Veeam Availability Console 3.0 Release Notes

This document provides last-minute information about Veeam Availability Console version 3.0, including system requirements and installation, as well as relevant information on technical support, documentation, online resources and so on.

The release version of Veeam Availability Console 3.0 is available through Veeam Community Forums starting from March 28th, 2019.

See next:
- System Requirements
- Sizing and Deployment Recommendations
- Installing Veeam Availability Console
- Uninstalling Veeam Availability Console
- Updating Veeam Availability Console
- Known Issues in Veeam Availability Console
- Licensing
- Contacting Veeam Software
System Requirements

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

Veeam Availability Console

Hardware

- **CPU**: modern x64 processor (minimum 4 cores)
- **Memory**: 4 GB RAM (minimum), 8GB RAM (recommended)

OS

Only 64-bit version of the following operating system is supported:

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows Server 2008 SP2
- Microsoft Windows 10
- Microsoft Windows 8.x
- Microsoft Windows 7 SP1

Software

- Microsoft SQL Server 2019/2017/2016/2014/2012 (SQL 2012 Express and SQL 2016 Express are included in the setup)
- Microsoft SQL Server 2012 Native Client (included in the setup)
- Microsoft .NET Framework 4.6 (included in the setup)
- Microsoft Internet Information Services (IIS) 7.0 or later
- Windows Installer 4.5
- Microsoft PowerShell 3.0 or later
- Microsoft Internet Explorer 11, Microsoft Edge 44 or later, Mozilla Firefox 66 or later, Google Chrome 73 or later
- Microsoft Report Viewer 2015 (included in the setup)
- PDF viewer for viewing reports

Veeam Cloud Connect

Platforms

- Veeam Backup & Replication
- VMware vCloud Director

**Software**
- Veeam Backup & Replication 9.5 Update 2
- Veeam Backup & Replication 9.5 Update 3.x
- Veeam Backup & Replication 9.5 Update 4.x (recommended)
- VMware vCloud Director 8.1 or later
- VMware vCloud Director 9.x

**Veeam Management Agents**
Machines running Veeam Availability Console management agents must meet the following requirements:

**Hardware**
- *CPU:* x86-64 processor architecture
- *Memory:* 2 GB RAM

**OS**
Both 64-bit and 32-bit (where applicable) versions of the following operating systems are supported except Server Core installations for server OS:
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows Server 2008 SP2
- Microsoft Windows 10
- Microsoft Windows 8.x
- Microsoft Windows 7 SP1

**Software**
- Microsoft .NET Framework 4.6 or later

**Network**
- 32 kbit/s when managing Veeam Agent for *Microsoft Windows*
- 64 kbit/s when managing Veeam Backup & Replication
Managed Computers

Veeam Availability Console can manage the following Veeam products:

**Platforms**

- Veeam Agent for Microsoft Windows 3.0
- Veeam Agent for Microsoft Windows 2.x
- Veeam Backup & Replication 9.5 (any update level)
- Veeam Backup & Replication 9.0 Update 2 or later (compatible)

**Software**

- Veeam Management Agent

**Network**

For remote network discovery rules based on the IP range option, discovered computers must have these firewall rules enabled:

- File and Printer Sharing (SMB-In), TCP port 445.
- Windows Management Instrumentation (WMI-In).
Sizing and Deployment Recommendations

Check the Deployment Guidelines document for achieving maximum performance of Veeam Availability Console in large-scale distributed environments.

The recommended deployment configuration can be equally used for POC deployments and deployments in production.
Installing Veeam Availability Console

To install Veeam Availability Console server and Web UI:

2. Mount the product ISO and use autorun or run the Setup.exe file.

Follow the installation procedure as described in Veeam Availability Console Deployment Guide.
Uninstalling Veeam Availability Console

1. From the Start menu, select Control Panel > Add or Remove Programs.
2. In the programs list, select the Veeam Availability Console and its components and click the Remove button.

For details on the uninstallation procedure, see Veeam Availability Console Deployment Guide, section Uninstalling Veeam Availability Console.
Updating Veeam Availability Console

Veeam Availability Console version 3.0 supports automated in-place upgrade from GA version that preserves all product settings and configuration.

Upgrade checklist:

1. Make sure all active Veeam Availability Console web UI sessions are closed before starting the update procedure.
2. Perform a backup of the SQL Server configuration database used by Veeam Availability Console, so that you can easily go back to the previous version in case of issues with the update.

Known Issues in Veeam Availability Console

The following is a list of issues known to exist at the time of the Veeam Availability Console 3.0:

General

- Special characters are not supported in user login names.
- Selecting multiple data rows via Shift+Click operation is not supported.
- Logging in to the VAC web site with domain user credentials is not supported when there is a managed company with the same name as the domain of the user.
- SQL Server using case sensitive collation is not supported.

Client Management

- Company creation wizard might return an error message if the “Use built-in network management capabilities” option is selected when using Veeam Cloud Connect 9.5 Update 2. To resolve this issue, click Cancel in the company creation wizard or update Veeam Cloud Connect to version 9.5 Update 3 or later.
- Editing settings of a company account configured with replica resources (hardware plans) may fail when using Veeam Availability Console web UI. To resolve that, use Veeam Cloud Connect console or update Veeam Cloud Connect to version 9.5 Update 3 or later.
- If tenant’s or sub-tenant’s password is changed using Veeam Cloud Connect console, then management agent connection settings will not be updated with the new settings. All agents need to be reconfigured manually. To work around this, update the tenant’s password using Veeam Availability Console web UI.
- After changing tenant’s or sub-tenant’s password, Veeam Agents services earlier than v3.0 must be restarted. This can be done using via VAC backup portal.
- After changing the tenant name on the Cloud Connect server, all backups stored in a cloud repository will start a new backup chain.

Veeam Agent for Microsoft Windows

- Agent deployed using 3rd party applications is removed from all views after revoking the license key from the agent or uninstalling the agent. To start managing this agent again, re-install management agent on the remote computer and register it in the backup portal.
- Restore point size is reported as total backup size in the backup portal UI when using Veeam Agent for Microsoft Windows 2.0. To resolve that, use Veeam Agent for Microsoft Windows 2.1 or later.
- Veeam Agent for Microsoft Windows backup is considered as a cloud backup copy even after removing this agent from the backup copy job targeted to the cloud repository. As a workaround, change target of the Veeam Agent for Microsoft Windows backup job and let Veeam Availability Console collect the updated job config.
- After enabling or disabling usage of wake-up timers in the Veeam Agent settings, the target computer must be restarted to apply these changes.
- Backup agent running version 2.x will not report any data about restore points, job states, and backup file size stored in a cloud repository if the connection to the Cloud Connect server is not available. To resolve this, make sure the Cloud Connect server is always reachable by a backup agent.
- When changing tenant’s password via console of a managed Veeam Backup & Replication server, all backup agents using the same credentials to connect to a cloud repository will not receive a new
password. To resolve this, either upgrade the backup agent to the most recent version or adjust agent settings manually.

- Changes of the backup agent settings may be displayed in VAC web UI with a delay. This is caused by the scheduling settings of the data collection task.

**VMware vCloud Director**

- Backup agents version 2.x do not support using vCloud Director tenants and sub-tenants in the job configuration. To resolve this, please upgrade the backup agent to the most recent version.

- After applying a cloud backup policy using vCloud Director tenants or sub-tenants, the user must specify tenant or sub-tenant credentials to start using a job.

**Backup Policies**

- Service provider cannot assign backup policies created by the managed client. To workaround that, the service provider needs to copy this backup policy first.

**Management Agent**

- Management agent changes the connection to the new cloud gateway IP-address only after a restart.

- Migrating management agents between companies is not supported. To start managing computer from the new company, re-install management agent.

- Connecting through client proxy server is not supported by the management agent.

- If master management agent uses custom user credentials to discover remote computers and install/patch Veeam Agent for Microsoft Windows, then after management agent failover operation (switching to the new management agent), custom credentials must be re-applied to the new master management agent.

- Master role cannot be manually assigned to the management agent from an External rule. Management agent is selected automatically.

- When unregistering service provider from the managed Veeam Backup & Replication server, management agent connection settings to the backup portal are also discarded. To resolve that, configure management agent connection settings manually.

- When changing tenant or sub-tenant password, make sure that all management agents using this tenant account are up-to-date, otherwise password will not be applied.

- Management agent will not collect any data when it is installed on a backup server manually without enabling the “Allow this Veeam Backup & Replication installation to be managed by the service provider” checkbox. To resolve this issue, enable the remote management checkbox in the Service Provider wizard on the backup server and restart the management agent service.

- Management agent may report a warning message that the security certificate of the backup portal has changed even if it was not. To resolve this, connect the management agent to the backup portal in the same format as it was specified in the security certificate of the VAC backup portal.

**Remote Computer Discovery**

- User with administrator privileges on the remote computer must be used for computer discovery. Usage of other accounts will cause discovery rule failure.

- Microsoft Active Directory discovery process may take a considerable time for domains with a large number of objects.
Alarms and Notifications

- Due to data collection engine scheduling, time stamps for triggered alarms might differ from the time of an actual event.
- Veeam Agent for Microsoft Windows v2.x job failure will not be reported if job is pointed to a disconnected Veeam Backup & Replication server.
- “VM without replica” alarm requires Veeam Backup & Replication 9.5 Update 3 or later to work.
- “VM without backup” alarm is not triggered for VMs contained in jobs that do not have any successful job sessions for the past period.
- Summary email notification setting is now global and cannot be selectively chosen for either discovery rules or alarms.
- Alarms tracking the number of stored agent backups in a cloud repository require Cloud Connect 9.5 Update 4 or later.
- All messages and alarms triggered on a Cloud Connect server will have a server time and date format. All other notifications will be using browser settings to display time and date information.

Monitoring and Reporting

- After decreasing available cloud repository quota for the company using Veeam Backup & Replication console, cloud repository quotas for managed locations are not decreased. To resolve that, use Veeam Availability Console web UI to change quotas.
- Managed VMs counter does not include VMs replicated to the cloud host. This issue is fixed in Veeam Backup & Replication 9.5 Update 3 or later.
- Backup to tape jobs do not display their destination in the Protected VMs report.
- When starting a File to Tape job twice, the job state will be reported as failed until the first job run is complete. Some jobs collected from the managed Veeam Backup & Replication servers for the first time might show “-” as their job status. To resolve that, re-run the job and wait for the new data collection is complete.
- Computer is considered to have a cloud backup in the customer portal of VAC, even if a cloud backup job never ran. To resolve this issue, run a backup job targeted to a cloud repository at least once.
- Overview dashboard will report agent backups transferred with a backup copy job of an unmanaged backup server to a cloud repository as local backups. To resolve this, install a management agent to that backup server.

Billing

- Upload and download traffic cannot be distributed between locations within the company. To resolve that, update Veeam Agent for Microsoft Windows to version 2.1 or later.
- Download Traffic/Data Transfer Out, Upload Traffic/Data Transmitted values might return invalid values when using Veeam Agent for Microsoft Windows 2.0. To resolve that, update Veeam Agent for Microsoft Windows to version 2.1 or later.
- Under certain conditions upload and download traffic might be misreported when using Veeam Backup & Replication 9.5 Update 2. To resolve that, update Veeam Backup & Replication server to version 9.5 Update 3 or later.
- Hardware plans with unlimited RAM resources are excluded from the quota usage dashboard.
• Rejected computers are ignored in the billing reports.
• Billing reports stop tracking backups created by Veeam Agent for Microsoft Windows pointed to the cloud repository if target for the backup job is changed from cloud repository to a non-cloud target repository.
• Managed VMs counter is displayed in invoices for customers running Veeam Backup & Replication 9.5 Update 1 (or later) only.
• Billing dashboard of the service provider will show incorrect data if the service provider and a reseller are using different currencies in subscription plans.
• All Cloud Connect servers must be upgraded to version 9.5 Update 4 to have accurate data in the cloud usage section of the invoice.
• Used Storage Quota reports incorrect data when GFS restore point is removed manually.
• Data Transfer Out metric is not calculated for VM replicas from a backup server that is not managed by Veeam Availability Console.
• Subscription plan created by a reseller will not be preserved in the managed company configuration, if this company is removed from the reseller. To resolve this, please assign a new subscription plan manually.
• If an invoice is generated before an hourly sync-up task in VAC is complete, all backup data will be aggregated into a default location. To resolve this, please re-generate the invoice in one hour.

Reseller Role
• When Cloud Connect is migrated to another server, all companies and resources that are hosted on that server and are managed by a reseller will be removed from that reseller. To resolve this, please re-add these companies to the reseller manually.

Licensing
• New VMs and new backup agents are not displayed in the licensing dashboard. To resolve that, install Veeam Cloud Connect 9.5 Update 3.
• Under certain circumstances license usage reports might contain incorrect data for Cloud Connect servers running version earlier than 9.5 Update 4.

ConnectWise Manage Plugin
• Companies with “Not Approved” or “Credit Hold” states are not displayed in the plugin UI.
• Subscription plan selection cannot be saved until at least one product is mapped or created in the ConnectWise Manage product catalog.
• ConnectWise Manage tickets created based on the “Computer without backup” and “VM without backup” alarms contain the missed RPO information as of the time when the alarm threshold was breached. To see the actual data of the missed RPO event, please use Veeam Availability Console web UI.
• The default data synchronization interval between Veeam Availability Console and its plugin for ConnectWise Manage is 5 minutes. This affects all configuration settings, including SMTP server configuration, etc. To change this interval, please contact Veeam Customer Technical Support team.
Upgrade

- Unresolved alarms for connection state issues are triggered again after upgrading Veeam Availability Console server.
- The size of the SQL Server transaction log may grow dramatically after the upgrade. To resolve it, please shrink the transaction logs manually using built-in functionality of Microsoft SQL Server Management Studio.
- If you are using a custom port for Veeam Availability Console web site, then make sure you specify this port both in IIS settings and in the web.config file before starting the upgrade procedure.
- After the update, all objects in the /computers resource in the VAC API will receive new IDs. If you are using these objects in the integration, then re-query these objects to get the list of new IDs.
- Automatic upgrade of the management agent installed on the Cloud Connect server cannot be performed when Veeam Availability Console had other Cloud Connect servers previously registered in the infrastructure. To resolve this issue, edit connection settings to the Cloud Connect server and retry the upgrade of the management agent.
- Managed computers not running Microsoft .NET Framework 4.6 will require a reboot upon upgrading Veeam Availability Console server and its management agents.
- Cloud Connect server must be switched to the maintenance mode before starting an upgrade procedure. Otherwise, Veeam Availability Console will collect inconsistent data from this server.
- Veeam Availability Console server OS must be running all latest Windows updates, otherwise upgrading to version 3.0 may fail.
- The predefined group of portal administrators is enabled by default regardless of the previous condition.
- Protected Computers and Protected VMs widgets will return zeroes after the upgrade. No resolution is required; all data will be updated within the next sync-up interval in VAC.
- Upgrade is not supported when Veeam Availability Console configuration database and the SQL Server Instance hosting its database have different collation settings.

Enterprise Mode

- Enterprise mode is no longer available upon upgrading to version 3.0. Customers using Veeam Availability Console for the Enterprise will be switched to a service provider-oriented UI.
- Alarm notification actions will be reset to default values after the upgrade.
- “Send email notification to %Departments Admins%” action is dropped from all custom alarms. To resolve this issue, please re-configure actions for these alarms.

RESTful APIs

- Veeam Availability Console 3.0 introduces a few breaking changes to the APIs. To see the full list of methods affected, please review this KB: https://www.veeam.com/KB2913
Licensing

To turn on Veeam Availability Console, you must first obtain a Veeam Instance License with Cloud Connect enabled and deploy Veeam Cloud Connect infrastructure.

- For VCSP users, you may use an existing Veeam Cloud Connect infrastructure. If you do not already have Veeam Cloud Connect installed, a free 1 Instance license has been made available to all partners on the License Management Portal (my.veeam.com).
- For Enterprise users, you may use an existing Veeam Cloud Connect infrastructure. If you do not already have Veeam Cloud Connect installed, contact your Veeam representative.

Then, deploy Veeam Availability Console and install the same license used for the Veeam Cloud Connect infrastructure.

Managing Veeam Backup & Replication

To manage Veeam Backup & Replication, enable the remote management checkbox in the client backup server. The client backup server may be licensed with any Veeam key (Subscription, Perpetual or Rental) with any paid Edition enabled.

NOTE:
You cannot use Veeam Availability Console to manage Veeam Backup & Replication Community Edition.

Managing Veeam Agent *for Microsoft Windows* (Standalone)

Veeam Availability Console may also be used as a management portal for Veeam Agent *for Microsoft Windows*, instead of deployment and management via Veeam Backup & Replication.

Install any VCSP Rental Veeam Instance License with the desired number of Instances (matching to the number of Servers and Workstations under management). A VCSP Rental license can be obtained from Veeam Sales.

Managing Veeam Cloud Connect Only

To manage Veeam Cloud Connect servers, add them to Veeam Availability Console. Licensing for this scenario is covered by your initial deployment.

For more information about using Veeam Availability Console to manage VCSP Rental licenses and usage reports, see the VCSP Rental Usage Reporting Guide.
Technical Documentation References

If you have any questions about Veeam Availability Console, you may use the following resources:

- Product web page: https://www.veeam.com/availability-console.html
- User guides: https://www.veeam.com/documentation-guides-datasheets.html
- Veeam Cloud & Service Provider (VCSP) community forum: https://forums.veeam.com/veeam-cloud-service-providers-forum-f34

To view the product help, press the F1 key or select Help > Online Help from the main menu.

Technical Support

We offer email and phone technical support for customers on maintenance and during the official evaluation period. For better experience, please provide the following when contacting our technical support:

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

To submit your support ticket or obtain additional information please visit www.veeam.com/support.html.

TIP:
BEFORE CONTACTING TECHNICAL SUPPORT, CONSIDER SEARCHING FOR A RESOLUTION ON VEEAM COMMUNITY FORUMS AT www.veeam.com/forums.
Contacting Veeam Software

At Veeam Software we pay close attention to comments from our customers. It is important to us not only to quickly help you with your technical support issues — we make it our mission to listen to your input, and to build our products with your suggestions in mind.

Should you have a Customer Support issue or question, please feel free to contact us. We have qualified technical and customer support staff available 24 hours a day, 7 days a week who will help you with any inquiry that you may have.

Customer Support

For the most up to date information about our support practices, business hours and contact details, please visit www.veeam.com/support.html. You can also use this page to submit a support ticket and download the support policy guide.

Company Contacts

For the most up to date information about company contacts and offices location, please visit www.veeam.com/contacts.