Veeam Disaster Recovery Orchestrator Release Notes

This document provides last-minute information about Veeam Disaster Recovery Orchestrator (Orchestrator), including system requirements and relevant information on technical support, documentation, online resources and so on.

The current version of Veeam Disaster Recovery Orchestrator is available for download at veeam.com/disaster-recovery-orchestrator-download.html starting from February 21, 2023.

> **NOTE:**
> The release build of Veeam Disaster Recovery Orchestrator is 6.0.0.3516, while the embedded Veeam Backup & Replication build is 12.0.0.1420 P20230412 and the embedded Veeam ONE build is 12.0.0.2498 P20230314.

See next:

System Requirements

Unless otherwise stated, all 3rd party software must be at the latest update or patch level.

Hardware

Hardware requirements depend on the size of the managed infrastructure.

Number of Orchestrated Systems*	0-100	100–1000	1000–5000	5000-10000	>10000
CPU	4 vCPUs (minimum) – 8 vCPUs (recommended) for the Orchestrator server 4 vCPUs (minimum) – 8 vCPUs (recommended) for the Microsoft SQL Server and Veeam ONE database	4 vCPUs (minimum) – 8 vCPUs (recommended) for the Orchestrator server 4 vCPUs (minimum) – 8 vCPUs (recommended) for the Microsoft SQL Server and Veeam ONE database	8 vCPUs (minimum) – 12 vCPUs (recommended) for the Orchestrator server 8 vCPUs (minimum) – 12 vCPUs (recommended) for the Microsoft SQL Server and Veeam ONE database	12 vCPUs (minimum) – 16 vCPUs (recommended) for the Orchestrator server 12 vCPUs (minimum) – 16 vCPUs (recommended) for the Microsoft SQL Server and Veeam ONE database	>16 vCPUs for the Orchestrator server >16 vCPUs for the Microsoft SQL Server and Veeam ONE database
Memory	8 GB (minimum) – 10 GB (recommended) for the Orchestrator server 4 GB (minimum) – 8 GB (recommended) for the Microsoft SQL Server and Veeam ONE database	8 GB (minimum) – 12 GB (recommended) for the Orchestrator server 4 GB (minimum) – 8 GB (recommended) for the Microsoft SQL Server and Veeam ONE database	12 GB (minimum) – 40 GB (recommended) for the Orchestrator server 8 GB (minimum) – 40 GB (recommended) for the Microsoft SQL Server and Veeam ONE database	30 GB (minimum) – 70 GB (recommended) for the Orchestrator server 40 GB (minimum) – 70 GB (recommended) for the Microsoft SQL Server and Veeam ONE database	>70 GB for the Orchestrator server >70 GB for the Microsoft SQL Server and Veeam ONE database
SQL Server	N/A	N/A	N/A	Disk IOPS 1000 (minimum)	Disk IOPS 2000 (minimum)

Hard Disk Space	30 GB for product installation and sufficient disk space for the Veeam ONE database (if installed locally). Use the Veeam ONE Database Calculator to size application data. 20 GB for the Microsoft SQL Server. By default, the Microsoft SQL Server database grows as follows: • ~1Mb per one Readiness Check Report or Plan Execution Report for a plan that includes 10 machines. • ~10Mb per one Readiness Check Report or Plan Execution Report for a plan that includes 100 machines. • ~100Mb per one Readiness Check Report or Plan Execution Report for a plan that includes 1000 machines. **Note**: SSD disks are recommended to use with the Microsoft SQL Server.

* The total number of protected machines used in orchestration plans, including vSphere VM and Veeam agent backups

OS

Only 64-bit versions of the following operating systems are supported:

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012

It is not recommended to install Orchestrator on a machine running Microsoft Windows Server Core, or on a Domain Controller.

User management

Windows domain-joined machine.

Microsoft SQL Server

Local and remote installations of the following versions of Microsoft SQL Server are supported:

- Microsoft SQL Server 2022
- Microsoft SQL Server 2019
- Microsoft SQL Server 2017 (2017 SP2 Express Edition is included in the setup)
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012

It is not recommended to use the Express Edition in any production Orchestrator deployments — it should only be used for product evaluation.

Veeam software

If a remote Veeam Backup & Replication server is used for backup and replication task management, it must be version 11a or later. Note that new functionality in Orchestrator version 6.0 such as cloud and agent plans will not be available until the remote server has been upgraded to version 12.

The Orchestrator agent can be deployed to Veeam Backup & Replication servers in the same domain, in a trusted domain or in a workgroup. Only Veeam Backup & Replication servers deployed on Microsoft Windows Server OS and running either Microsoft SQL or PostgreSQL database systems are supported.

Additional software

All components will be installed during setup.

For inline Report Template editing, Microsoft Word version 2010 SP2 or later is required.

VMware vSphere

- VMware vSphere 6.0, 6.5, 6.7, 7.0, 8.0 (up to vCenter Server 8.0a), 8.0 Update 1
- NSX-T Virtual Distributed Switch (N-VDS) networks v2.4 and later

The Orchestrator server must be connected to VMware vCenter Servers only. Direct connections to vSphere hosts are not supported.

Microsoft Azure connect through Veeam Backup & Replication

Microsoft Azure — for recovery of vSphere VM and Veeam agent backups, for both Windows and Linux.

Storage system

- HPE 3PAR 3.3.1 MU5
- HPE Primera 4.2 and 4.3
- HPE Alletra 9000
- NetApp ONTAP 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 9.9, 9.10, 9.11
- Lenovo DM 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 9.9, 9.10, 9.11

Required Permissions

The accounts used for installing and using Veeam Disaster Recovery Orchestrator must have the following permissions.

Account	Required Permission
Setup Account	The account used for product installation must be a domain user who has the Local Administrator permissions on the target machine.
Orchestrator Service Accounts	The accounts used to run Orchestrator services, Veeam Backup & Replication services and Veeam ONE services must have Local Administrator permissions on the Orchestrator server. The accounts must also be granted the *Log on as a service* right. For more information on Windows security policy settings, see Microsoft Docs.
Orchestrator Agent Account	The account used to install and run the Orchestrator agent on a Veeam Backup & Replication server must have the local Administrator, the Veeam Backup Administrator and the database Administrator permissions on the server.
Orchestrator User Accounts	The accounts used to log in to the Orchestrator UI must be granted the *Allow log on locally* right. For more information on Windows security policy settings, see Microsoft Docs.
vCenter Server Permissions	The account used to connect the vCenter Server to Orchestrator must have administrative permissions. You can either grant the Administrator role to the account or configure more granular permissions. For more information, see Veeam Backup & Replication Required Permissions and Veeam ONE Required Permissions. To be able to open sessions on the vCenter Server system, the account must also have the *Sessions.Validate session* privilege on the root vCenter Server. For more information on session privileges, see VMware Docs.
NetApp Storage System Permissions	The account used to connect the storage system to Orchestrator must be granted permissions described in section NetApp Data ONTAP Permissions.
HPE Storage System Permissions	The account used to connect the storage system to Orchestrator must be assigned the *Super* or *Edit* role. If the account is assigned the *Edit* role, both the account and the storage resources that you plan to access must belong to the same domain. **Note**: Multiple connections to a storage system using different credentials are not supported.
Microsoft SQL Server	Different sets of Microsoft SQL permissions are required in the following cases: • **Installation** (remote or local): the current account needs the *CREATE ANY DATABASE* permission on the SQL Server level. After the database is created, this account automatically gets a *db_owner* role and can perform all operations with the database. • **Operation**: the account used to run Orchestrator services, Veeam Backup & Replication services and Veeam ONE services requires the *db_owner* role, as well as permissions to execute stored procedures for the configuration databases on the Microsoft SQL Server. For more information, see Veeam Backup & Replication Required Permissions and Veeam ONE Required Permissions.
Orchestrator Credentials for Application Verification	The account used to run the **Verify SharePoint URL** step, must be assigned the *SharePoint_Shell_Access* role and must be a member of the *WSS_ADMIN_WPG* group on the processed VM. The account used to run the **Verify Exchange Mailbox** step, must be assigned the *ApplicationImpersonation* role on the processed VM.

What's New

Cloud DR

Orchestrated recovery to Microsoft Azure gives your business additional resiliency with disaster recovery (DR) to the cloud. Orchestrate the recovery of any backup as a VM in Microsoft Azure taking full advantage of the cloud scalability and Orchestrator automation capabilities. With support for backups of both physical servers and vSphere VMs, and both Windows and Linux operating systems, you can protect your entire estate with a cloud DR plan.

Clean DR

When faced with a ransomware attack, ensure you are restoring clean data by scanning for ransomware, malware and viruses during orchestrated recovery at-scale. This works with both vSphere VM and Veeam agent backups for recovery to VMware vSphere and Microsoft Azure. Automatically iterate virus scans through multiple restore points until the most recent clean one is found. Regularly scan restore points during DataLab™ testing, with the results shown in reports for improved visibility.

Agent DR

Quickly recover Veeam agent backups as VMs in both Microsoft Azure and VMware vSphere. Any workload protected by Veeam Agent for Windows or Linux can be recovered into the virtual environment as a VM. Automatically map physical networks to virtual networks during recovery, map physical resources such as CPU and memory to virtual machine types, and orchestrate the scalable recovery of multiple systems while reducing human error.

RTO and RPO tracking

The Home Page Dashboard now displays achieved recovery time objectives (RTOs) and recovery point objectives (RPOs) against desired targets for each recovery plan, and provides an at-a-glance view of your service level agreement (SLA) compliance.

Recovery Location tab in the Inventory view

The Inventory view in the Orchestrator UI home section now includes a tab showing available recovery locations (according to the scope access of the current state), providing Plan Authors more insight into their choice of location when launching a plan.

Improved credential management

It is now possible to create and store credentials for use and reuse when connecting to infrastructure such as Veeam Backup & Replication servers, VMware vCenters, and NetApp and HPE storage systems.

Known Issues

Technical limitations

- Restore plans created in Orchestrator can orchestrate recovery from backup files stored only in repositories of the following storage types: direct-attached storage (both Microsoft Windows and Linux), network-attached storage (SMB shares) and deduplicating storage appliances (Dell EMC Data Domain, ExaGrid, HPE StoreOnce and Quantum DXi).

  If you plan to run DataLab tests using deduplicating storage appliances, note the limitations described in this Veeam KB article).

- Orchestrator does not support recovery from tape storage.
- Orchestrator cannot recover to Microsoft Azure a VM that uses a Gateway subnet. This will be addressed in a future update.
- Orchestrator does not support testing of orchestration plans in DataLabs with network mapping from VSS\VDS to N-VDS.
- When performing Instant VM Recovery for a VM with N-VDS networks, Orchestrator does not connect the recovered VM to any networks.

  To work around the issue, go to the vSphere Client and select the **Connect at Power On** check box in the network adapter settings of the recovered VM. This issue will be addressed in a future update.

- Attempting to use the embedded Veeam Backup & Replication server to recover Veeam Agent for Windows backups will result in error *"Failed to find a valid restore point for the entire machine."* This will be addressed in the next product update. If you have a requirement to recover agent backups using the embedded backup server, contact Veeam Support for a patch.

Installation

- During product installation, it is possible to set any custom port numbers except 9402, 8543 and 20443. This is because the embedded Veeam Backup & Replication is hardcoded to use those ports.
- When you follow the Orchestrator installation wizard as described in the Veeam Disaster Recovery Orchestrator User Guide, you have an option to use an existing Microsoft SQL Server instance to host the Orchestrator database. When choosing the instance, keep in mind that Orchestrator does not support case-sensitive SQL Server databases.

Upgrade

- While orchestration of a remote Veeam Backup & Replication server of version 11a is supported in Orchestrator version 6.0, there may be minor issues such as temporary freezing during plan checks or execution.

  To address this issue, it is recommended to upgrade remote Veeam Backup & Replication servers to version 12 as soon as possible.

- Any performance instability during upgrade may result in issues with Orchestrator agents:
  - The embedded Veeam Backup & Replication server may show an incorrect version. To work around the issue, restart the Veeam Orchestrator Server Service.
  - Remote Veeam Backup & Replication servers may show a timeout issue. To work around the issue, repair the affected Orchestrator agents.
- After upgrade, remote users logged in to the Orchestrator UI using the Firefox browser with the default file cache settings may experience errors.

  To work around the issue, reload the page by pressing F5.

- If you try to upgrade Orchestrator to version 6.0 while the existing Orchestrator 5.0 databases are protected with SQL replication, the upgrade process will fail with an error. This is a known issue related to specific aspects of SQL replication.
- If you try to upgrade Orchestrator to version 6.0 while Orchestrator 5.0 is installed to a directory with a non-ASCII name, Orchestrator will not function properly anymore even though the upgrade process will complete successfully.

  To work around the issue, reinstall Orchestrator 5.0 to another directory using the existing databases, and then upgrade to Orchestrator 6.0.
- During the upgrade, some warning dialogs with text including *"Improved background retention"* and *"Active CDP Policy"* may be displayed. These are warnings related to the embedded Veeam Backup & Replication server and may appear if that server has been used for general backup/replication tasks. For full details of the actions to take upon any warning messages, see the Veeam Backup & Replication User Guide, section Upgrading to Veeam Backup & Replication 12.

Infrastructure

- If you change the certificate on a vCenter Server connected to Orchestrator, Orchestrator may fail to connect to the server.

  To work around the issue, edit the vCenter Server connection using the Orchestrator UI — step through the **Edit VMware vCenter Server** wizard, accepting the certificate when prompted.
- If you connect a vCenter Server to a remote Veeam Backup & Replication server added to Orchestrator, you must also connect the same vCenter Server directly to the Orchestrator server. Otherwise, Orchestrator will fail to map the VM inventory correctly and will be unable to locate VM backups and replicas when running orchestration plans. As a result, the plans will fail to complete.

  Orchestrator does not support a scenario where you connect a vCenter Server to Orchestrator using its IP address and to a remote Veeam Backup & Replication server using its FQDN. In this case, Orchestrator will not be able to execute orchestration plans successfully, and the plans will halt with the following error: *"Cannot find the host on the VBR server"*.
- If you have a VMware vCloud Director server added to your backup infrastructure, Orchestrator will not be able to process VMs managed by vCenter Servers connected to this server.
- To let Orchestrator connect to the Microsoft SQL Server instance that hosts the Orchestrator database, you must specify authentication credentials during Orchestrator Server installation. However, if you change the password later, you will not be able to modify the provided credentials, and Orchestrator will fail to connect to the SQL Server instance.

  To work around the issue, it is recommended that you use Windows Authentication when choosing credentials to connect to the Microsoft SQL Server. Alternatively, Veeam Customer Support can help you resolve the issue.

User roles

- When you perform initial configuration of the Orchestrator server, the Initial Configuration Wizard allows you to add users that will be assigned the *Administrator* role for the server. Please keep in mind that you cannot assign the role to a local Administrator. You cannot add local Administrators to any of the user groups provided by Orchestrator. Only domain accounts are supported.

Recovery locations

- If the name of a Virtual Distributed Switch used in recovery location network mapping contains the backslash character, the recovery of VMs will fail.

  The issue will be addressed in a future update.
- If you add an ESXi host to a restore recovery location and then move the host to another datacenter, Orchestrator will consider the host to be a new object. The same issue can occur if a Standard Network is

renamed. As a result of these issues, the configuration of the recovery location will become invalid and Orchestrator will not be able to use this location for recovery.

- For Orchestrator to discover vSphere Distributed Switches, they must be connected to at least one ESXi host.
- When Orchestrator restores VMs to a recovery location that has Instant VM Recovery enabled, VMs are added to the root VM folder. To work around the issue, move VMs to the required folder manually.
- If you add two or more re-IP rules when configuring a recovery location, the rules will be applied incorrectly. It is recommended to add only one re-IP rule per each recovery location.

  This issue will be addressed in a future update.

vSphere VM processing

- If a vSphere VM has a name that starts with a dot, Orchestrator will not be able to process that VM. This is a known VMware issue — some functionality is limited for infrastructure objects whose names start with a dot.
- If a vSphere VM stores its files on a dedicated swap datastore, Orchestrator will exclude the VM from the VM group related to that datastore — but only if the VM is protected by storage replication. If the VM is not protected by storage replication, Orchestrator will still include the VM in the VM group.

Orchestration plans

- RTO may be calculated incorrectly for plans that have been halted during execution. The incorrect RTO may be displayed in reports and dashboards. This issue will be addressed in a future update.
- Removing a CDP policy will result in the failure to map IP addresses from the failover range to the new location range.

  Do not remove CDP policies while the related plans are in progress.
- If you add new VMs to a VM group, these VMs will not be added to an orchestration plan that contains the VM group until the plan enters the *VERIFIED* or *NOT VERIFIED* state. This applies to all other stable and active states that the plan may acquire.

  For more information on plan states, see the Veeam Disaster Recovery Orchestrator User Guide, section Working with Orchestration Plans.
- If you have created multiple backup or replication jobs for one VM, and each job has its own target location, you will not be able to select which backup or replica to use when running orchestration plans. By design, Orchestrator will recover using the most recent restore point.
- To protect an inventory group after failover, you must configure a template backup job on the Veeam Backup & Replication server that processes the group. Otherwise, Orchestrator will not be able to locate the recovered VMs, and the *Protect VM Group* step will fail to complete.
- If a plan includes steps that require in-guest scripts to run on virtual machines being recovered, you may get the following error: *"RPC error: There are no more endpoints available from the endpoint mapper."*

  To work around the issue, add the *Shutdown Source VM* step to the plan. This will power off source VMs during the recovery process, and the in-guest scripts will be able to run on VMs successfully.

Storage failover

- After you restart the Veeam Orchestrator Server Service or reboot the Orchestrator server, storage plans may fail to complete successfully and readiness checks may show that the plans are not ready for failover.

  To work around the issue, wait 5–10 minutes for the inventory to be refreshed.
- Orchestrator does not support storage failover of VMs with RDM disks. When Orchestrator tries to register such a VM in a vCenter Server while executing a storage plan, the server returns the following error: *"Unable*

to enumerate all disks."

- Under certain circumstances, a plan may be halted after one or more **Register VM** steps have started but not completed, causing orphaned VMs to be created in the recovery location. These VMs should be removed manually.

  The issue will be addressed in a future update.

- Orchestrator does not support failover orchestration for volumes protected by SnapVault replication. If you create and try to run a NetApp storage plan containing at least one datastore protected by SnapVault replication, the whole plan will fail to execute.
- Orchestrator does not support failover orchestration for storage virtual machines (SVMs) protected by SnapMirror SVM replication. NetApp storage failover is orchestrated at the volume level only.
- If a VM has its data disk (.vmdk) and configuration file (.vmx) stored on separate datastores, and the VM was suspended when storage failover was performed, the datastore where the .vmx file is located must be processed by Orchestrator first. If Orchestrator attempts to process the datastore with the data disk first, the VM will fail to power on as the .vmx file will not contain the correct datastore GUIDs.

  To work around the issue, edit the .vmx file manually after all storage processing is complete. Contact Veeam Support for assistance if required.

- For datastores connected through the NFSv4.1 protocol, Orchestrator supports failover to a recovery location only in case 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.
- When performing storage failover, Orchestrator does not check whether iSCSI CHAP authentication and NetApp Kerberos authentication is configured for the datastores mounted in the DR site.

  To work around the issue, run a DataLab test before performing storage failover to make sure the authentication is configured properly.

- If a datastore is backed by several volumes (in a situation where LUNs of the datastore reside on several volumes), you will be able to protect such configuration with different SVMs and to create different storage recovery locations for these SVMs. However, in this case, Orchestrator will be unable to match the locations for the datastore, and the related plans will halt with errors.
- If you suspend a VM that stores its disk files on multiple datastores before creating a SnapMirror snapshot, and then include this VM in a storage plan, Orchestrator will not be able to execute the plan successfully. The plan will halt with the following error: *"Unable to access the virtual disk from the host. Either the host is disconnected from the datastore or has insufficient privilege."*
- At the moment, Orchestrator does not support orchestration of storage failover for objects of the type *Tag* and *VM Folder* on standalone Veeam Backup & Replication servers. No matter if you have a backup job with these objects configured on a standalone Veeam Backup & Replication server, Orchestrator will still execute and test the related storage plans on the embedded Veeam Backup & Replication server.

Reports

- When you edit a report template, save it first before closing. If you try closing the file before you save it, MS Word will offer you to save changes, but it will lock the file for up to 10 minutes.

VM console

- After you restart the Veeam Orchestrator Server Service, Orchestrator may fail to open the VM console and may display the "*Connection Failure*" error.

  To work around the issue, close the console and try opening it several minutes later.

Orchestrator agents

On the **Orchestrator Agents** tab of the **Administration** section of the Orchestrator UI you have an option to **Repair** a failed Orchestrator agent installed on a Veeam Backup & Replication server. However, when you try to do that, you may get the following error: *"Repair failed -> The specified service has been marked for deletion."*

You will encounter this error in case the Orchestrator agent is locked by another service running on the server. To work around the issue, log in to the server and make sure that:

1. The Microsoft Management Console, Task Manager and Process Explorer are closed.

   If any of these applications is running, close it.

2. The Veeam Orchestrator Agent Management Service (*VaoAgentSvc*), Veeam Orchestrator Agent for Backup (*VAOBackupAgent*), Veeam Orchestrator Agent for Enterprise Manager (*VAOEmAgent*) have been deleted or have the **StartUpType** value set to *Enabled*.

   If any of the services has the **StartUpType** value set to *Disabled*, restart the server.

Then try repairing the Orchestrator agent again.

Technical Documentation References

If you have any questions about Veeam Disaster Recovery Orchestrator, use the following resources:

- Product webpage: https://www.veeam.com/disaster-recovery-orchestrator.html
- User guides: https://www.veeam.com/documentation-guides-datasheets.html?prd=vao
- Community forums: https://forums.veeam.com/

Technical Support

Veeam offers email and phone technical support for customers on maintenance and during the official evaluation period. For better experience, please provide the following when contacting Veeam Customer Support:

- Version information for the product and its components
- Error message and/or accurate description of the problem you are having
- Log files

For your convenience, the Orchestrator UI allows you to collect logs for each Orchestrator component separately, or all together. 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.

> **TIP:**
>
> 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.

To submit your support ticket or obtain additional information, please visit the Veeam Customer Support Portal. Before contacting Veeam Customer Support, consider searching for a resolution on Veeam Community Forums.

Company Contacts

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