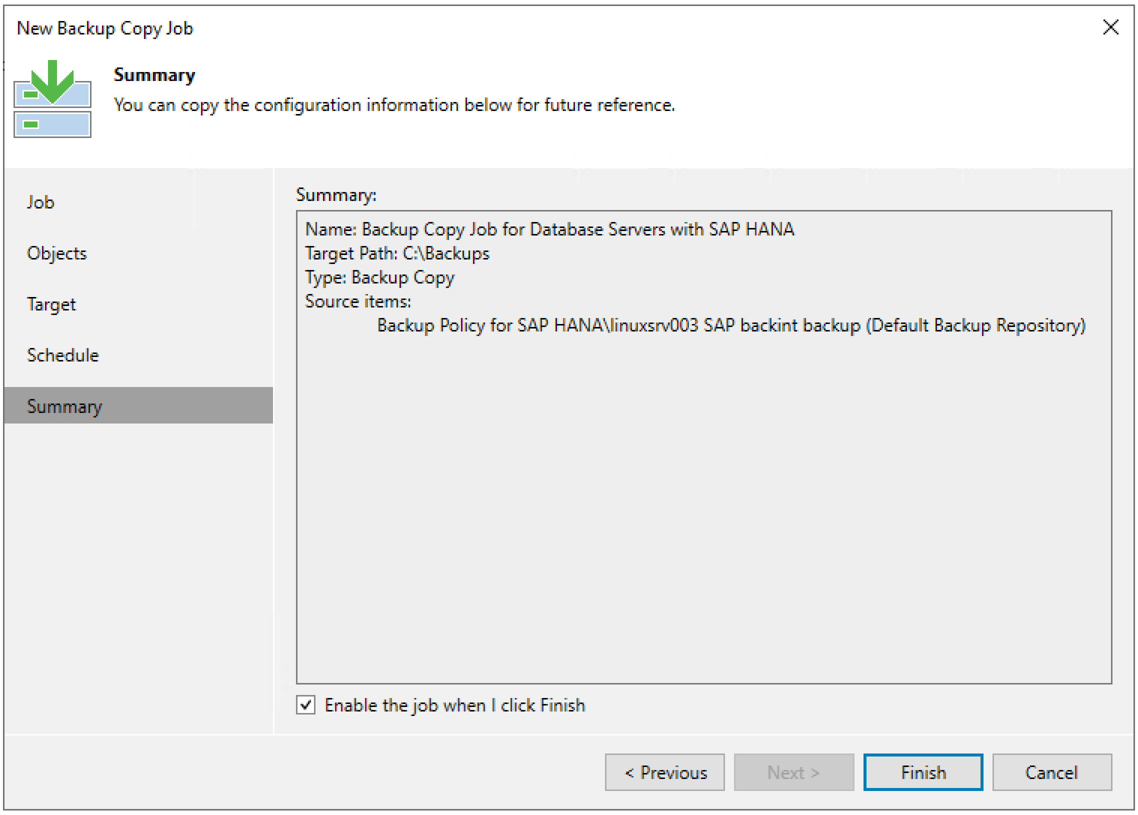
	12 AM	1	2	3	4	5	6	7	8	9	10	11	12 PM	1	2	3	4	5	6	7	8	9	10	11
Sunday	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Monday	■	■	■	■	■	■	■	□	□	□	□	□	□	□	□	□	□	□	■	■	■	■	■	■
Tuesday	■	■	■	■	■	■	■	□	□	□	□	□	□	□	□	□	□	□	■	■	■	■	■	■
Wednesday	■	■	■	■	■	■	■	□	□	□	□	□	□	□	□	□	□	□	■	■	■	■	■	■
Thursday	■	■	■	■	■	■	■	□	□	□	□	□	□	□	□	□	□	□	■	■	■	■	■	■
Friday	■	■	■	■	■	■	■	□	□	□	□	□	□	□	□	□	□	□	■	■	■	■	■	■
Saturday	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■

■ Enabled □ Disabled

Step 7. Review Backup Copy Job Settings

At the **Summary** step of the wizard, complete the procedure of backup copy job configuration.

1. Review details of the backup copy job.
2. Select the **Enable the job when I click Finish** check box if you want to start the job right after you finish working with the wizard.
3. Click **Finish** to close the wizard.



New Backup Copy Job

Summary

You can copy the configuration information below for future reference.

Summary:

Name: Backup Copy Job for Database Servers with SAP HANA
Target Path: C:\Backups
Type: Backup Copy
Source items:
Backup Policy for SAP HANA\linuxsrv003 SAP backint backup (Default Backup Repository)

☑ Enable the job when I click Finish

Reporting

You can view real-time statistics for rescan jobs, as well as application backup policies configured in Veeam Backup & Replication. You can also generate reports with statistics data for performed rescan job or backup job sessions. You can generate reports manually in the Veeam Backup & Replication console or set up Veeam Backup & Replication to send reports automatically by email.

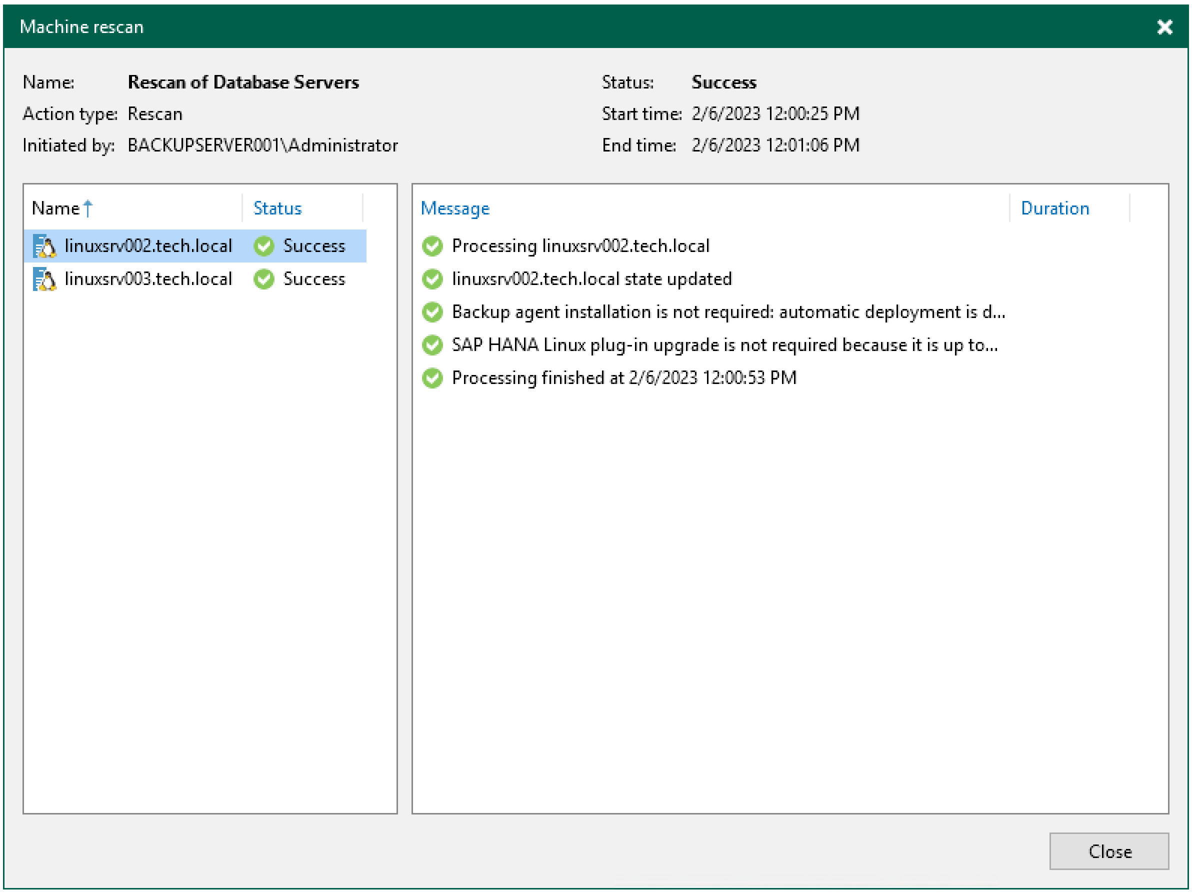
Viewing Rescan Job Statistics

You can view statistics about performed rescan job sessions. When you create a protection group or manually start the discovery process for a protection group or individual protected computer, Veeam Backup & Replication displays statistics for the currently running rescan job session. In the statistics window, Veeam Backup & Replication displays session duration details and a list of operations performed during the job.

In addition to overall rescan job statistics, the statistics window provides information on each protected computer processed within the rescan job session. To view the processing progress for a specific computer, select it in the list on the left.

You can also view statistics for any performed rescan job session. To view rescan job statistics, do one of the following:

- Open the **Inventory** view. In the inventory pane, select the necessary protection group and click **Statistics** on the ribbon or right-click the protection group and select **Statistics**.
- Open the **History** view. In the inventory pane, select the **System** node. In the working area, select the necessary rescan job session and click **Statistics** on the ribbon or right-click the rescan job session and select **Statistics**.



Name: **Rescan of Database Servers**
Action type: Rescan
Initiated by: BACKUPSERVER001\Administrator

Status: **Success**
Start time: 2/6/2023 12:00:25 PM
End time: 2/6/2023 12:01:06 PM

Name ↑	Status
linuxsrv002.tech.local	✓ Success
linuxsrv003.tech.local	✓ Success

Message	Duration
✓ Processing linuxsrv002.tech.local	
✓ linuxsrv002.tech.local state updated	
✓ Backup agent installation is not required: automatic deployment is d...	
✓ SAP HANA Linux plug-in upgrade is not required because it is up to...	
✓ Processing finished at 2/6/2023 12:00:53 PM	

Viewing Rescan Job Report

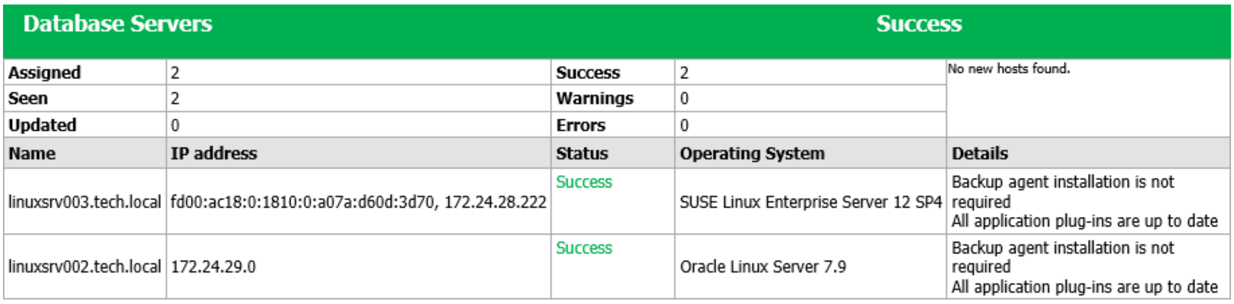
You can generate reports with details about rescan job sessions performed for a specific protection group. The report contains data on the latest rescan job session initiated for the job upon schedule. To generate a report:

1. Open the **Inventory** view.
2. In the inventory pane, select the necessary protection group and click **Report** on the ribbon or right-click the protection group and select **Report**.

The report contains the following data:

- Cumulative session statistics: details of the session performance, including the number of protected computers in the protection group and the number of newly discovered computers.
- Detailed statistics for every protected computer processed within the session: DNS name, IP address and operating system of the protected computer, list of warnings and errors (if any).

> TIP
>
> You can also set up Veeam Backup & Replication to send reports automatically by email. To learn more, see Enabling Email Reporting.



Database Servers **Success**

Assigned	2	**Success**	2	No new hosts found.
Seen	2	**Warnings**	0	
Updated	0	**Errors**	0	
Name	**IP address**	**Status**	**Operating System**	**Details**
linuxsrv003.tech.local	fd00:ac18:0:1810:0:a07a:d60d:3d70, 172.24.28.222	Success	SUSE Linux Enterprise Server 12 SP4	Backup agent installation is not required All application plug-ins are up to date
linuxsrv002.tech.local	172.24.29.0	Success	Oracle Linux Server 7.9	Backup agent installation is not required All application plug-ins are up to date

Viewing Backup Policy Statistics

You can view statistics about application backup policies configured in Veeam Backup & Replication. Veeam Backup & Replication displays statistics in the following way:

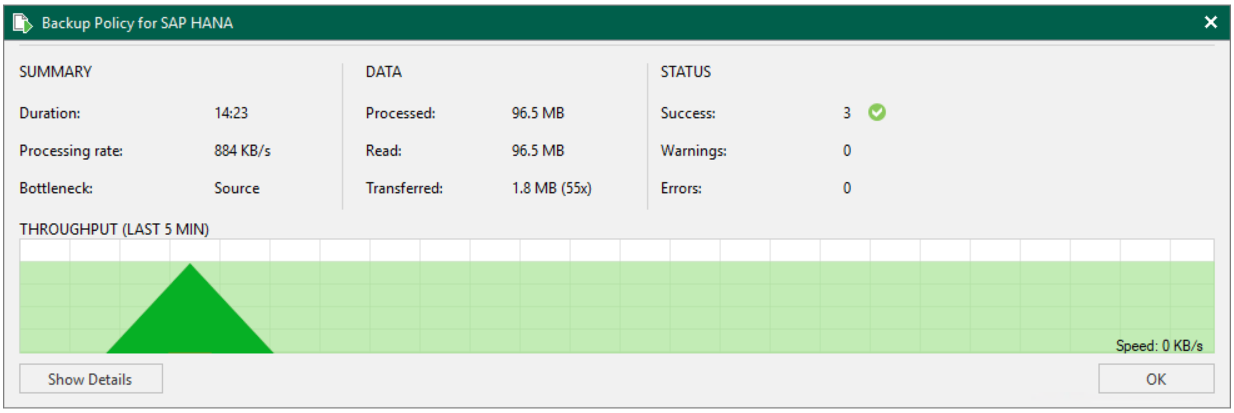
After the application backup policy session statistics becomes available in Veeam Backup & Replication, this statistics appears in the policy statistics window. The job session statistics becomes available in Veeam Backup & Replication at a different time depending on what target for backup files is selected in the backup policy settings:

- If an application backup policy whose settings are defined by the backup policy creates backup files on a Veeam backup repository, backup job session statistics is available in Veeam Backup & Replication on real-time basis.
- If an application backup policy creates backup files on a local drive of a computer, in a network shared folder or in a Veeam Cloud Connect repository, backup job session results are not passed to Veeam Backup & Replication in real time. Statistics for such backup sessions becomes available in Veeam Backup & Replication later, after rescan of a protection group that contains computers added to the backup policy. This process happens regularly upon the discovery schedule defined in the protection group settings.

> TIP
>
> In addition to backup policy statistics, Veeam Backup & Replication displays individual backup session statistics for each computer in the backup policy. You can view these statistics in the **Last 24 Hours** node of the **Home** view and in the **History** view of the Veeam backup console.

To view application backup policy statistics:

1. Open the **Home** view.
2. In the inventory pane, click the **Jobs** node.
3. In the working area, select the necessary statistics:
   - To get statistics for database data backup, double-click the necessary application backup policy. Alternatively, you can select the necessary application backup policy and click **Statistics** > **Instance backup** on the ribbon or right-click the backup policy and select **Statistics** > **Instance backup**.
   - To get statistics for database logs backup, select the necessary application backup policy and click **Statistics** > **Database logs backup** on the ribbon or right-click the backup policy and select **Statistics** > **Database logs backup**.



Backup Policy for SAP HANA

SUMMARY

Duration: 14:23
Processing rate: 884 KB/s
Bottleneck: Source

DATA

Processed: 96.5 MB
Read: 96.5 MB
Transferred: 1.8 MB (55x)

STATUS

Success: 3 ✓
Warnings: 0
Errors: 0

THROUGHPUT (LAST 5 MIN)

Speed: 0 KB/s

Viewing Backup Policy Report

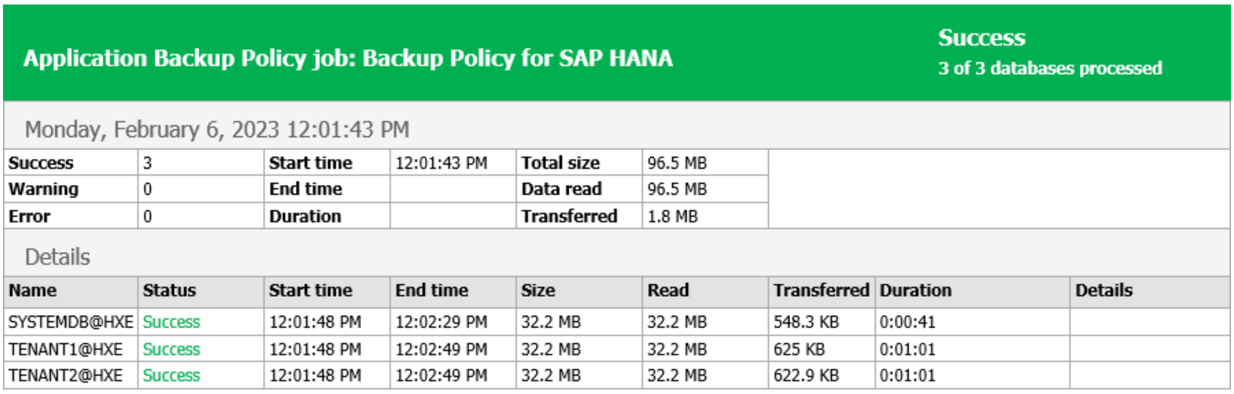
You can generate a report with details about application backup job sessions performed on protected computers added to a backup policy. The report contains data on the latest backup job session initiated for the backup policy. To generate a report:

1. Open the **Home** view.
2. In the inventory pane, click the **Jobs** node.
3. In the working area, select the necessary report:
   - To get report for database data backup, click **Report** > **Instance backup** on the ribbon or right-click the backup policy and select **Report** > **Instance backup**.
   - To get report for database logs backup, click **Report** > **Database logs backup** on the ribbon or right-click the backup policy and select **Report** > **Database logs backup**.

The report contains data on the latest job session:

- Cumulative session statistics: details on the number of protected computers specified in the backup policy settings, the number of computers to which settings of the backup policy are applied, and the number of disconnected computes, details of the session performance, amount of read, processed and transferred data.
- Detailed statistics for every protected computer processed within the session: processing duration details, backup data size, amount of read and transferred data, list of warnings and errors (if any).

> **TIP**
>
> You can also set up Veeam Backup & Replication to send reports automatically by email. To learn more, see Enabling Email Reporting.



Application Backup Policy job: Backup Policy for SAP HANA

Success
3 of 3 databases processed

Monday, February 6, 2023 12:01:43 PM

Success	3	**Start time**	12:01:43 PM	**Total size**	96.5 MB
Warning	0	**End time**		**Data read**	96.5 MB
Error	0	**Duration**		**Transferred**	1.8 MB

Details

Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
SYSTEMDB@HXE	Success	12:01:48 PM	12:02:29 PM	32.2 MB	32.2 MB	548.3 KB	0:00:41	
TENANT1@HXE	Success	12:01:48 PM	12:02:49 PM	32.2 MB	32.2 MB	625 KB	0:01:01	
TENANT2@HXE	Success	12:01:48 PM	12:02:49 PM	32.2 MB	32.2 MB	622.9 KB	0:01:01	

Enabling Email Reporting

You can set up Veeam Backup & Replication to send reports automatically by email. To do this, you must enable and configure global email notification settings in Veeam Backup & Replication. To learn more, see the Configuring Global Email Notification Settings section in the Veeam Backup & Replication User Guide.

In addition, you can enable and configure custom notification settings for a specific protection group, application backup policy. This may be useful if you want to change subject, notification rules or list of recipients for some reports.

Rescan Job Report

By default, after you enable and configure global email notification settings in Veeam Backup & Replication, Veeam Backup & Replication sends rescan job reports at 10:00 PM daily. Veeam Backup & Replication sends a separate report for every protection group that you configured. The report contains cumulative statistics for rescan job sessions performed within the last 24-hour period.

You can specify custom notification settings for a specific protection group. To learn more, see Advanced Settings.

Backup Policy Report

By default, after you enable and configure global email notification settings in Veeam Backup & Replication, Veeam Backup & Replication sends backup policy reports at 10:00 AM daily. Veeam Backup & Replication sends a separate report for every backup policy that you configured. The report contains cumulative statistics for backup job sessions performed for the last 24-hour period on computers to which the backup policy is applied.

You can specify custom notification settings for a specific backup policy. To learn more, see the following sections:

- Notification Settings for Veeam Plug-in for Oracle RMAN
- Notification Settings for Veeam Plug-in for SAP HANA
- Notification Settings for Veeam Plug-in for SAP on Oracle