



Veeam Disaster Recovery Orchestrator

Version 6.0

Operations Guide

April, 2023

© 2023 Veeam Software.

All rights reserved. All trademarks are the property of their respective owners.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means, without written permission from Veeam Software (Veeam). The information contained in this document represents the current view of Veeam on the issue discussed as of the date of publication and is subject to change without notice. Veeam shall not be liable for technical or editorial errors or omissions contained herein. Veeam makes no warranties, express or implied, in this document. Veeam may have patents, patent applications, trademark, copyright, or other intellectual property rights covering the subject matter of this document. All other trademarks mentioned herein are the property of their respective owners. Except as expressly provided in any written license agreement from Veeam, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

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	7
ABOUT THIS DOCUMENT	8
WELCOME TO VEEAM DISASTER RECOVERY ORCHESTRATOR	9
ACCESSING ORCHESTRATOR UI.....	10
CONFIGURING VEEAM DISASTER RECOVERY ORCHESTRATOR.....	13
Managing Permissions	14
Creating Scopes.....	15
Assigning User Roles and Permissions	17
Connecting Veeam Backup & Replication Servers	18
Uninstalling Orchestrator Agents	20
Repairing Orchestrator Agents	23
Connecting Infrastructure.....	26
Connecting Storage Systems.....	26
Connecting VMware vSphere Servers	30
Configuring Notification Settings	33
Step 1. Specify SMTP Settings	33
Step 2. Specify Email Notification Settings	34
Step 3. Subscribe to Notifications.....	35
Managing Inventory Groups.....	36
Allowing Access to Inventory Groups	37
Managing Recovery Locations.....	38
Adding Recovery Locations	40
Configuring Recovery Locations	79
Allowing Access to Recovery Locations	82
Configuring Plan Steps	83
Allowing Access to Plan Steps.....	84
Configuring Default Parameter Settings	85
Managing Credentials	88
Allowing Access to Credentials	89
Adding Credentials	90
Changing Passwords.....	91
Editing Template Jobs	92
Allowing Access to Template Jobs	93
Connecting DataLabs.....	94
Assigning and Configuring DataLabs	95
WORKING WITH ORCHESTRATION PLANS.....	97

Working with Replica Plans.....	98
Creating Replica Plans	98
Editing Replica Plans	111
Testing Replica Plans	111
Running and Scheduling Replica Plans	112
Working with CDP Replica Plans	150
Creating CDP Replica Plans	150
Editing CDP Replica Plans	161
Running and Scheduling CDP Replica Plans	162
Working with Restore Plans	196
Creating Restore Plans.....	196
Editing Restore Plans.....	210
Testing Restore Plans	210
Running and Scheduling Restore Plans	211
Working with Storage Plans	236
Creating Storage Plans.....	236
Editing Storage Plans.....	250
Testing Storage Plans	250
Running and Scheduling Storage Plans.....	251
Working with Cloud Plans.....	284
Creating Cloud Plans	284
Editing Cloud Plans	295
Running and Scheduling Cloud Plans.....	296
Editing Orchestration Plans	316
Configuring Plan Properties	317
Configuring Groups.....	318
Configuring Machines	322
Configuring Steps.....	323
Configuring Step Parameters	324
Testing Orchestration Plans	325
Creating Lab Groups	327
Starting On-Demand Plan Test.....	331
Configuring Test Scheduling	348
Viewing Test Results	360
GENERATING REPORTS.....	362
Managing Templates	363
Generating Plan Definition Report	365
Running Plan Readiness Check.....	368
Viewing DataLab Test Results.....	371

Viewing Plan Execution History	373
Configuring Report Options	375
REVIEWING DASHBOARDS	376
Administration Dashboard	376
Home Page Dashboard	377
ADDING CUSTOM SCRIPTS TO VEEAM DISASTER RECOVERY ORCHESTRATOR	379
Running Custom Scripts in Orchestrator	380
Configuring Common Parameters	382
Configuring Windows Credentials Parameter	383
Adding Credentials Parameter to Your Script	384
Adding Custom Parameters	385
Using Runtime Parameter Variables	386
Capturing Script Errors and Warnings	387
Adding Custom Script Step to Plan	388
APPENDIX A. ORCHESTRATION PLAN STEPS	389
Steps Available	389
Check VM Heartbeat	389
Create Cloud VM	390
Generate Event	391
Ping VM Network	392
Prepare DC for DataLab	393
Process CDP Replica VM	394
Process Replica VM	395
Register VM	396
Restore VM	397
Send Email	398
Shutdown Source VM	399
Start Service	400
Veeam Job Actions	401
Verify DNS Port	402
Verify Domain Controller Port	403
Verify Exchange Mailbox	404
Verify Exchange MAPI Connectivity	406
Verify Exchange Services	407
Verify Global Catalog Port	408
Verify Mail Server Port	409
Verify SharePoint URL	410
Verify SQL Database	411
Verify SQL Port	413

Verify Web Server Port	414
Verify Web Site (IIS).....	415
VM Power Actions	416
Custom Script.....	417
Protect VM Group.....	418
Parameter Variables	419
APPENDIX B. GROUPING AND CATEGORIZATION	421
APPENDIX C. GETTING TECHNICAL SUPPORT	423

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](https://www.veeam.com/documentation-guides-datasheets.html)
- Veeam R&D Forums: forums.veeam.com

About This Document

The guide is designed for IT professionals who plan to use Veeam Disaster Recovery Orchestrator. It is primarily aimed at administrators who manage enterprise environments and lack a flexible scalable automation system. Veeam Disaster Recovery Orchestrator provides a comprehensive set of features to ensure easy execution, testing and documentation of DR plans.

Veeam Disaster Recovery Orchestrator is built on top of Veeam Backup & Replication and Veeam ONE, and this guide assumes that you have a good understanding of these solutions.

Welcome to Veeam Disaster Recovery Orchestrator

Veeam Disaster Recovery Orchestrator (Orchestrator) extends the functionality of Veeam Data Platform by orchestrating recovery processes, with one-click orchestration plans for critical applications, and rich features for documentation and testing.

Orchestrator leverages the recovery capabilities of Veeam Backup & Replication to build disaster recovery workflows, automate recovery processes and eliminate error-prone manual steps. Orchestrator also provides reporting capabilities that let enterprises document their disaster recovery plans to meet compliance requirements. With Orchestrator, you can do the following:

- **Orchestrate recovery** – create workflows to orchestrate recovery operations for both virtual and physical machines to VMware vSphere and Microsoft Azure cloud environments.
- **Automate checks and tests** – schedule checks and tests to automate the verification of orchestration plans, with features such as isolated test labs and comprehensive readiness checks.
- **Meet compliance requirements** – view RPO and RTO achievements on the dashboard and generate automatically updated reports for orchestration plan checks, tests and executions, ensuring that requirements for compliance and audit are met.

Accessing Orchestrator UI

To access the Orchestrator UI, perform the following steps:

1. In a web browser, navigate to the Orchestrator UI web address.

The address consists of an FQDN of the Orchestrator server and the website port specified during installation (by default, **9898**). Note that the Orchestrator UI is available over HTTPS.

`https://<hostname>:<port>`

IMPORTANT

Internet Explorer is no longer supported. To access the Orchestrator UI, use Microsoft Edge, Google Chrome or Mozilla Firefox.

2. If you log in for the first time, specify credentials of the local Administrator who performed Orchestrator installation. The user name must be specified in the *DOMAIN\USERNAME* format.

To authenticate using the credentials provided when logging into the system, click **Log in as current user**.

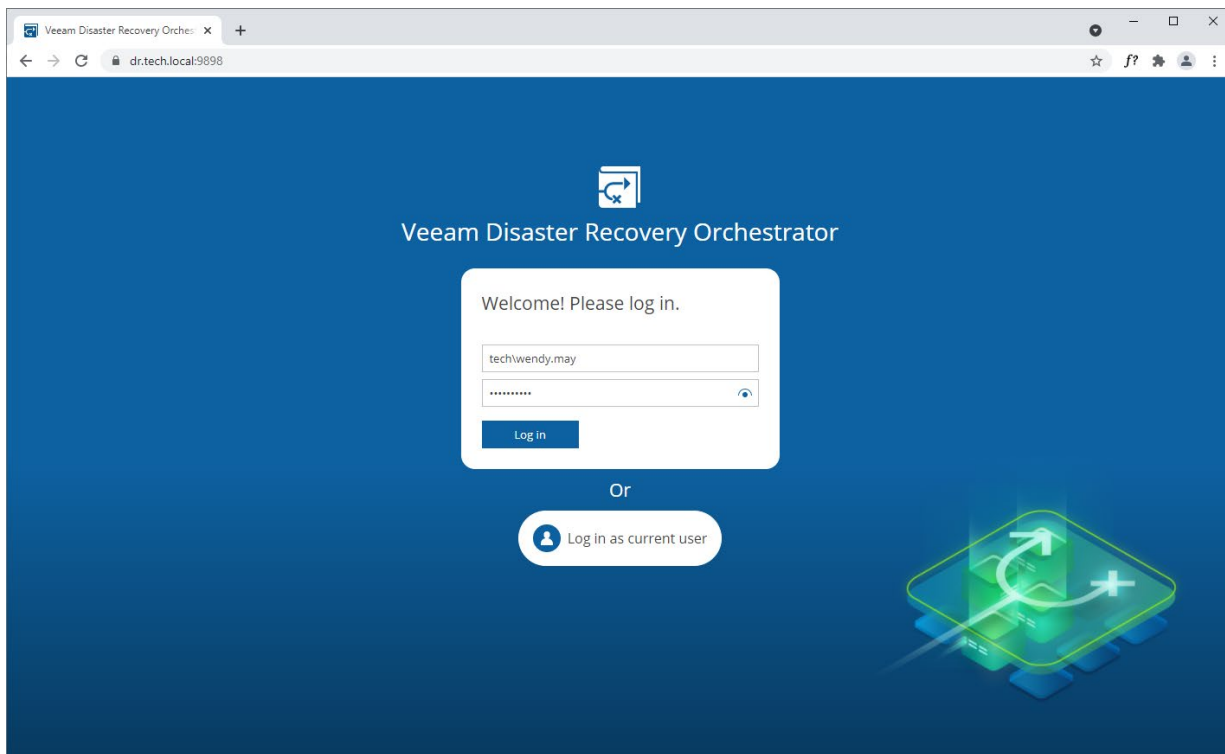
TIP

To be able to log in as the current user, you must first do the following:

1. Complete the Initial Configuration Wizard as described in the Veeam Disaster Recovery Orchestrator Deployment Guide, section [After You Install](#).
2. Enable the **Automatic logon with current user name and password** option in the security setting of your browser.

In future, you can configure users and roles to grant access to the Orchestrator UI. For more information, see the Veeam Disaster Recovery Orchestrator Operations Guide, section [Assigning User Roles and Permissions](#).

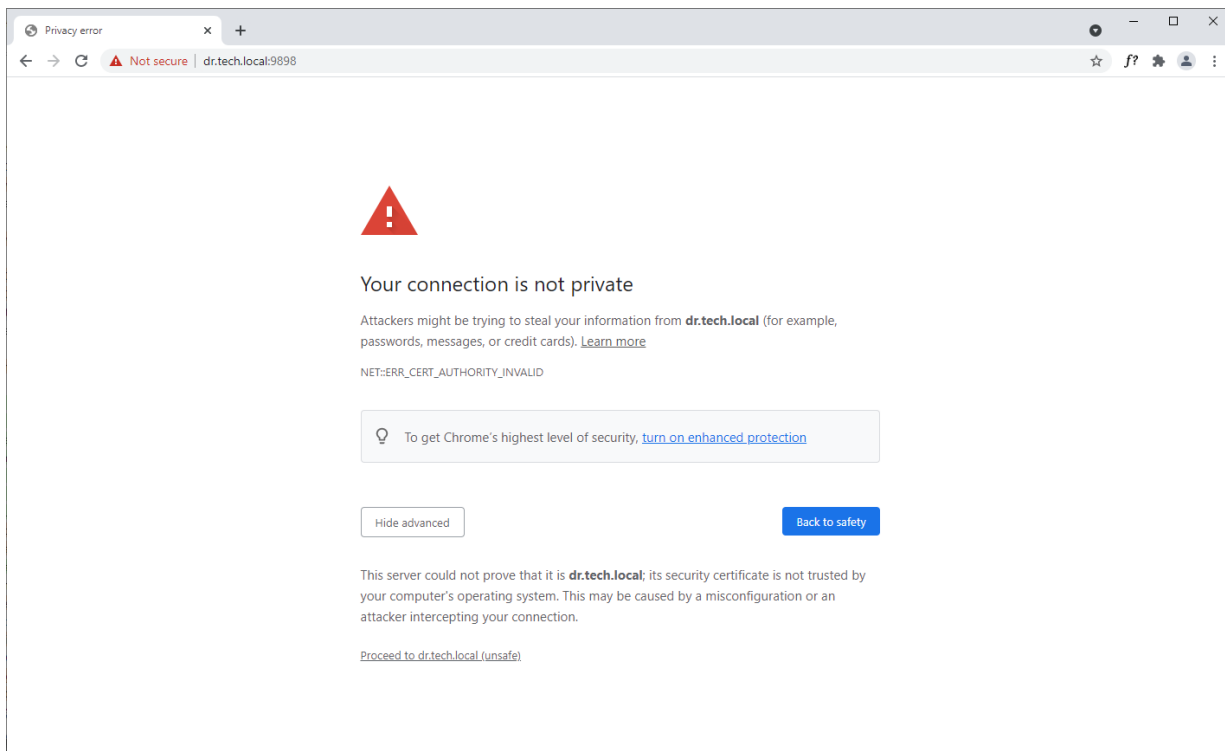
3. Click **Log in**.



Configuring Trusted Connection

The Orchestrator UI uses SSL to ensure secure data communication between Orchestrator and a web browser.

When you install Orchestrator, you can generate or choose a self-signed certificate. In this case, when you try to access the Orchestrator UI in a web browser, the browser will display a warning notifying that the connection is untrusted (although it is secured with SSL).



To eliminate the warning, import the self-signed certificate to client machines (the machines from which you plan to access the Orchestrator UI website). To learn how to import SSL certificates, see [this Microsoft KB article](#).

If you want to use the certificate generated during installation, perform the following steps:

1. Log in to the machine where Orchestrator is installed.
2. Open the Microsoft Management Console snap-in.
 - a. Navigate to **Certificates > Trusted Root Certification Authorities > Certificates**.
 - b. Export the *Veeam Self-Signed Certificate* following the instructions provided in [this Microsoft KB article](#).
3. Import the *Veeam Self-Signed Certificate* to client machines.

TIP

If you still have issues accessing the Orchestrator UI, check your browser settings to ensure that the Orchestrator UI site is included in the **Trusted Sites** list.

Logging Out

To log out of the Orchestrator UI, at the top right corner of the Veeam Disaster Recovery Orchestrator window, click the user name and then click **Logout**.

Configuring Veeam Disaster Recovery Orchestrator

To start working with Orchestrator, perform a number of steps for its configuration:

1. [\[Optional\] Create scopes to allow access to Orchestrator.](#)
2. [\[Optional\] For each scope, add users to specific roles.](#)
3. [Connect Veeam Backup & Replication servers.](#)
4. [Connect additional infrastructure such as vCenter Servers, NetApp and HPE storage.](#)
5. [Configure email notification settings.](#)
6. Use the **Scope Inclusions** page to modify the list of items included and excluded from each of the created scopes:
 - a. [Include inventory groups to be used in orchestration plans.](#)
 - b. [Include locations to be used to recover inventory groups.](#)
 - c. [Include plan steps to be performed while running the recovery process.](#)
 - d. [Include credentials under which orchestration plan steps will be launched.](#)
 - e. [Include template jobs to be used to reprotect inventory groups in orchestration plans.](#)
 - f. [Include DataLabs to be used to test orchestration plans.](#)

Managing Permissions

Orchestrator controls access to its functionality with the help of scopes. A scope defines what operations users can perform and what range of data is available to them in the Orchestrator UI.

For a scope, you can:

1. [Assign user roles to users from that scope](#). A user role limits the number of operations available in the Orchestrator UI to users with that role. Role-based access is controlled by adding Active Directory users and groups to the relevant role in the Orchestrator UI.

There are 3 roles that can be assigned to users and user groups working with the Orchestrator UI: *Administrator*, *Plan Author* and *Plan Operator*. For the role descriptions, see the Veeam Disaster Recovery Orchestrator Deployment Guide, section [Roles](#).

Orchestrator already provides one out-of-the-box *Admin Scope*. If you want to provide more granular permissions to users managing resources of the Orchestrator server, you can [create a new scope](#). However, you will be able to assign only the *Plan Author* and *Plan Operator* roles to users added to the scope.

NOTE

Plan Authors and Plan Operators in the *Admin Scope* have additional privileges compared to users in scopes that you create manually (for example, Plan Authors in the *Admin Scope* can edit any plan for any other scope, and Plan Operators in the *Admin Scope* can run any plan for any other scope).

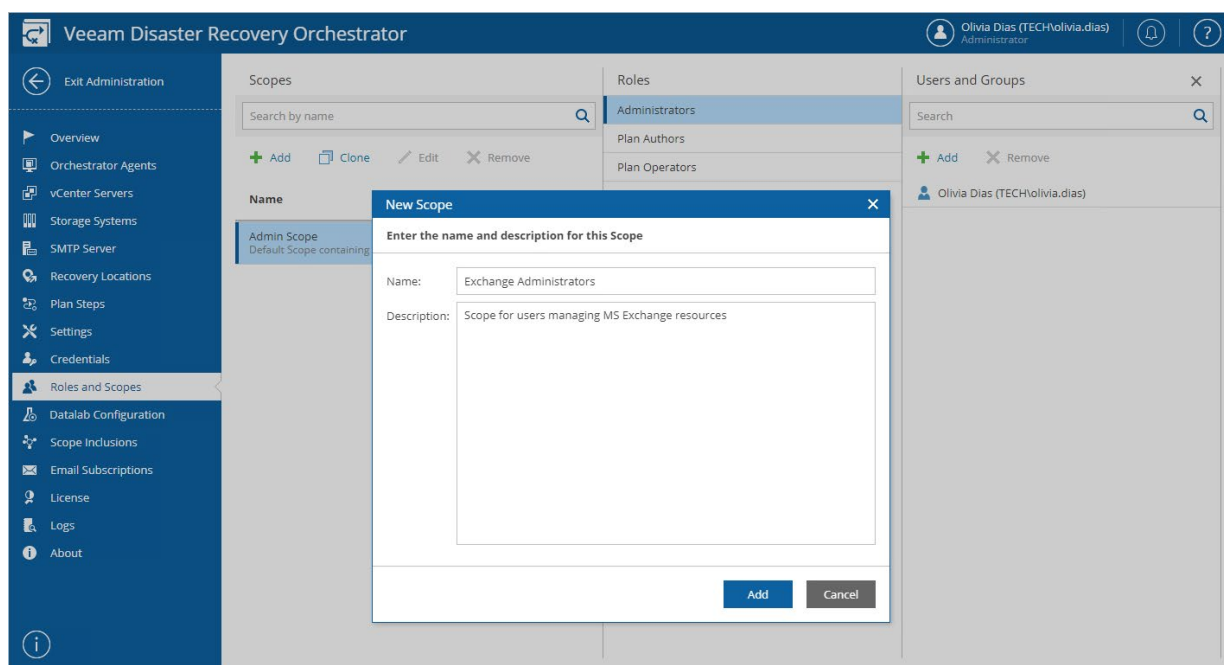
2. Limit the number of inventory items available in the Orchestrator UI to users from that scope. Inventory items are then used to [create orchestration plans](#).
 - a. Navigate to **Scope Inclusions**.
 - b. Follow the instructions provided in sections [Managing Inventory Groups](#), [Managing Recovery Locations](#), [Configuring Plan Steps](#), [Managing Credentials](#), [Connecting DataLabs](#) and [Editing Template Jobs](#).

Creating Scopes

To create a new scope:

1. Switch to the **Administration** page.
2. Navigate to **Roles and Scopes**.
3. In the **Scopes** column, click **Add**.
4. In the **New Scope** window:
 - a. Use the **Name** and **Description** fields to enter a name for the new scope and to provide a description for future reference.

The maximum length of the scope name is 64 characters; the following characters are not supported:
* : / \ ? " < > | .
 - b. Click **Add** to save the scope.



Cloning Scopes

You can also create a new scope by cloning a scope that already exists. When cloning a scope, you can copy its settings so that you do not have to configure the same settings once again for the new scope.

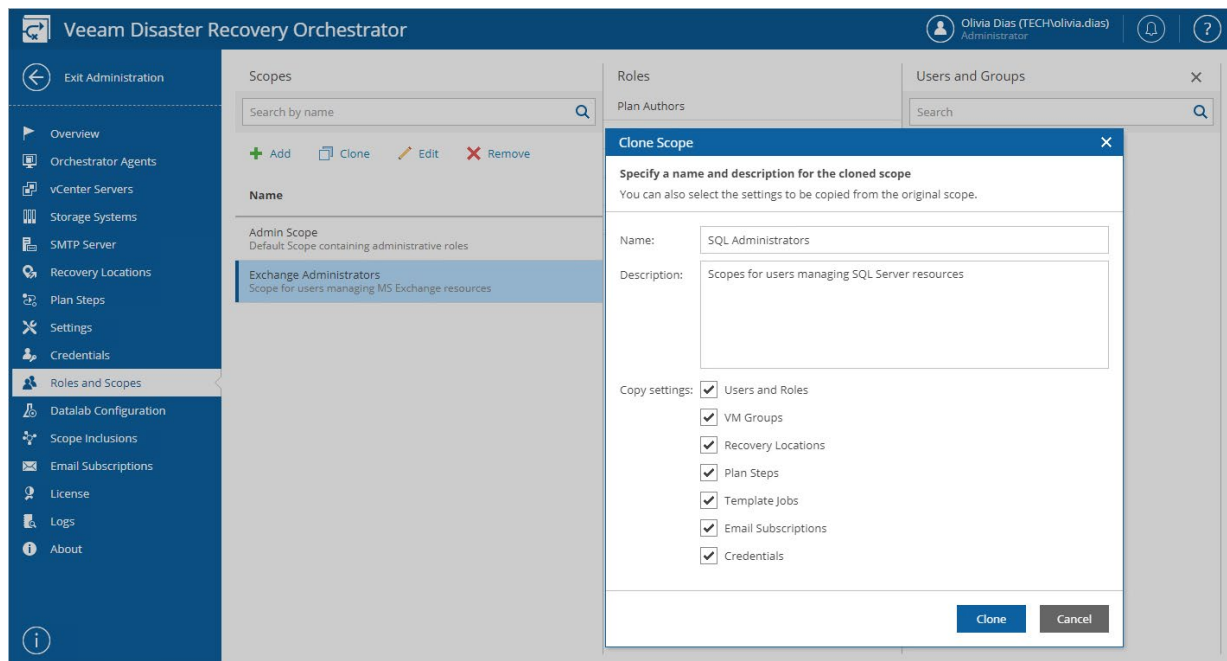
The new scope will have the same configuration as the existing scope, which means that all items configured for the existing scope will be applied to the new scope – except credentials. You will have to include credentials into the list of inventory items available for the new scope, as described in section [Managing Credentials](#).

To clone a scope:

1. Select an existing scope that you want to use as a template for the new scope.
2. In the **Scopes** column, click **Clone**.
3. In the **Clone Scope** window:
 - a. Use the **Name** and **Description** fields to enter a name for the new scope and to provide a description for future reference.

The maximum length of the scope name is 64 characters; the following characters are not supported:
* : / \ ? " < > | .

- b. In the **Copy settings** list, select check boxes next to settings that you want to copy from the existing scope.
- c. Click **Clone** to save the scope.



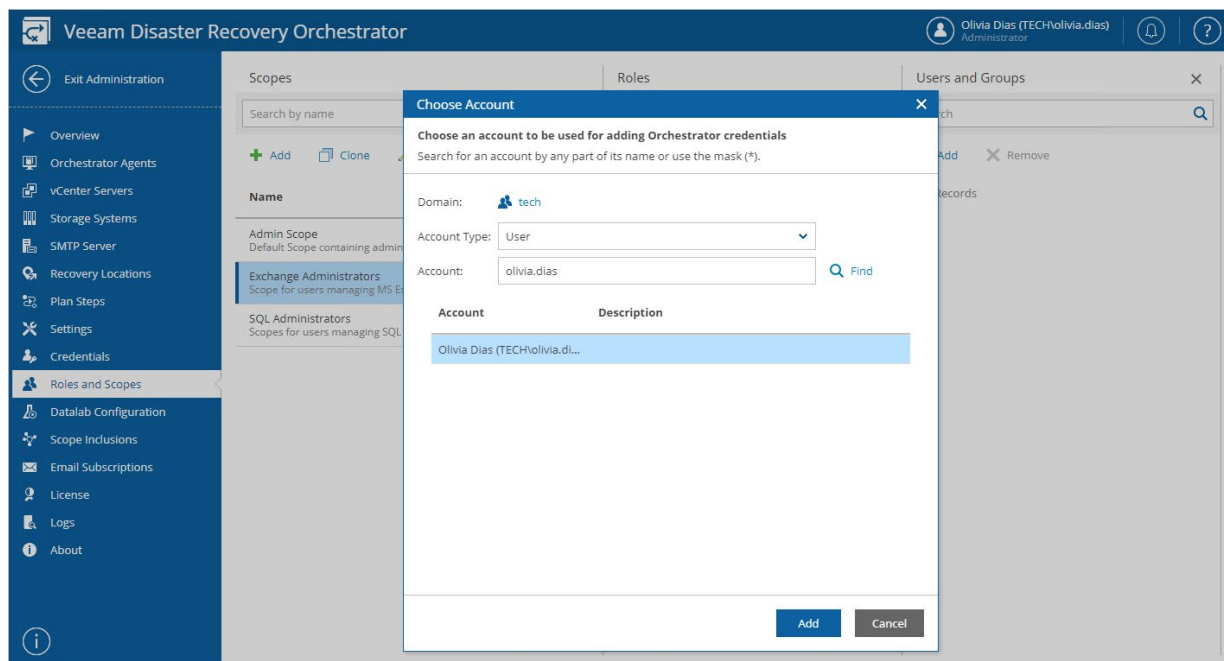
Assigning User Roles and Permissions

To assign a user role to an Active Directory user or a user group:

1. Switch to the **Administration** page.
2. Navigate to **Roles and Scopes**.
3. In the **Scopes** column, select the scope.
4. In the **Roles** column, choose the required role.
5. In the **Users and Groups** column, click **Add**.
6. In the **Choose Account** window:
 - a. From the **Account Type** list, select *User* or *Group*.
 - b. Use the **Account** and **Domain** fields to enter the user or group name and to select a domain to which the user or group belongs.

For more information on the required account permissions, see the Veeam Disaster Recovery Orchestrator Deployment Guide, section [Permissions](#).

 - c. Click **Find**.
 - d. Select the user or group, and click **Add**.



Connecting Veeam Backup & Replication Servers

To be able to orchestrate a remote Veeam Backup & Replication server, you must deploy an Orchestrator agent on the server. The Orchestrator agent will trigger orchestration commands on that server.

If you have already connected servers during initial Orchestrator UI configuration, you do not need to connect them again. For more information, see the [Veeam Disaster Recovery Orchestrator Deployment Guide](#), section [After You Install](#).

NOTE

Orchestrator supports connecting remote Veeam Backup & Replication servers that run the PostgreSQL database system.

To deploy an Orchestrator agent on a remote Veeam Backup & Replication server:

1. Switch to the **Administration** page.
2. Navigate to **Orchestrator Agents**.
3. Click **Install**.
4. Complete the **Install Orchestrator Agent** wizard:
 - a. At the **Settings** step of the wizard, specify the following connection settings:
 - i. Use the **Server type** options to specify whether the server is a Veeam Backup & Replication server or Veeam Backup Enterprise Manager server.

If you choose the **Veeam Enterprise Manager Server** option, Orchestrator agents will be deployed to all Veeam Backup & Replication servers managed by the Veeam Backup Enterprise Manager.
 - ii. Use the **DNS name or IP** field to enter a DNS name or an IP address of the server where you want to deploy the Orchestrator agent. The maximum length of the location name is 64 characters; the following characters are not supported: * : / \ ? " < > | .
 - iii. From the **Credentials** drop-down list, choose the necessary account for connecting to the server. For an account to be displayed in the **Credentials** list, it must be added to the configuration database as described in section [Adding Credentials](#). If you have not set up an account beforehand, click **Add** and follow the steps of the **Add Credential** wizard. For more information on the required account permissions, see the Veeam Disaster Recovery Orchestrator Deployment Guide, section [Permissions](#).

The provided credentials will be also used to launch the Orchestrator agent on the server. The user name must be specified in the *DOMAIN\USERNAME* format.

NOTE

If you want to connect an Enterprise Manager server, you must specify the credentials that were used when installing Veeam Backup Enterprise Manager.

The screenshot shows the 'Install Orchestrator Agent' wizard window. The left sidebar has 'Settings' selected. The main area is titled 'Choose the server where the Orchestrator agent will be deployed'. It contains the following fields:

- Server type:** Two radio buttons. 'Backup & Replication' is selected (indicated by a filled circle). 'Enterprise Manager' is unselected (indicated by an empty circle).
- DNS name or IP:** A text box containing '172.18.28.72'.
- Credentials:** A dropdown menu showing 'tech\olivia.dias' with a blue information icon to its left and an 'Add' button with a plus icon to its right.

At the bottom right, there are 'Next' and 'Cancel' buttons.

- b. At the **Summary** step of the wizard, review the connection details and click **Finish**.

The screenshot shows the 'Install Orchestrator Agent' wizard window at the 'Summary' step. The left sidebar has 'Summary' selected. The main area is titled 'Summary' and displays the following details:

- Server type:** Backup & Replication (with a server icon)
- Server name:** 172.18.28.72
- Credentials:** TECH\olivia.dias

At the bottom right, there are 'Previous', 'Finish', and 'Cancel' buttons.

Uninstalling Orchestrator Agents

If you no longer need a Veeam Backup & Replication server to be connected to Orchestrator, you can uninstall the Orchestrator agent running on the server.

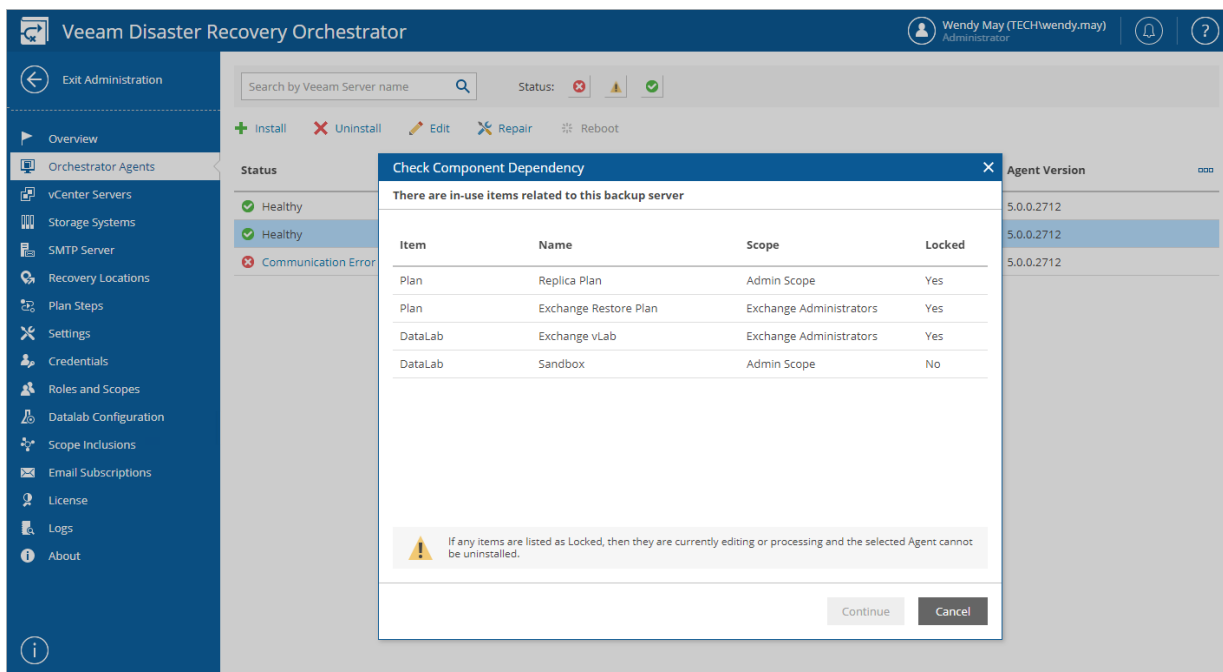
1. Select the Orchestrator agent and click **Uninstall**.
2. The **Check Component Dependency** window will inform you if any DataLabs or orchestration plans are related to the Veeam Backup & Replication server.
 - If any of the items occur to be *Locked*, Orchestrator will not be able to uninstall the Orchestrator agent.

In this case, wait until Orchestrator stops processing the items, power off plan testing in the locked DataLabs, reset the locked orchestration plans – and then try uninstalling the Orchestrator agent again.
 - If none of the items are *Locked*, click **Continue** to confirm the operation.

IMPORTANT

As soon as you uninstall the Orchestrator agent from the Veeam Backup & Replication server, all its related orchestration plans will no longer be able to run, and all its related DataLabs will be removed from Orchestrator.

All [template jobs](#) and [credentials](#) collected from the server will also be excluded from Orchestrator components, and the [Protect VM Group steps](#) that use any of these jobs will be removed from orchestration plans as well.



3. Complete the **Uninstall Orchestrator Agent** wizard:

a. At the **Settings** step of the wizard, specify the following settings:

- i. Choose whether you want to uninstall the Orchestrator agent regardless of the Veeam Backup & Replication server state.

If Orchestrator is not able to access the server, the Orchestrator agent will be removed from the Orchestrator database but will keep running on the Veeam Backup & Replication server.

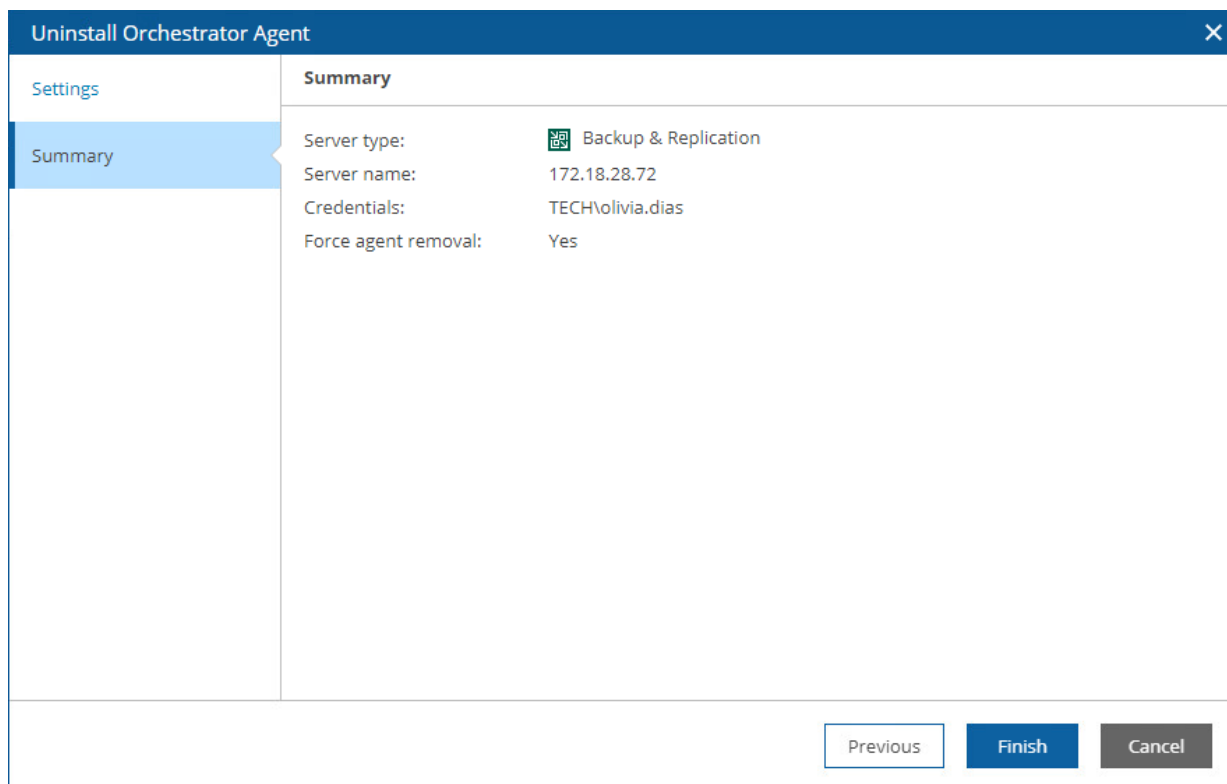
- ii. From the **Credentials** drop-down list, select the necessary account for connecting to the server. For an account to be displayed in the **Credentials** list, it must be added to the configuration database as described in section [Adding Credentials](#). If you have not set up an account beforehand, click **Add** and follow the steps of the **Add Credential** wizard. For more information on the required account permissions, see the Veeam Disaster Recovery Orchestrator Deployment Guide, section [Permissions](#).

The provided credentials will be also used to launch the Orchestrator agent on the server. The user name must be specified in the *DOMAIN\USERNAME* format.


The screenshot shows the 'Uninstall Orchestrator Agent' wizard window. The title bar is 'Uninstall Orchestrator Agent' with a close button. The left sidebar has 'Settings' selected and 'Summary' below it. The main area is titled 'Settings for agent uninstallation' with a subtitle 'You may force the removal of this agent from Orchestrator even if it cannot be contacted.' Below this, there is a text field for 'DNS name or IP:' containing '172.18.28.72'. A checkbox labeled 'Force removal of agent records from Orchestrator' is checked. Below that is a 'Credentials' section with a dropdown menu showing 'tech\olivia.dias (Credentials with administrative acce' and an 'Add' button with a plus icon. At the bottom right are 'Next' and 'Cancel' buttons.

Uninstall Orchestrator Agent	
Settings	Settings for agent uninstallation You may force the removal of this agent from Orchestrator even if it cannot be contacted.
Summary	DNS name or IP: 172.18.28.72 <input checked="" type="checkbox"/> Force removal of agent records from Orchestrator Credentials tech\olivia.dias (Credentials with administrative acce Add
<div>Next Cancel</div>	

b. At the **Summary** step, review the configured settings and click **Finish**.



The image shows a window titled "Uninstall Orchestrator Agent" with a close button (X) in the top right corner. On the left is a sidebar with two tabs: "Settings" and "Summary". The "Summary" tab is selected and highlighted in blue. The main area of the window displays the following configuration details:

Summary	
Server type:	 Backup & Replication
Server name:	172.18.28.72
Credentials:	TECH\olivia.dias
Force agent removal:	Yes

At the bottom right of the window, there are three buttons: "Previous" (disabled), "Finish" (active), and "Cancel" (disabled).

NOTE

If a Veeam Backup & Replication server is managed by Veeam Backup Enterprise Manager, you will not be able to uninstall the Orchestrator agent running on the server using the Orchestrator UI. In this case, remove the Veeam Backup & Replication server from Enterprise Manager as described in the [Veeam Backup Enterprise Manager Guide](#). After you remove the server from Enterprise Manager, it will be automatically removed from Orchestrator as well.

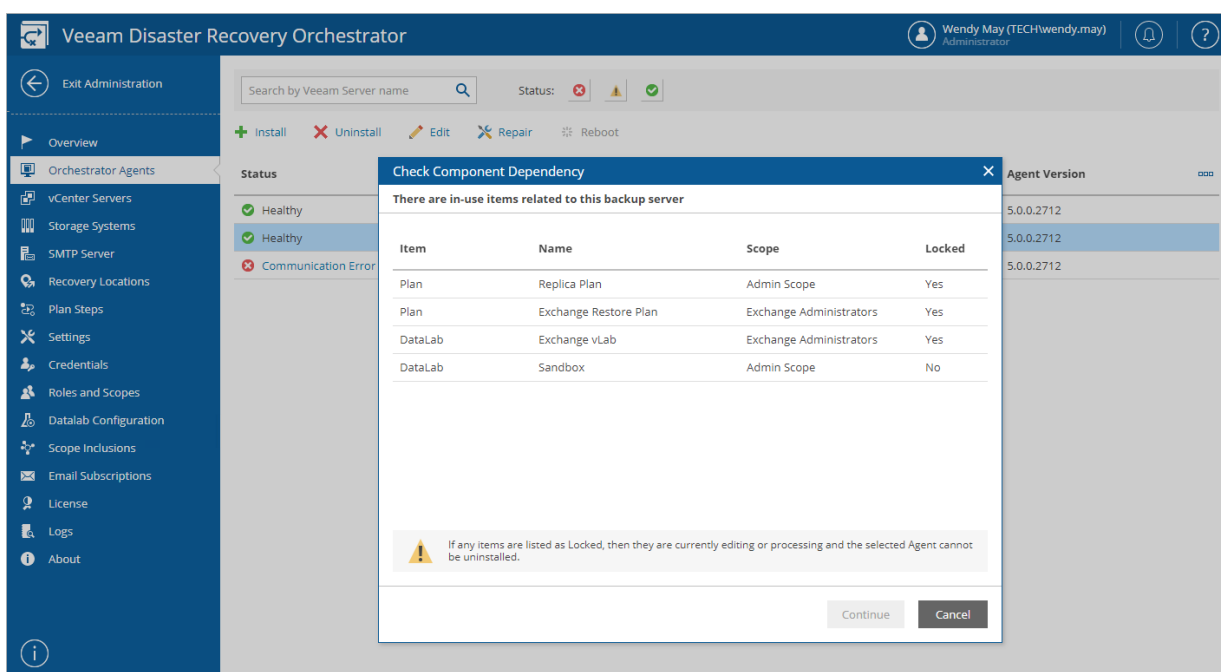
Repairing Orchestrator Agents

If you want to change credentials of a user account that you specified when connecting a Veeam Backup & Replication server to Orchestrator, or if you encounter a connection issue and a Veeam Backup & Replication server acquires the *Disconnected* state, you can repair the Orchestrator agent running on the server.

NOTE

If you [upgrade a remote Veeam Backup & Replication server](#) connected to Orchestrator, you must also repair the Orchestrator agent running on the server. However, it is recommended that you wait approximately 10 minutes before repairing the agent because Veeam ONE Client has to process infrastructure changes related to the upgrade.

1. Select the Orchestrator agent and click **Repair**.
2. The **Check Component Dependency** window will inform you if any DataLabs or orchestration plans are related to the Veeam Backup & Replication server.
 - If any of the items occur to be *Locked*, Orchestrator will not be able to repair the Orchestrator agent.
In this case, wait until Orchestrator stops processing the items, power off plan testing in the locked DataLabs, reset the locked orchestration plans – and then try repairing the Orchestrator agent again.
 - If none of the items are *Locked*, click **Continue** to confirm the operation.



3. Complete the **Repair Orchestrator Agent** wizard:

- a. At the **Settings** step, select the necessary account from the **Credentials** drop-down list for connecting to the Veeam Backup & Replication server. For an account to be displayed in the **Credentials** list, it must be added to the configuration database as described in section [Adding Credentials](#). If you have not set up an account beforehand, click **Add** and follow the steps of the **Add Credential** wizard. For more information on the required account permissions, see the Veeam Disaster Recovery Orchestrator Deployment Guide, section [Permissions](#).


The provided credentials will be also used to launch the Orchestrator agent on the server. The user name must be specified in the *DOMAIN\USERNAME* format.

The screenshot shows the 'Repair Orchestrator Agent' wizard window. The title bar is blue with the text 'Repair Orchestrator Agent' and a close button. The left sidebar has two tabs: 'Settings' (selected, highlighted in blue) and 'Summary'. The main content area is titled 'Repair Agent' and contains the text 'Agent repair will be attempted. You may change the credentials if required.' Below this, there are two fields: 'DNS name or IP:' with the value '172.18.28.72' and 'Credentials' with a dropdown menu showing 'tech\olivia.dias'. To the right of the dropdown is an 'Add' button with a plus icon. At the bottom right of the window are 'Next' and 'Cancel' buttons.

Repair Orchestrator Agent	
Settings	Repair Agent Agent repair will be attempted. You may change the credentials if required.
	DNS name or IP: 172.18.28.72 Credentials: tech\olivia.dias [Add]
Summary	
Next Cancel	

b. At the **Summary** step, review the configured settings and click **Finish**.

The screenshot shows a window titled "Repair Orchestrator Agent" with a close button (X) in the top right corner. On the left is a sidebar with two tabs: "Settings" and "Summary". The "Summary" tab is selected and highlighted in blue. The main area of the window is titled "Summary" and contains the following configuration details:

Server type:	 Backup & Replication
Server name:	172.18.28.72
Credentials:	TECH\olivia.dias

At the bottom right of the window, there are three buttons: "Previous" (disabled), "Finish" (active), and "Cancel" (disabled).

Connecting Infrastructure

If required, you can configure connections to vCenter Servers, and NetApp or HPE storage systems.

If you have already connected servers in the **Initial Configuration** wizard, you do not need to connect them again. For more information, see the Veeam Disaster Recovery Orchestrator Deployment Guide, section [After You Install](#).

NOTE

No additional connection is required for recovery to Microsoft Azure as Orchestrator will use the Microsoft Azure compute and storage credentials configured on the connected Veeam Backup & Replication servers.

Connecting Storage Systems

The following NetApp storage systems must be connected to Orchestrator:

- Any active storage virtual machine (SVM) that will be the source of the datastore disaster recovery relationship.
- Any active SVM that will be the destination of the SVM disaster recovery relationship.

IMPORTANT

Make sure that you have NetApp volumes and virtual volumes protected by storage replication. If you use authentication configured to control access to iSCSI targets, make sure that you define a list of initiators and their authentication methods for all hosts managed by the target vCenter Server. For more information on iSCSI initiator security management, see the [NetApp ONTAP Documentation Center](#). For more information on configuring CHAP parameters for iSCSI adapters, see [VMware Docs](#).

The following HPE storage systems must be connected to Orchestrator:

- Any active storage system that will be the primary system of the remote copy configuration.
- Any active storage system that will be the secondary system of the remote copy configuration.

IMPORTANT

To connect an HPE storage system, you must first enable the HPE 3PAR Web Services API (WSAPI) server as described in section [Enabling HPE 3PAR Web Services API Server](#).

To connect a storage system to Orchestrator:

1. Switch to the **Administration** page.
2. Navigate to **Storage Systems**.
3. Click **Add**.

4. Complete the **Connect Storage System** wizard:

- a. At the **Storage Vendor** step of the wizard, choose whether you want to connect a NetApp or an HPE storage system.

The screenshot shows a wizard window titled "Connect Storage System" with a close button (X) in the top right corner. On the left is a sidebar with three items: "Storage Vendor" (highlighted in blue), "Settings" (in blue text), and "Summary" (in grey text). The main area is titled "Choose storage vendor" and contains the text "Storage vendor:". Below this are two radio button options: "NetApp" (with a blue square icon and a selected radio button) and "HPE" (with a green square icon and an unselected radio button). At the bottom right of the main area are two buttons: "Next" (blue) and "Cancel" (grey).

- b. At the **Settings** step of the wizard, specify the following connection settings:

- i. Use the **DNS name or IP** field to enter a DNS name or an IP address of the storage system that will be connected to the Orchestrator server. The maximum length of the location name is 64 characters; the following characters are not supported: * : / \ ? " < > | .
- ii. From the **Credentials** drop-down list, choose the necessary account for connecting to the storage system.

For an account to be displayed in the **Credentials** list, it must be added to the configuration database as described in section [Adding Credentials](#). If you have not set up an account beforehand, click **Add** and follow the steps of the **Add Credential** wizard. For more information on the required account permissions, see the Veeam Disaster Recovery Orchestrator Deployment Guide, section [Permissions](#).

iii. If required, change the port number used for communication with the system.

If an untrusted security certificate is installed on the storage system, you will get a security warning. You can view the certificate and click **Remember and continue** – in this case, Orchestrator will remember the certificate thumbprint and will further trust the certificate when connecting to the storage system. Otherwise, you will not be able to proceed with the wizard.

The screenshot shows the 'Connect Storage System' wizard with the 'Settings' step selected. The left sidebar contains 'Storage Vendor', 'Settings', and 'Summary'. The main area is titled 'Specify storage system connection settings' and contains three fields: 'DNS name or IP' with the value '172.15.152.11', 'Port' with a dropdown set to '443', and 'Credentials' with a dropdown set to 'vsadmin'. An 'Add' button with a plus icon is next to the credentials field. At the bottom right are 'Previous', 'Next', and 'Cancel' buttons.

Connect Storage System	
Storage Vendor	Specify storage system connection settings
Settings	DNS name or IP: 172.15.152.11
	Port: 443
	Credentials: vsadmin
Summary	
<div>Previous Next Cancel</div>	

c. At the **Summary** step of the wizard, review the connection details and click **Finish**.

The screenshot shows the 'Connect Storage System' wizard with the 'Summary' step selected. The left sidebar contains 'Storage Vendor', 'Settings', and 'Summary'. The main area is titled 'Summary' and displays the connection details: 'Storage vendor: NetApp', 'Storage name: 172.15.152.11', 'Port: 443', and 'Credentials: vsadmin'. At the bottom right are 'Previous', 'Finish', and 'Cancel' buttons.

Connect Storage System	
Storage Vendor	Summary
Settings	Storage vendor: NetApp
	Storage name: 172.15.152.11
	Port: 443
	Credentials: vsadmin
Summary	
<div>Previous Finish Cancel</div>	

After you connect a storage system to Orchestrator, you must include the system in a [storage recovery location](#) (either new or already existing) so that Orchestrator can use this storage system when executing and testing [storage plans](#). To learn how to include target storage systems in storage recovery locations, see [Adding Storage Recovery Locations](#).

Enabling HPE 3PAR Web Services API Server

Orchestrator uses the HPE 3PAR Web Services API (WSAPI) server to communicate with HPE Primera and HPE 3PAR storage systems. When you add an HPE Primera or HPE 3PAR storage system to Orchestrator, it does not enable the WSAPI server automatically because it does not have enough privileges to perform this operation. This means that you must enable the server manually before connecting the storage system to Orchestrator.

To enable the WSAPI server running on an HPE Primera or HPE 3PAR storage system:

1. Log on to the Processor with administrator privileges:

```
#ssh <administrator account>@<SP IP Address>
```

2. Run the following command to view the current state of the WSAPI server:

```
#showwsapi
-- -State- -HTTP_State-
HTTP_Port -HTTPS_State- HTTPS_Port -Version-
Enabled   Active Enabled      8008
Enabled      8080          1.1
```

3. If the WSAPI server is not running, run the following command to start it:

```
#startwsapi
```

If the HTTPS port is disabled, run the following command to enable it:

```
#setwsapi -https enable
```

Connecting VMware vSphere Servers

To collect data about VMware vSphere infrastructure objects, you must configure connections to VMware vSphere servers. Only connections to vCenter Servers are supported.

IMPORTANT

To allow Orchestrator to process resource groups properly, you must connect vCenter Servers — not standalone ESXi hosts — to Veeam Backup & Replication servers orchestrated by Orchestrator. To learn how to add vCenter Servers to the backup infrastructure, see the Veeam Backup & Replication User Guide, section [Virtualization Servers and Hosts](#).

It is a requirement that Orchestrator has connections to the following vCenter Servers:

- All vCenter Servers managing source and replica VMs.
- The vCenter Server managing resources that will be used to recover VMs.
- All vCenter Servers managing VMs whose disks are located on the [connected storage systems](#).

IMPORTANT

Starting from VMware vSphere version 7.0 Update 3, [vSphere Cluster Services \(vCLS\)](#) is activated by default. Before you connect to a vCenter Server version 7.0 Update 3, you must configure vCLS datastore placement in the vSphere Client as described in [VMware vSphere documentation](#).

To configure a connection to a vCenter Server:

1. Switch to the **Administration** page.
2. Navigate to **VMware vCenter**.
3. Click **Add**.
4. Complete the **Connect VMware vCenter** wizard:
 - a. At the **Settings** step of the wizard, specify the following connection settings:
 - i. Use the **DNS name or IP** field to enter a DNS name or an IP address of the vCenter Server that will be connected to the Orchestrator agent. The maximum length of the location name is 64 characters; the following characters are not supported: * : / \ ? " < > | .
 - ii. From the **Credentials** drop-down list, choose the necessary account for connecting to the server. For an account to be displayed in the **Credentials** list, it must be added to the configuration database as described in section [Adding Credentials](#). If you have not set up an account beforehand, click **Add** and follow the steps of the **Add Credential** wizard. For more information on the required account permissions, see the Veeam Disaster Recovery Orchestrator Deployment Guide, section [Permissions](#).

iii. If required, change the port number used for communication with the server.

If an untrusted security certificate is installed on the vCenter Server, you will get a security warning. You can view the certificate and click **Remember and Continue** – in this case, Orchestrator will remember the certificate thumbprint and will further trust the certificate when connecting to the server. Otherwise, you will not be able to add the server.

The screenshot shows the 'Connect vCenter Server' wizard window. The left sidebar has 'Settings' and 'Summary' tabs, with 'Settings' currently selected. The main area is titled 'Specify vCenter Server connection settings'. It contains three input fields: 'DNS name or IP' with the value 'cdpvc.qahv1.veeam.local', 'Port' with a dropdown menu showing '443', and 'Credentials' with a dropdown menu showing 'tech\olivia.dias'. There is an 'Add' button with a plus icon next to the credentials field. At the bottom right, there are 'Next' and 'Cancel' buttons.

b. At the **Summary** step of the wizard, review the connection details and click **Finish**.

The screenshot shows the 'Connect vCenter Server' wizard window at the 'Summary' step. The left sidebar has 'Settings' and 'Summary' tabs, with 'Summary' currently selected. The main area is titled 'Summary' and displays the connection details: 'Server name: cdpvc.qahv1.veeam.local', 'Port: 443', and 'Credentials: TECH\olivia.dias'. At the bottom right, there are 'Previous', 'Finish', and 'Cancel' buttons.

Removing VMware vSphere Servers

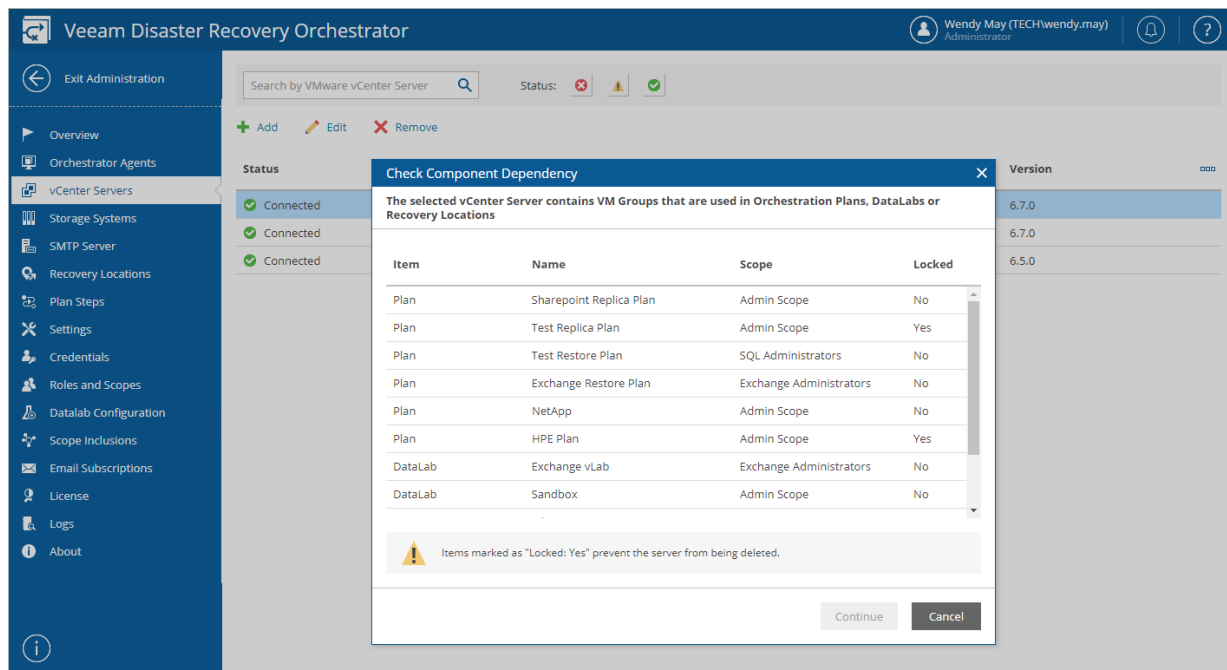
If you no longer need a vCenter Server to be connected to Orchestrator, you can remove the server.

1. Select the vCenter Server and click **Remove**.
2. The **Check Component Dependency** window will inform you if any DataLabs or orchestration plans are related to the vCenter Server.
 - If any of the items occur to be *Locked*, Orchestrator will not be able to remove the server.
In this case, wait until Orchestrator stops processing the items, reset the locked orchestration plans, power off plan testing in the locked DataLabs – and then try removing the vCenter Server again.
 - If none of the items are *Locked*, click **Continue** to confirm the operation.

IMPORTANT

As soon as you remove the vCenter Server from Orchestrator, all its related DataLabs will be removed from Orchestrator as well. All [inventory groups](#) that include VMs managed by the server will be excluded from Orchestrator components, and the VMs will be deleted from the related orchestration plans.

3. In the **Remove VMware vCenter Server** window, click **Yes** to remove the vCenter Server.



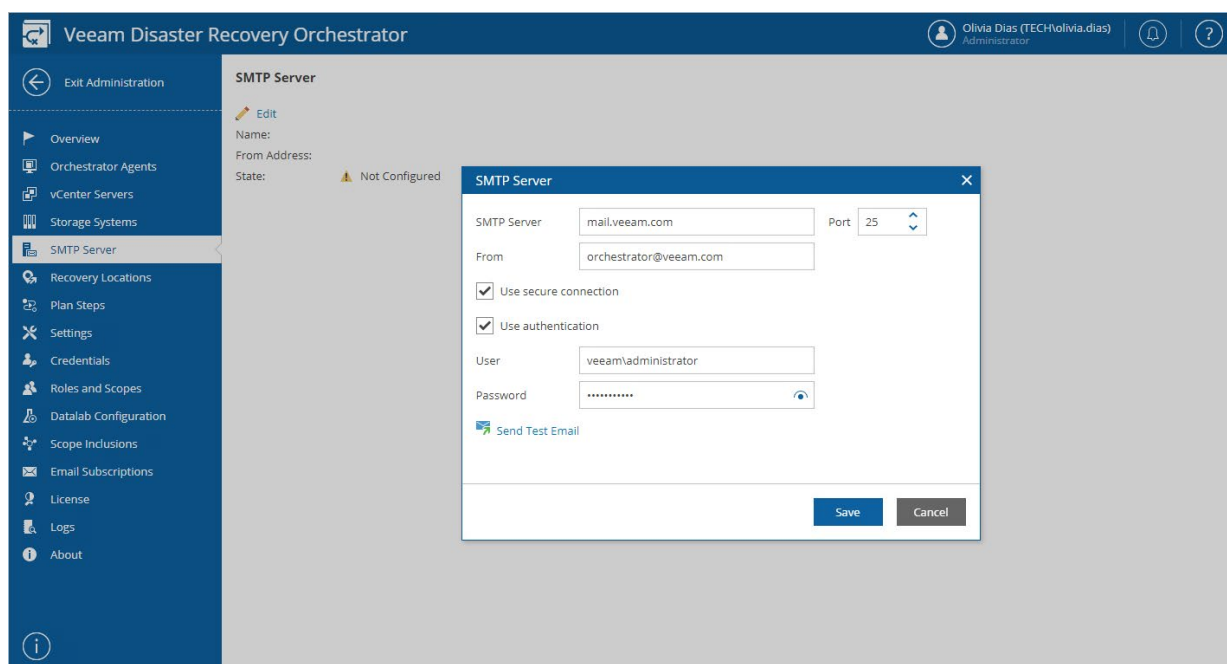
Configuring Notification Settings

The Orchestrator UI allows you to specify email notification settings for automated delivery of Orchestrator reports and documents.

Step 1. Specify SMTP Settings

To connect an SMTP server that will be used for sending email notifications:

1. Switch to the **Administration** page.
2. Navigate to **SMTP Server**.
3. Click **Edit**.
4. In the **SMTP Server** window:
 - a. In the **SMTP Server** field, enter a DNS name or an IP address of the SMTP server. All email notifications (including test messages) will be sent by this SMTP server.
 - b. In the **Port** field, change the SMTP communication port if required. The default SMTP port is **25**.
 - c. In the **From** field, enter an email address of the notification sender. This email address will be displayed in the **From** field of notifications.
 - d. For an SMTP server with SSL/TLS support, select the **Use secure connection** check box to enable SSL data encryption.
 - e. If your SMTP server requires authentication, select the **Use authentication** check box, and specify authentication credentials in the **User** and **Password** fields.
 - f. The Orchestrator UI allows you to send a test message to check whether you have configured all settings correctly. To do that, click **Send Test Email**.
 - g. Click **Save**.

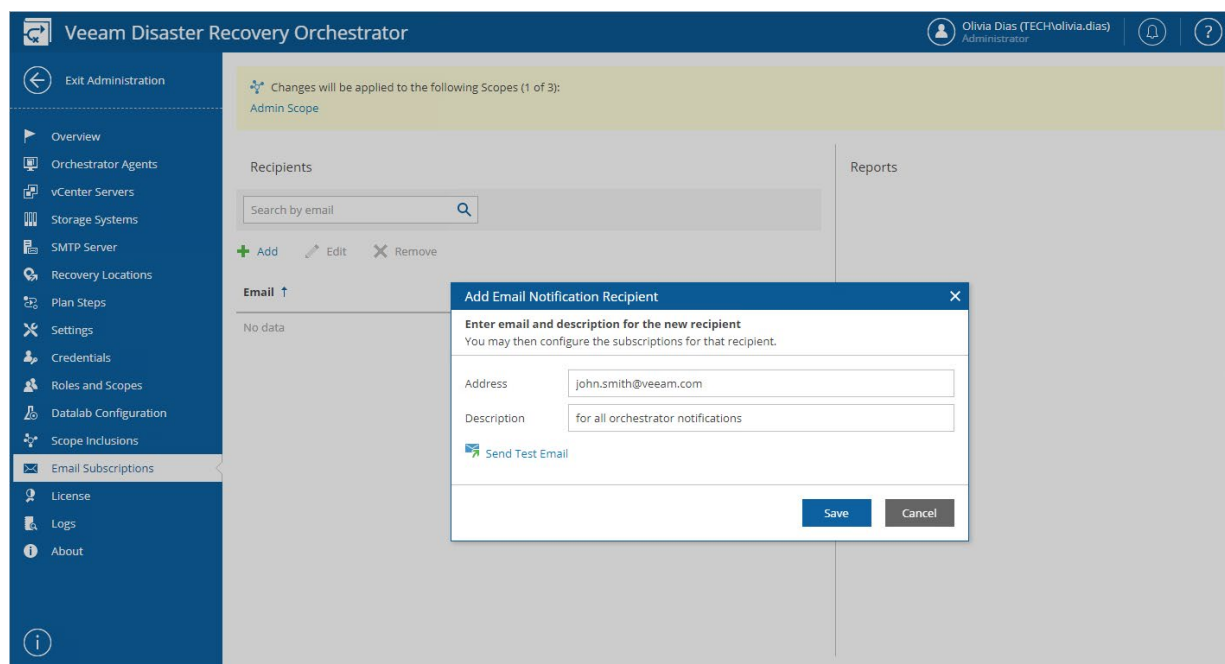


Step 2. Specify Email Notification Settings

Add email addresses that will receive report notifications for your Orchestrator server. These addresses will be available for subscription for [all created scopes](#).

To add recipients to whom notifications will be sent:

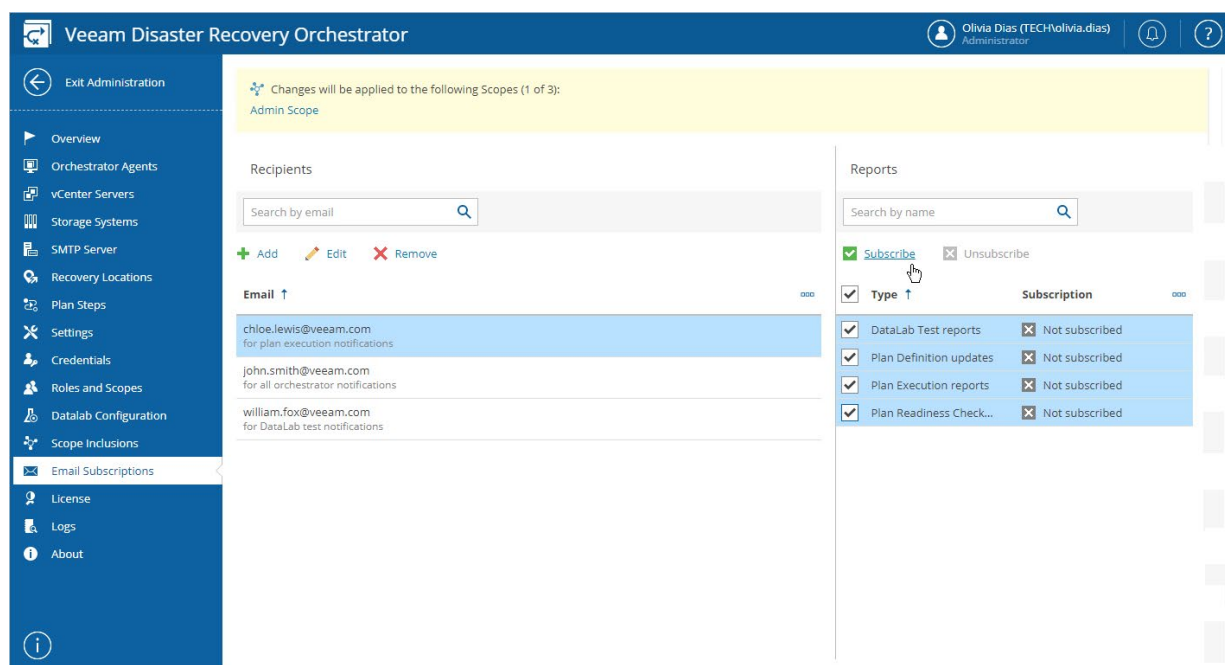
1. Switch to the **Administration** page.
2. Navigate to **Email Subscriptions**.
3. In the **Recipients** column, click **Add**.
4. In the **Add Email Notification Recipient** window:
 - a. In the **Address** field, enter an email address of a recipient.
 - b. In the **Description** field, enter a short description for the recipient, if required.
 - c. The Orchestrator UI allows you to send a test message to check whether you have configured email settings correctly. To do that, click **Send Test Email**. A test email will be sent to the specified email address.
 - d. Click **Save**.



Step 3. Subscribe to Notifications

After you have [added email addresses](#) that will receive notifications, subscribe to the desired reports.

1. Switch to the **Administration** page.
2. Navigate to **Email Subscriptions**.
3. Select a scope for which you want to create subscriptions:
 - a. Click the **Scopes** link.
 - b. In the **Change Scope** window, select a check box next to the required scope, and click **Apply**.
4. Select a recipient. A list of all available report types will be displayed in the **Reports** column.
5. Select check boxes next to the report types this address should subscribe to.
6. Click **Subscribe**.



Managing Inventory Groups

To create orchestration plans, you will use one or more inventory groups. Inventory groups are sets of virtual or physical machines that are managed by the embedded Veeam ONE server installed on the Orchestrator server.

The majority of inventory groups are created automatically, based on discovered items such as Veeam Backup & Replication jobs and protection groups, vSphere datastores, or vSphere VM tags. All inventory groups created this way are added to the list of inventory items on the **Scope Inclusions** page. After you include an inventory group in a specific scope, you can use the inventory group in plans for this scope.

Types of Inventory Groups

Inventory groups are the building blocks of orchestration plans and are created and populated using the embedded Veeam ONE server and its Business View engine. Orchestrator automatically creates a group for each of the following:

- Veeam backup job protecting vSphere VMs or Veeam agents (Windows or Linux).
- Veeam replica or CDP replica job protecting vSphere VMs.
- vSphere datastore containing VMs.
- vSphere datastore containing VMs and backed by a replicating storage system.
- Veeam agent protection group.
- vCenter Server tag for VMs (the group will be named *Category - Tag*).

NOTE

You can manage inventory groups manually using [custom categories configured in Veeam ONE Client](#). You can also group VMs based on [categorization data imported from 3rd party software](#).

Allowing Access to Inventory Groups

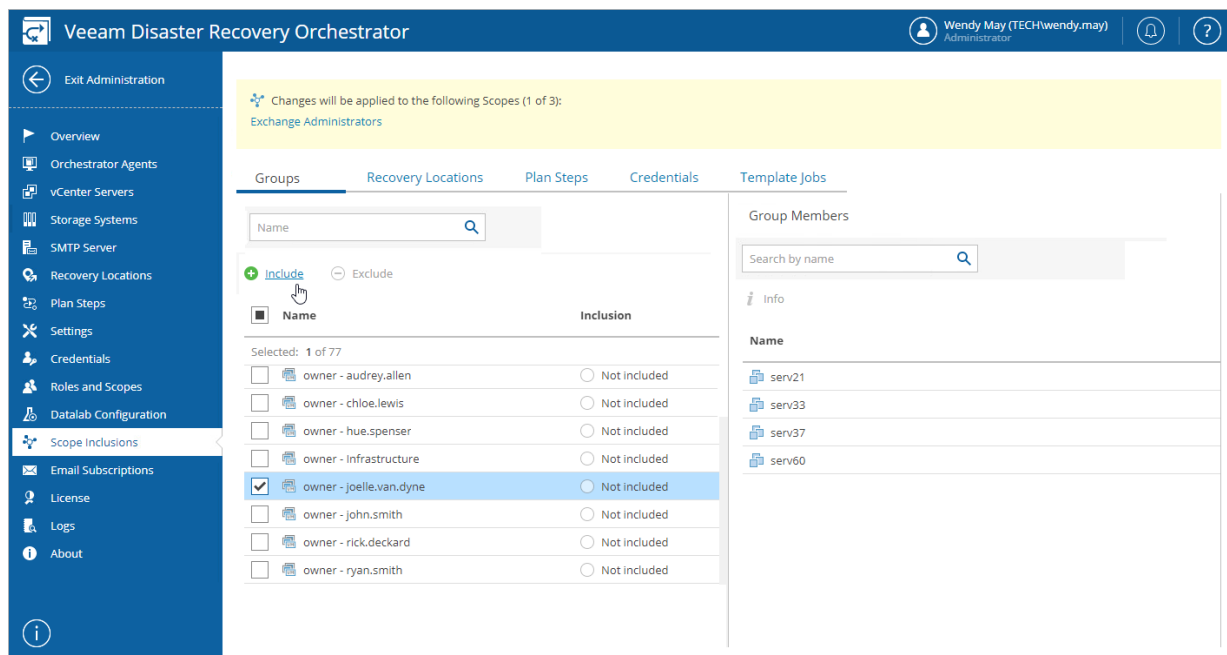
Unless an inventory group is *INCLUDED* into the list of inventory items for a scope, it will not be available for use in the scope. By default, all inventory groups are excluded from the newly created scopes; only the default *Admin Scope* has all discovered groups automatically included.

To modify the list of inventory groups available for a scope:

1. Switch to the **Administration** page.
2. Navigate to **Scope Inclusions > Groups**.
3. Select the scope:
 - a. Click the **Scopes** link.
 - b. In the **Change Scope** window, select a check box next to the required scope, and click **Apply**.
4. Select check boxes next to the necessary groups, and click **Include** or **Exclude**.

TIP

You can simultaneously edit the list of inventory items available for multiple scopes. To do that, select check boxes next to the required scopes in the **Change Scope** window. After you click **Include** or **Exclude**, the changes will be applied to all the selected scopes at the same time.



After you make an inventory group *INCLUDED* for a scope, Plan Authors will be able to add this group to orchestration plans for the scope. For more information on creating and editing orchestration plans, see [Working with Orchestration Plans](#).

Managing Recovery Locations

Recovery locations consist of resource groups (that is, infrastructure objects such as vSphere hosts) used as target locations when orchestrating recovery. Resource groups are managed by the embedded Veeam ONE server installed on the Orchestrator server.

Orchestrator provides 3 types of recovery locations – [Restore Recovery Locations](#), [Storage Recovery Locations](#) and [Cloud Recovery Locations](#).

Restore Recovery Locations

Restore recovery locations are used to define compute and storage resources in a vSphere environment required when [running restore plans](#) and [performing failback operations](#).

Before you run a restore plan or perform a failback operation, you can choose whether to recover machines to the original or to a new location:

- If you want to restore VMs to their original location, you do not need to configure any resources. However, the original VM location does not apply to Veeam agent backups, only to vSphere VM backups.

Orchestrator already includes a built-in recovery location named *Original VM Location* – if you select this location, Orchestrator will automatically detect the original location of processed VMs and restore the VMs to that location.

You can only customize datastore capacity level and enable Instant VM Recovery for the location. For more information, see [Configuring Original Recovery Location](#).

- If you want to restore machines to a different location, you must first categorize vCenter Server resources into restore recovery locations.

For more information on working with restore recovery locations, see sections [Adding Recovery Locations](#), [Configuring Recovery Locations](#) and [Allowing Access to Recovery Locations](#).

Storage Recovery Locations

Storage recovery locations are used to define target storage systems and compute resources required when [running storage plans](#).

Storage recovery locations are populated with connected storage systems, and with compute resources from connected vCenter Servers – vCenter Server resources are categorized into groups based on vCenter Server Tags on hosts and clusters. Resource membership in these groups cannot be edited in the Orchestrator UI – you must modify the tags in the vCenter environment. To learn how to tag infrastructure objects in the vSphere inventory, see [VMware Docs](#).

For more information on working with storage recovery locations, see sections [Adding Recovery Locations](#), [Configuring Recovery Locations](#) and [Allowing Access to Recovery Locations](#).

Cloud Recovery Locations

Cloud recovery locations are used to define cloud resources required when [running cloud plans](#).

Orchestrator 6.0 allows you to recover machines to Microsoft Azure. For limitations that may apply for restoring machines to Microsoft Azure, see the Veeam Backup & Replication User Guide, section [Limitations to Restore to Microsoft Azure](#).

NOTE

Restore to Microsoft Azure does not support [Azure Hybrid Benefit](#). This means that all machines recovered to Microsoft Azure are deployed as unlicensed VMs. If required, you can apply your on-premises license by enabling the Azure Hybrid Benefit option after recovery, which will allow you to run your Azure VMs at a reduced cost.

Before creating a cloud recovery location, ensure that:

- The Veeam Backup & Replication server that will manage the process of recovering machines to Microsoft Azure is running version 12.0 or later.
- You have a Microsoft Azure compute account added to the Veeam Backup & Replication server. For more information on adding a Microsoft Azure compute account, see the Veeam Backup & Replication User Guide, section [Microsoft Azure Compute Accounts](#).

For more information on working with cloud recovery locations, see sections [Adding Recovery Locations](#), [Configuring Recovery Locations](#) and [Allowing Access to Recovery Locations](#).

Adding Recovery Locations

All resource groups created based on vCenter Server tags will automatically become available for the creation of recovery locations in the Orchestrator UI. However, after you assign a tag to an object in the vSphere inventory, it may not be available in the Orchestrator UI immediately – the data synchronization process between Orchestrator and Veeam ONE occurs every 3 hours.

TIP

You can speed up the data synchronization process using Veeam ONE Reporter installed as part of the embedded Veeam ONE server. To do that:

1. In a web browser, navigate to the Veeam ONE Reporter web address.
The address consists of an FQDN of the Orchestrator server and the website port specified during installation (by default, **1239**). Note that Veeam ONE Reporter is available over HTTPS.
`https://hostname:1239/`
2. Navigate to **Data Collection**.
3. Click **Start**.

To add a recovery location to be used when running a restore plan or performing a failback operation, follow the instructions provided in section [Adding Restore Recovery Locations](#). To add a recovery location to be used when running a storage plan, follow the instructions provided in section [Adding Storage Recovery Locations](#). To add a recovery location to be used when running a cloud plan, follow the instructions provided in section [Adding Cloud Recovery Locations](#).

Adding Restore Recovery Locations

To add a restore recovery location:

1. Switch to the **Administration** page.
2. Navigate to **Recovery Locations**.
3. Click **Add**.
4. Complete the **New Recovery Location** wizard:
 - a. [Choose a recovery location type](#).
 - b. [Specify a recovery location name and description](#).
 - c. [Choose recovery options](#).
 - d. [Specify compute resources](#).
 - e. [Specify storage resources](#).
 - f. [Specify a datastore capacity level](#).
 - g. [Configure network mapping](#).
 - h. [Configure re-IP rules](#).
 - i. [Enable VM recovery across different locations in Veeam Backup & Replication](#).
 - j. [Finish working with the wizard](#).

Step 1. Choose Recovery Location Type

At the **Recovery Location Type** step of the wizard, select the **Restore** option.

New Recovery Location

Recovery Location Type

Recovery Location Name

Recovery Options

Compute Resources

Storage Resources

Storage Options

Agent Networks

VM Networks

Re-IP Rules

Data Sovereignty

Summary

Choose type of recovery location

☐ Storage

Contains storage systems, vSphere hosts to mount the storage, and VM network configuration.

☒ Restore

Contains vSphere hosts, datastores and VM network configuration.

☐ Cloud

A public cloud where Veeam agent and vSphere backups can be recovered as cloud VMs.

Next

Cancel

Step 2. Specify Recovery Location Name and Description

At the **Recovery Location Name** step of the wizard, use the **Name** and **Description** fields to enter a name for the new location and to provide a description for future reference. The maximum length of the location name is 64 characters; the following characters are not supported: * : / \ ? " < > | .

New Recovery Location

Recovery Location Type

Recovery Location Name

Recovery Options

Compute Resources

Storage Resources

Storage Options

Agent Networks

VM Networks

Re-IP Rules

Data Sovereignty

Summary

Enter a name and description for the Restore Recovery Location

Name:

Gold

Description:

High-priority tier location

Back

Next

Cancel

Step 3. Choose Recovery Options

At the **Recovery Options** step, specify whether you want to recover machines from vSphere backups, Veeam agent backups or both.

You can also choose whether you want to enable Instant VM Recovery for the location. With Instant VM Recovery, all processed machines will be immediately restored in the location by running directly from the backup files. Instant VM Recovery helps improve recovery time objectives (RTO), minimize disruption and downtime of the machines. For more information on the Instant VM Recovery feature, see the Veeam Backup & Replication User Guide, section [Instant VM Recovery](#).

Note that the Instant VM Recovery option is enabled by default (and you cannot disable it) when you recover machines from Veeam agent backups.

NOTE

Orchestrator currently supports recovering machines protected by Veeam Agent for Microsoft Windows and Veeam Agent for Linux only.

New Recovery Location

Recovery Location Type

Recovery Location Name

Recovery Options

Compute Resources

Storage Resources

Storage Options

Agent Networks

VM Networks

Re-IP Rules

Data Sovereignty

Summary

Recovery Options

Specify whether VMs and/or agents will be recovered here. Instant VM Recovery is required to restore agent backups.

☒ Recover Veeam agent backups


Recover new VMs from Veeam agent backups. Requires that Instant VM Recovery is enabled.

☒ Recover vSphere backups

Recover new VMs from vSphere backups.

☒ Enable instant VM Recovery

Launch VMs instantly from agent backups.

 Instant VM Recovery must be enabled if you plan to use this location for Quick Tests, or to restore agent backups.

Back

Next

Cancel

Step 4. Specify Compute Resources

At the **Compute Resources** step of the wizard, specify target hosts and clusters where recovered VMs will be registered. To do that, select the required resource groups in the list of available groups and click **Add**.

To view hosts and clusters in a resource group, select the group and click **View Resources**.

IMPORTANT

If you add a host to a recovery location and then move the host to another datacenter, or if you move a host from one vCenter Server to another, the host will be assigned a new vCenter MoRef ID, Orchestrator will consider the host to be a new infrastructure object, and the configuration of the recovery location will become invalid. As a result, Orchestrator will not be able to use this location for restore.

The screenshot shows the 'New Recovery Location' wizard with the 'Compute Resources' step selected in the left sidebar. The main area is titled 'Choose compute resource groups'. It features a search bar at the top right. Below the search bar, there are two lists: 'Available Groups' and 'Compute Groups'. The 'Available Groups' list contains 'Gold - Tier2' and 'Gold - Tier3'. The 'Compute Groups' list contains 'Gold - Tier1'. Between the two lists are 'Add >' and '< Remove' buttons. At the top right of the main area, there are 'Up', 'Down', and 'View Resources' icons. At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons.

Recovery Location Type	Recovery Location Name	Recovery Options	Compute Resources	Storage Resources	Storage Options	Agent Networks	VM Networks	Re-IP Rules	Data Sovereignty	Summary

Choose compute resource groups

Search

Available Groups ☐ Show empty Groups

- Gold - Tier2
- Gold - Tier3

Compute Groups

- Gold - Tier1

Back Next Cancel

Step 5. Specify Storage Resources

At the **Storage Resources** step of the wizard, specify destination datastores and datastore clusters where recovered VMs will be stored. To do that, select the required resource groups in the list of available groups and click **Add**.

For a resource group to be displayed in the **Available Groups** list, it must belong to the hosts and clusters selected at the [Compute Resources step](#).

To view datastores and datastore clusters included into a resource group, select the group and click **View Resources**.

The screenshot displays the 'New Recovery Location' wizard, specifically the 'Storage Resources' step. The interface is divided into a sidebar on the left and a main content area on the right.

Sidebar (Left): Contains a list of steps: Recovery Location Type, Recovery Location Name, Recovery Options, Compute Resources, **Storage Resources** (highlighted), Storage Options, Agent Networks, VM Networks, Re-IP Rules, Data Sovereignty, and Summary.

Main Content Area (Right): Titled 'Choose storage resource groups'. It features a search bar at the top. Below it, there are two columns: 'Available Groups' and 'Storage Groups'. The 'Available Groups' column lists four items: 'dpt - it', 'Gold - Tier2', 'Storage profile - Gold', and 'Storage profile - Silver', each with a green checkmark. The 'Storage Groups' column lists one item: 'Gold - Tier1', also with a green checkmark. Between these columns are 'Add >' and '< Remove' buttons. Above the 'Storage Groups' column are 'Up', 'Down', and 'View Resources' icons.

Footer: At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'. At the bottom left, there is an information icon and a note: 'Only Storage resources available to the previously selected Compute resources are shown here.'

Step 6. Specify Datastore Capacity Level

At the **Storage Options** step of the wizard, specify the datastore capacity level that must not be breached during the recovery process.

You can also choose whether you want Orchestrator to use backup files created by backup copy jobs when recovering machines. For more information on the way Orchestrator selects backup files and restore points to recover machines when performing restore operations, see [How Orchestrator Selects Backup Files](#).

New Recovery Location

Recovery Location Type

Recovery Location Name

Recovery Options

Compute Resources

Storage Resources

Storage Options

Agent Networks

VM Networks

Re-IP Rules

Data Sovereignty

Summary

Confirm storage options

vSphere Datastore Usage

Fill datastores up to:80% of capacity

Use Backup Copy Job Repository

If backup copies are located in the DR location, use them for recovery

☒ Use backup copy repository when restoring

i

If all datastores reach the threshold, the plan will halt.

Back

Next

Cancel

Step 7. Configure Network Mapping

[This step applies if you have selected the **Recover Veeam agent backups** at the **Recovery Options** step of the wizard, or if you have selected the **Recover vSphere backups** option and you want to enable the functionality of network mapping]

When you recover a VM from a vSphere backup, the recovered VM is connected to the same vSphere networks as the source VM; if the same networks are not available in the recovery location, you can create a network mapping table for the location so that the recovered VM is connected to the correct network. However, when you recover a machine from a Veeam agent backup, there are no vSphere networks that can be used — only the IP address of the source agent is known. Therefore, to recover Veeam agents, you must create at least one network mapping rule that maps an IP address range to a vSphere network so that the recovered VM is connected to the correct network.

To configure network mapping, at the **Network Mapping** step of the wizard, click **Add**. The **Add Network Mapping Rule** window will open.

1. Depending on whether you plan to recover machines from vSphere or Veeam agent backups, do the following in the **Source network** section:
 - To recover VMs from vSphere backups, from the **vCenter Server** list, select a vCenter Server that manages source VMs. Then, from the list of available networks, select a network to which the source VMs are connected.

For a vCenter Server to be displayed in the **vCenter Server** list, it must be connected to Orchestrator as described in section [Connecting VMware vSphere Servers](#).

- To recover machines from Veeam agent backups, specify a range of IP addresses that contains the IP addresses of the source agent machines. Alternatively, create a separate network mapping rule to map each individual IP address. Note that you must specify at least one network mapping rule.

NOTE

Orchestrator supports IP addresses in the IPv4 format only. If a machine that you want to recover has an IPv6 address, you must create the `0.0.0.0/0` mapping rule. Otherwise, Orchestrator may halt the recovery process.

2. In the **Target vSphere network** section, from the **vCenter Server** list, select a vCenter Server that will manage recovered VMs. Then, from the list of available networks, select a network to which the recovered VMs will be connected.

For a vCenter Server to be displayed in the **vCenter Server** list, it must be connected to Orchestrator as described in section [Connecting VMware vSphere Servers](#).

The screenshot shows the 'New Recovery Location' wizard in Veeam Disaster Recovery Orchestrator. The left sidebar contains a list of configuration steps: Recovery Location Type, Recovery Location Name, Recovery Options, Compute Resources, Storage Resources, Storage Options, Agent Networks, VM Networks (highlighted), Re-IP Rules, Data Sovereignty, and Summary. The main panel is titled 'Define network mapping to apply when recovering VMs from vSphere backups' and includes '+ Add', 'Edit', and 'Remove' icons. A 'Rule' section is visible below. Overlaid on this is the 'Add Network Mapping Rule' dialog box. The dialog has a title bar and a close button. Inside, it prompts the user to 'Enter a name for the rule and specify the source and target networks'. The 'Rule name' field contains 'VM Network in Prague to VM Network in Prague' and has a checked 'Set name automatically' checkbox. Below this, there are two columns: 'Source vSphere network' and 'Target vSphere network'. Each column contains three dropdown menus: 'vCenter Server' (both set to '172.17.52.34'), 'Datacenter' (both set to 'All Datacenters'), and 'Network' (both set to 'VM Network in Prague'). At the bottom of the dialog are 'Save' and 'Cancel' buttons. At the bottom of the main wizard window are 'Back', 'Next', and 'Cancel' buttons.

Step 8. Configure Re-IP Rules

[This step applies only if you want to enable the functionality of automatic IP address transformation for recovery of Microsoft Windows servers]

If the IP addressing scheme in the source location differs from the target location scheme, you can create re-IP rules for the recovery location, and Orchestrator will automatically reconfigure IP addresses of the recovered VMs. When recovering from a vSphere or agent backup, or failing back to a new location, Orchestrator checks if any of the specified re-IP rules will apply to the recovered VM: if a rule applies, Orchestrator will change the IP address configuration of the recovered VM using the Microsoft Windows registry.

IMPORTANT

To allow Orchestrator to reconfigure IP addresses of a recovered VM, the machine must have VMware Tools installed. This also applies to physical servers protected by Veeam agents if you plan to recover them to the VMware vSphere environment. The readiness check for any plan containing Veeam agents will confirm the presence of VMware Tools.

To configure a re-IP rule, at the **Re-IP Rules** step of the wizard, click **Add**. The **Add Re-IP Rule** window will open.

1. In the **Source VM** section, describe an IP numbering scheme adopted in the source location.
2. In the **Target VM** section, describe an IP numbering scheme adopted in the target location. Specify an IP address, subnet mask and default gateway that will be used for recovered VMs.
3. If necessary, define the DNS server addresses.
4. In the **Description** field, specify a brief outline for the rule or leave any related comments.
5. Click **Add**.

TIP

You can use the asterisk character (*) to specify a range of IP addresses.

New Recovery Location

Recovery Location Type

Recovery Location Name

Recovery Options

Compute Resources

Storage Resources

Storage Options

Agent Networks

VM Networks

Re-IP Rules

Data Sovereignty

Summary

Add Re-IP Rule

IP remapping

Source VM

Target VM

IP Address:

172 . 17 . 52 . *

172 . 17 . 53 . *

You can use the asterisk character (*) to specify a range of IP addresses (for example, 192.13.15.*).

Subnet mask:

255 . 255 . 254 . 0

255 . 255 . 254 . 0

Target VM options

Default gateway:

172 . 17 . 53 . 1

DNS server:

Preferred

Alternate

.

.

.

.

.

.

Description

Enter description text...

Add

Cancel

Back

Next

Cancel

Step 9. Enable VM Recovery Across Different Locations

To control data migration in the virtual infrastructure, Veeam Backup & Replication introduces infrastructure locations. A location defines a geographic region where an infrastructure object resides. To learn how to create and assign locations to infrastructure objects in Veeam Backup & Replication, see the Veeam Backup & Replication User Guide, section [Locations](#). To learn how to track geographical locations of production data, their copies and replicas, see the Veeam ONE Reporter User Guide, sections [Data Sovereignty Overview](#) and [Data Sovereignty Violations](#).

At the **Data Sovereignty** step of the wizard, choose whether you want Orchestrator to be able to recover VMs to a different location in Veeam Backup & Replication.

The screenshot shows the 'New Recovery Location' wizard in Veeam Backup & Replication. The left sidebar contains a list of steps: Recovery Location Type, Recovery Location Name, Recovery Options, Compute Resources, Storage Resources, Storage Options, Agent Networks, VM Networks, Re-IP Rules, Data Sovereignty (highlighted), and Summary. The main panel is titled 'Data Sovereignty' and contains the following text: 'Enforce data sovereignty using the infrastructure locations as defined in Veeam Backup & Replication. VMs will not be restored if data would breach the location boundary. For more information see the [Veeam Backup & Replication documentation](#).' Below this text is a checkbox labeled 'Enforce data sovereignty' which is checked. At the bottom right of the wizard are three buttons: 'Back', 'Next', and 'Cancel'.

New Recovery Location	
Recovery Location Type	Data Sovereignty
Recovery Location Name	Enforce data sovereignty using the infrastructure locations as defined in Veeam Backup & Replication. VMs will not be restored if data would breach the location boundary. For more information see the Veeam Backup & Replication documentation .
Recovery Options	<input checked="" type="checkbox"/> Enforce data sovereignty
Compute Resources	
Storage Resources	
Storage Options	
Agent Networks	
VM Networks	
Re-IP Rules	
Data Sovereignty	
Summary	

Back Next Cancel

Step 10. Finish Working with Wizard

At the **Summary** step of the wizard, review configuration information and click **Finish**.

New Recovery Location

Recovery Location Type

Recovery Location Name

Recovery Options

Compute Resources

Storage Resources

Storage Options

Agent Networks

VM Networks

Re-IP Rules

Data Sovereignty

Summary

Summary

Copy to clipboard

Properties

Recovery location name:

Restore Recovery Location

Type:

Restore

Description:

High-priority tier location

Recovery settings

Agents:

Enabled

VMs:

Enabled

Instant VM Recovery:

Enabled

Enforce data sovereignty:

Yes

Resources

Storage max usage %:

80

Use backup copies:

Yes

Compute Resources:

2 groups

Storage Resources:

1 group

Network mapping rules

Agent Networks:

1 rule

VM Networks:

1 rule

Re-IP Rules:

No rules chosen

Back

Finish

Cancel

Adding Storage Recovery Locations

To add a storage recovery location:

1. Switch to the **Administration** page.
2. Navigate to **Recovery Locations**.
3. Click **Add**.
4. Complete the **New Recovery Location** wizard:
 - a. [Choose a recovery location type](#).
 - b. [Specify a recovery location name and description](#).
 - c. [Choose a storage vendor](#).
 - d. [Specify target storage systems](#).
 - e. [Specify a target datacenter](#).
 - f. [Specify compute resources](#).
 - g. [Configure network mapping](#).
 - h. [Configure re-IP rules](#).
 - i. [Finish working with the wizard](#).

Step 1. Choose Recovery Location Type

At the **Recovery Location Type** step of the wizard, select the **Storage** option.

New Recovery Location

Recovery Location Type

Recovery Location Name

Storage Vendor

Target Storage Systems

Target Datacenter

Target Compute Resources

Network Mapping

Re-IP

Summary

Choose type of recovery location

☒ Storage

Contains storage systems, vSphere hosts to mount the storage, and VM network configuration.

☐ Restore

Contains vSphere hosts, datastores and VM network configuration.

☐ Cloud

A public cloud where Veeam agent and vSphere backups can be recovered as cloud VMs.

Next

Cancel

Step 2. Specify Recovery Location Name and Description

At the **Recovery Location Name** step of the wizard, use the **Name** and **Description** fields to enter a name for the new location and to provide a description for future reference. The maximum length of the location name is 64 characters; the following characters are not supported: * : / \ ? " < > | .

New Recovery Location

Recovery Location Type

Recovery Location Name

Storage Vendor

Target Storage Systems

Target Datacenter

Target Compute Resources

Network Mapping

Re-IP

Summary

Enter a name and description for the Storage Recovery Location

Name:

Critical Systems

Description:

High-priority tier location

Back

Next

Cancel

Step 3. Choose Storage Vendor

At the **Storage Vendor** step, choose whether NetApp or HPE storage systems will be used to recover VMs.

New Recovery Location

Recovery Location Type

Recovery Location Name

Storage Vendor

Target Storage Systems

Target Datacenter


Target Compute Resources


Network Mapping

Re-IP

Summary

Choose storage vendor

☒  NetApp ONTAP

☐  HPE Primera (3PAR)

Back

Next

Cancel

Step 4. Specify Target Storage Systems

At the **Target Storage Systems** step of the wizard, specify target storage systems to be used to recover VMs. To do that, select the required storage systems in the list of available systems and click **Add**.

To display the full list of all available storage systems including storage systems used in other storage recovery locations, select the **Show all systems** check box.

The screenshot shows the 'New Recovery Location' wizard at Step 4, 'Specify Target Storage Systems'. The left sidebar contains a list of steps: Recovery Location Type, Recovery Location Name, Storage Vendor, Target Storage Systems (highlighted), Target Datacenter, Target Compute Resources, Network Mapping, Re-IP, and Summary. The main area is titled 'Add Target Storage Systems' with the instruction 'Select Storage Systems that will be used to recover VMs.' It features a search bar, a 'View Datastores' link, and two columns: 'Available Systems' and 'Selected Systems'. The 'Available Systems' column contains one entry: '172.24.131.79 (pdcqastg14)'. The 'Selected Systems' column contains one entry: '172.24.131.57 (pdcqastg04)'. Between the columns are 'Add >' and '< Remove' buttons. A checkbox labeled 'Show all systems' is located above the 'Available Systems' list. At the bottom, there is an information icon and a note: 'To fail over VMs to the selected Storage Systems, Orchestrator will use settings configured for this Storage Recovery Location.' Navigation buttons 'Back', 'Next', and 'Cancel' are at the bottom right.

Recovery Location Type	Add Target Storage Systems	
Recovery Location Name	Select Storage Systems that will be used to recover VMs.	
Storage Vendor	<input type="text" value="Search"/>	
Target Storage Systems	View Datastores	
Target Datacenter	Available Systems <input type="checkbox"/> Show all systems	
Target Compute Resources	Selected Systems	
Network Mapping	172.24.131.79 (pdcqastg14) Add > < Remove 172.24.131.57 (pdcqastg04)	
Re-IP		
Summary		

To fail over VMs to the selected Storage Systems, Orchestrator will use settings configured for this Storage Recovery Location.

Back Next Cancel

Step 5. Specify Target Datacenter

At the **Target Datacenter** step of the wizard, select a vCenter Server that will manage recovered VMs, and then specify a datacenter to be used to recover VMs. The recovered VMs will be distributed across resources of this datacenter.

New Recovery Location

Recovery Location Type

Recovery Location Name

Storage Vendor

Target Storage Systems

Target Datacenter

Target Compute Resources

Network Mapping

Re-IP

Summary

Choose a target datacenter

Choose a datacenter that will be used to perform failover.

vCenter Server:

qahv1.veeam.local

Datacenter:

select...

Vklim_DC

VKlim_DC_2

Back

Next

Cancel

Step 6. Specify Compute Resources

At the **Target Compute Resources** step of the wizard, specify target hosts and clusters to which recovered volumes will be mounted. To do that, select a resource group in the list of available groups and click **Add**.

For a resource group to be displayed in the **Available Groups** list, it must belong to the datacenter selected at the [Target Datacenter step](#). If a resource group belongs to multiple datacenters at the same time, it will not be displayed in **Available Groups** list.

To view hosts and clusters in a resource group, select the group and click **View Resources**.

IMPORTANT

If you add a host to a recovery location and then move the host to another datacenter, or if you move a host from one vCenter Server to another, the host will be assigned a new vCenter MoRef ID, Orchestrator will consider the host to be a new infrastructure object, and the configuration of the recovery location will become invalid. As a result, Orchestrator will not be able to use this location for recovery.

New Recovery Location

Recovery Location Type

Recovery Location Name

Storage Vendor

Target Storage Systems

Target Datacenter

Target Compute Resources

Network Mapping

Re-IP

Summary

Add target compute resources

Select Groups that contain the necessary clusters and hosts to the Storage Recovery Location. These Groups will be used to mount replicated storage volumes.

Search

View Resources

Available Groups

Host2 - Host2

Host3 - Host3

Host4 - Host4

Host5 - Host5

Add >

< Remove

Selected Groups

Host1 - Host1

i

You can select only those Groups that have all their resources located on the Target Datacenter.

Back

Next

Cancel

Step 7. Configure Network Mapping

[This step applies only if you want to enable the functionality of network mapping]

By default, a recovered VM is connected to the same networks as the source VM. If the network configuration in the recovery location does not match the production network configuration, you can create a network mapping table for the location so that the recovered VM is connected to the correct network.

To configure network mapping, at the **Network Mapping** step of the wizard, click **Add**. The **Add Network Mapping Rule** window will open.

1. In the **Source vSphere network** section, from the **vCenter Server** list, select a vCenter Server that manages source VMs. Then, from the list of available networks, select a network to which the source VMs are connected.

For a vCenter Server to be displayed in the **vCenter Server** list, it must be connected to Orchestrator as described in section [Connecting VMware vSphere Servers](#).

2. In the **Target vSphere network** section, from the list of available networks, select a network to which recovered VMs will be connected.

Since [you have already specified the target datacenter](#) to be used, the wizard only allows you to change the target network.

The screenshot shows the 'New Recovery Location' wizard with the 'Network Mapping' step selected. The 'Add Network Mapping Rule' dialog is open, prompting the user to 'Enter a name for the rule and specify the source and target networks'.

Rule name: DPortGroup 4 (DC in folder - DSwitch in Datacenter) ☒ Set name automatically

Source vSphere network

- vCenter Server: cdpvc.qahv1.veeam.local
- Datacenter: All Datacenters
- Network: DPortGroup 4 (DC in folder - DSwitch in C) (selected)

Target vSphere network

- vCenter Server: vklimvc.qahv1.veeam.local
- Datacenter: VKlim_DC_2
- Network: DPortGroup2 (DSwitch2 in VKlim_DC_2) (selected)

The dialog includes 'Back', 'Next', and 'Cancel' buttons at the bottom right.

Step 8. Configure Re-IP Rules

[This step applies only if you want to enable the functionality of automatic IP address transformation for recovery of Microsoft Windows servers]

If the network configuration in the source location does not match the production network configuration, you can create re-IP rules for the recovery location, and Orchestrator will automatically reconfigure IP addresses of the recovered VMs. During storage failover, Orchestrator checks if any of the re-IP rules will apply to the recovered VM: if a rule applies, Orchestrator will change the IP address configuration of the recovered VM using the Microsoft Windows registry.

IMPORTANT

To allow Orchestrator to reconfigure IP addresses of a recovered VM, the VM must have VMware Tools installed.

To configure a re-IP rule, at the **Re-IP Rules** step of the wizard, click **Add**. The **Add Re-IP Rule** window will open.

1. In the **Source VM** section, describe an IP numbering scheme adopted in the source location.
2. In the **Target VM** section, describe an IP numbering scheme adopted in the target location. Specify an IP address, subnet mask and default gateway that will be used for recovered VMs.
3. If necessary, define the DNS server addresses.
4. In the **Description** field, specify a brief outline for the rule or leave any related comments.
5. Click **Add**.

TIP

You can use the asterisk character (*) to specify a range of IP addresses.

New Recovery Location

Recovery Location Type

Recovery Location Name

Storage Vendor

Target Storage Systems

Target Datacenter

Target Compute Resources

Network Mapping

Re-IP

Summary

Add Re-IP Rule

IP remapping

Source VM

Target VM

IP Address:

172 . 17 . 52 . *

172 . 17 . 53 . *

You can use the asterisk character (*) to specify a range of IP addresses (for example, 192.13.15.*).

Subnet mask:

255 . 255 . 254 . 0

255 . 255 . 254 . 0

Target VM options

Default gateway:

172 . 17 . 53 . 1

Preferred

Alternate

DNS server:

.

.

.

.

.

.

Description

Enter description text...

Add

Cancel

Back

Next

Cancel

Step 9. Finish Working with Wizard

At the **Summary** step of the wizard, review configuration information and click **Finish**.

New Recovery Location

Recovery Location Type

Recovery Location Name

Storage Vendor

Target Storage Systems

Target Datacenter

Target Compute Resources

Network Mapping

Re-IP

Summary

Recovery Location will be created with the settings below

Copy to clipboard

Properties

Recovery location name:

Critical Systems

Type:

Storage

Description:

High-priority tier location

Vendor:

NetApp ONTAP

Resources

Target vCenter Server:

vklimvctest.qahv1.veeam.local

Target datacenter:

VKlim_DcV8

Storage systems:

172.24.144.57 (svm-fc)

Compute resources:

1 group

Network mapping rules

VM Mappings:

1 rule

Re-IP Rules:

1 rule

Back

Finish

Cancel

Adding Cloud Recovery Locations

To add a cloud recovery location:

1. Switch to the **Administration** page.
2. Navigate to **Recovery Locations**.
3. Click **Add**.
4. Complete the **New Recovery Location** wizard:
 - a. [Choose a recovery location type](#).
 - b. [Specify a recovery location name and description](#).
 - c. [Specify recovery options](#).
 - d. [Choose backup servers](#).
 - e. [Choose a cloud subscription](#).
 - f. [Specify repositories](#).
 - g. [Configure proxies](#).
 - h. [Choose a region](#).
 - i. [Choose a resource group](#).
 - j. [Specify a cloud VM configuration](#).
 - k. [Configure network mapping](#).
 - l. [Specify a quarantine network](#).
 - m. [Finish working with the wizard](#).

Step 1. Choose Recovery Location Type

At the **Recovery Location Type** step of the wizard, select the **Cloud** option.

New Recovery Location

Recovery Location Type

Recovery Location Name

Recovery Options

Backup Servers

Subscription

Repositories

Proxies

Region

Resource Group

Cloud VM Configuration

Quarantine network

Summary

Choose type of recovery location

☐ Storage

Contains storage systems, vSphere hosts to mount the storage, and VM network configuration.

☐ Restore

Contains vSphere hosts, datastores and VM network configuration.

☒ Cloud

A public cloud where Veeam agent and vSphere backups can be recovered as cloud VMs.

Next

Cancel

Step 2. Specify Recovery Location Name and Description

At the **Recovery Location Name** step of the wizard, use the **Name** and **Description** fields to enter a name for the new location and to provide a description for future reference. The maximum length of the location name is 64 characters; the following characters are not supported: * : / \ ? " < > | .

New Recovery Location

Recovery Location Type

Recovery Location Name

Recovery Options

Backup Servers

Subscription

Repositories

Proxies

Region

Resource Group

Cloud VM Configuration

Quarantine network

Summary

Enter a name and description for the cloud recovery location

Name:

Cloud Recovery Location

Description:

Recovering to Microsoft Azure

Back

Next

Cancel

Step 3. Specify Recovery Options

At the **Recovery Options** step, specify whether you want to recover machines from vSphere backups, Veeam agent backups or both.

NOTE

Orchestrator only supports agent backups created by Veeam Agent for Microsoft Windows or Veeam Agent for Linux.

New Recovery Location

Recovery Location Type

Recovery Location Name

Recovery Options

Backup Servers

Subscription

Repositories

Proxies

Region

Resource Group

Cloud VM Configuration

Agent Network Mapping

VM Network Mapping

Quarantine network

Summary

Choose recovery Options

Specify whether VMs and/or agents will be recovered here

☒ Recover Veeam agent backups

Recover new VMs from Veeam agent backups.

☒ Recover vSphere backups

Recover new VMs from vSphere backups.

Back

Next

Cancel

Step 4. Choose Backup Servers

At the **Backup Servers** step of the wizard, select a Veeam Backup & Replication server that will manage the process of recovering machines to Microsoft Azure. Note that one Veeam Backup & Replication server can be associated with one recovery location only.

For a Veeam Backup & Replication server to be displayed in the list of available servers, it must be added to Orchestrator as described in section [Connecting Veeam Backup & Replication Servers](#).

IMPORTANT

- To restore workloads to Microsoft Azure, you must add a Microsoft Azure compute account to Veeam Backup & Replication. When you add an Azure compute account, Veeam Backup & Replication imports information about subscriptions and resources associated with this account. If you do not add a compute account to the configuration of a Veeam Backup & Replication server, you will not be able to choose the server when creating a cloud recovery location. For more information on adding Microsoft Azure compute accounts, see the Veeam Backup & Replication User Guide, section [Microsoft Azure Compute Accounts](#).
- The added account must have the permissions required to access Microsoft Azure resources. For more information, see the Veeam Backup & Replication User Guide, section [Creating Custom Role for Azure Account](#).

New Recovery Location

Recovery Location Type

Recovery Location Name

Recovery Options

Backup Servers

Subscription

Repositories

Proxies

Region

Resource Group

Cloud VM Configuration

Agent Network Mapping

VM Network Mapping

Quarantine network

Summary

Choose Veeam Backup & Replication server that will perform restore to this location

Backup Server

Veeam Backup & Replication Server	Version	Agent Status
178.24.18.184	12.0.0.1106	Healthy
172.04.28.207	12.0.0.1120	Healthy
VAO11	12.0.0.1276	Healthy

i

Only backups made by the selected server can be recovered. To use another server, create another location.

Back

Next

Cancel

Step 5. Choose Cloud Subscription

At the **Subscription** step of the wizard, select a Microsoft Azure cloud subscription whose resources you want to use to recover machines.

For a subscription to be displayed in the list of available subscriptions, it must be associated with the compute account added to Veeam Backup & Replication. For more information on adding Microsoft Azure compute accounts, see the Veeam Backup & Replication User Guide, section [Microsoft Azure Compute Accounts](#).

New Recovery Location

Recovery Location Type

Recovery Location Name

Recovery Options

Backup Servers

Subscription

Repositories

Proxies

Region

Resource Group

Cloud VM Configuration

Agent Network Mapping

VM Network Mapping

Quarantine network

Summary

Choose cloud subscription

Subscription

Subscription	Compute Account	Description
Enterprise	Veeam account	Account for restore

Back

Next

Cancel

Step 6. Specify Repositories

At the **Repositories** step of the wizard, specify backup repositories where the restore points of machines that you plan to recover are stored. To do that, select a repository in the list of available repositories and click **Add**.

For a backup repository to be displayed in the list of the available repositories, it must be added to the backup infrastructure as described in section [Adding Backup Repositories](#). You can use regular repositories (Windows, Linux), object storage (Microsoft Azure) and scale-out backup repositories. Tape and deduplicating storage appliances are not supported.

IMPORTANT

For Veeam Backup & Replication to be able to access the selected repositories using your cloud accounts, the credentials of these accounts must be kept up to date. This means that if you update credentials of a cloud account that is used to connect to a cloud service, you must also update these credentials in the Veeam Backup & Replication console as described in the Veeam Backup & Replication User Guide, section [Cloud Credentials Manager](#).

The screenshot shows the 'New Recovery Location' wizard in the Veeam Backup & Replication console. The left sidebar contains a list of configuration steps: Recovery Location Type, Recovery Location Name, Recovery Options, Backup Servers, Subscription, **Repositories** (highlighted), Proxies, Region, Resource Group, Cloud VM Configuration, Agent Network Mapping, VM Network Mapping, Quarantine network, and Summary. The main area is titled 'Choose repositories that will be used for cloud recovery'. It features a search bar at the top. Below it, there are two columns: 'Available repositories' and 'Selected repositories'. The 'Available repositories' column lists 'Default Backup Repository' and 'Empty repo', with 'Empty repo' selected. Between the columns are 'Add >' and '< Remove' buttons. The 'Selected repositories' column lists 'Backup copy' and 'Object storage repository 1'. At the bottom of the main area, there is an information icon and a message: 'All selected repositories will be searched for the latest restore point.' The bottom of the wizard has three buttons: 'Back', 'Next', and 'Cancel'.

New Recovery Location	
Recovery Location Type	Choose repositories that will be used for cloud recovery
Recovery Location Name	Search <input type="text"/>
Recovery Options	
Backup Servers	
Subscription	
Repositories	
Proxies	
Region	
Resource Group	
Cloud VM Configuration	
Agent Network Mapping	
VM Network Mapping	
Quarantine network	
Summary	

Available repositories		Selected repositories
Default Backup Repository	Add > < Remove	Backup copy
Empty repo		Object storage repository 1

Information: All selected repositories will be searched for the latest restore point.

Back Next Cancel

Step 7. Specify Proxies

Veeam Backup & Replication servers can use multiple dedicated backup proxies to speed up the recovery process. For more information on backup proxies, see the Veeam Backup & Replication User Guide, section [Backup Proxy](#).

At the **Proxies** step of the wizard, specify the proxies to be used. To do that, select a proxy in the list of available proxies and click **Add**. If you have selected a cloud repository as a target location for storing restore points at [step 6](#), choose a cloud proxy to speed up the recovery process.

IMPORTANT

To recover machines protected by Veeam Agent for Linux, ensure that you have added a proxy appliance for Linux to the backup infrastructure.

The screenshot shows the 'New Recovery Location' wizard in Veeam Backup & Replication. The 'Proxies' step is selected in the left-hand navigation pane. The main area is titled 'Choose cloud proxies that will be used for recovery'. It features a search bar at the top. Below the search bar, there are two columns: 'Available proxies' and 'Selected proxies'. The 'Available proxies' column currently shows 'No Records'. The 'Selected proxies' column contains one entry: 'WIN-A4C476RNAIB.tech.local'. Between these columns are two buttons: 'Add >' and '< Remove'. At the bottom of the main area, there is an information icon and a note: 'Multiple proxies will use a round-robin method. For details on deploying cloud proxies, see the [Veeam Backup & Replication documentation](#).' At the bottom right of the wizard, there are three buttons: 'Back', 'Next', and 'Cancel'.

Step 8. Choose Regions

At the **Regions** step of the wizard, select a Microsoft Azure region in which the recovered VMs will reside.

For a region to be displayed in the list of available regions, it must belong to the subscription specified at [step 5](#). Note that Early Updates Access Program (EUAP) regions are not supported.

NOTE

For Orchestrator to deploy the recovered VMs in the selected region, you must have sufficient resource quota allocated to your subscription. To learn how to check your quotas, see [Microsoft Azure documentation](#).

New Recovery Location

Recovery Location Type

Recovery Location Name

Recovery Options

Backup Servers

Subscription

Repositories

Proxies

Region

Resource Group

Cloud VM Configuration

Agent Network Mapping

VM Network Mapping

Quarantine network

Summary

Choose the region where VMs will be recovered.

Search

South Africa West

South Central US

Southeast Asia

South India

Sweden Central

Switzerland North

Switzerland West

UAE Central

UAE North

UK South

UK West

West Central US

West Europe

West India

West US

West US 2

West US 3

Back

Next

Cancel

Step 9. Choose Resource Group

At the **Resource Group** step of the wizard, select a resource group to which the recovered VMs will belong.

For a resource group to be displayed in the **Resource Group** list, it must be created for the region specified at [step 8](#) in the Microsoft Azure portal, as described in [Microsoft Docs](#).

New Recovery Location

Recovery Location Type

Recovery Location Name

Recovery Options

Backup Servers

Subscription

Repositories

Proxies

Region

Resource Group

Cloud VM Configuration

Agent Network Mapping

VM Network Mapping

Quarantine network

Summary

Choose resource group

Resource Group: asdasdasd_group

asdasdasd_group

Default-Storage-WestUS

veeam-confirm1 - rge3a43028093179597f9349aa9720f5d4daa

veeam-confirm- rg86611636ef48a88506a54324834e04457011

veeam-restorestaging-5b0502ea-0ec0-415c-8496-8992fa2ce0ae

Rescan

Back

Next

Cancel

Step 10. Specify Cloud VM Configuration

A VM configuration is a combination of a VM series and disk type that Orchestrator uses to create new VMs in Microsoft Azure.

To recover machines in a cloud plan, you must specify at least one VM configuration at the **Cloud VM Configuration** step of the wizard:

1. Click **Choose** in the **VM Series** field.
2. In the **Choose VM Series** window, specify the necessary VM series and click **Apply**.

To help you choose the VM series, the table in the **Choose VM Series** window will provide information on the maximums for the number of vCPU cores, system RAM and attached disks for each available VM size. For the full description of Microsoft Azure VM sizes, see [Microsoft Docs](#).

3. Use the **Disk** drop-down list to select the type of disks that will be attached to the recovered VMs.

The specified VM series will be used as the basis for machines recovered in Microsoft Azure as new VMs. The created VMs will be customized to best match the CPU and memory configuration of the source machines. If you want different machines to be recovered using different settings, you can add up to 2 more VM configurations. If you create another VM configuration, you must also modify the parameters of the **Create Cloud VM** step to use it, as described in section [Working with Cloud Plans](#).

New Recovery Location

Recovery Location Type

Recovery Location Name

Recovery Options

Backup Servers

Subscription

Repositories

Proxies

Region

Resource Group

Cloud VM Configuration

Agent Network Mapping

VM Network Mapping

Quarantine network

Summary

Create cloud VM configurations

Create at least one VM configuration. You can choose per-VM which configuration will be used for recovery when editing the plan.

Choose VM Series

Search by name

Refresh

Series	Max CPUs	Max RAM (GB)	Max Disks	Premium SSD
Standard_A	8	56	16	Not supported
Standard_A_v2	8	16	16	Not supported
Standard_Am_v2	8	64	16	Not supported
Standard_B1s	1	0.5	2	Supported
Standard_Bms	20	80	32	Supported
Standard_Bs	2	4	4	Supported
Standard_D	16	112	64	Not supported
Standard_D_v2	20	140	64	Not supported
Standard_D_v3	64	256	32	Not supported
Standard_D_v4	64	256	32	Not supported

i For VM specifications, see the [Microsoft Azure documentation](#).

Apply Cancel

Back Next Cancel

Step 11. Configure Network Mapping

When you recover a machine from a Veeam agent backup or a VM from a vSphere backup to a cloud environment, Orchestrator is not able to connect the recovered VM to the same networks as the source machine – that is why you must create at least one network mapping rule for the location so that the recovered VM is connected to the correct network.

To configure network mapping, at the **Network Mapping** step of the wizard, click **Add**. The **Add Network Mapping Rule** window will open.

1. Depending on whether you plan to recover machines from vSphere or agent backups, do the following in the **Source network** section:
 - To recover machines from Veeam agent backups, specify a range of IP addresses that contains the IP addresses of the source agent machines. Alternatively, create a separate network mapping rule to map each individual IP address.
 - To recover VMs from vSphere backups, from the **vCenter Server** list, select a vCenter Server that manages source VMs. Then, from the list of available networks, select a network to which the source VMs are connected.

For a vCenter Server to be displayed in the **vCenter Server** list, it must be connected to Orchestrator as described in section [Connecting VMware vSphere Servers](#).

NOTE

Orchestrator supports IP addresses in IPv4 format only. If a machine that you want to recover has an IPv6 address, you must create a mapping rule `0.0.0.0/0` (this will map all networks). Otherwise, Orchestrator may halt the recovery process.

2. In the **Target network** section, select a virtual network and a subnet to which you want to connect the recovered VMs. For a virtual network to be displayed in the **Cloud network** list, it must be created in the Microsoft Azure portal for the region selected at [step 8](#), as described in [Microsoft Docs](#). For a subnet to be displayed in the **Subnets** list, it must be created in the Microsoft Azure portal for the specified virtual network, as described in [Microsoft Docs](#).

You can also specify a security group (virtual firewall) that will be associated with the recovered VMs. For a network security group to be displayed in the **Security Groups** list, it must be created and associated to the necessary subnet in the Microsoft Azure portal as described in [Microsoft Docs](#).

IMPORTANT

If IP address ranges for different rules overlap, Orchestrator will use the mapping in the rule with the narrowest range.

New Recovery Location

Recovery Location Type

Recovery Location Name

Recovery Options

Backup Servers

Subscription

Repositories

Proxies

Region

Resource Group

Cloud VM Configuration

Agent Network Mapping

VM Network Mapping

Quarantine network

Summary

Define network mapping to apply when recovering Veeam agent backups

Search by name

Add Network Mapping Rule

Enter a name for the rule and specify the source and target networks

Rule name:
 ☒ Set name automatically

Source vSphere network

vCenter Server:

Datacenter:

Network:

Target cloud network

Cloud network:

Subnets:

Security Groups:

Step 12. Specify Quarantine Network

You can scan machine disks for possible ransomware before restoring them to the production environment. During ransomware scan, Orchestrator iterates through the number of restore points [specified while running the plan](#) one by one to detect a restore point with no viruses. By default, if all restore points of a machine are infected, Orchestrator halts the restore. However, you can instruct Orchestrator to restore the machine to a quarantine network. After you delete all malicious software, run the plan again to restore the machine to the recovery location.

At the **Quarantine Network** step of the wizard, specify a network and a subnet to which you want to connect the infected machines.

NOTE

Orchestrator allows you to perform ransomware scan only for those machines whose restore points are stored in on-premises repositories. If a restore point is stored in a cloud repository, Orchestrator will be unable to perform the scan. For more information, see [How Orchestrator Performs Ransomware Scan](#).

The screenshot shows the 'New Recovery Location' wizard in Veeam Disaster Recovery Orchestrator. The 'Quarantine network' step is selected in the left-hand navigation pane. The main content area is titled 'Quarantine network' and includes the instruction: 'Machines that fail a ransomware scan can be recovered to a quarantine network.' Below this, there is a checkbox labeled 'Specify quarantine network for ransomware recovery' which is checked. Underneath the checkbox, there are two dropdown menus: 'Cloud network:' with the value 'alesch-wus-vnet' and 'Subnets:' with the value 'default'. At the bottom right of the wizard, there are three buttons: 'Back', 'Next', and 'Cancel'.

New Recovery Location	
Recovery Location Type	Quarantine network Machines that fail a ransomware scan can be recovered to a quarantine network.
Recovery Location Name	
Recovery Options	
Backup Servers	
Subscription	
Repositories	
Proxies	
Region	
Resource Group	
Cloud VM Configuration	
Agent Network Mapping	
VM Network Mapping	
Quarantine network	<input checked="" type="checkbox"/> Specify quarantine network for ransomware recovery Cloud network: alesch-wus-vnet Subnets: default
Summary	

Back Next Cancel

Step 13. Finish Working with Wizard

At the **Summary** step of the wizard, review configuration information and click **Finish**.

New Recovery Location

Recovery Location Type

Recovery Location Name

Recovery Options

Backup Servers

Subscription

Repositories

Proxies

Region

Resource Group

Cloud VM Configuration

Agent Network Mapping

VM Network Mapping

Quarantine network

Summary

Summary

Copy to clipboard

Recovery location name:

Cloud Recovery Location

Type:

Cloud

Description:

Recovering to Microsoft Azure

Recover Agents:

Enabled

Recover VMs:

Enabled

Veeam infrastructure

Backup Servers:

172.04.28.207

Repositories:

1 repositories

Proxies:

1 proxies

Cloud settings

Subscription:

Enterprise

Region:

West US

Resource Group:

veeam-restorestaging-5b0502ea-0ec0-415c-8496-8992fa2ce0ae

Cloud VM configurations

Config 1:

Standard_B1s, StandardHDD

Network mapping rules

Agent Mappings:

1 rule

VM Mappings:

1 rule

Back

Finish

Cancel

Configuring Recovery Locations

If you want to change settings specified [while adding a recovery location](#), the Orchestrator UI allows you to customize the location.

1. Switch to the **Administration** page.
2. Navigate to **Recovery Locations**.
3. Select the location and click **Edit**.
4. Complete the **Edit Recovery Location** wizard:
 - To change the name and description of the location, follow the instructions provided in section [Adding Restore Recovery Locations](#) (step 2), [Adding Storage Recovery Locations](#) (step 2) or [Adding Cloud Recovery Location](#) (step 2).
 - To change the specified recovery options, follow the instructions provided in section [Adding Restore Recovery Locations](#) (step 3) or [Adding Cloud Recovery Locations](#) (step 3).
 - To configure network mapping, follow the instructions provided in section [Adding Restore Recovery Locations](#) (step 7), [Adding Storage Recovery Locations](#) (step 7) or [Adding Cloud Recovery Location](#) (step 11).
 - To configure re-IP rules for recovered VMs, follow the instructions provided in section [Adding Restore Recovery Locations](#) (step 8) or [Adding Storage Recovery Locations](#) (step 8).
 - [These steps apply only to restore recovery locations]

To change the target hosts and clusters where recovered VMs will be registered, follow the instructions provided in section [Adding Restore Recovery Locations](#) (step 4).

To change the destination datastores and datastore clusters where machine files will be stored, follow the instructions provided in section [Adding Restore Recovery Locations](#) (step 5).

To change the datastore capacity level that must not be breached during the recovery process, follow the instructions provided in section [Adding Restore Recovery Locations](#) (step 6).

To enable or disable VM recovery across different Veeam Backup & Replication locations, follow the instructions provided in section [Adding Restore Recovery Locations](#) (step 9).
 - [These steps apply only to storage recovery locations]

To change the target storage systems used to recover VMs, follow the instructions provided in section [Adding Storage Recovery Locations](#) (step 4).

To change the datacenter used to recover VMs, follow the instructions provided in section [Adding Storage Recovery Locations](#) (step 5).

To change target hosts and clusters to which recovered volumes will be mounted, follow the instructions provided in section [Adding Storage Recovery Locations](#) (step 6).
 - [These steps apply only to cloud recovery locations]

To change the Veeam Backup & Replication server that will manage the process of recovering machines to Microsoft Azure, follow the instructions provided in section [Adding Cloud Recovery Location](#) (step 4).

To change the Microsoft Azure cloud subscription, follow the instructions provided in section [Adding Cloud Recovery Location](#) (step 5).

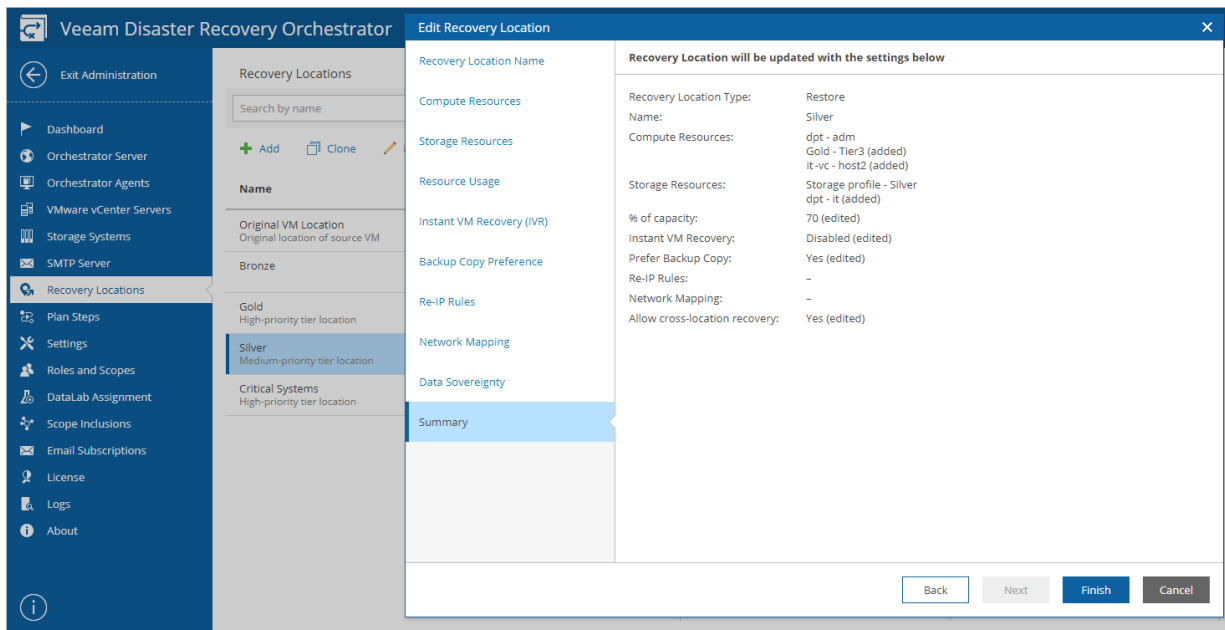
To change the repositories where the machine restore points are stored, follow the instructions provided in section [Adding Cloud Recovery Location](#) (step 6).

To change the cloud proxies used for job performance optimization, follow the instructions provided in section [Adding Cloud Recovery Location](#) (step 7).

To change the Microsoft Azure region in which the recovered VMs will reside, follow the instructions provided in section [Adding Cloud Recovery Location](#) (step 8).

To change the resource group to which the recovered VMs will belong, follow the instructions provided in section [Adding Cloud Recovery Location](#) (step 9).

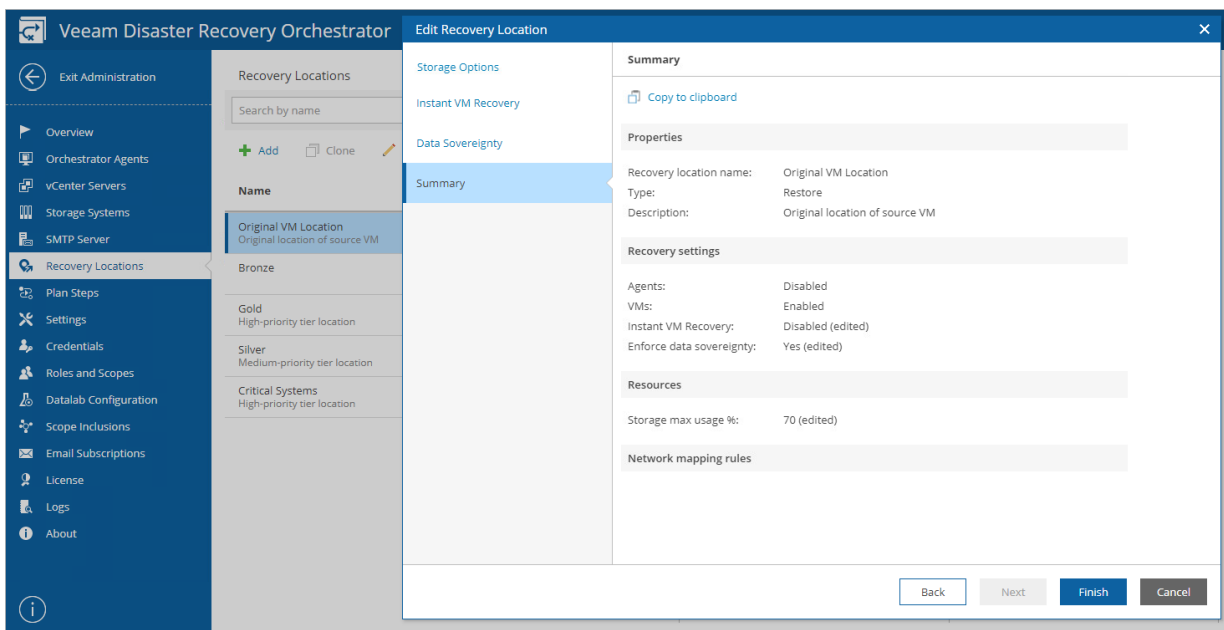
To specify or change the quarantine network that will be used for infected machines, follow the instructions provided in section [Adding Cloud Recovery Location](#) (step 12).



Configuring Original Recovery Location

Since all resource groups included in the *Original Recovery Location* are empty by default and depend on processed machines, you cannot customize its resource settings. However, you can still customize some general settings for the location:

1. Switch to the **Administration** page.
2. Navigate to **Recovery Locations**.
3. In the list of recovery locations, select *Original VM Location*, and click **Edit**.
4. Complete the **Edit Recovery Location** wizard:
 - To change the datastore capacity level that must not be breached during the recovery process and choose whether to use a backup copy repository when restoring machines, follow the instructions provided in section [Adding Restore Recovery Locations](#) (step 6).
 - To choose whether you want to enable Instant VM Recovery for the location, follow the instructions provided in section [Adding Restore Recovery Locations](#) (step 3).
 - To choose whether you want Orchestrator to be able to recover VMs across different locations in Veeam Backup & Replication when running orchestration plans, follow the instructions provided in section [Adding Restore Recovery Locations](#) (step 9).



Allowing Access to Recovery Locations

Unless a recovery location is *INCLUDED* into the list of inventory items for a scope, it will not be available for use in the scope. By default, all locations are excluded from newly created scopes; only the *Admin Scope* has all locations included.

NOTE

By design, the list of available recovery locations will always display restore and cloud recovery locations only. For storage recovery locations, there is no need to allow access – Orchestrator automatically identifies the locations to be used when running storage plans. For more information on the way Orchestrator analyzes storage recovery locations, see [How Orchestrator Places VMs During Storage Failover](#).

To modify the list of recovery locations available for a scope:

1. Switch to the **Administration** page.
2. Navigate to **Scope Inclusions > Recovery Locations**.
3. Select the scope:
 - a. Click the **Scopes** link.
 - b. In the **Change Scope** window, select a check box next to the required scope, and click **Apply**.
4. Select check boxes next to the necessary locations, and click **Include** or **Exclude**.

TIP

You can simultaneously edit the list of inventory items available for multiple scopes. To do that, select check boxes next to the required scopes in the **Change Scope** window. After you click **Include** or **Exclude**, the changes will be applied to all the selected scopes at the same time.

The screenshot shows the Veeam Disaster Recovery Orchestrator interface. The left sidebar contains navigation links: Exit Administration, Overview, Orchestrator Agents, vCenter Servers, Storage Systems, SMTP Server, Recovery Locations, Plan Steps, Settings, Credentials, Roles and Scopes, Datablab Configuration, Scope Inclusions, Email Subscriptions, License, Logs, and About. The main content area is titled 'Veeam Disaster Recovery Orchestrator' and shows a notification: 'Changes will be applied to the following Scopes (1 of 4): Exchange Administrators'. Below this, there are tabs for Groups, Recovery Locations (selected), Plan Steps, Credentials, and Template Jobs. A search bar is present. Below the search bar, there are buttons for '+ Include' and '- Exclude'. A table lists recovery locations with columns for Name and Inclusion. The 'Gold' location is selected and marked as 'Included'. The right-hand pane displays 'Location Settings' and 'Resources' for the selected location.

Name	Inclusion
<input type="checkbox"/> Original VM Location	<input checked="" type="radio"/> Included
<input checked="" type="checkbox"/> Gold	<input type="radio"/> Not included
<input type="checkbox"/> Cloud Recovery Location	<input type="radio"/> Not included

Location Settings

Properties

Recovery location name	Gold
Type	Restore
Recover Agents	Enabled
Recover VMs	Enabled
Instant VM Recovery	Enabled
Data sovereignty	Enabled
Description	High-priority tier location

Resources

Storage max usage, %	80
Use Backup Copies	Disabled
Compute resources	1 group
Storage resources	1 group

Network mapping rules

Agent mappings	2 rules
VM mappings	1 rule
Re-IP rules	1 rule

After you make a recovery location *INCLUDED* for a scope, Plan Authors will be able to use this location for restore and cloud plans in the scope, and also when running failback. For more information on creating and editing various plan types, see [Working with Replica Plans](#), [Working with CDP Replica Plans](#), [Working with Restore Plans](#) and [Working with Cloud Plans](#).

Configuring Plan Steps

Plan steps are the sequence of actions taken by the Orchestrator server during plan execution. For each machine in an inventory group included in an orchestration plan, 2 types of steps can be performed:

- [Default steps provided by Veeam](#)
- [Custom steps added by end user](#)

For detailed description of all available orchestration plan steps, see [Appendix. Orchestration Plan Steps](#).

Allowing Access to Plan Steps

NOTE

You cannot delete built-in steps provided by Veeam. This option is available for [custom steps](#) only.

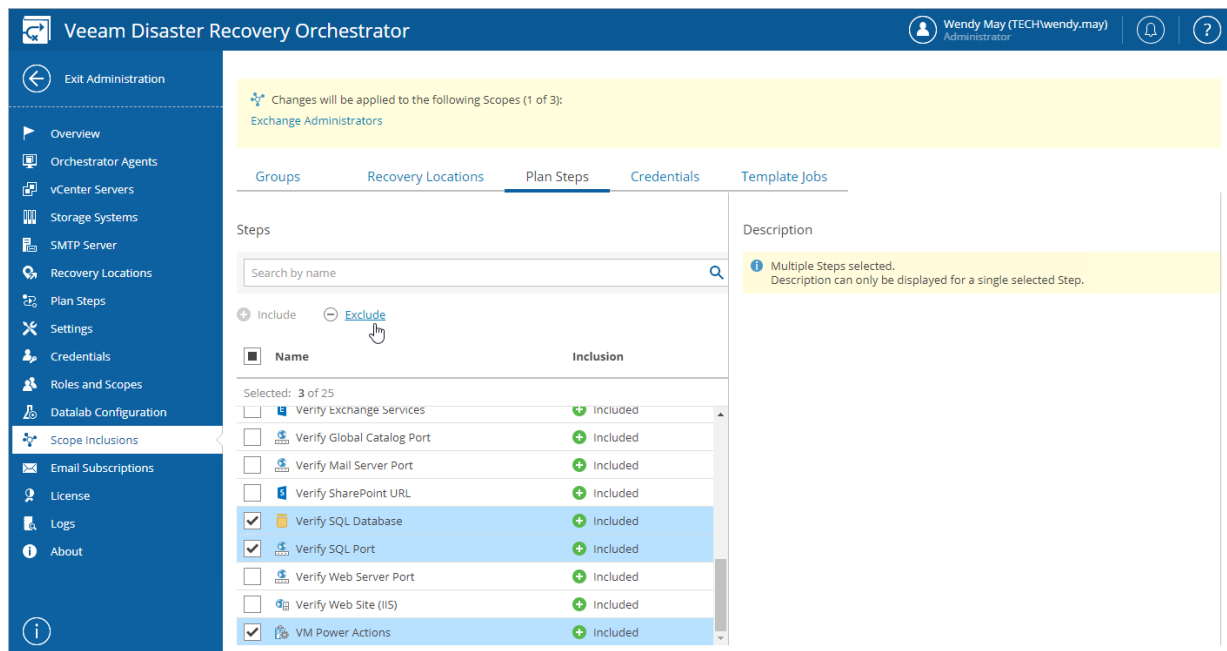
Unless a step is *INCLUDED* into the list of inventory items for a scope, it will not be available for use in the scope. By default, all existing steps are included in the inventory list for all scopes.

To modify the list of plan steps available for a scope:

1. Switch to the **Administration** page.
2. Navigate to **Scope Inclusions > Plan Steps**.
3. Select the scope:
 - a. Click the **Scopes** link.
 - b. In the **Change Scope** window, select a check box next to the required scope, and click **Apply**.
4. Select check boxes next to the necessary steps, and click **Include** or **Exclude**.

TIP

You can simultaneously edit the list of inventory items available for multiple scopes. To do that, select check boxes next to the required scopes in the **Change Scope** window. After you click **Include** or **Exclude**, the changes will be applied to all the selected scopes at the same time.



After you make a plan step *INCLUDED* for a scope, Plan Authors will be able to use this step when building orchestration plans for the scope. For more information on creating and editing orchestration plans, see [Working with Orchestration Plans](#).

Configuring Default Parameter Settings

To modify default parameter settings for a plan step:

1. Switch to the **Administration** page.
2. Navigate to **Plan Steps**.
3. In the **Steps** column, select the step and click **Edit**.
4. Complete the **Edit Default Step Parameters** wizard:
 - a. At the **Step Parameters** step:
 - i. In the **Step Parameters** column, select the required parameter.
 - ii. In the **Parameter Details** column, set the desired parameter values.

Edit Default Step Parameters

Step Parameters

Affected Plans

Summary

Specify default values for the step parameters

Step Parameters

Common Parameters

- Execute Location
- Windows Credentials
- Exchange Server
- Email Address
- Exchange Credentials

Parameter Details

During Failback and Undo: Skip

During Lab Tests: Execute

Critical Step: Yes

Timeout: 300

Retries: 10

Description:

This Step verifies the availability of the Microsoft Exchange mailbox by accessing the mailbox under an account with the provided credentials. The script requires Exchange Web Services (EWS) API to be installed where it runs.

Script Requirements:

- PowerShell 3.0 or later
- Windows 2008 R2 and later
- .NET 4.0 or later
- Exchange Server 2013 and later
- Exchange Web Services (EWS) API 2.1 or later

Next Finish Cancel

- b. At the **Affected Plans** step, review the list of plans whose steps will be updated to meet the parameter changes, and click **Next**.

Edit Default Step Parameters

Step Parameters

Affected Plans

Summary

The following plans use this step and will be affected by the parameter changes

i

Orchestrator will automatically update the default parameter values for steps in these plans.

Plan	Scope
Test Replica Plan	Admin Scope

Back

Next

Finish

Cancel

c. At the **Summary** step, review the configured settings and click **Finish**.

The screenshot shows a dialog box titled "Edit Default Step Parameters" with a close button (X) in the top right corner. On the left is a vertical sidebar with three tabs: "Step Parameters", "Affected Plans", and "Summary". The "Summary" tab is selected and highlighted in blue. The main area of the dialog is titled "See below for a summary for the Step". Below this title is a "Copy to clipboard" button with a document icon. Underneath is a section titled "Step Info" which contains the following details:

- Name:** Verify Exchange Mailbox
- Description:** This Step verifies the availability of the Microsoft Exchange mailbox by accessing the mailbox under an account with the provided credentials. The script requires Exchange Web Services (EWS) API to be installed where it runs.
- Script Requirements:**
 - PowerShell 3.0 or later
 - Windows 2008 R2 and later
 - .NET 4.0 or later
 - Exchange Server 2013 and later
 - Exchange Web Services (EWS) API 2.1 or later

At the bottom right of the dialog are four buttons: "Back", "Next", "Finish" (highlighted in blue), and "Cancel".

NOTE

The parameter settings will be changed only for plans that are NOT in the *IN USE* mode. For the list of modes that an orchestration plan can acquire, see [Running and Scheduling Replica Plans](#), [Running and Scheduling Restore Plans](#), [Running and Scheduling Storage Plans](#) and [Running and Scheduling Cloud Plans](#).

Managing Credentials

Orchestrator Administrators can choose which credentials will be visible to Plan Authors and available for use in orchestration plans. These credentials can be used in plans, for example, to run verification scripts inside the guest OS, or in other checks.

Orchestrator automatically collects all credentials from the connected Veeam Backup & Replication server and displays them in the Orchestrator UI. The Orchestrator UI allows you to [edit the existing credentials](#), and [add any domain and non-domain accounts](#).

NOTE

Orchestrator collects only [standard accounts](#) from connected Veeam Backup & Replication servers — it does not collect [Linux accounts](#) and [Linux private keys](#).

Allowing Access to Credentials

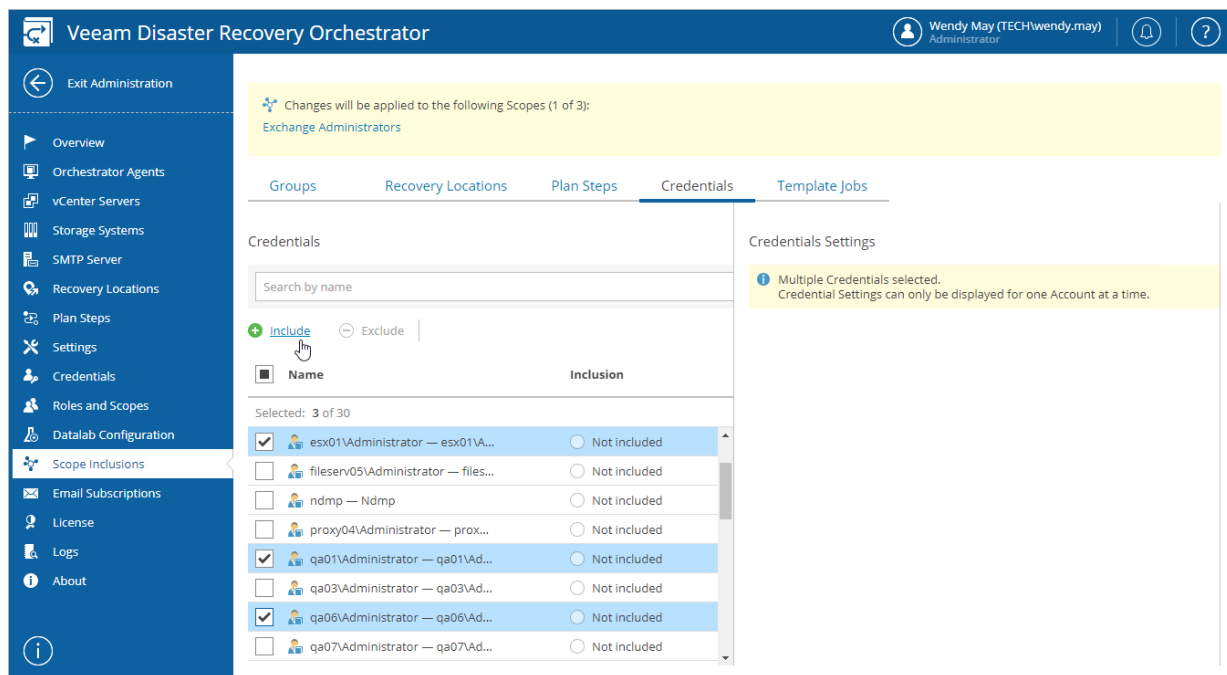
Unless a credential is *INCLUDED* into the list of inventory items for a scope, it will not be available for use in the scope. By default, all credentials are excluded from newly created scopes; only the *Admin Scope* has all credentials included.

To modify the list of credentials available for a scope:

1. Switch to the **Administration** page.
2. Navigate to **Scope Inclusions > Credentials**.
3. Select the scope:
 - a. Click the **Scopes** link.
 - b. In the **Change Scope** window, select a check box next to the required scope, and click **Apply**.
4. Select check boxes next to the necessary accounts, and click **Include** or **Exclude**.

TIP

You can simultaneously edit the list of inventory items available for multiple scopes. To do that, select check boxes next to the required scopes in the **Change Scope** window. After you click **Include** or **Exclude**, the changes will be applied to all the selected scopes at the same time.



After you make a credential *INCLUDED* for a scope, Plan Authors will be able to use this credential when configuring the **Windows Credentials** and **SQL Credentials** parameters for plan steps for the scope. For more information on creating and editing orchestration plans, see [Working with Orchestration Plans](#).

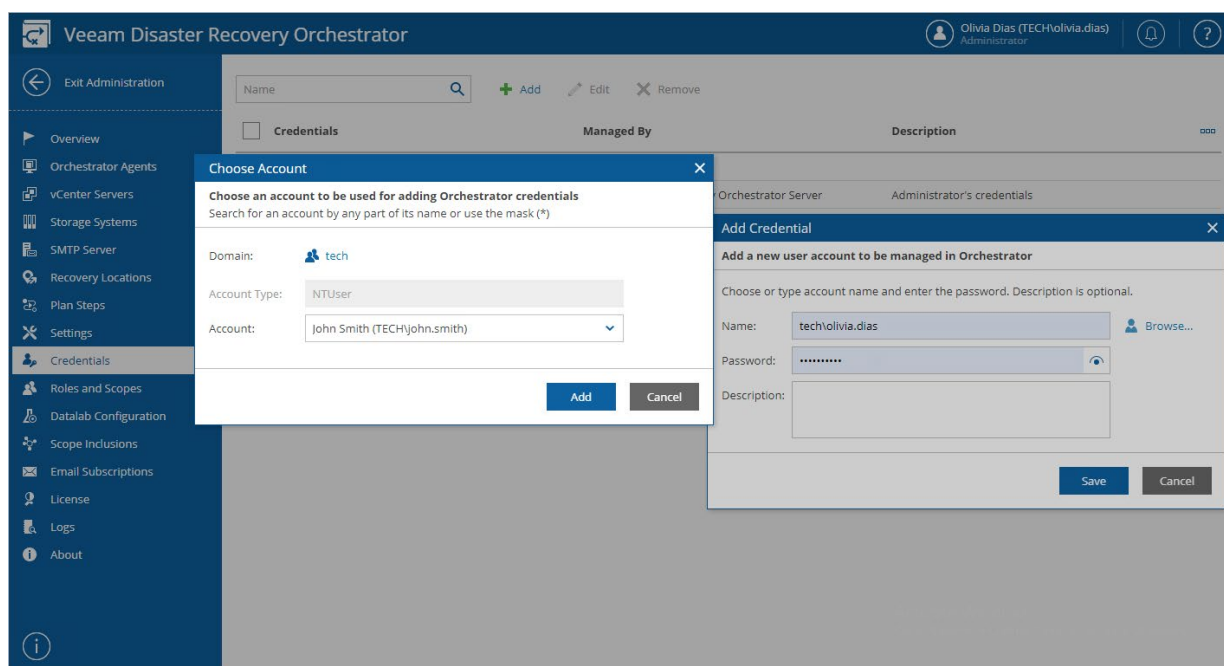
Adding Credentials

If you want to manually add credentials under which orchestration plan steps will be launched:

1. Switch to the **Administration** page.
2. Navigate to **Credentials**.
3. Click **Add**.
4. In the **Add Credential** window, click **Browse**.
5. In the **Choose Account** window:
 - a. In the **Domain** field, select a domain to which the account that you want to add belongs.
 - b. In the **Account** field, enter the account name.
 - c. Select the account and click **Add**.
6. In the **Add Credential** window, enter a password for the account that you want to add, provide a description for future reference, and click **Save**.

TIP

You can also add any credentials of your choice, even those that do not exist yet. To do that, in the **Add Credential** window, use the **Account** and **Password** fields to enter an account name and a password for the account, and click **Save**.



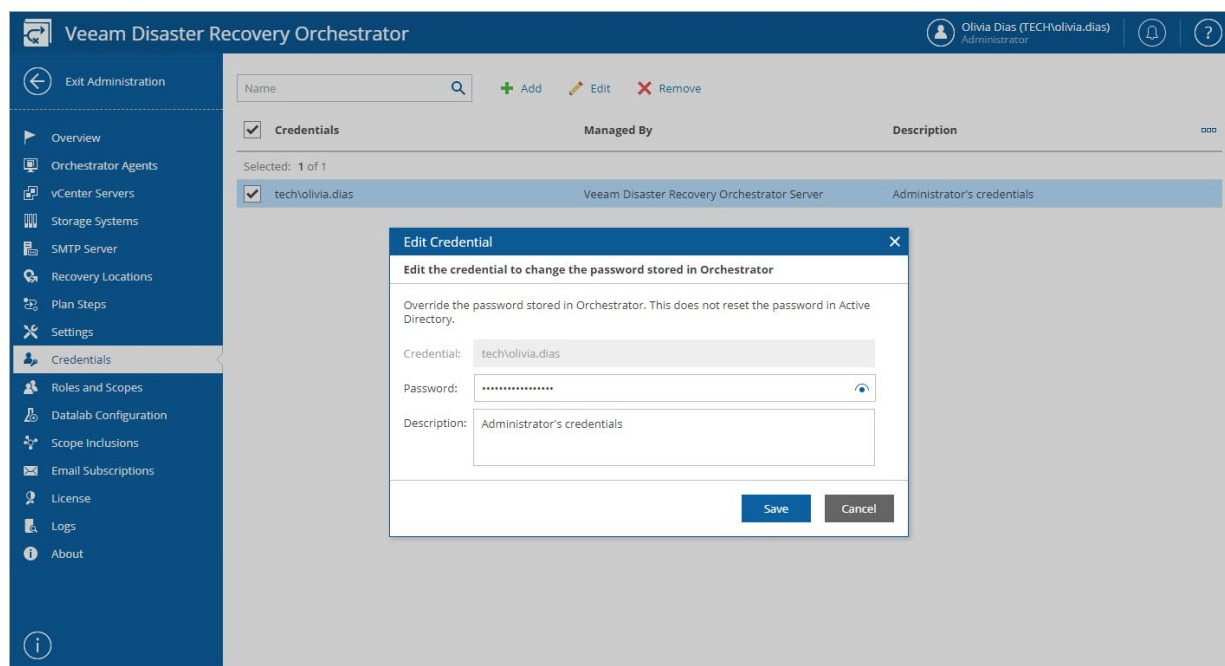
By default, all credentials are excluded from the newly created scopes; only the *Admin Scope* has all credentials included. To edit the list of credentials available for a scope and to include the new credentials, follow the instructions provided in section [Allowing Access to Credentials](#).

Changing Passwords

If you want to set a new password for an account, the default and preferred method is to change it in the Veeam Backup & Replication console. The new password will be synchronized automatically into Orchestrator.

You can also change a password for an account in the Orchestrator UI. However, keep in mind that if you change a password in the Orchestrator UI, the new password will not be synchronized into the Veeam Backup & Replication console.

1. Switch to the **Administration** page.
2. Navigate to **Credentials**.
3. Select a credential that you want to modify and click **Edit**.
4. In the **Edit Credential** window:
 - a. In the **Password** field, enter a new password.
 - b. Click **Save**.



Editing Template Jobs

When you create a [replica](#) or [restore](#) plan, you have an option to reprotect machines included in the plan as soon as the recovery process completes. Orchestrator will automatically create a new replication or backup job to reprotect the recovered VMs as part of the plan execution process.

To accomplish this, configure a template job on the Veeam Backup & Replication server that protects the required machines and is connected to your Orchestrator server. For Orchestrator to discover the job as a template, you must create a standard Veeam job and include the text *[VDRO Template]* in the job description.

NOTE

When creating a new replication or backup job, Orchestrator will copy all settings configured for the template job – except for **the guest processing settings**. If you want to enable application-aware processing for machines included in the plan, edit settings of the newly created job as described in the Veeam Backup & Replication User Guide, sections [Creating Backup Jobs](#) and [Creating Replication Jobs](#).

The screenshot shows the 'New Backup Job' window. On the left, a sidebar has a 'Name' section selected, with sub-items: Virtual Machines, Storage, Guest Processing, Schedule, and Summary. The main pane shows the 'Name' field containing 'Template Backup Job for Orchestrator' and the 'Description' field containing 'This job is a [VDRO Template] to reprotect failed-over VMs.'. Below these fields is an unchecked checkbox for 'High priority' with a note: 'Backup infrastructure resources are offered to high priority jobs first. Use this option for jobs sensitive to the start time, or jobs with strict RPO requirements.'. At the bottom right are four buttons: '< Previous' (disabled), 'Next >' (active), 'Finish' (disabled), and 'Cancel' (disabled).

After you create a template job on the Veeam Backup & Replication server, Orchestrator will collect this data and display it in the Orchestrator UI. Note that the data synchronization process between Orchestrator and the Veeam Backup & Replication server may take several minutes to complete.

NOTE

The Orchestrator template job can be configured per-inventory group in a plan. To do that, select the **Protect VM Groups** option when creating or editing the plan. With this option selected, a new job will be created for the inventory group. For more information, see [Overriding VM Recovery and Protection Settings](#).

Allowing Access to Template Jobs

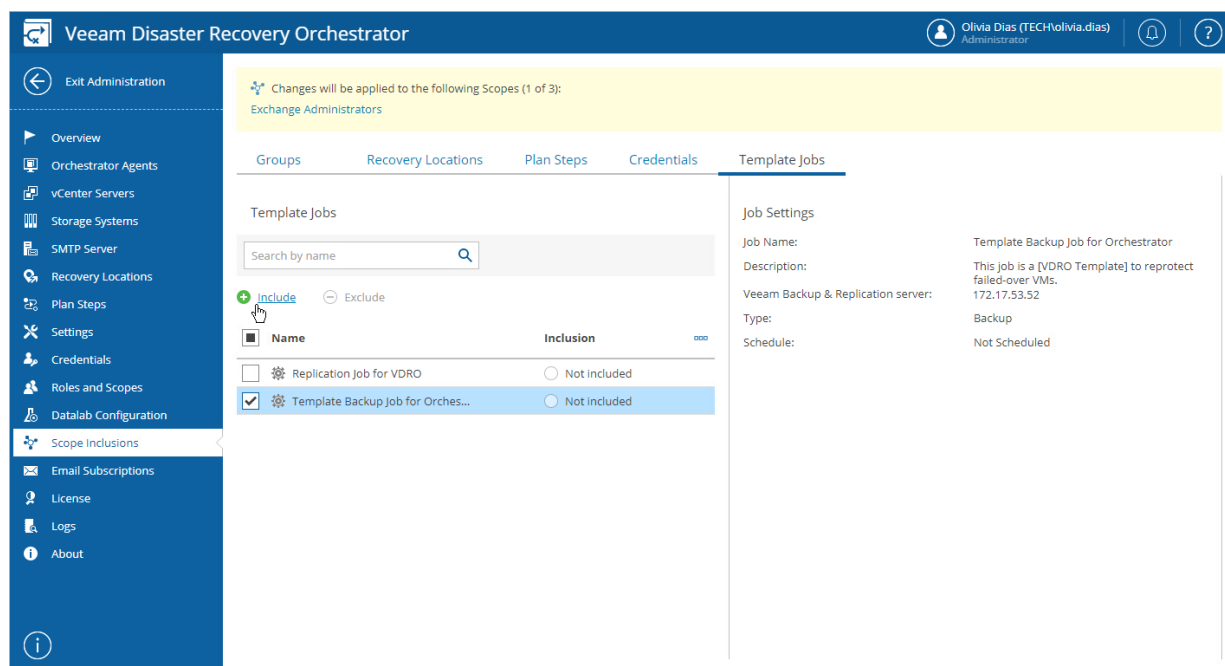
Unless a template job is *INCLUDED* into the list of inventory items for a scope, it will not be available for use in the scope. By default, all configured template jobs are excluded from newly created scopes; only the *Admin Scope* has all the jobs included.

To modify the list of template jobs available for a scope:

1. Switch to the **Administration** page.
2. Navigate to **Scope Inclusions > Template Jobs**.
3. Select the scope:
 - a. Click the **Scopes** link.
 - b. In the **Change Scope** window, select a check box next to the required scope, and click **Apply**.
4. Select check boxes next to the necessary jobs, and click **Include** or **Exclude**.

TIP

You can simultaneously edit the list of inventory items available for multiple scopes. To do that, select check boxes next to the required scopes in the **Change Scope** window. After you click **Include** or **Exclude**, the changes will be applied to all the selected scopes at the same time.



After you make a template job *INCLUDED* for a scope, Plan Authors will be able to use this job to protect machines included in replica and restore plans for the scope. For more information on creating and editing replica and restore plans, see [Working with Replica Plans](#) and [Working with Restore Plans](#).

Connecting DataLabs

To validate your disaster recovery plans without impacting the production infrastructure, you can configure automatic scheduled testing for the verification of vSphere and agent backups, VM replicas, applications and storage snapshots. For this purpose, Orchestrator uses DataLabs created in the Veeam Backup & Replication console. These DataLabs provide an isolated environment in which Orchestrator performs verification tests.

After you create a DataLab on a Veeam Backup & Replication server connected to your Orchestrator server, you must configure a connection to the VMware Server used to manage the lab, as described in section [Connecting VMware vSphere Servers](#). Otherwise, Orchestrator will not be able to discover the DataLab and make it available in the Orchestrator UI. Note that the data synchronization process between Orchestrator and the Veeam Backup & Replication server may take several minutes to complete.

Assigning and Configuring DataLabs

Unless a DataLab is *ASSIGNED* to a scope, it will not be visible for use in orchestration plans for the scope. By default, none of discovered DataLabs is assigned to any scope.

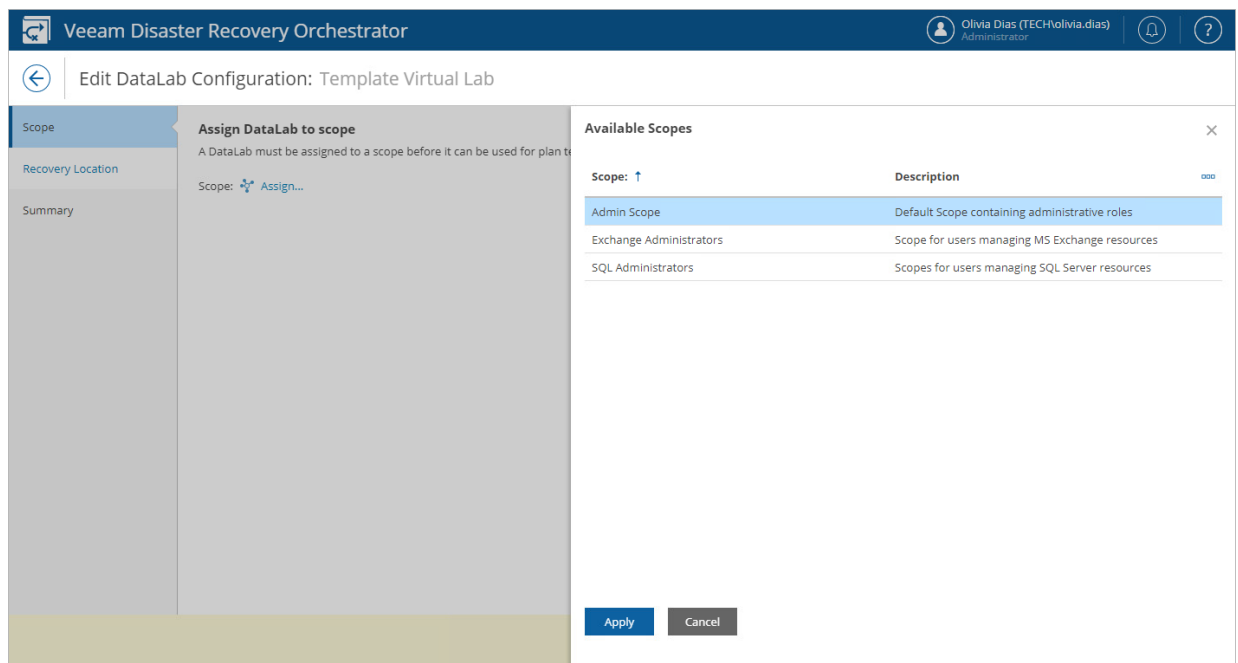
To modify the list of DataLabs available for a scope and to configure DataLab settings:

1. Switch to the **Administration** page.
2. Navigate to **DataLab Configuration**.
3. Select a DataLab and click **Edit**.
4. Complete the **Edit DataLab Configuration** wizard:
 - a. At the **Scope** step, click **Assign**. Select the required scope in the **Available Scopes** window and click **Apply**.

For a scope to be displayed in the **Available Scopes** list, it must be created and customized as described in section [Managing Permissions](#).

NOTE

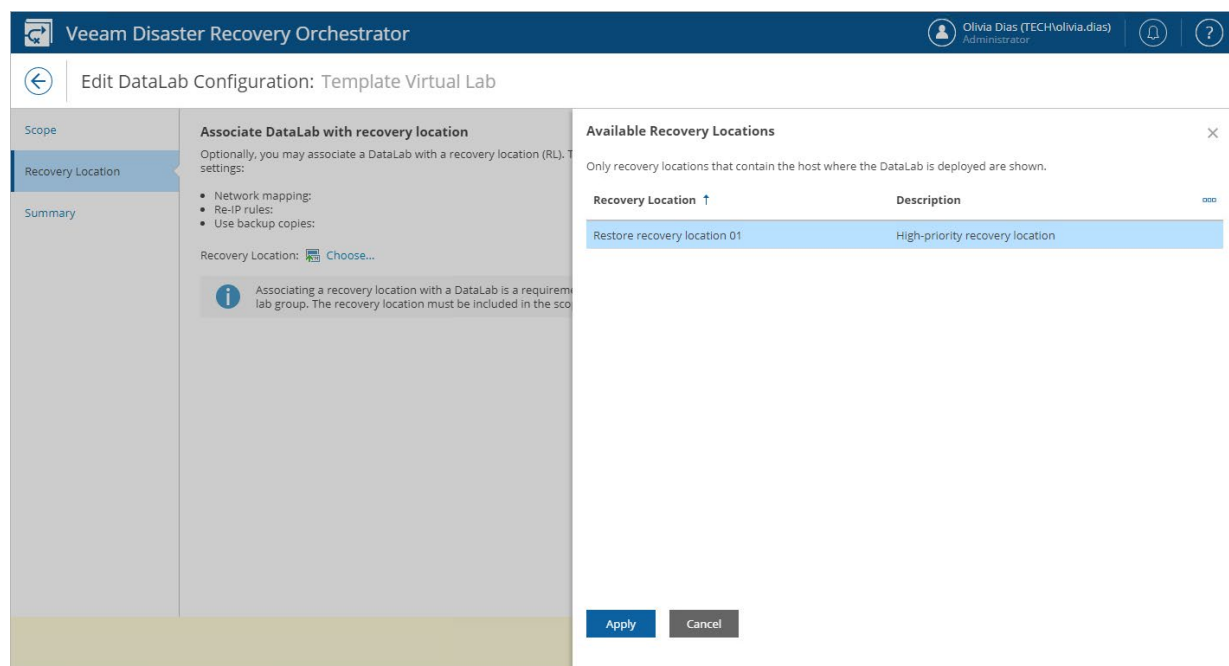
When you unassign a DataLab from a scope, all **lab groups** added to the DataLab are automatically deleted from the DataLab.



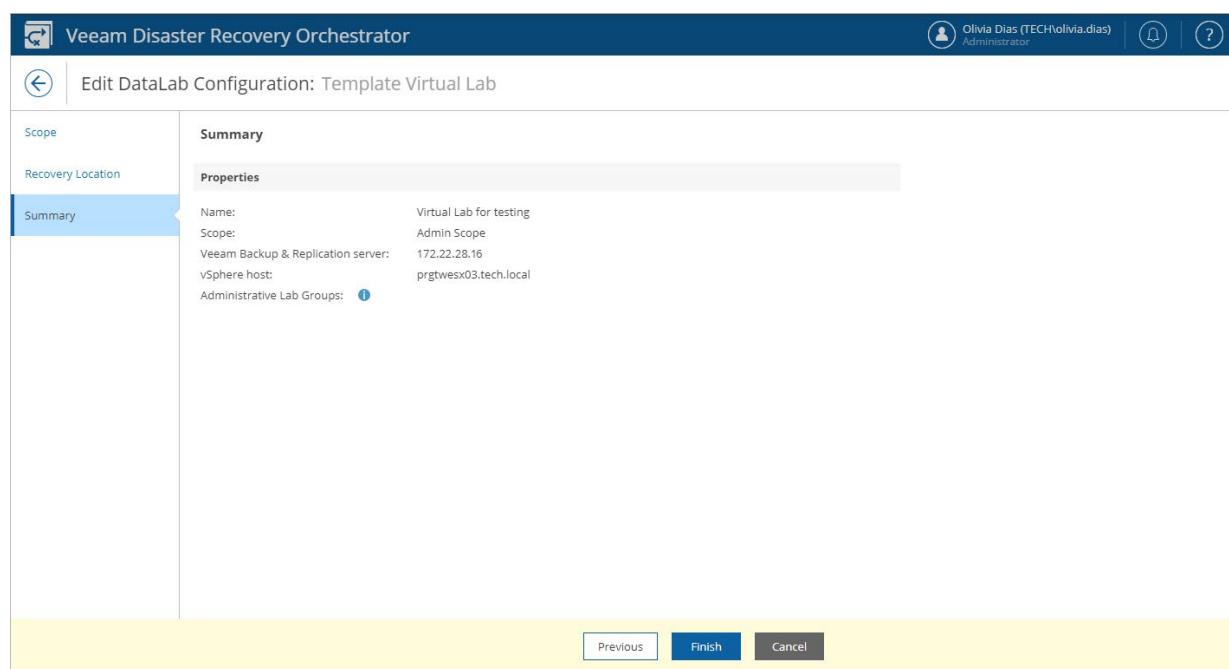
- b. [This step applies only if you want to verify machines in a DataLab that contains a lab group]

At the **Recovery Location** step, select a recovery location whose settings will be applied to the machines being verified to connect them to the correct network, to reconfigure machine IP addresses and to set the backup copy preference. For more information on these settings, see [Adding Restore Recovery Locations](#).

For a recovery location to be displayed in the list of available recovery locations, its [compute resources](#) must contain the host where the DataLab is deployed, and the location must be included into the selected scope as described in section [Allowing Access to Recovery Locations](#).



c. At the **Summary** step, review configuration information and click **Finish**.



After you make a DataLab *ASSIGNED* to a scope, Plan Authors will be able to use this lab for on-demand or scheduled testing of orchestration plans for the scope. For more information, see [Testing Replica Plans](#), [Testing Restore Plans](#) and [Testing Storage Plans](#).

Working with Orchestration Plans

Orchestrator uses the failover and data recovery functionality provided by Veeam Backup & Replication to automate recovery actions. In addition, Orchestrator provides vSphere VM recovery orchestration based on replicated storage snapshots created on NetApp and HPE storage systems. For these purposes, Orchestrator offers 5 types of orchestration plans:

- [Replica plans](#) – consist of vSphere VMs that should be failed over to replicas.
- [CDP replica plans](#) – consist of vSphere VMs that should be failed over to continuous data protection (CDP) replicas.
- [Restore plans](#) – consist of vSphere VM and Veeam agent backups that should be recovered to a VMware vSphere environment.
- [Storage plans](#) – consist of VMs that store their files on vSphere datastores backed by replicating NetApp and HPE storage systems.
- [Cloud plans](#) – consists of vSphere VM and Veeam agent backups that should be recovered to a Microsoft Azure cloud environment.

Orchestration plans are based on inventory groups. For more information on inventory groups, see [Managing Inventory Groups](#).

TIP

To see the full list of discovered inventory groups, navigate to **Inventory**. You can select any inventory group and click **Create Plan** to create an orchestration plan that will have the selected group preselected in the list of groups to recover.

Orchestration plans can be scheduled and chained to execute in sequence, and Orchestrator will automatically [produce and update detailed documentation](#). Execution of orchestration plans is simplified to allow simultaneous management of multiple plans that contain hundreds of machines.

Working with Replica Plans

The type of an orchestration plan you create depends on whether you intend to use Orchestrator to switch to VM replicas, to restore machines from backups or backup copies, or to serve data from a destination (NetApp) or secondary (HPE) volume in case a disaster strikes.

If you want to recover vSphere VMs protected by Veeam replication jobs, create a replica plan.

Creating Replica Plans

To create a replica plan:

1. Navigate to **Orchestration Plans**.
2. Click **Manage > New**.
3. Complete the **New Orchestration Plan** wizard:
 - a. [Specify a plan name and description](#).
 - b. [Choose a scope for the plan](#).
 - c. [Choose a type of the plan](#).
 - d. [Include inventory groups in the plan](#).
 - e. [Specify VM recovery options](#).
 - f. [Add steps to the plan](#).
 - g. [Specify credentials for the plan steps](#).
 - h. [Specify VM protection options](#).
 - i. [Specify the target RTO and RPO](#).
 - j. [Select a template for plan reports](#).
 - k. [Specify scheduling options for plan reports](#).
 - l. [Finish working with the wizard](#).

Step 1. Specify Plan Name and Description

At the **Plan Info** step of the wizard, use the **Plan Name** and **Description** fields to enter a name for the new plan and to provide a description for future reference. The maximum length of the plan name is 64 characters; the following characters are not supported: * : / \ ? " < > | .

You can also provide a contact name, email and telephone number of a person responsible for the plan.

New Orchestration Plan

Plan Info

Scope

Plan Type

Recovery Location

VM Groups

VM Recovery Options

VM Steps

RTO & RPO

Report Template

Report Scheduling

Summary

Provide details for the new Orchestration Plan

Plan Name:

Test Replica Plan

Description:

Evaluating failover

Contact Name:

John Smith

Contact Email:

john.smith@veeam.com

Contact Tel:

18002223344

Next

Cancel

Step 2. Choose Plan Scope

At the **Scope** step of the wizard, select a scope for which you want to create the plan.

For a scope to be displayed in the **Available Scopes** list, it must be created and customized as described in section [Managing Permissions](#).

New Orchestration Plan

Plan Info

Scope

Plan Type

Recovery Location

VM Groups

VM Recovery Options

VM Steps

RTO & RPO

Report Template

Report Scheduling

Summary

Choose a Scope

Type any part of Scope name to filter

Available Scopes

Admin Scope

Exchange Administrators

SQL Administrators

Back

Next

Cancel

Step 3. Choose Plan Type

At the **Plan Type** step of the wizard, select the **Replica** option.

New Replica Plan

Plan Info

Scope

Plan Type

VM Groups

VM Recovery Options

VM Steps

Protect VM Groups

RTO & RPO

Report Template

Report Scheduling

Summary

Choose the type of Plan

☐ Cloud

VMs will be recovered from VMs will be recovered from Veeam agent or vSphere backups into a cloud environment

☐ CDP Replica

VMs will be recovered from Veeam CDP (continuous data protection) replicas

☒ Replica

VMs will be recovered from Veeam replicas

☐ Storage

VMs will be recovered from replicated storage volumes

☐ Restore

VMs will be recovered from Veeam backups

Back

Next

Cancel

Step 4. Add Inventory Groups

At the **VM Groups** step of the wizard, select inventory groups that you want to recover, and click **Add** to include them in the plan.

For an inventory group to be displayed in the **Available Groups** list, it must be included into the list of inventory items available for the scope, as described in section [Allowing Access to Inventory Groups](#).

IMPORTANT

For Orchestrator to be able to recover a VM correctly, the VM must have VMware Tools installed. The presence of VMware Tools is checked automatically on the vCenter Server side – for both Windows-based and Linux-based VMs. To know how to install and upgrade VMware Tools in vSphere, see [this VMware KB article](#).

New Replica Plan

Plan Info

Scope

Plan Type

VM Groups

VM Recovery Options

VM Steps

Protect VM Groups

RTO & RPO

Report Template

Report Scheduling

Summary

Add VM Groups

Use View VMs control to check Group members, and Up/Down controls to change the recovery sequence.

Search

Available Groups

datastore - datastore1

datastore - enriqueDS

datastore - esx03-virt-ds1

datastore - KK-dat32

datastore - KK-vol01

datastore - kuvi-enr2

owner - joelle.van.dyne

Add

Remove

owner - john.smith

datastore - esx01-das3

Up

Down

View VMs

These options can be customized later on the Edit Plan page.

Back

Next

Cancel

Step 5. Specify VM Recovery Options

At the **VM Recovery Options** step of the wizard, use the **If the VM recovery encounters an error then** options to choose whether you want to halt plan execution if VM recovery fails. This option can also be customized later per-group [when editing the plan](#).

Use the **Recover the VMs in each group** options to choose whether you want to recover VMs in sequence or in parallel. If you select to process VMs simultaneously, use the **Recover simultaneously max of VMs** field to specify the maximum number of VMs processed at the same time.

The screenshot shows the 'New Replica Plan' wizard with the 'VM Recovery Options' step selected in the left sidebar. The main content area is titled 'Customize the default recovery options for all VMs in the Plan'. It contains three sections: 'If the VM recovery encounters an error then' with radio buttons for 'Halt the plan' (selected) and 'Proceed with the plan'; 'Recover the VMs in each group' with radio buttons for 'In parallel' (selected) and 'In sequence'; and 'Recover simultaneously max of:' with a spinner box set to '10' and the unit 'VMs'. An information banner at the bottom states: 'These options can be customized later on the Edit Plan page.' At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

New Replica Plan	
Plan Info	Customize the default recovery options for all VMs in the Plan
Scope	
Plan Type	
VM Groups	
VM Recovery Options	
VM Steps	
Protect VM Groups	
RTO & RPO	
Report Template	
Report Scheduling	
Summary	

If the VM recovery encounters an error then

☒ Halt the plan

☐ Proceed with the plan

Recover the VMs in each group

☒ In parallel

☐ In sequence

Recover simultaneously max of: 10 VMs

i These options can be customized later on the Edit Plan page.

Back Next Cancel

Step 6. Add Plan Steps

At the **VM Steps** step of the wizard, use the list of plan steps to select steps to be performed for each VM during failover.

For a step to be displayed in the **Available Steps** list, it must be included into the list of inventory items available for the scope, as described in section [Allowing Access to Plan Steps](#).

IMPORTANT

To allow the failover process to perform successfully, the **Process Replica VM** step must execute first.

By default, Orchestrator will perform the same selected steps in the same order for all new VMs that will later appear in the inventory groups included in the plan. However, you can change the step execution order and modify the list of steps individually for each VM, as described in section [Configuring Steps](#).

NOTE

If a VM is included in multiple inventory groups in the same plan, Orchestrator will only run the **Process Replica VM** step once. However, other steps for this VM will execute when processing it in each group.

The screenshot shows the 'New Replica Plan' wizard in the 'VM Steps' step. On the left is a navigation pane with options: Plan Info, Scope, Plan Type, VM Groups, VM Recovery Options, VM Steps (selected), VM Credentials, Protect VM Groups, RTO & RPO, Report Template, Report Scheduling, and Summary. The main area is titled 'Choose VM Steps' and contains a search bar, 'Up' and 'Down' arrows, and two lists: 'Available Steps' and 'Selected Steps'. The 'Available Steps' list includes: Process Replica VM, Check VM Heartbeat, Generate Event, Ping VM Network, Send Email, Shutdown Source VM, Start Service, Verify DNS Port, Verify Domain Controller Port, Verify Exchange Mailbox, Verify Exchange MAPI Connectivity, Verify Exchange Services, and Verify Global Catalog Port. The 'Selected Steps' list includes: Process Replica VM, Check VM Heartbeat, Verify Exchange Mailbox, Verify Exchange MAPI Connectivity, Verify Exchange Services, and Send Email (which is highlighted). Below the lists is an information icon and the text: 'These options can be customized later on the Edit Plan page.' At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

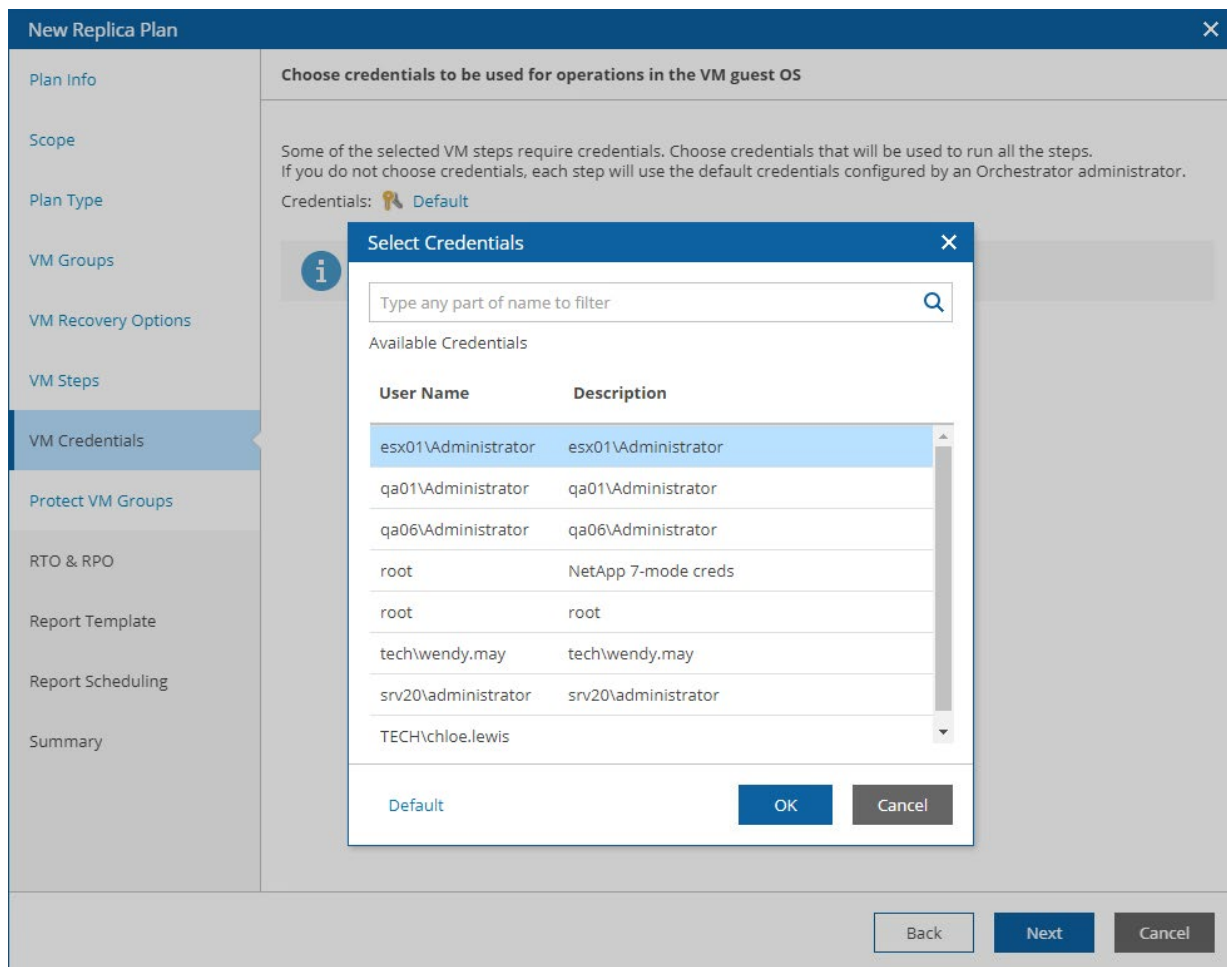
Available Steps	Selected Steps
Process Replica VM	Process Replica VM
Check VM Heartbeat	Check VM Heartbeat
Generate Event	Verify Exchange Mailbox
Ping VM Network	Verify Exchange MAPI Connectivity
Send Email	Verify Exchange Services
Shutdown Source VM	Send Email
Start Service	
Verify DNS Port	
Verify Domain Controller Port	
Verify Exchange Mailbox	
Verify Exchange MAPI Connectivity	
Verify Exchange Services	
Verify Global Catalog Port	

Step 7. Specify Credentials

[This step applies only if you have added one or more plan steps that require Windows credentials to run in-guest OS scripts inside VMs being processed. For the full list of steps that require authentication, see [Appendix. Orchestration Plan Steps](#)]

At the **VM Credentials** step of the wizard, specify credentials that will be used to access guest OSes of VMs. To do that, click the link in the **Credentials** section, and select the necessary credentials in the **Select Credentials** window. For a credential record to be displayed in the **Available Credentials** list, it must be included into the list of inventory items for the scope, as described in section [Allowing Access to Credentials](#).

If you do not specify any credentials, Orchestrator will use the default credentials defined when configuring plan steps on the **Administration** page of the Orchestrator UI, or you may specify the required credentials individually for each VM [when editing the plan](#).



Step 8. Specify VM Protection Options

At the **Protect VM Groups** step of the wizard, use the **Protect VM Groups after recovery** check box to choose whether you want to protect VMs in the plan post-recovery with a backup or replication job.

If you select the **Protect VM Groups after recovery** check box, you must specify a backup or replication job to be used as a template for a new job that will reprotect recovered VMs. To do that, from the **Template Job** list, select the required job.

For a template backup or replication job to be displayed in the **Template Job** list, it must be created and included into the list of inventory items for the scope, as described in section [Editing Template Jobs](#).

IMPORTANT

The new job will consume Veeam Backup & Replication licenses to protect the VM replicas. That is why you must take into account the number of licenses installed on the Veeam Backup & Replication server, so that the number of actually managed objects does not exceed the license limit.

The screenshot shows the 'New Replica Plan' wizard with the 'Protect VM Groups' step selected in the left-hand navigation pane. The main content area is titled 'Choose a reprotect option' and includes the instruction: 'Orchestrator can automatically create a new backup or replication job to reprotect the recovered VMs.' Below this, the 'Protect VM Groups after recovery' checkbox is checked. A 'Template Job' dropdown menu is set to 'Template Backup Job for Orchestrator [DR]'. An information icon (i) is present next to a note: 'This Step requires that the Veeam Backup & Replication server has enough licenses to run the new job. See the [Orchestrator documentation](#) for details.' At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

Step 9. Specify Target RTO and RPO

At the **RTO & RPO** step of the wizard, define your Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for the plan:

- The **Target RPO** defines the maximum acceptable period of data loss.
- The **Target RTO** represents the amount of time it should take to recover from an incident.

RTO and RPO performance will be recorded in the [Plan Readiness Check](#), [Plan Execution](#) and [DataLab Test](#) reports, and you will be able to track the achieved RTO and RPO objectives for each plan on the [Home Page Dashboard](#).

The screenshot shows the 'New Replica Plan' wizard with the 'RTO & RPO' step selected in the left sidebar. The main area is titled 'Define your Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for this plan'. It contains two sets of spinners for 'Target RTO' and 'Target RPO'. The 'Target RTO' is set to 1 hour, 0 minutes, and 0 seconds, with a description 'Maximum allowed time before the service is restored after a failure.' The 'Target RPO' is set to 24 hours, 0 minutes, and 0 seconds, with a description 'Maximum allowed loss of historical data after a failure.' At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons.

Field	Hours	Minutes	Seconds	Description
Target RTO	1	0	0	Maximum allowed time before the service is restored after a failure.
Target RPO	24	0	0	Maximum allowed loss of historical data after a failure.

Step 10. Select Report Template

At the **Report Template** step of the wizard, select a document template that will be used as the cover page for all Orchestrator reports. Use options in the **Document format** list to choose whether you want to generate documents in the DOCX or PDF format.

For a custom document template to be displayed in the **Available Templates** list, it must be created and customized as described in section [Managing Templates](#).

New Replica Plan

Plan Info

Scope

Plan Type

VM Groups

VM Recovery Options

VM Steps

VM Credentials

Protect VM Groups

RTO & RPO

Report Template

Report Scheduling

Summary

Choose the report template to be used for Plan reports and documentation

Type any part of name to filter

Available Templates

Veeam Default Template (DE)
Dieses Template ist ein Beispiel und sollte auf Ihre Bedürfnisse angepasst werden

Veeam Default Template
This is an example template, and should be cloned and customized to your requirements

Veeam Default Template (ES)
Esta es una plantilla de ejemplo, y debe ser clonada y personalizada de acuerdo con sus requisitos

Veeam Default Template (FR)
Ceci est un modèle qui doit être cloné et personnalisé selon vos besoins

Veeam Default Template (PT)
Este é um template de exemplo, e deve ser clonado e customizado de acordo com seus requerimentos

Veeam Default Template (CH)
这是一个示例模板，应进行复制并根据您的要求定制

Veeam Default Template (JP)
こちらはサンプル・テンプレートです。コピーして、要件に応じてカスタマイズしてください

Document format:

☒ PDF file

☐ Word document (.DOCX)

Back

Next

Cancel

Step 11. Specify Report Scheduling Options

At the **Report Scheduling** step of the wizard, choose whether you want to automatically generate the [Plan Definition](#) and [Plan Readiness Check](#) reports for the plan on a daily schedule. You can also choose whether you want to generate both reports immediately after you create the plan.

To specify the exact time at which the report will be generated, click the **Schedule** icon next to the **Update Plan Definition report daily at** or **Perform Plan Readiness Check daily at** check box, set the desired time, and click **Apply**.

New Replica Plan

Plan Info

Scope

Plan Type

VM Groups

VM Recovery Options

VM Steps

VM Credentials

Protect VM Groups

RTO & RPO

Report Template

Report Scheduling

Summary

Choose scheduling options for automatic Plan reporting

☒ Update Plan Definition report daily at: 1:13 PM

☒ Perform Plan Readiness Check daily at: 8:00 AM

i Reports will not be generated for plan

☒ Create Plan Definition when I click Finish

☒ Perform Readiness Check when I click Finish

Hours: 8 Minutes: 0

☒ AM ☐ PM

Apply **Cancel**

Back **Next** **Cancel**

Step 12. Finish Working with Wizard

At the **Summary** step of the wizard, review configuration information and click **Finish**.

New Replica Plan

Plan Info

Scope

Plan Type

VM Groups

VM Recovery Options

VM Steps

VM Credentials

Protect VM Groups

RTO & RPO

Report Template

Report Scheduling

Summary

See below for a summary for the new Plan

Copy to clipboard

Plan Name:Test Replica Plan

Description:Orchestrating failover

Contact Name:John Smith

Contact Email:john.smith@veeam.com

Contact Tel:18002223344

Scope:Exchange Administrators

Plan Type:Replica

VM Group(s):Datastore - esx01-das3

Recover VMs:Simultaneously (max 10)

If any VM fails:Halt the plan

Steps for New VM Template:Process Replica VM
Check VM Heartbeat
Verify Exchange Mailbox
Verify Exchange MAPI Connectivity
Verify Exchange Services
Send Email

Override Credentials:No

Credentials:Use Default

Protect VM Group, Job:No, N/A

Target RTO:1 Hour

Target RPO:24 Hours

Report Template, format:Veeam Default Template, PDF

Update Plan Definition report:Daily 1:13 PM

Perform Readiness Check:Daily 6:15 AM

Create Plan Definition report now:Yes

Run Readiness Check now:Yes

Back

Finish

Cancel

Editing Replica Plans

If you want to specify granular settings not provided in the [New Orchestration Plan wizard](#), the Orchestrator UI allows you to customize replica plans and configure the settings for groups, recovered VMs, plan steps and step parameters.

The procedures to edit replica, CDP replica, restore, storage and cloud plans are almost identical. For more information, see [Editing Orchestration Plans](#).

Testing Replica Plans

You can start on-demand plan testing and configure test scheduling for any replica plan. There is almost no difference between the procedures performed for replica, restore and storage plans. For more information, see [Testing Orchestration Plans](#).




Running and Scheduling Replica Plans

After you create and configure a replica plan, run a successful [readiness check](#) and a [DataLab test](#), the plan can be considered ready for failover. You can invoke various actions for the plan, depending on the current plan state.





Point in Time	Actions
New plan created	After plan creation, you can: <ul style="list-style-type: none">• Schedule a time for the plan to execute failover.• Run the plan to execute failover immediately.
Failover	After failover, you can: <ul style="list-style-type: none">• Perform permanent failover.• Fail back to the original or to a new location.
Failback	After failback, you can: <ul style="list-style-type: none">• Commit failback.
Any	At any point, you can: <ul style="list-style-type: none">• Halt the plan to interrupt its execution.• Undo to attempt reversal of the previous action.• Reset the plan to clear the current state and allow it to run again.

Plan States








Replica plans can acquire the following **default** states after creation. The same states are shown after resetting a plan, and after completing a test or a check.













Plan State	Icon	Description
NOT VERIFIED		Plan has never been tested, has never passed a readiness check, or has been changed since the last DataLab test or readiness check.
		Plan has failed to be tested or has failed to pass a readiness check.
VERIFIED		Plan has been tested successfully or has passed a readiness check.

Replica plans can acquire the following **stable** states after completing current processing:

Plan State	Icon	Description
HALTED		Plan has stopped due to either an error or user intervention.
FAILOVER		Process completed successfully.
UNDO FAILOVER		Process completed with one or more warnings.
PERMANENT FAILOVER		Process completed with one or more errors.
PREPARE FOR FAILBACK		
FAILBACK		
UNDO FAILBACK		
COMMIT FAILBACK		
TESTING HALTED		Plan testing has stopped due to either an error or user intervention.

Replica plans can acquire the following **active** states while in use or in progress:




Functionality	Tab	Plan Operator
Plan Management		
CREATING		Plan is being created.
EDITING		Plan is being edited.
SAVING		Plan is being saved. Note: Plan editing and execution are not available in this state.
RESETTING		Plan is being reset.
DELETING		Plan is being deleted.
Readiness Checks		
CHECKING		Plan readiness check is in progress.
		Plan readiness check is in progress; one or more warnings encountered.

Functionality	Tab	Plan Operator
		Plan readiness check is in progress; one or more errors encountered.
CHECK HALTING		Plan readiness check is halting.
Execution and Testing		
FAILOVER		Plan is executing.
		Plan is executing; one or more warnings encountered.
		Plan is executing; one or more errors encountered.
HALTING		Plan is halting.
TEST PENDING		Plan is waiting for the test lab to power on.
TESTING		Plan testing is in progress.
		Plan testing is in progress; one or more warnings encountered.
		Plan testing is in progress; one or more errors encountered.
TEST HALTING		Plan testing is halting.
POWERING OFF		Plan testing is being powered off.

NOTE

If you perform any infrastructure configuration changes (add, delete or rename VMs) or changes to Veeam ONE Client groups, Orchestrator will not automatically apply these changes to plans that are currently executing or testing – such plans are 'locked' and cannot be edited. The changes will take effect only if the plans enter the *VERIFIED* or *NOT VERIFIED* state.

Replica plans can acquire the following **modes**:

Plan Mode	Icon	Description
ENABLED		Plan is ready to be verified, tested and executed. Notes: Plan editing is not available. Automatic report updates are enabled.
DISABLED		Plan is ready to be edited and tested. Notes: Scheduled plan execution is not available. Automatic report updates are disabled.
IN USE		Plan is either in one of the active states (except the <i>EDITING</i> state) or in one of the stable states. Notes: Plan editing is not available. Automatic report updates are disabled.

TIP

When a plan is in an active state, you can switch to the **Plan Details** page, select a VM being recovered in the **Virtual Machines** column, and click the **VM Console** link to connect directly to the VM desktop.

Orchestrator will connect to the VM through the vCenter Server system. To avoid connection failures, make sure the following requirements are met:

1. The target vCenter Server that manages the VM is running VMware vCenter Server version 6.0 or later.
2. The SSL certificate used by the target vCenter Server is valid on the machine on which you are running the browser. If not, install root certificates from the vCenter Server on both the Orchestrator server and the machine. To learn how to download and install vCenter Server root certificates, see [this VMware KB article](#).

In vSphere 6.0 and later, each newly created ESXi host is by default provisioned with a self-signed certificate from the VMware Certificate Authority. If you want to use such a certificate when accessing the VM desktop, download the root CA certificate from the host where the VM is registered. To learn how to manage certificates for ESXi hosts, see [VMware Docs](#).

Before You Begin

To run a replica plan, it must be *ENABLED*. To enable a plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan.
3. From the **Manage** menu, select **Enable**.

If you do not enable a plan before you run it, the [Run Plan](#) wizard will force you to do that as soon as you try running the plan.

NOTES

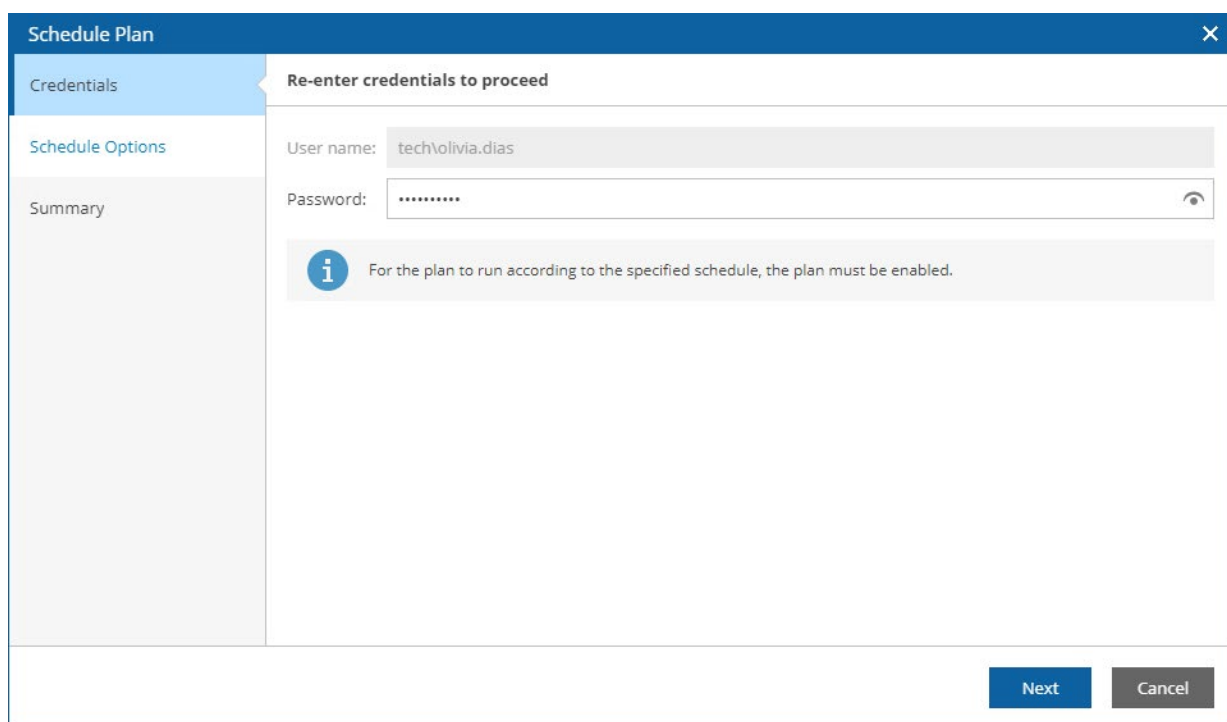
1. An Orchestrator Administrator or Plan Author can force-enable a plan in the **Run Plan** wizard. However, a Plan Operator will not be able to run a disabled replica plan.
For more information on roles that can be assigned to users and user groups working with the Orchestrator UI, see [Managing Permissions](#).
2. For security purposes, all 'real-world' actions associated with replica plans (such as failover and failback) require password confirmation.

Scheduling Failover

You can schedule a time for a replica plan to execute. Only the failover process can be scheduled – all other operations (failback, undo failover and so on) must be performed manually in the Orchestrator UI.

To schedule a replica plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Schedule**.
-OR-
Right-click the plan name and select **Launch > Schedule**.
3. Complete the **Schedule Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.



The screenshot shows the 'Schedule Plan' wizard in the Veeam Orchestrator UI. The window has a title bar 'Schedule Plan' with a close button. On the left is a sidebar with three tabs: 'Credentials' (selected), 'Schedule Options', and 'Summary'. The main area is titled 'Re-enter credentials to proceed'. It contains two input fields: 'User name:' with the value 'tech\olivia.dias' and 'Password:' with masked characters '*****'. There is a toggle icon for the password field. Below the fields is an information message: 'For the plan to run according to the specified schedule, the plan must be enabled.' At the bottom right are 'Next' and 'Cancel' buttons.

- b. At the **Schedule Options** step, set the **Scheduled execution** toggle to *On*, and choose whether you want to run the plan on schedule or after any other plan.
 - If you want to run the plan at a specific time, select the **Schedule on** option, click the **Schedule** icon, set the desired date and time, and click **Apply**.

- If you want to run the plan after another plan, select the **Schedule after** option and click **Choose a Plan**. Then, in the **Select Plan** window, select the necessary plan and click **OK**.

For a plan to be displayed in the **Available Plans** list, it must be *ENABLED* as described in section [Running and Scheduling Replica Plans](#).

The screenshot shows the 'Schedule Plan' wizard with the 'Schedule Options' step selected. The left sidebar has 'Credentials', 'Schedule Options', and 'Summary'. The main area displays the following:

- Header: **You may schedule this Plan to run at a specific time, or chain it to be executed after another Plan runs**. Subtext: Recovery will be performed using the most recent restore point.
- Scheduled execution: ☒ On
- ☐ Schedule on: 11/16/2022 10:30 AM (with a calendar icon)
- ☒ Schedule after: [Test Replica Plan](#)
- Information icon (i): You can schedule only the Failover and Restore actions for Orchestration Plans. Other actions (such as Failback) must be performed manually.

At the bottom right are buttons: Back, Next, and Cancel.

- At the **Summary** step, review configuration information and click **Finish**.

The screenshot shows the 'Schedule Plan' wizard with the 'Summary' step selected. The left sidebar has 'Credentials', 'Schedule Options', and 'Summary'. The main area displays the following:

- Header: **Plan will be scheduled with below settings. Click Finish to apply**
- [Copy to clipboard](#) (with a clipboard icon)
- Plan name: Replica Plan
- Schedule: Enabled
- Ransomware Scan: Disabled
- Choose scheduling options: After Plan: Restore plan

At the bottom right are buttons: Back, Finish, and Cancel.

TIP

You can disable a configured schedule if you no longer need it. To do that, set the **Scheduled execution** toggle to *Off* at the **Schedule Options** step of the **Schedule Plan** wizard.

Running Failover

The **Run** action causes VMs in a plan to fail over to their replicas. For more information on the replica failover process, see the Veeam Backup & Replication User Guide, section [Replica Failover](#).

To run a replica plan:

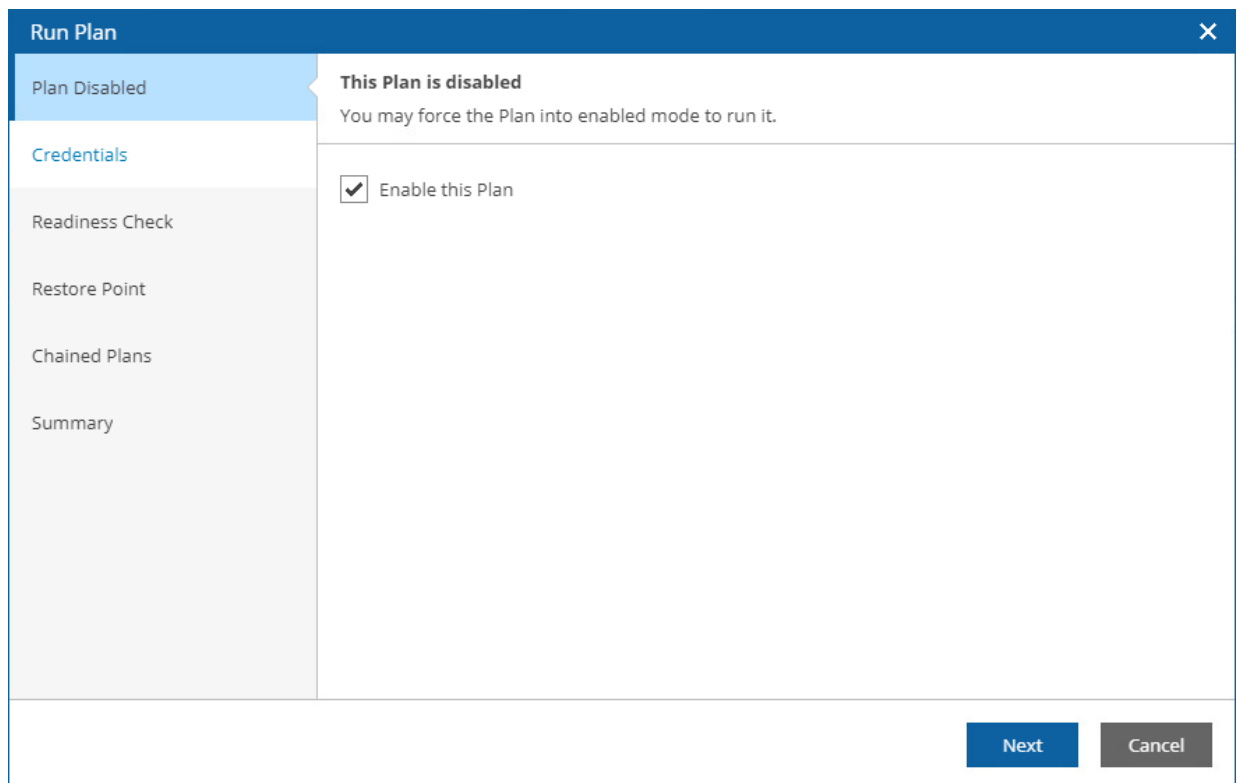
1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Run**.

-OR-

Click the plan name to switch to the **Plan Details** page, and click **Run**.

3. Complete the **Run Plan** wizard:
 - a. [This step applies only if you have not enabled the plan before running it]

At the **Plan Disabled** step, select the **Enable this Plan** check box.



The screenshot shows the 'Run Plan' wizard window. The title bar is 'Run Plan' with a close button. The left sidebar contains the following steps: 'Plan Disabled' (selected), 'Credentials', 'Readiness Check', 'Restore Point', 'Chained Plans', and 'Summary'. The main content area for the 'Plan Disabled' step displays the message 'This Plan is disabled' and 'You may force the Plan into enabled mode to run it.' Below this message is a checked checkbox labeled 'Enable this Plan'. At the bottom right of the window are two buttons: 'Next' and 'Cancel'.

- b. For security purposes, at the **Credentials** step, retype your password.

The screenshot shows the 'Run Plan' dialog box with the 'Credentials' step selected in the left sidebar. The main area is titled 'Re-enter credentials to proceed'. It contains two input fields: 'User name:' with the value 'tech\olivia.dias' and 'Password:' with masked characters '*****'. A 'Show/Hide' eye icon is next to the password field. At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

- c. At the **Readiness Check** step, review the results of the most recent readiness check run for the plan to make sure the plan will be able to complete successfully.

The screenshot shows the 'Run Plan' dialog box with the 'Readiness Check' step selected in the left sidebar. The main area is titled 'Review readiness check report'. It includes a 'Copy to clipboard' link with a document icon, and the following details: 'Executed: 11/25/2022 11:07 AM', 'Result: ⚠ Warning', and 'Details: 0 Errors, 1 Warning'. There is also a 'Download report' link with a download icon. At the bottom, there is an information icon and a message: 'It is highly recommended to run a readiness check before executing a plan.' At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

- d. At the **Restore Point** step, choose a restore point that will be used to recover VM replicas.

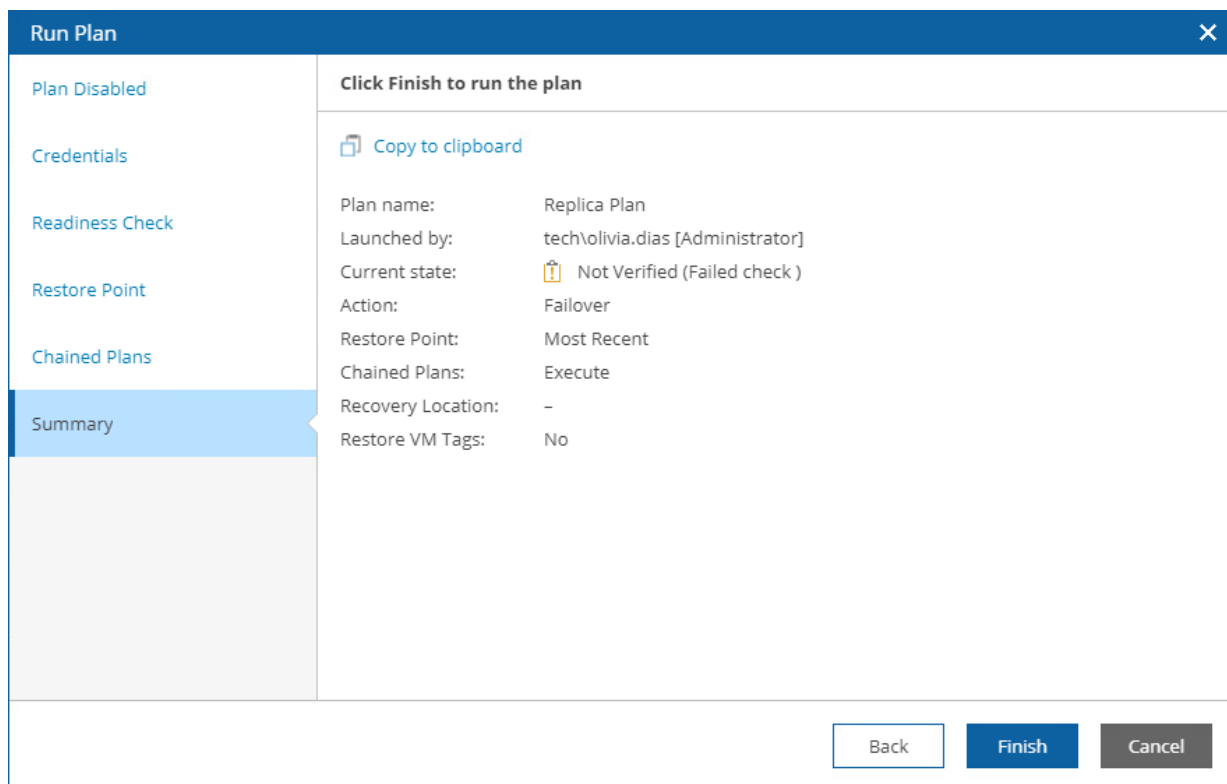
The screenshot shows the 'Run Plan' dialog box with the 'Restore Point' step selected in the left sidebar. The main area is titled 'Choose restore point' and contains two radio button options: 'Use the latest Restore Point' (which is selected) and 'Use most recent Restore Point before: 11/25/2022 11:07 AM' (with a calendar icon). At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons.

- e. [This step applies only if you have any other orchestration plans scheduled to run after the plan completes]



At the **Chained Plans** step, select the **Also execute the chained plans** check box to proceed to execution of subsequent plans after the current plan enters the *FAILOVER* state.

The screenshot shows the 'Run Plan' dialog box with the 'Chained Plans' step selected in the left sidebar. The main area has a header stating 'This Plan is part of a chain, and other Plans will execute when it is complete.' Below this is a checked checkbox labeled 'Also execute the chained plans'. A warning message with a yellow triangle icon states: 'Even Plans which are disabled will be forced to run. All Plans will all use the same restore point option.' At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons.

e. At the **Summary** step, review configuration information and click **Finish**.



The screenshot shows the 'Run Plan' dialog box with the 'Summary' step selected. The configuration details are as follows:

Click Finish to run the plan	
 Copy to clipboard	
Plan name:	Replica Plan
Launched by:	tech\olivia.dias [Administrator]
Current state:	 Not Verified (Failed check)
Action:	Failover
Restore Point:	Most Recent
Chained Plans:	Execute
Recovery Location:	-
Restore VM Tags:	No

At the bottom right, there are three buttons: 'Back', 'Finish', and 'Cancel'.

The plan goal is to reach the *FAILOVER* state. If any critical error is encountered, the plan will stop with the *HALTED* state. To learn how to work with *HALTED* replica plans, see [Managing Halted Plans](#).

Halting Failover

The **Halt** action interrupts plan execution. Any currently executing steps will be completed, then the plan will enter the *HALTED* state. To learn how to work with *HALTED* replica plans, see [Managing Halted Plans](#).

To stop a running replica plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Halt**.

-OR-

Click the plan name to switch to the **Plan Details** page, and click **Halt**.

3. Complete the **Halt Plan** wizard:
 - a. For security purposes, at the **Enter Credentials** step, retype your password.

The screenshot shows a 'Halt Plan' wizard window with a dark blue header and a close button (X) in the top right corner. On the left is a vertical sidebar with three tabs: 'Credentials' (highlighted in blue), 'Schedule Impact', and 'Summary'. The main area of the wizard is titled 'Re-enter credentials to proceed'. It contains two input fields: 'User name:' with the text 'tech\olivia.dias' and 'Password:' with masked characters '*****'. A small eye icon is visible to the right of the password field. At the bottom right of the window are two buttons: 'Next' (blue) and 'Cancel' (grey).

- b. [This step applies only if you have any other orchestration plans scheduled to run after the plan completes]

At the **Schedule Impact** steps, choose whether you want to proceed with or cancel execution of subsequent plans after the current plan enters the *HALTED* state.

The screenshot shows the 'Halt Plan' dialog box with the 'Schedule Impact' tab selected. The left sidebar contains 'Credentials', 'Schedule Impact', and 'Summary'. The main area has two radio buttons: 'Cancel the schedule and do not execute the subsequent Plans' (selected) and 'Continue the schedule and launch the next Plan now'. Below these is a warning icon and text: 'There are other Plan(s) scheduled in a chain to failover after this Plan completes. Choose the options for those scheduled Plans below.' At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

- c. At the **Summary** step, review configuration information and click **Finish**.

The screenshot shows the 'Halt Plan' dialog box with the 'Summary' tab selected. The left sidebar contains 'Credentials', 'Schedule Impact', and 'Summary'. The main area has a heading 'Click Finish to halt the plan' and a 'Copy to clipboard' button. Below is a table of configuration information:

Plan name:	Replica Plan
Halted by:	tech\olivia.dias [Administrator]
Current state:	✓ Failover
Action:	Halt
Schedule Impact:	Restore Plan – Scheduled chain cancelled

Below the table is an information icon and text: 'Halting a plan before it reaches a stable state may cause your environment to enter an inconsistent state, requiring manual troubleshooting and a reset of the plan to resolve.' At the bottom right are 'Back', 'Finish', and 'Cancel' buttons.

Finalizing Failover

Orchestrator provides you a number of options to finalize failover to VM replicas:

- **Permanent Failover** — as a result, VM replicas in the disaster recovery site will no longer be treated as replicas. Restore point snapshots will be deleted, and the source VMs will be removed from replication jobs.

For more information on the permanent failover process, see the Veeam Backup & Replication User Guide, section [Permanent Failover](#).

- **Failback** — you can choose whether you want to fail back to the original or to a new location.
 - If failing back to the original location, you will switch from VM replicas back to the source VMs. The source VMs will be restored to the current state of their replicas.
 - If failing back to a new location, all VM replica files will be copied to the location and used to recover the VMs there.

Failback is a temporary stage that must be further finalized. After confirming that the failed-back VMs operate correctly, you can perform the **Commit failback** operation. Alternatively, [undo failback](#) to return the plan back to the *FAILOVER* state.

For more information on the replica failback process, see the Veeam Backup & Replication User Guide, sections [Replica Failback](#) and [Commit Failback](#).

Depending on the selected option, the plan may enter the *PERMANENT FAILOVER*, *FAILBACK*, *COMMIT FAILBACK* or *HALTED* state. To learn how to work with *HALTED* replica plans, see [Managing Halted Plans](#).

Running Permanent Failover

To perform permanent failover for a plan in the *FAILOVER* state:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Continue**.
-OR-
Click the plan name to switch to the **Plan Details** page, and click **Continue**.
3. Complete the **Run Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.

The screenshot shows the 'Run Plan' wizard window. The left sidebar contains the following steps: 'Credentials' (highlighted in blue), 'Progress Plan', 'Recovery Location', 'Quick Rollback', 'VM Tags', 'Switchover', and 'Summary'. The main area is titled 'Re-enter credentials to proceed' and contains two input fields: 'User name:' with the value 'tech\olivia.dias' and 'Password:' with masked characters '*****'. A toggle icon (an eye) is visible next to the password field. At the bottom right, there are two buttons: 'Next' (blue) and 'Cancel' (gray).

b. At the **Progress Plan** step, select the **Permanent failover** option.

The screenshot shows the 'Run Plan' dialog box with the 'Progress Plan' step selected in the left sidebar. The main area is titled 'Choose one of the following options' and contains two radio buttons: 'Failback / Prepare to failback' and 'Permanent failover'. The 'Permanent failover' option is selected. Below the radio buttons is an information icon and a message: 'After permanent failover completes, undo and failback options will not be available.' At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

c. At the **Summary** step, review configuration information and click **Finish**.

The screenshot shows the 'Run Plan' dialog box with the 'Summary' step selected in the left sidebar. The main area is titled 'Click Finish to run the plan' and contains a 'Copy to clipboard' link. Below this, there is a summary of the plan configuration: Plan name: Replica Plan, Launched by: tech\olivia.dias [Administrator], Current state: ✓ Failover (Complete, no errors, no warnings), and Action: Failover – Permanent. At the bottom right, there are three buttons: 'Back', 'Finish', and 'Cancel'.

NOTE

Failback will no longer be an option once the permanent failover process is complete.

Running Failback

To perform failback for a plan in the *FAILOVER* state:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Continue**.
-OR-
Click the plan name to switch to the **Plan Details** page, and click **Continue**.
3. Complete the **Run Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.

The screenshot shows the 'Run Plan' wizard window. The left sidebar contains the following steps: 'Credentials' (highlighted in blue), 'Progress Plan', 'Recovery Location', 'Quick Rollback', 'VM Tags', 'Switchover', and 'Summary'. The main area is titled 'Re-enter credentials to proceed' and contains two input fields: 'User name:' with the text 'tech\olivia.dias' and 'Password:' with masked characters '.....'. A toggle icon (an eye) is visible next to the password field. At the bottom right, there are two buttons: 'Next' (blue) and 'Cancel' (gray).

- b. At the **Progress Plan** step, select the **Failback / Prepare to failback** option.

The screenshot shows the 'Run Plan' dialog box. On the left, a sidebar lists steps: Credentials, Progress Plan (highlighted), Recovery Location, Quick Rollback, VM Tags, Switchover, and Summary. The main panel is titled 'Choose one of the following options' and contains two radio buttons. The first radio button, labeled 'Failback / Prepare to failback', is selected. The second radio button is labeled 'Permanent failover'. Below these options is an information icon (i) followed by the text: 'Failback to the original location or to a new location, or synchronize disks to prepare for failback later.' At the bottom right of the dialog are three buttons: 'Back', 'Next', and 'Cancel'.

- c. At the **Recovery Location** step, select a location to which VMs will be recovered.

For a recovery location to be displayed in the list of available locations, it must be created and included into the list of inventory items available for the scope, as described in section [Managing Recovery Locations](#).

NOTE

Orchestrator will perform failback using all [settings configured for the location](#) — except Instant VM Recovery and backup copy preference. These settings are not applicable to failback operations.

Run Plan

Credentials

Progress Plan

Recovery Location

Quick Rollback

VM Tags

Switchover

Summary

Choose recovery location

Selecting the original VM location will fail back to the source VMs. Using any other recovery location will create new VMs.

Type any part of name to filter

Name	VMs	Agents	Instant VM Reco...
Original VM Location	Enabled	Disabled	Enabled
Restore Recovery Location	Enabled	Enabled	Enabled

Back

Next

Cancel

If you want to fail back to a new recovery location and the selected location includes multiple hosts, datastores and networks, Orchestrator will use the round-robin algorithm to recover VMs. For more information, see [How Orchestrator Places VMs During Failback](#).

d. [This step applies only if you have selected the Original VM Location]

At the **Quick Rollback** step, choose whether you want to instruct Orchestrator to synchronize changed data blocks only – this may help you speed up the failback process significantly.

130 | Veeam Disaster Recovery Orchestrator | Operations Guide

For more information on the quick rollback process, see the Veeam Backup & Replication User Guide, section [Quick Rollback](#).

The screenshot shows the 'Run Plan' dialog box with the 'Quick Rollback' step selected in the left sidebar. The main area is titled 'Choose quick rollback option'. It contains a checked checkbox labeled 'Use quick rollback'. Below this is an information box with an 'i' icon and the text: 'Quick rollback is appropriate if failover was caused by a software problem or user error. Do not use this option if the failover was caused by a hardware problem, storage issue, or power loss.' At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

- e. At the **VM Tags** step, choose whether you want the recovered VMs to have the same tags as the source VMs.

The screenshot shows the 'Run Plan' dialog box with the 'VM Tags' step selected in the left sidebar. The main area is titled 'Choose whether to restore VM tags'. It contains a checked checkbox labeled 'Restore VM tags'. At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

- f. At the **Switchover** step, choose whether you want to switch from VM replicas to the source VMs immediately or to synchronize the VM disks without actually performing failback.

If you select the **Prepare for failback** option, Orchestrator will switch from VM replicas to the source VMs when you run the plan next time.

The screenshot shows the 'Run Plan' dialog box with the 'Switchover' step selected in the left sidebar. The main area is titled 'Choose when to perform replica switchover'. It contains two radio button options: 'Failback now' (selected) with the description 'Switchover replicas immediately', and 'Prepare for failback' with the description 'Switchover replicas on next plan run'. Below these options is an information icon and a note: 'This option will synchronize VM disks then trigger failback immediately.' At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

- g. At the **Summary** step, review configuration information and click **Finish**.

The screenshot shows the 'Run Plan' dialog box with the 'Summary' step selected in the left sidebar. The main area is titled 'Click Finish to run failback'. It features a 'Copy to clipboard' button and a list of configuration details: Plan name: Replica Plan; Launched by: tech\olivia.dias [Administrator]; Current state: ✓ Failover (Complete, no errors, no warnings); Action: Failback to Production; Recovery Location: Original VM Location; Restore VM Tags: Yes; Quick Rollback: Yes; Switchover: Failback now. At the bottom right, there are three buttons: 'Back', 'Finish', and 'Cancel'.

How Orchestrator Places VMs During Failback

To fail back VMs included into a replica plan to a new recovery location, Orchestrator uses the following algorithm:

1. The solution looks through all hosts added to the location as [compute resources](#) to detect the first available host. This is the host where the first processed VM will be registered.
2. Orchestrator applies the mapping specified in the [network mapping table](#) for the location to set the required network configuration of the recovered VM.

Orchestrator checks whether the network configuration of the detected host matches the required network configuration. If these configurations do not match, Orchestrator goes back to step 1.

3. In the list of datastores connected to the host as [storage resources](#), Orchestrator searches for the first datastore that both is available and has enough capacity. This is the datastore where files of the VM will be stored.

To calculate the datastore capacity and make sure that it has enough space to accommodate the recovered VM, Orchestrator uses the threshold that you specify [when creating or configuring the location](#).

NOTE

The failure of steps 1–3 for a VM from a [critical inventory group](#) halts the plan in the following cases:

- If none of the discovered hosts is available, or if none of the hosts has network configuration that matches the required network configuration of the recovered VM.
- If none of the discovered datastores is available, or if none of the datastores meets the capacity requirements.

To learn how to work with *HALTED* replica plans, see [Managing Halted Plans](#).

4. When Orchestrator starts processing the next VM, the solution looks through all hosts added to the location as compute resources to detect the next available host:
 - If Orchestrator detects such a host, this is the host where the VM will be registered.
 - If there are no more available hosts, Orchestrator uses the host detected at step 1 to register the VM.

Then, Orchestrator goes through steps 2–3 to detect the target network and datastore for the VM.

5. Orchestrator repeats step 4 for all other VMs included in the plan until all the VMs are recovered. The order in which the VMs are processed depends on the **VM Recovery Options** defined [while configuring the plan](#).

If datastores added to the recovery location as storage resources breach the capacity threshold before all the VMs are recovered, the failure of this step for a VM from a critical inventory group halts the plan. To troubleshoot the issue, configure the location to add more datastores and try running the halted plan again. To learn how to work with *HALTED* replica plans, see [Managing Halted Plans](#).

Committing Failback

To commit failback for a plan in the *FAILBACK* state:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Continue**.
-OR-
Click the plan name to switch to the **Plan Details** page, and click **Continue**.
3. Complete the **Run Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.

The screenshot shows a 'Run Plan' dialog box with a dark blue header and a close button (X) in the top right corner. The dialog is divided into two main sections. On the left is a sidebar with two tabs: 'Credentials' (which is selected and highlighted in light blue) and 'Summary'. The 'Summary' tab is currently inactive. The main area on the right is titled 'Re-enter credentials to proceed'. It contains two input fields: 'User name:' with the text 'tech\wendy.may' and 'Password:' with a masked password represented by ten dots. To the right of the password field is a small eye icon for toggling visibility. At the bottom right of the dialog are two buttons: 'Next' (in blue) and 'Cancel' (in grey).

b. At the **Summary** step, review configuration information and click **Finish**.

The screenshot shows the 'Run Plan' dialog box with the 'Summary' tab selected. The dialog contains the following information:

Click Finish to commit failback	
Copy to clipboard	
Plan name:	Replica Plan
Launched by:	tech\olivia.dias [Administrator]
Current state:	✔ Failback (Complete, no errors, no warnings)
Action:	Commit Failback
Recovery Location:	-
Restore VM Tags:	No

At the bottom, there is an information icon and a note: "Commit failback only updates the configuration of the jobs and replicas in the Veeam Backup & Replication server. It takes no action in the virtual infrastructure." Below the dialog, there are three buttons: 'Back', 'Finish' (highlighted in blue), and 'Cancel'.

TIP

After the commit failback process completes, Orchestrator will leave the plan in the *IN USE* state. By design, this makes the results of the commit failback process accessible in the Orchestrator UI as long as required, and also prevents the plan from being modified by any automatic updates related to infrastructure changes.

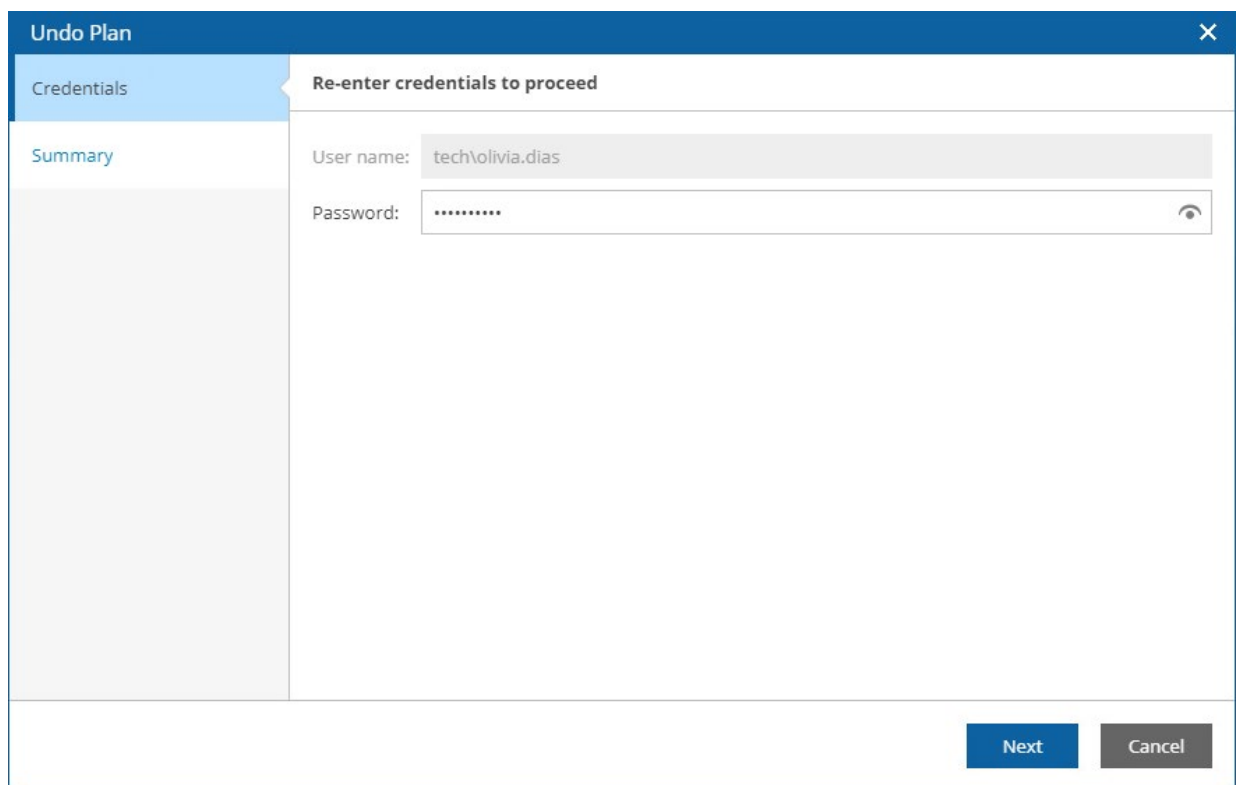
If you want to perform any further actions with the plan (for example, to test the plan, to run readiness checks or to execute the plan again), reset the plan as described in section [Resetting Replica Plans](#).

Undoing Failover

The **Undo Failover** action powers off VM replicas running on target hosts and roll back to the VM state before failover. For more information on the undo failover operation, see the Veeam Backup & Replication User Guide, section [Undo Failover](#).

To perform an undo operation for a plan in the *FAILOVER* state:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Undo**.
-OR-
Click the plan name to switch to the **Plan Details** page, and click **Undo**.
3. Complete the **Undo Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.



The screenshot shows the 'Undo Plan' wizard window. The title bar is 'Undo Plan' with a close button. The left sidebar has two tabs: 'Credentials' (selected) and 'Summary'. The main area is titled 'Re-enter credentials to proceed'. It contains two input fields: 'User name:' with the text 'tech\olivia.dias' and 'Password:' with masked characters '*****'. There is an eye icon to the right of the password field. At the bottom right, there are two buttons: 'Next' (blue) and 'Cancel' (gray).

b. At the **Summary** step, review configuration information and click **Finish**.

Undo Plan [X]

Credentials

Summary

Click **Finish** to undo the most recent steps

Copy to clipboard

Plan name: Replica Plan

Undo by: TECH\olivia.dias [Administrator]

Current state: Failover (Halted, 83% complete, 1 error, no warnings)

Undo action: Undo Failover

i Undo will attempt to revert the plan to the last stable state. After undo is initiated:

- The run control will be disabled until the undo process has completed.
- The halt control may be used to halt the undo process.
- After halting use the undo control to resume the undo process.

During undo any errors will be ignored.

Back Finish Cancel

If the undo failover process encounters an error while being performed, it will not be halted automatically – the plan will proceed until the process completes. To terminate the undo failover process manually, use the **Halt** option to stop the currently running plan as described in section [Halting Failover](#). To resume the undo failover process again, use the **Undo** option.

Undoing Failback

The **Undo Failback** action powers on VM replicas running on target hosts and switches from the production VMs back to the VM replicas – as a result, the plan acquires the *FAILOVER* state. For more information on the undo failback operation, see the Veeam Backup & Replication User Guide, section [Undo Failback](#).

To perform an undo operation for a plan in the *PREPARE FOR FAILBACK* or *FAILBACK* state:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Undo**.
-OR-
Click the plan name to switch to the **Plan Details** page, and click **Undo**.
3. Complete the **Undo Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.

The screenshot shows a window titled "Undo Plan" with a close button (X) in the top right corner. The window has a left sidebar with two tabs: "Credentials" (selected) and "Summary". The main area is titled "Re-enter credentials to proceed" and contains two input fields: "User name:" with the text "tech\wendy.may" and "Password:" with masked characters ".....". A small eye icon is visible to the right of the password field. At the bottom right, there are two buttons: "Next" (blue) and "Cancel" (gray).

b. At the **Summary** step, review configuration information and click **Finish**.

Undo Plan

Credentials

Summary

Click **Finish** to undo the most recent steps

Copy to clipboard

Plan name: Replica Plan

Undo by: tech\olivia.dias [Administrator]

Current state: Failback (Complete, no errors, no warnings)

Undo action: Undo Failback

Undo will attempt to revert the plan to the last stable state. After undo is initiated:

- The run control will be disabled until the undo process has completed.
- The halt control may be used to halt the undo process.
- After halting use the undo control to resume the undo process.

During undo any errors will be ignored.

Back Finish Cancel

If the undo failback process encounters an error while being performed, it will not be halted automatically – the plan will proceed until the process completes. To terminate the undo failback process manually, use the **Halt** option to stop the currently running plan as described in section [Halting Failover](#). To resume the undo failback process again, use the **Undo** option.

Resetting Replica Plans

If a replica plan becomes inconsistent with the virtual environment, you can reset the plan. This will return the plan to the *DISABLED* state, without making any changes to the external virtual infrastructure.

To reset a replica plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Manage** menu, select **Reset**.
-OR-
Right-click the plan name and select **Manage > Reset**.
3. Complete the **Reset Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.

The screenshot shows the 'Reset Plan' wizard window. The title bar is 'Reset Plan' with a close button. The left sidebar has three tabs: 'Credentials' (selected), 'Quick Check', and 'Summary'. The main area is titled 'Re-enter credentials to proceed'. It contains two input fields: 'User name:' with the text 'tech\olivia.dias' and 'Password:' with masked characters '*****'. There is a toggle icon for the password field. Below the fields is an information box with an 'i' icon and the text: 'Reset will take no actions on VMs or replicas in your infrastructure. It will reinitialize the Plan in Orchestrator only. For *Halted* plans it is recommended to use Undo, not Reset.' At the bottom right are 'Next' and 'Cancel' buttons.

- b. At the **Quick Check** step, select the **Perform a Quick Check after reset is complete** check box to run a **readiness check** after the rest.

The screenshot shows the 'Reset Plan' dialog box with the 'Quick Check' tab selected. The left sidebar contains 'Credentials', 'Quick Check', and 'Summary'. The main area displays the message 'It is recommended to run a Quick Check after resetting the plan' and a checked checkbox for 'Perform a Quick Check after reset is complete'. At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

Reset Plan	
Credentials	It is recommended to run a Quick Check after resetting the plan
Quick Check	<input checked="" type="checkbox"/> Perform a Quick Check after reset is complete
Summary	

Back Next Cancel

- c. At the **Summary** step, review configuration information and click **Finish**.

The screenshot shows the 'Reset Plan' dialog box with the 'Summary' tab selected. The left sidebar contains 'Credentials', 'Quick Check', and 'Summary'. The main area displays the message 'Plan will be reset using the options below. Press Finish to reset the Plan' and a 'Copy to clipboard' link. Below this, the configuration details are listed: Plan Name: Replica Plan, Reset by: TECH\olivia.dias [Administrator], Current State: Failsafe (Halted, 83% complete, 1 error, no warnings), and Quick Check: Yes. At the bottom right are 'Back', 'Finish', and 'Cancel' buttons.

Reset Plan	
Credentials	Plan will be reset using the options below. Press Finish to reset the Plan
Quick Check	Copy to clipboard
Summary	<p>Plan Name: Replica Plan</p> <p>Reset by: TECH\olivia.dias [Administrator]</p> <p>Current State: ⊖ Failsafe (Halted, 83% complete, 1 error, no warnings)</p> <p>Quick Check: Yes</p>

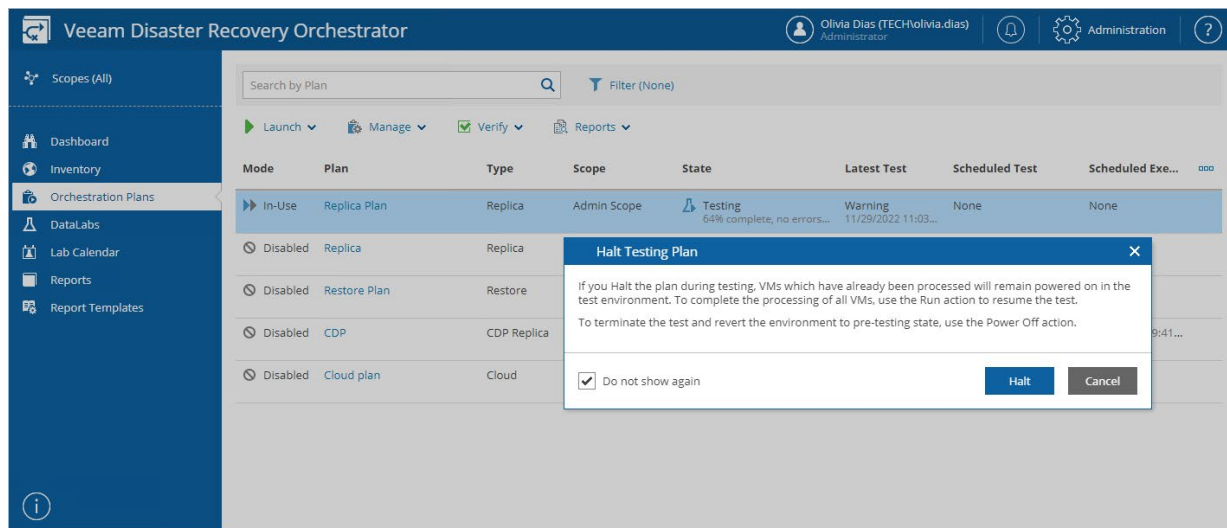
Back Finish Cancel

Halting Plan Testing

The **Halt** action interrupts plan testing. You may need to halt plan testing, for example, if you need to fix some environment-related issues and then [proceed with testing later](#) (in this case, VM replicas will still continue to run). Or you may need to stop the testing process completely, for example, if you no longer need to test the selected replica plan (in this case, VM replicas will be reverted to the latest restore point).

To halt testing of a replica plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Verify** menu, select **Halt DataLab Test**.
-OR-
Right-click the plan name and select **Verify > Halt DataLab Test**.
3. In the **Halt Testing Plan** window, click **Halt** to confirm the action.



To cancel testing of a replica plan:

1. Select the plan. From the **Verify** menu, select **Power Off DataLab Test**.
-OR-
Right-click the plan name and select **Verify > Power Off DataLab Test**.
2. In the **Power Off Testing Plan** window, click **Power Off** to confirm the action.

Veeam Disaster Recovery Orchestrator

Olivia Dias (TECH\olivia.dias)

Administrator

Administration

Scopes (All)

Dashboard

Inventory

Orchestration Plans

DataLabs

Lab Calendar

Reports

Report Templates

Search by Plan

Filter (None)

Launch Manage Verify Reports

Mode	Plan	Type	Scope	State	Latest Test	Scheduled Test	Scheduled Exe...
In-Use	Replica Plan	Replica	Admin Scope	Testing 64% complete, no errors...	Warning 11/29/2022 11:03...	None	None
Disabled	Replica	Replica				None	None
Disabled	Restore Plan	Restore				None	None
Disabled	CDP	CDP Replica				None	11/29/2022 9:41...
Disabled	Cloud plan	Cloud				None	None

Power Off Testing Plan

If you run the Power Off action when testing a plan, Orchestrator will stop the testing process as soon as the currently executed step completes, and revert the test environment to the pre-testing state.

Power OffCancel

Managing Halted Replica Plans

If a critical step fails for a VM from a [critical inventory group](#), the plan may enter the *HALTED* state. To troubleshoot reasons why a plan failed, use the **Plan Execution Report** generated as soon as the currently performed action completes. For more information on how to track plan performance history, see [Viewing Plan Execution History](#).

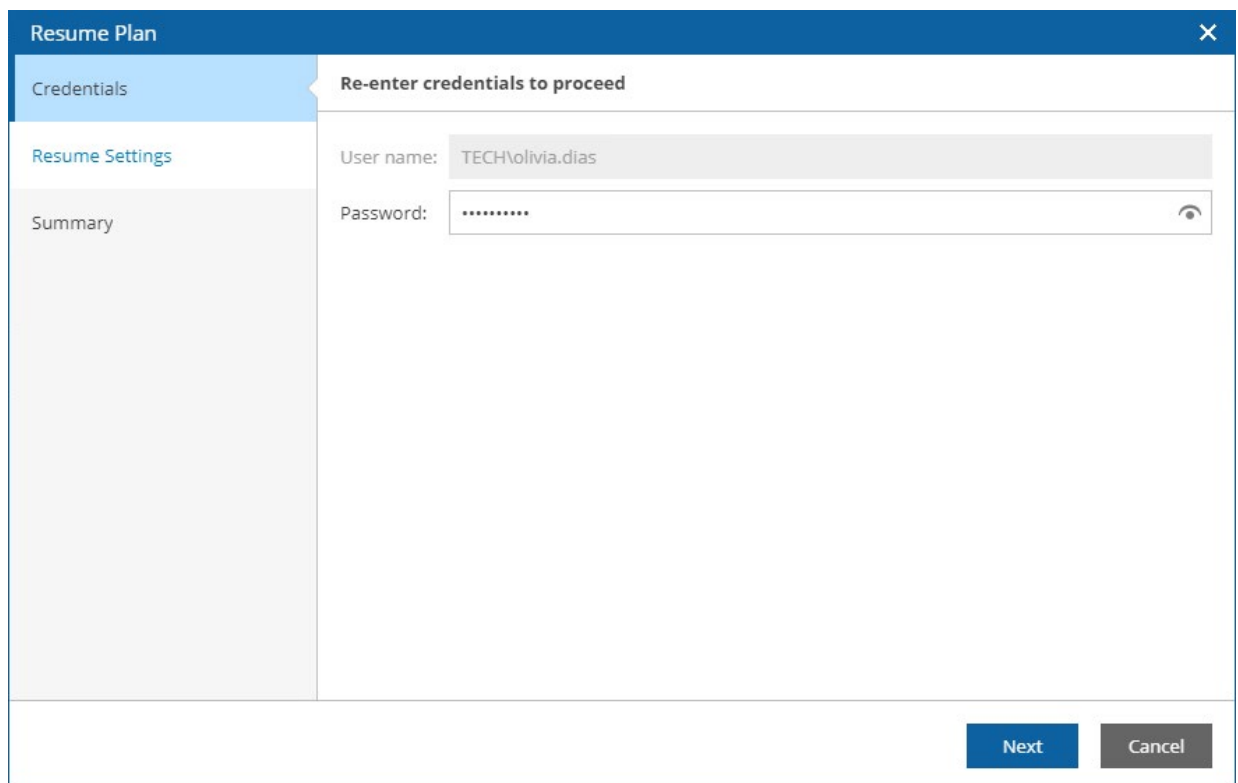
After you eliminate the problem that caused the plan to become *HALTED*, you have the following options to resume the plan:

- Repeat the last failed step.
- Proceed to the next step.

Running Halted Replica Plans

To run a *HALTED* replica plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Continue**.
-OR-
Click the plan name to switch to the **Plan Details** page, and click **Continue**.
3. Complete the **Run Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.



The screenshot shows a 'Resume Plan' dialog box with a dark blue header and a close button (X) in the top right corner. On the left, there is a vertical sidebar with three tabs: 'Credentials' (highlighted in light blue), 'Resume Settings', and 'Summary'. The main area of the dialog is titled 'Re-enter credentials to proceed'. It contains two input fields: 'User name:' with the text 'TECH\volivia.dias' and 'Password:' with masked characters '*****'. A small eye icon is visible to the right of the password field. At the bottom right, there are two buttons: 'Next' (blue) and 'Cancel' (grey).

- b. At the **Resume Settings** step, select an option to resume plan execution.

Choose whether you want to proceed with plan execution from the next plan step or to retry the failed step.

The screenshot shows the 'Resume Plan' dialog box with the 'Resume Settings' step selected in the left sidebar. The main area is titled 'Choose one of the following options' and contains two radio button options: 'Retry failed step' (selected) and 'Proceed to next step'. Below the options, there is an information icon and a note: 'If VMs are being processed in parallel, then multiple failed steps may be retried.' At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

Resume Plan	
Credentials	Choose one of the following options <input checked="" type="radio"/> Retry failed step If the most recently executed step failed, it will be retried <input type="radio"/> Proceed to next step The plan will proceed to the next step <div> If VMs are being processed in parallel, then multiple failed steps may be retried.</div>
Resume Settings	
Summary	
<div>BackNextCancel</div>	

- c. At the **Summary** step, review configuration information and click **Finish**. The failover process will be started.

The screenshot shows the 'Resume Plan' dialog box with the 'Summary' step selected in the left sidebar. The main area is titled 'Click Finish to resume the plan' and contains a 'Copy to clipboard' link. Below this, there is a table of configuration information. At the bottom right, there are three buttons: 'Back', 'Finish', and 'Cancel'.

Resume Plan															
Credentials	Click Finish to resume the plan Copy to clipboard <table><tr><td>Plan name:</td><td>Replica Plan</td></tr><tr><td>Launched by:</td><td>TECH\olivia.dias [Administrator]</td></tr><tr><td>Current state:</td><td> Failover (Halted, 83% complete, 1 error, no warnings)</td></tr><tr><td>Action:</td><td>Resume – Failover</td></tr><tr><td>Resume by:</td><td>Retry failed Step</td></tr><tr><td>Recovery Location:</td><td>–</td></tr><tr><td>Restore VM Tags:</td><td>No</td></tr></table>	Plan name:	Replica Plan	Launched by:	TECH\olivia.dias [Administrator]	Current state:	Failover (Halted, 83% complete, 1 error, no warnings)	Action:	Resume – Failover	Resume by:	Retry failed Step	Recovery Location:	–	Restore VM Tags:	No
Plan name:		Replica Plan													
Launched by:		TECH\olivia.dias [Administrator]													
Current state:	Failover (Halted, 83% complete, 1 error, no warnings)														
Action:	Resume – Failover														
Resume by:	Retry failed Step														
Recovery Location:	–														
Restore VM Tags:	No														
Resume Settings															
Summary															
<div>BackFinishCancel</div>															

Resuming Plan Testing

To start the *HALTED* plan testing process:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Verify** menu, select **Continue DataLab Test**.

-OR-

Right-click the plan name and select **Verify > Continue DataLab Test**.

3. Complete the **Resume DataLab Test** wizard:
 - a. At the **Resume Test** step, select an option to resume test execution.

Choose whether you want to proceed with test execution from the next plan step or to retry the failed step.

The screenshot shows a dialog box titled "Resume DataLab Test" with a close button (X) in the top right corner. The dialog has a sidebar on the left with two tabs: "Resume Test" (selected) and "Summary". The main content area of the "Resume Test" tab displays the heading "You have the following options to resume this Plan test." followed by two radio button options: "Retry failed" (selected) with the subtext "If the last executed step failed, it will be retried", and "Proceed to next" with the subtext "The plan will proceed to the next step". At the bottom right of the dialog are two buttons: "Next" (blue) and "Cancel" (grey).

- b. At the **Summary** step, review configuration information and click **Finish**. The testing process will be started.

Resume DataLab Test

Resume Test

Summary

Your settings are summarized below

Plan Name:

Scope:

DataLab:

Plan State:

Action:

Resume by:

Replica Plan 01

Admin Scope

Testing Plan 01

Testing – Halted

Resume Testing

Retry failed Step

Back

Finish

Cancel

Undoing Halted Replica Plans

To perform an undo operation for a *HALTED* replica plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Undo**.
-OR-
Click the plan name to switch to the **Plan Details** page, and click **Undo**.
3. Complete the **Undo Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.

The screenshot shows a window titled "Undo Plan" with a close button (X) in the top right corner. The window is divided into two main sections. On the left is a sidebar with two tabs: "Credentials" (which is selected and highlighted in blue) and "Summary". The "Summary" tab is currently inactive. The main area of the window is titled "Re-enter credentials to proceed". It contains two input fields: "User name:" with the text "tech\olivia.dias" entered, and "Password:" with a masked password "*****" and a toggle icon (an eye) to the right. At the bottom right of the window, there are two buttons: "Next" (in blue) and "Cancel" (in grey).

- b. At the **Summary** step, review configuration information and click **Finish**. The failover process will be started.

Undo Plan

Credentials

Summary

Click Finish to undo the most recent steps

Copy to clipboard

Plan name: Replica Plan
Undo by: tech\olivia.dias [Administrator]
Current state: Failover (Halted, 15% complete, 10 errors, 1 warning)
Undo action: Undo Failover

Undo will attempt to revert the plan to the last stable state.
After undo is initiated:

- The run control will be disabled until the undo process has completed.
- The halt control may be used to halt the undo process.
- After halting use the undo control to resume the undo process.

During undo any errors will be ignored.

Back

Finish

Cancel

If a plan repeatedly enters the *HALTED* state due to misconfiguration or changes in the external environment, the only option left may be to **RESET** the plan.

Resetting Halted Replica Plans

To reset a *HALTED* replica plan, follow the instructions provided in section [Resetting Replica Plans](#).

NOTE

When you reset a replica plan, Orchestrator returns it to the *DISABLED* state without making any changes to the external virtual infrastructure. You may need to deal with any infrastructure reconfiguration manually.

Working with CDP Replica Plans

The type of an orchestration plan you create depends on whether you intend to use Orchestrator to switch to VM replicas, to restore machines from backups or backup copies, or to serve data from a destination (NetApp) or secondary (HPE) volume in case a disaster strikes.

If you want to recover vSphere VMs protected by Veeam CDP policies, create a CDP replica plan.

Creating CDP Replica Plans

To create a CDP replica plan:

1. Navigate to **Orchestration Plans**.
2. Click **Manage > New**.
3. Complete the **New Orchestration Plan** wizard:
 - a. [Specify a plan name and description](#).
 - b. [Choose a scope for the plan](#).
 - c. [Choose a type of the plan](#).
 - d. [Include inventory groups in the plan](#).
 - e. [Specify VM recovery options](#).
 - f. [Add steps to the plan](#).
 - g. [Specify credentials for the plan steps](#).
 - h. [Specify the target RTO and RPO](#).
 - i. [Select a template for plan reports](#).
 - j. [Specify scheduling options for plan reports](#).
 - k. [Finish working with the wizard](#).

Step 1. Specify Plan Name and Description

At the **Plan Info** step of the wizard, use the **Plan Name** and **Description** fields to enter a name for the new plan and to provide a description for future reference. The maximum length of the plan name is 64 characters; the following characters are not supported: * : / \ ? " < > | .

You can also provide a contact name, email and telephone number of a person responsible for the plan.

New Orchestration Plan

Plan Info

Scope

Plan Type

Recovery Location

VM Groups

VM Recovery Options

VM Steps

RTO & RPO

Report Template

Report Scheduling

Summary

Provide details for the new Orchestration Plan

Plan Name:

Test CDP Replica Plan

Description:

Evaluating continuous data protection

Contact Name:

Hue Spenser

Contact Email:

hue.spenser@veeam.com

Contact Tel:

18005556677

Next

Cancel

Step 2. Choose Plan Scope

At the **Scope** step of the wizard, select a scope for which you want to create the plan.

For a scope to be displayed in the **Available Scopes** list, it must be created and customized as described in section [Managing Permissions](#).

New Orchestration Plan

Plan Info

Scope

Plan Type

Recovery Location

VM Groups

VM Recovery Options

VM Steps

RTO & RPO

Report Template

Report Scheduling

Summary

Choose a Scope

Type any part of Scope name to filter

Available Scopes

Admin Scope

SQL Administrators

Exchange Administrators

Back

Next

Cancel

Step 3. Choose Plan Type

At the **Plan Type** step of the wizard, select the **CDP Replica** option.

New CDP Replica Plan

Plan Info

Plan Type

VM Groups

VM Recovery Options

VM Steps

RTO & RPO

Report Template

Report Scheduling

Summary

Choose the type of Plan

☐ Cloud

VMs will be recovered from Veeam agent or vSphere backups into a cloud environment

☒ CDP Replica

VMs will be recovered from Veeam CDP (continuous data protection) replicas

☐ Replica

VMs will be recovered from Veeam replicas

☐ Storage

VMs will be recovered from replicated storage volumes

☐ Restore

VMs will be recovered from Veeam agent or vSphere backups into a VMware vSphere environment

Back

Next

Cancel

Step 4. Add Inventory Groups

At the **VM Groups** step of the wizard, select inventory groups that you want to recover, and click **Add** to include them in the plan.

For an inventory group to be displayed in the **Available Groups** list, it must be included into the list of inventory items available for the scope, as described in section [Allowing Access to Inventory Groups](#).

IMPORTANT

For Orchestrator to be able to recover a VM correctly, the VM must have VMware Tools installed. The presence of VMware Tools is checked automatically on the vCenter Server side – for both Windows-based and Linux-based VMs. To know how to install and upgrade VMware Tools in vSphere, see [this VMware KB article](#).

New CDP Replica Plan

Plan Info

Scope

Plan Type

VM Groups

VM Recovery Options

VM Steps

RTO & RPO

Report Template

Report Scheduling

Summary

Add VM Groups

Use View VMs control to check Group members, and Up/Down controls to change the recovery sequence.

Search

Available Groups

MK (cdpvc) - mk_normlinux_5

owner - audrey.allen

owner - chloe.lewis

owner - Infrastructure

owner - joelle.van.dyne

owner - john.smith

owner - rick.deckard

owner - ryan.smith

owner - sara.baker

owner - shared

owner - stan.smith

owner - wendy.may

Veeam-InstantVMRecovery - RestAPITag

Add

Remove

Show empty Groups

Plan Groups

Datastore - mk_vol_5

Datastore - mk_vol_9

owner - hue.spenser

Up

Down

View VMs

These options can be customized later on the Edit Plan page.

Back

Next

Cancel

Step 5. Specify VM Recovery Options

At the **VM Recovery Options** step of the wizard, use the **If the VM recovery encounters an error then** options to choose whether you want to plan execution if VM recovery fails. This option can also be customized later per-group [when editing the plan](#).

Use the **Recover the VMs in each group** options to choose whether you want to recover VMs in sequence or in parallel. If you select to process VMs simultaneously, use the **Recover simultaneously max of VMs** field to specify the maximum number of VMs processed at the same time.

The screenshot shows the 'New CDP Replica Plan' wizard with the 'VM Recovery Options' step selected in the left sidebar. The main panel is titled 'Customize the default recovery options for all VMs in the Plan'. It contains the following options:

- If the VM recovery encounters an error then:**
 - ☒ Halt the plan
 - ☐ Proceed with the plan
- Recover the VMs in each group:**
 - ☒ In parallel
 - ☐ In sequence
- Recover simultaneously max of:** 10 VMs (with a spinner control)

An information message at the bottom states: 'These options can be customized later on the Edit Plan page.' At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons.

Step 6. Add Plan Steps

At the **VM Steps** step of the wizard, use the list of plan steps to select steps to be performed for each VM during failover.

For a step to be displayed in the **Available Steps** list, it must be included into the list of inventory items available for the scope, as described in section [Allowing Access to Plan Steps](#).

IMPORTANT

To allow the failover process to perform successfully, the **Process CDP Replica VM** step must execute first.

By default, Orchestrator will perform the same selected steps in the same order for all new VMs that will later appear in the inventory groups included in the plan. However, you can change the step execution order and modify the list of steps individually for each VM, as described in section [Configuring Steps](#).

NOTE

If a VM is included in multiple inventory groups in the same plan, Orchestrator will only run the **Process CDP Replica VM** step once. However, other steps for this VM will execute when processing it in each group.

New CDP Replica Plan

Plan Info

Scope

Plan Type

VM Groups

VM Recovery Options

VM Steps

VM Credentials

RTO & RPO

Report Template

Report Scheduling

Summary

Choose VM Steps

Add Steps to be executed for all VMs in the Plan. These Steps will also be used for all new VMs added to the Plan in the future.

Search

Available Steps

- Verify DNS Port
- Verify Domain Controller Port
- Verify Exchange Mailbox
- Verify Exchange MAPI Connectivity
- Verify Exchange Services
- Verify Global Catalog Port
- Verify Mail Server Port
- Verify SharePoint URL
- Verify SQL Database
- Verify SQL Port
- Verify Web Server Port
- Verify Web Site (IIS)
- VM Power Actions

Add >

< Remove

Selected Steps

- Process CDP Replica VM
- Check VM Heartbeat
- Ping VM Network
- Start Service
- VM Power Actions

Up Down

These options can be customized later on the Edit Plan page.

Back Next Cancel

Step 7. Specify Credentials

[This step applies only if you have added one or more plan steps that require Windows credentials to run in-guest OS scripts inside VMs being processed. For the full list of steps that require authentication, see [Appendix. Orchestration Plan Steps](#)]

At the **VM Credentials** step of the wizard, specify credentials that will be used to access guest OSes of VMs. To do that, click the link in the **Credentials** section, and select the necessary credentials in the **Select Credentials** window. For a credential record to be displayed in the **Available Credentials** list, it must be included into the list of inventory items for the scope, as described in section [Allowing Access to Credentials](#).

If you do not specify any credentials, Orchestrator will use the default credentials defined when configuring plan steps on the **Administration** page of the Orchestrator UI, or you may specify the required credentials individually for each VM [when editing the plan](#).

New CDP Replica Plan

Plan Info

Scope

Plan Type

VM Groups

VM Recovery Options

VM Steps

VM Credentials

RTO & RPO

Report Template

Report Scheduling

Summary

Choose credentials to be used for operations in the VM guest OS

Some of the selected VM steps require credentials. Choose credentials that will be used to run all the steps. If you do not choose credentials, each step will use the default credentials configured by an Orchestrator administrator.

Credentials: Default

Select Credentials

Type any part of name to filter

Available Credentials

User Name	Description
John Smith (TECH\jo...	esx02\Administrator
tech\olivia.dias	Administrator's credentials

Default OK Cancel

Back Next Cancel

Step 8. Specify Target RTO and RPO

At the **RTO & RPO** step of the wizard, define your Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for the plan:

- The **Target RPO** defines the maximum acceptable period of data loss.
- The **Target RTO** represents the amount of time it should take to recover from an incident.

RTO and RPO performance will be recorded in the [Plan Readiness Check](#), [Plan Execution](#) and [DataLab Test](#) reports, and you will be able to track the achieved RTO and RPO objectives for each plan on the [Home Page Dashboard](#).

New CDP Replica Plan

×

Plan Info

Scope

Plan Type

VM Groups

VM Recovery Options

VM Steps

VM Credentials

RTO & RPO

Report Template

Report Scheduling

Summary

Define your Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for this plan

Hours:Minutes:Seconds:

Target RTO:100

Maximum allowed time before the service is restored after a failure.

Hours:Minutes:Seconds:

Target RPO:0015

Maximum allowed loss of historical data after a failure.

Back

Next

Cancel

Step 9. Select Report Template

At the **Report Template** step of the wizard, select a document template that will be used as the cover page for all Orchestrator reports. Use options in the **Document format** list to choose whether you want to generate documents in the DOCX or PDF format.

For a custom document template to be displayed in the **Available Templates** list, it must be created and customized as described in section [Managing Templates](#).

New CDP Replica Plan

Plan Info

Scope

Plan Type

VM Groups

VM Recovery Options

VM Steps

VM Credentials

RTO & RPO

Report Template

Report Scheduling

Summary

Choose the report template to be used for Plan reports and documentation

Type any part of name to filter

Available Templates

Veeam Default Template (DE)
Dieses Template ist ein Beispiel und sollte auf Ihre Bedürfnisse angepasst werden

Veeam Default Template
This is an example template, and should be cloned and customized to your requirements

Veeam Default Template (ES)
Esta es una plantilla de ejemplo, y debe ser clonada y personalizada de acuerdo con sus requisitos

Veeam Default Template (FR)
Ceci est un modèle qui doit être cloné et personnalisé selon vos besoins

Veeam Default Template (PT)
Este é um template de exemplo, e deve ser clonado e customizado de acordo com seus requerimentos

Veeam Default Template (CH)
这是一个示例模板，应进行复制并根据您的要求定制

Veeam Default Template (JP)
こちらはサンプル・テンプレートです。コピーして、要件に応じてカスタマイズしてください

Document format:

☒ PDF file

☐ Word document (.DOCX)

Back

Next

Cancel

159 | Veeam Disaster Recovery Orchestrator | Operations Guide

Step 10. Specify Report Scheduling Options

At the **Report Scheduling** step of the wizard, choose whether you want to automatically generate the [Plan Definition](#) and [Plan Readiness Check](#) reports for the plan on a daily schedule. You can also choose whether you want to generate both reports immediately after you create the plan.

To specify the exact time at which the report will be generated, click the **Schedule** icon next to the **Update Plan Definition report daily at** or **Perform Plan Readiness Check daily at** check box, set the desired time, and click **Apply**.

New CDP Replica Plan

Plan Info

Scope

Plan Type

VM Groups

VM Recovery Options

VM Steps

VM Credentials

RTO & RPO

Report Template

Report Scheduling

Summary

Choose scheduling options for automatic Plan reporting

☒ Update Plan Definition report daily at: 7:00 AM

☒ Perform Plan Readiness Check daily at: 9:40 AM

i Reports will not be generated for plan

☒ Create Plan Definition when I click Finish

☒ Perform Readiness Check when I click Finish

Hours: 9 Minutes: 40

☒ AM ☐ PM

Apply **Cancel**

Back **Next** **Cancel**

Step 11. Finish Working with Wizard

At the **Summary** step of the wizard, review configuration information and click **Finish**.

The screenshot shows the 'New CDP Replica Plan' wizard in the 'Summary' step. The left sidebar lists the steps: Plan Info, Scope, Plan Type, VM Groups, VM Recovery Options, VM Steps, VM Credentials, RTO & RPO, Report Template, Report Scheduling, and Summary (which is highlighted). The main area displays a summary of the configuration for the 'Test CDP Replica Plan'. At the bottom right, there are three buttons: 'Back', 'Finish', and 'Cancel'.

See below for a summary for the new Plan	
Copy to clipboard	
Plan Name:	Test CDP Replica Plan
Description:	Evaluating continuous data protection
Contact Name:	Hue Spenser
Contact Email:	hue.spenser@veeam.com
Contact Tel:	18005556677
Scope:	Admin Scope
Plan Type:	CDP Replica
VM Group(s):	Datastore - mk_vol_5 Datastore - mk_vol_9 owner - hue.spenser
Recover VMs:	Simultaneously (max 10)
If any VM fails:	Halt the plan
Steps for New VM Template:	Process CDP Replica VM Check VM Heartbeat Ping VM Network Start Service VM Power Actions
Override Credentials:	Yes, John Smith (TECH\john.smith)
Credentials:	John Smith (TECH\john.smith)
Target RTO:	1 Hour
Target RPO:	15 Seconds
Report Template, format:	Veeam Default Template, PDF
Update Plan Definition report:	Daily 7:00 AM
Perform Readiness Check:	Daily 9:40 AM
Create Plan Definition report now:	Yes
Run Readiness Check now:	Yes

Editing CDP Replica Plans

If you want to specify granular settings not provided in the [New Orchestration Plan wizard](#), the Orchestrator UI allows you to customize CDP replica plans and configure the settings for groups, recovered VMs, plan steps and step parameters.

The procedures to edit replica, CDP replica, restore, storage and cloud plans are almost identical. For more information, see [Editing Orchestration Plans](#).




Running and Scheduling CDP Replica Plans

After you create and configure a CDP replica plan, and run a successful [readiness check](#), the plan can be considered ready for failover. You can invoke various actions for the plan, depending on the current plan state.




Point in Time	Actions
New plan created	After plan creation, you can: <ul style="list-style-type: none">• Schedule a time for the plan to execute failover.• Run the plan to execute failover immediately.
Failover	After failover, you can: <ul style="list-style-type: none">• Perform permanent failover.• Fail back to the original or to a new location.
Failback	After failback, you can: <ul style="list-style-type: none">• Commit failback.
Any	At any point, you can: <ul style="list-style-type: none">• Halt the plan to interrupt its execution.• Undo to attempt reversal of the previous action.• Reset the plan to clear the current state and allow it to run again.

Plan States









CDP replica plans can acquire the following **default** states after creation. The same states are shown after resetting a plan and after completing a check.






Plan State	Icon	Description
NOT VERIFIED		Plan has never passed a readiness check or has been changed since the last readiness check.
		Plan has failed to pass a readiness check.
VERIFIED		Plan has successfully passed a readiness check.

CDP replica plans can acquire the following **stable** states after completing current processing:

Plan State	Icon	Description
HALTED		Plan has stopped due to either an error or user intervention.
FAILOVER		Process completed successfully.
UNDO FAILOVER		Process completed with one or more warnings.
PERMANENT FAILOVER		Process completed with one or more errors.
PREPARE FOR FAILBACK		
FAILBACK		
UNDO FAILBACK		
COMMIT FAILBACK		

CDP replica plans can acquire the following **active** states while in use or in progress:




Functionality	Tab	Plan Operator
Plan Management		
CREATING		Plan is being created.
EDITING		Plan is being edited.
SAVING		Plan is being saved. Note: Plan editing and execution are not available in this state.
RESETTING		Plan is being reset.
DELETING		Plan is being deleted.
Readiness Checks		
CHECKING		Plan readiness check is in progress.
		Plan readiness check is in progress; one or more warnings encountered.
		Plan readiness check is in progress; one or more errors encountered.

Functionality	Tab	Plan Operator
CHECK HALTING		Plan readiness check is halting.
Execution		
FAILOVER		Plan is executing.
		Plan is executing; one or more warnings encountered.
		Plan is executing; one or more errors encountered.
HALTING		Plan is halting.

NOTE

If you perform any infrastructure configuration changes (add, delete or rename VMs) or changes to Veeam ONE Client groups, Orchestrator will not automatically apply these changes to plans that are currently executing or testing – such plans are 'locked' and cannot be edited. The changes will take effect only if the plans enter the *VERIFIED* or *NOT VERIFIED* state.

CDP replica plans can acquire the following **modes**:

Plan Mode	Icon	Description
ENABLED		Plan is ready to be verified and executed. Notes: Plan editing is not available. Automatic report updates are enabled.
DISABLED		Plan is ready to be edited. Notes: Scheduled plan execution is not available. Automatic report updates are disabled.
IN USE		Plan is either in one of the active states (except the <i>EDITING</i> state) or in one of the stable states. Notes: Plan editing and disabling are not available. And automatic report updates are disabled.

TIP

When a plan is in an active state, you can switch to the **Plan Details** page, select a VM being recovered in the **Virtual Machines** column, and click the **VM Console** link to connect directly to the VM desktop.

Orchestrator will connect to the VM through the vCenter Server system. To avoid connection failures, make sure the following requirements are met:

1. The target vCenter Server that manages the VM is running VMware vCenter Server version 6.0 or later.
2. The SSL certificate used by the target vCenter Server is valid on the machine on which you are running the browser. If not, install root certificates from the vCenter Server on both the Orchestrator server and the machine. To learn how to download and install vCenter Server root certificates, see [this VMware KB article](#).

In vSphere 6.0 and later, each newly created ESXi host is by default provisioned with a self-signed certificate from the VMware Certificate Authority. If you want to use such a certificate when accessing the VM desktop, download the root CA certificate from the host where the VM is registered. To learn how to manage certificates for ESXi hosts, see [VMware Docs](#).

Before You Begin

To run a CDP replica plan, it must be *ENABLED*. To enable a plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan.
3. From the **Manage** menu, select **Enable**.

If you do not enable a plan before you run it, the [Run Plan](#) wizard will force you to do that as soon as you try running the plan.

NOTES

1. An Orchestrator Administrator or Plan Author can force-enable a plan in the **Run Plan** wizard. However, a Plan Operator will not be able to run a disabled CDP replica plan.
For more information on roles that can be assigned to users and user groups working with the Orchestrator UI, see [Managing Permissions](#).
2. For security purposes, all 'real-world' actions associated with CDP replica plans (such as failover and failback) require password confirmation.

Scheduling Failover

You can schedule a time for a CDP replica plan to execute. Only the failover process can be scheduled – all other operations (failback, undo failover and so on) must be performed manually in the Orchestrator UI.

To schedule a CDP replica plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Schedule**.
-OR-
Right-click the plan name and select **Launch > Schedule**.
3. Complete the **Schedule Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.

The screenshot shows the 'Schedule Plan' wizard with the 'Credentials' step selected. The wizard has a sidebar with 'Credentials', 'Schedule Options', and 'Summary'. The main area is titled 'Re-enter credentials to proceed' and contains two input fields: 'User name:' with the value 'tech\olivia.dias' and 'Password:' with masked characters. An information icon and message state: 'For the plan to run according to the specified schedule, the plan must be enabled.' At the bottom right are 'Next' and 'Cancel' buttons.

- b. At the **Schedule Options** step, set the **Scheduled execution** toggle to *On*, and choose whether you want to run the plan on schedule or after any other plan.
 - If you want to run the plan at a specific time, select the **Schedule on** option, click the **Schedule** icon, set the desired date and time, and click **Apply**.

- If you want to run the plan after another plan, select the **Schedule after** option and click **Choose a Plan**. Then, in the **Select Plan** window, select the necessary plan and click **OK**.

For a plan to be displayed in the **Available Plans** list, it must be *ENABLED* as described in section [Running and Scheduling CDP Replica Plans](#).

The screenshot shows the 'Schedule Plan' wizard with the 'Schedule Options' step selected. The left sidebar has 'Credentials', 'Schedule Options', and 'Summary'. The main area displays the following:

- Header: **You may schedule this Plan to run at a specific time, or chain it to be executed after another Plan runs**. Subtext: Recovery will be performed using the most recent restore point.
- Scheduled execution: ☒ On
- ☐ Schedule on: 11/16/2022 10:30 AM (with a calendar icon)
- ☒ Schedule after: [Test Replica Plan](#)
- Information icon (i): You can schedule only the Failover and Restore actions for Orchestration Plans. Other actions (such as Failback) must be performed manually.

At the bottom right are buttons: Back, Next, and Cancel.

- At the **Summary** step, review configuration information and click **Finish**.

The screenshot shows the 'Schedule Plan' wizard with the 'Summary' step selected. The left sidebar has 'Credentials', 'Schedule Options', and 'Summary'. The main area displays the following:

- Header: **Plan will be scheduled with below settings. Click Finish to apply**
- [Copy to clipboard](#) (with a clipboard icon)
- Plan name: CDP Plan
- Schedule: Enabled
- Ransomware Scan: Disabled
- Choose scheduling options: After Plan: Restore plan

At the bottom right are buttons: Back, Finish, and Cancel.

TIP

You can disable a configured schedule if you no longer need it. To do that, set the **Scheduled execution** toggle to *Off* at the **Schedule Options** step of the **Schedule Plan** wizard.

Running Failover

The **Run** action causes VMs in a plan to fail over to their replicas. For more information on the failover process, see the Veeam Backup & Replication User Guide, section [Failover](#).

To run a CDP replica plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Run**.
-OR-
Click the plan name to switch to the **Plan Details** page, and click **Run**.
3. Complete the **Run Plan** wizard:
 - a. [This step applies only if you have not enabled the plan before running it]

At the **Plan Disabled** step, select the **Enable this Plan** check box.

Run Plan [X]

Plan Disabled

This Plan is disabled
You may force the Plan into enabled mode to run it.

☒ Enable this Plan

Next Cancel

- b. For security purposes, at the **Credentials** step, retype your password.

The screenshot shows a 'Run Plan' dialog box with a sidebar on the left and a main content area on the right. The sidebar contains the following steps: 'Plan Disabled', 'Credentials' (highlighted in blue), 'Restore Point Type', 'Readiness Check', 'Restore Point', 'Chained Plans', and 'Summary'. The main content area is titled 'Re-enter credentials to proceed' and contains two input fields: 'User name' with the value 'tech\wendy.may' and 'Password' with masked characters. At the bottom right of the dialog are three buttons: 'Back', 'Next', and 'Cancel'.

- c. At the **Restore Point Type** step, choose whether you want to use a short-term or long-term restore point to recover VM replicas:
- Short-term restore points are replicated states that are created with the shortest RPO (several seconds or minutes) and stored according to the short-term retention settings (no longer than several hours).

- Long-term restore points are restore points that are created with a longer RPO (several hours) and stored according to the long-term retention settings (up to several days). Depending on the specified CDP policy settings, long-term restore points can be application-consistent and crash-consistent.

For more information on CDP retention policies, see the Veeam Backup & Replication User Guide, section [Creating CDP Policies](#).

Run Plan [X]

Plan Disabled

Credentials

Restore Point Type

Readiness Check

Restore Point

Chained Plans

Summary

Choose restore point type

☒ Use short-term restore points
Shortest RPO (minutes or seconds). Not application-aware.

☐ Use long-term restore points
Longer RPO (hours). May be application-aware, depending on the CDP policy settings.

[Back](#) [Next](#) [Cancel](#)

- d. At the **Readiness Check** step, review the results of the most recent readiness check run for the plan to make sure the plan will be able to complete successfully.

The screenshot shows the 'Run Plan' dialog box with the 'Readiness Check' step selected in the left sidebar. The main area is titled 'Review readiness check report'. It contains a 'Copy to clipboard' button, execution details (Executed: 11/17/2022 7:41 AM, Result: Warning, Details: 0 Errors, 1 Warning), and a 'Download report' button. A warning icon and message state: 'It is highly recommended to run a readiness check before executing a plan.' At the bottom are 'Back', 'Next', and 'Cancel' buttons.

Run Plan	
<ul style="list-style-type: none">Plan DisabledCredentialsRestore Point TypeReadiness CheckRestore PointChained PlansSummary	Review readiness check report
	Copy to clipboard
	Executed: 11/17/2022 7:41 AM
	Result: Warning
	Details: 0 Errors, 1 Warning
	Download report
	It is highly recommended to run a readiness check before executing a plan.
<div>BackNextCancel</div>	

- e. At the **Restore Point** step, choose a restore point that will be used to recover VM replicas.

The screenshot shows the 'Run Plan' dialog box with the 'Restore Point' step selected in the left sidebar. The main area is titled 'Choose restore point'. It contains two radio button options: 'Use the latest Restore Point' (selected) and 'Use most recent Restore Point before: 11/17/2022 7:56 AM' (with a calendar icon). At the bottom are 'Back', 'Next', and 'Cancel' buttons.

Run Plan		
<ul style="list-style-type: none">Plan DisabledCredentialsRestore Point TypeReadiness CheckRestore PointChained PlansSummary	Choose restore point	
	<input checked="" type="radio"/> Use the latest Restore Point	
	<input type="radio"/> Use most recent Restore Point before: 11/17/2022 7:56 AM	
<div>BackNextCancel</div>		

- f. [This step applies only if you have any other orchestration plans scheduled to run after the plan completes]

At the **Chained Plans** step, select the **Also execute the chained plans** check box to proceed to execution of subsequent plans after the current plan enters the *FAILOVER* state.

The screenshot shows the 'Run Plan' dialog box with the 'Chained Plans' step selected in the left sidebar. The main content area displays the message 'This Plan is part of a chain, and other Plans will execute when it is complete.' Below this, the checkbox 'Also execute the chained plans' is checked. A warning icon and text state: 'Even Plans which are disabled will be forced to run. All Plans will all use the same restore point option.' The bottom of the dialog features 'Back', 'Next', and 'Cancel' buttons.

- g. At the **Summary** step, review configuration information and click **Finish**.

The screenshot shows the 'Run Plan' dialog box with the 'Summary' step selected in the left sidebar. The main content area displays the message 'Click Finish to run the plan' and a 'Copy to clipboard' button. Below this, a list of configuration details is shown:

Plan name:	CDP Plan
Launched by:	tech\olivia.dias [Administrator]
Current state:	Not Verified (Failed check)
Action:	Failover
Restore Point Type:	Short-term
Restore Point:	Most Recent
Chained Plans:	Execute
Recovery Location:	-
Restore VM Tags:	No

The bottom of the dialog features 'Back', 'Finish', and 'Cancel' buttons.

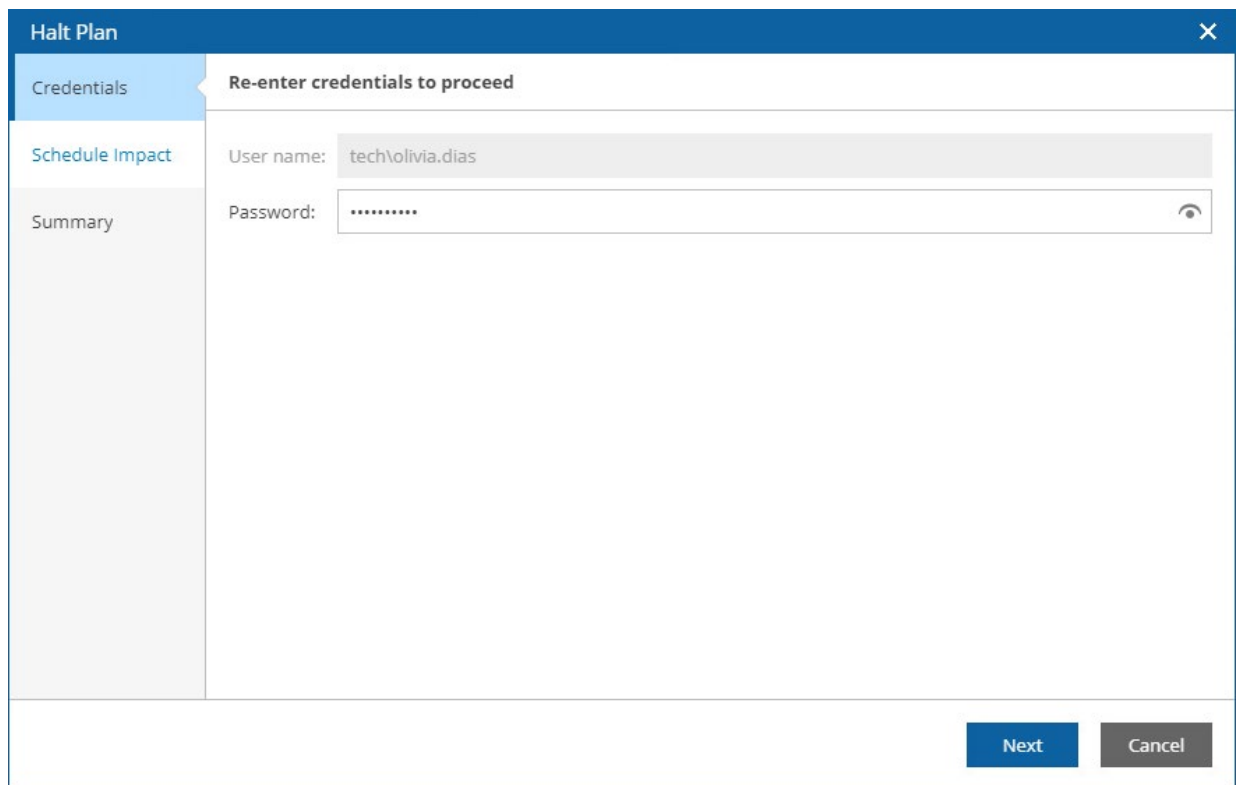
The plan goal is to reach the *FAILOVER* state. If any critical error is encountered, the plan will stop with the *HALTED* state. To learn how to work with *HALTED* CDP replica plans, see [Managing Halted Plans](#).

Halting Failover

The **Halt** action interrupts plan execution. Any steps currently executing will be completed, then the plan will enter the *HALTED* state. To learn how to work with *HALTED* CDP replica plans, see [Managing Halted Plans](#).

To stop a running CDP replica plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Halt**.
-OR-
Click the plan name to switch to the **Plan Details** page, and click **Halt**.
3. Complete the **Halt Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.



The screenshot shows a 'Halt Plan' dialog box with a dark blue header and a close button (X) in the top right corner. On the left is a vertical sidebar with three tabs: 'Credentials' (highlighted in blue), 'Schedule Impact', and 'Summary'. The main area of the dialog is titled 'Re-enter credentials to proceed'. It contains two input fields: 'User name:' with the text 'tech\olivia.dias' and 'Password:' with masked characters '.....'. A small eye icon is visible to the right of the password field. At the bottom right, there are two buttons: 'Next' (blue) and 'Cancel' (grey).

- b. [This step applies only if you have any other orchestration plans scheduled to run after the plan completes]

At the **Schedule Impact** step, choose whether you want to proceed with or cancel execution of subsequent plans after the current plan enters the *HALTED* state.

The screenshot shows the 'Halt Plan' dialog box with the 'Schedule Impact' tab selected. The left sidebar contains 'Credentials', 'Schedule Impact', and 'Summary'. The main area has two radio buttons: 'Cancel the schedule and do not execute the subsequent Plans' (selected) and 'Continue the schedule and launch the next Plan now'. Below these is a warning icon and text: 'There are other Plan(s) scheduled in a chain to failover after this Plan completes. Choose the options for those scheduled Plans below.' At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

- c. At the **Summary** step, review configuration information and click **Finish**.

The screenshot shows the 'Halt Plan' dialog box with the 'Summary' tab selected. The left sidebar contains 'Credentials', 'Schedule Impact', and 'Summary'. The main area has a header 'Click Finish to halt the plan' and a 'Copy to clipboard' button. Below is a table of configuration information:

Plan name:	Replica Plan
Halted by:	tech\olivia.dias [Administrator]
Current state:	✓ Failover
Action:	Halt
Schedule Impact:	Restore Plan – Scheduled chain cancelled

Below the table is an information icon and text: 'Halting a plan before it reaches a stable state may cause your environment to enter an inconsistent state, requiring manual troubleshooting and a reset of the plan to resolve.' At the bottom right are 'Back', 'Finish', and 'Cancel' buttons.

Finalizing Failover

Orchestrator provides you a number of options to finalize failover to VM replicas:

- **Permanent Failover** — as a result, VM replicas in the disaster recovery site will no longer be treated as replicas. Restore point snapshots will be deleted, and the source VMs will be removed from CDP policies.

For more information on the permanent failover process, see the Veeam Backup & Replication User Guide, section [Permanent Failover](#).

- **Failback** — you can choose whether you want to fail back to the original or to a new location.
 - If failing back to the original location, you will switch from VM replicas back to the source VMs. The source VMs will be restored to the current state of their replicas.
 - If failing back to a new location, all VM replica files will be transported to the location and used to recover the VMs there.

Failback is a temporary stage that must be further finalized. After confirming that the failed-back VMs operate correctly, you can perform the **Commit failback** operation. Alternatively, [undo failback](#) to return the plan back to the *FAILOVER* state.

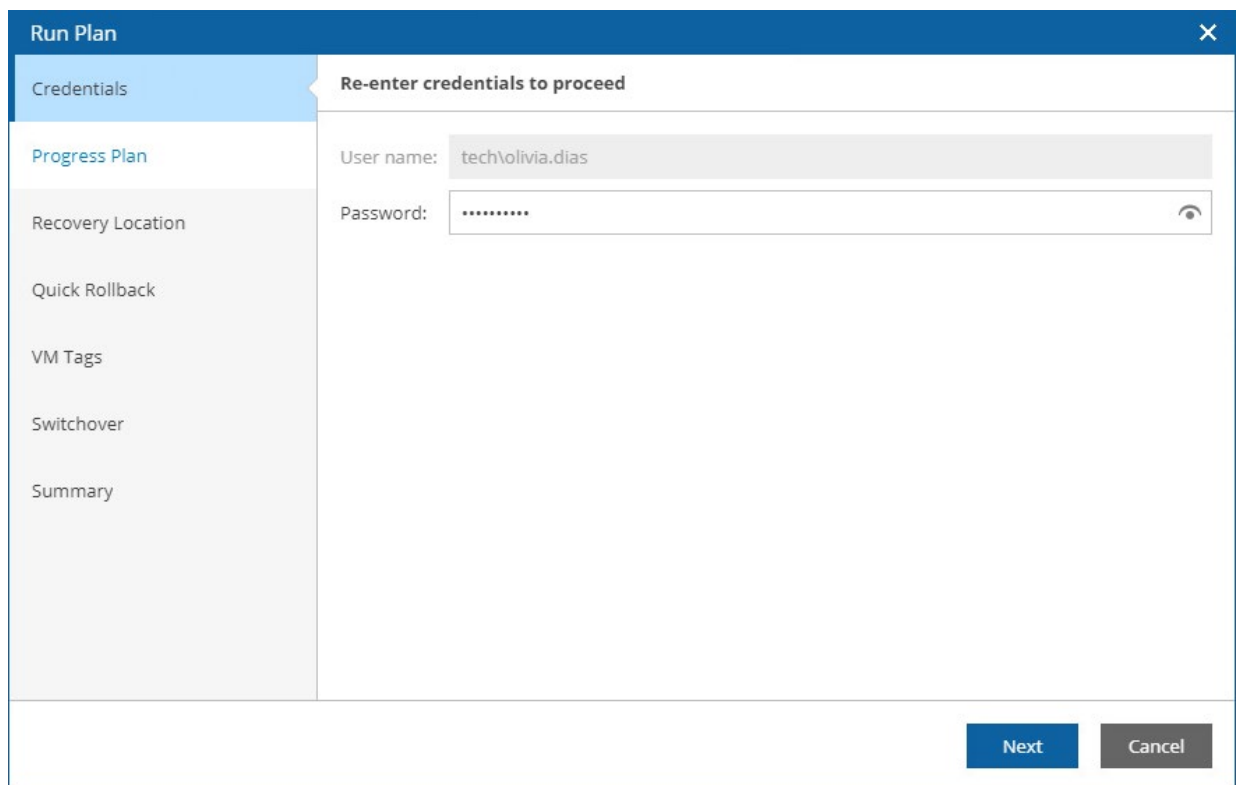
For more information on the replica failback process, see the Veeam Backup & Replication User Guide, sections [Failback](#) and [Commit Failback](#).

Depending on the selected option, the plan may enter the *PERMANENT FAILOVER*, *FAILBACK*, *COMMIT FAILBACK* or *HALTED* state. To learn how to work with *HALTED* CDP replica plans, see [Managing Halted Plans](#).

Running Permanent Failover

To perform permanent failover for a plan in the *FAILOVER* state:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Continue**.
-OR-
Click the plan name to switch to the **Plan Details** page, and click **Continue**.
3. Complete the **Run Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.



The screenshot shows the 'Run Plan' wizard window. The left sidebar contains the following steps: 'Credentials' (highlighted in blue), 'Progress Plan', 'Recovery Location', 'Quick Rollback', 'VM Tags', 'Switchover', and 'Summary'. The main area is titled 'Re-enter credentials to proceed' and contains two input fields: 'User name:' with the value 'tech\olivia.dias' and 'Password:' with masked characters '*****'. A toggle icon (an eye) is visible next to the password field. At the bottom right, there are two buttons: 'Next' (blue) and 'Cancel' (gray).

b. At the **Progress Plan** step, select the **Permanent failover** option.

The screenshot shows the 'Run Plan' dialog box with the 'Progress Plan' step selected in the left sidebar. The main area is titled 'Choose one of the following options' and contains two radio button options: 'Failback / Prepare to failback' and 'Permanent failover'. The 'Permanent failover' option is selected. Below the options is an information icon and a message: 'After permanent failover completes, undo and failback options will not be available.' At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

c. At the **Summary** step, review configuration information and click **Finish**.

The screenshot shows the 'Run Plan' dialog box with the 'Summary' step selected in the left sidebar. The main area is titled 'Click Finish to run the plan' and contains a 'Copy to clipboard' link. Below this, the following configuration information is displayed:

Plan name:	CDP Plan
Launched by:	tech\olivia.dias [Administrator]
Current state:	✔ Failover (Complete, no errors, no warnings)
Action:	Failover – Permanent

At the bottom right, there are three buttons: 'Back', 'Finish', and 'Cancel'.

NOTE

Failback will no longer be an option once the permanent failover process is complete.

Running Failback

To start failback for a plan in the *FAILOVER* state:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Continue**.
-OR-
Click the plan name to switch to the **Plan Details** page, and click **Continue**.
3. Complete the **Run Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.

The screenshot shows the 'Run Plan' wizard window. The left sidebar contains the following steps: 'Credentials' (highlighted in blue), 'Progress Plan' (in blue text), 'Recovery Location', 'Quick Rollback', 'VM Tags', 'Switchover', and 'Summary'. The main area is titled 'Re-enter credentials to proceed' and contains two input fields: 'User name:' with the value 'tech\olivia.dias' and 'Password:' with masked characters '*****'. A toggle icon is visible next to the password field. At the bottom right, there are 'Next' and 'Cancel' buttons.

- b. At the **Progress Plan** step, select the **Failback / Prepare to failback** option.

The screenshot shows the 'Run Plan' dialog box. On the left, a sidebar lists steps: Credentials, Progress Plan (highlighted), Recovery Location, Quick Rollback, VM Tags, Switchover, and Summary. The main panel is titled 'Choose one of the following options' and contains two radio buttons. The first radio button, labeled 'Failback / Prepare to failback', is selected. The second radio button is labeled 'Permanent failover'. Below these options is an information icon (i) followed by the text: 'Failback to the original location or to a new location, or synchronize disks to prepare for failback later.' At the bottom right of the dialog are three buttons: 'Back', 'Next', and 'Cancel'.

- c. At the **Recovery Location** step, select a location to which VMs will be recovered.

For a recovery location to be displayed in the list of available locations, it must be created and included into the list of inventory items available for the scope, as described in section [Managing Recovery Locations](#).

NOTE

Orchestrator will perform failback using all [settings configured for the location](#) — except Instant VM Recovery and backup copy preference. These settings are not applicable to failback operations.

Run Plan

Credentials

Progress Plan

Recovery Location

Quick Rollback

VM Tags

Switchover

Summary

Choose recovery location

Selecting the original VM location will fail back to the source VMs. Using any other recovery location will create new VMs.

Type any part of name to filter

Name	VMs	Agents	Instant VM Reco...
Original VM Location	Enabled	Disabled	Enabled
Restore Recovery Location	Enabled	Enabled	Enabled

Back

Next

Cancel

If you want to fail back to a new recovery location and the selected location includes multiple hosts, datastores and networks, Orchestrator will use the round-robin algorithm to recover VMs. For more information, see [How Orchestrator Places VMs During Failback](#).

d. [This step applies only if you have selected the Original VM Location]

At the **Quick Rollback** step, you can choose whether you want to instruct Orchestrator to synchronize changed data blocks only – this may help you speed up the failback process significantly.

180 | Veeam Disaster Recovery Orchestrator | Operations Guide

For more information on the quick rollback process, see the Veeam Backup & Replication User Guide, section [Quick Rollback](#).

The screenshot shows the 'Run Plan' dialog box with the 'Quick Rollback' step selected in the left sidebar. The main area is titled 'Choose quick rollback option'. It contains a checked checkbox labeled 'Use quick rollback'. Below this is an information box with an 'i' icon and the text: 'Quick rollback is appropriate if failover was caused by a software problem or user error. Do not use this option if the failover was caused by a hardware problem, storage issue, or power loss.' At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

- e. At the **VM Tags** step, choose whether you want the recovered VMs to have the same tags as the source VMs.

The screenshot shows the 'Run Plan' dialog box with the 'VM Tags' step selected in the left sidebar. The main area is titled 'Choose whether to restore VM tags'. It contains a checked checkbox labeled 'Restore VM tags'. At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

- f. At the **Switchover** step, choose whether you want to switch from VM replicas to the source VMs immediately or to synchronize the VM disks without actually performing failback.

If you select the **Prepare for failback** option, Orchestrator will switch from VM replicas to the source VMs when you run the plan next time.

The screenshot shows the 'Run Plan' dialog box with the 'Switchover' step selected in the left sidebar. The main area is titled 'Choose when to perform replica switchover'. It contains two radio button options: 'Failback now' (selected) with the subtext 'Switchover replicas immediately', and 'Prepare for failback' with the subtext 'Switchover replicas on next plan run'. Below these options is an information icon (i) and a message: 'This option will synchronize VM disks then trigger failback immediately.' At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

- g. At the **Summary** step, review configuration information and click **Finish**.

The screenshot shows the 'Run Plan' dialog box with the 'Summary' step selected in the left sidebar. The main area is titled 'Click Finish to run failback'. It features a 'Copy to clipboard' button with a document icon. Below this is a list of configuration details: Plan name: CDP Plan; Launched by: tech\olivia.dias [Administrator]; Current state: ✔ Failover (Complete, no errors, no warnings); Action: Failback to Production; Recovery Location: Original VM Location; Restore VM Tags: Yes; Quick Rollback: Yes; Switchover: Failback now. At the bottom right, there are three buttons: 'Back', 'Finish', and 'Cancel'.

How Orchestrator Places VMs During Failback

To fail back VMs included into a CDP replica plan to a new recovery location, Orchestrator uses the following algorithm:

1. The solution looks through all hosts added to the location as [compute resources](#) to detect the first available host. This is the host where the first processed VM will be registered.
2. Orchestrator applies the mapping specified in the [network mapping table](#) for the location to set the required network configuration of the recovered VM.

Orchestrator checks whether the network configuration of the detected host matches the required network configuration. If these configurations do not match, Orchestrator goes back to step 1.

3. In the list of datastores connected to the host as [storage resources](#), Orchestrator searches for the first datastore that both is available and has enough capacity. This is the datastore where files of the VM will be stored.

To calculate the datastore capacity and make sure that it has enough space to accommodate the recovered VM, Orchestrator uses the threshold that you specify [when creating or configuring the location](#).

NOTE

The failure of steps 1–3 for a VM from a [critical inventory group](#) halts the plan in the following cases:

- If none of the discovered hosts is available, or if none of the hosts has network configuration that matches the required network configuration of the recovered VM.
- If none of the discovered datastores is available, or if none of the datastores meets the capacity requirements.

To learn how to work with *HALTED* CDP replica plans, see [Managing Halted Plans](#).

4. When Orchestrator starts processing the next VM, the solution looks through all hosts added to the location as compute resources to detect the next available host:
 - If Orchestrator detects such a host, this is the host where the VM will be registered.
 - If there are no more available hosts, Orchestrator uses the host detected at step 1 to register the VM.

Then, Orchestrator goes through steps 2–3 to detect the target network and datastore for the VM.

5. Orchestrator repeats step 4 for all other VMs included in the plan until all the VMs are recovered. The order in which the VMs are processed depends on the **VM Recovery Options** defined [while configuring the plan](#).

If datastores added to the recovery location as storage resources breach the capacity threshold before all the VMs are recovered, the failure of this step for a VM from a critical inventory group halts the plan. To troubleshoot the issue, configure the location to add more datastores and try running the halted plan again. To learn how to work with *HALTED* CDP replica plans, see [Managing Halted Plans](#).

Committing Failback

To commit failback for a plan in the *FAILBACK* state:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Continue**.
-OR-
Click the plan name to switch to the **Plan Details** page, and click **Continue**.
3. Complete the **Run Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.

The screenshot shows a 'Run Plan' dialog box with a dark blue header and a close button (X) in the top right corner. The dialog is divided into two main sections. On the left is a sidebar with two tabs: 'Credentials' (which is selected and highlighted in light blue) and 'Summary'. The 'Summary' tab is currently inactive. The main area on the right is titled 'Re-enter credentials to proceed'. It contains two input fields: 'User name:' with the text 'tech\wendy.may' and 'Password:' with a masked password represented by ten dots. To the right of the password field is a small eye icon for toggling visibility. At the bottom right of the dialog, there are two buttons: a blue 'Next' button and a grey 'Cancel' button.

b. At the **Summary** step, review configuration information and click **Finish**.

The screenshot shows the 'Run Plan' dialog box with the 'Summary' tab selected. The dialog contains the following information:

Click Finish to commit failback	
Copy to clipboard	
Plan name:	CDP Plan
Launched by:	tech\olivia.dias [Administrator]
Current state:	✔ Failback (Complete, no errors, no warnings)
Action:	Commit Failback
Recovery Location:	-
Restore VM Tags:	No

At the bottom, there is an information icon and a note: "Commit failback only updates the configuration of the jobs and replicas in the Veeam Backup & Replication server. It takes no action in the virtual infrastructure." Below the dialog, there are three buttons: 'Back', 'Finish' (highlighted in blue), and 'Cancel'.

TIP

After the commit failback process completes, Orchestrator will leave the plan in the *IN USE* state. By design, this makes the results of the commit failback process accessible in the Orchestrator UI as long as required, and also prevents the plan from being modified by any automatic updates related to infrastructure changes.

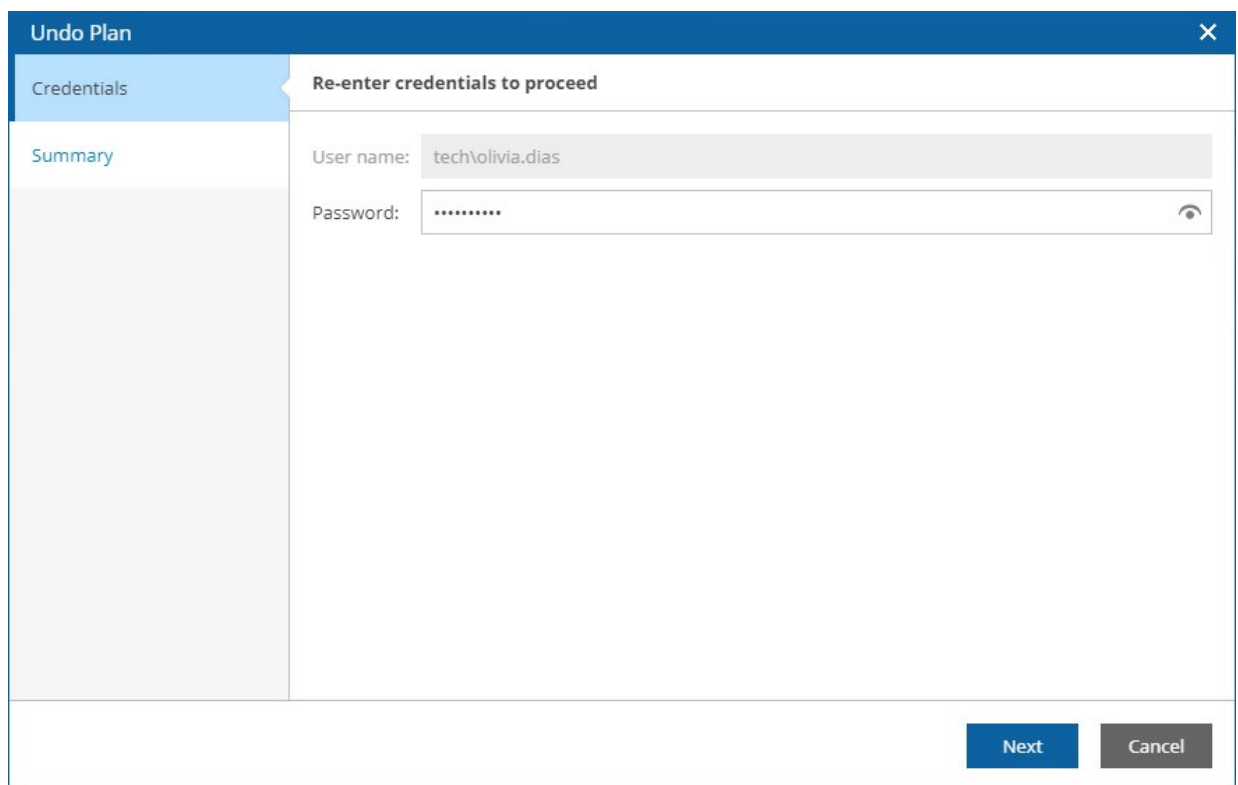
If you want to perform any further actions with the plan (for example, to test the plan, to run readiness checks or to execute the plan again), reset the plan as described in section [Resetting CDP Replica Plans](#).

Undoing Failover

The **Undo Failover** action powers off VM replicas running on target hosts and roll back to the VM state before failover. For more information on the undo failover operation, see the Veeam Backup & Replication User Guide, section [Undo Failover](#).

To perform an undo operation for a plan in the *FAILOVER* state:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Undo**.
-OR-
Click the plan name to switch to the **Plan Details** page, and click **Undo**.
3. Complete the **Undo Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.



The screenshot shows the 'Undo Plan' wizard window. The title bar is blue with the text 'Undo Plan' and a close button. The window is divided into two main sections. On the left is a sidebar with two tabs: 'Credentials' (selected, highlighted in blue) and 'Summary'. The main area on the right is titled 'Re-enter credentials to proceed'. It contains two input fields: 'User name:' with the text 'tech\olivia.dias' and 'Password:' with a masked password '*****'. There is a small eye icon to the right of the password field. At the bottom right of the window are two buttons: 'Next' (blue) and 'Cancel' (gray).

b. At the **Summary** step, review configuration information and click **Finish**.

Undo Plan [X]

Credentials

Summary

Click **Finish** to undo the most recent steps

Copy to clipboard

Plan name: CDP Plan

Undo by: TECH\olivia.dias [Administrator]

Current state: Failover (Halted, 83% complete, 1 error, no warnings)

Undo action: Undo Failover

i Undo will attempt to revert the plan to the last stable state.
After undo is initiated:

- The run control will be disabled until the undo process has completed.
- The halt control may be used to halt the undo process.
- After halting use the undo control to resume the undo process.

During undo any errors will be ignored.

Back Finish Cancel

If the undo failover process encounters an error while being performed, it will not be halted automatically – the plan will proceed until the process completes. To terminate the undo failover process manually, use the **Halt** option to stop the currently running plan as described in section [Halting Failover](#). To resume the undo failover process again, use the **Undo** option.

Undoing Failback

The **Undo Failback** action powers on VM replicas running on target hosts and switches from the production VMs back to the VM replicas – as a result, the plan acquires the *FAILOVER* state. For more information on the undo failback operation, see the Veeam Backup & Replication User Guide, section [Undo Failback](#).

To perform an undo operation for a plan in the *PREPARE FOR FAILBACK* or *FAILBACK* state:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Undo**.
-OR-
Click the plan name to switch to the **Plan Details** page, and click **Undo**.
3. Complete the **Undo Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.

The screenshot shows a window titled "Undo Plan" with a close button (X) in the top right corner. The window has a left sidebar with two tabs: "Credentials" (selected) and "Summary". The main area is titled "Re-enter credentials to proceed" and contains two input fields: "User name:" with the text "tech\wendy.may" and "Password:" with masked characters "*****". A small eye icon is visible to the right of the password field. At the bottom right, there are two buttons: "Next" (blue) and "Cancel" (gray).

b. At the **Summary** step, review configuration information and click **Finish**.

Undo Plan [X]

Credentials

Summary

Click **Finish** to undo the most recent steps

Copy to clipboard

Plan name: CDP Plan

Undo by: tech\olivia.dias [Administrator]

Current state: Failback (Complete, no errors, no warnings)

Undo action: Undo Failback

Undo will attempt to revert the plan to the last stable state. After undo is initiated:

- The run control will be disabled until the undo process has completed.
- The halt control may be used to halt the undo process.
- After halting use the undo control to resume the undo process.

During undo any errors will be ignored.

Back Finish Cancel

If the undo failback process encounters an error while being performed, it will not be halted automatically – the plan will proceed until the process completes. To terminate the undo failback process manually, use the **Halt** option to stop the currently running plan as described in section [Halting Failover](#). To resume the undo failback process again, use the **Undo** option.

Resetting CDP Replica Plans

If a CDP replica plan becomes inconsistent with the virtual environment, you can reset the plan. This will return the plan to the *DISABLED* state, without making any changes to the external virtual infrastructure.

To reset a CDP replica plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Manage** menu, select **Reset**.
-OR-
Right-click the plan name and select **Manage > Reset**.
3. Complete the **Reset Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.

The screenshot shows the 'Reset Plan' wizard window. The left sidebar contains three tabs: 'Credentials' (selected), 'Quick Check', and 'Summary'. The main area is titled 'Re-enter credentials to proceed'. It contains two input fields: 'User name' with the value 'tech\olivia.dias' and 'Password' with masked characters '*****'. A blue information icon is next to a warning message: 'Reset will take no actions on VMs or replicas in your infrastructure. It will reinitialize the Plan in Orchestrator only. For *Halted* plans it is recommended to use Undo, not Reset.' At the bottom right, there are 'Next' and 'Cancel' buttons.

- b. At the **Quick Check** step, select the **Perform a Quick Check after reset is complete** check box to run a **readiness check** after the reset.

The screenshot shows the 'Reset Plan' dialog box with the 'Quick Check' tab selected. The left sidebar contains 'Credentials', 'Quick Check', and 'Summary'. The main area displays the message 'It is recommended to run a Quick Check after resetting the plan' and a checked checkbox for 'Perform a Quick Check after reset is complete'. At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

Reset Plan	
Credentials	It is recommended to run a Quick Check after resetting the plan
Quick Check	<input checked="" type="checkbox"/> Perform a Quick Check after reset is complete
Summary	

Back Next Cancel

- c. At the **Summary** step, review configuration information and click **Finish**.

The screenshot shows the 'Reset Plan' dialog box with the 'Summary' tab selected. The left sidebar contains 'Credentials', 'Quick Check', and 'Summary'. The main area displays the message 'Plan will be reset using the options below. Press Finish to reset the Plan' and a 'Copy to clipboard' link. Below this, the following configuration information is listed: Plan Name: CDP Plan, Reset by: TECH\olivia.dias [Administrator], Current State: - Failover (Halted, 83% complete, 1 error, no warnings), and Quick Check: Yes. At the bottom right are 'Back', 'Finish', and 'Cancel' buttons.

Reset Plan	
Credentials	Plan will be reset using the options below. Press Finish to reset the Plan
Quick Check	Copy to clipboard
Summary	Plan Name: CDP Plan Reset by: TECH\olivia.dias [Administrator] Current State: - Failover (Halted, 83% complete, 1 error, no warnings) Quick Check: Yes

Back Finish Cancel

Managing Halted CDP Replica Plans

If a critical step fails for a VM from a [critical inventory group](#), the plan may enter the *HALTED* state. To troubleshoot reasons why a plan failed, use the **Plan Execution Report** generated as soon as the currently performed action completes. For more information on how to track plan performance history, see [Viewing Plan Execution History](#).

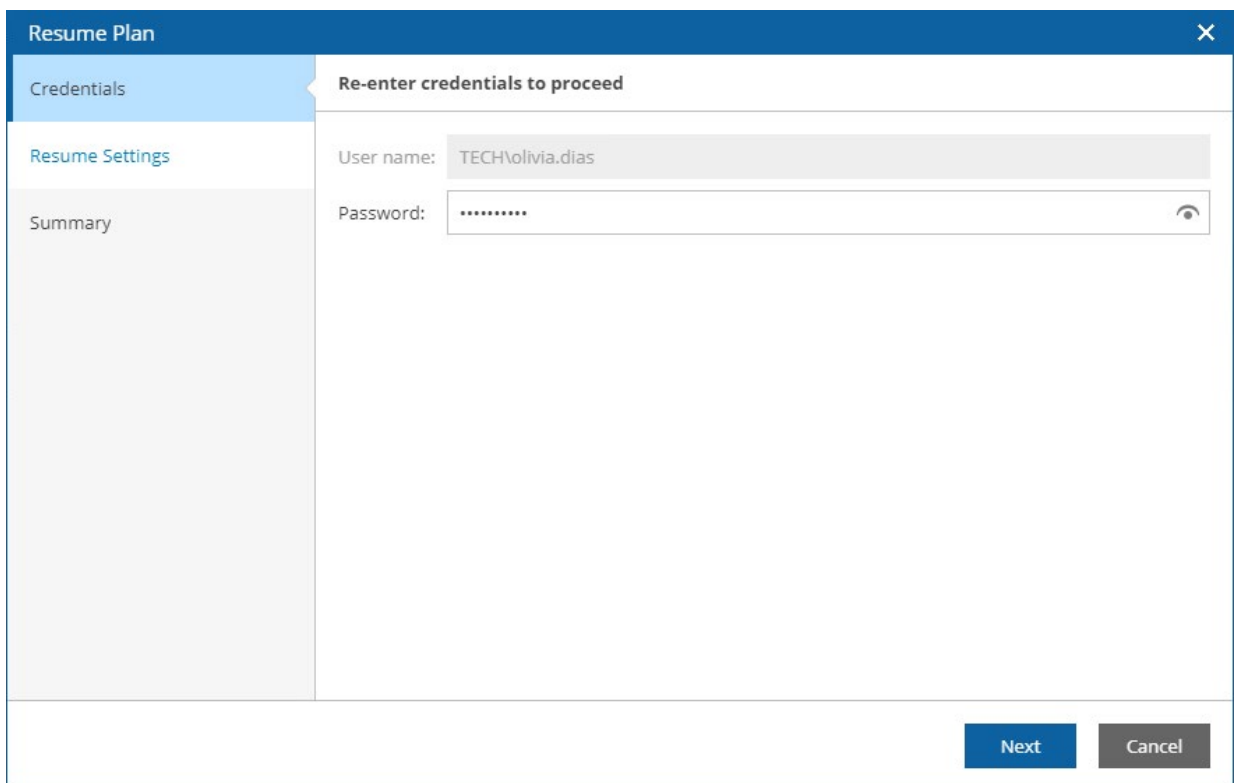
After you eliminate the problem that caused the plan to become *HALTED*, you have the following options to resume the plan:

- Repeat the last failed step.
- Proceed to the next step.

Running Halted CDP Replica Plans

To run a *HALTED* CDP replica plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Continue**.
-OR-
Click the plan name to switch to the **Plan Details** page, and click **Continue**.
3. Complete the **Run Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.



The screenshot shows a 'Resume Plan' dialog box with a close button (X) in the top right corner. On the left is a sidebar with three tabs: 'Credentials' (selected and highlighted in blue), 'Resume Settings', and 'Summary'. The main area is titled 'Re-enter credentials to proceed' and contains two input fields: 'User name:' with the text 'TECH\volivia.dias' and 'Password:' with masked characters '*****'. A small eye icon is visible to the right of the password field. At the bottom right, there are two buttons: 'Next' (blue) and 'Cancel' (grey).

- b. At the **Resume Settings** step, select an option to resume plan execution.

Choose whether you want to proceed with plan execution from the next plan step or to retry the failed step.

The screenshot shows the 'Resume Plan' dialog box with the 'Resume Settings' step selected in the left sidebar. The main area is titled 'Choose one of the following options' and contains two radio button options: 'Retry failed step' (selected) and 'Proceed to next step'. Below the options is an information box stating: 'If VMs are being processed in parallel, then multiple failed steps may be retried.' At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

Resume Plan	
Credentials	Choose one of the following options
Resume Settings	<input checked="" type="radio"/> Retry failed step If the most recently executed step failed, it will be retried
Summary	<input type="radio"/> Proceed to next step The plan will proceed to the next step
	i If VMs are being processed in parallel, then multiple failed steps may be retried.
<div>Back Next Cancel</div>	

- c. At the **Summary** step, review configuration information and click **Finish**. The failover process will be started.

The screenshot shows the 'Resume Plan' dialog box with the 'Summary' step selected in the left sidebar. The main area is titled 'Click Finish to resume the plan' and contains a 'Copy to clipboard' link and a list of configuration details: Plan name: CDP Plan, Launched by: TECH\olivia.dias [Administrator], Current state: Failover (Halted, 83% complete, 1 error, no warnings), Action: Resume – Failover, Resume by: Retry failed Step, Recovery Location: –, and Restore VM Tags: No. At the bottom right are 'Back', 'Finish', and 'Cancel' buttons.

Resume Plan	
Credentials	Click Finish to resume the plan
Resume Settings	Copy to clipboard
Summary	Plan name: CDP Plan Launched by: TECH\olivia.dias [Administrator] Current state: - Failover (Halted, 83% complete, 1 error, no warnings) Action: Resume – Failover Resume by: Retry failed Step Recovery Location: – Restore VM Tags: No
<div>Back Finish Cancel</div>	

Undoing Halted CDP Replica Plans

To perform an undo operation for a *HALTED* CDP replica plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Undo**.
-OR-
Click the plan name to switch to the **Plan Details** page, and click **Undo**.
3. Complete the **Undo Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.

The screenshot shows a window titled "Undo Plan" with a close button (X) in the top right corner. The window is divided into two main sections. On the left is a sidebar with two tabs: "Credentials" (which is selected and highlighted in blue) and "Summary". The "Summary" tab is currently inactive. The main area of the window is titled "Re-enter credentials to proceed". It contains two input fields: "User name:" with the text "tech\olivia.dias" entered, and "Password:" with a masked password "*****" and a toggle icon (an eye) to the right. At the bottom right of the window, there are two buttons: "Next" (in blue) and "Cancel" (in grey).

- b. At the **Summary** step, review configuration information and click **Finish**. The failover process will be started.

Undo Plan

Credentials

Summary

Click **Finish** to undo the most recent steps

Copy to clipboard

Plan name: CDP Plan

Undo by: tech\olivia.dias [Administrator]

Current state: Failover (Halted, 15% complete, 10 errors, 1 warning)

Undo action: Undo Failover

i Undo will attempt to revert the plan to the last stable state. After undo is initiated:

- The run control will be disabled until the undo process has completed.
- The halt control may be used to halt the undo process.
- After halting use the undo control to resume the undo process.

During undo any errors will be ignored.

Back Finish Cancel

If a plan repeatedly enters the *HALTED* state due to misconfiguration or changes in the external environment, the only option left may be to **RESET** the plan.

Resetting Halted CDP Replica Plans

To reset a *HALTED* CDP replica plan, follow the instructions provided in section [Resetting CDP Replica Plans](#).

NOTE

When you reset a CDP replica plan, Orchestrator returns it to the *DISABLED* state without making any changes to the external virtual infrastructure. You may need to deal with any infrastructure reconfiguration manually.

Working with Restore Plans

The type of an orchestration plan you create depends on whether you intend to use Orchestrator to switch to VM replicas, to restore machines from backups or backup copies, or to serve data from a destination (NetApp) or secondary (HPE) volume in case a disaster strikes.

If you want to recover machines from vSphere and Veeam agent backups to a VMware vSphere environment, create a restore plan.

Creating Restore Plans

To create a restore plan:

1. Navigate to **Orchestration Plans**.
2. Click **Manage > New**.
3. Complete the **New Orchestration Plan** wizard:
 - a. [Specify a plan name and description](#).
 - b. [Choose a scope for the plan](#).
 - c. [Choose a type of the plan](#).
 - d. [Select a recovery location for the plan](#).
 - e. [Include inventory groups in the plan](#).
 - f. [Specify VM recovery options](#).
 - g. [Add steps to the plan](#).
 - h. [Specify credentials for the plan steps](#).
 - i. [Specify VM protection options](#).
 - j. [Specify the target RTO and RPO](#).
 - k. [Select a template for plan reports](#).
 - l. [Specify scheduling options for plan reports](#).
 - m. [Finish working with the wizard](#).

Step 1. Specify Plan Name and Description

At the **Plan Info** step of the wizard, use the **Plan Name** and **Description** fields to enter a name for the new plan and to provide a description for future reference. The maximum length of the plan name is 64 characters; the following characters are not supported: * : / \ ? " < > | .

You can also provide a contact name, email and telephone number of a person responsible for the plan.

New Orchestration Plan

Plan Info

Scope

Plan Type

Recovery Location

VM Groups

VM Recovery Options

VM Steps

RTO & RPO

Report Template

Report Scheduling

Summary

Provide details for the new Orchestration Plan

Plan Name:

Test Restore Plan

Description:

Orchestrating restore

Contact Name:

Chloe Lewis

Contact Email:

chloe.lewis@veeam.com

Contact Tel:

18003334455

Next

Cancel

Step 2. Choose Plan Scope

At the **Scope** step of the wizard, select a scope for which you want to create the plan.

For a scope to be displayed in the **Available Scopes** list, it must be created and customized as described in section [Managing Permissions](#).

New Orchestration Plan

Plan Info

Scope

Plan Type

Recovery Location

VM Groups

VM Recovery Options

VM Steps

RTO & RPO

Report Template

Report Scheduling

Summary

Choose a Scope

Type any part of Scope name to filter

Available Scopes

Admin Scope

Exchange Administrators

SQL Administrators

Back

Next

Cancel

Step 3. Choose Plan Type

At the **Plan Type** step of the wizard, select the **Restore** option.

New Replica Plan

Plan Info

Plan Type

VM Groups

VM Recovery Options

VM Steps

Protect VM Groups

RTO & RPO

Report Template

Report Scheduling

Summary

Choose the type of Plan

☐ Cloud

VMs will be recovered from Veeam agent or vSphere backups into a cloud environment

☐ CDP Replica

VMs will be recovered from Veeam CDP (continuous data protection) replicas

☒ Replica

VMs will be recovered from Veeam replicas

☐ Storage

VMs will be recovered from replicated storage volumes

☐ Restore

VMs will be recovered from Veeam agent or vSphere backups into a VMware vSphere environment

Back

Next

Cancel

Step 4. Select Recovery Location

At the **Recovery Location** step of the wizard, select a location to which inventory groups included in the plan will be restored.

For a recovery location to be displayed in the list of available recovery locations, it must be created and included into the list of inventory items available for the scope, as described in section [Managing Recovery Locations](#).

New Restore Plan

Plan Info

Scope

Plan Type

Recovery Location

VM Groups

VM Recovery Options

VM Steps

Protect VM Groups

RTO & RPO

Report Template

Report Scheduling

Summary

Choose a default recovery location

Choose a recovery location where backups will be restored as new VMs.

Search by Recovery Location

Name	VMs	Agents	Instant VM Recovery
Original VM Location	Enabled	Disabled	Disabled
Gold	Enabled	Enabled	Enabled

i

You can change the recovery location when launching the Plan.

Back

Next

Cancel

Step 5. Add Inventory Groups

At the **VM Groups** step of the wizard, select inventory groups that you want to recover, and click **Add** to include them in the plan.

For an inventory group to be displayed in the **Available Groups** list, it must be included into the list of inventory items available for the scope, as described in section [Allowing Access to Inventory Groups](#).

IMPORTANT

For Orchestrator to be able to recover a machine correctly, the machine must have VMware Tools installed:

- For VMs recovered from Veeam agent backups, Orchestrator automatically verifies whether VMware Tools are installed on all machines included in a plan when running a readiness check or a DataLab test for the plan. However, this verification is supported for Windows-based machines only. For Linux-based machines, you must perform the verification manually.
- For VMs recovered from vSphere backups, the verification is performed automatically on the vCenter Server side — for both Windows-based and Linux-based VMs. To know how to install and upgrade VMware Tools in vSphere, see [this VMware KB article](#).

New Restore Plan

Plan Info

Scope

Plan Type

Recovery Location

VM Groups

VM Recovery Options

VM Steps

Protect VM Groups

RTO & RPO

Report Template

Report Scheduling

Summary

Add VM Groups

Use View VMs control to check Group members, and Up/Down controls to change the recovery sequence.

Search

Available Groups ☐ Show empty Groups

Datastore - datastore2

Datastore - esx01-das2

Datastore - esx04-ds2

Datastore - KK-vol03

Datastore - kuvi-esxi65_store

Datastore - kuvi-nfs2

owner - audrey.allen

owner - shared

owner - stan.smith

owner - wendy.may

Add >

< Remove

Plan Groups

Datastore - esx01-das1

owner - chloe.lewis

Up Down View VMs

These options can be customized later on the Edit Plan page.

Back Next Cancel

Step 6. Specify VM Recovery Options

At the **VM Recovery Options** step of the wizard, use the **If the VM recovery encounters an error then** options to choose whether you want to halt plan execution if machine recovery fails. This option can also be customized later per-group [when editing the plan](#).

Use the **Recover the VMs in each group** options to choose whether you want to recover machines in sequence or in parallel. If you select to process machines simultaneously, use the **Recover simultaneously max of VMs** field to specify the maximum number of VMs processed at the same time.

If you want the recovered VMs to have the same tags as the source machines, select the **Restore VM Tags** check box.

The screenshot shows the 'New Restore Plan' wizard with the 'VM Recovery Options' step selected in the left sidebar. The main panel is titled 'Customize the default recovery options for all VMs in the Plan'. It contains the following options:

- If the VM recovery encounters an error then:**
 - ☒ Halt the plan
 - ☐ Proceed with the plan
- Recover the VMs in each group:**
 - ☒ In parallel
 - ☐ In sequence
- Recover simultaneously max of:** 10 VMs (with a spinner control)
- ☐ Restore VM Tags

An information message at the bottom states: 'These options can be customized later on the Edit Plan page.' The bottom of the wizard has 'Back', 'Next', and 'Cancel' buttons.

Step 7. Add Plan Steps

At the **VM Steps** step of the wizard, use the list of plan steps to select steps to be performed for each machine during restore.

For a step to be displayed in the **Available Steps** list, it must be included into the list of inventory items available for the scope, as described in section [Allowing Access to Plan Steps](#).

IMPORTANT

To allow the restore process to perform successfully, the **Restore VM** step must execute first.

By default, Orchestrator will perform the same selected steps in the same order for all new machines that will later appear in the inventory groups included in the plan. However, you can change the step execution order and modify the list of steps individually for each machine, as described in section [Configuring Steps](#).

NOTE

If a VM is included in multiple inventory groups in the same plan, Orchestrator will only run the **Restore VM** step once. However, other steps for this VM will execute when processing it in each group.

The screenshot shows the 'New Restore Plan' wizard with the 'VM Steps' tab selected. The interface is divided into a left sidebar with navigation links and a main content area. The sidebar links are: Plan Info, Scope, Plan Type, Recovery Location, VM Groups, VM Recovery Options, **VM Steps**, VM Credentials, Protect VM Groups, RTO & RPO, Report Template, Report Scheduling, and Summary. The main content area is titled 'Choose VM Steps' and includes a search bar, 'Up' and 'Down' arrows, and two lists: 'Available Steps' and 'Selected Steps'. The 'Available Steps' list contains: Restore VM, Check VM Heartbeat, Generate Event, Ping VM Network, Send Email, Shutdown Source VM, Start Service, Verify DNS Port, Verify Domain Controller Port, Verify Exchange Mailbox, Verify Exchange MAPI Connectivity, Verify Exchange Services, and Verify Global Catalog Port. The 'Selected Steps' list contains: Restore VM, Check VM Heartbeat, Verify SharePoint URL, Verify SQL Database, Verify SQL Port, and Send Email. An 'Add >' button is between the lists, and a '< Remove' button is below it. A footer bar at the bottom has 'Back', 'Next', and 'Cancel' buttons. An information icon and text at the bottom of the main area state: 'These options can be customized later on the Edit Plan page.'

Available Steps	Selected Steps
Restore VM	Restore VM
Check VM Heartbeat	Check VM Heartbeat
Generate Event	Verify SharePoint URL
Ping VM Network	Verify SQL Database
Send Email	Verify SQL Port
Shutdown Source VM	Send Email
Start Service	
Verify DNS Port	
Verify Domain Controller Port	
Verify Exchange Mailbox	
Verify Exchange MAPI Connectivity	
Verify Exchange Services	
Verify Global Catalog Port	

Step 8. Specify Credentials

[This step applies only if you have added one or more plan steps that require Windows credentials to run in-guest OS scripts inside machines being processed. For the full list of steps that require authentication, see [Appendix. Orchestration Plan Steps](#)]

At the **VM Credentials** step of the wizard, specify credentials that will be used to access guest OSes of machines. To do that, click the link in the **Credentials** section, and select the necessary credentials in the **Select Credentials** window. For a credential record to be displayed in the **Available Credentials** list, it must be included into the list of inventory items for the scope, as described in section [Allowing Access to Credentials](#).

If you do not specify any credentials, Orchestrator will use the default credentials defined when configuring plan steps on the **Administration** page of the Orchestrator UI, or you may specify the required credentials for each machine or inventory group individually [when editing the plan](#).

The screenshot shows the 'New Restore Plan' wizard in the Veeam Orchestrator UI. The 'VM Credentials' step is active. A 'Select Credentials' dialog box is open, displaying a list of available credentials. The 'TECH\chloe.lewis' credential is selected. The dialog box has a search bar at the top and a table of credentials below. The table has two columns: 'User Name' and 'Description'. The 'TECH\chloe.lewis' credential is highlighted in blue. The dialog box also has 'Default', 'OK', and 'Cancel' buttons at the bottom.

User Name	Description
qa09\Administrator	qa09\Administrator
qa10\Administrator	qa10\Administrator
root	Dell EMC Isilon
root	esx02\Administrator
srv19\Administrator	srv19\Administrator
tech\wendy.may	tech\wendy.may
srv28\administrator	srv28\administrator
TECH\chloe.lewis	

Step 9. Specify VM Protection Options

At the **Protect VM Groups** step of the wizard, use the **Protect VM Groups after recovery** check box to choose whether you want to protect VMs in the plan post-recovery with a backup or replication job.

If you select the **Protect VM Groups after recovery** check box, you must specify a backup or replication job to be used as a template for a new job that will reprotect recovered VMs. To do that, from the **Template Job** list, select the required job.

For a template backup or replication job to be displayed in the **Template Job** list, it must be created and included into the list of inventory items for the scope, as described in section [Editing Template Jobs](#).

IMPORTANT

The new job will consume Veeam Backup & Replication licenses to protect the machines. That is why you must take into account the number of licenses installed on the Veeam Backup & Replication server, so that the number of managed objects does not exceed the license limit.

The screenshot shows the 'New Restore Plan' wizard with the 'Protect VM Groups' step selected in the left-hand navigation pane. The main content area is titled 'Choose a reprotect option' and includes the instruction: 'Orchestrator can automatically create a new backup or replication job to reprotect the recovered VMs.' Below this, the checkbox 'Protect VM Groups after recovery' is checked. A 'Template Job' dropdown menu is set to 'Template Backup Job for Orchestrator [172.17.53.52]'. An information icon (i) is present next to a note: 'This Step requires that the Veeam Backup & Replication server has enough licenses to run the new job. See the [Orchestrator documentation](#) for details.' At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

Step 10. Specify Target RTO and RPO

At the **RTO & RPO** step of the wizard, define your Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for the plan:

- The **Target RPO** defines the maximum acceptable period of data loss.
- The **Target RTO** represents the amount of time it should take to recover from an incident.

NOTE

If you choose to perform ransomware scan [while running the plan](#), Orchestrator will scan only one disk per repository mount server at a time. This process may take a while, affecting the plan RTO.

RTO and RPO performance will be recorded in the [Plan Readiness Check](#), [Plan Execution](#) and [DataLab Test](#) reports, and you will be able to track the achieved RTO and RPO objectives for each plan on the [Home Page Dashboard](#).

The screenshot shows the 'New Restore Plan' wizard with the 'RTO & RPO' step selected in the left sidebar. The main area is titled 'Define your Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for this plan'. It contains two sections: 'Target RTO' and 'Target RPO'. Each section has three input fields for 'Hours', 'Minutes', and 'Seconds'. The 'Target RTO' fields are set to 1 hour, 0 minutes, and 0 seconds, with a description 'Maximum allowed time before the service is restored after a failure.' below them. The 'Target RPO' fields are set to 24 hours, 0 minutes, and 0 seconds, with a description 'Maximum allowed loss of historical data after a failure.' below them. At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons.

Field	Hours	Minutes	Seconds	Description
Target RTO	1	0	0	Maximum allowed time before the service is restored after a failure.
Target RPO	24	0	0	Maximum allowed loss of historical data after a failure.

Step 11. Select Report Template

At the **Report Template** step of the wizard, select a document template that will be used as the cover page for all Orchestrator reports. Use options in the **Document format** list to choose whether you want to generate documents in the DOCX or PDF format.

For a custom document template to be displayed in the **Available Templates** list, it must be created and customized as described in section [Managing Templates](#).

New Restore Plan

Plan Info

Scope

Plan Type

Recovery Location

VM Groups

VM Recovery Options

VM Steps

VM Credentials

Protect VM Groups

RTO & RPO

Report Template

Report Scheduling

Summary

Choose the report template to be used for Plan reports and documentation

Type any part of name to filter

Available Templates

Veeam Default Template (DE)
Dieses Template ist ein Beispiel und sollte auf Ihre Bedürfnisse angepasst werden

Veeam Default Template
This is an example template, and should be cloned and customized to your requirements

Veeam Default Template (ES)
Esta es una plantilla de ejemplo, y debe ser clonada y personalizada de acuerdo con sus requisitos

Veeam Default Template (FR)
Ceci est un modèle qui doit être cloné et personnalisé selon vos besoins

Veeam Default Template (PT)
Este é um template de exemplo, e deve ser clonado e customizado de acordo com seus requerimentos

Veeam Default Template (CH)
这是一个示例模板，应进行复制并根据您的要求定制

Veeam Default Template (JP)
こちらはサンプル・テンプレートです。コピーして、要件に応じてカスタマイズしてください

Document format:

☒ PDF file

☐ Word document (.DOCX)

Back

Next

Cancel

Step 12. Specify Report Scheduling Options

At the **Report Scheduling** step of the wizard, choose whether you want to automatically generate the [Plan Definition](#) and [Plan Readiness Check](#) reports for the plan on a daily schedule. You can also choose whether you want to generate both reports immediately after you create the plan.

To specify the exact time at which the report will be generated, click the **Schedule** icon next to the **Update Plan Definition report daily at** or **Perform Plan Readiness Check daily at** check box, set the desired time, and click **Apply**.

New Restore Plan

Plan Info

Scope

Plan Type

Recovery Location

VM Groups

VM Recovery Options

VM Steps

VM Credentials

Protect VM Groups

RTO & RPO

Report Template

Report Scheduling

Summary

Choose scheduling options for automatic Plan reporting

☒ Update Plan Definition report daily at: 8:24 AM

☒ Perform Plan Readiness Check daily at: 7:10 AM

i Reports will not be generated for plan

☒ Create Plan Definition when I click Finish

☒ Perform Readiness Check when I click Finish

Hours: 7 Minutes: 10

☒ AM ☐ PM

Apply **Cancel**

Back **Next** **Cancel**

Step 13. Finish Working with Wizard

At the **Summary** step of the wizard, review configuration information and click **Finish**.

New Restore Plan

Plan Info

Scope

Plan Type

Recovery Location

VM Groups

VM Recovery Options

VM Steps

VM Credentials

Protect VM Groups

RTO & RPO

Report Template

Report Scheduling

Summary

See below for a summary for the new Plan

Copy to clipboard

Plan Name:

Test Restore Plan

Description:

Evaluating restore

Contact Name:

Chloe Lewis

Contact Email:

chloe.lewis@veeam.com

Contact Tel:

18003334455

Scope:

SQL Administrators

Plan Type:

Restore

VM Group(s):

Datastore - esx01-das1
owner - chloe.lewis

Recovery Location:

Original VM Location (IVR Enabled - Yes)

Recover VMs:

Simultaneously (max 10)

If any VM fails:

Halt the plan

Restore VM Tags:

No

Steps for New VM Template:

Restore VM
Check VM Heartbeat
Verify SharePoint URL
Verify SQL Database
Verify SQL Port
Send Email

Override Credentials:

Yes, Template Backup Job for Orchestrator

Credentials:

Use Default

Protect VM Group, Job:

No, N/A

Target RTO:

1 Hour

Target RPO:

24 Hours

Report Template, format:

Veeam Default Template (DE), PDF

Update Plan Definition report:

Daily 8:24 AM

Back

Finish

Cancel

Editing Restore Plans

If you want to specify granular settings not provided in the [New Orchestration Plan wizard](#), the Orchestrator UI allows you to customize restore plans and configure the settings for groups, recovered VMs, plan steps and step parameters.

The procedures to edit replica, CDP replica, restore, storage and cloud plans are almost identical. For more information, see [Editing Orchestration Plans](#).

Testing Restore Plans

You can start on-demand plan testing and configure test scheduling for any restore plan. There is almost no difference between the procedures performed for replica, restore and storage plans. For more information, see [Testing Orchestration Plans](#).




Running and Scheduling Restore Plans

After you create and configure a restore plan, run a successful [readiness check](#) and a [DataLab test](#), the plan can be considered ready for restore. You can invoke various actions for the plan, depending on the current plan state.






Point in Time	Actions
New plan created	After plan creation, you can: <ul style="list-style-type: none">• Schedule a time for the plan to execute restore.• Run the plan to execute restore immediately.
Any	At any point, you can: <ul style="list-style-type: none">• Halt the plan to interrupt its execution.• Reset the plan to clear the current state and allow it to run again.

Plan States










Restore plans can acquire the following **default** states after creation. The same states are shown after resetting a plan, and after completing a test or a check.











Plan State	Icon	Description
NOT VERIFIED		Plan has never been tested, has never passed a readiness check, or has been changed since the last DataLab test or readiness check.
		Plan has failed to be tested or has failed to pass a readiness check.
VERIFIED		Plan has been tested successfully or has passed a readiness check.

Restore plans can acquire the following **stable** states after completing current processing:

Plan State	Icon	Description
HALTED		Plan has stopped due to either an error or user intervention.
RESTORED		Restore process completed successfully.
		Restore process completed with one or more warnings.
		Restore process completed with one or more errors.
TESTING HALTED		Plan testing has stopped due to either an error or user intervention.

Restore plans can acquire the following **active** states while in use or in progress:




Functionality	Tab	Plan Operator
Plan Management		
CREATING		Plan is being created.
EDITING		Plan is being edited.
SAVING		Plan is being saved. Note: Plan editing and execution are not available in this state.
RESETTING		Plan is being reset.
DELETING		Plan is being deleted.
Readiness Checks		
CHECKING		Plan readiness check is in progress.
		Plan readiness check is in progress; one or more warnings encountered.
		Plan readiness check is in progress; one or more errors encountered.
CHECK HALTING		Plan readiness check is halting.
Execution and Testing		

Functionality	Tab	Plan Operator
RESTORE		Plan is executing.
		Plan is executing; one or more warnings encountered.
		Plan is executing; one or more errors encountered.
HALTING		Plan is halting.
TEST PENDING		Plan is waiting for the test lab to power on.
TESTING		Plan testing is in progress.
		Plan testing is in progress; one or more warnings encountered.
		Plan testing is in progress; one or more errors encountered.
TEST HALTING		Plan testing is halting.
POWERING OFF		Plan testing is being powered off.

NOTE

If you perform any infrastructure configuration changes (add, delete or rename VMs) or changes to Veeam ONE Client groups, Orchestrator will not automatically apply these changes to plans that are currently executing or testing – such plans are 'locked' and cannot be edited. The changes will take effect only if the plans enter the *VERIFIED* or *NOT VERIFIED* state.

Restore plans can acquire the following **modes**:

Plan Mode	Icon	Description
ENABLED		Plan is ready to be verified, tested and executed. Notes: Plan editing is not available. Automatic report updates are enabled.
DISABLED		Plan is ready to be edited and tested. Notes: Scheduled plan execution is not available. Automatic report updates are disabled.
IN USE		Plan is either in one of the active states (except the <i>EDITING</i> state) or in one of the stable states. Notes: Plan editing is not available. Automatic report updates are disabled.

TIP

When a plan is in an active state, you can switch to the **Plan Details** page, select a VM being recovered in the **Virtual Machines** column, and click the **VM Console** link to connect directly to the VM desktop.

Orchestrator will connect to the VM through the vCenter Server system. To avoid connection failures, make sure the following requirements are met:

1. The target vCenter Server that manages the VM is running VMware vCenter Server version 6.0 or later.
2. The SSL certificate used by the target vCenter Server is valid on the machine on which you are running the browser. If not, install root certificates from the vCenter Server on both the Orchestrator server and the machine. To learn how to download and install vCenter Server root certificates, see [this VMware KB article](#).

In vSphere 6.0 and later, each newly created ESXi host is by default provisioned with a self-signed certificate from the VMware Certificate Authority. If you want to use such a certificate when accessing the VM desktop, download the root CA certificate from the host where the VM is registered. To learn how to manage certificates for ESXi hosts, see [VMware Docs](#).

Before You Begin

To run a restore plan, it must be *ENABLED*. To enable a plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan.
3. From the **Manage** menu, select **Enable**.

If you do not enable a plan before you run it, the [Run Plan](#) wizard will force you to do that as soon as you try running the plan.

NOTES

1. An Orchestrator Administrator or Plan Author can force-enable a plan in the **Run Plan** wizard. However, a Plan Operator will not be able to run a disabled restore plan.
For more information on roles that can be assigned to users and user groups working with the Orchestrator UI, see [Managing Permissions](#).
2. For security purposes, all 'real-world' actions associated with restore plans require password confirmation.

Scheduling Restore

You can schedule a time for a restore plan to execute. Only the restore process can be scheduled – all other operations must be performed manually in the Orchestrator UI.

To schedule a restore plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Schedule**.
-OR-
Right-click the plan name and select **Launch > Schedule**.
3. Complete the **Schedule Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.

The screenshot shows the 'Schedule Plan' wizard with the 'Credentials' step selected. The main area is titled 'Re-enter credentials to proceed'. It contains two input fields: 'User name:' with the value 'tech\olivia.dias' and 'Password:' with masked characters '*****'. An information icon (i) is present next to the password field. Below the input fields, a message states: 'For the plan to run according to the specified schedule, the plan must be enabled.' At the bottom right, there are 'Next' and 'Cancel' buttons. The left sidebar shows the wizard steps: 'Credentials' (selected), 'Schedule Options', 'Ransomware Scan', and 'Summary'.

- b. At the **Schedule Options** step, set the **Scheduled execution** toggle to *On*, and choose whether you want to run the plan on schedule or after any other plan.
 - If you want to run the plan at a specific time, select the **Schedule on** option, click the **Schedule** icon, set the desired date and time, and click **Apply**.

- If you want to run the plan after another plan, select the **Schedule after** option and click **Choose a Plan**. Then, in the **Select Plan** window, select the necessary plan and click **OK**.

For a plan to be displayed in the **Available Plans** list, it must be *ENABLED* as described in section [Running and Scheduling Restore Plans](#).

Schedule Plan [X]

Credentials

Schedule Options

Ransomware Scan

Summary

You may schedule this Plan to run at a specific time, or chain it to be executed after another Plan runs
Recovery will be performed using the most recent restore point.

Scheduled execution: ☒ On

☐ Schedule on 11/15/2022 10:31 AM [Calendar icon]

☒ Schedule after [Exchange Restore Plan](#)

i You can schedule only the Failover and Restore actions for Orchestration Plans. Other actions (such as Failback) must be performed manually.

[Back](#) [Next](#) [Cancel](#)

- At the **Ransomware Scan** step, choose whether you want to check restore points created for machines included in the plan for possible ransomware.

By default, Orchestrator checks 10 recently created restore points for each machine and halts the plan if all the restore points are infected. However, you can specify the maximum number of restore points to check and instruct Orchestrator to restore the machine to the selected recovery location without connecting it to any network.

For more information on ransomware scan, see [How Orchestrator Performs Ransomware Scan](#).

IMPORTANT

- Ransomware scan is supported only for Windows-based machines.
- Ransomware scan is not supported for restore points stored in external repositories.

The screenshot shows the 'Schedule Plan' wizard with the 'Ransomware Scan' step selected. The left sidebar contains links for 'Credentials', 'Schedule Options', 'Ransomware Scan', and 'Summary'. The main content area is titled 'Specify ransomware scan options' and includes a description: 'Scan restore points for viruses, malware and ransomware using Veeam Secure Restore. Virus-scanning can iterate through multiple restore points, starting with the most recent, until a clean point is found. For more information see the [User Guide](#).' Below this, there is a checkbox labeled 'Scan a maximum of' with a value of '10' in a spinner box, followed by the text 'previous restore points'. Under the heading 'If no clean restore point found', there are two radio button options: 'Cancel the restore and proceed to the next step' (which is selected) and 'Complete the restore but do not connect the VM to the network'. At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

d. At the **Summary** step, review configuration information and click **Finish**.

The screenshot shows the 'Schedule Plan' wizard with the 'Summary' step selected. The left sidebar contains links for 'Credentials', 'Schedule Options', 'Ransomware Scan', and 'Summary'. The main content area is titled 'Plan will be scheduled with below settings. Click Finish to apply'. Below this title is a 'Copy to clipboard' button. A list of settings is displayed: 'Plan name: Restore Plan', 'Schedule: Enabled', 'Ransomware Scan: Enabled', 'Restore points to scan (max): 10', 'If no clean restore point found: Cancel restore', and 'Choose scheduling options: After Plan: Exchange Restore Plan'. At the bottom right, there are three buttons: 'Back', 'Finish', and 'Cancel'.

TIP

You can disable a configured schedule if you no longer need it. To do that, set the **Scheduled execution** toggle to *Off* at the **Schedule Options** step of the **Schedule Plan** wizard.

Running Restore

The **Run** action causes machines in a plan to recover from their backup files. For more information on the data recovery process, see the Veeam Backup & Replication User Guide, section [Data Recovery](#).

TIP

If the Veeam Backup & Replication server that protects plan machines becomes unavailable, the plan will fail to complete successfully. However, in case the repository that stores the required backup files is still available, you will be able to work around the issue. To do that, [connect the repository to any other Veeam Backup & Replication server](#) added to Orchestrator, and [perform a rescan operation](#) for this repository.

To run a restore plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Run**.
-OR-
Click the plan name to switch to the **Plan Details** page, and click **Run**.
3. Complete the **Run Plan** wizard:
 - a. [This step applies only if you have not enabled the plan before running it]

At the **Plan Disabled** step, select the **Enable this Plan** check box.

The screenshot shows the 'Run Plan' wizard window. The left sidebar contains a list of steps: 'Plan Disabled' (selected), 'Credentials', 'Readiness Check', 'Recovery Location', 'Restore Point', 'Chained Plans', 'Ransomware Scan', and 'Summary'. The main area displays the 'Plan Disabled' step with the message 'This Plan is disabled' and 'You may force the Plan into enabled mode to run it.' Below this message is a checkbox labeled 'Enable this Plan' which is checked. At the bottom right, there are 'Next' and 'Cancel' buttons.

- b. For security purposes, at the **Credentials** step, retype your password.

The screenshot shows the 'Run Plan' dialog box with the 'Credentials' step selected in the left sidebar. The main area is titled 'Re-enter credentials to proceed'. It contains two input fields: 'User name:' with the value 'tech\olivia.dias' and 'Password:' with masked characters '*****'. A 'Show/Hide' eye icon is next to the password field. At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

Run Plan	
Plan Disabled	Re-enter credentials to proceed User name: tech\olivia.dias Password: ***** <div>Back Next Cancel</div>
Credentials	
Readiness Check	
Recovery Location	
Restore Point	
Chained Plans	
Ransomware Scan	
Summary	

- c. At the **Readiness Check** step, review the results of the most recent readiness check run for the plan to make sure the plan will be able to complete successfully.

The screenshot shows the 'Run Plan' dialog box with the 'Readiness Check' step selected in the left sidebar. The main area is titled 'Review readiness check report'. It includes a 'Copy to clipboard' link, execution details (Executed: 1/27/2023 8:10 AM, Result: Warning, Details: 0 Errors, 1 Warning), and a 'Download report' link. A warning message at the bottom states: 'It is highly recommended to run a readiness check before executing a plan.' At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

Run Plan	
Plan Disabled	Review readiness check report Copy to clipboard Executed: 1/27/2023 8:10 AM Result: ⚠ Warning Details: 0 Errors, 1 Warning Download report <div>It is highly recommended to run a readiness check before executing a plan.</div> <div>Back Next Cancel</div>
Credentials	
Readiness Check	
Recovery Location	
Restore Point	
Chained Plans	
Ransomware Scan	
Summary	

- d. At the **Recovery Location** step, select a location to which inventory groups included in the plan will be restored.

For a recovery location to be displayed in the list of available locations, it must be created and included into the list of inventory items available for the scope, as described in section [Managing Recovery Locations](#).

Name	VMs	Agents	Instant VM Recovery
Original VM Location	Enabled	Disabled	Disabled
Gold	Enabled	Enabled	Enabled

If the selected recovery location includes multiple hosts, datastores and networks, Orchestrator will use the round-robin algorithm to restore machines added to the plan. For more information, see [How Orchestrator Places VMs During Restore](#).

- e. At the **Restore Point** step, choose a restore point that will be used to recover machines.

IMPORTANT

Recovering data from the archive tier is not supported. If you select the **Use most recent Restore Point before** option, make sure to choose a restore point that is stored in either the capacity or the performance tier. For more information on Veeam Backup & Replication tiering options, see the Veeam Backup & Replication User Guide, section [Scale-Out Backup Repository](#).

The screenshot shows the 'Run Plan' dialog box with the 'Restore Point' step selected in the left sidebar. The main area is titled 'Choose restore point' and contains two radio button options: 'Use the latest Restore Point' (which is selected) and 'Use most recent Restore Point before: 11/15/2022 10:44 AM' (with a calendar icon). At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

- f. [This step applies only if you have any other orchestration plans scheduled to run after the plan completes]

At the **Chained Plans** step, select the **Also execute the chained plans** check box to proceed to execution of subsequent plans after the current plan enters the *RESTORED* state.

The screenshot shows the 'Run Plan' dialog box with the 'Chained Plans' step selected in the left sidebar. The main area has a header 'This Plan is part of a chain, and other Plans will execute when it is complete.' Below this is a checked checkbox labeled 'Also execute the chained plans'. A warning message with a yellow triangle icon states: 'Even Plans which are disabled will be forced to run. All Plans will all use the same restore point option.' At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

- g. At the **Ransomware Scan** step, choose whether you want to check restore points created for machines included in the plan for possible ransomware.

By default, Orchestrator checks 10 recently created restore points for each machine and halts the plan if all the restore points are infected. However, you can specify the maximum number of restore points to check and instruct Orchestrator to restore the machine to the selected recovery location without connecting it to any network.

For more information on ransomware scan, see [How Orchestrator Performs Ransomware Scan](#).

IMPORTANT

- Ransomware scan is supported only for Windows-based machines.
- Ransomware scan is not supported for restore points stored in object storage repositories.

The screenshot shows the 'Run Plan' dialog box with the 'Ransomware Scan' step selected in the left sidebar. The main area is titled 'Specify ransomware scan options'. It contains a checkbox 'Scan a maximum of' with a value of '10' and the text 'previous restore points'. Below this, it says 'If no clean restore point found' and provides two radio button options: 'Cancel the restore and proceed to the next step' (selected) and 'Complete the restore but do not connect the VM to the network'. At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

Run Plan	
Plan Disabled	Specify ransomware scan options Scan restore points for viruses, malware and ransomware using Veeam Secure Restore. Virus-scanning can iterate through multiple restore points, starting with the most recent, until a clean point is found. For more information see the User Guide .
Credentials	
Readiness Check	
Recovery Location	
Restore Point	
Ransomware Scan	
Summary	
<div>BackNextCancel</div>	

h. At the **Summary** step, review configuration information and click **Finish**.

The screenshot shows the 'Run Plan' dialog box with the 'Summary' step selected in the left sidebar. The main area is titled 'Click Finish to run the plan'. It includes a 'Copy to clipboard' icon and button. Below is 'Plan information' with details: Plan name (Exchange Restore Plan), Launched by (tech\olivia.dias [Administrator]), Current state (Not Verified (Failed check, no errors, 1 warning)), Action (Restore), Restore Point (Most Recent), and Recovery Location (Original VM Location (IVR Enabled - Yes)). Below that is 'Ransomware scan' information: Ransomware Scan (Enabled), Restore points to scan (max) (10), and If no clean restore point found (Cancel restore). At the bottom right are 'Back', 'Finish', and 'Cancel' buttons.

Run Plan	
Plan Disabled	Click Finish to run the plan Copy to clipboard Plan information Plan name: Exchange Restore Plan Launched by: tech\olivia.dias [Administrator] Current state: Not Verified (Failed check, no errors, 1 warning) Action: Restore Restore Point: Most Recent Recovery Location: Original VM Location (IVR Enabled - Yes) Ransomware scan Ransomware Scan: Enabled Restore points to scan (max): 10 If no clean restore point found: Cancel restore
Credentials	
Readiness Check	
Recovery Location	
Restore Point	
Chained Plans	
Ransomware Scan	
Summary	
<div>BackFinishCancel</div>	

The plan goal is to reach the *RESTORED* state. If any critical error is encountered, the plan will stop with the *HALTED* state. To learn how to work with *HALTED* restore plans, see [Managing Halted Plans](#).

How Orchestrator Places VMs During Restore

To restore machines included into a restore plan to a recovery location, Orchestrator uses the following algorithm:

1. The solution looks through all hosts added to the location as [compute resources](#) to detect the first available host. This is the host where the first processed machine will be registered.
2. Orchestrator applies the mapping specified in the [network mapping table](#) for the location to set the required network configuration of the recovered VM.

Orchestrator checks whether the network configuration of the detected host matches the required network configuration. If these configurations do not match, Orchestrator goes back to step 1.

3. In the list of datastores connected to the host as [storage resources](#), Orchestrator searches for the first datastore that both is available and has enough capacity. This is the datastore where files of the machine will be stored.

To calculate the datastore capacity and make sure that it has enough space to accommodate the recovered VM, Orchestrator uses the threshold that you specify [when creating or configuring the location](#).

When calculating the amount of free space available on a datastore, Orchestrator assumes that the swap file of the processed machine will be restored to this datastore as well. Orchestrator also takes into account that all disk files of the machine will be restored to the same datastore that stores the .VMX file, regardless of whether the source machine stores its disk files on multiple datastores. This may influence the resulting capacity estimation and the way Orchestrator searches for datastores to restore machines.

NOTE

The failure of steps 1–3 for a machine from a [critical inventory group](#) halts the plan in the following cases:

- If none of the discovered hosts is available, or if none of the hosts has network configuration that matches the required network configuration of the recovered VM.
- If none of the discovered datastores is available, or if none of the datastores meets the capacity requirements.

To learn how to work with *HALTED* restore plans, see [Managing Halted Plans](#).

4. When Orchestrator starts processing the next machine, the solution looks through all hosts added to the location as compute resources to detect the next available host:
 - If Orchestrator detects such a host, this is the host where the machine will be registered.
 - If there are no more available hosts, Orchestrator uses the host detected at step 1 to register the machine.

Then Orchestrator goes through steps 2–3 to detect the target network and datastore for the machine.

5. Orchestrator repeats step 4 for all other machines included in the plan until all the machines are restored. The order in which the machines are processed depends on the **VM Recovery Options** defined [while configuring the plan](#).

If datastores added to the recovery location as storage resources breach the capacity threshold before all the machines are restored, the failure of this step for a machine from a critical group halts the plan. To troubleshoot the issue, configure the location to add more datastores and try running the halted plan again. To learn how to work with *HALTED* restore plans, see [Managing Halted Plans](#).

How Orchestrator Selects Backup Files

Generally, when performing restore to a recovery location, Orchestrator looks through the list of all restore points created for a machine to choose a restore point that meets the date requirement specified in the [Run Plan wizard](#). The backup file that contains the chosen restore point is used to recover the machine.

However, when you use [backup copy capabilities offered by Veeam Backup & Replication](#), you have multiple instances of the same backup data existing in different locations. This situation may influence the way Orchestrator chooses backup files to recover machines.

In case Orchestrator detects 2 backup files containing the chosen restore point — one file created by a backup job and the other file created by a backup copy job — uses one of these files depending on the [backup copy preference settings configured for the recovery location](#):

- With backup copy preference enabled, Orchestrator uses the backup file produced by the backup copy job
- With backup copy preference disabled, Orchestrator uses the backup file produced by the backup job.

NOTE

When you [move backup files of a backup copy job](#) to another repository in the Veeam Backup & Replication console, Orchestrator becomes unable to use the restore points of the moved backup files for restore because of incorrect timestamps. That is why make sure to turn both the backup job and the backup copy job to create new restore points after you perform the move operation.

How Orchestrator Performs Ransomware Scan

Before you run a restore plan to recover a machine to the production environment, Orchestrator allows you to perform ransomware scan for the protected machine using [Veeam Secure Restore](#). You can also perform the scan when testing a restore plan in a DataLab.

While running a restore plan, Orchestrator performs ransomware scan in the following way:

1. Disks of a machine that is being restored are mounted to the [mount server](#).
2. On the mount server, antivirus software is triggered to scan files from the mounted disks.
3. Orchestrator iterates through the number of restore points [specified while running the plan](#) one by one to detect a restore point with no viruses.
4. If a clean restore point is detected, Orchestrator successfully restores the machine to the selected recovery location.

If no clean restore point is detected, Orchestrator either halts the plan or restores the machine to the selected recovery location without connecting it to any network, depending on the [configured restore point settings](#).

NOTE

If restore points of all machines included in the plan are stored in one repository, Orchestrator will process machines one by one. This process may take a while, affecting the plan RTO.

While testing a restore plan, Orchestrator performs ransomware scan in the following way:

1. Disks of a machine that is being tested are mounted to the [mount server](#).
2. On the mount server, antivirus software is triggered to scan files from the mounted disks.
3. Orchestrator checks the most recent restore point for possible ransomware.

4. If the restore point is clean, Orchestrator marks the point as *Healthy*. When a restore point is marked as *Healthy*, Orchestrator requires less time to process the machine while testing the plan next time.

If the restore point is infected, the DataLab test fails and the plan acquires the *TESTING HALTED* state. To learn how to manage halted testing, see [Halting Plan Testing](#).

The results of ransomware scan are included in [Readiness Check](#), [DataLab Test](#) and [Plan Execution](#) reports.

Requirements and Limitations for Ransomware Scan

To allow Orchestrator to perform ransomware scan, the following prerequisites must be met:

- Ransomware scan is supported only for Windows-based machines. Ransomware scan is not supported for restore points stored in object storage repositories.
- The Veeam Backup & Replication server that protects the machine being processed is running version 12 or later.
- Antivirus software must be installed on the mount server and support the command line interface (CLI). The following antivirus software is supported: Microsoft Defender, Kaspersky, ESET and Symantec Protection Engine.

Halting Restore

The **Halt** action interrupts plan execution. Any steps currently executing will be completed, then the plan will enter the *HALTED* state. To learn how to work with *HALTED* restore plans, see [Managing Halted Plans](#).

To stop a running restore plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Halt**.

-OR-

Click the plan name to switch to the **Plan Details** page, and click **Halt**.

3. Complete the **Halt Plan** wizard:

- a. For security purposes, at the **Credentials** step, retype your password.

The screenshot shows the 'Halt Plan' wizard with the 'Credentials' step selected. The title bar is 'Halt Plan' with a close button. The left sidebar has three items: 'Credentials' (selected), 'Schedule Impact', and 'Summary'. The main area is titled 'Re-enter credentials to proceed'. It contains two input fields: 'User name:' with the text 'tech\olivia.dias' and 'Password:' with masked characters '.....'. There is an eye icon to the right of the password field. At the bottom right, there are 'Next' and 'Cancel' buttons.

- b. [This step applies only if you have any other orchestration plans scheduled to run after the plan completes]

At the **Schedule Impact** step, choose whether you want to proceed with or cancel execution of subsequent plans after the current plan enters the *HALTED* state.

The screenshot shows the 'Halt Plan' wizard with the 'Schedule Impact' step selected. The title bar is 'Halt Plan' with a close button. The left sidebar has three items: 'Credentials', 'Schedule Impact' (selected), and 'Summary'. The main area has two radio buttons: 'Cancel the schedule and do not execute the subsequent Plans' (selected) and 'Continue the schedule and launch the next Plan now'. Below the radio buttons is a warning message with a yellow triangle icon: 'There are other Plan(s) scheduled in a chain to failover after this Plan completes. Choose the options for those scheduled Plans below.' At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons.

- c. At the **Summary** step, review configuration information and click **Finish**.

Halt Plan [X]

Credentials

Schedule Impact

Summary

Click Finish to halt the plan

Copy to clipboard

Plan name: Restore Plan

Halted by: tech\olivia.dias [Administrator]

Current state: Restore

Action: Halt

Halting a plan before it reaches a stable state may cause your environment to enter an inconsistent state, requiring manual troubleshooting and a reset of the plan to resolve.

Back Finish Cancel

Resetting Restore Plans

If a restore plan becomes inconsistent with the virtual environment, you can reset the plan. This will return the plan to the *DISABLED* state, without making any changes to the external virtual infrastructure.

To reset a restore plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Manage** menu, select **Reset**.

-OR-

Right-click the plan name and select **Manage > Reset**.

3. Complete the **Reset Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.

The screenshot shows the 'Reset Plan' wizard with the 'Credentials' step selected. The left sidebar contains 'Credentials', 'Quick Check', and 'Summary'. The main area is titled 'Re-enter credentials to proceed'. It contains two input fields: 'User name' with the value 'tech\olivia.dias' and 'Password' with masked characters '*****'. Below the fields is an information icon and a message: 'Reset will take no actions on VMs or replicas in your infrastructure. It will reinitialize the Plan in Orchestrator only. For *Halted* plans it is recommended to use Undo, not Reset.' At the bottom right are 'Next' and 'Cancel' buttons.

- b. At the **Quick Check** step, select the **Perform a Quick Check after reset is complete** check box to run a **readiness check** after the reset.

The screenshot shows the 'Reset Plan' wizard with the 'Quick Check' step selected. The left sidebar contains 'Credentials', 'Quick Check', and 'Summary'. The main area is titled 'It is recommended to run a Quick Check after resetting the plan'. It contains a single checkbox labeled 'Perform a Quick Check after reset is complete', which is checked. At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

- c. At the **Summary** step, review configuration information and click **Finish**.

Reset Plan

Credentials

Quick Check

Summary

Plan will be reset using the options below. Press Finish to reset the Plan

Copy to clipboard

Plan Name: Restore plan

Reset by: TECH\olivia.dias [Administrator]

Current State: Restore (Halted, 16% complete, 10 errors, no warnings)

Quick Check: Yes

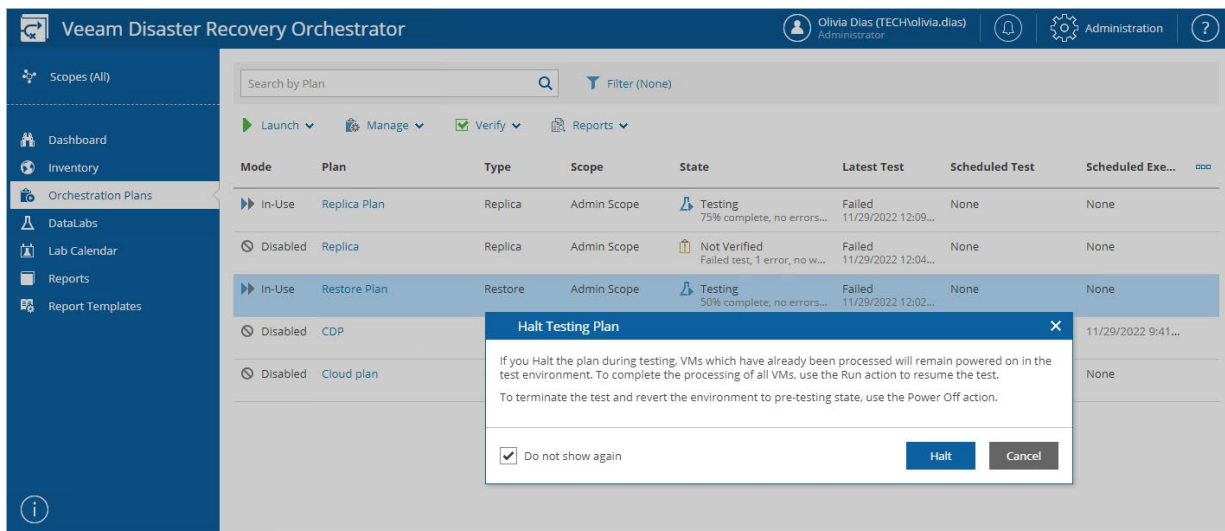
Back Finish Cancel

Halting Plan Testing

The **Halt** action interrupts plan testing. You may need to halt plan testing, for example, if you need to fix some environment-related issues and then [proceed with testing later](#) (in this case, recovered VMs will still continue to run). Or you may need to stop the testing process completely, for example, if you no longer need to test the selected restore plan (in this case, recovered VMs will be deleted).

To halt testing of a restore plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Verify** menu, select **Halt DataLab Test**.
-OR-
Right-click the plan name and select **Verify > Halt DataLab Test**.
3. In the **Halt Testing Plan** window, click **Halt** to confirm the action.



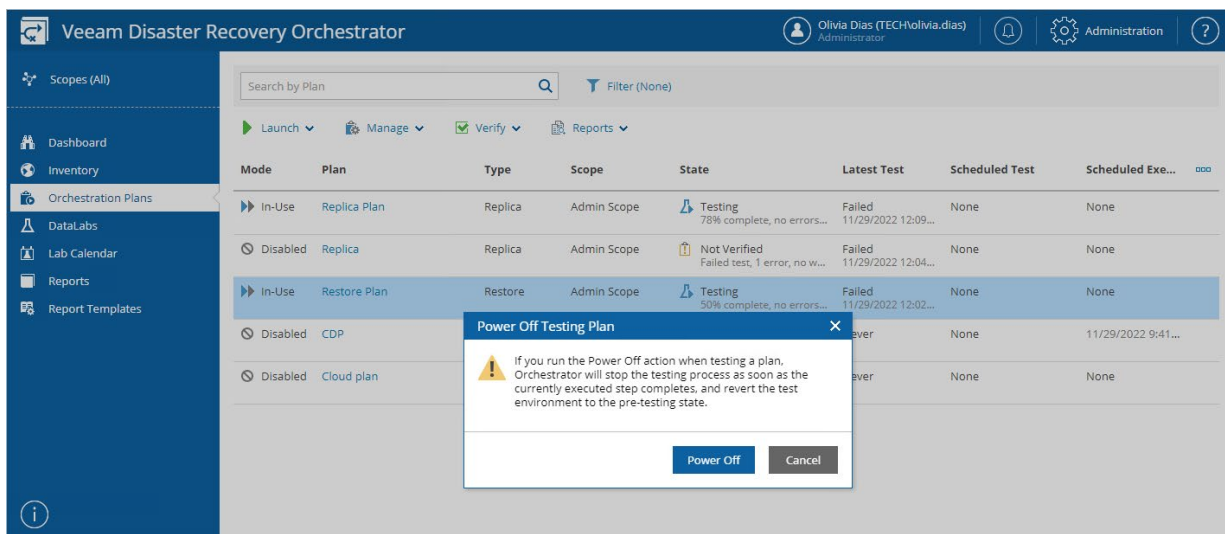
To cancel testing of a restore plan:

1. Select the plan. From the **Verify** menu, select **Power Off DataLab Test**.

-OR-

Right-click the plan name and select **Verify > Power Off DataLab Test**.

2. In the **Power Off Testing Plan** window, click **Power Off** to confirm the action.



Managing Halted Restore Plans

If a critical step fails for a machine from a [critical inventory group](#), the plan may enter the *HALTED* state. To troubleshoot reasons why a plan failed, use the **Plan Execution Report** generated as soon as the currently performed action completes. For more information on how to track plan performance history, see [Viewing Plan Execution History](#).

After you eliminate the problem that caused the plan to become *HALTED*, you have the following options to resume the plan:

- Repeat the last failed step.
- Proceed to the next step.

Running Halted Restore Plans

To run a *HALTED* restore plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Continue**.
-OR-
Click the plan name to switch to the **Plan Details** page, and click **Continue**.
3. Complete the **Resume Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.

The screenshot shows a 'Resume Plan' dialog box with a dark blue header and a close button (X) in the top right corner. On the left is a sidebar with three items: 'Credentials' (highlighted in light blue), 'Resume Settings', and 'Summary'. The main area is titled 'Re-enter credentials to proceed' and contains two input fields: 'User name:' with the text 'TECH\olivia.dias' and 'Password:' with masked characters '*****'. A small eye icon is to the right of the password field. At the bottom right are two buttons: 'Next' (blue) and 'Cancel' (grey).

- b. At the **Resume Settings** step, select an option to resume plan execution.

Choose whether you want to proceed with plan execution from the next plan step or to retry the failed step.

The screenshot shows the 'Resume Plan' dialog box with the 'Resume Settings' tab selected. The left sidebar contains 'Credentials', 'Resume Settings', and 'Summary'. The main area is titled 'Choose one of the following options' and contains two radio button options: 'Retry failed step' (selected) and 'Proceed to next step'. Below these options is an information icon and a note: 'If VMs are being processed in parallel, then multiple failed steps may be retried.' At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

Resume Plan	
Credentials	Choose one of the following options
Resume Settings	<p><input checked="" type="radio"/> Retry failed step If the most recently executed step failed, it will be retried</p> <p><input type="radio"/> Proceed to next step The plan will proceed to the next step</p> <p>i If VMs are being processed in parallel, then multiple failed steps may be retried.</p>
Summary	
<div>Back Next Cancel</div>	

- c. At the **Summary** step, review configuration information and click **Finish**. The restore process will be started.

The screenshot shows the 'Resume Plan' dialog box with the 'Summary' tab selected. The left sidebar contains 'Credentials', 'Resume Settings', and 'Summary'. The main area is titled 'Click Finish to resume the plan' and contains a 'Copy to clipboard' button. Below this is a 'Plan information' section with details: Plan name (Restore plan), Launched by (TECHVolivia.dias [Administrator]), Current state (Restore (Halted, 16% complete, 10 errors, no warnings)), Action (Resume - Restore), Resume by (Retry failed Step), and Recovery Location. Below this is a 'Ransomware scan' section with Ransomware Scan (Disabled). At the bottom right are 'Back', 'Finish', and 'Cancel' buttons.

Resume Plan	
Credentials	Click Finish to resume the plan
Resume Settings	<div>Copy to clipboard</div>
Summary	<p>Plan information</p> <p>Plan name: Restore plan</p> <p>Launched by: TECHVolivia.dias [Administrator]</p> <p>Current state: - Restore (Halted, 16% complete, 10 errors, no warnings)</p> <p>Action: Resume - Restore</p> <p>Resume by: Retry failed Step</p> <p>Recovery Location:</p> <p>Ransomware scan</p> <p>Ransomware Scan: Disabled</p>
<div>Back Finish Cancel</div>	

Resuming Plan Testing

To start the *HALTED* restore plan testing process:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Verify** menu, select **Continue DataLab Test**.

-OR-

Right-click the plan name and select **Verify > Continue DataLab Test**.

3. Complete the **Resume DataLab Test** wizard:
 - a. At the **Resume Test** step, select an option to resume test execution.

Choose whether you want to proceed with test execution from the next plan step or to retry the failed step.

The screenshot shows a dialog box titled "Resume DataLab Test" with a close button (X) in the top right corner. The dialog is divided into two main sections. On the left is a sidebar with two tabs: "Resume Test" (which is highlighted in blue) and "Summary". The main area on the right contains the heading "You have the following options to resume this Plan test." Below this heading are two radio button options. The first option, "Retry failed step", is selected (indicated by a filled radio button) and includes the text "If the most recently executed step failed, it will be retried". The second option, "Proceed to next step", is unselected (indicated by an empty radio button) and includes the text "The plan will proceed to the next step". At the bottom right of the dialog, there are two buttons: "Next" (in blue) and "Cancel" (in grey).

- b. At the **Summary** step, review configuration information and click **Finish**. The testing process will be started.

Resume DataLab Test

Resume Test

Summary

Your settings are summarized below

Plan Name:	Restore Plan
Scope:	Admin Scope
DataLab:	Testing Plan 01
Plan State:	Testing – Halted
Action:	Resume Testing
Resume by:	Retry failed Step

[Back](#) [Finish](#) [Cancel](#)

Resetting Halted Restore Plans

To reset a *HALTED* restore plan, follow the instructions provided in section [Resetting Restore Plans](#).

NOTE

When you reset a restore plan, Orchestrator returns it to the *DISABLED* state without making any changes to the external virtual infrastructure. You may need to deal with any infrastructure reconfiguration manually.

Working with Storage Plans

The type of an orchestration plan you create depends on whether you intend to use Orchestrator to switch to VM replicas, to restore machines from backups or backup copies, or to serve data from a destination (NetApp) or secondary (HPE) volume in case a disaster strikes.

If you want to recover volumes protected by storage replication, create a storage plan.

NOTE

It is recommended that you drive the creation and transfer of storage snapshots using Veeam Backup & Replication, as described in the Veeam Backup & Replication User Guide, section [Integration with Storage Systems](#).

Creating Storage Plans

To create a storage plan:

1. Navigate to **Orchestration Plans**.
2. Click **Manage > New**.
3. Complete the **New Orchestration Plan** wizard:
 - a. [Specify a plan name and description](#).
 - b. [Choose a scope for the plan](#).
 - c. [Choose a type of the plan](#).
 - d. [Choose a storage vendor for the plan](#).
 - e. [Include inventory groups in the plan](#).
 - f. [Specify VM recovery options](#).
 - g. [Add steps to the plan](#).
 - h. [Specify credentials for the plan steps](#).
 - i. [Specify the target RTO and RPO](#).
 - j. [Select a template for plan reports](#).
 - k. [Specify scheduling options for plan reports](#).
 - l. [Finish working with the wizard](#).

Step 1. Specify Plan Name and Description

At the **Plan Info** step of the wizard, use the **Plan Name** and **Description** fields to enter a name for the new plan and to provide a description for future reference. The maximum length of the plan name is 64 characters; the following characters are not supported: * : / \ ? " < > | .

You can also provide a contact name, email and telephone number of a person responsible for the plan.

New Orchestration Plan

Plan Info

Scope

Plan Type

Recovery Location

VM Groups

VM Recovery Options

VM Steps

RTO & RPO

Report Template

Report Scheduling

Summary

Provide details for the new Orchestration Plan

Plan Name:

Test Storage Plan

Description:

Evaluating storage failover

Contact Name:

Wendy May

Contact Email:

wendy.may@veeam.com

Contact Tel:

18004445566

Next

Cancel

Step 2. Choose Plan Scope

At the **Scope** step of the wizard, select a scope for which you want to create the plan.

For a scope to be displayed in the **Available Scopes** list, it must be created and customized as described in section [Managing Permissions](#).

New Orchestration Plan

Plan Info

Scope

Plan Type

Recovery Location

VM Groups

VM Recovery Options

VM Steps

RTO & RPO

Report Template

Report Scheduling

Summary

Choose a Scope

Type any part of Scope name to filter

Available Scopes

Admin Scope

Exchange Administrators

SQL Administrators

Back

Next

Cancel

Step 3. Choose Plan Type

At the **Plan Type** step of the wizard, select the **Storage** option.

New Storage Plan

Plan Info

Plan Type

Storage Vendor

VM Groups

VM Recovery Options

VM Steps

RTO & RPO

Report Template

Report Scheduling

Summary

Choose the type of Plan

☐ Cloud

VMs will be recovered from Veeam agent or vSphere backups into a cloud environment

☐ CDP Replica

VMs will be recovered from Veeam CDP (continuous data protection) replicas

☐ Replica

VMs will be recovered from Veeam replicas

☒ Storage

VMs will be recovered from replicated storage volumes

☐ Restore

VMs will be recovered from Veeam agent or vSphere backups into a VMware vSphere environment

Back

Next

Cancel

Step 4. Choose Storage Vendor

At the **Storage Vendor** step of the wizard, choose whether VMs that you plan to recover are located on datastores backed by NetApp or HPE storage systems.

New Storage Plan

Plan Info

Scope

Plan Type

Storage Vendor

VM Groups

VM Recovery Options

VM Steps


RTO & RPO


Report Template

Report Scheduling

Summary

Choose storage vendor

☒  NetApp ONTAP

☐  HPE Primera (3PAR)

Back

Next

Cancel

Step 5. Add Inventory Groups

At the **VM Groups** step of the wizard, select inventory groups that you want to recover, and click **Add** to include them in the plan. Note that you must add VMs that are running on source storage volumes — not destination volumes.

For an inventory group to be displayed in the **Available Groups** list, it must be included into the list of inventory items available for the scope, as described in section [Allowing Access to Inventory Groups](#). By default, the list shows those inventory groups that relate to datastores protected by storage replication and datastores backed by storage systems added to Orchestrator — to display groups that contain empty datastores as well, select the **Show all datastore groups** check box.

IMPORTANT

1. Since Orchestrator orchestrates storage failover at the volume level, all VMs that belong to a specific datastore must be processed as part of the same storage plan.
2. If a VM that you want to fail over stores its disk files on multiple datastores, make sure to include in the plan all inventory groups related to these datastores.
Also, make sure to include the group with the .VMX file into the plan first, before the groups with .VMDK files.
3. If the VMs that you want to fail over belong to a datastore in a VMware Storage DRS cluster, make sure to include in the plan all inventory groups related to this cluster.
4. Failover to the same VMware vSphere datacenter where the source VMs reside is not supported.
5. Failover of VMs that store disks on volumes protected using SnapVault is not supported.
6. Failover of VMs with RDM disks is not supported.
7. For datastores connected through the NFSv4.1 protocol, Orchestrator supports failover to a recovery location only in the case that target hosts included in the location have the NFSv3 export policy enabled (since the recovered datastores will be mounted to the hosts through NFSv3).
For datastores connected through other protocols, no limitations apply.
8. If the LUN ID of a datastore where the selected inventory groups belong is higher than 256, Orchestrator may not be able to orchestrate storage failover properly. If the LUN ID is higher than 256, make sure that your equipment supports this ID.
9. For Orchestrator to be able to recover a VM correctly, the VM must have VMware Tools installed. The presence of VMware Tools is checked automatically on the vCenter Server side — for both Windows-based and Linux-based VMs. To know how to install and upgrade VMware Tools in vSphere, see [this VMware KB article](#).

New Storage Plan

Plan Info

Scope

Plan Type

Storage Vendor

VM Groups

VM Recovery Options

VM Steps

RTO & RPO

Report Template

Report Scheduling

Summary

Add VM Groups

Use View VMs control to check Group members, and Up/Down controls to change the recovery sequence.

Search

Available Groups

☐ Show all datastore groups

Datastore - ID_store_1

Datastore - kuvi_3par_big

Datastore - kuvi-enr2

Datastore - mk_vol_11

Datastore - mk_vol_5

Datastore - mk_vol_6

Datastore - mk_vol_7

Datastore - mk_vol_8

Datastore - mk_vol_9

Add >

< Remove

Plan Groups

Datastore - 3PAR stg04 Vol1

Datastore - 3PAR stg04 Vol2

You can add only datastore-based VM Groups to storage plans. By default, the Available Groups list displays only those groups related to datastores backed by storage volumes.

Back

Next

Cancel

242 | Veeam Disaster Recovery Orchestrator | Operations Guide

Step 6. Specify VM Recovery Options

At the **VM Recovery Options** step of the wizard, use the **If the VM recovery encounters an error then** options to choose whether you want to halt plan execution if VM recovery fails. This option can also be customized later per-group [when editing the plan](#).

Use the **Recover the VMs in each group** options to choose whether you want to recover VMs in sequence or in parallel. If you select to process VMs simultaneously, use the **Recover simultaneously max of VMs** field to specify the maximum number of VMs processed at the same time.

The screenshot shows the 'New Storage Plan' wizard with the 'VM Recovery Options' step selected in the left sidebar. The main content area is titled 'Customize the default recovery options for all VMs in the Plan'. It contains two sections of radio button options. The first section, 'If the VM recovery encounters an error then', has 'Halt the plan' selected. The second section, 'Recover the VMs in each group', has 'In parallel' selected. Below these is a field 'Recover simultaneously max of:' with a value of '10' and the unit 'VMs'. An information banner at the bottom states: 'These options can be customized later on the Edit Plan page.' At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

New Storage Plan	
Plan Info	Customize the default recovery options for all VMs in the Plan If the VM recovery encounters an error then <input checked="" type="radio"/> Halt the plan <input type="radio"/> Proceed with the plan Recover the VMs in each group <input checked="" type="radio"/> In parallel <input type="radio"/> In sequence Recover simultaneously max of: <input type="text" value="10"/> VMs <div><i>i</i> These options can be customized later on the Edit Plan page.</div>
Scope	
Plan Type	
Storage Vendor	
VM Groups	
VM Recovery Options	
VM Steps	
RTO & RPO	
Report Template	
Report Scheduling	
Summary	
<div>BackNextCancel</div>	

Step 7. Add Plan Steps

At the **VM Steps** step of the wizard, use the list of plan steps to select steps to be performed for each VM during storage failover.

For a step to be displayed in the **Available Steps** list, it must be included into the list of inventory items available for the scope, as described in section [Allowing Access to Plan Steps](#).

IMPORTANT

To allow the storage failover process to perform successfully, the **Register VM** step must execute first.

By default, Orchestrator will perform the same selected steps in the same order for all new VMs that will later appear in the inventory groups included in the plan. However, you can change the step execution order and modify the list of steps individually for each VM, as described in section [Configuring Steps](#).

NOTE

If a VM is included in multiple inventory groups in the same plan, Orchestrator will only run the **Register VM** step once. However, other steps for this VM will execute when processing it in each group.

The screenshot shows the 'New Storage Plan' wizard with the 'VM Steps' tab selected. The interface is divided into a left sidebar with navigation options and a main content area. The main content area is titled 'Choose VM Steps' and includes a search bar, 'Up' and 'Down' arrows, and two lists: 'Available Steps' and 'Selected Steps'. The 'Available Steps' list contains 15 items, with 'Register VM' at the top. The 'Selected Steps' list contains 5 items, with 'Register VM' at the top. A 'Send Email' step is highlighted in the 'Selected Steps' list. At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons. A note at the bottom of the main content area states: 'These options can be customized later on the Edit Plan page.'

Available Steps	Selected Steps
Register VM	Register VM
Check VM Heartbeat	Check VM Heartbeat
Generate Event	Verify Domain Controller Port
Ping VM Network	VM Power Actions
Send Email	Send Email
Shutdown Source VM	
Start Service	
Verify DNS Port	
Verify Domain Controller Port	
Verify Exchange Mailbox	
Verify Exchange MAPI Connectivity	
Verify Exchange Services	
Verify Global Catalog Port	

Step 8. Specify Credentials

[This step applies only if you have added one or more plan steps that require Windows credentials to run in-guest OS scripts inside VMs being processed. For the full list of steps that require authentication, see [Appendix. Orchestration Plan Steps](#)]

At the **VM Credentials** step of the wizard, specify credentials that will be used to access guest OSes of VMs. To do that, click the link in the **Credentials** section, and select the necessary credentials in the **Select Credentials** window. For a credential record to be displayed in the **Available Credentials** list, it must be included into the list of inventory items for the scope, as described in section [Allowing Access to Credentials](#).

If you do not specify any credentials, Orchestrator will use the default credentials defined when configuring plan steps on the **Administration** page of the Orchestrator UI, or you may specify the required credentials for each VM or inventory group individually [when editing the plan](#).

The screenshot shows the 'New Storage Plan' wizard in the Veeam Orchestrator UI. The 'VM Credentials' step is active. A 'Select Credentials' dialog box is open, displaying a list of available credentials. The 'prg2016\administr...' credential is selected. The dialog box includes a search bar, a table of credentials, and buttons for 'Default', 'OK', and 'Cancel'.

User Name	Description
prg0061\wbr	prg0061.local
prg2016\administr...	prg2016.local
prg2016\cifs	cifs user
prg2016\sql	sql user
prg2016\test1	test1 user

Step 9. Specify Target RTO and RPO

At the **RTO & RPO** step of the wizard, define your Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for the plan:

- The **Target RPO** defines the maximum acceptable period of data loss.
- The **Target RTO** represents the amount of time it should take to recover from an incident.

RTO and RPO performance will be recorded in the [Plan Readiness Check](#), [Plan Execution](#) and [DataLab Test](#) reports, and you will be able to track the achieved RTO and RPO objectives for each plan on the [Home Page Dashboard](#).

New Storage Plan

×

Plan Info

Scope

Plan Type

Storage Vendor

VM Groups

VM Recovery Options

VM Steps

VM Credentials

RTO & RPO

Report Template

Report Scheduling

Summary

Define your Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for this plan

Hours:Minutes:Seconds:

Target RTO:100

Maximum allowed time before the service is restored after a failure.

Hours:Minutes:Seconds:

Target RPO:2400

Maximum allowed loss of historical data after a failure.

Back

Next

Cancel

Step 10. Select Report Template

At the **Report Template** step of the wizard, select a document template that will be used as the cover page for all Orchestrator reports. Use options in the **Document format** list to choose whether you want to generate documents in the DOCX or PDF format.

For a custom document template to be displayed in the **Available Templates** list, it must be created and customized as described in section [Generating Reports](#).

New Storage Plan

Plan Info

Scope

Plan Type

Storage Vendor

VM Groups

VM Recovery Options

VM Steps

VM Credentials

RTO & RPO

Report Template

Report Scheduling

Summary

Choose the report template to be used for Plan reports and documentation

Type any part of name to filter

Available Templates

Veeam Default Template

This is an example template, and should be cloned and customized to your requirements

Veeam Default Template (DE)

Dieses Template ist ein Beispiel und sollte auf Ihre Bedürfnisse angepasst werden

Veeam Default Template (ES)

Esta es una plantilla de ejemplo, y debe ser clonada y personalizada de acuerdo con sus requisitos

Veeam Default Template (FR)

Ceci est un modèle qui doit être cloné et personnalisé selon vos besoins

Veeam Default Template (PT)

Este é um template de exemplo, e deve ser clonado e customizado de acordo com seus requerimentos

Veeam Default Template (CH)

这是一个示例模板，应进行复制并根据您的要求定制

Veeam Default Template (JP)

こちらはサンプル・テンプレートです。コピーして、要件に応じてカスタマイズしてください

Document format:

☒ PDF file

☐ Word document (.DOCX)

Back

Next

Cancel

Step 11. Specify Report Scheduling Options

At the **Report Scheduling** step of the wizard, choose whether you want to automatically generate the [Plan Definition](#) and [Plan Readiness Check](#) reports for the plan on a daily schedule. You can also choose whether you want to generate both reports immediately after you create the plan.

To specify the exact time at which the report will be generated, click the **Schedule** icon next to the **Update Plan Definition report daily at** or **Perform Plan Readiness Check daily at** check box, set the desired time, and click **Apply**.

New Storage Plan

Plan Info

Scope

Plan Type

Storage Vendor

VM Groups

VM Recovery Options

VM Steps

VM Credentials

RTO & RPO

Report Template

Report Scheduling

Summary

Choose scheduling options for automatic Plan reporting

☒ Update Plan Definition report daily at: 11:20 AM

☒ Perform Plan Readiness Check daily at: 6:45 AM

i Reports will not be generated for plan

☒ Create Plan Definition when I click Finish

☒ Perform Readiness Check when I click Finish

Hours: 6 Minutes: 45

☒ AM ☐ PM

Apply **Cancel**

Back **Next** **Cancel**

Step 12. Finish Working with Wizard

At the **Summary** step of the wizard, review configuration information and click **Finish**.

New Storage Plan

Plan Info

Scope

Plan Type

Storage Vendor

VM Groups

VM Recovery Options

VM Steps

VM Credentials

RTO & RPO

Report Template

Report Scheduling

Summary

See below for a summary for the new Plan

Copy to clipboard

Plan Name:

Test Storage Plan

Description:

Evaluating storage failover

Contact Name:

Wendy May

Contact Email:

wendy.may@veeam.com

Contact Tel:

18004445566

Scope:

Admin Scope

Plan Type:

Storage

Vendor:

HPE Primera

VM Group(s):

Datastore - 3PAR stg04 Vol1

Recover VMs:

Simultaneously (max 10)

If any VM fails:

Halt the plan

Steps for New VM Template:

Register VM

Check VM Heartbeat

Verify Domain Controller Port

VM Power Actions

Send Email

Start Service

Override Credentials:

Yes, admin

Credentials:

admin

Target RTO:

1 Hour

Target RPO:

24 Hours

Report Template, format:

Veeam Default Template, PDF

Update Plan Definition report:

Daily 7:00 AM

Perform Readiness Check:

Daily 8:00 AM

Create Plan Definition report now:

Yes

Run Readiness Check now:

Yes

Back

Finish

Cancel

Editing Storage Plans

If you want to specify granular settings not provided in the [New Orchestration Plan wizard](#), the Orchestrator UI allows you to customize storage plans and configure the settings for groups, recovered VMs, plan steps and step parameters.

The procedures to edit replica, CDP replica, restore, storage and cloud plans are almost identical. For more information, see [Editing Orchestration Plans](#).

Testing Storage Plans

You can start on-demand plan testing and configure test scheduling for any storage plan. There is almost no difference between the procedures performed for replica, restore and storage plans. For more information, see [Testing Orchestration Plans](#).




Running and Scheduling Storage Plans

After you create and configure a storage plan, run a successful [readiness check](#) and a [DataLab test](#), the plan can be considered ready for failover. You can invoke various actions for the plan, depending on the current plan state.






Point in Time	Actions
New plan created	After plan creation, you can: <ul style="list-style-type: none">• Schedule a time for the plan to execute failover.• Run the plan to execute failover immediately.
Any	At any point, you can: <ul style="list-style-type: none">• Halt the plan to interrupt its execution.• Undo to attempt reversal of the previous action.• Reset the plan to clear the current state and allow it to run again (for example, to fail back).

Plan States










Storage plans can acquire the following **default** states after creation. The same states are shown after resetting a plan, and after completing a test or a check.











Plan State	Icon	Description
NOT VERIFIED		Plan has never been tested, has never passed a readiness check, or has been changed since the last DataLab test or readiness check.
		Plan has failed to be tested or has failed to pass a readiness check.
VERIFIED		Plan has been tested successfully or has passed a readiness check.

Storage plans can acquire the following **stable** states after completing current processing:

Plan State	Icon	Description
HALTED		Plan has stopped due to either an error or user intervention.
FAILOVER		Process completed successfully.
UNDO FAILOVER		Process completed with one or more warnings.
		Process completed with one or more errors.
TESTING HALTED		Plan testing has stopped due to either an error or user intervention.

Storage plans can acquire the following **active** states while in use or in progress:




Functionality	Tab	Plan Operator
Plan Management		
CREATING		Plan is being created.
EDITING		Plan is being edited.
SAVING		Plan is being saved. Note: Plan editing and execution are not available in this state.
RESETTING		Plan is being reset.
DELETING		Plan is being deleted.
Readiness Checks		
CHECKING		Plan readiness check is in progress.
		Plan readiness check is in progress; one or more warnings encountered.
		Plan readiness check is in progress; one or more errors encountered.
CHECK HALTING		Plan readiness check is halting.
Execution and Testing		

Functionality	Tab	Plan Operator
FAILOVER		Plan is executing.
		Plan is executing; one or more warnings encountered.
		Plan is executing; one or more errors encountered.
HALTING		Plan is halting.
TEST PENDING		Plan is waiting for the test lab to power on.
TESTING		Plan testing is in progress.
		Plan testing is in progress; one or more warnings encountered.
		Plan testing is in progress; one or more errors encountered.
TEST HALTING		Plan testing is halting.
POWERING OFF		Plan testing is being powered off.

NOTE

If you perform any infrastructure configuration changes (add, delete or rename VMs) or changes to Veeam ONE Client groups, Orchestrator will not automatically apply these changes to plans that are currently executing or testing – such plans are 'locked' and cannot be edited. The changes will take effect only if the plans enter the *VERIFIED* or *NOT VERIFIED* state.

Storage plans can acquire the following **modes**:

Plan Mode	Icon	Description
ENABLED		Plan is ready to be verified, tested and executed. Notes: Plan editing is not available. Automatic report updates are enabled in this mode.
DISABLED		Plan is ready to be edited and tested. Notes: Scheduled plan execution is not available. Automatic report updates are disabled in this mode.
IN USE		Plan is either in one of the active states (except the <i>EDITING</i> state) or in one of the stable states. Notes: Plan editing is not available. Automatic report updates are disabled in this mode.

TIP

When a plan is in an active state, you can switch to the **Plan Details** page, select a VM being recovered in the **Virtual Machines** column, and click the **VM Console** link to connect directly to the VM desktop.

Orchestrator will connect to the VM through the vCenter Server system. To avoid connection failures, make sure the following requirements are met:

1. The target vCenter Server that manages the VM is running VMware vCenter Server version 6.0 or later.
2. The SSL certificate used by the target vCenter Server is valid on the machine on which you are running the browser. If not, install root certificates from the vCenter Server on both the Orchestrator server and the machine. To learn how to download and install vCenter Server root certificates, see [this VMware KB article](#).

In vSphere 6.0 and later, each newly created ESXi host is by default provisioned with a self-signed certificate from the VMware Certificate Authority. If you want to use such a certificate when accessing the VM desktop, download the root CA certificate from the host where the VM is registered. To learn how to manage certificates for ESXi hosts, see [VMware Docs](#).

Before You Begin

To run a storage plan, it must be *ENABLED*. To enable a plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan.
3. From the **Manage** menu, select **Enable**.

If you do not enable a plan before you run it, the [Run Plan](#) wizard will force you to do that as soon as you try running the plan.

NOTES

1. An Orchestrator Administrator or Plan Author can force-enable a plan in the **Run Plan** wizard. However, a Plan Operator will not be able to run a disabled storage plan.
For more information on roles that can be assigned to users and user groups working with the Orchestrator UI, see [Managing Permissions](#).
2. For security purposes, all 'real-world' actions associated with storage plans require password confirmation.

Scheduling Storage Failover

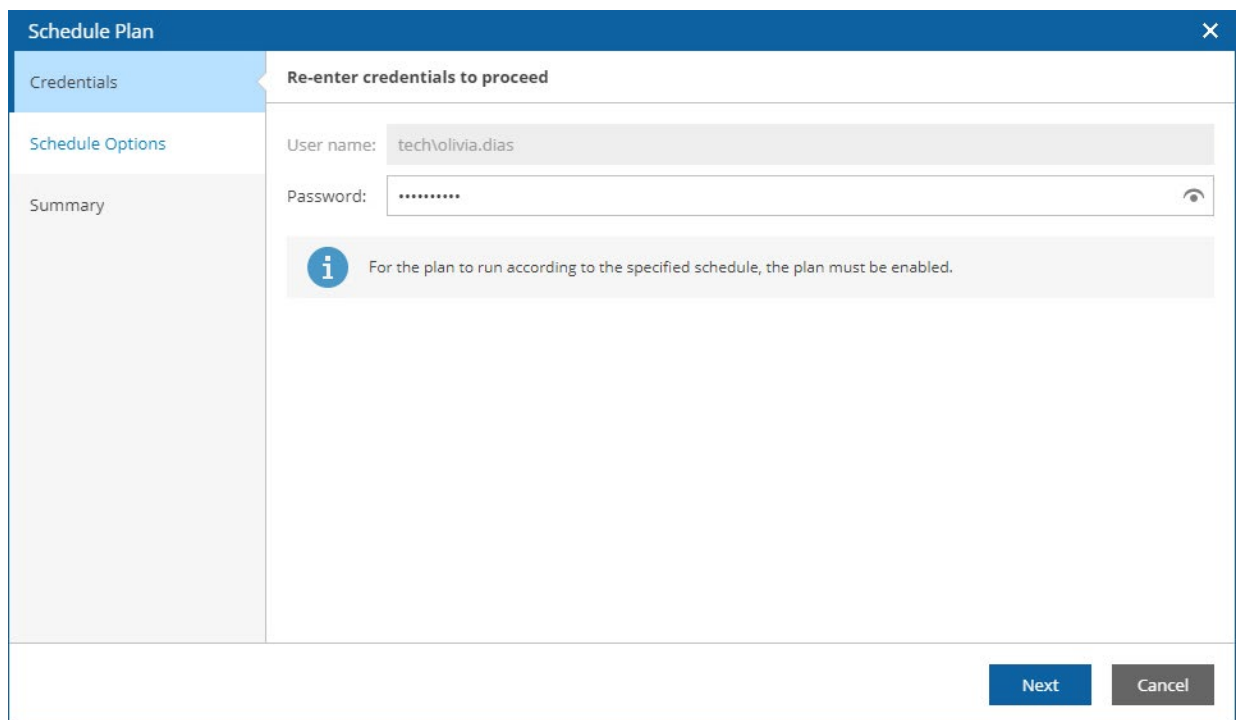
You can schedule a time for a storage plan to execute. Only the failover process can be scheduled — all other operations must be performed manually in the Orchestrator UI.

NOTE

If you configure a schedule for a storage plan, Orchestrator will not be able to trigger reverse replication to reprotect volumes included in the plan — this option is available only when you [run the storage failover process manually](#).

To schedule a storage plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Schedule**.
-OR-
Right-click the plan name and select **Launch > Schedule**.
3. Complete the **Schedule Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.



The screenshot shows the 'Schedule Plan' wizard in the Veeam Orchestrator UI. The window has a blue title bar with the text 'Schedule Plan' and a close button. On the left, there is a sidebar with three tabs: 'Credentials' (selected and highlighted in blue), 'Schedule Options', and 'Summary'. The main area of the wizard is titled 'Re-enter credentials to proceed'. It contains two input fields: 'User name:' with the text 'tech\olivia.dias' and 'Password:' with masked characters '*****'. To the right of the password field is an eye icon for toggling visibility. Below the input fields is an information icon (a blue circle with a white 'i') followed by the text: 'For the plan to run according to the specified schedule, the plan must be enabled.' At the bottom right of the wizard, there are two buttons: 'Next' (blue) and 'Cancel' (gray).

- b. At the **Schedule Options** step, set the **Scheduled execution** toggle to *On*, and choose whether you want to run the plan on schedule or after any other plan.
 - If you want to run the plan at a specific time, select the **Schedule on** option, click the **Schedule** icon, set the desired date and time, and click **Apply**.

- If you want to run the plan after another plan, select the **Schedule after** option and click **Choose a Plan**. Then, in the **Select Plan** window, select the necessary plan and click **OK**.

For a plan to be displayed in the **Available Plans** list, it must be *ENABLED* as described in section [Running and Scheduling Storage Plans](#).

The screenshot shows the 'Schedule Plan' wizard with the 'Schedule Options' step selected. The left sidebar has 'Credentials', 'Schedule Options', and 'Summary'. The main area displays the following:

- Header:** You may schedule this Plan to run at a specific time, or chain it to be executed after another Plan runs. Recovery will be performed using the most recent restore point.
- Scheduled execution:** A toggle switch is set to 'On'.
- Schedule on:** An option with a radio button, showing a date/time picker for '11/16/2022 10:30 AM' and a calendar icon.
- Schedule after:** An option with a selected radio button, showing a link to 'Test Replica Plan'.
- Information box:** A blue 'i' icon followed by the text: 'You can schedule only the Failover and Restore actions for Orchestration Plans. Other actions (such as Failback) must be performed manually.'

At the bottom right are three buttons: 'Back', 'Next', and 'Cancel'.

- At the **Summary** step, review configuration information and click **Finish**.

The screenshot shows the 'Schedule Plan' wizard with the 'Summary' step selected. The left sidebar has 'Credentials', 'Schedule Options', and 'Summary'. The main area displays the following:

- Header:** Plan will be scheduled with below settings. Click Finish to apply.
- Copy to clipboard:** A link with a clipboard icon.
- Summary table:**

Plan name:	Storage Plan
Schedule:	Enabled
Ransomware Scan:	Disabled
Choose scheduling options:	After Plan: Restore plan

At the bottom right are three buttons: 'Back', 'Finish', and 'Cancel'.

TIP

You can disable a configured schedule if you no longer need it. To do that, set the **Scheduled execution** toggle to *Off* at the **Schedule Options** step of the **Schedule Plan** wizard.

Running Storage Failover

The **Run** action causes VMs in a plan to fail over to destination (NetApp) or secondary (HPE) storage volumes. For more information on the data recovery process, see the [NetApp ONTAP Documentation Center](#) and [Hewlett Packard Enterprise Support Center](#).

Running NetApp Storage Failover

To run a NetApp storage plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Run**.
-OR-
Click the plan name to switch to the **Plan Details** page, and click **Run**.
3. Complete the **Run Plan** wizard:
 - a. [This step applies only if you have not enabled the plan before running it]

At the **Plan Disabled** step, select the **Enable this Plan** check box.

The screenshot shows a 'Run Plan' wizard window with a dark blue header and a close button (X) in the top right corner. On the left is a vertical sidebar with a light blue background, containing the following steps: 'Plan Disabled' (highlighted with a blue bar), 'Credentials', 'Readiness Check', 'Snapshot Timestamp', 'Chained Plans', 'Reprotect Volumes', and 'Summary'. The main area of the wizard has a white background. At the top of this area, it says 'This Plan is disabled' in bold, followed by the text 'You may force the Plan into enabled mode to run it.' Below this text is a checkbox that is checked, with the label 'Enable this Plan' to its right. At the bottom right of the wizard, there are two buttons: a blue 'Next' button and a grey 'Cancel' button.

- b. For security purposes, at the **Credentials** step, retype your password.

The screenshot shows the 'Run Plan' dialog box with the 'Credentials' step selected in the left sidebar. The main area is titled 'Please re-enter credentials to proceed'. It contains two input fields: 'User name' with the value 'tech\wendy.may' and 'Password' with masked characters. An information icon and message state: 'If you launch the Run action for a plan, Orchestrator will attempt to transit the plan to the next logical state (Failover, Restore or Failback)'. At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

Run Plan	
Plan Disabled	Please re-enter credentials to proceed User name: tech\wendy.may Password: <i>If you launch the Run action for a plan, Orchestrator will attempt to transit the plan to the next logical state (Failover, Restore or Failback).</i>
Credentials	
Readiness Check	
Snapshot Timestamp	
Chained Plans	
Reprotect Volumes	
Summary	
<div>BackNextCancel</div>	

- c. At the **Readiness Check** step, review the results of the most recent readiness check run for the plan to make sure the plan will be able to complete successfully.

The screenshot shows the 'Run Plan' dialog box with the 'Readiness Check' step selected in the left sidebar. The main area is titled 'Review readiness check report'. It includes a 'Copy to clipboard' link, execution details (Executed: 11/17/2022 4:51 PM, Result: Success, Details: 0 Errors, 0 Warnings), and a 'Download report' link. An information icon and message state: 'It is highly recommended to run a readiness check before executing a plan.' At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

Run Plan	
Plan Disabled	Review readiness check report <a>Copy to clipboard Executed: 11/17/2022 4:51 PM Result: Success Details: 0 Errors, 0 Warnings <a>Download report <i>It is highly recommended to run a readiness check before executing a plan.</i>
Credentials	
Readiness Check	
Snapshot Timestamp	
Chained Plans	
Reprotect Volumes	
Summary	
<div>BackNextCancel</div>	

- d. At the **Snapshot Timestamp** step, select a snapshot that will be used to recover VMs.

To choose target storage systems to be used to recover VMs, Orchestrator will analyze settings specified during the configuration of storage recovery locations. For more information, see [How Orchestrator Places VMs During Storage Failover](#).

NOTE

This setting applies only to volumes protected by asynchronous replication. If a volume is protected by synchronous replication, Orchestrator will always use the most recent replicated data. This is a limitation of the synchronous SnapMirror technology.

The screenshot shows the 'Run Plan' dialog box with the 'Snapshot Timestamp' step selected in the left sidebar. The main area is titled 'Choose snapshot timestamp' and contains two radio button options: 'Use the most recent storage snapshot' (selected) and 'Use the most recent snapshot before: 11/18/2022 6:17 AM' (with a calendar icon). An information message states: 'Volumes that are protected with synchronous replication will always use the most recent data.' At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

Run Plan	
Plan Disabled	Choose snapshot timestamp <input checked="" type="radio"/> Use the most recent storage snapshot <input type="radio"/> Use the most recent snapshot before: 11/18/2022 6:17 AM <div> Volumes that are protected with synchronous replication will always use the most recent data.</div>
Credentials	
Readiness Check	
Snapshot Timestamp	
Chained Plans	
Reprotect Volumes	
Summary	
<div>BackNextCancel</div>	

- e. [This step applies only if you have any other orchestration plans scheduled to run after the plan completes]

At the **Chained Plans** step, select the **Also execute the chained plans** check box to proceed to execution of subsequent plans after the current plan enters the *FAILOVER* state.

The screenshot shows the 'Run Plan' dialog box with the 'Chained Plans' step selected in the left sidebar. The main area displays the text 'This Plan is part of a chain, and other Plans will execute when it is complete.' Below this, the checkbox 'Also execute the chained plans' is checked. A warning message with a yellow triangle icon states: 'Even Plans which are disabled will be forced to run. All Plans will all use the same restore point option.' At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

- f. At the **Reprotect Volumes** step, choose whether you want Orchestrator to trigger reverse replication to reprotect volumes included in the plan. This option can be useful if you plan to fail back to the production location.

If you select the **Trigger reverse replication to reprotect the failed-over volumes** check box, Orchestrator will add the **Protect Storage Volumes** step to the [list of plan steps](#). This step will resynchronize the data protection relationship in the reverse direction as soon as the storage failover process completes.

NOTE

When running the **Protect Storage Volumes** step, Orchestrator only triggers the reprotect operation and reports whether the step itself started successfully — Orchestrator does not check whether the operation of resynchronizing the relationship in the reverse direction completes successfully.

For more information on what a reprotect operation does, see the [NetApp ONTAP Documentation Center](#).

IMPORTANT

The **Protect Storage Volumes** step will interfere with the existing jobs that use storage snapshots in Veeam Backup & Replication. Since the step reverses the source and destination roles of SnapMirror relationships, these jobs will no longer function properly after the storage failover process completes.

To work around the issue, add the **Veeam Job Actions** step to the [list of pre-plan steps](#) before running the plan. To disable a job, specify its name when [configuring the step parameters](#).

g. At the **Summary** step, review configuration information and click **Finish**.

The plan goal is to reach the *FAILOVER* state. If any critical error is encountered, the plan will stop with the *HALTED* state. To learn how to work with *HALTED* storage plans, see [Managing Halted Plans](#).

TIP

After the storage failover process completes, Orchestrator will leave the plan in the *IN USE* state. By design, this makes the results of the storage failover process accessible in the Orchestrator UI as long as required, and also prevents the plan from being modified by any automatic updates related to infrastructure changes.

If you want to perform any further actions with the plan (for example, to test the plan, to run readiness checks or to execute the plan again), reset the plan as described in section [Resetting Storage Plans](#).

How Orchestrator Manages Storage Failover

Storage failover is a process of switching your virtual infrastructure from the source storage system in the production site to the destination storage system in the disaster recovery site. During storage failover, fully functional VMs are recovered to the required snapshots on the specified target storage system — as a result, you can access services and applications you need with minimum disruption.

Orchestrator orchestrates storage failover in the following way when running a NetApp storage plan:

1. Before Orchestrator starts processing [inventory groups included in the plan](#), it performs a number of pre-plan steps to prepare the failover environment:
 - a. Orchestrator runs the **VM Power Actions** step to shut down source VMs running in the production vCenter Server. To answer VM questions that appear while shutting the VMs down, Orchestrator applies default answers specified in the [vCenter Server settings](#).

The **VM Power Actions** step has a preconfigured timeout parameter that defines the exact amount of time for the step to execute. If step execution time exceeds the defined parameter value, Orchestrator powers the source VMs off.
 - b. Orchestrator runs the **Storage Failover** step. It breaks the SnapMirror relationship between the source and destination storage volumes, mounts the destination volumes to the target vCenter Server, and then mounts the recovered datastores to all hosts in the required storage recovery location.

For more information on the way Orchestrator identifies storage recovery locations required to recover datastores, see [How Orchestrator Places VMs During Storage Failover](#).
2. When processing inventory groups, Orchestrator registers target VMs on hosts in the disaster recovery site, and then powers the VMs on.

For more information on the way Orchestrator defines hosts where recovered VMs will be registered, see [How Orchestrator Places VMs During Storage Failover](#).
3. After Orchestrator finishes processing inventory groups, it performs a number of post-plan steps to finalize the storage failover process:
 - a. Orchestrator runs the **Unregister VMs** step to unregister source VMs from hosts in the production site.
 - b. Orchestrator runs the **Unmount Datastore** step to unmount the source volumes from the source vCenter Server.
 - c. [This step applies only if you have selected the **Reprotect storage volumes after failover** check box at the **Reprotect Volumes** step of the [Run Plan wizard](#)]

Orchestrator runs the **Protect Storage Volumes** step to reprotect volumes included in the plan by resynchronizing the data protection relationship in the reverse direction.

NOTE

When Orchestrator orchestrates storage failover, it handles specific internal elements under the hood — protection groups and storage items:

- A protection group is an object protected by storage replication. In terms of NetApp, it is a storage volume, either source or destination.
- A storage item is an object that can be connected to the target vCenter Server as a storage device or an NFS file share to create a datastore. In terms of NetApp, it is a volume, a LUN or a qtree.

Protection groups and storage items were introduced into Orchestrator to exclusively support the storage failover process. That is why the Orchestrator UI does not show these elements, but you may come across them in some reports and log entries.

How Orchestrator Places VMs During Storage Failover

To fail over VMs to destination storage volumes, Orchestrator performs the following steps:

1. The solution looks through all datastores included into the plan as [plan groups](#).

For each datastore, Orchestrator identifies a storage recovery location to be used to recover VMs whose disks are stored on this datastore, and mounts the recovered datastore to all hosts added to the storage recovery location as [compute resources](#).

TIP

If a datastore is protected by multiple storage systems, Orchestrator takes into account only those systems that are added to storage recovery locations as described in section [Adding Storage Recovery Locations](#).

This allows you to exclude unnecessary storage systems from the list of locations used to recover VMs.

If Orchestrator fails to mount any of the recovered datastores to any of the hosts, the plan halts. To learn how to manage halted storage plans, see [Managing Halted Storage Plans](#).

2. To define hosts where the recovered VMs will be registered, Orchestrator performs the following steps:
 - a. The solution looks through all hosts added to the storage recovery location as compute resources to detect a host that meets the following requirements:
 - The host is available
 - The required datastore is mounted to the host
 - b. Orchestrator applies the mapping specified in the [network mapping table](#) for the storage recovery location to define the required network configuration of the recovered VM.

The solution checks whether the network configuration of the detected host matches the required network configuration:

- If these configurations do not match, Orchestrator goes back to step 2A.
 - If these configurations do match, the first processed VM will be registered on this host.
- c. When Orchestrator starts processing the next VM, the solution looks through all hosts added to the location as compute resources to detect the next available host.

If Orchestrator detects such a host, this is the host where the VM will be registered. If there are no more available hosts, Orchestrator uses the host detected at step 2B to register the VM.
 - d. Orchestrator repeats step 2C for all other VMs included in the plan until all the VMs are registered. The order in which the VMs are processed depends on the [VM recovery options](#) defined while configuring the plan.

NOTE

The failure of steps 2A–2D for a VM from a [critical inventory group](#) halts the plan in the following cases:

- If none of the discovered hosts is available.
- If none of the hosts has network configuration that matches the required network configuration of the recovered VMs.

To learn how to work with *HALTED* storage plans, see [Managing Halted Plans](#).

Running HPE Storage Failover

TIP

After an HPE storage plan enters the *FAILOVER* state, you will have to [perform a number of additional steps](#) if you want to switch from the recovered VMs back to the VMs running on primary volumes. To make the failback process easier, it is recommended that you enable the auto synchronize option for the remote copy group before you run the plan. To learn how to enable the auto synchronize option, see the [Hewlett Packard Enterprise Support Center](#).

To run an HPE storage plan:

1. Select the plan. From the **Launch** menu, select **Run**.
-OR-
Click the plan name to switch to the **Plan Details** page, and click **Run**.
2. Complete the **Run Plan** wizard:
 - a. [This step applies only if you have not enabled the plan before running it]

At the **Plan Disabled** step, select the **Enable this Plan** check box.

The screenshot shows a 'Run Plan' wizard window with a dark blue header and a light blue sidebar. The sidebar contains the following steps: 'Plan Disabled' (selected), 'Credentials', 'Readiness Check', 'Chained Plans', and 'Summary'. The main content area has a title 'This Plan is disabled' and a subtitle 'You may force the Plan into enabled mode to run it.' Below this, there is a checkbox labeled 'Enable this Plan' which is checked. At the bottom right, there are two buttons: 'Next' (blue) and 'Cancel' (gray).

b. For security purposes, at the **Credentials** step, retype your password.

The screenshot shows the 'Run Plan' wizard window. The left sidebar contains a list of steps: 'Plan Disabled', 'Credentials' (highlighted in blue), 'Readiness Check', 'Chained Plans', and 'Summary'. The main area is titled 'Re-enter credentials to proceed' and contains two input fields: 'User name:' with the text 'tech\wendy.may' and 'Password:' with masked characters '••••••••'. A small eye icon is visible next to the password field. At the bottom right, there are three buttons: 'Back', 'Next' (highlighted in blue), and 'Cancel'.

NOTE

For HPE storage plans, the **Run Plan** wizard does not offer you to choose a restore point that will be used to recover VMs. By design, Orchestrator will always use the most recent replicated data. This is a limitation of HPE storage systems.

- c. At the **Readiness Check** step, review the results of the most recent readiness check run for the plan to make sure the plan will be able to complete successfully.

The screenshot shows the 'Run Plan' dialog box with the 'Readiness Check' step selected in the left sidebar. The main area displays the 'Review readiness check report' section. It includes a 'Copy to clipboard' button, execution details (Executed: 11/17/2022 11:50 AM, Result: Success, Details: 0 Errors, 0 Warnings), and a 'Download report' button. A warning message at the bottom states: 'It is highly recommended to run a readiness check before executing a plan.' Navigation buttons 'Back', 'Next', and 'Cancel' are at the bottom right.

Run Plan	
Plan Disabled	Review readiness check report Copy to clipboard Executed: 11/17/2022 11:50 AM Result: ✓ Success Details: 0 Errors, 0 Warnings Download report <div> It is highly recommended to run a readiness check before executing a plan.</div>
Credentials	
Readiness Check	
Chained Plans	
Summary	

Back Next Cancel

- d. [This step applies only if you have any other orchestration plans scheduled to run after the plan completes]

At the **Chained Plans** step, select the **Also execute the chained plans** check box to proceed to execution of subsequent plans after the current plan enters the *FAIL/OVER* state.

The screenshot shows the 'Run Plan' dialog box with the 'Chained Plans' step selected in the left sidebar. The main area displays the message 'This Plan is part of a chain, and other Plans will execute when it is complete.' Below this is a checked checkbox for 'Also execute the chained plans'. A warning message with an exclamation mark icon states: 'Even Plans which are disabled will be forced to run. All Plans will all use the same restore point option.' Navigation buttons 'Back', 'Next', and 'Cancel' are at the bottom right.

Run Plan	
Plan Disabled	This Plan is part of a chain, and other Plans will execute when it is complete. <input checked="" type="checkbox"/> Also execute the chained plans <div> Even Plans which are disabled will be forced to run. All Plans will all use the same restore point option.</div>
Credentials	
Readiness Check	
Chained Plans	
Summary	

Back Next Cancel

g. At the **Summary** step, review configuration information and click **Finish**.

The plan goal is to reach the *FAILOVER* state. If any critical error is encountered, the plan will stop with the *HALTED* state. To learn how to work with *HALTED* storage plans, see [Managing Halted Plans](#).

TIP

After the storage failover process completes, Orchestrator will leave the plan in the *IN USE* state. By design, this makes the results of the storage failover process accessible in the Orchestrator UI as long as required, and also prevents the plan from being modified by any automatic updates related to infrastructure changes.

If you want to perform any further actions with the plan (for example, to test the plan, to run readiness checks or to execute the plan again), reset the plan as described in section [Resetting Storage Plans](#).

How Orchestrator Manages Storage Failover

Storage failover is a process of switching your virtual infrastructure from the primary storage system in the production site to the secondary storage system in the disaster recovery site. During storage failover, fully functional VMs are recovered to the most recent restore points on the specified target storage system – as a result, you can access services and applications you need with minimum disruption.

Orchestrator orchestrates storage failover in the following way when running an HPE storage plan:

1. Before Orchestrator starts processing [inventory groups included in the plan](#), it performs a number of pre-plan steps to prepare the failover environment:
 - a. Orchestrator runs the **VM Power Actions** step to shut down source VMs running in the production vCenter Server. To answer VM questions that appear while shutting the VMs down, Orchestrator applies default answers specified in the [vCenter Server settings](#).

The **VM Power Actions** step has a preconfigured timeout parameter that defines the exact amount of time for the step to execute. If step execution time exceeds the defined parameter value, Orchestrator powers the source VMs off.
 - b. Orchestrator runs the **Storage Failover** step. It stops the remote copy group, performs failover on the remote copy group, mounts the secondary volumes to the target vCenter Server, and then mounts the recovered datastores to all hosts in the required storage recovery location.

For more information on the way Orchestrator identifies storage recovery locations required to recover datastores, see [How Orchestrator Places VMs During Storage Failover](#).
2. When processing inventory groups, Orchestrator registers target VMs on hosts in the disaster recovery site, and then powers the VMs on.

For more information on the way Orchestrator defines hosts where recovered VMs will be registered, see [How Orchestrator Places VMs During Storage Failover](#).
3. After Orchestrator finishes processing inventory groups, it performs a number of post-plan steps to finalize the storage failover process:
 - a. Orchestrator runs the **Unregister VMs** step to unregister source VMs from hosts in the production site.
 - b. Orchestrator runs the **Unmount Datastore** step to unmount the source volumes from the source vCenter Server.

NOTE

When Orchestrator orchestrates storage failover, it handles specific internal elements under the hood – protection groups and storage items:

- A protection group is an object protected by storage replication. In terms of HPE, it is a storage volume, either primary or secondary.
- A storage item is an object that can be connected to the target vCenter Server as a storage device to create a datastore. In terms of HPE, it is a volume or a LUN.

Protection groups and storage items were introduced into Orchestrator to exclusively support the storage failover process. That is why the Orchestrator UI does not show these elements, but you may come across them in some reports and log entries.

How Orchestrator Places VMs During Storage Failover

To fail over VMs to secondary storage volumes, Orchestrator performs the following steps:

1. The solution looks through all datastores included into the plan as [plan groups](#).

For each datastore, Orchestrator identifies a storage recovery location to be used to recover VMs whose disks are stored on this datastore, and mounts the recovered datastore to all hosts added to the storage recovery location as [compute resources](#).

TIP

If a datastore is protected by multiple storage systems, Orchestrator takes into account only those systems that are added to storage recovery locations as described in section [Adding Storage Recovery Locations](#).

This allows you to exclude unnecessary storage systems from the list of locations used to recover VMs.

If Orchestrator fails to mount any of the recovered datastores to any of the hosts, the plan halts. To learn how to manage halted storage plans, see [Managing Halted Storage Plans](#).

2. To define hosts where the recovered VMs will be registered, Orchestrator performs the following steps:
 - a. The solution looks through all hosts added to the storage recovery location as compute resources to detect a host that meets the following requirements:
 - The host is available
 - The required datastore is mounted to the host
 - b. Orchestrator applies the mapping specified in the [network mapping table](#) for the storage recovery location to define the required network configuration of the recovered VM.

The solution checks whether the network configuration of the detected host matches the required network configuration:

- If these configurations do not match, Orchestrator goes back to step 2A.
 - If these configurations do match, the first processed VM will be registered on this host.
- c. When Orchestrator starts processing the next VM, the solution looks through all hosts added to the location as compute resources to detect the next available host.

If Orchestrator detects such a host, this is the host where the VM will be registered. If there are no more available hosts, Orchestrator uses the host detected at step 2B to register the VM.
 - d. Orchestrator repeats step 2C for all other VMs included in the plan until all the VMs are registered. The order in which the VMs are processed depends on the [VM recovery options](#) defined while configuring the plan.

NOTE

The failure of steps 2A–2D for a VM from a [critical inventory group](#) halts the plan in the following cases:

- If none of the discovered hosts is available.
- If none of the hosts has network configuration that matches the required network configuration of the recovered VMs.

To learn how to work with *HALTED* storage plans, see [Managing Halted Plans](#).

Halting Storage Failover

The **Halt** action interrupts plan execution. Any steps currently executing will be completed, then the plan will enter the *HALTED* state. To learn how to work with *HALTED* storage plans, see [Managing Halted Plans](#).

To stop a running storage plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Halt**.
-OR-
Click the plan name to switch to the **Plan Details** page, and click **Halt**.
3. Complete the **Halt Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.

The screenshot shows a 'Halt Plan' wizard window with a dark blue header and a close button (X) in the top right corner. On the left is a vertical sidebar with three tabs: 'Credentials' (highlighted in blue), 'Schedule Impact' (in blue text), and 'Summary' (in grey text). The main area of the window is titled 'Re-enter credentials to proceed' and contains two input fields. The 'User name:' field is pre-filled with 'tech\olivia.dias'. The 'Password:' field contains a series of dots and has a small eye icon to its right for toggling visibility. At the bottom right of the window are two buttons: a blue 'Next' button and a grey 'Cancel' button.

- b. [This step applies only if you have any other orchestration plans scheduled to run after the plan completes]

At the **Schedule Impact** step, choose whether you want to proceed with or cancel execution of subsequent plans after the current plan enters the *HALTED* state.

The screenshot shows the 'Halt Plan' dialog box with the 'Schedule Impact' tab selected. The left sidebar contains 'Credentials', 'Schedule Impact', and 'Summary'. The main area has two radio buttons: 'Cancel the schedule and do not execute the subsequent Plans' (selected) and 'Continue the schedule and launch the next Plan now'. Below these is a warning message: 'There are other Plan(s) scheduled in a chain to failover after this Plan completes. Choose the options for those scheduled Plans below.' At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

- c. At the **Summary** step, review configuration information and click **Finish**.

The screenshot shows the 'Halt Plan' dialog box with the 'Summary' tab selected. The left sidebar contains 'Credentials', 'Schedule Impact', and 'Summary'. The main area displays the following information: 'Click Finish to halt the plan', a 'Copy to clipboard' button, and a table with the following details:

Plan name:	Storage Plan
Halted by:	tech\olivia.dias [Administrator]
Current state:	✓ Failover
Action:	Halt
Schedule Impact:	Restore Plan – Scheduled chain cancelled

Below the table is an information icon and a warning: 'Halting a plan before it reaches a stable state may cause your environment to enter an inconsistent state, requiring manual troubleshooting and a reset of the plan to resolve.' At the bottom right are 'Back', 'Finish', and 'Cancel' buttons.

Resetting Storage Plans

After you run a storage plan and it acquires the *FAILOVER* state, you must reset the plan if you wish to run it again (for example, to [perform failback](#)). The **Reset** action returns the plan to the *DISABLED* state and updates the Orchestrator database to reflect the changes made to the location of VMs included in the plan. The configuration of plan steps and their parameter settings in this case remain the same.

You may also require to reset a storage plan if the plan becomes inconsistent with the virtual environment. This will return the plan to the *DISABLED* state, without making any changes to the external virtual infrastructure.

To reset a storage plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Manage** menu, select **Reset**.
-OR-
Right-click the plan name and select **Manage > Reset**.
3. Complete the **Reset Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.

The screenshot shows the 'Reset Plan' wizard with the 'Credentials' step selected. The wizard has a sidebar with 'Credentials', 'Quick Check', and 'Summary'. The main area is titled 'Re-enter credentials to proceed' and contains fields for 'User name' (tech\olivia.dias) and 'Password' (masked with dots). A warning message states: 'Reset will take no actions on VMs or replicas in your infrastructure. It will reinitialize the Plan in Orchestrator only. For *Halted* plans it is recommended to use Undo, not Reset.' At the bottom right are 'Next' and 'Cancel' buttons.

Reset Plan	
Credentials	Re-enter credentials to proceed
Quick Check	User name: tech\olivia.dias
Summary	Password:
	i Reset will take no actions on VMs or replicas in your infrastructure. It will reinitialize the Plan in Orchestrator only. For <i>Halted</i> plans it is recommended to use Undo, not Reset.
	Next Cancel

- b. At the **Quick Check** step, select the **Perform a Quick Check after reset is complete** check box to run a **readiness check** after the reset.

The screenshot shows the 'Reset Plan' dialog box with the 'Quick Check' tab selected. The left sidebar contains 'Credentials', 'Quick Check', and 'Summary'. The main area displays the message 'It is recommended to run a Quick Check after resetting the plan' and a checked checkbox for 'Perform a Quick Check after reset is complete'. At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

Reset Plan	
Credentials	It is recommended to run a Quick Check after resetting the plan
Quick Check	<input checked="" type="checkbox"/> Perform a Quick Check after reset is complete
Summary	

Back Next Cancel

- c. At the **Summary** step, review configuration information and click **Finish**.

The screenshot shows the 'Reset Plan' dialog box with the 'Summary' tab selected. The left sidebar contains 'Credentials', 'Quick Check', and 'Summary'. The main area displays the message 'Plan will be reset using the options below. Press Finish to reset the Plan' and a 'Copy to clipboard' link. Below this, the configuration details are listed: Plan Name: Storage Plan, Reset by: TECH\olivia.dias [Administrator], Current State: - Failover (Halted, 83% complete, 1 error, no warnings), and Quick Check: Yes. At the bottom right are 'Back', 'Finish', and 'Cancel' buttons.

Reset Plan	
Credentials	Plan will be reset using the options below. Press Finish to reset the Plan
Quick Check	Copy to clipboard
Summary	<p>Plan Name: Storage Plan</p> <p>Reset by: TECH\olivia.dias [Administrator]</p> <p>Current State: - Failover (Halted, 83% complete, 1 error, no warnings)</p> <p>Quick Check: Yes</p>

Back Finish Cancel

Orchestrating Failback with NetApp Storage Plans

After you run a NetApp storage plan and want to fail back to VMs running on source volumes, you must perform the following steps:

1. Reset the plan as described in section [Resetting Storage Plans](#).
2. Wait approximately 5 minutes for Orchestrator to collect data on the updated configuration.
3. Run a readiness check to ensure the plan is ready for failback as described in section [Running Plan Readiness Check](#).
4. Run the plan again as described in section [Running Storage Failover](#).

TIP

If the **Reprotect storage volumes after failover** check box at the **Reprotect Volumes** step of the [Run Plan wizard](#) was not selected during the previous failover, you should first reverse the protection relationship between the source and destination volumes as described in the [NetApp ONTAP Documentation Center](#).

Orchestrating Failback with HPE Storage Plans

After you run an HPE storage plan and want to fail back to VMs running on primary volumes, you must perform the following steps:

1. Reset the plan as described in section [Resetting Storage Plans](#).
2. Wait approximately 5 minutes for Orchestrator to collect data on the updated configuration.
3. Run a readiness check to ensure the plan is ready for failback as described in section [Running Plan Readiness Check](#).
4. Run the plan again as described in section [Running Storage Failover](#).
5. Perform the start operation for the remote copy group as described in the Hewlett Packard Enterprise Support Center for [3PAR storage systems](#) and [Primera storage systems](#)

TIP

If you have not enabled the auto synchronize option for the remote copy group [before running the plan](#), you should also:

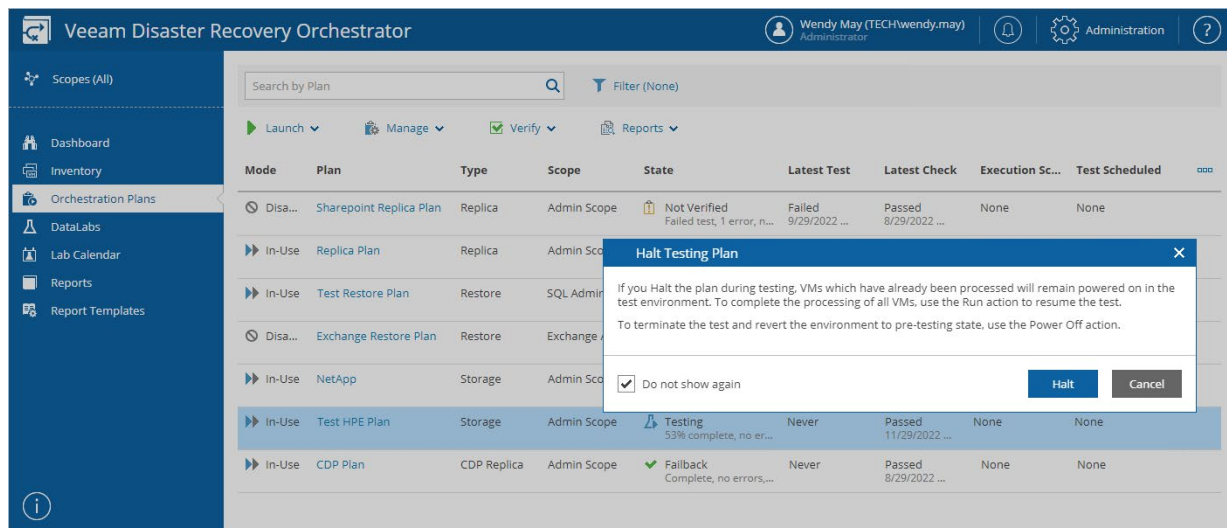
1. Perform the recover operation for the remote copy group as described in the Hewlett Packard Enterprise Support Center for [3PAR storage systems](#) and [Primera storage systems](#).
2. Connect to the target storage system through SSH and run the following command:
`setrcopygroup reverse -stopgroups -natural <remotecopygroupname>`
3. Perform the start operation for the remote copy group as described in the Hewlett Packard Enterprise Support Center for [3PAR storage systems](#) and [Primera storage systems](#).

Halting Plan Testing

The **Halt** action interrupts plan testing. You may need to halt plan testing, for example, if you need to fix some environment-related issues and then [proceed with testing later](#) (in this case, recovered VMs will still continue to run). Or you may need to stop the testing process completely, for example, if you no longer need to test the selected storage plan (in this case, recovered VMs will be deleted).

To halt testing of a storage plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Verify** menu, select **Halt DataLab Test**.
-OR-
Right-click the plan name and select **Verify > Halt DataLab Test**.
3. In the **Halt Testing Plan** window, click **Halt** to confirm the action.



To cancel testing of a storage plan:

1. Select the plan. From the **Verify** menu, select **Power Off DataLab Test**.
-OR-
Right-click the plan name and select **Verify > Power Off DataLab Test**.
2. In the **Power Off Testing Plan** window, click **Power Off** to confirm the action.

Veeam Disaster Recovery Orchestrator

Wendy May (TECHwendy.may)
Administrator
Administration

Scopes (All)

Dashboard
Inventory
Orchestration Plans
DataLabs
Lab Calendar
Reports
Report Templates

Search by Plan
Filter (None)

Launch
Manage
Verify
Reports

Mode	Plan	Type	Scope	State	Latest Test	Latest Check	Execution Sc...	Test Scheduled
Disa...	Sharepoint Replica Plan	Replica	Admin Scope	Not Verified Failed test, 1 error, n...	Failed 9/1/2021 2:32:...	Passed 8/27/2021 8:50...	None	None
In-Use	Replica Plan	Replica	Admin Scope	Permanent Failover Complete, no errors,...	Failed 9/1/2021 2:30:...	Passed 8/23/2021 2:31...	None	9/3/2021 3:30 AM
In-Use	Test Restore Plan	Restore	SQL Administ...	Testing Halted, 71% complet...	Failed	Warning	Run after 4HR	9/3/2021 3:30 AM
Disa...	Exchange Restore Plan	Restore	Exchange Ad...	Not Verified Failed check, no erro...				
In-Use	NetApp	Storage	Admin Scope	Failover Halted, 16% complet...				
In-Use	Test HPE Plan	Storage	Admin Scope	Testing 53% complete, no er...				
In-Use	CDP Plan	CDP Replica	Admin Scope	Failback Complete, no errors,...				

Power Off DataLab

If you run the Power Off action for a running DataLab, Orchestrator will power off the DataLab network appliance and revert the test environment to the pre-testing state.

Orchestrator will stop lab processing as soon as the currently executed step completes.

Power Off
Cancel

Managing Halted Storage Plans

If a critical step fails for a VM from a [critical inventory group](#), the plan may enter the *HALTED* state. To troubleshoot reasons why a plan failed, use the Plan Execution History Report generated as soon as the currently performed action completes. For more information on how to track plan performance history, see [Viewing Plan Execution History](#).

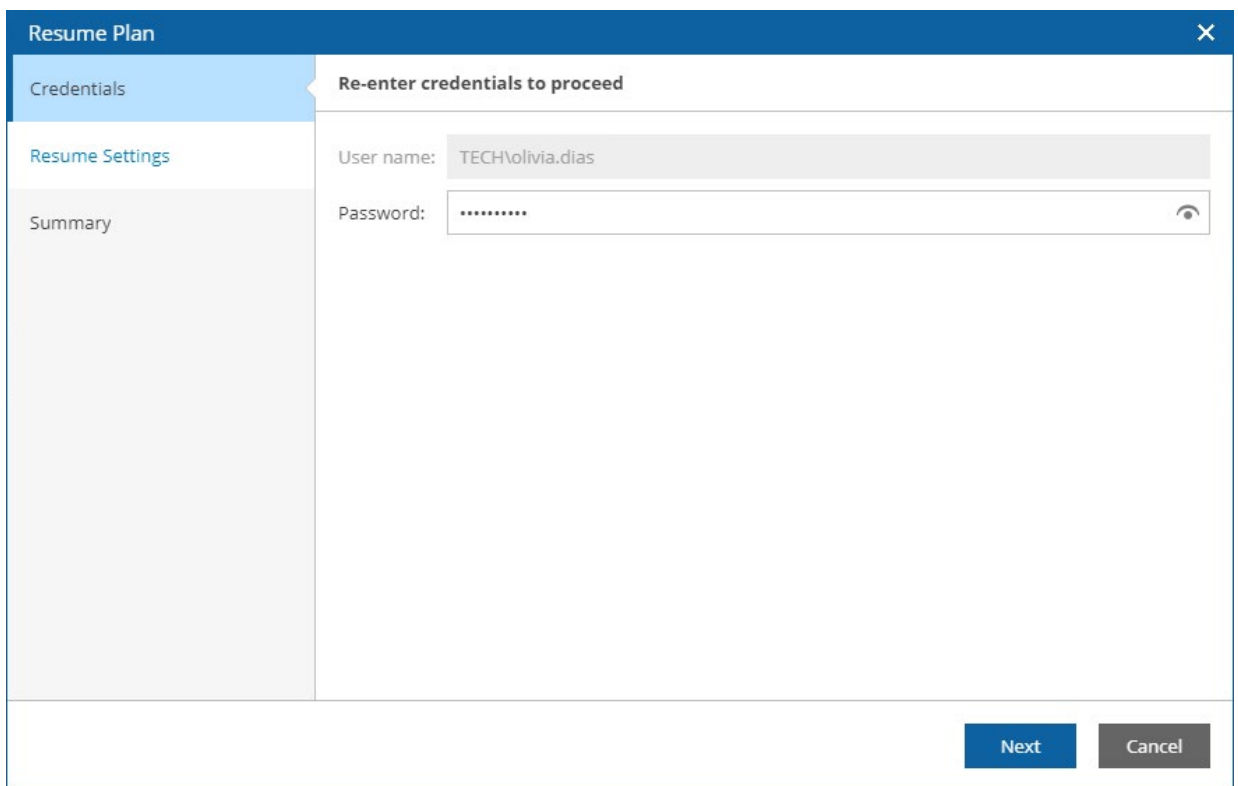
After you eliminate the problem that caused the plan to become *HALTED*, you have the following options to resume the plan:

- Repeat the last failed step.
- Proceed to the next step.

Running Halted Storage Plans

To run a *HALTED* storage plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Continue**.
-OR-
Click the plan name to switch to the **Plan Details** page, and click **Continue**.
3. Complete the **Run Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.



The screenshot shows a 'Resume Plan' dialog box with a blue header and a close button (X) in the top right corner. On the left, there is a sidebar with three tabs: 'Credentials' (selected and highlighted in blue), 'Resume Settings', and 'Summary'. The main area of the dialog is titled 'Re-enter credentials to proceed'. It contains two input fields: 'User name:' with the text 'TECH\volivia.dias' and 'Password:' with masked characters '*****'. A small eye icon is visible to the right of the password field. At the bottom right, there are two buttons: 'Next' (blue) and 'Cancel' (gray).

- b. At the **Resume Settings** step, select an option to resume plan execution.

Choose whether you want to proceed with plan execution from the next plan step or to retry the failed step.

NOTE

If you select the **Retry failed step** option, Orchestrator will execute the **Storage Failover** step again only in case the plan halts when trying to execute the **Register VM** step. For more information on steps performed by Orchestrator, see [Appendix. Orchestration Plan Steps](#).

The screenshot shows the 'Resume Plan' dialog box with the 'Resume Settings' tab selected. The left sidebar contains 'Credentials', 'Resume Settings', and 'Summary'. The main area is titled 'Choose one of the following options' and contains two radio button options: 'Retry failed step' (selected) and 'Proceed to next step'. Below the options is an information box stating: 'If VMs are being processed in parallel, then multiple failed steps may be retried.' At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

Resume Plan	
Credentials	Choose one of the following options
Resume Settings	<p><input checked="" type="radio"/> Retry failed step If the most recently executed step failed, it will be retried</p> <p><input type="radio"/> Proceed to next step The plan will proceed to the next step</p> <p>i If VMs are being processed in parallel, then multiple failed steps may be retried.</p>
Summary	
<div>Back Next Cancel</div>	

- c. At the **Summary** step, review configuration information and click **Finish**. The failover process will be started.

The screenshot shows the 'Resume Plan' dialog box with the 'Summary' tab selected. The left sidebar contains 'Credentials', 'Resume Settings', and 'Summary'. The main area is titled 'Click Finish to resume the plan' and contains a 'Copy to clipboard' button. Below this is a table of configuration information. At the bottom right are 'Back', 'Finish', and 'Cancel' buttons.

Resume Plan											
Credentials	Click Finish to resume the plan										
Resume Settings	<p> Copy to clipboard</p> <table><tr><td>Plan name:</td><td>NFS</td></tr><tr><td>Launched by:</td><td>TECH\olivia.dias [Administrator]</td></tr><tr><td>Reprotect:</td><td>Disabled i</td></tr><tr><td>Current state:</td><td>- Failover (Halted, 50% complete, 1 error, 1 warning)</td></tr><tr><td>Action:</td><td>Resume – Failover</td></tr></table>	Plan name:	NFS	Launched by:	TECH\olivia.dias [Administrator]	Reprotect:	Disabled i	Current state:	- Failover (Halted, 50% complete, 1 error, 1 warning)	Action:	Resume – Failover
Plan name:	NFS										
Launched by:	TECH\olivia.dias [Administrator]										
Reprotect:	Disabled i										
Current state:	- Failover (Halted, 50% complete, 1 error, 1 warning)										
Action:	Resume – Failover										
Summary											
<div>Back Finish Cancel</div>											

Resuming Plan Testing

To start the *HALTED* storage plan testing process:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Verify** menu, select **Continue DataLab Test**.

-OR-

Right-click the plan name and select **Verify > Continue DataLab Test**.

3. Complete the **Resume DataLab Test** wizard:
 - a. At the **Resume Test** step, select an option to resume test execution.

Choose whether you want to proceed with test execution from the next plan step or to retry the failed step.

The screenshot shows a dialog box titled "Resume DataLab Test" with a close button (X) in the top right corner. The dialog is divided into two main sections. On the left is a sidebar with two tabs: "Resume Test" (which is selected and highlighted in blue) and "Summary". The main area on the right contains the heading "You have the following options to resume this Plan test." Below this heading are two radio button options. The first option, "Retry failed", is selected with a filled radio button and includes the text "If the last executed step failed, it will be retried". The second option, "Proceed to next", is unselected with an empty radio button and includes the text "The plan will proceed to the next step". At the bottom right of the dialog, there are two buttons: a blue "Next" button and a grey "Cancel" button.

- b. At the **Summary** step, review configuration information and click **Finish**. The testing process will be started.

Resume DataLab Test

Resume Test

Summary

Your settings are summarized below

Plan Name:

Scope:

DataLab:

Plan State:

Action:

Resume by:

Replica Plan 01

Admin Scope

Testing Plan 01

Testing – Halted

Resume Testing

Retry failed Step

Back

Finish

Cancel

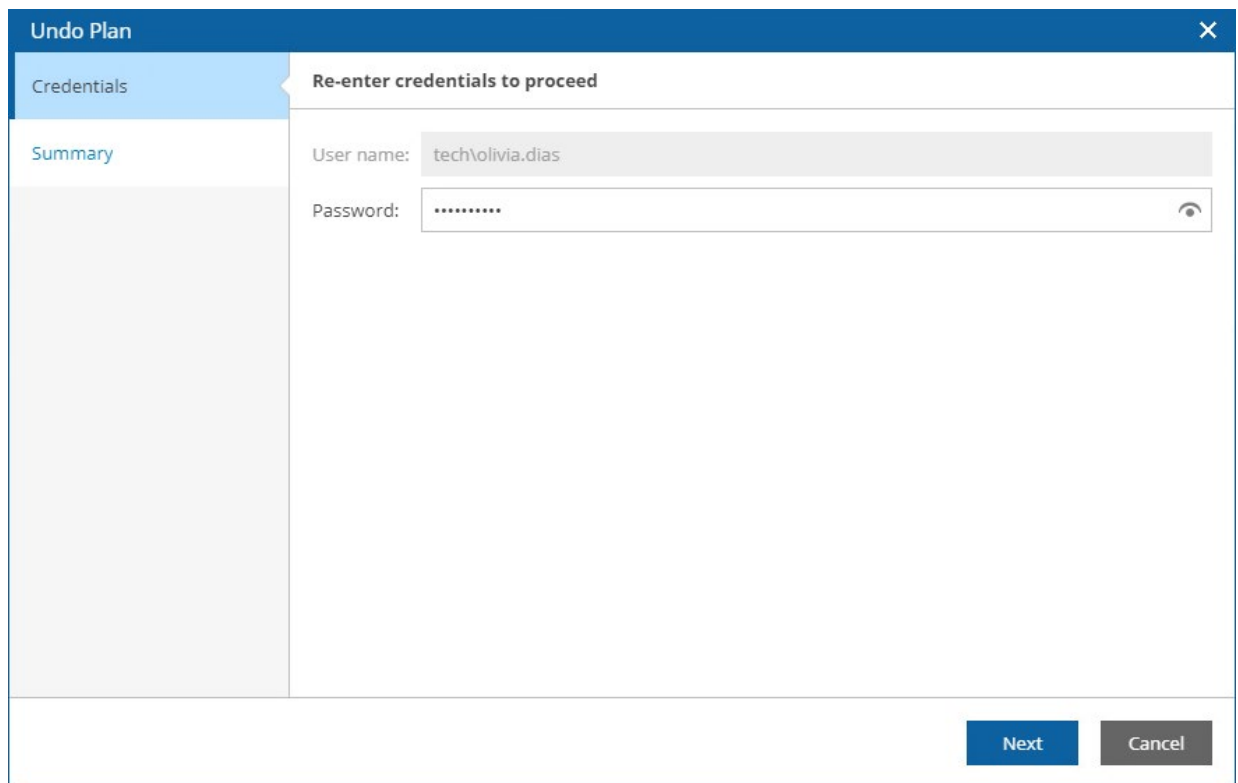
Undoing Halted Storage Plans

NOTE

This action is currently not supported for HPE storage systems.

To perform an undo operation for a *HALTED* storage plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Undo**.
-OR-
Click the plan name to switch to the **Plan Details** page, and click **Undo**.
3. Complete the **Undo Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.



The screenshot shows a web-based wizard titled "Undo Plan" with a close button (X) in the top right corner. The wizard has two tabs: "Credentials" (active) and "Summary". The "Credentials" tab contains the heading "Re-enter credentials to proceed". Below this, there are two input fields: "User name:" with the text "tech\olivia.dias" and "Password:" with masked characters "*****". A small eye icon is visible to the right of the password field. At the bottom right of the wizard, there are two buttons: "Next" (blue) and "Cancel" (gray).

b. At the **Summary** step, review configuration information and click **Finish**.

Undo Plan

Credentials

Summary

Click **Finish** to undo the most recent steps

Copy to clipboard

Plan name: Storage Plan

Undo by: TECH\olivia.dias [Administrator]

Current state: Failover (Halted, 83% complete, 1 error, no warnings)

Undo action: Undo Failover

i Undo will attempt to revert the plan to the last stable state. After undo is initiated:

- The run control will be disabled until the undo process has completed.
- The halt control may be used to halt the undo process.
- After halting use the undo control to resume the undo process.

During undo any errors will be ignored.

Back Finish Cancel

If a plan repeatedly enters the *HALTED* state due to misconfiguration or changes in the external environment, the only option left may be to **RESET** the plan.

Resetting Halted Storage Plans

To reset a *HALTED* storage plan, follow the instructions provided in section [Resetting Storage Plans](#).

NOTE

When you reset a storage plan, Orchestrator returns it to the *DISABLED* state without making any changes to the external virtual infrastructure. You may need to deal with any infrastructure reconfiguration manually.

Working with Cloud Plans

The type of an orchestration plan you create depends on whether you intend to use Orchestrator to switch to VM replicas, to restore machines from backups or backup copies, or to serve data from a destination (NetApp) or secondary (HPE) volume in case a disaster strikes.

If you want to recover machines from vSphere and Veeam agent backups to a cloud environment, create a cloud plan.

Creating Cloud Plans

To create a cloud plan:

1. Navigate to **Orchestration Plans**.
2. Click **Manage > New**.
3. Complete the **New Orchestration Plan** wizard:
 - a. [Specify a plan name and description](#).
 - b. [Choose a scope for the plan](#).
 - c. [Choose a type of the plan](#).
 - d. [Choose a recovery location](#).
 - e. [Include inventory groups in the plan](#).
 - f. [Specify VM recovery options](#).
 - g. [Add steps to the plan](#).
 - h. [Specify the target RTO and RPO](#).
 - i. [Select a template for plan reports](#).
 - j. [Specify scheduling options for plan reports](#).
 - k. [Finish working with the wizard](#).

Step 1. Specify Plan Name and Description

At the **Plan Info** step of the wizard, use the **Plan Name** and **Description** fields to enter a name for the new plan and to provide a description for future reference. The maximum length of the plan name is 64 characters; the following characters are not supported: * : / \ ? " < > | .

You can also provide a contact name, email and telephone number of a person responsible for the plan.

New Orchestration Plan

Plan Info

Scope

Plan Type

Recovery Location

VM Groups

VM Recovery Options

VM Steps

RTO & RPO

Report Template

Report Scheduling

Summary

Provide details for the new Orchestration Plan

Plan Name:

Cloud plan

Description:

Creating a test cloud plan

Contact Name:

John Smith

Contact Email:

john.smith@veeam.com

Contact Tel:

18002223344

Back

Finish

Cancel

Step 2. Choose Plan Scope

At the **Scope** step of the wizard, select a scope for which you want to create the plan.

For a scope to be displayed in the **Available Scopes** list, it must be created and customized as described in section [Managing Permissions](#).

New Orchestration Plan

Plan Info

Scope

Plan Type

Recovery Location

VM Groups

VM Recovery Options

VM Steps

RTO & RPO

Report Template

Report Scheduling

Summary

Choose a Scope

Type any part of Scope name to filter

Available Scopes

Admin Scope

Exchange Administrators

Back

Next

Cancel

Step 3. Choose Plan Type

At the **Plan Type** step of the wizard, select the **Cloud** option.

New Cloud Plan

Plan Info

Plan Type

Recovery Location

VM Groups

VM Recovery Options

VM Steps

RTO & RPO

Report Template

Report Scheduling

Summary

Choose the type of Plan

☒ Cloud

VMs will be recovered from Veeam agent or vSphere backups into a cloud environment

☐ CDP Replica

VMs will be recovered from Veeam CDP (continuous data protection) replicas

☐ Replica

VMs will be recovered from Veeam replicas

☐ Storage

VMs will be recovered from replicated storage volumes

☐ Restore

VMs will be recovered from Veeam agent or vSphere backups into a VMware vSphere environment

Back

Next

Cancel

Step 4. Select Recovery Location

At the **Recovery Location** step of the wizard, select a location to which inventory groups included in the plan will be restored.

For a recovery location to be displayed in the list of available locations, it must be created and included into the list of available inventory items, as described in section [Managing Recovery Locations](#).

New Cloud Plan

Plan Info

Scope

Plan Type

Recovery Location

VM Groups

VM Recovery Options

VM Steps

RTO & RPO

Report Template

Report Scheduling

Summary

Choose a default recovery location

Choose a recovery location where backups will be restored as new VMs.

Search by Recovery Location

Name

Description

Cloud Recovery Location

For restoring to Azure

i

You can change the recovery location when launching the Plan.

Back

Next

Cancel

Step 5. Add Inventory Groups

At the **VM Groups** step of the wizard, select inventory groups that you want to recover, and click **Add** to include them in the plan.

For an inventory group to be displayed in the **Available Groups** list, it must be included into the list of inventory items available for the scope, as described in section [Allowing Access to Inventory Groups](#).

Plan Info

Scope

Plan Type

Recovery Location

VM Groups

VM Recovery Options

VM Steps

RTO & RPO

Report Template

Report Scheduling

Summary

Add VM Groups

Use View VMs control to check Group members, and Up/Down controls to change the recovery sequence.

Search

Q

Available Groups

☐ Show empty Groups

MK (cdpvc) - mk_normlinux_5

owner - audrey.allen

owner - chloe.lewis

owner - Infrastructure

owner - joelle.van.dyne

owner - john.smith

owner - rick.deckard

owner - ryan.smith

owner - sara.baker

owner - shared

owner - stan.smith

owner - wendy.may

Veeam-InstantVMRecovery - RestAPITag

Add >

< Remove

Plan Groups

Datastore - mk_vol_5

Datastore - mk_vol_9

owner - hue.spenser

i

These options can be customized later on the Edit Plan page.

Back

Next

Cancel

Step 6. Specify VM Recovery Options

At the **VM Recovery Options** step of the wizard, use the **If the VM recovery encounters an error then** options to choose whether you want to halt plan execution if machine recovery fails. This option can also be customized later per-group [when editing the plan](#).

Use the **Recover the VMs in each group** options to choose whether you want to recover machines in sequence or in parallel. If you select to process machines simultaneously, use the **Recover simultaneously max of VMs** field to specify the maximum number of VMs processed at the same time.

The screenshot shows the 'New Cloud Plan' wizard with the 'VM Recovery Options' step selected in the left sidebar. The main content area is titled 'Customize the default recovery options for all VMs in the Plan'. It contains three sections: 'If the VM recovery encounters an error then' with radio buttons for 'Halt the plan' (selected) and 'Proceed with the plan'; 'Recover the VMs in each group' with radio buttons for 'In parallel' (selected) and 'In sequence'; and 'Recover simultaneously max of:' with a spinner box set to '10' and the unit 'VMs'. An information banner at the bottom states: 'These options can be customized later on the Edit Plan page.' At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

New Cloud Plan	
Plan Info	Customize the default recovery options for all VMs in the Plan
Scope	If the VM recovery encounters an error then
Plan Type	<input checked="" type="radio"/> Halt the plan
Recovery Location	<input type="radio"/> Proceed with the plan
VM Groups	Recover the VMs in each group
VM Recovery Options	<input checked="" type="radio"/> In parallel
VM Steps	<input type="radio"/> In sequence
RTO & RPO	Recover simultaneously max of: 10 VMs
Report Template	<i>These options can be customized later on the Edit Plan page.</i>
Report Scheduling	
Summary	
<div>Back Next Cancel</div>	

Step 7. Add Plan Steps

At the **VM Steps** step of the wizard, use the list of plan steps to select steps to be performed for each machine during cloud restore.

For a step to be displayed in the **Available Steps** list, it must be included into the list of inventory items available for the scope, as described in section [Allowing Access to Plan Steps](#).

IMPORTANT

To allow the cloud restore process to perform successfully, the **Create Cloud VM** step must execute first.

By default, Orchestrator will perform the same selected steps in the same order for all new machines that will later appear in the inventory groups included in the plan. However, you can change the step execution order and modify the list of steps individually for each machine, as described in section [Configuring Steps](#).

NOTE

If a VM is included in multiple inventory groups in the same plan, Orchestrator will only run the **Create Cloud VM** step once. However, other steps for this VM will execute when processing it in each group.

New Cloud Plan

Plan Info

Scope

Plan Type

Recovery Location

VM Groups

VM Recovery Options

VM Steps

RTO & RPO

Report Template

Report Scheduling

Summary

Choose VM Steps

Add Steps to be executed for all VMs in the Plan. These Steps will also be used for all new VMs added to the Plan in the future.

Search

Q

Up

Down

Available Steps

Create Cloud VM

Generate Event

Hello world

Send Email

Shutdown Source VM

VM Power Actions

Add >

< Remove

Selected Steps

Create Cloud VM

Shutdown Source VM

Send Email

i

These options can be customized later on the Edit Plan page.

Back

Next

Cancel

291 | Veeam Disaster Recovery Orchestrator | Operations Guide

Step 8. Specify Target RTO and RPO

At the **RTO & RPO** step of the wizard, define your Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for the plan:

- The **Target RPO** defines the maximum acceptable period of data loss.
- The **Target RTO** represents the amount of time it should take to recover from an incident.

NOTE

If you choose to perform ransomware scan [while running the plan](#), Orchestrator will scan one disk per repository mount server at a time. This process may take a while, affecting the plan RTO.

RTO and RPO performance will be recorded in the [Plan Readiness Check](#), [Plan Execution](#) and [DataLab Test](#) reports, and you will be able to track the achieved RTO and RPO objectives for each plan on the [Home Page Dashboard](#).

The screenshot shows the 'New Cloud Plan' wizard with the 'RTO & RPO' step selected in the left sidebar. The main area is titled 'Define your Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for this plan'. It contains two sets of spinner controls. The 'Target RTO' is set to 1 hour, 0 minutes, and 0 seconds, with a description 'Maximum allowed time before the service is restored after a failure.' The 'Target RPO' is set to 24 hours, 0 minutes, and 0 seconds, with a description 'Maximum allowed loss of historical data after a failure.' At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

Field	Hours	Minutes	Seconds	Description
Target RTO	1	0	0	Maximum allowed time before the service is restored after a failure.
Target RPO	24	0	0	Maximum allowed loss of historical data after a failure.

Step 9. Select Report Template

At the **Report Template** step of the wizard, select a document template that will be used as the cover page for all Orchestrator reports. Use options in the **Document format** list to choose whether you want to generate documents in the DOCX or PDF format.

For a custom document template to be displayed in the **Available Templates** list, it must be created and customized as described in section [Managing Templates](#).

New Cloud Plan

Plan Info

Scope

Plan Type

Recovery Location

VM Groups

VM Recovery Options

VM Steps

RTO & RPO

Report Template

Report Scheduling

Summary

Choose the report template to be used for Plan reports and documentation

Type any part of name to filter

Available Templates

Veeam Default Template (DE)
Dieses Template ist ein Beispiel und sollte auf Ihre Bedürfnisse angepasst werden

Veeam Default Template
This is an example template, and should be cloned and customized to your requirements

Veeam Default Template (ES)
Esta es una plantilla de ejemplo, y debe ser clonada y personalizada de acuerdo con sus requisitos

Veeam Default Template (FR)
Ceci est un modèle qui doit être cloné et personnalisé selon vos besoins

Veeam Default Template (PT)
Este é um template de exemplo, e deve ser clonado e customizado de acordo com seus requerimentos

Veeam Default Template (CH)
这是一个示例模板，应进行复制并根据您的要求定制

Veeam Default Template (JP)
こちらはサンプル・テンプレートです。コピーして、要件に応じてカスタマイズしてください

Document format: ☒ PDF file
☐ Word document (.DOCX)

Back

Next

Cancel

Step 10. Specify Report Scheduling Options

At the **Report Scheduling** step of the wizard, choose whether you want to automatically generate the [Plan Definition](#) and [Plan Readiness Check](#) reports for the plan on a daily schedule. You can also choose whether you want to generate both reports immediately after you create the plan.

To specify the exact time at which the report will be generated, click the **Schedule** icon next to the **Update Plan Definition report daily at** or **Perform Plan Readiness Check daily at** check box, set the desired time, and click **Apply**.

New Cloud Plan

Plan Info

Scope

Plan Type

Recovery Location

VM Groups

VM Recovery Options

VM Steps

RTO & RPO

Report Template

Report Scheduling

Summary

Choose scheduling options for automatic Plan reporting

☒ Update Plan Definition report daily at: 9:42 AM

☒ Perform Plan Readiness Check daily at: 8:45 AM

i Reports will not be generated for plan

☒ Create Plan Definition when I click Finish

☒ Perform Readiness Check when I click Finish

Hours: 8 Minutes: 45

☒ AM ☐ PM

Apply **Cancel**

Back **Next** **Cancel**

Step 11. Finish Working with Wizard

At the **Summary** step of the wizard, review configuration information and click **Finish**.

The screenshot shows the 'New Cloud Plan' wizard in the Summary step. The left sidebar contains a list of steps: Plan Info, Scope, Plan Type, Recovery Location, VM Groups, VM Recovery Options, VM Steps, RTO & RPO, Report Template, Report Scheduling, and Summary. The Summary step is currently selected and highlighted. The main area displays a summary of the configuration for the new plan, with a 'Copy to clipboard' button at the top. The summary is organized into two columns: configuration items on the left and their values on the right. At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

See below for a summary for the new Plan	
Plan Name:	Cloud plan
Scope:	Admin Scope
Plan Type:	Cloud
VM Group(s):	Datastore - esx01-das1 owner - chloe.lewis Datastore - esx02-das2
Recovery Location:	Cloud Recovery Location (IVR Enabled - No)
Recover VMs:	Simultaneously (max 10)
If any VM fails:	Halt the plan
Steps for New VM Template:	Create Cloud VM Shutdown Source VM Send Email
Override Credentials:	No
Credentials:	Use Default
Target RTO:	1 Hour
Target RPO:	24 Hours
Report Template, format:	Veeam Default Template, PDF
Update Plan Definition report:	Daily 9:42 AM
Perform Readiness Check:	Daily 8:45 AM
Create Plan Definition report now:	Yes
Run Readiness Check now:	Yes

Editing Cloud Plans

If you want to specify granular settings not provided in the [New Orchestration Plan wizard](#), the Orchestrator UI allows you to customize cloud plans and configure the settings for groups, recovered VMs, plan steps and step parameters.

The procedures to edit replica, CDP replica, restore, storage and cloud plans are almost identical. For more information, see [Editing Orchestration Plans](#).




Running and Scheduling Cloud Plans

After you create and configure a cloud plan, run a successful [readiness check](#), the plan can be considered ready for restore. You can invoke various actions for the plan, depending on the current plan state.





Point in Time	Actions
New plan created	After plan creation, you can: <ul style="list-style-type: none">• Schedule a time for the plan to execute restore.• Run the plan to execute restore immediately.
Any	At any point, you can: <ul style="list-style-type: none">• Halt the plan to interrupt its execution.• Reset the plan to clear the current state and allow it to run again.

Plan States














Cloud plans can acquire the following **default** states after creation. The same states are shown after resetting a plan and after completing a check.

Plan State	Icon	Description
NOT VERIFIED		Plan has never passed a readiness check or has been changed since the last readiness check.
		Plan has failed to pass a readiness check.
VERIFIED		Plan has successfully passed a readiness check.

Cloud plans can reach the following **stable** states after completing current processing:

Plan State	Icon	Description
HALTED		Plan has stopped due to either an error or user intervention.
RESTORED		Restore process completed successfully.
		Restore process completed with one or more warnings.
		Restore process completed with one or more errors.




Cloud plans can acquire the following **active** states while in use or in progress:

Functionality	Tab	Plan Operator
Plan Management		
CREATING		Plan is being created.
EDITING		Plan is being edited.
SAVING		Plan is being saved. Note: Plan editing and execution are not available in this state.
RESETTING		Plan is being reset.
DELETING		Plan is being deleted.
Readiness Checks		
CHECKING		Plan readiness check is in progress.
		Plan readiness check is in progress; one or more warnings encountered.
		Plan readiness check is in progress; one or more errors encountered.
CHECK HALTING		Plan readiness check is halting.
Execution		
RESTORE		Plan is executing.
		Plan is executing; one or more warnings encountered.
		Plan is executing; one or more errors encountered.
HALTING		Plan is halting.

NOTE

If you perform any infrastructure configuration changes (add, delete or rename VMs) or changes to Veeam ONE Client groups, Orchestrator will not automatically apply these changes to plans that are currently executing or testing — such plans are 'locked' and cannot be edited. The changes will take effect only if the plans enter the *VERIFIED* or *NOT VERIFIED* state.

Cloud plans can acquire the following **modes**:

Plan Mode	Icon	Description
ENABLED		Plan is ready to be verified and executed. Notes: Plan editing is not available. Automatic report updates are enabled.
DISABLED		Plan is ready to be edited. Notes: Scheduled plan execution is not available. Automatic report updates are disabled.
IN USE		Plan is either in one of the active states (except the <i>EDITING</i> state) or in one of the stable states. Notes: Plan editing is not available. Automatic report updates are disabled.

Before You Begin

To run a restore plan, it must be *ENABLED*. To enable a plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan.
3. From the **Manage** menu, select **Enable**.

If you do not enable a plan before you run it, the [Run Plan](#) wizard will force you to do that as soon as you try running the plan.

NOTES

1. An Orchestrator Administrator or Plan Author can force-enable a plan in the **Run Plan** wizard. However, a Plan Operator will not be able to run a disabled replica plan.
For more information on roles that can be assigned to users and user groups working with the Orchestrator UI, see [Managing Permissions](#).
2. For security purposes, all 'real-world' actions associated with restore plans require password confirmation.

Scheduling Cloud Restore

You can schedule a time for a cloud plan to execute. Only the restore process can be scheduled — all other operations must be performed manually in the Orchestrator UI.

To schedule a cloud plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Schedule**.
-OR-
Right-click the plan name and select **Launch > Schedule**.
3. Complete the **Schedule Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.

The screenshot shows the 'Schedule Plan' wizard with the 'Credentials' step selected. The left sidebar contains 'Credentials', 'Schedule Options', 'Ransomware Scan', and 'Summary'. The main area is titled 'Re-enter credentials to proceed' and contains a 'User name' field with 'tech\olivia.dias' and a 'Password' field with masked characters. An information icon and message state: 'For the plan to run according to the specified schedule, the plan must be enabled.' At the bottom right are 'Next' and 'Cancel' buttons.

- b. At the **Schedule Options** step, set the **Scheduled execution** toggle to *On*, and choose whether you want to run the plan on schedule or after any other plan.
 - If you want to run the plan at a specific time, select the **Schedule on** option, click the **Schedule** icon, set the desired date and time, and click **Apply**.

- If you want to run the plan after another plan, select the **Schedule after** option and click **Choose a Plan**. Then, in the **Select Plan** window, select the necessary plan and click **OK**.

For a plan to be displayed in the **Available Plans** list, it must be *ENABLED* as described in section [Running and Scheduling Restore Plans](#).

- c. At the **Ransomware Scan** step, choose whether you want to check restore points created for machines included in the plan for possible ransomware.

By default, Orchestrator checks 10 recently created restore points for each machine and halts the plan if all the restore points are infected. However, you can specify the maximum number of restore points to check and instruct Orchestrator to connect the machine to a quarantine network if no clean restore point is found. For more information on ransomware scan, see [How Orchestrator Performs Ransomware Scan](#).

For more information on ransomware scan, see [How Orchestrator Performs Ransomware Scan](#).

IMPORTANT

- Ransomware scan is supported only for Windows-based machines.
- Ransomware scan is not supported for restore points stored in object storage repositories.

The screenshot shows the 'Schedule Plan' wizard with the 'Ransomware Scan' step selected. The left sidebar contains links for 'Credentials', 'Schedule Options', 'Ransomware Scan', and 'Summary'. The main content area is titled 'Specify ransomware scan options' and includes a description: 'Scan restore points for viruses, malware and ransomware using Veeam Secure Restore. Virus-scanning can iterate through multiple restore points, starting with the most recent, until a clean point is found. For more information see the [User Guide](#).' Below this, there is a checkbox 'Scan a maximum of' which is checked, followed by a numeric input field set to '10' and a dropdown arrow, and the text 'previous restore points'. Under the heading 'If no clean restore point found', there are two radio button options: 'Cancel the restore and proceed to the next step' (which is selected) and 'Complete the restore but do not connect the VM to the network'. At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

d. At the **Summary** step, review configuration information and click **Finish**.

The screenshot shows the 'Schedule Plan' wizard with the 'Summary' step selected. The left sidebar contains links for 'Credentials', 'Schedule Options', 'Ransomware Scan', and 'Summary'. The main content area is titled 'Plan will be scheduled with below settings. Click Finish to apply'. Below this title is a 'Copy to clipboard' icon and text. A list of settings is displayed: 'Plan name: Cloud Plan', 'Schedule: Enabled', 'Ransomware Scan: Enabled', 'Restore points to scan (max): 10', 'If no clean restore point found: Cancel restore', and 'Choose scheduling options: After Plan: Exchange Restore Plan'. At the bottom right, there are three buttons: 'Back', 'Finish', and 'Cancel'.

TIP

You can disable a configured schedule if you no longer need it. To do that, set the **Scheduled execution** toggle to *Off* at the **Schedule Options** step of the **Schedule Plan** wizard.

Running Cloud Restore

The **Run** action causes machines in a plan to recover from their backup files. For more information on the data recovery process, see the Veeam Backup & Replication User Guide, section [Data Recovery](#).

TIP

If the Veeam Backup & Replication server that protects plan machines becomes unavailable, the plan will fail to complete successfully. However, in case the repository that stores the required backup files is still available, you will be able to work around the issue. To do that, [connect the repository to any other Veeam Backup & Replication server](#) added to Orchestrator, and [perform the rescan operation](#) for this repository.

To run a cloud plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Run**.
-OR-
Click the plan name to switch to the **Plan Details** page, and click **Run**.
3. Complete the **Run Plan** wizard:
 - a. [This step applies only if you have not enabled the plan before running it]

At the **Plan Disabled** step, select the **Enable this Plan** check box.

The screenshot shows the 'Run Plan' wizard window. The left sidebar contains a list of steps: 'Plan Disabled' (selected), 'Credentials', 'Readiness Check', 'Recovery Location', 'Restore Point', 'Chained Plans', 'Ransomware Scan', and 'Summary'. The main area displays the 'Plan Disabled' step with the message 'This Plan is disabled' and 'You may force the Plan into enabled mode to run it.' Below this message is a checkbox labeled 'Enable this Plan' which is checked. At the bottom right, there are 'Next' and 'Cancel' buttons.

- b. For security purposes, at the **Credentials** step, retype your password.

The screenshot shows the 'Run Plan' dialog box with the 'Credentials' step selected in the left sidebar. The main area is titled 'Re-enter credentials to proceed'. It contains two input fields: 'User name:' with the text 'tech\olivia.dias' and 'Password:' with masked characters '*****'. A small eye icon is visible next to the password field. At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

- c. At the **Readiness Check** step, review the results of the most recent readiness check run for the plan to make sure the plan will be able to complete successfully.

The screenshot shows the 'Run Plan' dialog box with the 'Readiness Check' step selected in the left sidebar. The main area is titled 'Review readiness check report'. It contains a 'Copy to clipboard' link, a summary of the check results, and a 'Download report' link. The summary shows: 'Executed: 1/27/2023 8:10 AM', 'Result: Warning' (with a warning icon), and 'Details: 0 Errors, 1 Warning'. At the bottom, there is an information icon and a message: 'It is highly recommended to run a readiness check before executing a plan.' At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

- d. At the **Recovery Location** step, select a location to which inventory groups included in the plan will be restored.

For a recovery location to be displayed in the list of available locations, it must be created and included into the list of inventory items available for the scope, as described in section [Managing Recovery Locations](#).

Name	VMs	Agents	Instant VM Recovery
Original VM Location	Enabled	Disabled	Disabled
Gold	Enabled	Enabled	Enabled

Buttons: Back, Next, Cancel

If the selected recovery location includes multiple hosts, datastores and networks, Orchestrator will use the round-robin algorithm to restore machines added to the plan. For more information, see [How Orchestrator Places VMs During Cloud Restore](#).

- e. At the **Restore Point** step, choose a restore point that will be used to recover machines.

IMPORTANT

Recovering data from the archive tier is not supported. If you select the **Use most recent Restore Point before** option, make sure to choose a restore point that is stored in either the capacity or the performance tier. For more information on Veeam Backup & Replication tiering options, see the Veeam Backup & Replication User Guide, section [Scale-Out Backup Repository](#).

The screenshot shows the 'Run Plan' dialog box with the 'Restore Point' step selected in the left sidebar. The main area is titled 'Choose restore point' and contains two radio button options: 'Use the latest Restore Point' (which is selected) and 'Use most recent Restore Point before: 11/15/2022 10:44 AM' (with a calendar icon). At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

- f. [This step applies only if you have any other orchestration plans scheduled to run after the plan completes]

At the **Chained Plans** step, select the **Also execute the chained plans** check box to proceed to execution of subsequent plans after the current plan enters the *RESTORED* state.

The screenshot shows the 'Run Plan' dialog box with the 'Chained Plans' step selected in the left sidebar. The main area has a header stating 'This Plan is part of a chain, and other Plans will execute when it is complete.' Below this is a checked checkbox labeled 'Also execute the chained plans'. A warning message with a yellow triangle icon states: 'Even Plans which are disabled will be forced to run. All Plans will all use the same restore point option.' At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

- g. At the **Ransomware Scan** step, choose whether you want to check restore points created for machines included in the plan for possible ransomware.

By default, Orchestrator checks 10 recently created restore points for each machine and halts the plan if all the restore points are infected. However, you can specify the maximum number of restore points to check and instruct Orchestrator to connect the machine to a quarantine network if no clean restore point is found.

For more information on ransomware scan, see [How Orchestrator Performs Ransomware Scan](#).

IMPORTANT

- Ransomware scan is supported only for Windows-based machines.
- Ransomware scan is not supported for restore points stored in object storage repositories.

The screenshot shows the 'Run Plan' dialog box with the 'Ransomware Scan' step selected in the left sidebar. The main area is titled 'Specify ransomware scan options'. It contains a checkbox 'Scan a maximum of' with a value of '10' and the text 'previous restore points'. Below this, it says 'If no clean restore point found' and provides two radio button options: 'Cancel the restore and proceed to the next step' (selected) and 'Complete the restore but do not connect the VM to the network'. At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

Plan Disabled	Credentials	Readiness Check	Recovery Location	Restore Point	Ransomware Scan	Summary
Specify ransomware scan options Scan restore points for viruses, malware and ransomware using Veeam Secure Restore. Virus-scanning can iterate through multiple restore points, starting with the most recent, until a clean point is found. For more information see the User Guide .						
<input checked="" type="checkbox"/> Scan a maximum of <input type="text" value="10"/> previous restore points						
If no clean restore point found						
<input checked="" type="radio"/> Cancel the restore and proceed to the next step						
<input type="radio"/> Complete the restore but do not connect the VM to the network						
<div>BackNextCancel</div>						

h. At the **Summary** step, review configuration information and click **Finish**.

The screenshot shows the 'Run Plan' dialog box with the 'Summary' step selected in the left sidebar. The main area is titled 'Click Finish to run the plan'. It contains a 'Copy to clipboard' button and a 'Plan information' section with the following details: Plan name: Cloud Plan, Launched by: tech\olivia.dias [Administrator], Current state: Not Verified (Failed check, no errors, 1 warning), Action: Failover, Restore Point: Most Recent, Chained Plans: Execute, Recovery Location: Cloud RL, and Restore VM Tags: No. Below this is a 'Ransomware scan' section with: Ransomware Scan: Enabled, Restore points to scan (max): 10, and If no clean restore point found: Cancel restore. At the bottom right are 'Back', 'Finish', and 'Cancel' buttons.

Plan Disabled	Credentials	Readiness Check	Recovery Location	Restore Point	Chained Plans	Ransomware Scan	Summary
Click Finish to run the plan							
<div>Copy to clipboard</div>							
Plan information							
Plan name: Cloud Plan							
Launched by: tech\olivia.dias [Administrator]							
Current state: Not Verified (Failed check, no errors, 1 warning)							
Action: Failover							
Restore Point: Most Recent							
Chained Plans: Execute							
Recovery Location: Cloud RL							
Restore VM Tags: No							
Ransomware scan							
Ransomware Scan: Enabled							
Restore points to scan (max): 10							
If no clean restore point found: Cancel restore							
<div>BackFinishCancel</div>							

The plan goal is to reach the *RESTORED* state. If any critical error is encountered, the plan will stop with the *HALTED* state. To learn how to work with *HALTED* restore plans, see [Managing Halted Plans](#).

How Orchestrator Places VMs During Cloud Restore

To restore machines included into a cloud plan to a new cloud recovery location, Orchestrator uses the following algorithm:

1. Orchestrator checks the connection to the [selected backup server](#) and the availability of the [Azure subscription on the server](#).
2. Orchestrator checks the connections to [all backup repositories](#) that store restore points of all machines added to the plan.

If the list of selected repositories contains a cloud repository, Orchestrator also checks whether the [region specified for the recovery location](#) matches the repository region. If the regions do not match, Orchestrator notifies that the recovery process will involve cross-region data transfer.
3. Orchestrator checks whether the [configured backup proxies](#) are connected to the selected Veeam Backup & Replication server.
4. Orchestrator checks whether the [selected resource group](#) is still present in Microsoft Azure.
5. Orchestrator applies the mapping specified in the [network mapping table](#) for the location to set the required network configuration of the first processed machine. Orchestrator also checks whether the network configuration of the source machine matches the required network configuration.

NOTE

The failure of steps 1–5 for a machine from a [critical inventory group](#) halts the plan in the following cases:

- If the selected Veeam Backup & Replication server is not available.
- If the source machine does not have network configuration that matches the required network configuration of the recovered VM.
- If the backup repository that stores restore points of the processed machine is not available.
- If none of the configured backup proxies is available.
- If the selected resource group is not present in Microsoft Azure.

To learn how to work with *HALTED* cloud plans, see [Managing Halted Plans](#).

6. Orchestrator verifies whether the VM configuration specified when [creating the recovery location](#) matches the VM configuration specified when [configuring the plan step parameters](#). It also checks whether the VM series in the VM configuration is available in the selected region and whether the machine can be restored using these series:
 - If the number of machine disks exceeds the maximum number of disks supported for the selected series, the plan halts.
 - If the number of CPUs or the amount of RAM required for the recovered VM exceeds the series capacity, Orchestrator displays a warning notifying that the maximum amount of available resources will be used for recovery.
7. Orchestrator repeats steps 5 and 6 for all other machines included in the plan until all the machines are restored. The order in which the machines are processed depends on the **VM Recovery Options** defined [while configuring the plan](#).

How Orchestrator Performs Ransomware Scan

Before you run a cloud plan to recover a machine to the production environment, Orchestrator allows you to perform ransomware scan for the protected machine using [Veeam Secure Restore](#).

When running a cloud plan, Orchestrator performs ransomware scan in the following way:

1. Disks of the machine that is being restored are mounted to the [mount server](#).
2. On the mount server, antivirus software is triggered to scan files from the mounted disks.
3. Orchestrator iterates through the number of restore points [specified while running the plan](#) one by one to detect a restore point with no viruses.
4. If a clean restore point is detected, Orchestrator successfully restores the machine to the selected recovery location.

If no clean restore point is detected, Orchestrator either halts the plan or restores the machine to a quarantine network depending on the [configured restore point settings](#).

NOTE

If restore points of all machines included in the plan are stored in one repository, Orchestrator will process machines one by one. This process may take a while, affecting the plan RTO.

The results of ransomware scan are included in the [Readiness Check](#) and [Plan Execution](#) reports.

Requirements and Limitations for Ransomware Scan

To allow Orchestrator to perform ransomware scan, the following prerequisites must be met:

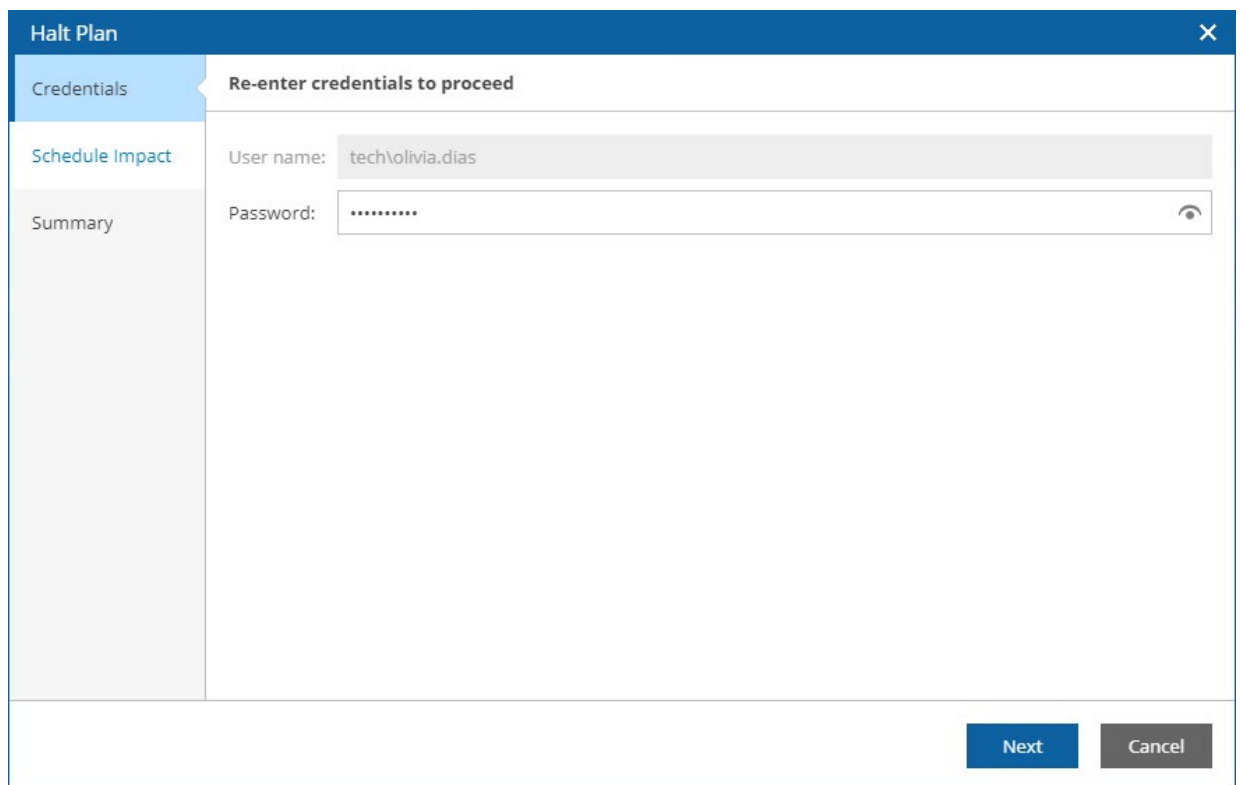
- Ransomware scan is supported only for Windows-based machines. Ransomware scan is not supported for restore points stored in object storage repositories.
- The Veeam Backup & Replication server that manages the process of recovering machines to Microsoft Azure must run version 12 or later.
- Antivirus software must be installed on the mount server and support the command line interface (CLI). The following antivirus software is supported: Microsoft Defender, Kaspersky, ESET and Symantec Protection Engine.

Halting Cloud Restore

The **Halt** action interrupts plan execution. Any steps currently executing will be completed, then the plan will enter the *HALTED* state. To learn how to work with *HALTED* restore plans, see [Managing Halted Plans](#).

To stop a running cloud plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Halt**.
-OR-
Click the plan name to switch to the **Plan Details** page, and click **Halt**.
3. Complete the **Halt Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.



The screenshot shows a 'Halt Plan' wizard window with a dark blue header and a close button (X) in the top right corner. On the left is a sidebar with three tabs: 'Credentials' (selected and highlighted in blue), 'Schedule Impact' (in blue text), and 'Summary' (in grey text). The main area of the wizard has a title bar that says 'Re-enter credentials to proceed'. Below this, there are two input fields: 'User name:' with the text 'tech\olivia.dias' and 'Password:' with masked characters '*****'. A small eye icon is visible to the right of the password field. At the bottom right of the wizard, there are two buttons: 'Next' (blue) and 'Cancel' (grey).

- b. [This step applies only if you have any other orchestration plans scheduled to run after the plan completes]

At the **Schedule Impact** steps, choose whether you want to proceed with or cancel execution of subsequent plans after the current plan enters the *HALTED* state.

The screenshot shows the 'Halt Plan' dialog box with the 'Schedule Impact' tab selected. The left sidebar contains 'Credentials', 'Schedule Impact', and 'Summary'. The main area has two radio buttons: 'Cancel the schedule and do not execute the subsequent Plans' (selected) and 'Continue the schedule and launch the next Plan now'. Below these is a warning message: 'There are other Plan(s) scheduled in a chain to failover after this Plan completes. Choose the options for those scheduled Plans below.' At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

- c. At the **Summary** step, review configuration information and click **Finish**.

The screenshot shows the 'Halt Plan' dialog box with the 'Summary' tab selected. The left sidebar contains 'Credentials', 'Schedule Impact', and 'Summary'. The main area has a heading 'Click Finish to halt the plan' and a 'Copy to clipboard' button. Below this is a summary of the plan: Plan name: Cloud Plan, Halted by: tech\olivia.dias [Administrator], Current state: Restore (with a play button icon), and Action: Halt. At the bottom is an information message: 'Halting a plan before it reaches a stable state may cause your environment to enter an inconsistent state, requiring manual troubleshooting and a reset of the plan to resolve.' At the bottom right are 'Back', 'Finish', and 'Cancel' buttons.

Resetting Cloud Plans

If a cloud plan becomes inconsistent with the virtual environment, you can reset the plan. This will return the plan to the *DISABLED* state, without making any changes to the external virtual infrastructure.

To reset a cloud plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Manage** menu, select **Reset**.
-OR-
Right-click the plan name and select **Manage > Reset**.
3. Complete the **Reset Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.

The screenshot shows a 'Reset Plan' dialog box with a blue header and a close button (X) in the top right corner. On the left is a sidebar with three tabs: 'Credentials' (selected and highlighted in blue), 'Quick Check', and 'Summary'. The main area is titled 'Re-enter credentials to proceed'. It contains two input fields: 'User name:' with the text 'tech\olivia.dias' and 'Password:' with masked characters '*****'. To the right of the password field is an eye icon for toggling visibility. Below the fields is an information box with a blue 'i' icon and the text: 'Reset will take no actions on VMs or replicas in your infrastructure. It will reinitialize the Plan in Orchestrator only. For *Halted* plans it is recommended to use Undo, not Reset.' At the bottom right are two buttons: 'Next' (blue) and 'Cancel' (gray).

- b. At the **Quick Check** step, select the **Perform a Quick Check after reset is complete** check box to run a **readiness check** after the reset.

The screenshot shows the 'Reset Plan' dialog box with the 'Quick Check' tab selected. The left sidebar contains 'Credentials', 'Quick Check', and 'Summary'. The main area has a header 'It is recommended to run a Quick Check after resetting the plan' and a checkbox labeled 'Perform a Quick Check after reset is complete' which is checked. At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

Reset Plan	
Credentials	It is recommended to run a Quick Check after resetting the plan
Quick Check	<input checked="" type="checkbox"/> Perform a Quick Check after reset is complete
Summary	

Back Next Cancel

- c. At the **Summary** step, review configuration information and click **Finish**.

The screenshot shows the 'Reset Plan' dialog box with the 'Summary' tab selected. The left sidebar contains 'Credentials', 'Quick Check', and 'Summary'. The main area has a header 'Plan will be reset using the options below. Press Finish to reset the Plan' and a 'Copy to clipboard' link. Below this is a summary of the plan: Plan Name: Restore plan, Reset by: TECH\olivia.dias [Administrator], Current State: Restore (Halted, 16% complete, 10 errors, no warnings), and Quick Check: Yes. At the bottom right are 'Back', 'Finish', and 'Cancel' buttons.

Reset Plan	
Credentials	Plan will be reset using the options below. Press Finish to reset the Plan
Quick Check	Copy to clipboard
Summary	<p>Plan Name: Restore plan</p> <p>Reset by: TECH\olivia.dias [Administrator]</p> <p>Current State: ⊘ Restore (Halted, 16% complete, 10 errors, no warnings)</p> <p>Quick Check: Yes</p>

Back Finish Cancel

Managing Halted Cloud Plans

If a critical step fails for a machine from a [critical inventory group](#), the plan may enter the *HALTED* state. To troubleshoot reasons why a plan failed, use the **Plan Execution Report** generated as soon as the currently performed action completes. For more information on how to track plan performance history, see [Viewing Plan Execution History](#).

After you eliminate the problem that caused the plan to become *HALTED*, you have the following options to resume the plan:

- Repeat the last failed step.
- Proceed to the next step.

Running Halted Cloud Plans

To run a *HALTED* cloud plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan. From the **Launch** menu, select **Continue**.
-OR-
Click the plan name to switch to the **Plan Details** page, and click **Continue**.
3. Complete the **Run Plan** wizard:
 - a. For security purposes, at the **Credentials** step, retype your password.

The screenshot shows a 'Resume Plan' dialog box with a dark blue header and a close button (X) in the top right corner. On the left is a sidebar with three tabs: 'Credentials' (selected and highlighted in light blue), 'Resume Settings', and 'Summary'. The main area is titled 'Re-enter credentials to proceed' and contains two input fields: 'User name:' with the text 'TECH\olivia.dias' and 'Password:' with masked characters '*****'. A small eye icon is to the right of the password field. At the bottom right are two buttons: 'Next' (blue) and 'Cancel' (grey).

- b. At the **Resume Settings** step, select an option to resume plan execution.

Choose whether you want to proceed with plan execution from the next plan step or to retry the failed step.

The screenshot shows the 'Resume Plan' dialog box with the 'Resume Settings' tab selected. The left sidebar contains 'Credentials', 'Resume Settings', and 'Summary'. The main area is titled 'Choose one of the following options' and contains two radio button options: 'Retry failed step' (selected) and 'Proceed to next step'. Below the options is an information icon and a note: 'If VMs are being processed in parallel, then multiple failed steps may be retried.' At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

Resume Plan	
Credentials	Choose one of the following options
Resume Settings	<p><input checked="" type="radio"/> Retry failed step If the most recently executed step failed, it will be retried</p> <p><input type="radio"/> Proceed to next step The plan will proceed to the next step</p> <p>i If VMs are being processed in parallel, then multiple failed steps may be retried.</p>
Summary	
<div>Back Next Cancel</div>	

- c. At the **Summary** step, review configuration information and click **Finish**. The restore process will be started.

The screenshot shows the 'Resume Plan' dialog box with the 'Summary' tab selected. The left sidebar contains 'Credentials', 'Resume Settings', and 'Summary'. The main area is titled 'Click Finish to resume the plan' and contains a 'Copy to clipboard' link and a list of configuration details. At the bottom right are 'Back', 'Finish', and 'Cancel' buttons.

Resume Plan	
Credentials	Click Finish to resume the plan
Resume Settings	Copy to clipboard
Summary	<p>Plan name: Cloud Plan</p> <p>Launched by: tech\olivia.dias [Administrator]</p> <p>Current state: - Restore (Halted, 99% complete, 1 error, 1 warning)</p> <p>Action: Resume – Restore</p> <p>Resume by: Retry failed Step</p> <p>Recovery Location: Cloud RL</p> <p>Restore VM Tags: No</p>
<div>Back Finish Cancel</div>	

Resetting Halted Cloud Plans

To reset a *HALTED* cloud plan, follow the instructions provided in section [Resetting Restore Plans](#).

NOTE

When you reset a cloud plan, Orchestrator returns it to the *DISABLED* state without making any changes to the external virtual infrastructure. You may need to deal with any infrastructure reconfiguration manually.

Editing Orchestration Plans

In addition to default orchestration plan settings that you specify when creating a plan, you can also specify granular settings to customize the plan. The Orchestrator UI allows you to adjust the following:

- [Plan properties](#)
- [Group settings](#)
- [Machine settings](#)
- [Plan step settings](#)
- [Step parameter settings](#)

NOTE

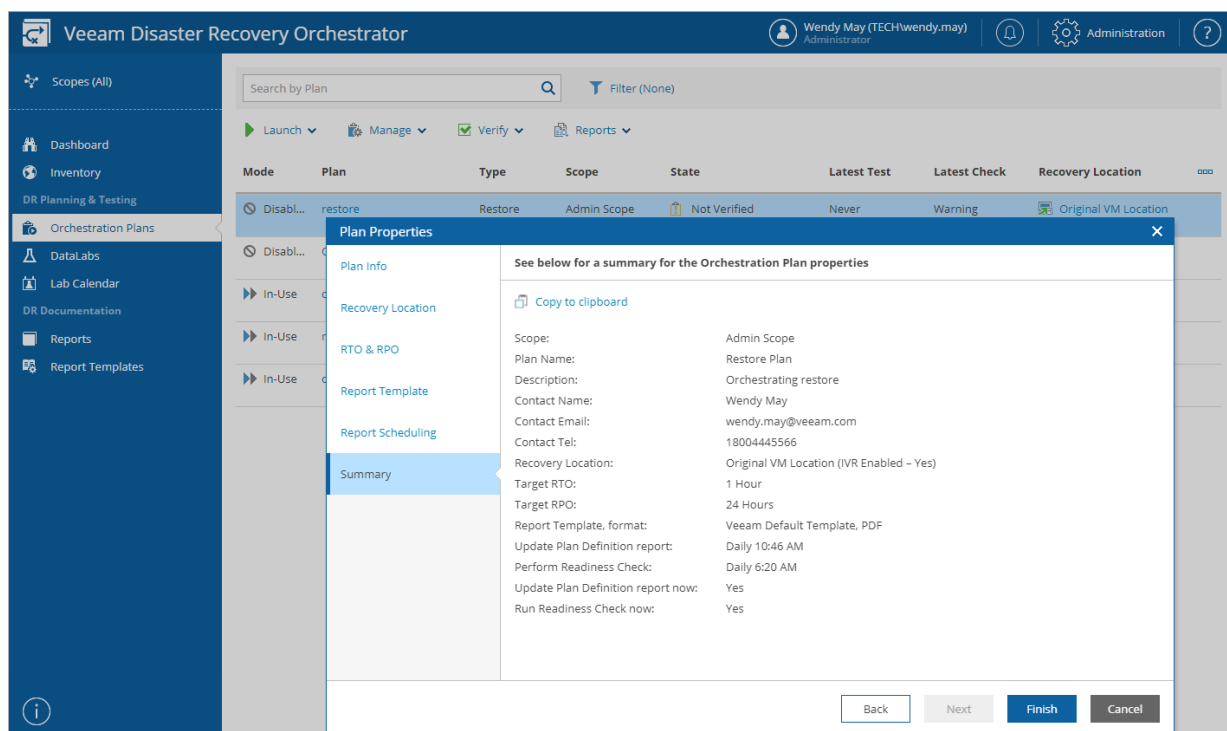
You cannot edit an orchestration plan if the plan is in the *IN USE* mode. If an orchestration plan is in the *ENABLED* mode, you can edit only plan properties. To allow editing plan properties and other plan settings, you must disable the plan.

For the list of modes that different types of orchestration plans can acquire, see [Running and Scheduling Replica Plans](#), [Running and Scheduling CDP Replica Plans](#), [Running and Scheduling Restore Plans](#), [Running and Scheduling Storage Plans](#) and [Running and Scheduling Cloud Plans](#).

Configuring Plan Properties

For each orchestration plan, you can configure settings specified while creating the plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan and click **Manage > Properties**.
3. Complete the **Plan Properties** wizard:
 - a. To provide a new name, description, contact name, email or telephone number of a person responsible for the plan, follow the instructions provided in section [Creating Replica Plans](#) (step 1), [Creating CDP Replica Plans](#) (step 1), [Creating Restore Plans](#) (step 1), [Creating Storage Plans](#) (step 1) or [Creating Cloud Plans](#) (step 1).
 - b. [This step applies only to cloud and restore plans] To select a new location to which inventory groups included in the plan will be restored, follow the instructions provided in section [Creating Restore Plans](#) (step 4) or [Creating Cloud Plans](#) (step 4).
 - c. To modify the configured Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for the plan, follow the instructions provided in section [Creating Replica Plans](#) (step 9), [Creating CDP Replica Plans](#) (step 8), [Creating Restore Plans](#) (step 10), [Creating Storage Plans](#) (step 9) or [Creating Cloud Plans](#) (step 8).
 - d. To select a new document template that will be used to create documents for the plan, follow the instructions provided in section [Creating Replica Plans](#) (step 10), [Creating CDP Replica Plans](#) (step 9), [Creating Restore Plans](#) (step 11), [Creating Storage Plans](#) (step 10) or [Creating Cloud Plans](#) (step 9).
 - e. To choose whether you want to automatically generate the [Plan Definition](#) and [Plan Readiness Check](#) reports for the plan, follow the instructions provided in section [Creating Replica Plans](#) (step 11), [Creating CDP Replica Plans](#) (step 10), [Creating Restore Plans](#) (step 12), [Creating Storage Plans](#) (step 11) or [Creating Cloud Plans](#) (step 11).
 - f. At the **Summary** step of the wizard, review configuration information and click **Finish**.



Configuring Groups

Options in the **Plan Groups** column allow you to:

- [Add and remove inventory groups from a plan](#)
- [Change the processing order for groups in a plan](#)
- [Turn on and turn off post-recovery protection of machines in a group](#)
- [Customize recovery settings for machines in a group](#)

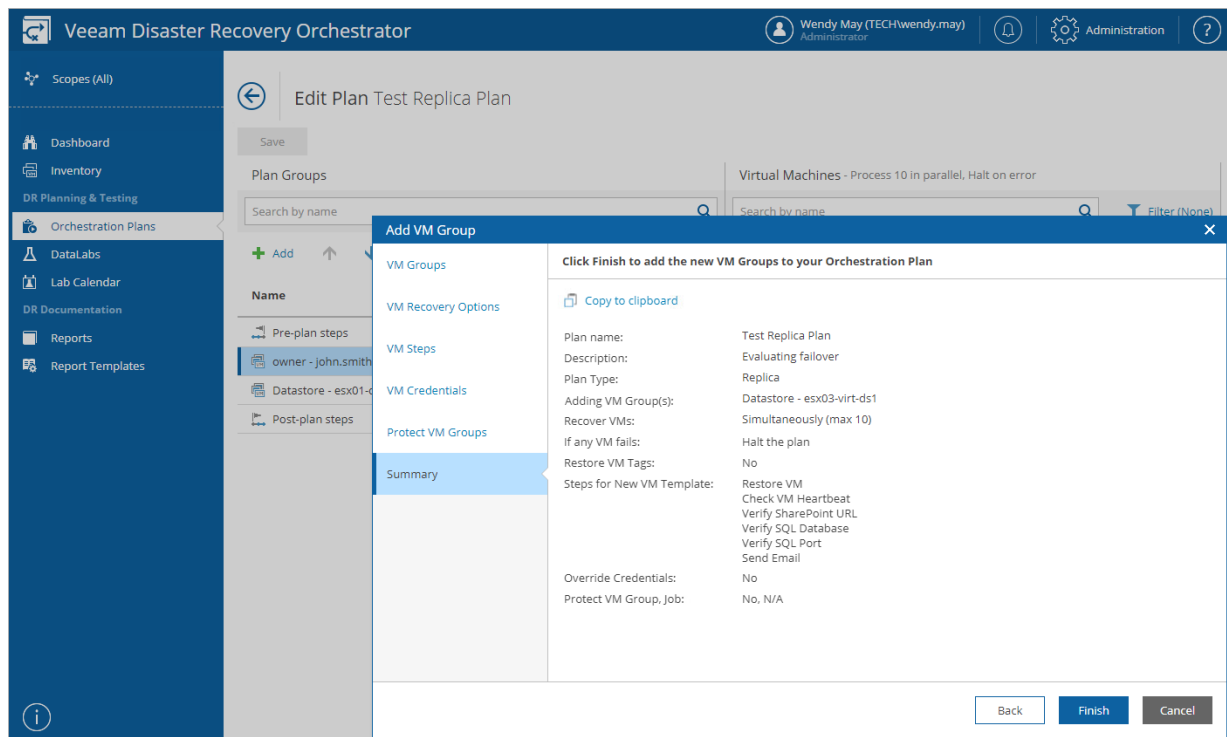
Managing Inventory Groups

You may need to add new inventory groups or remove some groups from an orchestration plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan and click **Manage > Edit**.
3. On the **Edit Plan** page:
 - To remove an inventory group, in the **Plan Groups** column, select the group and click **Delete**.
 - To add an inventory group, in the **Plan Groups** column, click **Add**.

Complete the **Add VM Group** wizard:

- i. To configure VM recovery options and to choose default steps that will be performed for all machines in the group, follow the instructions provided in section [Creating Replica Plans](#) (steps 5–7), [Creating CDP Replica Plans](#) (steps 5–7), [Creating Restore Plans](#) (steps 6–8), [Creating Storage Plans](#) (steps 6–8) or [Creating Cloud Plans](#) (steps 6–7).
 - ii. [This step applies only to replica and restore plans] To select a template job that will be used to protect machines included in the plan, follow the instructions provided in section [Creating Replica Plans](#) (step 8) or [Creating Restore Plans](#) (step 9).
 - iii. At the **Summary** step of the wizard, review configuration information and click **Finish**.
5. To save changes made to the plan settings, click **Save**.



Setting Group Processing Order

Inventory groups in an orchestration plan are processed in the order they appear in the **Plan Groups** list. If some machines in a group are dependent upon machines in other groups, make sure that the required group is recovered first.

To change the processing order for inventory groups included into an orchestration plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan and click **Manage > Edit**.
3. On the **Edit Plan** page:
 - a. In the **Plan Groups** column, select an inventory group.
 - b. To move the group up or down the list, use the **Up** and **Down** arrows in the **Plan Groups** column.
 - c. To save changes made to the plan settings, click **Save**.

NOTE

By design, each orchestration plan contains 2 default groups — *Pre-plan steps* and *Post-plan steps*. These groups include plan steps that run before and after the recovery process. You cannot change the processing order for the *Pre-plan steps* and *Post-plan steps* groups, but you can add and remove steps for these groups. For more information, see [Configuring Steps](#).

Veeam Disaster Recovery Orchestrator

Wendy May (TECHwendy.may) Administrator

Administration

Scopes (All)

Dashboard

Inventory

Orchestration Plans

DataLabs

Lab Calendar

Reports

Report Templates

Edit Plan Test Replica Plan

Save

Plan Groups

Search by name

+ Add ↑ ↓ Properties X Delete

Name	Process
Pre-plan steps	In sequence
owner - john.smith - Halt on error	10 in parallel
Datastore - esx01-das3 - Halt on error	10 in parallel
Datastore - esx03-virt-ds1 - Halt on error	10 in parallel
Post-plan steps	In sequence

Virtual Machines - Process 10 in parallel, Halt on error

Search by name

Filter (None)

↑ ↓ Edit Steps Info

Name

Selected: 0 of 6

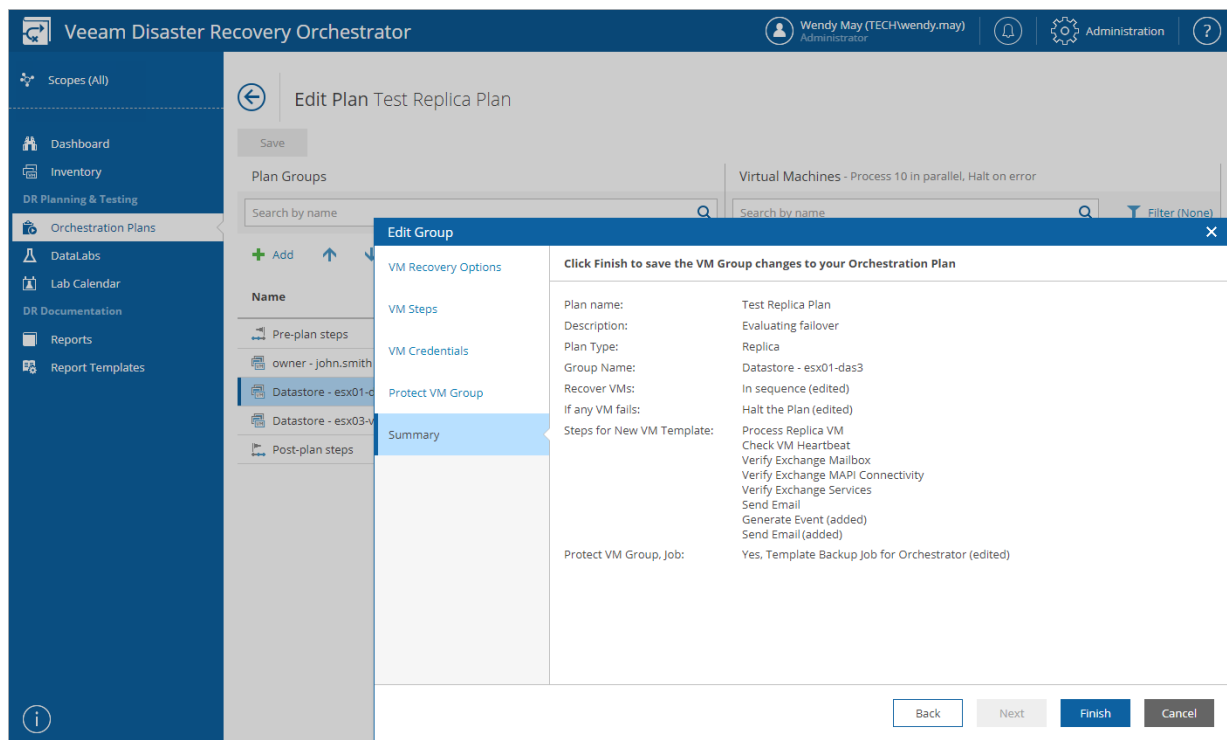
- apache02
- apache02_replica
- cloud_backup
- oraclelinux
- shell
- srv08

Overriding VM Recovery and Protection Settings

For each group in an orchestration plan, you can enable, disable or change machine processing options:

1. Navigate to **Orchestration Plans**.
2. Select the plan and click **Manage > Edit**.
3. On the **Edit Plan** page:
 - a. In the **Plan Groups** column, select an inventory group and click **Properties**.
 - b. Complete the **Edit Group** wizard:
 - i. To choose VM recovery options for the group, follow the instructions provided in section [Creating Replica Plans](#) (step 5), [Creating CDP Replica Plans](#) (step 5), [Creating Restore Plans](#) (step 6), [Creating Storage Plans](#) (step 6) or [Creating Cloud Plans](#) (step 6).
 - ii. To add steps to be performed during recovery for new machines in the inventory group, and to specify credentials to run in-guest OS scripts inside machines being tested or recovered, follow the instructions provided in section [Creating Replica Plans](#) (steps 6-7), [Creating CDP Replica Plans](#) (steps 6-7), [Creating Restore Plans](#) (steps 7-8), [Creating Storage Plans](#) (steps 7-8) or [Creating Cloud Plans](#) (step 7).

To add steps to be performed during recovery for existing machines in the inventory group, follow the instructions provided in section [Configuring Steps](#).
 - iii. [This step applies only to replica and restore plans] To choose VM protection options for the inventory group, follow the instructions provided in section [Creating Replica Plans](#) (step 8) or [Creating Restore Plans](#) (step 9).
 - iv. At the **Summary** step of the wizard, review configuration information and click **Finish**.
- c. To save changes made to the plan settings, click **Save**.



Configuring Machines

The order in which machines in an orchestration plan are processed depends on the **VM Recovery Options** configured while creating the plan:

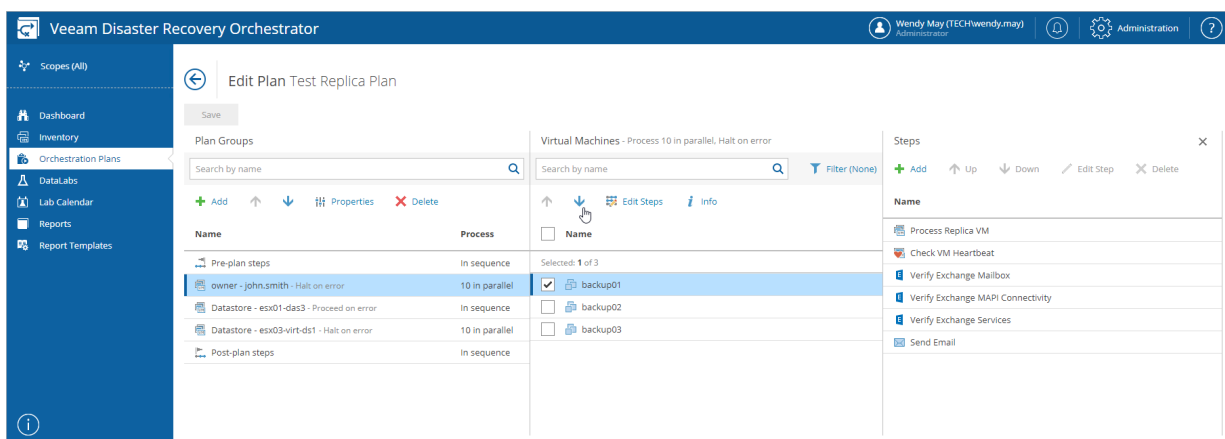
- If the **Recover the VMs in each group > In sequence** option is selected for an inventory group, machines in the group will be processed in the order they appear in the **Virtual Machines** list.
- If the **Recover the VMs in each group > In parallel** option is selected for an inventory group, a limited number of machines in the group will be processed at the same time.

If you select this option, you will also have to configure the maximum number of machines processed simultaneously. For more information, see [Creating Replica Plans](#) (step 5), [Creating CDP Replica Plans](#) (step 5), [Creating Restore Plans](#) (step 6), [Creating Storage Plans](#) (step 6) or [Creating Cloud Plans](#) (step 6).

- If new machines are added to an inventory group, the entire machine list will be resorted and then processed in the alphabetical order.

If some machines are dependent on other machines, ensure the required machines are started first. To define the recovery order for machines included in an inventory group:

1. Navigate to **Orchestration Plans**.
2. Select the plan and click **Manage > Edit**.
3. On the **Edit Plan** page:
 - a. In the **Plan Groups** column, select an inventory group.
 - b. To move machines included in the group up or down the list, use the **Up** and **Down** arrows in the **Virtual Machines** column.
 - c. To save changes made to the plan settings, click **Save**.



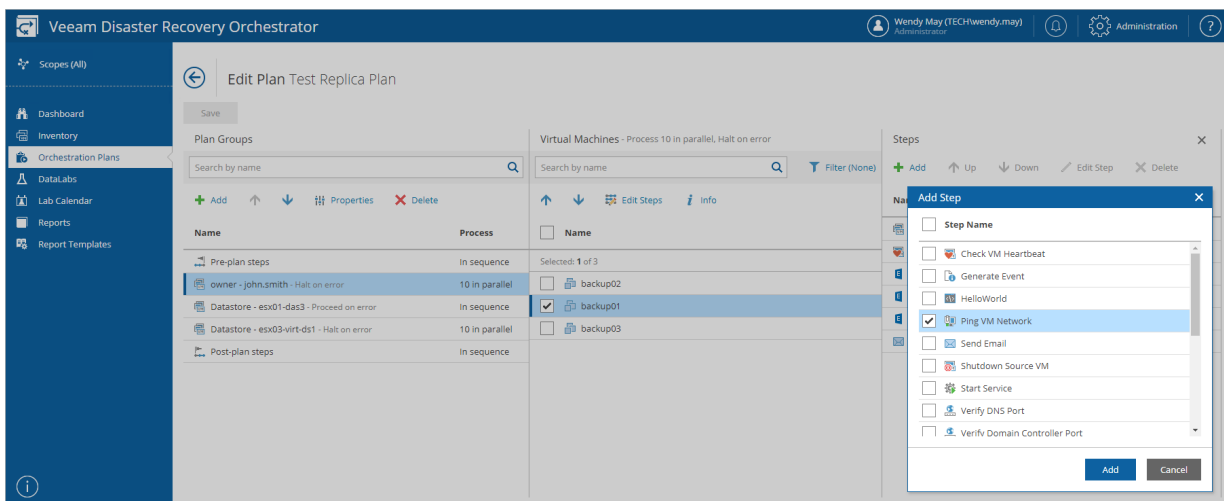
Configuring Steps

For each machine included in an orchestration plan, you can add and remove steps performed when processing the machine:

1. Navigate to **Orchestration Plans**.
2. Select the plan and click **Manage > Edit**.
3. On the **Edit Plan** page:
 - a. In the **Plan Groups** column, select an inventory group.
 - b. In the **Virtual Machines** column, select a machine.
 - c. The **Steps** column will display the list of steps to perform for the machine.
 - To change the step execution order, use the **Up** and **Down** arrows to move steps up and down the list.
 - To remove a step, select the step and click **Delete**.
 - To add a step, click **Add**. The **Add Step** window will be displayed. Use the list of plan steps available for the scope to select steps to be performed for the machine during recovery. For more information on adding plan steps, see [Configuring Veeam Disaster Recovery Orchestrator](#).
 - d. To save changes made to the plan settings, click **Save**.

TIP

You can simultaneously add steps for multiple machines in each inventory group. To do that, select an inventory group in the **Plan Groups** column, select the necessary machines in the **Virtual Machines** column and then click **Edit Steps**. In the **Edit Steps** window, click **Add** in the **Steps** column, select the required steps that you want to add and then click **Add**. After you click **Apply**, the changes will be applied to all the selected machines in the group.



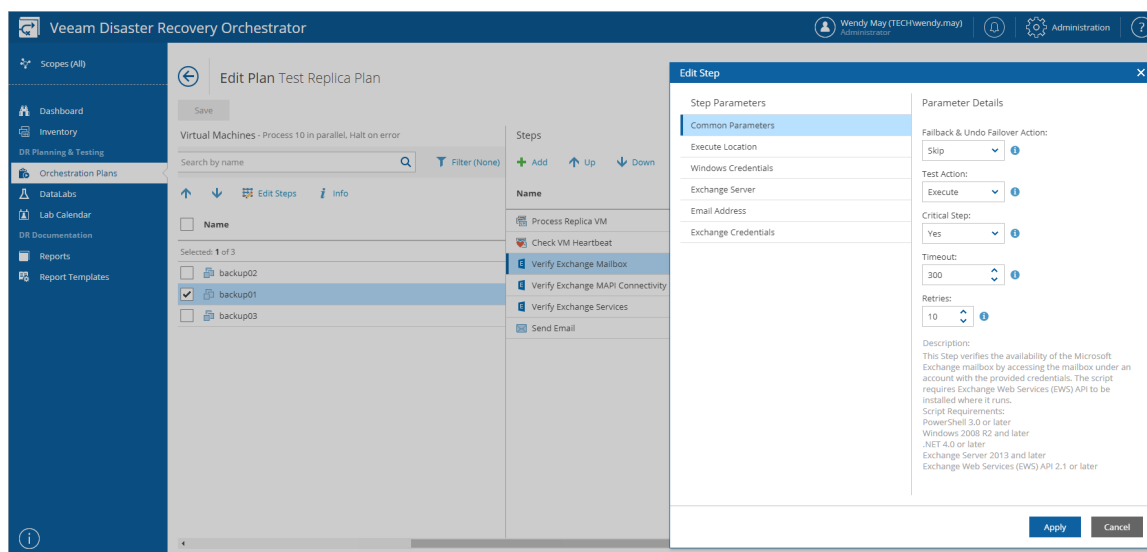
Configuring Step Parameters

For each plan step performed during recovery, you can customize parameter settings:

1. Navigate to **Orchestration Plans**.
2. Select the plan and click **Manage > Edit**.
3. On the **Edit Plan** page:
 - a. In the **Plan Groups** column, select an inventory group.
 - b. In the **Virtual Machines** column, select a machine.
 - c. In the **Steps** column, select a step and click **Edit Step**.
 - d. In the **Edit Step** window:
 - i. In the **Step Parameters** section, select the required parameter.
Common Parameters (*Timeout*, *Retries* and so on) are used for all steps and are grouped under a single container for convenience and readability. Additional parameters specific to the step are shown below the *Common Parameters* container.
 - ii. In the **Parameter Details** section, set the desired parameter values.
 - iii. Click **Apply**.
 - e. To save changes made to the plan settings, click **Save**.

TIP

You can simultaneously modify step parameter settings for multiple machines in each inventory group. To do that, select an inventory group in the **Plan Groups** column, select the necessary machines in the **Virtual Machines** column and then click **Edit Steps**. In the **Edit Steps** window, select the required step and its parameter that you want to customize, and set the desired parameter values in the **Parameter Details** column. After you click **Apply**, the changes will be applied to all the selected machines in the group.



For detailed description of step parameters that you can configure for orchestration plan steps, see [Appendix. Orchestration Plan Steps](#).

Testing Orchestration Plans

Before you run an orchestration plan, you can use an isolated Orchestrator DataLab to test the entire plan, including the verification of vSphere and agent backups, replicas and storage snapshots. All changes made to machines during a lab session will be discarded as soon as the testing process is over.

NOTE

Testing is currently not supported for CDP replica and cloud plans.

Orchestrator DataLabs are based on Veeam Backup & Replication virtual labs. While a Veeam Backup & Replication virtual lab is an appliance VM that creates an isolated network, Orchestrator adds the capability to easily create multiple test environments, to perform recovery and application verification including custom scripts, and to generate detailed reporting.

DataLabs may be powered on independently from orchestration plans and used for other test cases (for example, to test patches or upgrades). You can add one or more orchestration plans to any running lab and verify the plans there. You may choose to keep the lab running, so that additional tests can be performed.

To test an orchestration plan:

1. In the Veeam Backup & Replication console, create a virtual lab that will be used to start vSphere and agent backups, replicas and storage snapshots.

For more information, see the Veeam Backup & Replication User Guide, section [Virtual Lab](#).

IMPORTANT

When creating a virtual lab, consider the following:

- To test a replica or restore plan, the virtual lab must be created on a Veeam Backup & Replication server that manages backup and replication jobs protecting machines included in the plan.
- To test a storage plan, the virtual lab must be created on a Veeam Backup & Replication server that protects the storage system where VMs included in the plan belong. If the storage system is not protected by any Veeam Backup & Replication server, the virtual lab must be created on the embedded Veeam Backup & Replication server.

2. Assign the lab to the required scope.

For more information, see [Connecting DataLabs](#).

3. [Create a lab group to provide the test environment for the vSphere and agent backups, replicas and storage snapshots to be verified.](#)

Most VMs require a domain controller to boot and start services successfully. If the orchestration plan does not include a domain controller, then ensure that the lab group includes a VM with the Domain Controller role, and that this VM has a correct IP addressing scheme for the DR site. Otherwise, the VMs in the plan will fail to verify.

4. [Start on-demand plan testing](#) or [configure test scheduling](#).

To ensure that an orchestration plan is automatically and regularly verified, you can schedule the plan for automated lab testing.

5. [View plan test results](#).

NOTE

The test will not run unless the plan is in the *ENABLED* or *DISABLED* mode. The test will also not run if the plan is currently being edited.

For the list of modes that a replica plan can acquire, see [Running and Scheduling Replica Plans](#). For the list of modes that a restore plan can acquire, see [Running and Scheduling Restore Plans](#). For the list of modes that a storage plan can acquire, see [Running and Scheduling Storage Plans](#).

Creating Lab Groups

In most cases, a machine does not work in isolation but has dependencies on other services and components, such as Active Directory or DNS. To verify such a machine, the DataLab will have to supply all services on which this machine is dependent. For this purpose, Orchestrator uses lab groups.

NOTE

If an orchestration plan contains a particular inventory group or machine, do not attempt to test this plan in a DataLab that includes a lab group with the same machine or inventory group.

To create a lab group for a DataLab:

1. Navigate to **DataLabs**.
2. In the **DataLabs** column, click the DataLab name.
For a DataLab to be displayed in the **DataLabs** list, it must be assigned to the scope as described in section [Assigning and Configuring DataLabs](#).
3. On the **DataLab Details** page, in the **DataLab** column, select the DataLab and click **Edit**.
4. On the **Edit DataLab** page, in the **Lab Groups** column, click **Add** to include inventory groups in the DataLab.
5. Complete the **Add Lab Group** wizard:
 - a. At the **Lab Group Type** step, choose whether the lab group will contain VMs recovered from backups or replicas.
 - b. At the **VM Groups** step, select the required inventory groups and click **Add** to include them in the lab group.
For an inventory group to be displayed in the **Available Groups** list, it must be included into the list of inventory items available for the scope, as described in section [Allowing Access to Inventory Groups](#).
 - c. To configure VM recovery options and choose default steps that will be performed for machines in the lab group, follow the instructions provided in section [Creating Replica Plans](#) (steps 5-7), [Creating Restore Plans](#) (steps 6-8), or [Creating Storage Plans](#) (steps 6-8).

TIP

By default, Orchestrator skips a number of steps during the plan testing process — **Generate Event**, **Send Email**, **Shutdown Source VM** and **VM Power Actions**. That is why when you create a DataLab, you cannot add these steps at the **VM Steps** step of the wizard.

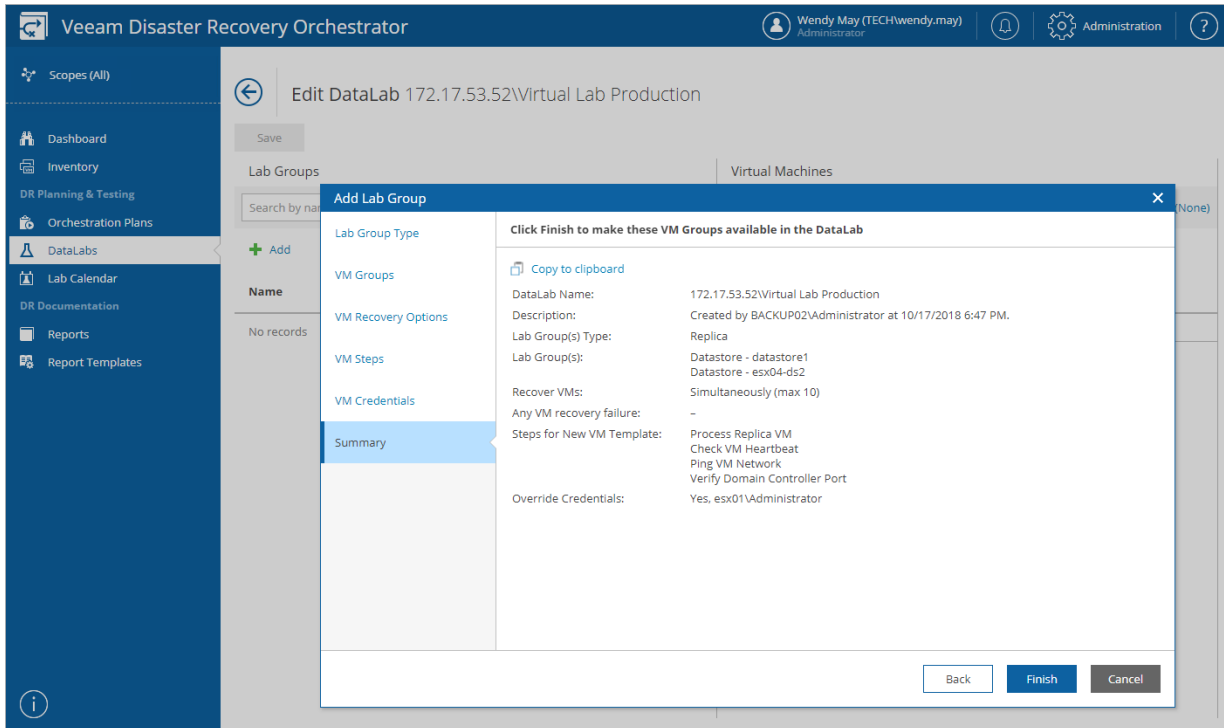
If you want to add these steps, close the **Add Lab Group** wizard, configure the **During Lab Test** parameter for each step as described in section [Configuring Step Parameters](#), and then run the wizard again.

- d. At the **Summary** step, review configuration information and click **Finish**.
6. To save changes made to the DataLab settings, click **Save**.

IMPORTANT

A common use case for lab groups is to provide domain controllers for the test environment. If there are domain controllers in a lab group, it is essential to add the **Prepare DC for DataLab** step. By design, it will automatically become the first step in the step execution order.

You may also optionally add domain controller-specific checks, such as **Verify Domain Controller Port** and **Verify Global Catalog Port**. These steps must be performed after the **Ping VM Network** step.



NOTE

There is no clear use case for replicating a domain controller. Failing over to a domain controller that contains an old version of the Active Directory database is not recommended by Microsoft. The only real use case for replicating a domain controller is to use it in an isolated lab group, and you may need to create a replication job specifically for that purpose.

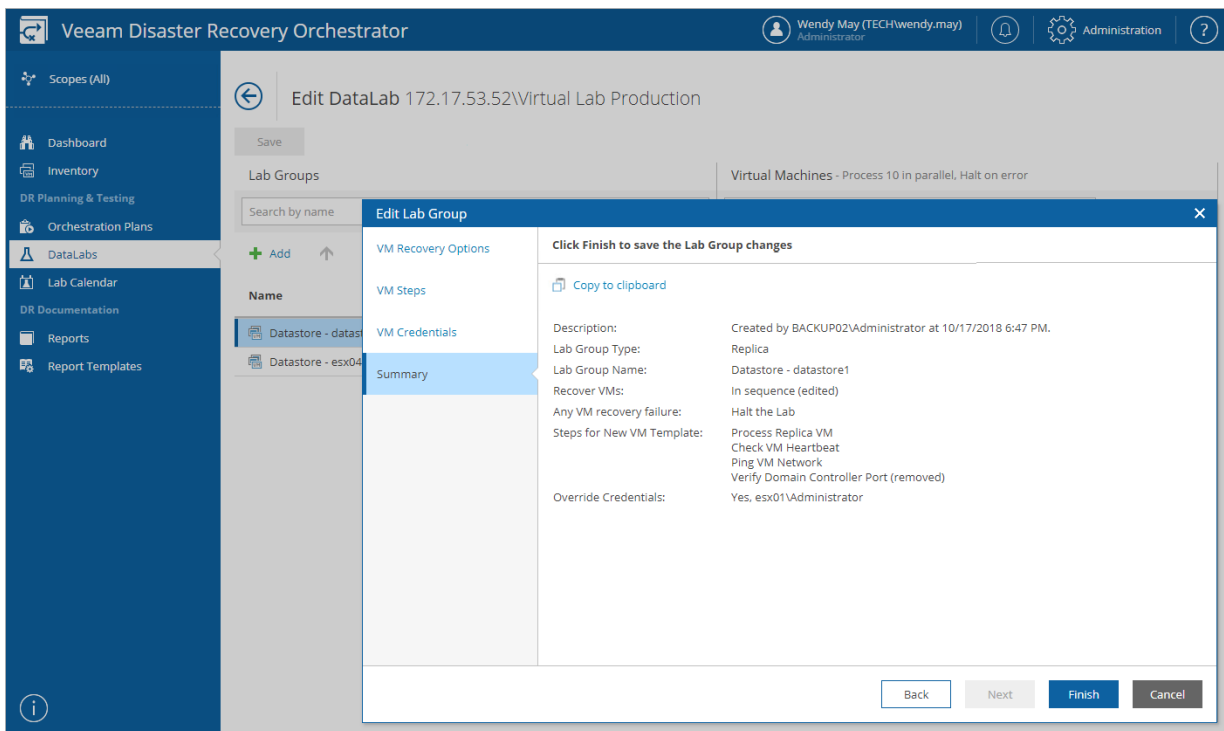
To learn how to restore a domain controller from an image-aware backup, see [this Veeam KB article](#). To learn how to back up a domain controller, see [this Veeam KB article](#).

Configuring Lab Groups

If required, you can customize lab group settings, in much the same way as [editing an orchestration plan](#).

1. Navigate to **DataLabs**.
2. In the **DataLabs** column, select the newly created lab group.
 - To customize VM recovery options and change default steps that will be performed for machines in the lab group, click **Properties**.

In the **Edit Lab Group** wizard, specify the required settings following the instructions provided in section [Creating Replica Plans](#) (steps 5–7), [Creating Restore Plans](#) (steps 6–8), or [Creating Storage Plans](#) (steps 6–8), and click **Finish**.
 - To define the order in which machines will be started, use the **Up** and **Down** arrows in the **Virtual Machines** column.
 - To select steps performed when processing each machine, select a machine in the **Virtual Machines** column, click **Edit Steps**, and follow the instruction provided in section [Configuring Steps](#).
 - To modify parameter settings for each step, select a step in the **Steps** column, click **Edit Step**, and follow the instruction provided in section [Configuring Step Parameters](#).
 - To delete the lab group, click **Delete**.
3. To save changes made to the lab group settings, click **Save**.



Working with Default Lab Groups

Default lab groups are lab groups created by an Administrator but available for plan testing by Plan Authors and Plan Operators for any scope.

To allow Plan Authors and Plan Operators to use a lab group as a default group when testing plans for their scope:

1. Assign a DataLab to the scope as described in section [Assigning and Configuring DataLabs](#).
2. Add the lab group to the DataLab as described in section [Creating Lab Groups](#).

The added lab group will now be considered to be a default lab group. The DataLab with the lab group will become available for the scope, and Plan Authors and Plan Operators will be able to use the group for plan testing. The lab group will be preselected in the [Run Lab Tests](#) and [Create Test Schedule](#) wizards, and it will start before all other lab groups in the DataLab every time Orchestrator powers on the lab to test an orchestration plan.

NOTE

Plan Authors and Plan Operators cannot edit default lab groups or delete them from DataLabs because these groups can be managed only by Administrators. However, if an Administrator assigns a DataLab to the *Admin Scope*, lab groups added to the DataLab will not be treated as default lab groups. This means that Plan Authors will still be able to edit and delete these lab groups as described in section [Configuring Lab Groups](#).

Starting On-Demand Plan Test

DataLab testing may be started on-demand for any orchestration plan in the *ENABLED* or *DISABLED* state.

Testing Replica Plans

To start on-demand testing for a replica plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan.
3. From the **Verify** menu, choose **Run DataLab Test**.
4. Complete the **Run DataLab Test** wizard:
 - a. [Select a DataLab](#).
 - b. [Choose whether you want to power off the lab after the testing process is over](#).
 - c. [Add lab groups](#).
 - d. [Finish working with the wizard](#).
6. [Track the progress of plan testing](#).

Step 1. Select DataLab

At the **DataLab** step of the wizard, select a DataLab in which the plan will be verified.

For a DataLab to be displayed in the **Available DataLabs** list, it must be assigned to the scope as described in section [Assigning and Configuring DataLabs](#).

The screenshot shows the 'Run DataLab Test' wizard interface. The title bar is 'Run DataLab Test' with a close button. The left sidebar contains the following steps: 'DataLab' (selected), 'Power Options', 'Choose Lab Groups', and 'Summary'. The main area is titled 'Choose a DataLab' and features a search bar with the placeholder text 'Type any part of Lab name to filter'. Below the search bar is a table titled 'Available DataLabs' with two rows:

172.17.53.15\Exchange vLab	Powered Off
DRVirtual Lab 2	Powered Off

At the bottom right of the wizard, there are two buttons: 'Next' and 'Cancel'.

Step 2. Choose Power Options

At the **Power Options** step of the wizard, choose an action to perform after the testing process is over:

- To power off plan VMs and the lab, select the **Test then power off immediately** option.
- To keep plan VMs and the lab running in case you are willing to perform further tests, select the **Test then power off after** option.

Use the **Test then power off after** field to book a time slot in the lab schedule and prevent other tests from being scheduled for the same period.

NOTE

If you have selected a starting or running lab at the **DataLab** step of the wizard, the lab will not be powered off after the testing process is over — even if the **Test then power off immediately** option is selected. In this case, Orchestrator will power off only plan VMs and keep the lab running.

The screenshot shows the 'Run DataLab Test' wizard window. The left sidebar contains four steps: 'DataLab', 'Power Options' (which is highlighted in blue), 'Choose Lab Groups', and 'Summary'. The main area is titled 'Estimate the expected test duration' and contains two radio button options. The first option, 'Test then power off immediately', is unselected. The second option, 'Test then power off after', is selected. To the right of the second option is a numeric input field containing the value '2', followed by a 'hours' label. At the bottom right of the window are three buttons: 'Back', 'Next', and 'Cancel'.

Run DataLab Test	
DataLab	Estimate the expected test duration
Power Options	<input type="radio"/> Test then power off immediately
Choose Lab Groups	<input checked="" type="radio"/> Test then power off after 2 hours
Summary	
<div>Back Next Cancel</div>	

Step 3. Add Lab Groups

At the **Choose Lab Groups** step of the wizard, add the required lab groups to support the test environment.

For a lab group to be displayed in the **Available Lab Groups** list, it must be created and configured as described in section [Creating Lab Groups](#).

NOTE

All default lab groups previously created by an Administrator will automatically become preselected in the **Lab Groups to use** list, and you will not be able to remove them. For more information, see [Working with Default Lab Groups](#).

Run DataLab Test

DataLab

Power Options

Choose Lab Groups

Summary

Choose Lab Groups to be used in the DataLab environment

You cannot remove default Lab Groups added by a Orchestrator Administrator.

Type any part of VM Group name to filter

View VMs

Available Lab Groups

No Records

Add >

< Remove

Lab Groups to use

prgtwesr00

Back

Next

Cancel

Step 4. Finish Working with Wizard

At the **Summary** step of the wizard, review configuration information and click **Finish**.

The screenshot shows the 'Run DataLab Test' wizard window. The left sidebar contains a list of steps: DataLab, Power Options, Choose Lab Groups, and Summary. The 'Summary' step is currently selected and highlighted. The main area of the wizard displays the following configuration details:

Your settings are summarised below.	
Plan Name:	Replica Plan
Scope:	Exchange Administrators
DataLab:	172.17.53.15\Exchange vLab
Lab Group(s):	prgtwesr00
Power Options:	Test and keep powered on for 2 Hours

At the bottom right of the wizard, there are three buttons: 'Back', 'Finish', and 'Cancel'. The 'Finish' button is highlighted in blue.

Step 5. Track Test Progress

The lab will power on, start lab groups and begin testing the plan. To track the lab progress, switch to the [DataLab Details page](#).

TIP

If the lab halts, the plan will fail to be tested. To learn how to resume plan testing, see [Managing Halted Replica Plans](#).

As soon as the test is over, the [DataLab Test Report](#) will be generated. The plan and the DataLab will be powered off or will keep running, depending on the power options chosen in the **Run DataLab Test** wizard.

NOTE

Even if you have enabled the **Test then power off after** option, the test will be considered to be completed when all plan steps have been run. The DataLab Test Report will be generated at that point.

If you want to receive notifications on errors that occur while powering off the DataLab, you must connect an SMTP server, add recipients and subscribe to **DataLab Test reports** as described in section [Configuring Notification Settings](#).

Testing Restore Plans

To start on-demand testing for a restore plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan.
3. From the **Verify** menu, choose **Run DataLab Test**.
4. Complete the **Run DataLab Test** wizard:
 - a. [Choose a test method](#).
 - b. [Select a DataLab](#).
 - c. [Select a recovery location](#).
 - d. [Choose whether you want to power off the lab after the testing process is over](#).
 - e. [Add lab groups](#).
 - f. [Choose whether you want to check restore points for possible ransomware](#).
 - g. [Finish working with the wizard](#).
6. [Track the progress of plan testing](#).

Step 1. Choose Test Method

At the **Test Method** step of the wizard, choose whether you want to verify both backups of plan machines and the recovery location used to restore the machines, or backups only.

- If you select the **Quick Test** option, Orchestrator will verify whether machines included in the plan will be able to recover from their backup files.

In this case, plan machines will be verified in the Instant VM Recovery environment.

- If you select the **Full Restore Test** option, Orchestrator will not only verify that vSphere and agent backups are ready-to-use, but also check that the recovery location to which the machines will be restored is available and has enough resources to support the recovery process.

In both cases, Orchestrator will run all verification steps added to the plan to make sure that the plan will be able to complete successfully.

The screenshot shows the 'Run DataLab Test' wizard window. The title bar is 'Run DataLab Test' with a close button. The left sidebar contains the following steps: 'Test Method' (highlighted), 'DataLab', 'Recovery Location', 'Power Options', 'Choose Lab Groups', 'Ransomware scan', and 'Summary'. The main area is titled 'Choose the test method' and contains two radio button options: 'Quick Test' and 'Full Restore Test'. The 'Full Restore Test' option is selected. Below the 'Quick Test' option, the text reads: 'Orchestrator will perform a quick test in the Instant VM Recovery environment and will require minimal additional storage space.' Below the 'Full Restore Test' option, the text reads: 'Orchestrator will perform a full restore in the recovery location and will require sufficient storage space to recover all machines. This method gives the most accurate value for real-world RTO and performance.' At the bottom right, there are 'Next' and 'Cancel' buttons.

Run DataLab Test	
Test Method	Choose the test method
DataLab	<input type="radio"/> Quick Test Orchestrator will perform a quick test in the Instant VM Recovery environment and will require minimal additional storage space.
Recovery Location	<input checked="" type="radio"/> Full Restore Test Orchestrator will perform a full restore in the recovery location and will require sufficient storage space to recover all machines. This method gives the most accurate value for real-world RTO and performance.
Power Options	
Choose Lab Groups	
Ransomware scan	
Summary	
Next Cancel	

Step 2. Select DataLab

At the **DataLab** step of the wizard, select a DataLab in which the plan will be verified.

For a DataLab to be displayed in the **Available DataLabs** list, it must be assigned to the scope as described in section [Assigning and Configuring DataLabs](#).

Run DataLab Test

Test Method

DataLab

Recovery Location

Power Options

Choose Lab Groups

Ransomware scan

Summary

Choose a DataLab

Type any part of Lab name to filter

Available DataLabs

172.17.53.15\SQL vLab

172.17.53.111\Virtual Lab 1

Back

Next

Cancel

Step 3. Select Recovery Location

At the **Recovery Location** step of the wizard, select a location to which inventory groups included in the plan will be restored.

For a recovery location to be displayed in the list of available recovery locations, it must be created and included into the list of inventory items available for the scope, as described in section [Managing Recovery Locations](#).

TIPS

1. For the test to run successfully, you must map isolated networks of the virtual lab to all target networks present in the [network mapping table](#) of the selected recovery location. In case you want any of the recovered VMs to be connected to the same networks as the source machines, you must map isolated networks of the virtual lab to those source networks.

To do that, configure the **Isolated Networks** settings of the virtual lab in the Veeam Backup & Replication console, as described in the Veeam Backup & Replication User Guide, section [Recovery Verification](#).

2. If you have selected the **Quick Test** option at the **Test Method** step of the wizard, you can only select a location that has [Instant VM Recovery enabled](#).

If you want to test the plan using a location with Instant VM Recovery enabled (location A) but then to restore to a location with Instant VM Recovery disabled (location B), clone the location B and change the Instant VM Recovery setting for the clone. Then, use the location A for testing and the location B for the recovery.

Name	VMs	Agents	Instant VM Recovery
Original VM Location	Enabled	Disabled	Disabled
Gold	Enabled	Enabled	Enabled

Step 4. Choose Power Options

At the **Power Options** step of the wizard, choose an action to perform after the testing process is over:

- To power off plan machines and the lab, select the **Test then power off immediately** option.
- To keep plan machines and the lab running in case you are willing to perform further tests, select the **Test then power off after** option.

Use the **Test then power off after** field to book a time slot in the lab schedule and prevent other tests from being scheduled for the same period.

NOTE

If you have selected a starting or running lab at the **DataLab** step of the wizard, the lab will not be powered off after the testing process is over — even if the **Test then power off immediately** option is selected. In this case, Orchestrator will power off only plan machines and keep the lab running.

The screenshot shows the 'Run DataLab Test' wizard window. The left sidebar contains the following steps: Test Method, DataLab, Recovery Location, Power Options (highlighted), Choose Lab Groups, Ransomware scan, and Summary. The main area is titled 'Estimate the expected test duration' and contains two radio button options: 'Test then power off immediately' (unselected) and 'Test then power off after' (selected). The 'Test then power off after' option has a spinner box set to '1' and the unit 'hours'. Below these options is an information icon (i) with the text: 'Plan VMs and the DataLab will be powered off when the specified time period expires regardless of whether the testing process is over or not.' At the bottom right of the window are three buttons: 'Back', 'Next', and 'Cancel'.

Step 5. Add Lab Groups

At the **Choose Lab Groups** step of the wizard, add the required lab groups to support the test environment.

For a lab group to be displayed in the **Available Lab Groups** list, it must be created and configured as described in section [Creating Lab Groups](#).

NOTE

All default lab groups previously created by an Administrator will automatically become preselected in the **Lab Groups to use** list, and you will not be able to remove them. For more information, see [Working with Default Lab Groups](#).

The screenshot shows the 'Run DataLab Test' wizard window. The left sidebar contains a list of steps: Test Method, DataLab, Recovery Location, Power Options, Choose Lab Groups (highlighted), Ransomware scan, and Summary. The main area is titled 'Choose Lab Groups to be used in the DataLab environment' and includes a note: 'You cannot remove default Lab Groups added by a Orchestrator Administrator.' Below this is a search bar with the placeholder 'Type any part of VM Group name to filter' and a magnifying glass icon. To the right of the search bar is a 'View VMs' link. The main area is divided into two sections: 'Available Lab Groups' on the left, which currently shows 'No Records', and 'Lab Groups to use' on the right, which contains a single entry 'Datastore - esx01 -das02'. Between these two sections are 'Add >' and '< Remove' buttons. At the bottom right of the window are 'Back', 'Next', and 'Cancel' buttons.

Step 6. Run Ransomware Scan

At the **Ransomware scan** step of the wizard, choose whether you want to check restore points created for machines included in the plan for possible ransomware.

By design, Orchestrator checks only the most recently created restore point for each machine and stops plan testing if the restore point is infected. For more information on ransomware scan, see [How Orchestrator Performs Ransomware Scan](#).

IMPORTANT

- Ransomware scan is supported only for Windows-based machines.
- Ransomware scan is not supported for restore points stored in object storage repositories.

Run DataLab Test

Test Method

DataLab

Recovery Location

Power Options

Choose Lab Groups

Ransomware Scan

Summary

Ransomware Scan

Scan restore points for viruses, malware and ransomware using Veeam Secure Restore. Virus-scanning can iterate through multiple restore points, starting with the most recent, until a clean point is found. For more information see the [User Guide](#).

☒ Run ransomware scan

Back

Next

Cancel

TIP

Orchestrator does not scan machines added to lab groups. If you want to perform ransomware scan for machines included in a lab group, add these machines to a restore plan.

Step 7. Finish Working with Wizard

At the **Summary** step of the wizard, review configuration information and click **Finish**.

Run DataLab Test

Test Method

DataLab

Recovery Location

Power Options

Choose Lab Groups

Ransomware scan

Summary

Your settings are summarized below

Plan Name:

Test Restore Plan

Scope:

SQL Administrators

DataLab:

172.17.53.15\SQL vLab

Lab Group(s):

Datastore - esx01-das2

Power Options:

Test and keep powered on for 1 Hour

Test Method:

Full Restore Test

Recovery Location:

Original VM Location (IVR Enabled - Yes)

Ransomware Scan:

Enabled

Restore points to scan (max):

1

If no clean restore point found:

Cancel restore

Back

Finish

Cancel

Step 8. Track Test Progress

The lab will power on, start lab groups and begin testing the plan. To track the lab progress, switch to the [DataLab Details page](#).

TIP

If the lab halts, the plan will fail to be tested. To learn how to resume plan testing, see [Managing Halted Restore Plans](#).

As soon as the test is over, the [DataLab Test Report](#) will be generated. The plan and the DataLab will be powered off or will keep running, depending on the power options chosen in the **Run DataLab Test** wizard.

NOTE

Even if you have enabled the **Test then power off after** option, the test will be considered to be completed when all plan steps have been run. The DataLab Test Report will be generated at that point.

If you want to receive notifications on errors that occur while powering off the DataLab, you must connect an SMTP server, add recipients and subscribe to **DataLab Test reports** as described in section [Configuring Notification Settings](#).

Testing Storage Plans

To start on-demand testing for a storage plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan.
3. From the **Verify** menu, choose **Run DataLab Test**.
4. Complete the **Run DataLab Test** wizard:
 - a. [Select a DataLab](#).
 - b. [Choose whether you want to power off the lab after the testing process is over](#).
 - c. [Add lab groups](#).
 - d. [Finish working with the wizard](#).
6. [Track the progress of plan testing](#).

Step 1. Select DataLab

At the **DataLab** step of the wizard, select a DataLab in which the plan will be verified.

For a DataLab to be displayed in the **Available DataLabs** list, it must be assigned to the scope as described in section [Assigning and Configuring DataLabs](#).

The screenshot shows the 'Run DataLab Test' wizard interface. The title bar is 'Run DataLab Test' with a close button. The left sidebar has four items: 'DataLab' (selected), 'Power Options', 'Choose Lab Groups', and 'Summary'. The main content area is titled 'Choose a DataLab'. It features a search bar with the placeholder text 'Type any part of Lab name to filter' and a magnifying glass icon. Below the search bar is a table titled 'Available DataLabs'.

Available DataLabs	
DRVirtual Lab 1	Powered Off
DRISandbox01	Powered Off

At the bottom right of the wizard, there are two buttons: 'Next' and 'Cancel'.

Step 2. Choose Power Options

At the **Power Options** step of the wizard, choose an action to perform after the testing process is over:

- To power off plan VMs and the lab, select the **Test then power off immediately** option.
- To keep plan VMs and the lab running in case you are willing to perform further tests, select the **Test then power off after** option.

Use the **Test then power off after** field to book a time slot in the lab schedule and prevent other tests from being scheduled for the same period.

NOTE

If you have selected a starting or running lab at the **DataLab** step of the wizard, the lab will not be powered off after the testing process is over — even if the **Test then power off immediately** option is selected. In this case, Orchestrator will power off only plan VMs and keep the lab running.

The screenshot shows the 'Run DataLab Test' wizard with the 'Power Options' step selected. The left sidebar contains links for 'DataLab', 'Power Options' (highlighted), 'Choose Lab Groups', and 'Summary'. The main area is titled 'Estimate the expected test duration' and contains two radio button options: 'Test then power off immediately' and 'Test then power off after'. The 'Test then power off after' option is selected, and a time field next to it shows '2' hours. Below the options is an information icon and a note: 'Plan VMs and the DataLab will be powered off when the specified time period expires regardless of whether the testing process is over or not.' At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

Run DataLab Test	
DataLab	Estimate the expected test duration
Power Options	<input type="radio"/> Test then power off immediately
Choose Lab Groups	<input checked="" type="radio"/> Test then power off after <input type="text" value="2"/> hours
Summary	<p>i Plan VMs and the DataLab will be powered off when the specified time period expires regardless of whether the testing process is over or not.</p>
<div>Back Next Cancel</div>	

Step 3. Add Lab Groups

At the **Choose Lab Groups** step of the wizard, add the required lab groups to support the test environment.

For a lab group to be displayed in the **Available Lab Groups** list, it must be created and configured as described in section [Creating Lab Groups](#).

NOTE

All default lab groups previously created by an Administrator will automatically become preselected in the **Lab Groups to use** list, and you will not be able to remove them. For more information, see [Working with Default Lab Groups](#).

Run DataLab Test

DataLab

Power Options

Choose Lab Groups

Summary

Choose Lab Groups to be used in the DataLab environment

You cannot remove default Lab Groups added by a Orchestrator Administrator.

Type any part of VM Group name to filter

View VMs

Available Lab Groups

Datastore - esx01-das1

Datastore - esx02-ds1

Datastore - esx02-ds2

Add >

< Remove

Lab Groups to use

DR Test Group - Yes

Back

Next

Cancel

Step 4. Finish Working with Wizard

At the **Summary** step of the wizard, review configuration information and click **Finish**.

Run DataLab Test

DataLab

Power Options

Choose Lab Groups

Summary

Your settings are summarised below

Plan Name:

HPE Plan

Scope:

Admin Scope

DataLab:

DR\Sandbox01

Lab Group(s):

DR Test Group - Yes

Power Options:

Test and keep powered on for 2 Hours

Back

Finish

Cancel

Step 5. Track Test Progress

The lab will power on, start lab groups and begin testing the plan. To track the lab progress, switch to the [DataLab Details page](#).

TIP

If the lab halts, the plan will fail to be tested. To learn how to resume plan testing, see [Managing Halted Storage Plans](#).

During the plan testing process, Orchestrator will create temporary clones of destination storage volumes using the [NetApp FlexClone technology](#) (for NetApp storage systems) and temporary snapshots of secondary volumes (for HPE storage systems). You can tell the resulting FlexClone volumes and temporary snapshots by the `_VDROLAB` suffix appended to their names.

IMPORTANT

To allow Orchestrator to create a clone of a destination volume, make sure the aggregate of the volume is assigned to the storage virtual machine that manages the volume. To learn how to assign aggregates to storage virtual machines, see the [NetApp ONTAP Documentation Center](#).

As soon as the test is over, the [DataLab Test Report](#) will be generated. The plan and the DataLab will be powered off or will keep running, depending on the power options chosen in the **Run DataLab Test** wizard.

NOTE

Even if you have enabled the **Test then power off after** option, the test will be considered to be completed when all plan steps have been run. The DataLab Test Report will be generated at that point.

If you want to receive notifications on errors that occur while powering off the DataLab, you must connect an SMTP server, add recipients and subscribe to **DataLab Test reports** as described in section [Configuring Notification Settings](#).

Configuring Test Scheduling

To schedule orchestration plan testing:

1. Navigate to **Lab Calendar** and click **Create Schedule**.
2. Complete the **Create Test Schedule** wizard:
 - a. [Select a scope for the schedule](#).
 - b. [Specify a schedule name and description](#).
 - c. [Select a DataLab](#).
 - d. [Add lab groups](#).
 - e. [Specify scheduling settings](#).
 - f. [Select plans that you want to test](#).
 - g. [Choose test options](#).
 - h. [Choose whether you want to power off the lab after the testing process is over](#).
 - i. [Choose whether you want to check restore points for possible ransomware](#).
 - j. [Finish working with the wizard](#).
4. [Track the progress of plan testing](#)

NOTE

When Orchestrator tests a plan according to a specific schedule, the duration of the testing process equals the RTO value configured when creating the plan. If you instruct Orchestrator to test multiple plans at the same time, the duration of the testing process equals the maximum of the configured plan RTO values. Therefore, Orchestrator does not allow you to schedule other tests in the same DataLab until the RTO is over.

Step 1. Choose Schedule Scope

At the **Scope** step of the wizard, select a scope for which you want to create the schedule.

For a scope to be displayed in the **Available Scopes** list, it must be created and customized as described in section [Managing Permissions](#).

Create Test Schedule

Scope

Schedule Info

Choose Plans

DataLab

Choose Lab Groups

Recurrence and Start

Power Options

Summary

Choose a Scope

Type any part of Scope name to filter

Available Scopes

Admin Scope

Exchange Administrators

SQL Administrators

Next

Cancel

Step 2. Specify Schedule Name and Description

At the **Schedule Info** step of the wizard, use the **Name** and **Description** fields to enter a name for the new schedule and to provide a description for future reference. The maximum length of the schedule name is 64 characters; the following characters are not supported: * : / \ ? " < > | .

Create Test Schedule

Scope

Schedule Info

Choose Plans

DataLab

Choose Lab Groups

Recurrence and Start

Power Options

Summary

Type the name and description for the test schedule

Name:

FrSchedule

Description:

Regular plan testing that occurs on Fridays

Back

Next

Cancel

Step 3. Select Plans

At the **Choose Plans** step of the wizard, select orchestration plans to be tested in a DataLab. Use the **Add** and **Remove** controls to manage available plans.

NOTE

If you select multiple plans, they all will be tested at the same time.

Create Test Schedule

Scope

Schedule Info

Choose Plans

DataLab

Choose Lab Groups

Recurrence and Start

Restore Options

Power Options

Ransomware Scan

Summary

Choose the Plans to be tested in the DataLab environment

Multiple Plans will test simultaneously.

Type any part of Plan name to filter

Available Plans

Replica

Replica

Add >

< Remove

Plans to test

Test Restore Plan

Restore

Back

Next

Cancel

Step 4. Select DataLab

At the **DataLab** step of the wizard, select a DataLab that you want to use to verify the selected orchestration plans.

For a DataLab to be displayed in the **Available DataLabs** list, it must be assigned to the scope as described in section [Assigning and Configuring DataLabs](#).

Create Test Schedule

Scope

Schedule Info

Choose Plans

DataLab

Choose Lab Groups

Recurrence and Start

Restore Options

Power Options

Ransomware Scan

Summary

Choose a DataLab

Type any part of Lab name to filter

Available DataLabs

DRVirtual Lab 1

DR\Sandbox01

Back

Next

Cancel

Step 5. Add Lab Groups

At the **Choose Lab Groups** step of the wizard, add the required lab groups to support the test environment.

For a lab group to be displayed in the **Available Lab Groups** list, it must be created and configured as described in section [Creating Lab Groups](#).

NOTE

All default lab groups previously created by an Administrator will automatically become preselected in the **Lab Groups to use** list, and you will not be able to remove them. For more information, see [Working with Default Lab Groups](#).

Create Test Schedule

Scope

Schedule Info

Choose Plans

DataLab

Choose Lab Groups

Recurrence and Start

Restore Options

Power Options

Ransomware Scan

Summary

Choose Lab Groups to be used in the DataLab environment

You cannot remove default Lab Groups added by a Orchestrator Administrator.

DataLab: Template Virtual Lab

Type any part of VM Group name to filter

View VMs

Available Lab Groups

Lab Groups to use

Only Groups previously configured using Edit Lab are available.

Back

Next

Cancel

Step 6. Specify Scheduling Settings

At the **Recurrence and Start** step of the wizard, define scheduling settings for the lab:

1. In the **Recurrence** section, choose the necessary option:
 - **Once** – to test plans once on the specified day.
 - **Weekly on** – to start testing once a week on the specified day.
 - **Monthly on** – to start testing once a month on the specified day.
2. Click the **Schedule** icon in the **Start** section, configure the necessary schedule, and click **Apply**.

The screenshot shows the 'Create Test Schedule' wizard with the 'Recurrence and Start' step selected in the left sidebar. The main panel is titled 'Choose recurrence and start'. It contains two sections: 'Start' and 'Recurrence'. The 'Start' section has a text input field showing '11/21/2022 2:55 PM' and a calendar icon. The 'Recurrence' section has three radio button options: 'Once', 'Weekly on', and 'Monthly on'. The 'Weekly on' option is selected. To the right of 'Weekly on' is a dropdown menu showing 'Friday' with a downward arrow. Below the 'Monthly on' option are two empty dropdown menus. At the bottom right of the wizard are three buttons: 'Back', 'Next', and 'Cancel'.

Scope	Choose recurrence and start
Scope	
Schedule Info	
Choose Plans	
DataLab	
Choose Lab Groups	
Recurrence and Start	Choose recurrence and start
Restore Options	
Power Options	
Ransomware Scan	
Summary	

Start

11/21/2022 2:55 PM

Recurrence

☐ Once

☒ Weekly on Friday

☐ Monthly on

Back Next Cancel

Step 7. Choose Restore Options

[This step applies only if you have included at least one restore plan in the **Plans to test** list at the **Choose Plans** step of the wizard]

At the **Restore Options** step of the wizard, choose whether you want to verify both backups of plan machines and the recovery location used to restore the machines, or backups only.

- If you select the **Quick Test** option, Orchestrator will check whether machines included in the plan will be able to recover from their backup files.

In this case, plan machines will be verified in the Instant VM Recovery environment.

- If you select the **Full Restore Test** option, Orchestrator will not only verify that vSphere and agent backups are ready-to-use, but also check that the recovery location to which the machines will be restored is available and has enough resources to support the recovery process.

In this case, Orchestrator will run all verification steps added to the plan to make sure that the plan will be able to complete successfully.

TIP

For the test to run successfully, you must map isolated networks of the virtual lab to all target networks present in the [network mapping table](#) of the selected recovery location. In case you want any of the recovered VMs to be connected to the same networks as the source machines, you must map isolated networks of the virtual lab to those source networks.

To do that, configure the isolated networks settings of the virtual lab in the Veeam Backup & Replication console, as described in the Veeam Backup & Replication User Guide, section [Recovery Verification](#).

The screenshot shows the 'Create Test Schedule' wizard with the 'Restore Options' step selected in the left sidebar. The main area is titled 'Choose a restore mode that will be used to test Restore Plans with this Schedule'. It contains two radio button options: 'Quick Test' and 'Full Restore Test'. The 'Full Restore Test' option is selected. Below each option is a descriptive paragraph. At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

Create Test Schedule	
Scope	Choose a restore mode that will be used to test Restore Plans with this Schedule
Schedule Info	<input type="radio"/> Quick Test Orchestrator will perform a quick test in the Instant VM Recovery environment and will require minimal additional storage space.
Choose Plans	<input checked="" type="radio"/> Full Restore Test Orchestrator will perform a full restore in the recovery location and will require sufficient storage space to recover all machines. This method gives the most accurate value for real-world RTO and performance.
DataLab	
Choose Lab Groups	
Recurrence and Start	
Restore Options	
Power Options	
Ransomware Scan	
Summary	
<div>Back Next Cancel</div>	

Step 8. Choose Power Options

At the **Power Options** step of the wizard, choose an action to perform after the testing process is over:

- To power off plan machines and the lab, select the **Test then power off immediately** option.
- To keep plan machines and the lab running in case you are willing to perform further tests, select the **Test then power off after** option.

Use the **Test then power off after** field to book a time slot in the lab schedule and prevent other tests from being scheduled for the same period.

NOTE

If you have selected a starting or running lab at the **DataLab** step of the wizard, the lab will not be powered off after the testing process is over — even if the **Test then power off immediately** option is selected. In this case, Orchestrator will power off only plan machines and keep the lab running.

The screenshot shows the 'Create Test Schedule' wizard with the 'Power Options' step selected in the left sidebar. The main area is titled 'Specify an expected test duration' with a subtitle 'This will help organize the DataLab schedule and let other users see how long the test may take.' There are two radio button options: 'Test then power off immediately' (unselected) and 'Test then power off after' (selected). The 'Test then power off after' option has a numeric input field set to '1' and a unit dropdown set to 'hours'. Below these options is an information box with an 'i' icon and the text: 'Plan VMs and the DataLab will be powered off when the specified time period expires regardless of whether the testing process is over or not.' At the bottom right of the wizard are three buttons: 'Back', 'Next', and 'Cancel'.

Create Test Schedule	
<ul style="list-style-type: none">ScopeSchedule InfoChoose PlansDataLabChoose Lab GroupsRecurrence and StartRestore OptionsPower OptionsRansomware ScanSummary	Specify an expected test duration This will help organize the DataLab schedule and let other users see how long the test may take.
	<input type="radio"/> Test then power off immediately
	<input checked="" type="radio"/> Test then power off after <input type="text" value="1"/> <input type="button" value="↑"/> <input type="button" value="↓"/> hours
	<div><div>i</div><div>Plan VMs and the DataLab will be powered off when the specified time period expires regardless of whether the testing process is over or not.</div></div>

Step 9. Run Ransomware Scan

[This step applies only if you have included at least one restore plan in the **Plans to test** list at the **Choose Plans** step of the wizard]

At the **Ransomware Scan** step of the wizard, choose whether you want to check restore points created for machines included in the plan for possible ransomware.

By design, Orchestrator checks only the most recently created restore point for each machine and stops plan testing if the restore point is infected. For more information on ransomware scan, see [How Orchestrator Performs Ransomware Scan](#).

IMPORTANT

- Ransomware scan is supported only for Windows-based machines.
- Ransomware scan is not supported for restore points stored in object storage repositories.

Create Test Schedule

Scope

Schedule Info

Choose Plans

DataLab

Choose Lab Groups

Recurrence and Start

Restore Options

Power Options

Ransomware Scan

Summary

Specify ransomware scan options

Scan restore points for viruses, malware and ransomware using Veeam Secure Restore. Virus-scanning can iterate through multiple restore points, starting with the most recent, until a clean point is found. For more information see the [User Guide](#).

☒

 Scan a maximum of

10

 previous restore points

If no clean restore point found

☒

 Cancel the restore and proceed to the next step

☐

 Complete the restore but do not connect the VM to the network

Back

Next

Cancel

Step 10. Finish Working with Wizard

At the **Summary** step of the wizard, review configuration information and click **Finish**.

Create Test Schedule

Scope

Schedule Info

Choose Plans

DataLab

Choose Lab Groups

Recurrence and Start

Restore Options

Power Options

Ransomware Scan

Summary

A test schedule will be created with below settings

Copy to clipboard

Name:

FrSchedule

Description:

Regular plan testing that occurs on Fridays

Scope:

Admin Scope

Plans to test:

Test Restore Plan

DataLab:

DR\Sandbox01

Lab Group(s):

Datastore - esx04-ds2

Schedule:

Weekly on Friday (from 11/21/2022)

Power Options:

Test and keep powered on for 1 Hour

Restore Options:

Full Restore Test

Ransomware Scan:

Enabled

Restore points to scan (max):

10

If no clean restore point found:

Complete restore

Back

Finish

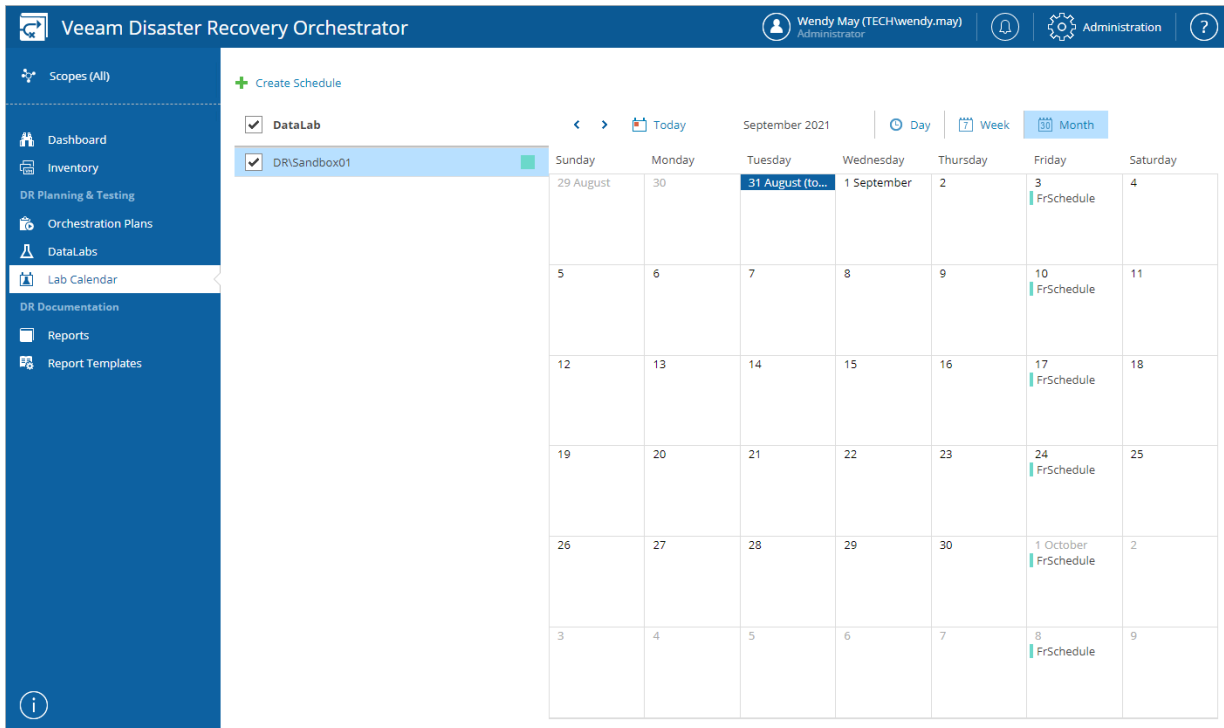
Cancel

Step 11. Track Test Progress

The created schedule will be displayed in the calendar.

TIP

You can delete a configured schedule if you no longer need it. To do that, select the schedule in the calendar, and click **Delete** at the **Details** step of the **Edit Test Schedule** wizard.



When the scheduled day and time comes, Orchestrator will power on the lab, start lab groups and begin testing the selected plans. To track lab progress, switch to the [DataLab Details](#) page.

As soon as the test is over, the [DataLab Test Report](#) will be generated. The plans and the DataLab will be powered off or will keep running, depending on the power options chosen in the **Create Test Schedule** wizard.

IMPORTANT

The selected lab will power off, all scheduled plans will fail to be tested, and the DataLab Test Report will not be generated if one of the following conditions is met:

- The lab halts.
- The lab enters either the *HALTING*, *HALTED*, *POWERING OFF* or *EDITING* state.
- The lab occurs to be already running and to include lab groups that differ from those added when configuring the schedule.

To learn how to resume plan testing, see [Managing Halted Storage Plans](#).

If you want to receive notifications on errors that occur while starting and stopping orchestration plan testing, you must connect an SMTP server, add recipients and subscribe to **DataLab Test reports** as described in section [Configuring Notification Settings](#).

Viewing Test Results

To track the plan testing progress:

1. Navigate to **DataLabs**. In the **DataLabs** column, click the lab name.

-OR-

Navigate to **Orchestration Plans** and click the name of the plan being tested.

TIP

You can connect directly to the desktop of a VM being recovered. To do that, select the VM in the **Virtual Machines** column, and click the **VM Console** link.

Orchestrator will connect to the VM through the vCenter Server system. To avoid connection failures, make sure the following requirements are met:

1. The target vCenter Server that manages the VM is running VMware vCenter Server version 6.0 or later.
2. The SSL certificate used by the target vCenter Server is valid on the machine on which you are running the browser. If not, install root certificates from the vCenter Server on both the Orchestrator server and the machine. To learn how to download and install vCenter Server root certificates, see [this VMware KB article](#).

In vSphere 6.0 and later, each newly created ESXi host is by default provisioned with a self-signed certificate from the VMware Certificate Authority. If you want to use such a certificate when accessing the VM desktop, download the root CA certificate from the host where the VM is registered. To learn how to manage certificates for ESXi hosts, see [VMware Docs](#).

The **DataLab Details** page will display real-time testing details. To track testing progress for inventory groups, machines and steps in the orchestration plan, click the plan name.

NOTE

The plan will enter the *TEST PENDING* state until the lab and all lab groups are started.

The screenshot shows the Veeam Disaster Recovery Orchestrator interface. The top navigation bar includes the Veeam logo, the title 'Veeam Disaster Recovery Orchestrator', and user information 'Wendy May (TECHwendy.may) Administrator'. The left sidebar contains navigation links: Scopes (All), Dashboard, Inventory, Orchestration Plans, DataLabs (selected), Lab Calendar, Reports, and Report Templates. The main content area is titled 'DataLab Details: DR\iu-310661-vlab' and shows a progress bar at 59% with the status 'Starting: No errors, no warnings'. Below this, there are two tables: 'DataLab & Plans' and 'Lab Groups'. The 'DataLab & Plans' table has columns for 'DataLab' and 'State'. It lists 'DR\iu-310661-vlab' with a 'Starting' state (59% complete, no errors, no warnings) and 'Test Restore Plan' with a 'Test Pending' state (Waiting for lab). The 'Lab Groups' table has columns for 'Name' and 'Status'. It lists 'DataLab Appliance - Process in sequence' (Running), 'dpt - mrk - Process 10 in parallel, Halt on error' (Running), and 'owner - audrey.allen - Process 10 in parallel, Halt...' (Queued).

DataLab	State
DR\iu-310661-vlab	Starting 59% complete, no errors, no...
Test Restore Plan	Test Pending Waiting for lab

Name	Status
DataLab Appliance - Process in sequence	Running
dpt - mrk - Process 10 in parallel, Halt on error	Running
owner - audrey.allen - Process 10 in parallel, Halt...	Queued

Test verification results will be displayed on the **Orchestration Plans** page, in the **Latest Test** and **State** columns.

Mode	Plan	Type	Scope	State	Latest Test	Latest Check	Scheduled Test	Scheduled Exe...
Disa...	Sharepoint Replica Plan	Replica	Admin Scope	Checking 33% complete	Never	Passed 9/1/2021 3:18...	None	None
In-Use	Replica Plan	Replica	Admin Scope	Permanent Failover Complete, no errors,...	Passed 9/1/2021 2:30...	Passed 8/23/2021 2:31...	9/3/2021 3:30 AM	None
In-Use	Test Restore Plan	Restore	SQL Administ...	Restore 60% complete, no er...	Passed 9/1/2021 2:49...	Warning 9/1/2021 2:44...	9/3/2021 3:30 AM	Run after "HP...
Disa...	Exchange Restore Plan	Restore	Exchange Ad...	Not Verified Failed check, no erro...	Failed 9/1/2021 2:33...	Warning 9/1/2021 2:58...	None	None
In-Use	NetApp	Storage	Admin Scope	Failover 13% complete, 2 err...	Never	Failed 9/1/2021 2:30...	None	None
In-Use	Test HPE Plan	Storage	Admin Scope	Testing 48% complete, no er...	Never	Passed 9/1/2021 2:57...	None	None
In-Use	CDP Plan	CDP Replica	Admin Scope	Failback Complete, no errors,...	Never	Passed 8/24/2021 9:31...	None	None

After the test finishes, Orchestrator will generate the [DataLab Test Report](#).

Generating Reports

Orchestrator comes with a number of reports that allow you to:

- Obtain plan configuration and change tracking data. For more information, see [Generating Plan Definition Report](#).
- Check plan configuration before running orchestration plans. For more information, see [Running Plan Readiness Check](#).
- Obtain the results of plan testing and execution. For more information, see [Viewing DataLab Test Results](#) and [Viewing Plan Execution History](#).

You can then use the reports to send them by email to engineers, auditors and managers, and to troubleshoot issues that prevent the recovery process from completing successfully. Reports are sent as PDF and DOCX files attached to report notifications. To learn how to add recipients to whom notifications will be sent, see [Configuring Notification Settings](#).

Before You Begin

All reports generated by Orchestrator are prefixed by a cover page — a report template that you select when creating a plan. This template can be edited in-line in Orchestrator using the Microsoft Word integration. When reports are generated, they are appended to the cover page template.

Orchestrator includes 7 instances of the default report template that come in the following languages: English, Japanese, Chinese, Portuguese, French, Spanish, German. Each default template instance contains example text and can be used as is — however, it is recommended to [clone and customize a template for your specific needs](#).

Note that not all parts of the default template can be modified. Some sections are visible but cannot be edited by users. These sections are automatically filled out with the plan information when a report is generated.

Managing Templates

By design, you cannot customize a Veeam default template instance itself. To generate an orchestration plan report based on a modified template, you must create a clone of an out-of-the-box template, edit the template using Microsoft Word integration, and then select it as the **Report Template** for the plan.

1. Navigate to **Report Templates**.
2. In the **Templates** column, select the default template and click **Clone**. This will create a copy of the template.
3. In the **Clone Template** window, enter a name and description for the new template, select a scope for which the template will be available, and click **Clone**.
5. Select the new template and click **Edit**. This will launch Microsoft Word.

If you are prompted for a password, specify the credentials that you used to access the Orchestrator UI.

IMPORTANT

To allow the Microsoft Word integration, Microsoft Word component of SP2 for Microsoft Office 2010 or later must be installed on the machine where the Orchestrator UI runs.

6. Customize the default template as required and save the document. All changes will be automatically uploaded to Orchestrator.

If you want to include plan properties in the report based on the customized template, you can insert the following dynamic variables: *~Created*, *~TimeZone*, *~PlanType*, *~PlanName*, *~PlanDescription*, *~PlanContactName*, *~PlanContactEmail*, *~PlanContactTel*, *~Site*, *~SiteScopeName*, *~SiteDescription*, *~SiteContactName*, *~SiteContactEmail*, *~SiteContactTel*, *~ServerName*, *~MachinesInPlan*, *~GroupsInPlan*, *~ReportType*, *~TargetRTO* and *~TargetRPO*. To populate these variables while generating the report output, Orchestrator will use properties specified during the plan creation process.

To insert a variable:

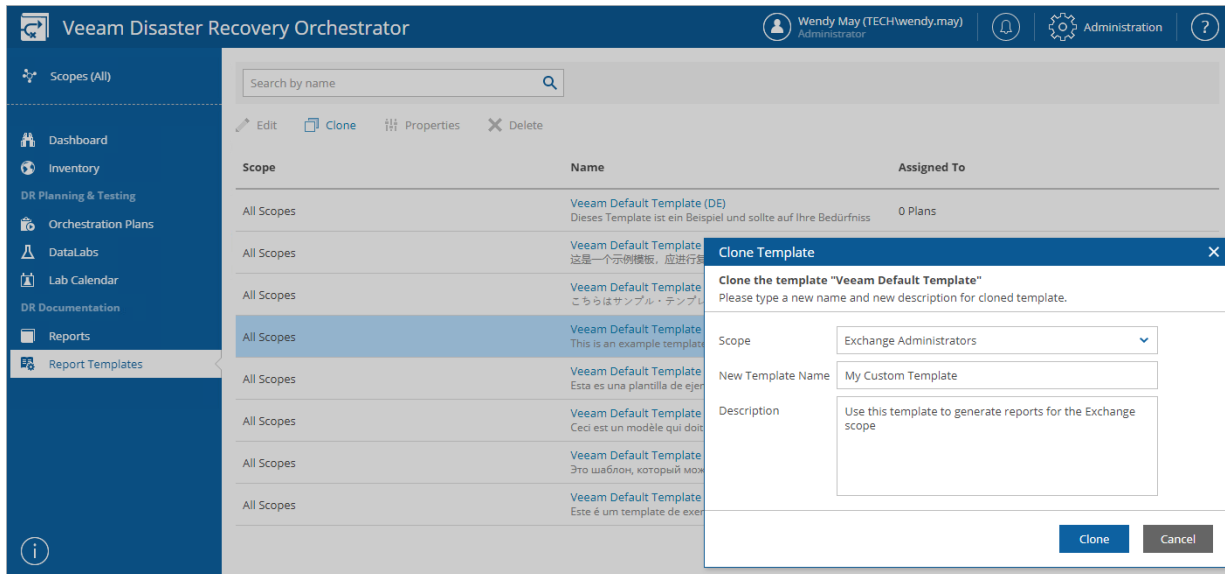
- a. Switch to the **Developer** tab. By default, the Microsoft Word ribbon does not show the tab. To display the tab:
 - i. Click **File > Options**.
 - ii. In the **Word Options** window, switch to the **Customize Ribbon** tab, select the **Developer** check box in the **Main Tabs** list, and click **OK**.
- b. Select text areas where you want to insert the variable.
- c. Click the **Rich Text Content Control** button.
- d. In the control field, enter the required variable.

NOTE

Orchestrator reports do not support Microsoft Word interactive elements (such as comments, footnotes and charts). If you include such elements in a template, they will not be included in the resulting report.

7. Navigate to **Orchestration Plans**.

8. Select the modified template as a **Report Template** for the plan. To do that, follow the instructions provided in section [Creating Replica Plans](#), [Creating CDP Replica Plans](#), [Creating Restore Plans](#), [Creating Storage Plans](#) or [Creating Cloud Plans](#).



Generating Plan Definition Report

As soon as you create an orchestration plan, you will be able to generate the **Plan Definition Report**. The report provides an easily shareable view of the following: it will show all inventory groups, steps and parameters defined by the plan, and an audit log of all changes made since the plan was created.

This document is ideal for auditors and managers, and can be used to obtain a sign-off from application owners who need to verify plan configuration.

By default, Orchestrator runs the Plan Definition Report automatically for every *ENABLED* orchestration plan at 7:00 AM daily. You can also generate the report on demand:

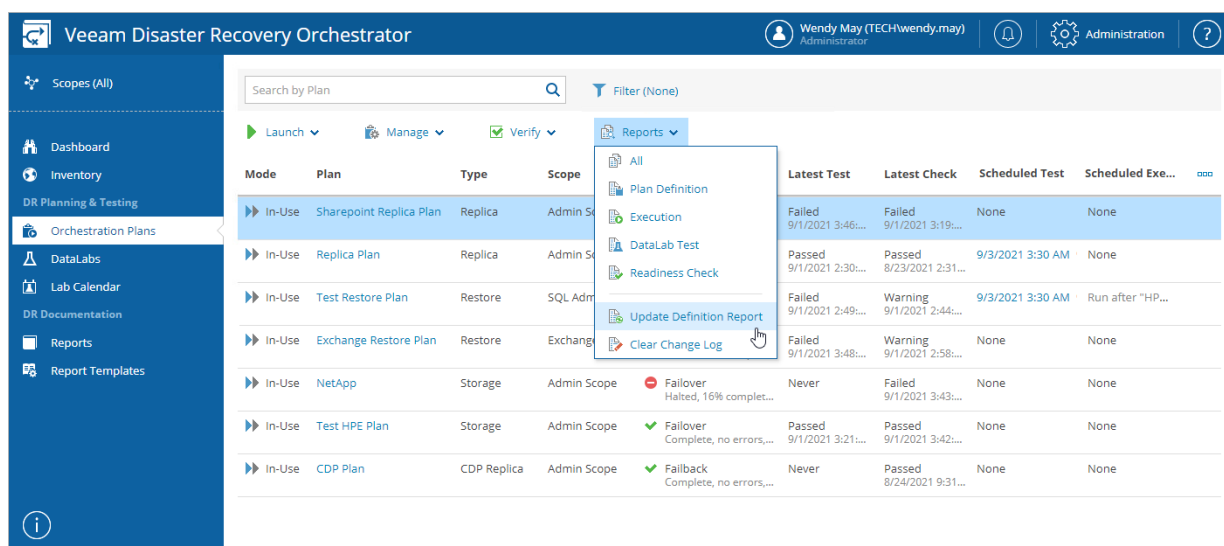
1. Navigate to **Orchestration Plans**.
2. Select a plan.
3. From the **Reports** menu, select **Update Definition Report**.

-OR-

Right-click the plan and select **Update Definition Report** from the drop-down menu.

NOTE

The **Update Definition Report** link will be unavailable in case the plan is being edited.



To access the report for an orchestration plan:

1. On the **Orchestration Plans** page, select the plan.
2. From the **Reports** menu, select **Plan Definition**.

The **Reports** page will be displayed. The **Show Plan Definition reports** option will be automatically enabled to display the available Plan Definition Report for the plan.

3. Click the plan name to download and open the Plan Definition Report.

Veeam Disaster Recovery Orchestrator

Olivia Dias (TECH@olivia.dias)
Administrator

Administration

Scopes (All)

Dashboard
Inventory
Orchestration Plans
DataLabs
Lab Calendar
Reports
Report Templates

Show:
Report type: Plan Definition
Date: All Time

Test Storage Plan
Delete
Download

Plan	Report Type	Scope	Operation	Result	Date
Selected: 0 of 4					
Test Storage Plan 2	Plan Definition	Admin Scope	Export	Generated	11/18/2022 6:51 AM
Test Storage Plan 2	Plan Definition - Summary	Admin Scope	Export	Generated	11/18/2022 6:51 AM
Test Storage Plan	Plan Definition	Admin Scope	Export	Generated	11/17/2022 11:50 AM
Test Storage Plan	Plan Definition - Summary	Admin Scope	Export	Generated	11/17/2022 11:50 AM

The Plan Definition Report will use the default report template or a [custom template](#). After the template pages, the plan definition will be appended.

By default, Orchestrator generates two types of reports:

- A summary report that includes a plan overview and summary of inventory groups included in the plan with drill-down hyperlinks to individual machines.
- A full report that also includes details on the recovery location specified for the plan, information on specific steps that will run during the recovery process and the plan change log, which allows you to track who changed plan settings, when and what was changed.

Plan Steps & Default Parameters

Process Replica VM

Parameter	Description	Default Value
Description	<p>This Step is a default step for every VM added to a Replica Plan. The Step performs the following actions depending on the plan mode.</p> <p>Failover Now mode: the Step starts the replica VM from the selected restore point.</p> <p>Undo Failover mode: the Step performs the Undo Failover operation for the replica VM by discarding all changes made to the replica VM since failover.</p> <p>Failback mode: the Step performs the Failback operation for the replica VM and applies all changes made to the source VM since failover.</p>	None
Failback Timeout	Timeout (in minutes) used for failback process. A value of zero (the default) means no timeout, so Orchestrator will wait for failback to complete.	0
Failback & Undo Failover Action	Choose Execute or Skip to define whether this step is executed during Undo Failover and Failback operations.	Execute
Test Action	Choose Execute or Skip to define whether this step is executed during plan testing in DataLab	Execute
Critical Step	Choose Yes or No to define whether this step is critical to the VM recovery. If critical step, then failure will cause the VM to be marked as failed	Yes
Failover Timeout	Timeout (in seconds) for the failover (and undo failover) processes.	1200
Retries	Number of retries to perform in case the step fails on the first try.	2
Power On Source VM after Undo	Choose Yes or No to define whether the source VM will be powered on during the Undo Failover operation.	Yes

Check license and availability

Parameter	Description	Default Value
Description	This step checks whether Orchestrator is licensed to recover this system as a VM. If not, the check displays the ordinal number of the VM in the license queue.	None
Critical Step	Choose Yes or No to define whether this step is critical to the VM recovery. If critical step, then failure will cause the VM to be marked as failed	Yes
Timeout	Timeout (in seconds) for the step	300
Retries	Number of retries to perform in case the step fails on the first try.	1
Failback & Undo Failover Action	Choose Execute or Skip to define whether this step is executed during Undo Failover and Failback operations.	Execute
Test Action	Choose Execute or Skip to define whether this step is executed during plan testing in DataLab	Execute

TIP

The plan change log may grow very large over time. To clear the change log history, do the following:

1. Select the plan. From the **Reports** menu, select **Clear Change Log**.
-OR-
Right-click the plan name and select **Reports > Clear Change Log**.
2. For security purposes, in the **Clear Change Log** window, retype your password.

To minimize the load on the server and filter the report output, you can specify the report detail level as described in section [Configuring Report Options](#).

Running Plan Readiness Check

Readiness Check is a very low-impact and fast method to confirm that configuration of an orchestration plan matches the DR environment, and therefore the plan should run successfully.

The readiness check will work through every plan step to perform specific checks against each item included in a plan. It allows you to ensure the following:

- Storage systems are detected and prepared for failover
- Datastores included in storage plans are protected by storage replication
- Replica VMs are detected and ready for failover
- Backups are detected and ready for restore
- Veeam Backup & Replication servers are online and available
- Infrastructure such as VMware vCenter, NetApp and HPE storage is online and available
- Required credentials are provided
- Required step parameters are configured

The readiness check is almost zero-impact and completes very quickly. It can therefore be run very frequently. For example, it is recommended that you run the readiness check in the following cases:

- After you create a plan, run the readiness check to verify whether the plan will be able to run successfully.
- After you edit a plan, run the readiness check to confirm that the changes are valid.
- After you test a plan in a DataLab, run the readiness check to confirm that replicas were shut down successfully and are ready for failover.
- After you make some changes to the virtual infrastructure, run the readiness check to confirm that recovery locations used for restore plans still have available resources to complete the recovery process.

By default, Orchestrator runs the readiness check automatically for every *ENABLED* orchestration plan at 8:00 AM daily. To run the check manually for a plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan.
3. From the **Verify** menu, select **Run Readiness Check**.
-OR-
Right-click the plan and select **Run Readiness Check** from the drop-down menu.
4. In the **Run Readiness Check** window, click **OK**.

Mode	Plan	Type	State	Latest Check	Latest Test	Scheduled Test	Scheduled Exe...		
In-Use	Sharepoint Replica Plan	Rep...	Testing	Halted, 83% complet...	Failed	9/1/2021 3:19...	Failed	9/1/2021 3:46...	
In-Use	Replica Plan	Rep...	Permanent Failover	Complete, no errors,...	Passed	8/23/2021 2:31...	Passed	9/1/2021 2:30...	
In-Use	Test Restore Plan	Restore	SQL Administ...	Restored	Complete, 2 errors, ...	Warning	9/1/2021 2:44...	Failed	9/1/2021 2:49...
In-Use	Exchange Restore Plan	Restore	Exchange Ad...	Testing	Halted, 83% complet...	Warning	9/1/2021 2:58...	Failed	9/1/2021 3:48...
Disa...	NetApp	Storage	Admin Scope	Not Verified	Failed check, 11 erro...	Failed	9/2/2021 10:28...	Never	None
In-Use	Test HPE Plan	Storage	Admin Scope	Fallover	Halted, 28% complet...	Passed	9/1/2021 3:42...	Passed	9/1/2021 3:21...
In-Use	CDP Plan	CDP Replica	Admin Scope	Falback	Complete, no errors,...	Passed	8/24/2021 9:31...	Never	None

As soon as the readiness check completes, the **State** and **Latest Check** columns will display the check result. The state information (*Verified* or *Not Verified*) is a rollup of the Readiness Check and DataLab test results.

To view details of the readiness check for an orchestration plan:

1. On the **Orchestration Plans** page, select the plan.
2. From the **Reports** menu, select **Readiness Check**.

The **Reports** page will be displayed. The **Show Readiness Check reports** option will be automatically enabled to list all available Readiness Check Reports for the plan.

3. Click the plan name to download and open the Readiness Check Report.

Plan	Report Type	Scope	Operation	Result	Date
Test Replica Restore	Readiness Check	Admin Scope	Checked	Success	11/16/2022 11:14 AM
Test Replica Restore	Readiness Check - Summary	Admin Scope	Checked	Success	11/16/2022 11:14 AM

The Readiness Check Report will use the default report template or a [custom template](#). After the template pages, the results of all readiness checks will be appended.

By default, Orchestrator generates two types of reports:

- A summary report that includes a plan overview and summary of inventory groups included in the plan with drill-down hyperlinks to specific machines and color-coded results of checking every plan step.

- A full report that also includes details on the recovery location specified for the plan and information on specific steps that will run during the recovery process.

Summary

Result	Details
[!] Warning	1 Warnings

Execution Details

Item	Details
Run/Scheduled By	Olivia Dias (TECH\olivia.dias)
Duration (HH:mm:ss)	00:00:03

Plan

Result	Group	Details
✓ Ready	Pre-Plan Steps	No errors
[!] Warning	Replication Job for Testing:172.24.28.186	1 VM(s) with warnings
✓ Ready	Post-Plan Steps	No errors

RPO

Result	Check	Details
[i] Info	RPO	Target RPO is 24:00:00 (HH:mm:ss)
✗ Not ready	Target RPO Met	No
✗ Not ready	Number of RPO failures	1
✗ Not ready	Worst RPO failure	Restore point age 317:39:03 (HH:mm:ss)

Licensing

Result	Check	Details
[i] Info	Summary	0 of 125 license instances used
✓ Ready	Usage	0 licenses are used in this plan (0 managed VMs, 1 new)
✓ Ready	Expiry	The license will expire in 397 days
✓ Ready	Exceeded	The license limit is not exceeded on the Orchestrator server

To minimize the load on the server and filter the report output, you can specify the report detail level as described in section [Configuring Report Options](#).

TIP

Summary information on readiness check results over all scopes will be also available on the [Home Page Dashboard](#).

Viewing DataLab Test Results

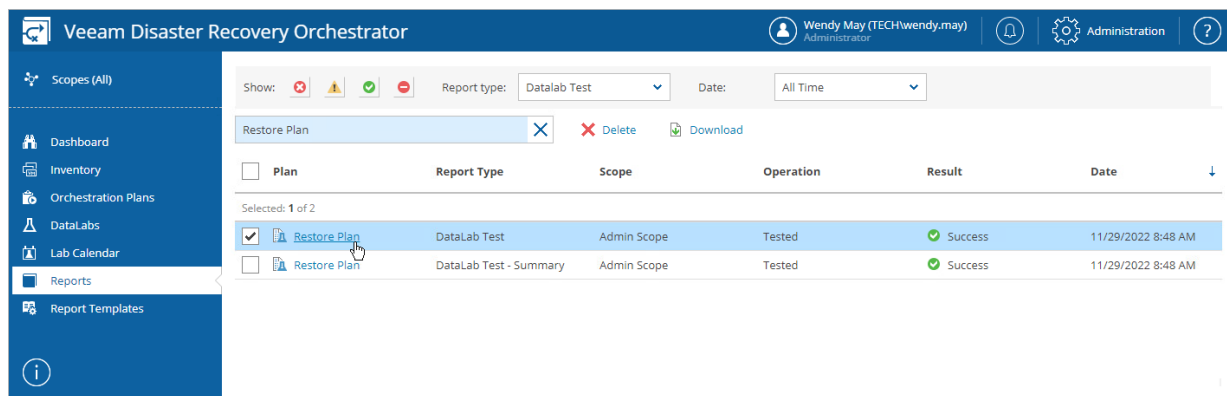
After you test a plan in an isolated Orchestrator DataLab, Orchestrator will generate the **DataLab Test Report**. The report contains test execution details and provides information on configured test environment. Summary information on plan test results for all scopes will be also available on the [Home Page Dashboard](#).

To access the report for an orchestration plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan.
3. From the **Reports** menu, select **DataLab Test**.

The **Reports** page will be displayed. The **Show DataLab Test reports** option will be automatically enabled to list all available DataLab Test Reports for the plan.

4. Click the plan name to download and open the DataLab Test Report.



The DataLab Test Report will use the default report template or a [custom template](#). After the template pages, the results of DataLab testing will be appended. The report will contain both the results of starting the DataLab and lab groups, and of testing the plan.

By default, Orchestrator generates two types of reports:

- A summary report that includes a plan overview, summary of inventory groups included in the plan, with drill-down hyperlinks to specific machines and color-coded results of testing every plan step.

- A full report that also includes details on the DataLab appliance and specific steps that will run during the recovery process. For every group, machine and step included in the plan, the processing start time and duration will be recorded.

Group Details

move rhel

[Back to All Groups](#)

mb_rhel

Result	Step	Start Time	End Time	Duration
✓ Success	Check license and availability	2:17:37 AM	2:17:37 AM	00:00:00
* Error	Process Replica VM	2:17:37 AM	2:17:37 AM	00:00:00
[!] Skipped	Check VM Heartbeat			Not run.

Step Details

Check license and availability

Timestamp	Details
2:17:37 AM	The VM is licensed
2:17:37 AM	Waiting for VM availability...
2:17:37 AM	VM is ready for processing

Process Replica VM

Timestamp	Details
2:17:37 AM	Step 'Process Replica VM' execution started. Plan mode = Tested
2:17:37 AM	The VM is included in only one group in the plan
2:17:37 AM	Source vCenter is online
2:17:37 AM	Information on the source VM is found in the VeeamONE database
2:17:37 AM	[Error] Replica for the 'mb_rhel' does not exist
2:17:37 AM	Step 'Process Replica VM' execution finished

Check VM Heartbeat

Timestamp	Details
No data	

To minimize the load on the server and filter the report output, you can specify the report detail level as described in section [Configuring Report Options](#).

TIP

Summary information on readiness check results over all scopes will be also available on the [Home Page Dashboard](#).

Viewing Plan Execution History

For each executed orchestration plan (that is, upon transition from one stable state to another), Orchestrator will generate the **Plan Execution Report**. The report contains plan performance details and provides information on each processed machine and any errors encountered during plan execution.

To access the report for an orchestration plan:

1. Navigate to **Orchestration Plans**.
2. Select the plan.
3. From the **Reports** menu, choose **Execution**.

The **Reports** page will be displayed. The **Show Execution reports** option will be automatically enabled to list all available Plan Execution Reports for the plan.

4. Click the report name to download and open the Plan Execution Report.

The screenshot shows the Veeam Disaster Recovery Orchestrator interface. The left sidebar contains navigation options: Scopes (All), Dashboard, Inventory, DR Planning & Testing, Orchestration Plans, DataLabs, Lab Calendar, DR Documentation, Reports (selected), and Report Templates. The main area displays the 'Reports' page for a selected plan, 'Restore Plan'. At the top, there are filters for 'Show:' (with icons for error, warning, success, and info), 'Report type:' (set to 'Execution'), and 'Date:' (set to 'All Time'). Below the filters, there are buttons for 'Delete' and 'Download'. A table lists the execution history with columns: Plan, Report Type, Scope, Operation, Result, and Date. The table shows 5 items, with the first one selected. The results are as follows:

Plan	Report Type	Scope	Operation	Result	Date
Restore Plan	Execution	Admin Scope	Restore	Halted	11/29/2022 7:50 AM
Restore Plan	Execution - Summary	Admin Scope	Restore	Halted	11/29/2022 7:50 AM
Plan Restore Plan was ...	Execution	Admin Scope	Reset	Disabled	11/29/2022 6:50 AM
Restore Plan	Execution	Admin Scope	Restore	Success	11/28/2022 11:38 AM
Restore Plan	Execution - Summary	Admin Scope	Restore	Success	11/28/2022 11:38 AM

The Plan Execution Report will use the default report template or a [custom template](#). After the template pages, the results of plan execution will be appended.

By default, Orchestrator generates two types of reports:

- A summary report that includes a plan overview, summary of inventory groups included in the plan, with drill-down hyperlinks to specific machines and color-coded results of processing every plan step.

- A detailed report that also includes information on specific steps that will run during the recovery process. For every group, machine and step included in the plan, the processing start time and duration will be recorded.

Summary

Overall Result	Issue Count
✓ Success	No errors

Execution Details

Item	Details
Run/Scheduled By	Wendy May (TECH\wendy.may)
Restore Point	Use the latest Restore Point
Start Time	11/17/2022 7:39:42 AM, (UTC-08:00) Pacific Time (US & Canada)
End Time	11/17/2022 7:47:33 AM, (UTC-08:00) Pacific Time (US & Canada)
Start State	Not Verified
End State	Failover - Complete
Duration (HH:mm:ss)	00:07:51

Plan

Result	Group	Start Time	End Time	Duration
✓ Success	Pre-Plan Steps	7:39:44 AM	7:41:24 AM	00:01:40
✓ Success	Asynch Group	7:41:24 AM	7:44:34 AM	00:03:10
✓ Success	SS Group	7:44:34 AM	7:47:14 AM	00:02:40
✓ Success	Post-Plan Steps	7:47:14 AM	7:47:32 AM	00:00:18

RPO

Result	Check	Details
[i] Info	RPO	Target RPO is 24:00:00 (HH:mm:ss)
✓ Success	Target RPO Met	Yes
✓ Success	Number of RPO failures	None
✓ Success	Worst RPO failure	None

RTO

Result	Check	Details
[i] Info	RTO	Target RTO is 01:00:00 (HH:mm:ss)
[i] Info	Duration	Plan execution duration was 00:07:51 (HH:mm:ss)
✓ Success	Target RTO Met	RTO achieved

Recovery Locations

Result	Resource	Details
✓ Success	SVM1	No errors

To minimize the load on the server and filter the report output, you can specify the report detail level as described in section [Configuring Report Options](#).

TIP

Summary information on plan execution results over all Orchestrator scopes will be also available on the [Home Page Dashboard](#).

Configuring Report Options

By default, all Orchestrator reports are generated with the highest level of detail. To minimize the load on the server and filter the report output, you can specify less granular report settings.

1. Switch to the **Administration** page.
2. Navigate to **Settings**.
3. In the **Report detail level** section, choose the report type that you want Orchestrator to generate.

IMPORTANT

This will apply to all Orchestrator reports in all scopes.

The screenshot shows the Veeam Disaster Recovery Orchestrator Administration interface. The left sidebar contains a navigation menu with the following items: Overview, Orchestrator Agents, vCenter Servers, Storage Systems, SMTP Server, Recovery Locations, Plan Steps, Settings (highlighted), Credentials, Roles and Scopes, Datalab Configuration, Scope Inclusions, Email Subscriptions, License, Logs, and About. The main content area is titled 'Orchestrator server details' and includes a 'Save' button and a warning message: 'The changes have not been saved yet'. The 'Orchestration Server' section contains the following fields: Name (Columbus), Description (Server to orchestrate data recovery), Contact Name (John Smith), Contact Email (john.smith@veeam.com), and Contact Tel (18002223344). The 'Report detail level' section has the heading 'Generate reports as specified below' and three radio button options: 'Two reports, both summary and all details (recommended)' (selected), 'One report with all details', and 'One summary report'. A warning message at the bottom states: 'This will apply to all reports in all scopes.'

Veeam Disaster Recovery Orchestrator

Olivia Dias (TECH\olivia.dias) Administrator

Exit Administration

Overview

Orchestrator Agents

vCenter Servers

Storage Systems

SMTP Server

Recovery Locations

Plan Steps

Settings

Credentials

Roles and Scopes

Datalab Configuration

Scope Inclusions

Email Subscriptions

License

Logs

About

Orchestrator server details

Save

The changes have not been saved yet

Orchestration Server

Name: Columbus

Description: Server to orchestrate data recovery

Contact Name: John Smith

Contact Email: john.smith@veeam.com

Contact Tel: 18002223344

Report detail level

Generate reports as specified below

☒ Two reports, both summary and all details (recommended)

☐ One report with all details

☐ One summary report

This will apply to all reports in all scopes.

Reviewing Dashboards

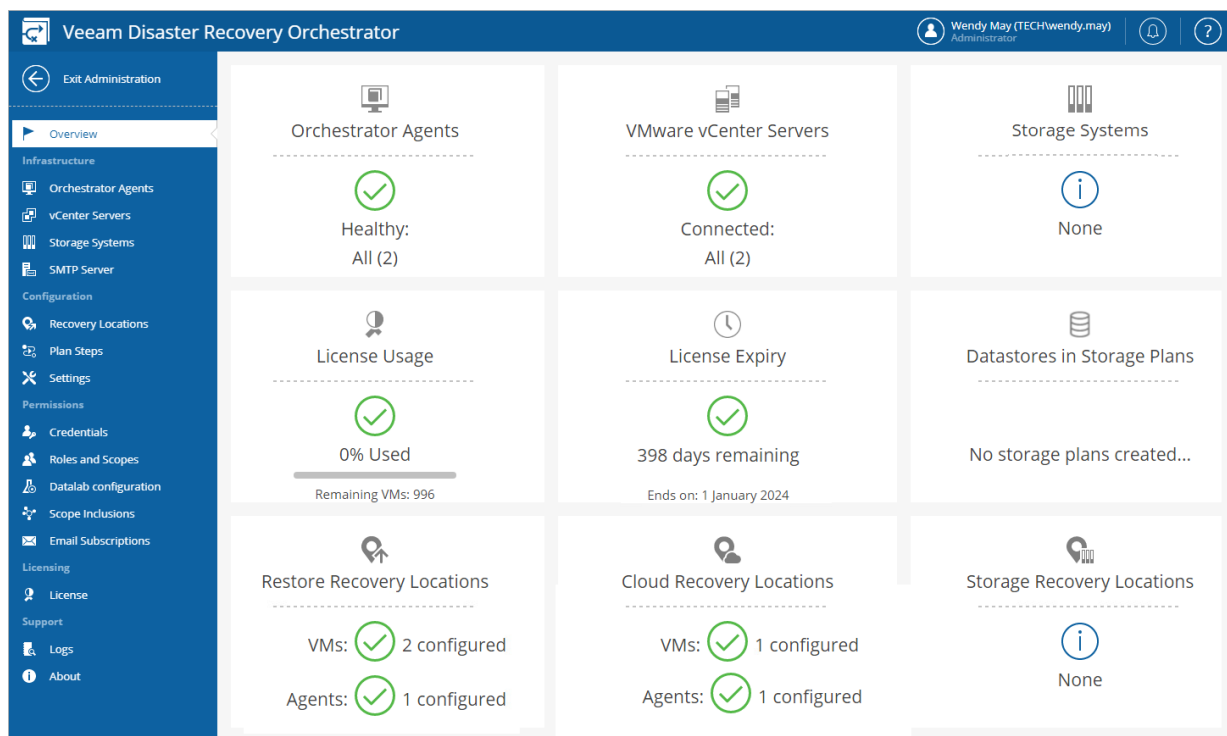
Orchestrator comes with 2 dashboards that allow you to:

- Track the health state of the connected infrastructure. For more information, see [Administration Dashboard](#).
- Analyze the readiness for disaster recovery operations across different scopes. For more information, see [Home Page Dashboard](#).

Administration Dashboard

The dashboard on the **Administration** tab of the Orchestrator UI provides at-a-glance real-time overview of your infrastructure:

- Shows the state of the connected Veeam Backup & Replication servers, vCenter Servers and storage systems.
- Displays information on license usage across the whole infrastructure.
- Shows the replication status of datastores included in storage plans.
- Displays all configured recovery locations.



Home Page Dashboard

The dashboard on the home tab of the Orchestrator UI provides an overview of all orchestration plans for the selected scope:

- **Plan Execution** chart shows the number of:
 - Halted plans
 - Plans completed successfully
 - Plans completed with warnings
 - Plans not run yet

The worst state of a plan execution is *Halted*. It means that the plan has stopped processing because of a critical error.

- **Plan Readiness Check** chart shows the number of:
 - Failed checks
 - Checks completed successfully
 - Checks completed with warnings
 - Plans not checked yet

The worst state of a plan readiness check is *Failed*. It means that the plan is not in the ready-to-run state.

- **Plan DataLab Testing** chart shows the number of:
 - Failed plan tests
 - Plan tests completed successfully
 - Plan tests completed with warnings
 - Plan tests completed with errors
 - Plans not tested yet

The worst state of a plan testing is *Failed*. It means that the test has stopped because of a critical error for a machine from a critical inventory group in the lab.

- The **Top plans by RPO Issues** and **Top plans by RTO Issues** panes show top 5 orchestration plans with the worst RPO and RTO failures, allowing you to track the achieved objectives versus targets for all plans to ensure you are meeting business service level agreements (SLAs).

- The **Current Issues** pane provides details on the most recent errors and warnings encountered while executing plans, performing plan testing and running readiness checks.

To switch to the **Plan Details** page and see the list of issues that occurred while performing plan steps for a problematic machine, click the machine name in the **VM** column. To read the message of the most recent error or warning that occurred while processing the machine, click the link in the **State** column.

The screenshot displays the Veeam Disaster Recovery Orchestrator interface. The top navigation bar includes the user profile 'Wendy May (TECHwendy.may) Administrator' and links to 'Administration' and a help icon. The left sidebar contains navigation options: 'Scopes (All)', 'Dashboard', 'Inventory', 'DR Planning & Testing', 'Orchestration Plans', 'DataLabs', 'Lab Calendar', 'DR Documentation', 'Reports', and 'Report Templates'.

The main dashboard area is divided into several sections:

- Plan Execution:** Shows counts for Running (3 of 5), Warning (2), Not Running (2), and Success (2).
- Plan Readiness Check:** Shows counts for Checked (4 of 5), Warning (3), Check Required (1), and Passed (2).
- Plan DataLab Testing:** Shows 'Test Required All'.
- Top plans by RPO Issues:** A table listing plans and their RPO status.
- Top plans by RTO Issues:** A table listing plans and their RTO status.
- Current Issues:** A table listing the most recent errors and warnings.

Top plans by RPO Issues Table:

Plan	Achieved RPO	Target RPO
Restore Plan	Exceeded by ...	1 d
CDP	Check to calc...	1 d
mb_linux2	Check to calc...	1 h
Cloud plan	Passed	15 sec
Replica Plan	Passed	15 sec

Top plans by RTO Issues Table:

Plan	Achieved RTO	Target RTO
Restore Plan	Test to calcul...	1 h
CDP	Test to calcul...	1 h
mb_linux2	Execute to ca...	1 h
Cloud plan	Passed	3 h
Replica Plan	Passed	1 h

Current Issues Table:

Plan	VM	Action	Step	State	Duration
Restore Plan	srv08	Check	Process Replica VM	Warning	1 sec
Restore Plan	backup01	Execution	Restore - Recovery	Warning	0 sec
Restore Plan	Pre-Plan	Check	Process CDP Replica VM	Warning	1 sec
Restore Plan	Pre-Plan	Check	Start Service	Warning	0 sec
CDP	vi-rr2	Execution	Process CDP Replica VM	Warning	4 sec

Adding Custom Scripts to Veeam Disaster Recovery Orchestrator

If you have a PowerShell script that you want to run as part of the recovery process, you can upload your script into Orchestrator, and it will be executed when you run your plan.

The script can run on a Veeam Backup & Replication server, on the Orchestrator server or inside each machine included in the plan. You can customize settings required for script execution and pass various parameters into the script: credentials, runtime variables (such as *vm_name* or *plan_state*) and any other custom parameters you require. Script output will be captured in plan details in the Orchestrator UI, and in [Plan Execution](#) and [DataLab Test](#) reports.

NOTE

Due to [Microsoft Azure limitations](#), script output for cloud plans is limited to 4096 bytes.

This section will demonstrate how to upload a simple example script into Orchestrator.

```
Param(
    [Parameter(Mandatory=$true)]
    [string]$folderName
)
try {
    $fileName = "HelloWorld.txt"
    "Hello World!" | Out-File -FilePath "$folderName\$fileName"
    Write-Host "File $fileName was created in folder $folderName"
}
catch {
    Write-Error "Failed to create file in folder $folderName"
    Write-Error $_.Exception.Message
}
```

Requirements

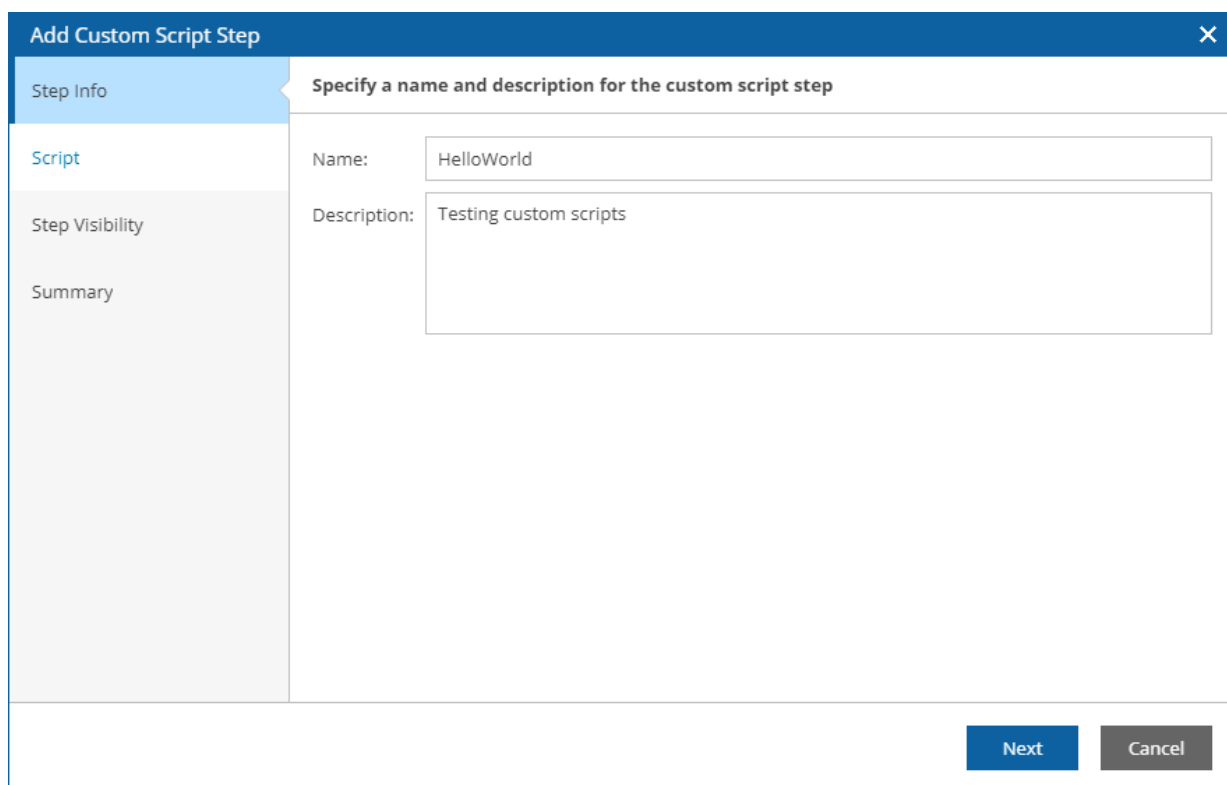
If you want to create a custom script and execute it when running an orchestration plan, you must take into account the following considerations.

- The script you want to use must be a PowerShell script. Orchestrator 6.0 supports PowerShell scripts only.
- To allow the script to run inside a machine guest OS, it is required that you have Microsoft PowerShell 3.0 and .Net Framework 4.0 installed on each machine for which you enable the custom script step.
- To allow the script to run on a Veeam Backup & Replication server, no additional software is required.

Running Custom Scripts in Orchestrator

To upload an existing script into Orchestrator:

1. Switch to the **Administration** page.
2. Navigate to **Plan Steps**.
3. In the **Steps** column, click **Add**.
4. Complete the **Add Custom Script Step** wizard:
 - a. At the **Step Info** step, enter a name for the custom script step and to provide a description for future reference. The maximum length of the step name is 64 characters; the following characters are not supported: * : / \ ? " < > | .



The screenshot shows the 'Add Custom Script Step' wizard in the Veeam Orchestrator interface. The window has a blue title bar with the text 'Add Custom Script Step' and a close button. On the left, there is a sidebar with four tabs: 'Step Info' (selected and highlighted in blue), 'Script', 'Step Visibility', and 'Summary'. The main area of the wizard is titled 'Specify a name and description for the custom script step'. It contains two input fields: 'Name:' with the value 'HelloWorld' and 'Description:' with the value 'Testing custom scripts'. At the bottom right, there are two buttons: 'Next' (blue) and 'Cancel' (gray).

- b. At the **Script** step, browse to the script file.

The screenshot shows the 'Add Custom Script Step' dialog box with the 'Step Info' tab selected. The 'Script' step is highlighted in the left sidebar. The main area is titled 'Browse to the necessary script file'. It shows a 'File:' field with a file icon and the text 'HelloWorld.ps1'. Below it is a 'Preview:' section containing a PowerShell script. At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

Add Custom Script Step [X]

Step Info

Script

Step Visibility

Summary

Browse to the necessary script file

File: HelloWorld.ps1

Preview:

```
Param(
    [Parameter(Mandatory=$true)]
    [string]$folderName
)

try {
    $fileName = "HelloWorld.txt"
    "Hello World!" | Out-File -FilePath "$folderName\$fileName"
    Write-Host "File $fileName was created in folder $folderName"
}
catch {
    Write-Error "Failed to create file in folder $folderName"
    Write-Error $_.Exception.Message
}
```

Export Script...

Back Next Cancel

- c. At the **Step Visibility** step, use the **Include this Step in all Orchestrator Scopes** check box to choose whether users of any scope will be able to use the script when creating and launching orchestration plans.

If you do not select the **Include this Step in all Orchestrator Scopes** check box, you can enable the script on a per-scope basis. For more information on managing plan steps, see [Configuring Veeam Disaster Recovery Orchestrator](#).

The screenshot shows the 'Add Custom Script Step' dialog box with the 'Step Visibility' tab selected. The 'Step Info' and 'Script' steps are visible in the left sidebar. The main area contains a message about default scope inclusion and a checked checkbox for 'Include this Step in all Orchestrator Scopes'. At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

Add Custom Script Step [X]

Step Info

Script

Step Visibility

Summary

By default, the Custom Script Step will be included in all Orchestrator Scopes

If you do not want the Step to be included in all Scopes, clear the check box below. You can later control step visibility per-scope using the *Plan Components - Plan Steps* page.

☒ Include this Step in all Orchestrator Scopes

Back Next Cancel

- c. At the **Summary** step, review configuration information and click **Finish**.

Configuring Common Parameters

After you [create a custom script step](#), you can set a list of default parameters for script execution. Orchestrator already includes a number of out-of-the-box common default parameters that you can configure as described in section [Configuring Parameter Settings](#):

IMPORTANT

To allow the script to run inside the guest OS of a processed machine, it is required that you have Microsoft PowerShell 3.0 and .Net Framework 4.0 installed on each machine for which you enable this step.

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for machine recovery. If you mark the step as <i>Critical</i> , its failure for a machine from a critical inventory group will halt the plan.	No
Execute Location	Defines whether the script will run on the Veeam Backup & Replication server, on the Orchestrator server or in-guest of the machine.	Veeam Backup Server
Windows Credentials	Credentials required to gain access to the in-guest OS. Note: Applies only if the Execute Location parameter value is set to <i>In-Guest OS</i> .	—
Timeout	Maximum amount of time (in seconds) for the step to execute.	300
Retries	Number of retries that will be attempted if the step fails on the first try.	10
Failback & Undo Failover Action	Defines whether the step will be executed during the Failback and Undo Failover operations.	Skip
Test Action	Defines whether the step will be executed during plan testing in a DataLab.	Skip

To specify credentials that the script will use to run within the guest OS of a processed machine, follow the instructions provided in section [Configuring Windows Credentials Parameter](#).

Configuring Windows Credentials Parameter

If you want to provide credentials that the script will use to run within the guest OS of a machine included in an orchestration plan, do the following:

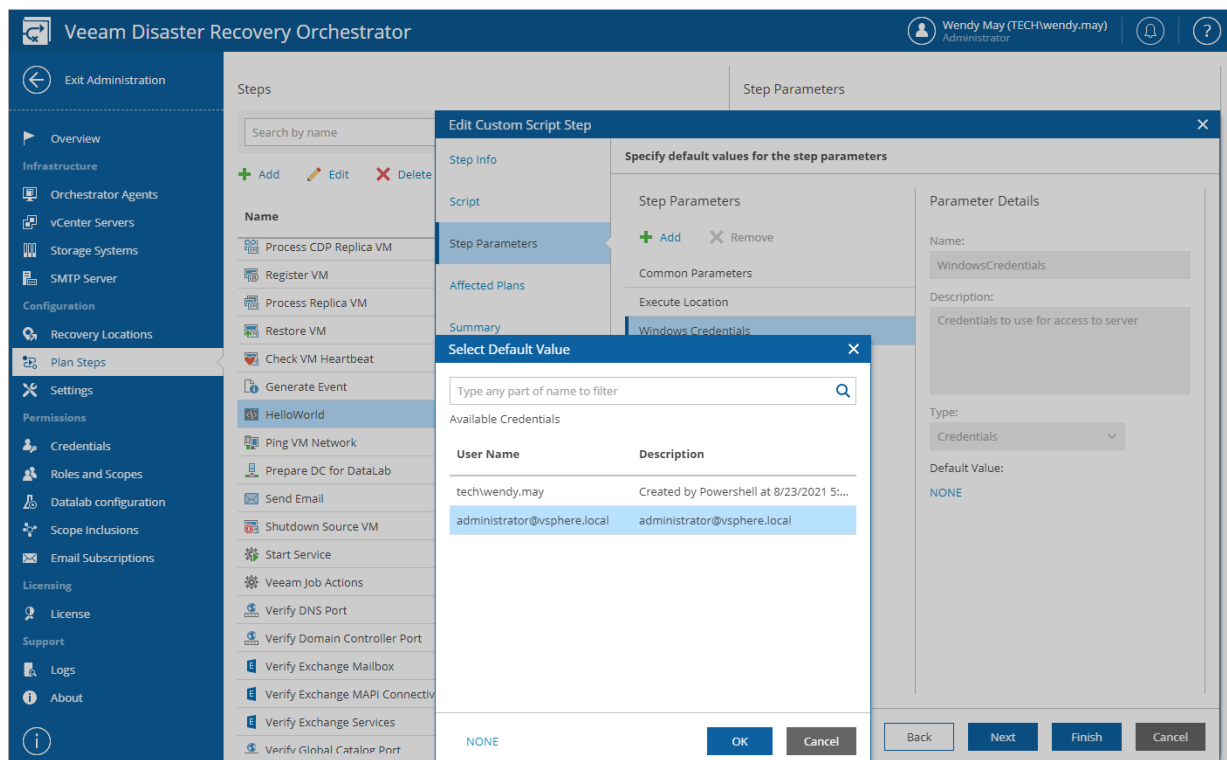
1. Add credentials that the script will use to connect to the machine when performing recovery as described in section [Managing Credentials](#).
2. Navigate to **Plan Steps**.
3. In the **Steps** column, select the script step and click **Edit**.
4. Complete the **Edit Custom Script Step** wizard:
 - a. At the **Step Parameters** step:
 - i. In the **Step Parameters** column, select *Windows Credentials*.
 - ii. In the **Parameter Details** column, click the *NONE* link below to the **Default Value** field.
 - iii. In the **Select Default Value** window, select the necessary credentials and click **OK**.
 - b. [This step applies only if you set the [Execute Location parameter](#) value to *Veeam Backup Server* or *Orchestrator Server*]

At the **Affected Plans** step, review the list of plans that will be updated to reflect the changes made to the step parameters.

- c. At the **Summary** step, review the configured settings and click **Finish**.

NOTE

If you do not specify any credentials, the script will fail to run, and the [Readiness Check test](#) will report that the **Windows Credentials** parameter settings are not configured.



Adding Credentials Parameter to Your Script

You may add multiple custom parameters of the *Credentials* type. To pass the credentials to the script, Orchestrator uses the following parameter name convention.

In the script file, a parameter with the *Credentials* type will split into 2 parameters: the first one will contain a user name and the second one will contain a password. For example, if you add a credential parameter named *SQLCreds*, Orchestrator will pass it to the script as *\$SQLCredsUsername* and *\$SQLCredsPassword*.

```
Param(  
    [string]$SQLCredsUsername,  
    [string]$SQLCredsPassword  
)
```

IMPORTANT

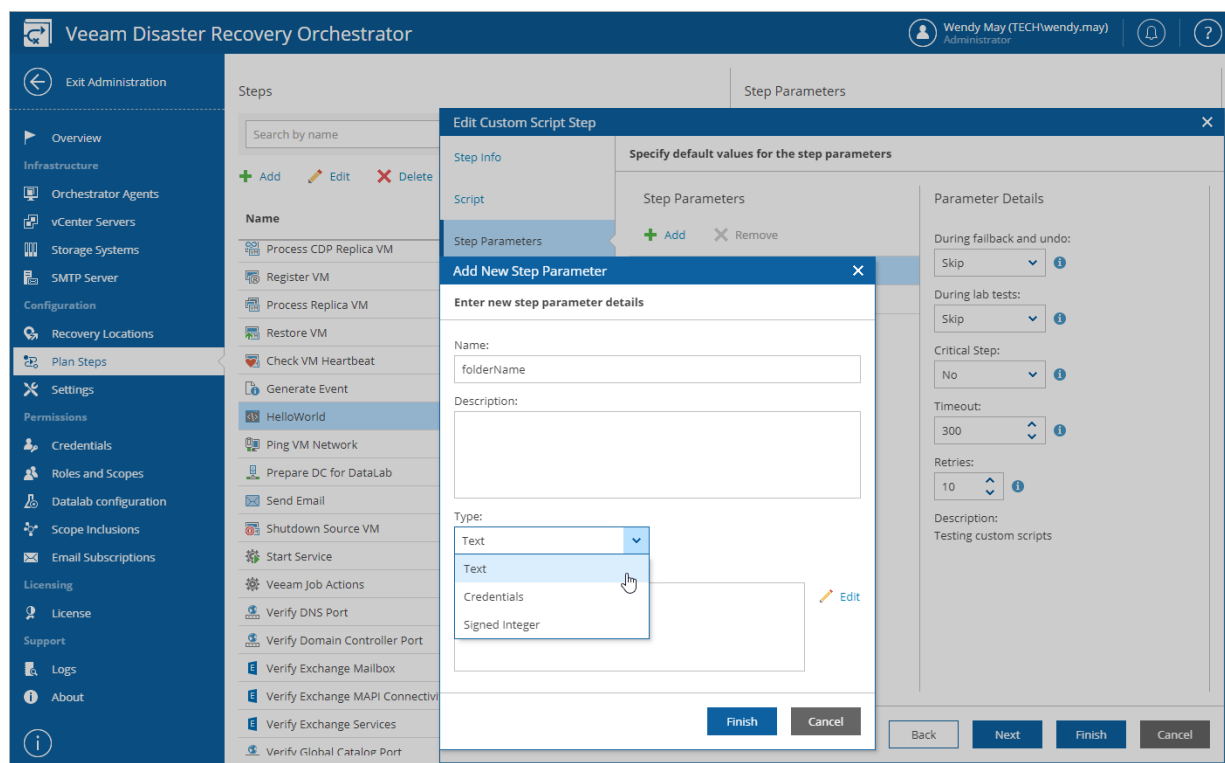
The statement must contain a comma-separated list of variables prefixed with a data type. Default values are optional.

Adding Custom Parameters

You may add any other custom parameters that your script requires (particularly, parameters of the *Credentials*, *Text* and *Integer* types).

In our example, the parameter *folderName* is required. Add this parameter as follows:

1. Switch to the **Administration** page.
2. Navigate to **Plan Steps**.
3. In the **Steps** column, select the script step and click **Edit**.
4. Complete the **Edit Custom Script Step** wizard:
 - a. At the **Step Parameters** step:
 - i. In the **Step Parameters** column, click **Add**.
 - ii. In the **Add New Step Parameter** window, specify a name for the parameter that you want to add (in this case, *folderName*), select an appropriate parameter type (in this case, *Text*), enter a value that you want to assign to the parameter (you can leave this field empty for the value to be set when the step is added to a plan), and click **Finish**.
 - b. At the **Affected Plans** step, review the list of plans that will be updated to reflect the changes made to the step parameters.
 - c. At the **Summary** step, review the configured settings and click **Finish**.

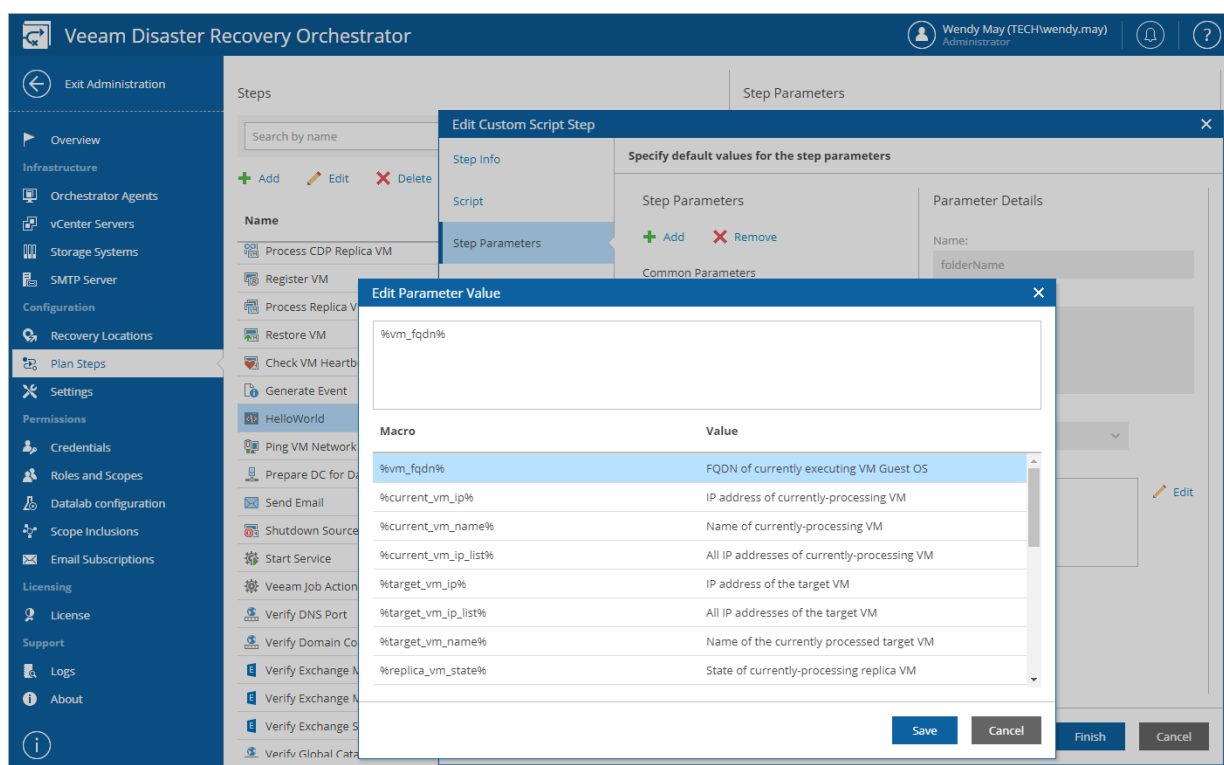


Using Runtime Parameter Variables

Orchestrator allows you to pass runtime variables into the script.

In our example, the *folderName* custom parameter has been [added recently](#), and it is required to specify a default value for it. Set a custom variable as the default value as follows:

1. Switch to the **Administration** page.
2. Navigate to **Plan Steps**.
3. In the **Steps** column, select the script step and click **Edit**.
4. Complete the **Edit Custom Script Step** wizard:
 - a. At the **Step Parameters** step:
 - i. In the **Step Parameters** column, select the parameter.
 - ii. In the **Parameter Details** column, click the **Edit** button next to the **Default Value** field.
 - iii. In the **Edit Parameter Value** window, in the list of available variables, double-click the value you want to assign to the parameter, and click **Save**.
 - b. At the **Affected Plans** step, review the list of plans that will be updated to reflect the changes made to the step parameters.
 - c. At the **Summary** step, review the configured settings and click **Finish**.



For more information on parameter variables that you can pass into a script, see [Appendix. Orchestration Plan Steps](#).

Capturing Script Errors and Warnings

To log any custom script information into step details and execution reports, make sure to use the [Write-Host](#) cmdlet in the script. To indicate errors and warnings occurred during script execution and to pass this data to Orchestrator, make sure to use the [Write-Error](#) and [Write-Warning](#) cmdlets in the script. This will post script output in the Orchestrator UI, and also in [Plan Execution](#) and [DataLab Test](#) reports.

If no errors and warnings occur during script execution, Orchestrator will report the *Success* execution state. Otherwise, in case a number of warnings and errors occurs, Orchestrator will report the worst state.

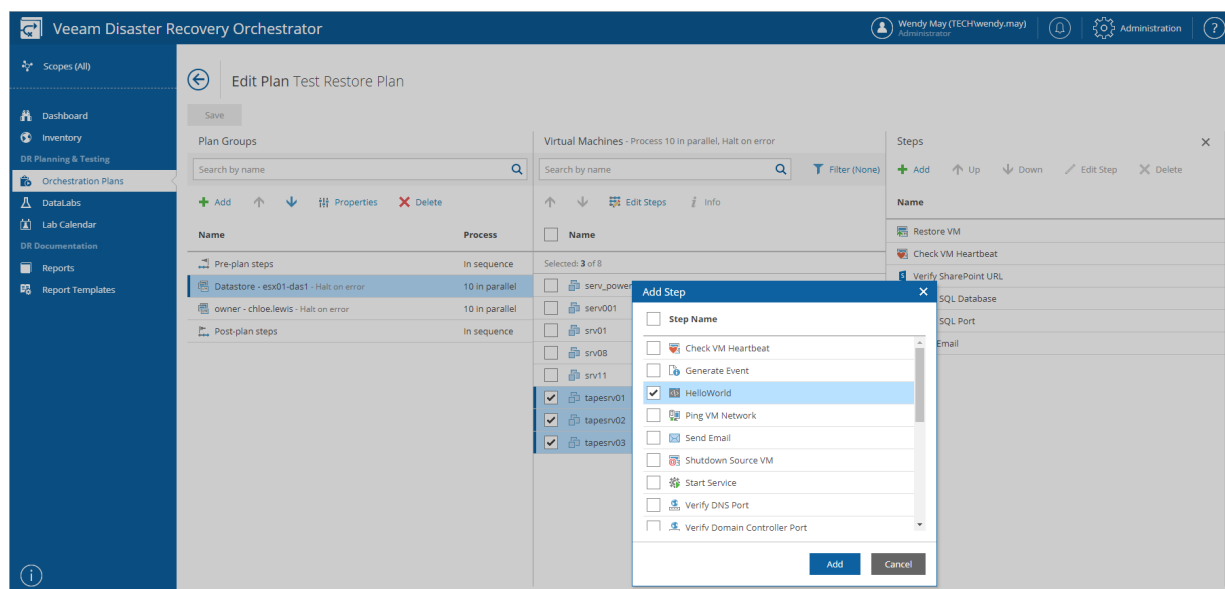
Adding Custom Script Step to Plan

For each machine included in an orchestration plan, you can add a custom script step to be performed when processing the machine:

1. Navigate to **Orchestration Plans**.
2. Select the plan and click **Manage > Edit**.
3. On the **Edit Plan** page:
 - a. In the **Plan Groups** column, select an inventory group.
 - b. In the **Virtual Machines** column, select a machine.
 - c. The **Steps** column will display the list of steps to perform for the machine.
 - i. Click **Add**.
 - ii. In the **Add Step** window, from the list of steps available for the plan, select the custom script step, and click **Add**. For more information on adding plan steps, see [Configuring Veeam Disaster Recovery Orchestrator](#).
 - d. To save changes made to the plan settings, click **Save**.

TIP

You can also add a custom step to be performed for all machines in an inventory group as described in section [Overriding VM Recovery and Protection Settings](#).



After you add the custom step for the machine in the plan, check step parameter settings and modify them if required. For more information, see [Configuring Step Parameters](#).

Appendix A. Orchestration Plan Steps

For every machine included in an orchestration plan, there are steps to be performed in sequence. This section provides information on these steps.

Orchestration plan steps require various parameters that are passed between steps, are available when editing and adding a step, and are used in messages. Steps can accept results from previous steps as input, and output to subsequent steps. Step execution results are displayed on the **Plan Details** page.

To learn how to configure step parameters, see [Editing Orchestration Plans](#).

Steps Available

During failover to the DR site and restore to a recovery location, the Orchestrator server performs the list of steps described in this section.

Check VM Heartbeat

This step checks heartbeat of the recovered VM using VMware Tools. If VMware Tools are not installed, remove this step from the plan.

You can override the following parameters for the **Check VM Heartbeat** step:

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for machine recovery. If you mark the step as <i>Critical</i> , its failure for a machine from a critical inventory group will halt the plan.	Yes
Heartbeat Count	Number of heartbeats to execute.	4
Heartbeat Await	Amount of time (in seconds) to wait between heartbeats.	10
Timeout	Maximum amount of time (in seconds) for the step to execute.	600
Retries	Number of retries that will be attempted if the step fails on the first try.	0
During Failback and Undo	Defines whether the step will be executed during the Failback and Undo Failover operations.	Skip
During Lab Tests	Defines whether the step will be executed during plan testing in a DataLab.	Execute

Create Cloud VM

This step restores the selected machine from a vSphere or Veeam agent backup to the recovery location specified for the plan.

You can override the following parameters for the **Create Cloud VM** step:

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for machine recovery. If you mark the step as <i>Critical</i> , its failure for a machine from a critical inventory group will halt the plan.	Yes
Restored VM Name	Name under which the machine will be recovered and registered. Note: By default, the recovered VM has the name of the source machine. If you want to recover the machine to the same datacenter where the source machine is registered and the source machine still resides there, it is recommended that you change the parameter value to avoid conflicts.	<i>%source_machine_name%</i>
Public IP	Defines whether a public IP address will be assigned to the recovered VM.	No
VM Configuration	Defines the VM configuration to be used to recover machines.	Configuration 1
Restore Timeout (minutes)	Maximum amount of time (in minutes) for the step to execute. Note: The default parameter value is set to 0, which means that Orchestrator will wait for the step to complete for as long as required. However, if you run the Halt action to halt the restore process, Orchestrator will halt the plan immediately, despite the infinite timeout value.	0
Retries	Number of retries that will be attempted if the step fails on the first try.	2

Generate Event

This step generates events in the Windows event log on the Orchestrator server.

You can override the following parameters for the **Generate Event** step:

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for machine recovery. If you mark the step as <i>Critical</i> , its failure for a machine from a critical inventory group will halt the plan.	No
Event Text	Event description. Note: You can use the default text, or define <i>%values%</i> which will populate during plan execution.	Plan <i>%plan_name%</i> is in state <i>%plan_state%</i>
Timeout	Maximum amount of time (in seconds) for the step to execute.	60
Retries	Number of retries that will be attempted if the step fails on the first try.	6
During Failback and Undo	Defines whether the step will be executed during the Failback and Undo Failover operations.	Execute
During Lab Tests	Defines whether the step will be executed during plan testing in a DataLab. Note: If you set the parameter value to <i>Execute</i> , keep in mind that all actions performed while testing the plan will not be reverted when the test is over.	Skip

Ping VM Network

This step pings the selected machine and VMNICs until stable response is received or timeout exceeds.

You can override the following parameters for the **Ping VM Network** step:

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for machine recovery. If you mark the step as <i>Critical</i> , its failure for a machine from a critical inventory group will halt the plan.	No
Timeout	Maximum amount of time (in seconds) for the step to execute.	600
Retries	Number of retries that will be attempted if the step fails on the first try.	0
During Failback and Undo	Defines whether the step will be executed during the Failback and Undo Failover operations.	Skip
During Lab Tests	Defines whether the step will be executed during plan testing in a DataLab.	Execute

Prepare DC for DataLab

This step is required for a domain controller to be started in a test lab environment. This must always be the first step for the domain controller in a lab group.

IMPORTANT

Starting a domain controller deployed on a physical machine is not supported.

This step ensures the VM will reboot to exit DSRM (Directory Services Restore Mode) and therefore will function correctly as a domain controller in the lab.

The **Prepare DC for DataLab** step has the following parameters, but they are not editable:

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for VM recovery. If you mark the step as <i>Critical</i> , its failure for a VM from a critical inventory group will halt the plan.	Yes
Timeout	Maximum amount of time (in seconds) for the step to execute.	60
Retries	Number of retries that will be attempted if the step fails on the first try.	0
During Failback and Undo	Defines whether the step will be executed during the Failback and Undo Failover operations.	Skip
During Lab Tests	Defines whether the step will be executed during plan testing in a DataLab.	Execute

Process CDP Replica VM

This step performs a number of actions that depend on the plan state:

- **Failover** — you will fail over from the source VM to the VM replica using the selected restore point. The VM replica will be powered on.
- **Undo Failover** — you will switch back to the source VM. Changes made to the VM replica will be discarded. The source VM will be powered on.
- **Failback** — you will fail back from the VM replica to the source VM. Changes made to the VM replica will be synchronized with the source VM. The source VM will be powered on.

You can override the following parameters for the **Process CDP Replica VM** step:

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for VM recovery. If you mark the step as <i>Critical</i> , its failure for a VM from a critical inventory group will halt the plan.	Yes
Power On Source VM After Undo	Defines whether the source VM will be powered on during the Undo Failover operation.	Yes
Failover Timeout	Timeout (in seconds) used for the Failover and Undo Failover operations.	1200
Failback Timeout	Timeout (in minutes) used for the Failback operation. Note: The default parameter value is set to <i>0</i> , which means that Orchestrator will wait for the step to complete for as long as required. However, if you run the Halt action to halt the failback process, Orchestrator will halt the plan immediately, despite the infinite timeout value.	0
Retries	Number of retries that will be attempted if the step fails on the first try.	2
During Failback and Undo	Defines whether the step will be executed during the Failback and Undo Failover operations.	Execute (not editable)
During Lab Tests	Defines whether the step will be executed during plan testing in a DataLab. Note: The default parameter value is set to <i>Skip</i> since the current product version does not support testing of CDP replica plans.	Skip (not editable)

Process Replica VM

This step performs a number of actions that depend on the plan state:

- **Failover** — you will fail over from the source VM to the VM replica using the selected restore point. The VM replica will be powered on.
- **Undo Failover** — you will switch back to the source VM. Changes made to the VM replica will be discarded. The source VM will be powered on.
- **Failback** — you will fail back from the VM replica to the source VM. Changes made to the VM replica will be synchronized with the source VM. The source VM will be powered on.

You can override the following parameters for the **Process Replica VM** step:

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for VM recovery. If you mark the step as <i>Critical</i> , its failure for a VM from a critical inventory group will halt the plan.	Yes
Power On Source VM After Undo	Defines whether the source VM will be powered on during the Undo Failover operation.	Yes
Failover Timeout	Timeout (in seconds) used for the Failover and Undo Failover operations.	1200
Failback Timeout	Timeout (in minutes) used for the Failback operation. Note: The default parameter value is set to <i>0</i> , which means that Orchestrator will wait for the step to complete for as long as required. However, if you run the Halt action to halt the failback process, Orchestrator will halt the plan immediately, despite the infinite timeout value.	0
Retries	Number of retries that will be attempted if the step fails on the first try.	2
During Failback and Undo	Defines whether the step will be executed during the Failback and Undo Failover operations.	Execute (not editable)
During Lab Tests	Defines whether the step will be executed during plan testing in a DataLab.	Execute (not editable)

Register VM

This step registers the selected VM on a host from a storage recovery location, changes the IP address configuration of the VM, applies the mapping specified for the location, and then powers the VM on.

NOTE

Before powering a recovered VM on, Orchestrator removes all unused swap (.VSWP) files from the default VM directory. If a custom location is used to store swap files, Orchestrator will not be able to remove them.

You can override the following parameters for the **Register VM** step:

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for VM recovery. If you mark the step as <i>Critical</i> , its failure for a VM from a critical inventory group will halt the plan.	Yes
Timeout	Maximum amount of time (in seconds) for the step to execute.	1200
Retries	Number of retries that will be attempted if the step fails on the first try.	2
During Lab Tests	Defines whether the step will be executed during plan testing in a DataLab.	Execute (not editable)

Restore VM

This step restores the selected machine to the recovery location specified for the plan.

You can override the following parameters for the **Restore VM** step:

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for machine recovery. If you mark the step as <i>Critical</i> , its failure for a machine from a critical inventory group will halt the plan.	Yes
Restored VM Name	Name under which the machine will be recovered and registered. Note: By default, the recovered VM has the name of the source machine. If you want to recover the machine to the same datacenter where the source machine is registered and the source machine still resides there, it is recommended that you change the parameter value to avoid conflicts.	<i>%source_machine_name%</i>
Restore Timeout (minutes)	Maximum amount of time (in minutes) for the step to execute. Note: The default parameter value is set to <i>0</i> , which means that Orchestrator will wait for the step to complete for as long as required. However, if you run the Halt action to halt the restore process, Orchestrator will halt the plan immediately, despite the infinite timeout value.	0
Retries	Number of retries that will be attempted if the step fails on the first try.	2
During Lab Tests	Defines whether the step will be executed during plan testing in a DataLab.	Execute (not editable)

Send Email

This step sends an email using the configured SMTP server and subscribed email addresses.

You can override the following parameters for the **Send Email** step:

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for machine recovery. If you mark the step as <i>Critical</i> , its failure for a machine from a critical inventory group will halt the plan.	No
Recipients	Recipients of the email. Note: To add multiple addresses, use commas.	—
Subject	Subject of the email. Note: You can use the default text, or define <i>%values%</i> which will populate during plan execution.	Orchestrator Email notification for <i>%plan_name%</i>
Body	Body of the email. Note: You can use the default text, or define <i>%values%</i> which will populate during plan execution.	Plan <i>%plan_name%</i> is in state <i>%plan_state%</i>
Timeout	Maximum amount of time (in seconds) for the step to execute.	60
Retries	Number of retries that will be attempted if the step fails on the first try.	6
During Failback and Undo	Defines whether the step will be executed during the Failback and Undo Failover operations.	Execute
During Lab Tests	Defines whether the step will be executed during plan testing in a DataLab. Note: If you set the parameter value to <i>Execute</i> , keep in mind that all actions performed while testing the plan will not be reverted when the test is over.	Skip

Shutdown Source VM

This step shuts down the selected source VM. It does not affect the recovered VM.

You can override the following parameters for the **Shutdown Source VM** step:

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for VM recovery. If you mark the step as <i>Critical</i> , its failure for a VM from a critical inventory group will halt the plan.	No
Timeout	Maximum amount of time (in seconds) for the step to execute.	300
Shutdown Action	Defines whether the step will shut down the guest OS of the source VM. Note: The <i>Shutdown OS</i> option requires VMware Tools to be installed in the guest OS.	Shutdown OS
Retries	Number of retries that will be attempted if the step fails on the first try.	1
During Failback and Undo	Defines whether the step will be executed during the Failback and Undo Failover operations.	Skip (not editable)
During Lab Tests	Defines whether the step will be executed during plan testing in a DataLab. Note: If you set the parameter value to <i>Execute</i> , keep in mind that all actions performed while testing the plan will not be reverted when the test is over.	Skip

Start Service

This step starts the Windows Service on the processed machine.

You can override the following parameters for the **Start Service** step:

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for machine recovery. If you mark the step as <i>Critical</i> , its failure for a machine from a critical inventory group will halt the plan.	Yes
Service Name	Name of the service to start. Note: A short ServiceName must be used.	—
Windows Credentials	Credentials required to gain access to the in-guest OS.	—
Execute Location	Defines whether the script will run on the Veeam Backup & Replication server, on the Orchestrator server or the in-guest OS.	In-Guest OS (not editable)
Timeout	Maximum amount of time (in seconds) for the step to execute.	300
Retries	Number of retries that will be attempted if the step fails on the first try.	10
During Failback and Undo	Defines whether the step will be executed during the Failback and Undo Failover operations.	Execute
During Lab Tests	Defines whether the step will be executed during plan testing in a DataLab.	Execute

Veeam Job Actions

This step allows you to perform the following job actions required to support plans: enable, disable, start and stop. For example, this step can be useful if you need to disable existing jobs that use storage snapshots in Veeam Backup & Replication.

You can override the following parameters for the **Veeam Job Actions** step:

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for machine recovery. If you mark the step as <i>Critical</i> , its failure for a machine from a critical inventory group will halt the plan.	Yes
Job Name	Name of the job to perform actions on.	—
Action	Action to perform on the job.	Enable
Wait for Completion	Defines whether Orchestrator will wait for the action to complete before proceeding to the next step.	Yes
Timeout	Maximum amount of time (in seconds) for the step to execute.	600
Retries	Number of retries that will be attempted if the step fails on the first try.	3
During Failback and Undo	Defines whether the step will be executed during the Failback and Undo Failover operations.	Skip
During Lab Tests	Defines whether the step will be executed during plan testing in a DataLab.	Execute

Verify DNS Port

This step verifies the port used to connect to the recovered VM with the Domain Naming Service role.

You can override the following parameters for the **Verify DNS Port** step:

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for machine recovery. If you mark the step as <i>Critical</i> , its failure for a machine from a critical inventory group will halt the plan.	Yes
Server	Name of the server to check. Note: The DNS name or IP address should be used.	%current_vm_ip_list%
Port	Port number to check for access to the DNS Service.	53
Execute Location	Defines whether the script will run on the Veeam Backup & Replication server, on the Orchestrator server or the in-guest OS.	Veeam Backup Server (not editable)
Timeout	Maximum amount of time (in seconds) for the step to execute.	300
Retries	Number of retries that will be attempted if the step fails on the first try.	10
During Failback and Undo	Defines whether the step will be executed during the Failback and Undo Failover operations.	Skip
During Test Tests	Defines whether the step will be executed during plan testing in a DataLab.	Execute

Verify Domain Controller Port

This step verifies the port used to connect to the recovered VM with the Active Directory DC role.

You can override the following parameters for the **Verify Domain Controller Port** step:

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for machine recovery. If you mark the step as <i>Critical</i> , its failure for a machine from a critical inventory group will halt the plan.	Yes
Server	Name of the server to check. Note: The DNS name or IP address should be used.	%current_vm_ip_list%
Port	Port number to check for access to the LDAP AD Service.	389
Execute Location	Defines whether the script will run on the Veeam Backup & Replication server, on the Orchestrator server or the in-guest OS.	Veeam Backup Server (not editable)
Timeout	Maximum amount of time (in seconds) for the step to execute.	300
Retries	Number of retries that will be attempted if the step fails on the first try.	10
During Failback and Undo	Defines whether the step will be executed during the Failback and Undo Failover operations.	Skip
During Lab Tests	Defines whether the step will be executed during plan testing in a DataLab.	Execute

Verify Exchange Mailbox

This step verifies the Exchange Mail Server accessibility.

IMPORTANT

1. To allow the script to run inside the guest OS of a processed machine, it is required that you have Microsoft PowerShell 3.0, .Net Framework 4.0 and Exchange Server 2010 (or later) installed on each machine for which you enable this step.
2. To allow the script to gain access the Exchange Mail Server to verify the Exchange mailbox, the Exchange Server must run Microsoft Exchange Web Services Managed API 2.1 (or later). The script will use the EWS Managed API to access the server.
3. To allow the script to verify the Exchange mailbox, the Exchange Mail Server must run Microsoft Windows Server 2008 R2 (or later).
4. The account used to run the script must have the *ApplicationImpersonation* permissions on the Exchange Mail Server. However, keep in mind that once you assign these permissions to the account, the Active Directory synchronization process may take up to 15 minutes for one Active Directory Site (and longer if there are multiple AD Sites involved).

After the synchronization process is over, replicate or back up your Lab Group Domain Controller so the account used to test plans also has the permissions. To learn how to manage impersonation rights, see [this CodeTwo KB article](#).

You can override the following parameters for the **Verify Exchange Mailbox** step:

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for machine recovery. If you mark the step as <i>Critical</i> , its failure for a machine from a critical inventory group will halt the plan.	Yes
Windows Credentials	Credentials required to gain access to the in-guest OS.	—
Exchange Credentials	Credentials required to gain access to the Exchange mailbox.	—
Email Address	Email address of the mailbox to check.	—
Exchange Server	Name of the machine where the Microsoft Exchange Web Services Managed API runs.	<i>%vm_fqdn%</i>
Execute Location	Defines whether the script will run on the Veeam Backup & Replication server, on the Orchestrator server or the in-guest OS.	In-Guest OS (not editable)
Timeout	Maximum amount of time (in seconds) for the step to execute.	300

Parameter	Description	Default Value
Retries	Number of retries that will be attempted if the step fails on the first try.	10
During Failback and Undo	Defines whether the step will be executed during the Failback and Undo Failover operations.	Skip
During Lab Tests	Defines whether the step will be executed during plan testing in a DataLab.	Execute

Verify Exchange MAPI Connectivity

This step logs on to all active databases on the local server to verify connectivity to the system mailbox.

IMPORTANT

1. To allow the script to run inside the guest OS of a processed machine, it is required that you have Microsoft PowerShell 3.0, .Net Framework 4.0 and Exchange Server 2013 (or later) installed on each machine for which you enable this step.
2. To allow the script to verify connectivity to the mailbox, the local server must run Microsoft Windows Server 2008 R2 (or later).

You can override the following parameters for the **Verify Exchange MAPI Connectivity** step:

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for machine recovery. If you mark the step as <i>Critical</i> , its failure for a machine from a critical inventory group will halt the plan.	Yes
Windows Credentials	Credentials required to gain access to the in-guest OS.	—
Execute Location	Defines whether the script will run on the Veeam Backup & Replication server, on the Orchestrator server or the in-guest OS.	In-Guest OS (not editable)
Timeout	Maximum amount of time (in seconds) for the step to execute.	300
Retries	Number of retries that will be attempted if the step fails on the first try.	10
During Failback and Undo	Defines whether the step will be executed during the Failback and Undo Failover operations.	Skip
During Lab Tests	Defines whether the step will be executed during plan testing in a DataLab.	Execute

Verify Exchange Services

This step verifies that Microsoft Exchange services are running on the recovered VM.

IMPORTANT

1. To allow the script to run inside the guest OS of a processed machine, it is required that you have Microsoft PowerShell 3.0, .Net Framework 4.0 and Exchange Server 2013 (or later) installed on each machine for which you enable this step.
2. To allow the script to verify that the services are running on the selected machine, the machine must run Microsoft Windows Server 2008 R2 (or later).

You can override the following parameters for the **Verify Exchange Services** step:

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for machine recovery. If you mark the step as <i>Critical</i> , its failure for a machine from a critical inventory group will halt the plan.	Yes
Windows Credentials	Credentials required to gain access to the in-guest OS.	—
Exchange Server	Name of the machine where Microsoft Exchange Server runs.	<i>%vm_fqdn%</i>
Execute Location	Defines whether the script will run on the Veeam Backup & Replication server, on the Orchestrator server or the in-guest OS.	In-Guest OS (not editable)
Timeout	Maximum amount of time (in seconds) for the step to execute.	300
Retries	Number of retries that will be attempted if the step fails on the first try.	10
During Failback and Undo	Defines whether the step will be executed during the Failback and Undo Failover operations.	Skip
During Lab Tests	Defines whether the step will be executed during plan testing in a DataLab.	Execute

Verify Global Catalog Port

This step verifies the port used to connect to the recovered VM with the Global Catalog role.

You can override the following parameters for the **Verify Global Catalog Port** step:

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for machine recovery. If you mark the step as <i>Critical</i> , its failure for a machine from a critical inventory group will halt the plan.	Yes
Server	Name of the server to check. Note: The DNS name or IP address should be used.	<i>%current_vm_ip_list%</i>
Port	Port number to check for access to the LDAP GC Service.	3268
Execute Location	Defines whether the script will run on the Veeam Backup & Replication server, on the Orchestrator server or the in-guest OS.	Veeam Backup Server (not editable)
Timeout	Maximum amount of time (in seconds) for the step to execute.	300
Retries	Number of retries that will be attempted if the step fails on the first try.	10
During Failback and Undo	Defines whether the step will be executed during the Failback and Undo Failover operations.	Skip
During Lab Tests	Defines whether the step will be executed during plan testing in a DataLab.	Execute

Verify Mail Server Port

This step verifies the port used to connect to the recovered VM with the Mail Server role.

You can override the following parameters for the **Verify Mail Server Port** step:

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for machine recovery. If you mark the step as <i>Critical</i> , its failure for a machine from a critical inventory group will halt the plan.	Yes
Server	Name of the server to check. Note: The DNS name or IP address should be used.	%current_vm_ip_list%
Port	Port number to check for access to the SMTP Service.	25
Execute Location	Defines whether the script will run on the Veeam Backup & Replication server, on the Orchestrator server or the in-guest OS.	Veeam Backup Server (not editable)
Timeout	Maximum amount of time (in seconds) for the step to execute.	300
Retries	Number of retries that will be attempted if the step fails on the first try.	10
During Failback and Undo	Defines whether the step will be executed during the Failback and Undo Failover operations.	Skip
During Lab Tests	Defines whether the step will be executed during plan testing in a DataLab.	Execute

Verify SharePoint URL

This step verifies the SharePoint Server accessibility.

IMPORTANT

1. To allow the script to run inside the guest OS of a processed machine, it is required that you have Microsoft PowerShell 3.0, .Net Framework 4.0 and SharePoint 2013 (or later) installed on each machine for which you enable this step.
2. To allow the script to verify the SharePoint Server accessibility, the server must run Microsoft Windows Server 2008 R2 (or later).
3. The account used to run the script must be assigned the *SharePoint_Shell_Access* role and must be a member of the *WSS_ADMIN_WPG* group on each processed machine.

You can override the following parameters for the **Verify SharePoint URL** step:

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for machine recovery. If you mark the step as <i>Critical</i> , its failure for a machine from a critical inventory group will halt the plan.	Yes
Windows Credentials	Credentials required to gain access to the in-guest OS.	—
SharePoint URL	Name of the SharePoint Server to check.	—
Execute Location	Defines whether the script will run on the Veeam Backup & Replication server, on the Orchestrator server or the in-guest OS.	In-Guest OS (not editable)
Timeout	Maximum amount of time (in seconds) for the step to execute.	300
Retries	Number of retries that will be attempted if the step fails on the first try.	10
During Failback and Undo	Defines whether the step will be executed during the Failback and Undo Failover operations.	Skip
During Lab Tests	Defines whether the step will be executed during plan testing in a DataLab.	Execute

Verify SQL Database

This step verifies the SQL database instance accessibility.

IMPORTANT

1. To allow the script to run inside the guest OS of a processed machine, it is required that you have Microsoft PowerShell 3.0, .Net Framework 4.0 and SQL Server 2008 (or later) installed on each machine for which you enable this step.
2. To allow the script to verify the SQL database instance accessibility, the verified SQL Server instance must run Microsoft Windows Server 2008 R2 (or later).
3. To allow the script to connect to the verified SQL Server instance, Orchestrator uses an account whose credentials are specified as values for either the [Windows Credentials](#) or [SQL Credentials](#) parameter. The account must have the *VIEW ANY DATABASE* permission. For more information, see [Microsoft Docs](#).

You can override the following parameters for the **Verify SQL Database** step:

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for machine recovery. If you mark the step as <i>Critical</i> , its failure for a machine from a critical inventory group will halt the plan.	Yes
Windows Credentials	Credentials required to gain access to the SQL Server instance that uses <i>Windows Authentication</i> . If the SQL Server instance you want to check uses <i>Windows Authentication</i> , the provided credentials will be used to connect to both the in-guest OS and the SQL instance. In this case, specify a value for the Windows Credentials parameter, and leave the SQL Credentials parameter value empty.	—
SQL Credentials	SQL account credentials required to gain access to the SQL Server instance that uses <i>SQL Server Authentication</i> . If the SQL Server instance you want to check uses <i>SQL Server Authentication</i> , Orchestrator will use SQL Server credentials to access the SQL instance, and Windows credentials to access the in-guest OS. That is why you must specify values for both the SQL Credentials and Windows Credentials parameters. Note: The SQL Credentials parameter does not accept Windows credentials.	—
SQL Instance	Name of the SQL instance to check. Note: To check all detected instances, select <i>ALL</i> .	ALL

Parameter	Description	Default Value
SQL DB	Name of the SQL database to check. Note: To check all detected databases, select <i>ALL</i> .	ALL
Execute Location	Defines whether the script will run on the Veeam Backup & Replication server, on the Orchestrator server or the in-guest OS.	In-Guest OS (not editable)
Timeout	Maximum amount of time (in seconds) for the step to execute.	300
Retries	Number of retries that will be attempted if the step fails on the first try.	10
During Failback and Undo	Defines whether the step will be executed during the Failback and Undo Failover operations.	Skip
During Lab Tests	Defines whether the step will be executed during plan testing in a DataLab.	Execute

Verify SQL Port

This step verifies the port used to connect to the recovered VM with the SQL Server role.

You can override the following parameters for the **Verify SQL Port** step:

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for machine recovery. If you mark the step as <i>Critical</i> , its failure for a machine from a critical inventory group will halt the plan.	Yes
Server	Name of the server to check. Note: The DNS name or IP address should be used.	%current_vm_ip_list%
Port	Port number to check for access to the SQL Service.	1433
Execute Location	Defines whether the script will run on the Veeam Backup & Replication server, on the Orchestrator server or the in-guest OS.	Veeam Backup Server (not editable)
Timeout	Maximum amount of time (in seconds) for the step to execute.	300
Retries	Number of retries that will be attempted if the step fails on the first try.	10
During Failback and Undo	Defines whether the step will be executed during the Failback and Undo Failover operations.	Skip
During Lab Tests	Defines whether the step will be executed during plan testing in a DataLab.	Execute

Verify Web Server Port

This step verifies the port used to connect to the recovered VM with the Web Server role.

You can override the following parameters for the **Verify Web Server Port** step:

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for machine recovery. If you mark the step as <i>Critical</i> , its failure for a machine from a critical inventory group will halt the plan.	Yes
Server	Name of the server to check. Note: The DNS/NETBIOS name or IP address should be used.	<i>%current_vm_ip_list%</i>
Port	Port number to check for access to the Web Service.	80
Execute Location	Defines whether the script will run on the Veeam Backup & Replication server, on the Orchestrator server or the in-guest OS.	Veeam Backup Server (not editable)
Timeout	Maximum amount of time (in seconds) for the step to execute.	300
Retries	Number of retries that will be attempted if the step fails on the first try.	10
During Failback and Undo	Defines whether the step will be executed during the Failback and Undo Failover operations.	Skip
During Lab Tests	Defines whether the step will be executed during plan testing in a DataLab.	Execute

Verify Web Site (IIS)

This step verifies the website accessibility.

IMPORTANT

1. To allow the script to run inside the guest OS of a processed machine, it is required that you have Microsoft PowerShell 3.0, .Net Framework 4.0 and IIS 8.0 (or later) installed on each machine for which you enable this step.
2. To allow the script to verify the website accessibility, the processed machine must run Microsoft Windows Server 2008 R2 (or later).

You can override the following parameters for the **Verify Web Site (IIS)** step:

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for machine recovery. If you mark the step as <i>Critical</i> , its failure for a machine from a critical inventory group will halt the plan.	Yes
Windows Credentials	Credentials required to gain access to the in-guest OS.	—
Website Name	Name of the website to check.	Default Web Site
Execute Location	Defines whether the script will run on the Veeam Backup & Replication server, on the Orchestrator server or the in-guest OS.	In-Guest OS (not editable)
Timeout	Maximum amount of time (in seconds) for the step to execute.	300
Retries	Number of retries that will be attempted if the step fails on the first try.	10
During Failback and Undo	Defines whether the step will be executed during the Failback and Undo Failover operations.	Skip
During Lab Tests	Defines whether the step will be executed during plan testing in a DataLab.	Execute

VM Power Actions

This step allows you to perform the following VM power actions required to support orchestration plans: power on, power off, shutdown, suspend and resume. For example, this step can be useful if you need to power off non-critical VMs in the DR site to free resources required for recovery.

IMPORTANT

Do not use this step to perform power actions on replica VMs. These actions are automatically performed during the [Process Replica VM](#) step execution.

You can override the following parameters for the **VM Power Actions** step:

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for VM recovery. If you mark the step as <i>Critical</i> , its failure for a VM from a critical inventory group will halt the plan.	No
VM Names	Names of the VMs to perform power actions on. Note: To add multiple VMs, use commas.	—
vCenter Name	Name of the vCenter Server where the VMs are located. Note: Use separate step instances for each VMware connection.	—
Power Action	Power action to perform on the VMs.	Power On
Timeout	Maximum amount of time (in seconds) for the step to execute.	300
Retries	Number of retries that will be attempted if the step fails on the first try.	1
During Failback and Undo	Defines whether the step will be executed during the Failback and Undo Failover operations. Note: If you set the parameter value to <i>Execute</i> , the step will perform an action opposite to that specified for the Power Action parameter. For example, if you set the Power Action parameter value to <i>Power On</i> , the step will power off the selected VMs during the Failback and Undo Failover operations.	Execute

Parameter	Description	Default Value
During Lab Tests	<p>Defines whether the step will be executed during plan testing in a DataLab.</p> <p>Note: If you set the parameter value to <i>Execute</i>, keep in mind that all actions performed while testing the plan will not be reverted when the test is over.</p>	Skip

Custom Script

If you have [customized your own script](#) to be used when running an orchestration plan, you can override the following parameters for the **Custom Script** step:

IMPORTANT

To allow the script to run inside the guest OS of a processed machine, it is required that you have Microsoft PowerShell 3.0 and .Net Framework 4.0 installed on each machine for which you enable this step.

Parameter	Description	Default Value
Critical Step	<p>Defines whether the step is critical for machine recovery.</p> <p>If you mark the step as <i>Critical</i>, its failure for a machine from a critical inventory group will halt the plan.</p>	No
Execute Location	Defines whether the script will run on the Veeam Backup & Replication server, on the Orchestrator server or the in-guest OS.	Veeam Backup Server
Windows Credentials	<p>Credentials required to gain access to the in-guest OS.</p> <p>Applies only if the Execute Location parameter value is set to <i>In-Guest OS</i>.</p>	—
Timeout	Maximum amount of time (in seconds) for the step to execute.	300
Retries	Number of retries that will be attempted if the step fails on the first try.	10
During Failback and Undo	Defines whether the step will be executed during the Failback and Undo Failover operations.	Skip
During Lab Tests	Defines whether the step will be executed during plan testing in a DataLab.	Skip

Protect VM Group

When you [create a new orchestration plan](#) or [add an inventory group to an existing plan](#), you have an option to run the **Protect VM Group** step to protect machines included in the plan.

This step creates a new template-based backup or replication job to back up or replicate machines in the specified inventory group as soon as the recovery process completes. Note that for replica plans, the template job will run only after the plan enters the *PERMANENT FAILOVER* state.

IMPORTANT

The Veeam Backup & Replication server on which the template backup or replication job has been created must be connected to the vCenter Server that manages target machines.

You can override the following parameters for the **Protect VM Group** step:

Parameter	Description	Default Value
Critical Step	Defines whether the step is critical for machine recovery. If you mark the step as <i>Critical</i> , its failure for a machine from a critical inventory group will halt the plan.	No
Timeout	Maximum amount of time (in seconds) for the step to execute.	300
Retries	Number of retries that will be attempted if the step fails on the first try.	0
During Lab Tests	Defines whether the step will be executed during plan testing in a DataLab.	Skip (not editable)

Parameter Variables

Parameter variables are passed between steps during plan execution, and are available when editing and adding step parameters.

You can define the following variables for any step parameter that allows plain text to be entered:

Parameter Variable	Content
%vm_fqdn%	FQDN of the currently processed machine
%current_vm_ip%	IP address of the currently processed VM
%current_vm_name%	Name of the currently processed VM
%current_vm_ip_list%	All IP addresses of the currently processed VM
%replica_vm_ip%	IP address of the currently processed replica VM
%replica_vm_ip_list%	All IP addresses of the currently processed replica VM
%replica_vm_name%	Name of the currently processed replica VM
%replica_vm_state%	State of the currently processed replica VM
%source_machine_name%	Name of the source machine
%source_vm_ip%	IP address of the source VM
%source_vm_ip_list%	All IP addresses of the source VM
%source_vm_name%	Name of the source VM
%plan_name%	Name of the orchestration plan
%vao_server_name%	Name of the Orchestrator server
%plan_state%	Current state of the orchestration plan
%plan_test_mode%	Boolean variable that indicates whether the plan is currently being tested (True/False)

Parameter Variable	Content
%group_name%	Name of the currently processed inventory group
%plan_summary%	Output information on the orchestration plan (error/warning/success for all steps)
%group_summary%	Output information on the currently processed inventory group
%vm_summary%	Output information on the currently processed VM
%vao_ui%	URL to access HOME page of the Orchestrator UI
%plan_vms%	List of all machines included in the orchestration plan

Appendix B. Grouping and Categorization

IMPORTANT

Out of the box, Veeam ONE Client comes with the predefined category named B&R Job. This category includes groups of VMs protected by Veeam backup jobs, Veeam replication jobs and Veeam CDP policies that are managed by Veeam Backup & Replication servers connected to Orchestrator. Note that vCenter Servers where these VMs belong must also be connected to Orchestrator to allow Veeam ONE Client to categorize the VMs.

DO NOT rename or edit the *B&R Job* category in Veeam ONE Client — this may cause errors when trying to use inventory groups from the category in orchestration plans. You can delete this category if you no longer need it. To learn how to delete categories, see the Veeam Disaster Recovery Orchestrator Group Management Guide, section [Deleting Categories](#).

Tag-Based Categorization

[This section does not apply to machines protected by Veeam agents]

You can group VMs based on vCenter Server tags that dynamically categorize objects by metadata attached in the vSphere inventory. VM membership in these groups cannot be edited in the Orchestrator UI — you must modify group properties in Veeam ONE Client or modify tags in the vSphere environment.

To learn how to group VMs using tags collected from the vCenter Server, see the Veeam Disaster Recovery Orchestrator Group Management Guide, section [Tag-Based Categorization](#). To learn how to create tag categories and assign tags to infrastructure objects in the vSphere inventory, see [VMware Docs](#).

TIP

After you create a tag category, edit a tag category or assign a tag to an object in the vSphere inventory, the changes may not appear in the Orchestrator UI immediately — the data synchronization process between Orchestrator and Veeam ONE may take more than 3 hours to complete.

You can speed up the data synchronization process using Veeam ONE Reporter installed as part of the embedded Veeam ONE server. To do that:

1. In a web browser, navigate to the Veeam ONE Reporter web address.
The address consists of an FQDN of the Orchestrator server and the website port specified during installation (by default, **1239**). Note that Veeam ONE Reporter is available over HTTPS.
`https://hostname:1239/`
2. Navigate to **Data Collection**.
3. Click **Start**.

Custom Categorization

You can create your own categories and inventory groups using the functionality of Veeam ONE Client. Machine membership in these groups cannot be edited in the Orchestrator UI – you must modify group properties in Veeam ONE Client. You can group machines using the following methods:

- **Single-parameter categorization** creates a group for each unique value of the selected property.
- **Multiple-condition categorization** allows you to combine multiple conditions that evaluate machine properties for creating groups.
- **Categorization with grouping expressions** creates a set of groups and includes machines with matching attributes into these groups.

To learn how to group machines in Veeam ONE Client, see the Veeam Disaster Recovery Orchestrator Group Management Guide, sections [Single-Parameter Categorization](#), [Multiple-Condition Categorization](#) and [Categorization with Grouping Expressions](#).

Import-Based Categorization

You can synchronize Business View categorization data with categorization data from 3rd party software. If you have already categorized machines outside Veeam ONE Client, you can describe the categorization model using a CSV file and then import this file to Veeam ONE Client. Machine membership in these groups cannot be edited in the Orchestrator UI – you must modify categorization data in the CSV file and then import the file again.

To learn how to import categorization data using CSV files, see the Veeam Disaster Recovery Orchestrator Group Management Guide, section [Import-Based Categorization](#).

Appendix C. Getting Technical Support

Veeam offers email and phone technical support for customers on maintenance and during the official evaluation period. For better experience, provide the following details when contacting Veeam Customer Support:

- Version information for the product and its components
- Error message or accurate description of the problem you are facing
- Log files

For your convenience, the Orchestrator UI allows you to collect logs for each Orchestrator component separately. To do that:

1. Switch to the **Administration** page.
2. Navigate to **Logs**.
3. Select a check box next to the server where the Orchestrator component runs.
4. Click **Download Logs**. Logs will be saved locally in the default download folder.

NOTE

Every archive with log files that you download contains an anonymized file with the current Orchestrator configuration and statistical information. This file can be used by Orchestrator product management to improve the product. No information will be shared outside of Veeam at any time.

The screenshot displays the Veeam Disaster Recovery Orchestrator Administration interface. The left sidebar contains navigation links: Overview, Orchestrator Agents, vCenter Servers, Storage Systems, SMTP Server, Recovery Locations, Plan Steps, Settings, Credentials, Roles and Scopes, Datalab configuration, Scope Inclusions, Email Subscriptions, License, Logs (selected), and About. The main content area is titled 'Veeam Disaster Recovery Orchestrator' and shows a search bar for 'Server Name'. Below the search bar, there is a 'Download Logs' button and a date range selector set to 'From 13/08/2021 To 13/08/2021'. A table lists servers with columns for 'Server Name', 'Logs', and 'Progress'. The table shows 12 rows of data, with 4 rows selected (indicated by blue highlights and checked checkboxes). The selected rows are: dr.tech.local (Veeam Disaster Recovery Orchestrator Server Service), dr.tech.local (Orchestrator Agent on Veeam Backup & Replication server (e...)), 172.17.53.52 (Orchestrator Agent on Veeam Backup & Replication server), and 172.17.53.61 (Orchestrator Agent on Veeam Backup & Replication server).

Server Name	Logs	Progress
<input checked="" type="checkbox"/> dr.tech.local	Veeam Disaster Recovery Orchestrator Server Service	
<input checked="" type="checkbox"/> dr.tech.local	Orchestrator Agent on Veeam Backup & Replication server (e...	
<input type="checkbox"/> dr.tech.local	Embedded Veeam Backup & Replication server	
<input type="checkbox"/> dr.tech.local	Veeam ONE (embedded)	
<input type="checkbox"/> dr.tech.local	Orchestrator Web UI logs	
<input checked="" type="checkbox"/> 172.17.53.52	Orchestrator Agent on Veeam Backup & Replication server	
<input type="checkbox"/> 172.17.53.52	Veeam Backup & Replication server	
<input checked="" type="checkbox"/> 172.17.53.61	Orchestrator Agent on Veeam Backup & Replication server	
<input type="checkbox"/> 172.17.53.61	Veeam Backup & Replication server	
<input type="checkbox"/> 172.17.53.117	Orchestrator Agent on Veeam Backup & Replication server	
<input type="checkbox"/> 172.17.53.117	Veeam Backup & Replication server	