veeam

Veeam ONE

Version 12

Monitoring Guide

August, 2023

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

Contents

Contacting Veeam Software

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

Customer Support

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

Company Contacts

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

Online Support

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

- Full documentation set: veeam.com/documentation-guides-datasheets.html

- Veeam R&D Forums: forums.veeam.com

About This Document

This document provides information about Veeam ONE Client. The document includes configuration details and information about capabilities that Veeam ONE Client offers for Veeam Backup & Replication, VMware vSphere and Microsoft Hyper-V infrastructures.

This document does not include information about working with Veeam ONE alarms. For more information on configuring and using Veeam ONE alarms, see Veeam ONE Working with Alarms Guide.

Intended Audience

The guide is designed for anyone who plans to use the Veeam ONE solution. It is primarily aimed at administrators managing Veeam Backup & Replication, VMware vSphere and Microsoft Hyper-V environments, but can also be helpful for other current and perspective Veeam ONE users.

About Veeam ONE Client

Veeam ONE Client comes as a part of the integrated Veeam ONE solution. It is the primary tool for monitoring Veeam Backup & Replication, Veeam Backup for Microsoft 365, VMware Cloud Director, VMware vSphere, and Microsoft Hyper-V environments. Veeam ONE Client provides complete visibility of the virtual and backup infrastructure and allows you to:

- Manage, view and interact with alarms and monitoring data

- Analyze performance of virtual and backup infrastructure objects

- Keep an eye on multi-tenant environments

- Track the efficiency of data protection in the virtual environment

- Generate reports and administer monitoring settings

- Speed up troubleshooting and quickly isolate root causes of performance issues before they become problems.

With Veeam ONE Client, you can monitor the virtual and backup environment from different perspectives:

- **Virtual infrastructure monitoring**

  Veeam ONE Client discovers the virtual infrastructure and provides complete visibility of its health status and performance. With predefined and custom alarms, performance charts, dashboards, reports, and an extensive knowledge base, you can always stay aware of the important events and eliminate potential problems in the virtual environment.

- **VMware Cloud Director monitoring**

  Veeam ONE Client provides monitoring capabilities for multi-tenant clouds provisioned with VMware VMware Cloud Director. A comprehensive view of cloud resources allows you to sustain consistent processes for VMware Cloud Director operational framework and maintain established service levels.

- **Business view monitoring**

  Veeam ONE Client allows you to monitor and alert on the virtual infrastructure presented from the business perspective — the perspective that is based on your company needs and priorities. You can group virtual infrastructure objects by such criteria as business unit, department, purpose, SLA and so on.

- **Data protection monitoring**

  Veeam ONE integrates with Veeam Backup & Replication and Veeam Backup for Microsoft 365 to collect real-time statistics from backup servers. You can track the latest status of data protection operations in the managed environment, receive immediate alarms whenever a potential problem can cause data loss, monitor performance of backup infrastructure components to optimize workloads, and plan capacity of backup infrastructure resources.

Accessing Veeam ONE Client

To access Veeam ONE Client:

1. Log on to the machine where Veeam ONE Client is installed.

2. From the **Microsoft Windows Start** menu, choose **Veeam ONE Client**.

3. In the authentication window, specify the FQDN or IP address of a server where the Veeam ONE Server component runs and enter the credentials of the account used to connect to Veeam ONE Client. To connect using credentials of the account under which you are logged on to the machine, select the **Log in as current user** check box.

   The user account must either:

   o Be a member of the *Veeam ONE Administrators* or *Veeam ONE Read-Only Users* group. For more information on user groups, see section Security Groups of the Veeam ONE Deployment Guide.

   This prerequisite applies both to the VMware vSphere and Microsoft Hyper-V platforms.

   o Have permissions assigned to objects in the vCenter Server or VMware Cloud Director inventory hierarchy. For more information on assigning permissions to objects, see Veeam ONE Multi-Tenant Monitoring and Reporting.

   This prerequisite applies to the VMware vSphere platform only.

4. Click **Connect**.

5. If Veeam ONE is configured to display a consent banner, read the banner content and click **I Agree**.

   For more information on configuring consent banner, see Banners.

To create a shortcut for the connection, click **Save Shortcut**. You can create one shortcut for every Veeam ONE server. The server name will be saved after the first successful login.

> **NOTE**
>
> If you want to save credentials for a connection in a shortcut, you must agree to save these credentials in the Windows Credentials Manager.

Other Ways to Access Veeam ONE Client

To gain a faster access to Veeam ONE Client, you can launch it without providing user credentials in the authentication window.

- To launch Veeam ONE Client under the account of a user that is currently logged to the machine, in the command shell call the `Monitor.exe` file that resides in the installation directory and pass the `/currentuser` parameter. For example:

  ```
  "C:\Program Files\Veeam\Veeam ONE\Veeam ONE Monitor Client\Monitor.exe"
  /currentuser
  ```

- To launch Veeam ONE Client with explicit user credentials, in the command shell call the `Monitor.exe` file that resides in the installation directory and pass the `/username` and `/password` parameters. For example:

  ```
  "C:\Program Files\Veeam\Veeam ONE\Veeam ONE Monitor Client\Monitor.exe"
  /username tech\john.smith /password PaSSw0rd
  ```

You can save this set of commands as a Windows shortcut and use it to quickly access Veeam ONE Client.

Veeam ONE Client User Interface

Veeam ONE Client user interface is designed to let you quickly locate the required commands, facilitate monitoring of your infrastructure and speed up the investigation and troubleshooting process. This section describes the basic elements and features of the Veeam ONE Client user interface:

- Toolbar and Main Menu

- Inventory Pane

- Information Pane

- Actions Pane

- Configuration Issues Pane

- System Tray Icon

- Full Screen Mode
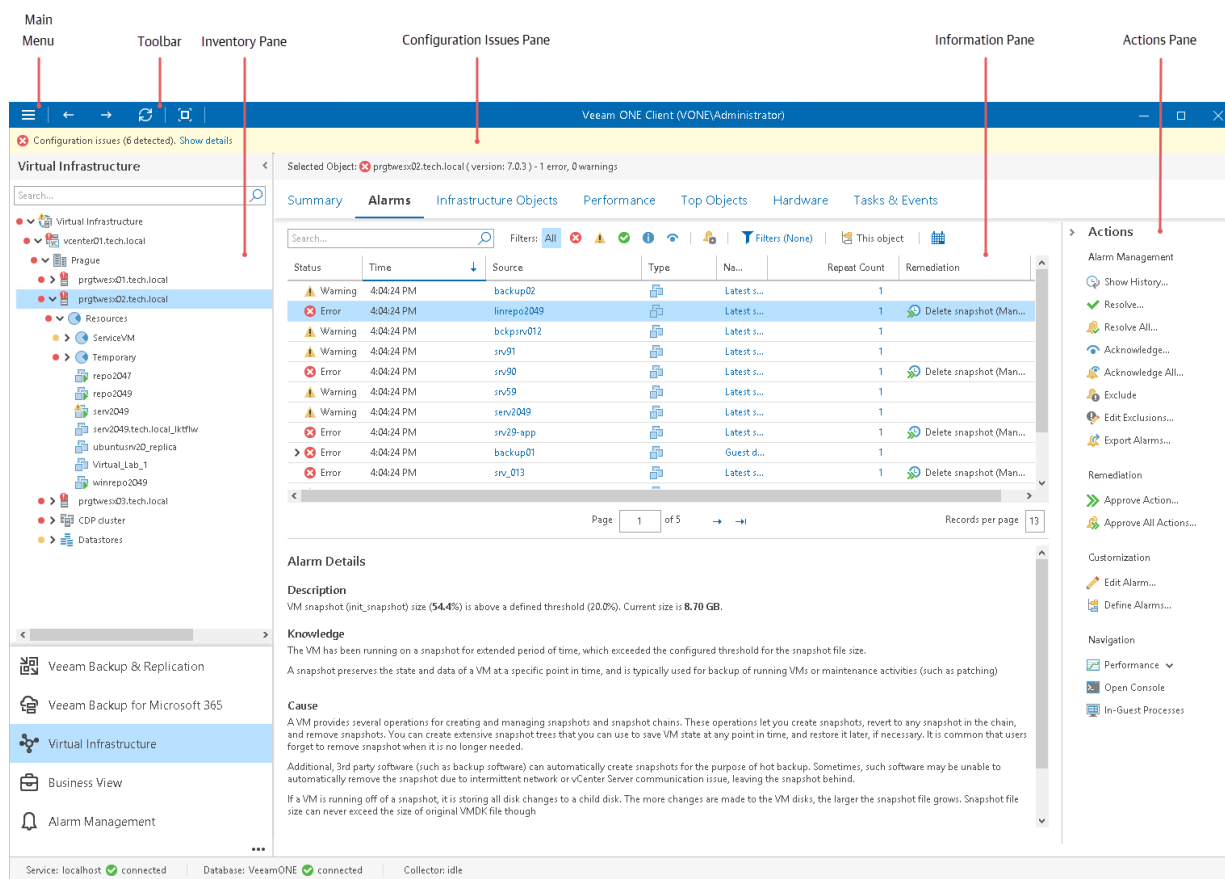
Toolbar and Main Menu

Toolbar

Veeam ONE Client toolbar provides access to frequently used commands.

- **Back/Forward** — navigate to the previous/next visited view in the Veeam ONE Client.

- **Refresh** — retrieve the latest collected data from the Veeam ONE Monitoring Service to show up-to-date information in the Veeam ONE Client. To perform this command, you can also press `[F5]` on the keyboard.

- **Full Screen** — switch to the full screen mode. To perform this command, you can also press `[F11]` on the keyboard.

  For more information on full screen mode, see Full Screen Mode.

- **Get Full Version** (present in Community Edition Mode or if the current license is outdated) — access the webpage where you can download Veeam free trial that allows you to use Veeam ONE with no functionality restrictions for a limited period of time.

Main Menu

Veeam ONE Client main menu provides access to the following commands and features:

- **Add Server** — connect a new virtualization server, VMware Cloud Director, or Veeam Backup & Replication server. To perform this command, you can also press `[CTRL+I]` on the keyboard.

  For more information on connecting servers, see section Connecting Servers of the Veeam ONE Deployment Guide.

- **Notifications** — open the **Notification Settings** wizard.

  For more information on configuring notifications, see section Configuring Notification Settings of the Veeam ONE Deployment Guide.

- **Reports** — create a report for an infrastructure object selected in the inventory pane.

  For more information on creating reports, see Generating Reports.

- **Alarm Modeling** — forecast the number of alarms that will be triggered for an infrastructure object selected in the inventory pane.

  For more information on alarm modeling, see Modeling Alarm Number.

- **Settings** — view or change Veeam ONE client and server settings.

  For more information on customizing settings, see Configuring Veeam ONE Client.

- **Credentials Manager** — view and manage credentials records.

  For more information on working with credentials, see Credentials Manager.

- **License** — view license information, change and update the license file, and send license usage reports.

  For more information on Veeam ONE licensing, see section Licensing Veeam ONE of the Veeam ONE Deployment Guide.

- **Help** — open Veeam ONE Client help, export log files and check the current version of Veeam ONE Client. To open help topics, you can also press `[F1]` on the keyboard.
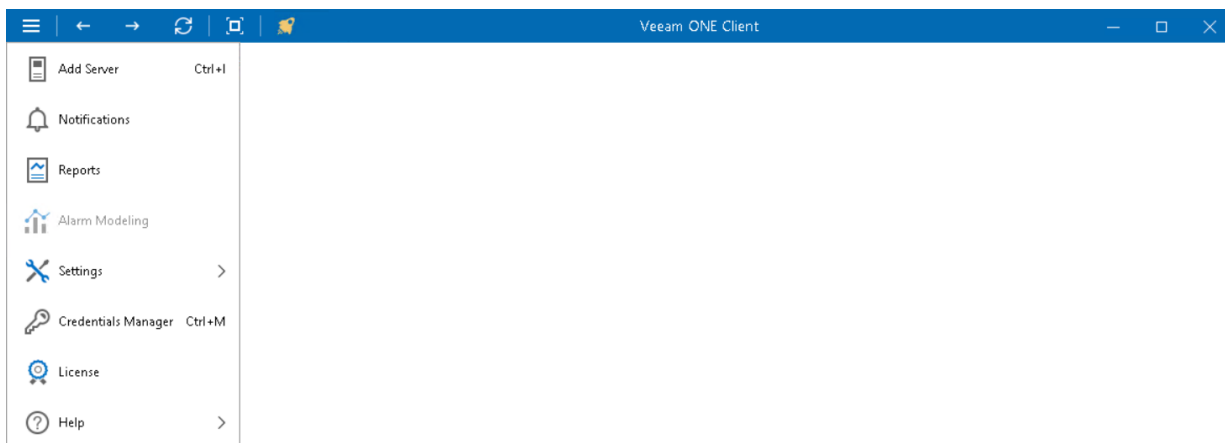
Inventory Pane

The inventory pane on the left shows a hierarchical list of infrastructure objects. The buttons at the bottom of the inventory pane allow you to switch between Veeam ONE Client views.

Each node in the hierarchy tree reflects the state of a corresponding infrastructure object. If there exist unresolved alarms for the object, Veeam ONE Client displays on the node an icon of an alarm with the highest severity.

Veeam ONE reflects the state of child objects on parent nodes to let you easily find problematic objects. For example, if an error alarm was triggered for a host, the error icon will be displayed on the host node. In addition, a red downward error will be shown on the parent cluster node and on the parent management server node to indicate that an error has occurred on the child host. If necessary, you can change Veeam ONE Client settings to display icons next to affected objects only.

- To search for a Veeam Backup & Replication, Veeam Backup for Microsoft 365, virtual infrastructure, VMware Cloud Director or Business View infrastructure component, use the search field at the top of the inventory tree.

  The search results will depend on the selected view.

- To expand/collapse all tree nodes, right-click the root node in the inventory pane and choose **Expand all/Collapse all** from the shortcut menu.

- To show all objects with errors and warnings in the hierarchy, right-click the root node in the inventory pane and choose **Show all error objects** from the shortcut menu.

  Veeam ONE Client will expand all nodes that have child objects with registered errors or warnings.

- To hide and show the inventory pane, use the collapse/expand arrow at the top right corner of the inventory pane.

- To change the inventory view display settings, click the ellipsis at the bottom right corner of the inventory pane and select the necessary options.
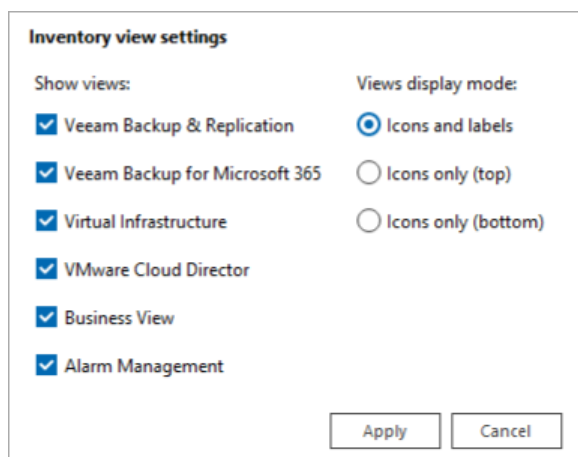
For more information on changing display settings, see Other Settings.

Veeam Backup & Replication

The **Veeam Backup & Replication** tree displays a hierarchical list of connected Veeam Backup Enterprise Manager servers, Veeam Backup & Replication servers, and components of the backup infrastructure — backup proxies, backup repositories, WAN Accelerators, tape servers, cloud repositories, and cloud gateways.
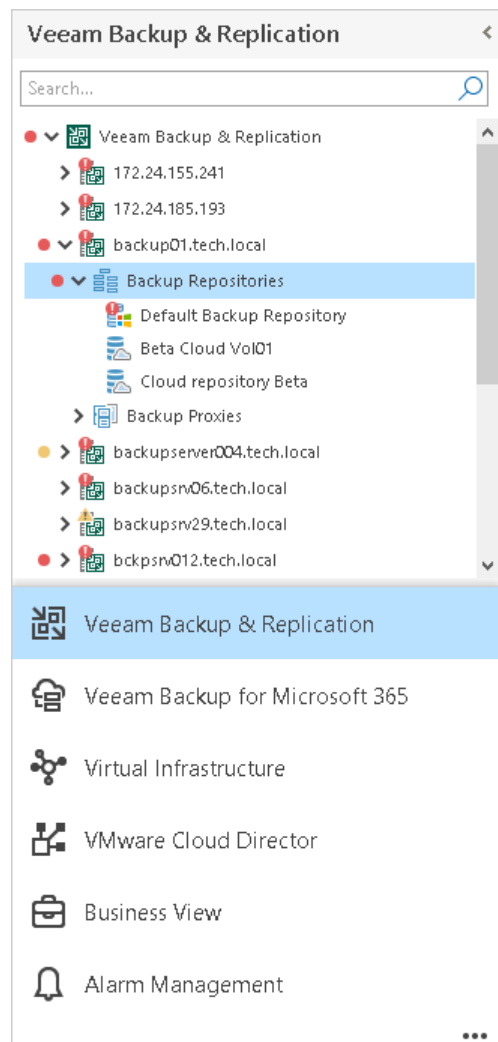
Veeam Backup for Microsoft 365

The **Veeam Backup for Microsoft 365** tree displays a hierarchical list of connected Veeam Backup for Microsoft 365 servers and components of the backup infrastructure — backup proxies and backup repositories.
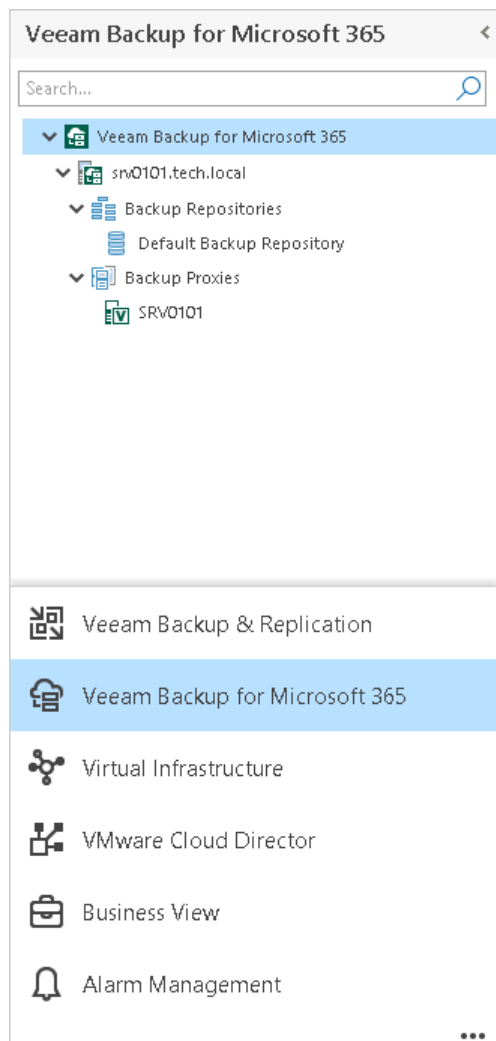
Virtual Infrastructure

The **Virtual Infrastructure** tree displays a hierarchical list of virtual infrastructure objects — vCenter Servers/SCVMM servers, clusters, hosts, folders, VMs, storage objects and so on. It shows the virtual infrastructure in inventory terms, similar to vCenter Server/SCVMM topology presentation.

If you connect a VMware Cloud Director server to Veeam ONE, the Virtual Infrastructure inventory tree will display vCenter Servers attached to VMware Cloud Director and VMware Cloud Director VMs. To hide VMware Cloud Director VMs from the Virtual Infrastructure inventory, enable the **Hide VMware Cloud Director VMs from Virtual Infrastructure tree** option in Veeam ONE server settings. For more information on the VMware Cloud Director display settings, see Other Settings.
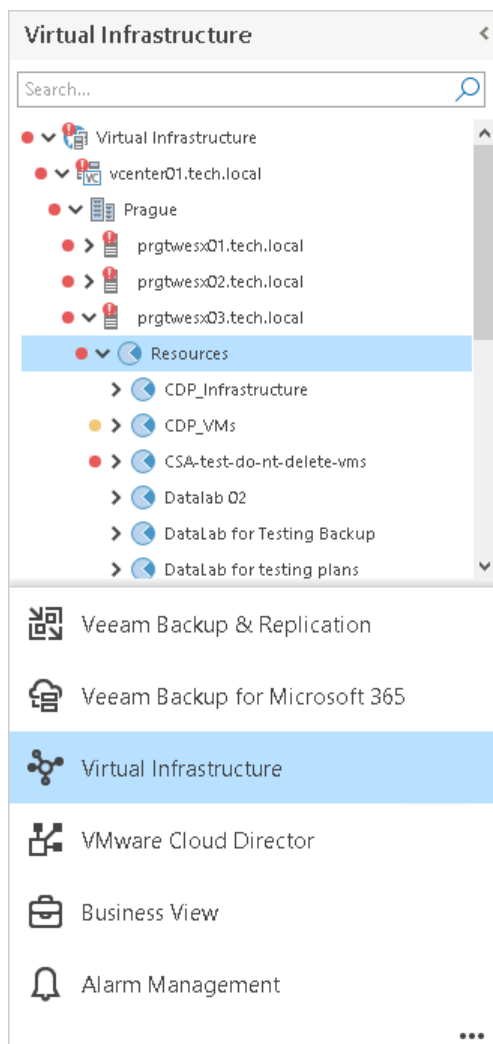
VMware Cloud Director

The VMware Cloud Director tree displays a hierarchical list of VMware Cloud Director objects — provider VDCs, organizations, organization VDCs, vApps, and VMs.
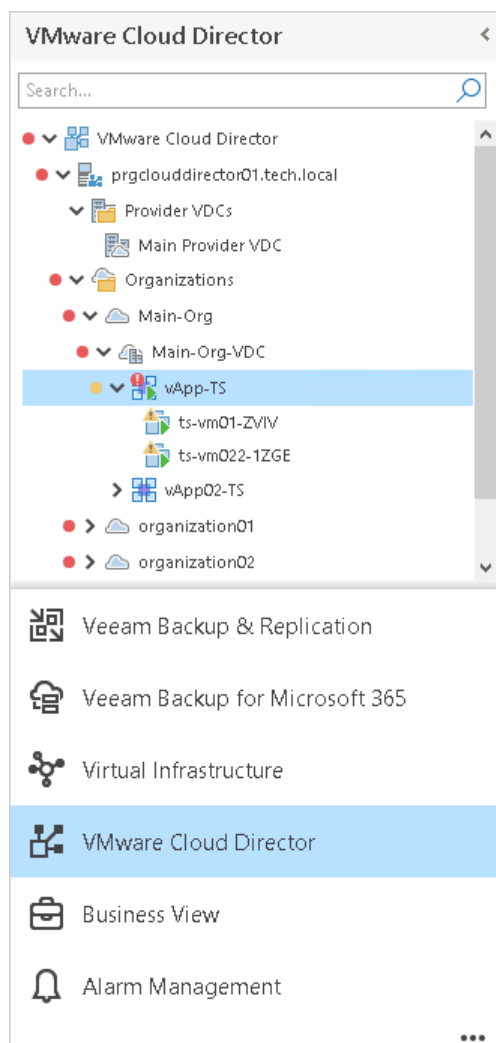
Business View

The **Business View** tree displays a hierarchical list of categorization groups configured in Business View. It presents the infrastructure topology in business terms and allows you to monitor, alert and report on custom categorization units in your environment.

By default, Veeam ONE Client hides the *Uncategorized* group for all Business View categories in the inventory tree. To make it available in the Business View hierarchy, disable the **Hide ungrouped objects from Business View tree** option in Veeam ONE Client server settings. For more information on changing Business View display settings, see Hiding Ungrouped Objects.
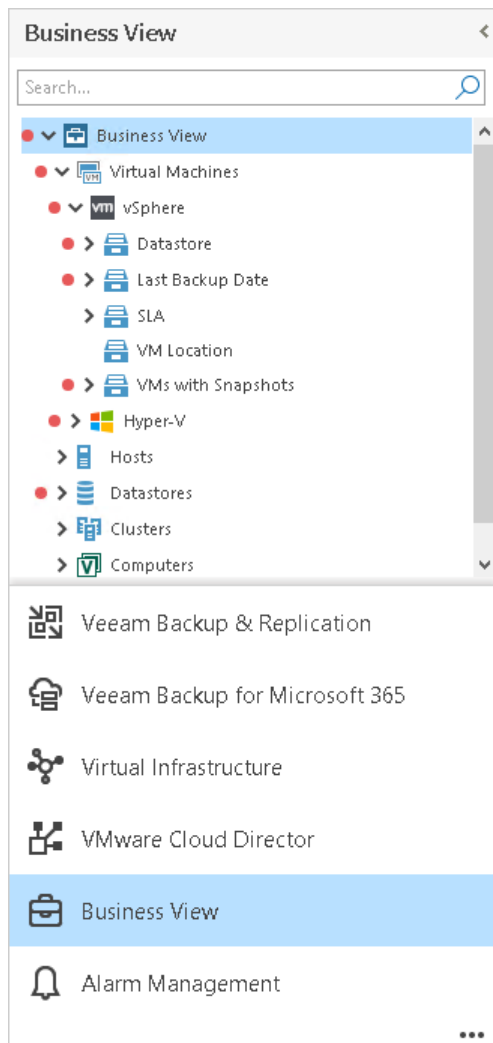
Alarm Management

The **Alarm Management** tree displays the list of available alarm types. Use the **Alarm Management** view to manage predefined alarms or create new alarms.
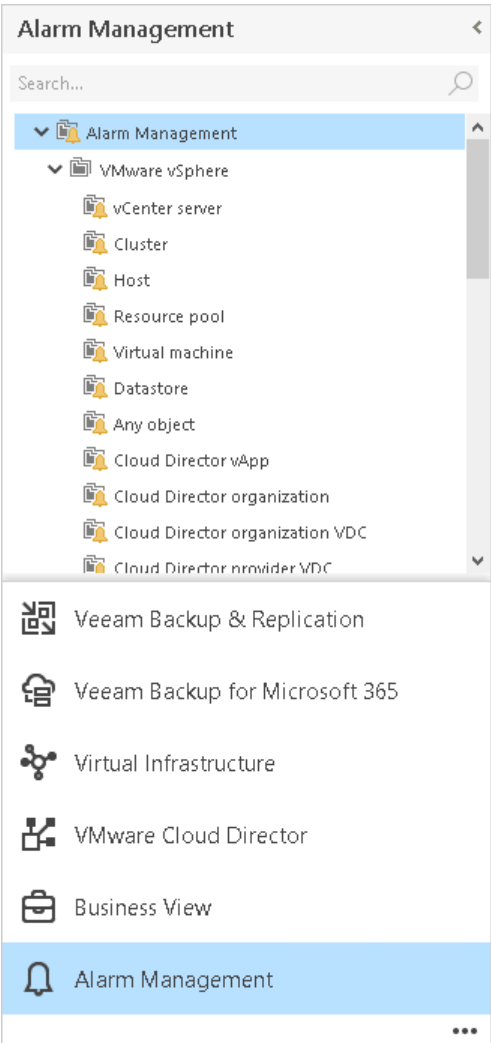
Information Pane

The information pane is the main working area used for managing alarms, viewing performance data and accomplishing other operations for monitoring your virtual and data protection environment.

Tabs in the information pane allow you to switch between Veeam ONE Client dashboards. The set of available dashboards varies depending on the object selected in the inventory tree.

Actions Pane

The **Actions** pane on the right displays links to tasks and commands that can be initiated by the user. The pane becomes available when you open the **Veeam ONE Agents** or **Alarms** tabs, or switch to the **Alarm Management** view. You can hide and show the pane using the collapse/expand arrows.

Options displayed on the pane depend on the object type selected in the information pane. For example, if you select a VM in the inventory pane and open the list of triggered alarms for this VM, all alarm actions, object actions, and navigation actions will be available in the **Actions** pane. If you select a storage object in the inventory pane, some navigation actions will become unavailable as they do not apply to storage objects. For more information on working with alarm actions, see Working with Alarms.

> **Actions**
>
> Alarm Management
> - Show History...
> - Resolve...
> - Resolve All...
> - Acknowledge...
> - Acknowledge All...
> - Exclude
> - Edit Exclusions...
> - Export History...
>
> Remediation
> - Approve Action...
> - Approve All Actions...
>
> Customization
> - Edit Alarm...
> - Define Alarms...
>
> Navigation
> - Performance ⌄
> - Open Console
> - In-Guest Processes
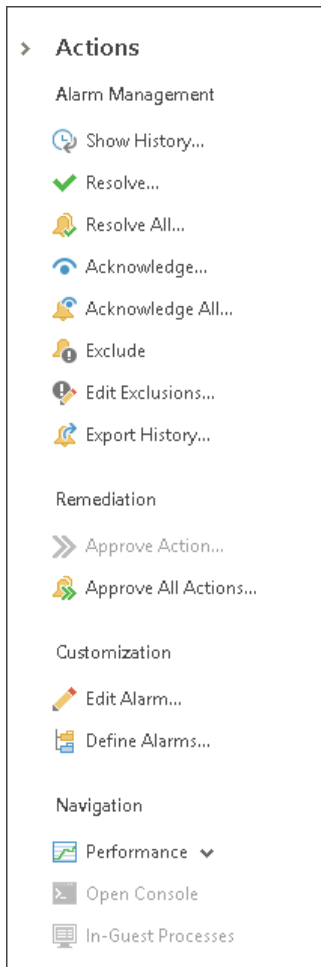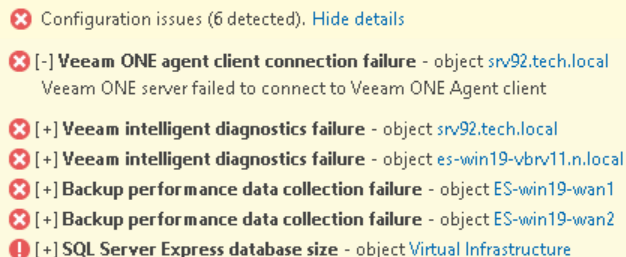
In a similar manner, if you open the **Alarm Management** section and select the **Alarm Management** node in the inventory pane, the **New** action will become unavailable, as you must select a particular object to create a new alarm.
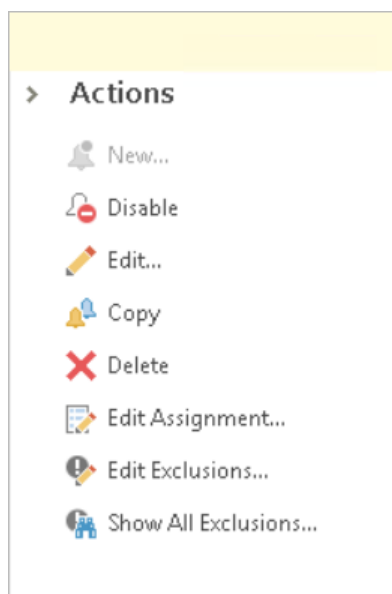
Configuration Issues Pane

The **Configuration issues** pane displays information on alarms triggered as a result of internal Veeam ONE configuration issues (such as lost connection to a virtual server, data collection failure, license expiration and so on). To view details of internal alarms, click the **Show details** link on the pane. For more information on working with internal configuration alarms, see Working with Internal Alarms.

System Tray Icon

To facilitate monitoring of your infrastructure, Veeam ONE Client adds its icon to the system tray as the status indicator.

- If the virtual or data protection infrastructure is functioning properly, the icon color will be green.

- If a warning or error is triggered, the color will turn yellow or red.

- As soon as the health status of your infrastructure returns to normal, the color changes back to green.

To learn about the number of warnings and errors that occurred, move the cursor over the icon.

Full Screen Mode

The full screen mode displays only the information pane for the selected object and allows you to hide unnecessary interface elements that may distract your attention. To switch to the full screen mode, do one of the following:

- Press [F11] on the keyboard.

- On the toolbar, click the full screen icon.

In the full screen mode, the toolbar is not displayed at all, which allows you to concentrate on monitoring the virtual or backup environment state and have only the most crucial information displayed. You can collapse and expand the inventory pane and actions pane if necessary.

To exit the full screen mode:

- Press [F11] on the keyboard.

- In the top right corner, click **Exit Full Screen**.

Configuring Veeam ONE Client

Veeam ONE Client does not require complex configuration and is ready for use right after the installation. However, before you start using Veeam ONE Client, you may need to check and adjust its default configuration.

1. Configure server connections.

2. Configure Veeam ONE client settings.

3. Configure Veeam ONE server settings.

> **NOTE:**
>
> To be able to configure Veeam ONE server settings, a user must be a member of the *Veeam ONE Administrators* group on a machine where the Veeam ONE Server component is installed. To be able to configure Veeam ONE client settings, a user must be a member of the *Veeam ONE Administrators* or *Veeam ONE Read-Only Users* or group on a machine where the Veeam ONE Server component is installed. For more information on Veeam ONE security groups, see section Security Groups of the Veeam ONE Deployment Guide.

Configuring Server Connections

To collect information about the managed virtual infrastructure and track the efficiency of data protection, you must configure connections to VMware vSphere, VMware Cloud Director, Microsoft Hyper-V virtual management servers, Veeam Backup & Replication and Veeam Backup for Microsoft 365 servers in Veeam ONE Client. Configured connection settings are automatically propagated to all Veeam ONE components.

For more information on how to connect servers in Veeam ONE Client, see section Connecting Servers of the Veeam ONE Deployment Guide.

Credentials Manager

You can use the Credentials Manager to create and maintain a list of credentials records that you plan to use to connect to components in the virtual and backup infrastructure.

The Credentials Manager lets you create the following types of credentials records:

- Standard account

- Linux private key

Adding Standard Accounts

You can create a credentials record for an account that you plan to use to connect to infrastructure objects and their guest OS.

To create a new standard credentials record:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the main menu, click **Credentials Manager**.

   Alternatively, press `[CTRL + M]` on the keyboard.

3. Click **Add** > **Standard account**.

4. In the **Username** field, enter a user name for the account that you want to add. You can also click **Browse** to select an existing user account.

5. In the **Password** field, enter a password for the account that you want to add. To view the entered password, click and hold the eye icon on the right of the field.

6. In the **Description** field, enter a description for the created credentials record.

   As there can be a number of similar account names, for example, Administrator, it is recommended that you provide a meaningful unique description for the credentials record so that you can distinguish it in the list. The description is shown in brackets, following the user name.

7. Click **Save**.
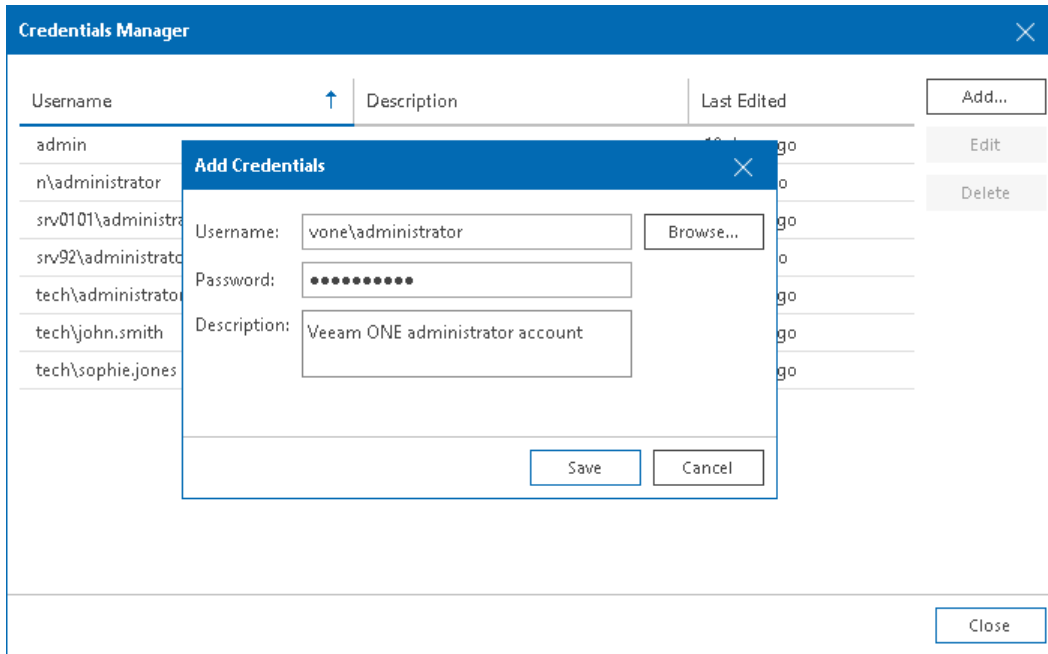
Adding Linux Private Keys

You can add a credentials record to connect to Linux machines using the Identity/Pubkey authentication method.

> **NOTE:**
>
> To use this method, you must first generate a pair of keys using a key generation utility, for example, ssh-keygen. Place the public key on a Linux server. To do this, add the public key to the `authorized_keys` file in the `.ssh/` directory in the home directory on the Linux machine. Place the private key in some folder on the Veeam ONE server or in a network shared folder.

To create a new credentials record using the Identity/Pubkey authentication method:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the main menu, click **Credentials Manager**.

   Alternatively, press `[CTRL + M]` on the keyboard.

3. Click **Add** > **Linux private key**.

4. In the **Username** field, specify a user name for the created credentials record.

5. In the **Password** field, specify the password for the user account.

6. Click **Browse** next to the **Private key** field to select a private key file.

7. In the **Passphrase** field, specify a passphrase for the private key on the backup server.

8. In the **Description** field, enter a description for the created credentials record.

   As there can be a number of similar account names, for example, Root, it is recommended that you supply a meaningful unique description for the credentials record so that you can distinguish it in the list.

9. Click **Save**.
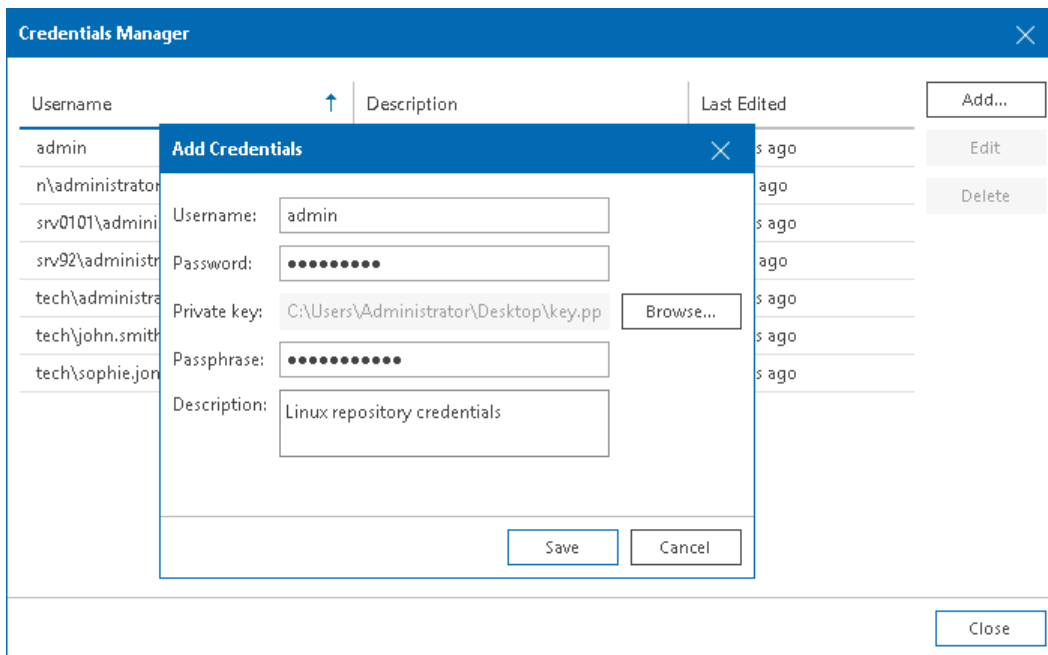
Editing and Deleting Credentials Records

You can edit or delete credentials records that you have created.

To edit a credentials record:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the main menu, click **Credentials Manager**.

   Alternatively, press [CTRL + M] on the keyboard.

3. Select the credentials record in the list and click **Edit**.

4. If the credentials record is already used for any component in the infrastructure, Veeam ONE will display a warning. Click **Edit** to confirm your intention.

5. Edit settings of the credentials record as required and click **Save**.

To delete a credentials record:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the main menu, click **Credentials Manager**.

   Alternatively, press [CTRL + M] on the keyboard.

3. Select the credentials record in the list and click **Delete**.

   If the credentials record is already used for any component in the infrastructure, Veeam ONE will display a warning. In this case, you need to connect to an infrastructure object with new credentials before deleting current credentials record.

Veeam ONE Client Settings

Veeam ONE client settings include:

- General settings

- Color settings

- Charts settings

- Tabs view settings

- Other settings

General Settings

In client general settings, you can specify an FQDN name or IP address of a machine where the Veeam ONE Server component is installed.

To specify client general settings:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Monitor.

2. In the main menu, click **Settings** > **Client Settings**.

   Alternatively, press `[CTRL + O]` on the keyboard.

3. In the **Client Settings** window, open the **General** tab.

4. In the **Host settings** section, specify an FQDN or IP address of a machine where the Veeam ONE Server component is installed.

   o If the connection to the Veeam ONE Server component is successful, the **Veeam ONE Monitoring Server** field is filled automatically with the name of the machine where Veeam ONE Server component is installed or localhost.

   o If Veeam ONE Server component is not found on the specified machine, Veeam ONE will prompt you to specify the correct name in the client settings.

Color Settings

In color settings, you can create a custom color scheme that will be used to display graphs on performance charts.

To specify color settings:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Monitor.

2. In the main menu, click **Settings** > **Client Settings**.

   Alternatively, press `[CTRL + O]` on the keyboard.

3. In the **Client Settings** window, open the **Colors** tab.

4. Create a custom color scheme that must be used to display graphs on performance charts.

   You can add colors from the color palette, remove and edit existing colors, as well as sort them as required. Colors at the top are used first for graphs on performance charts.
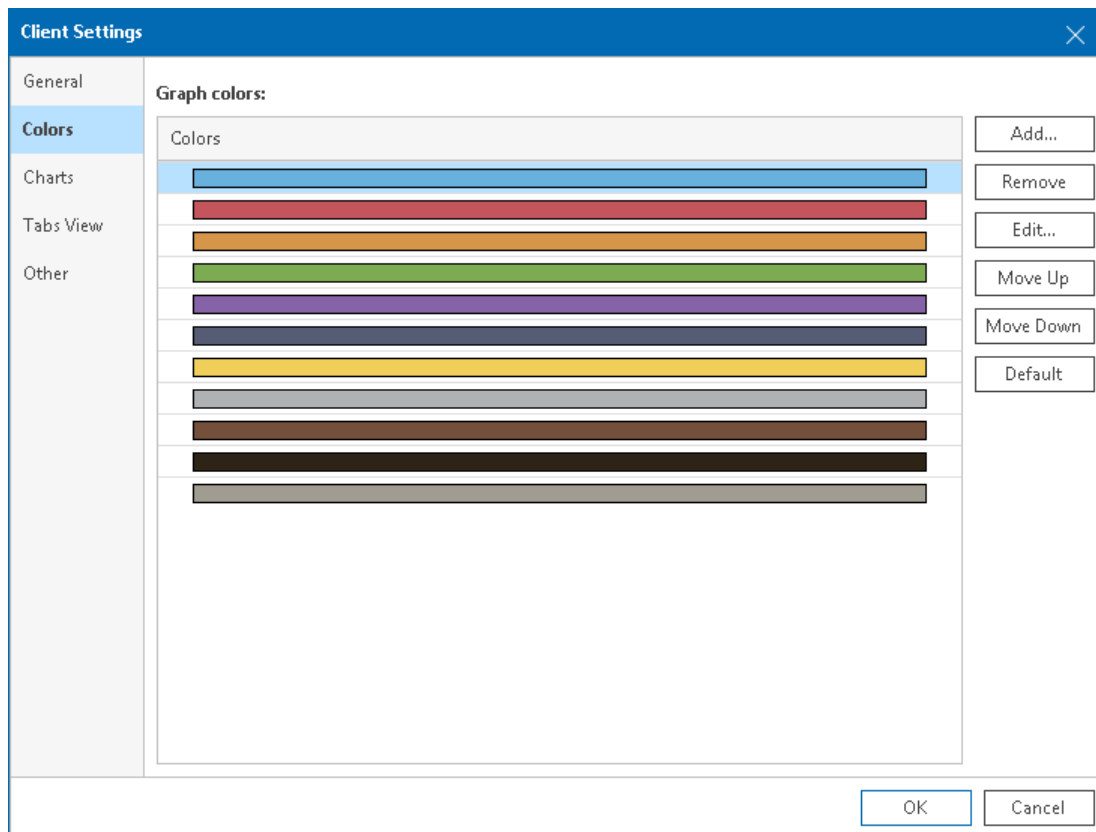
Charts Settings

In charts settings, you can customize display preferences for graphs on performance charts.

To specify charts settings:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Monitor.

2. In the main menu, click **Settings** > **Client Settings**.

   Alternatively, press `[CTRL + O]` on the keyboard.

3. In the **Client Settings** window, open the **Charts** tab.

4. In the **Chart options** section, configure display preferences for graphs in performance charts:

   o In the **Graphic type** section, choose how line graphs must be presented in charts — as 2D or 3D line graphs.

   o In the **Layer type** section, choose how graphs layer must be presented in charts — as line layer or area layer.

   For samples of graphic type and layer type combinations, see Graphic and Layer Type Samples.

5. In the **Overall** graphs section, specify whether top line thresholds must be present on the **Overview** tab.

   If the **Auto-scale** check box is enabled, the Y-axis will scale automatically to match the range of the displayed data.

   For samples of the **Overview** tabs with the **Auto-scale** option enabled and disabled, see Auto-Scale Samples.
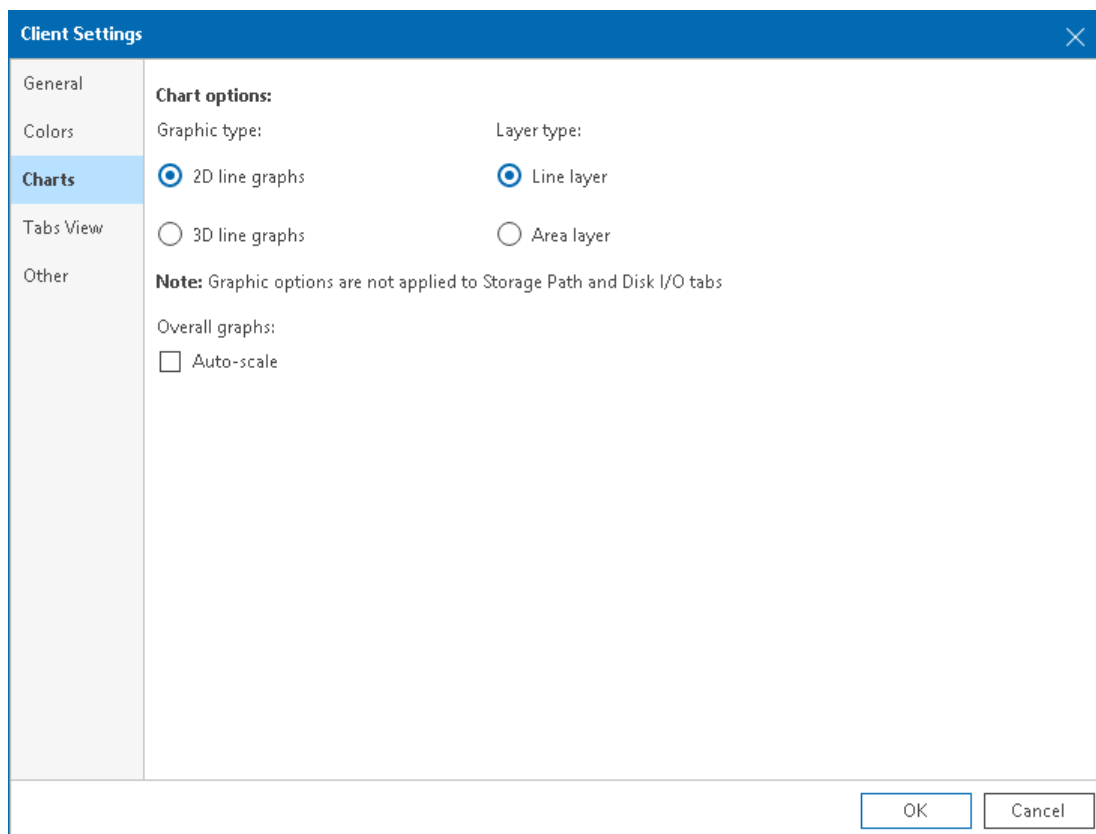
Graphic and Layer Type Samples

You can choose to show graphs in 2D or 3D, as plain lines or filled areas.

The following images illustrate how different combinations of line graphs and layer types will be reflected on performance charts:

- 2D line graphs with line layer
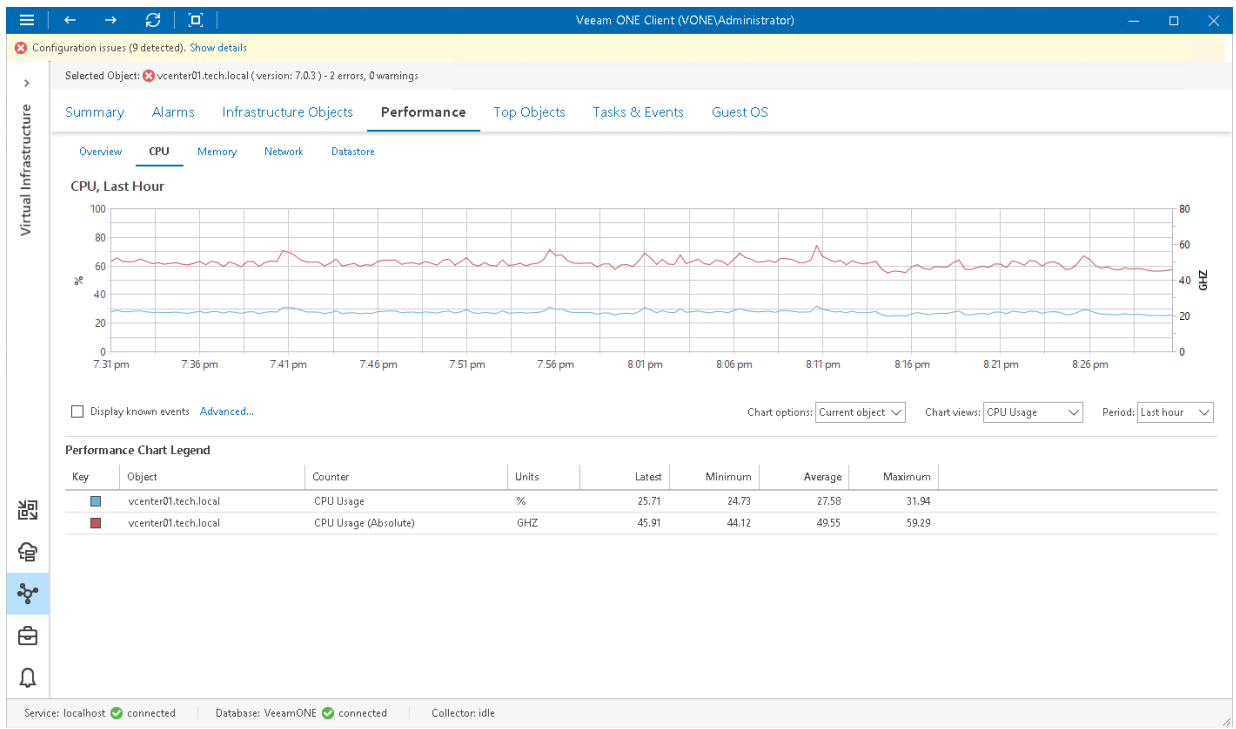
- 3D line graphs with line layer
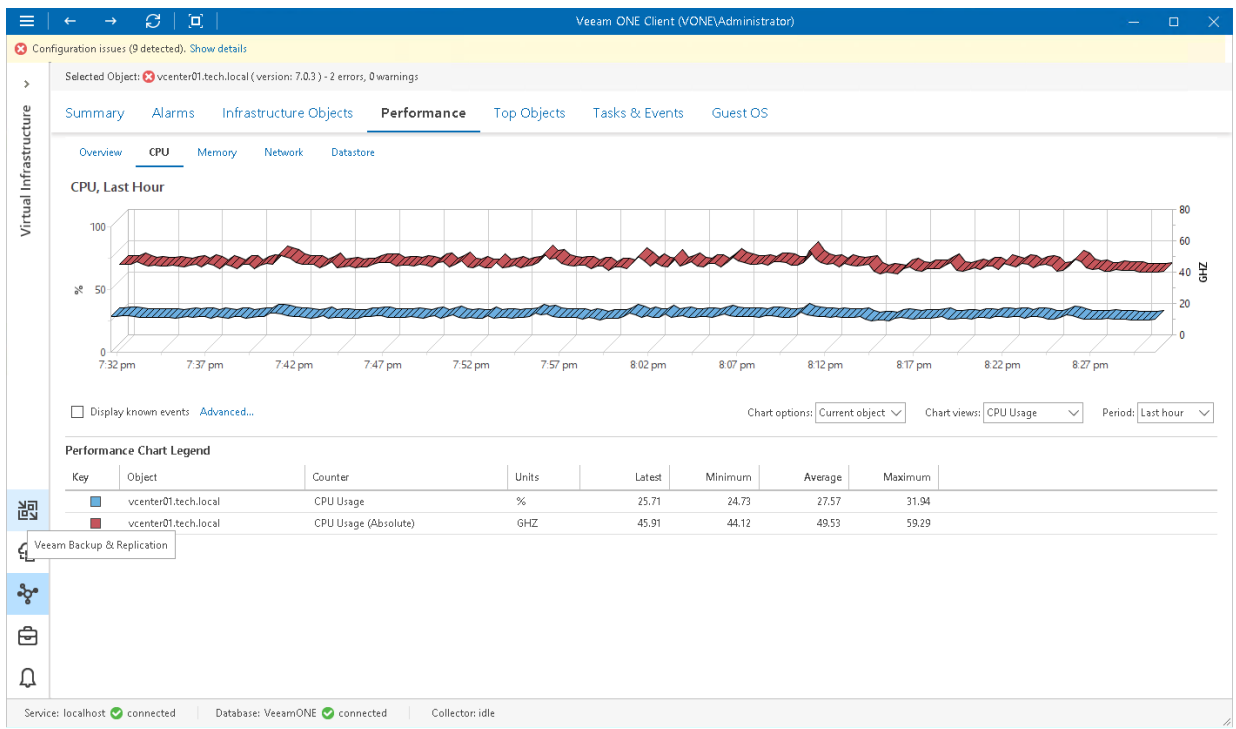
- 2D line graphs with area layer
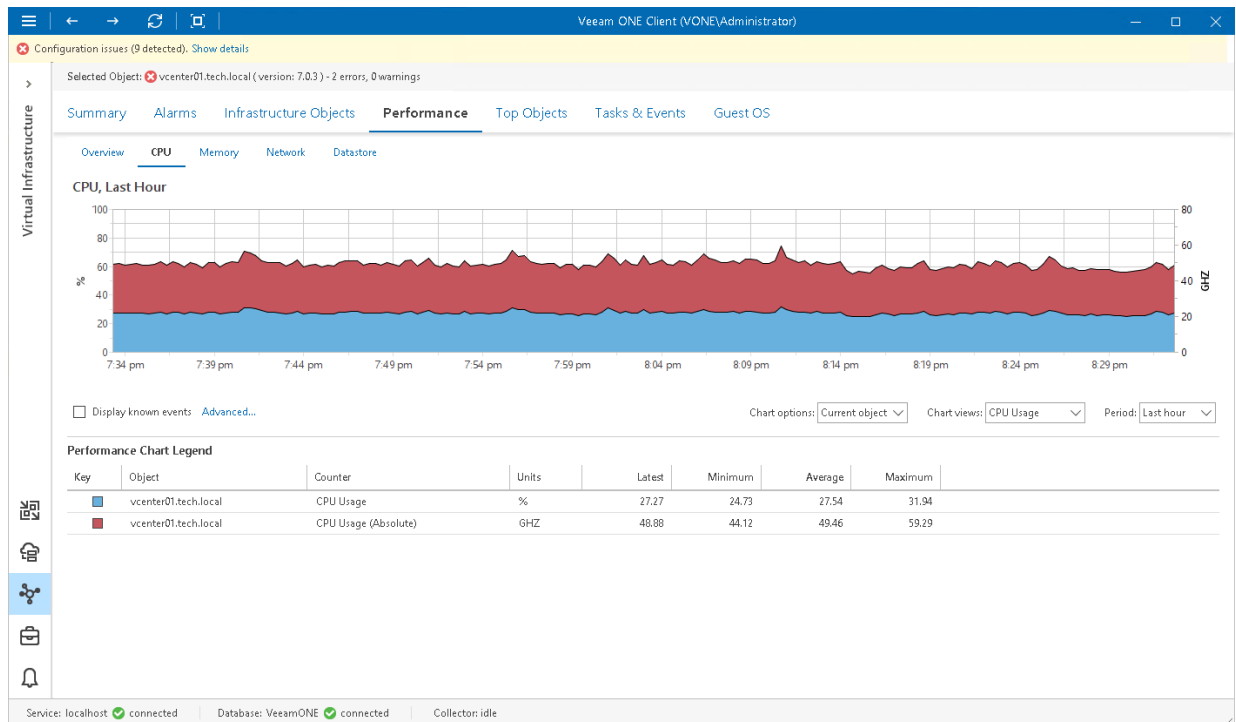
- 3D line graphs with area layer
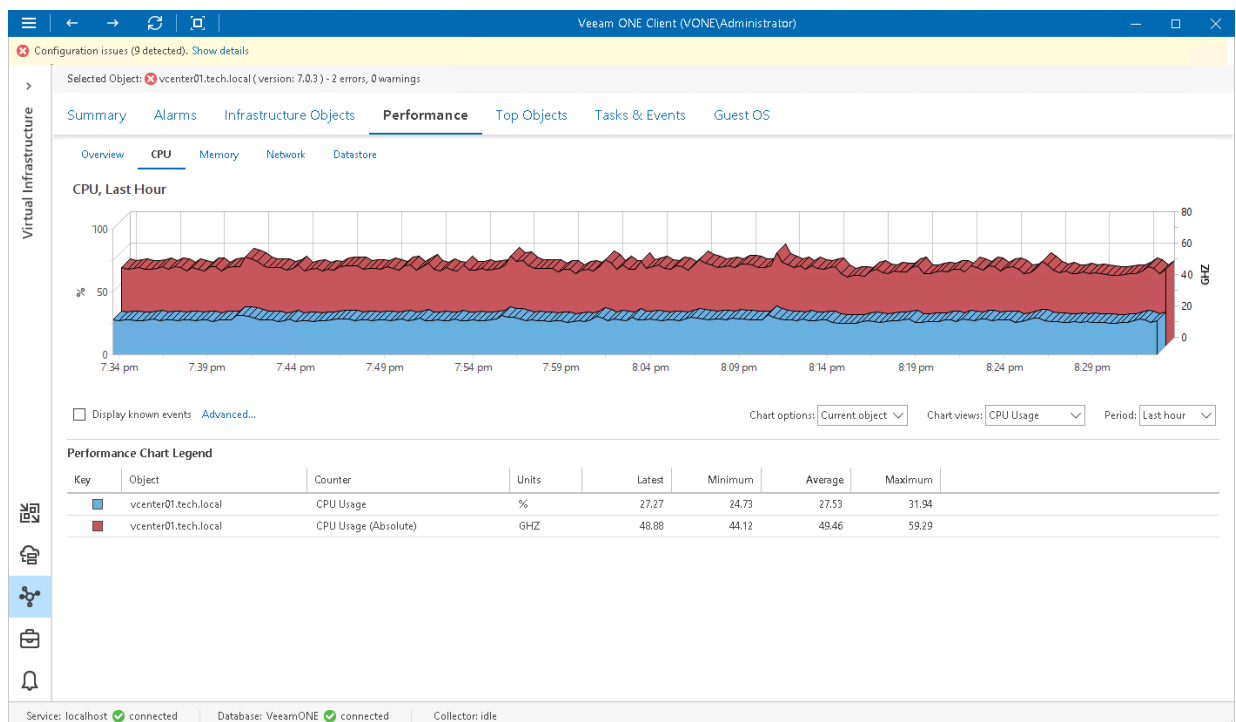
Auto-Scale Samples

The **Auto-scale** option allows you to enable auto-scaling if you want to remove top line thresholds from performance charts on the **Overview** tab. With auto-scale enabled, the Y-axis scales automatically, to match the range of the displayed data.

- Auto-scale disabled
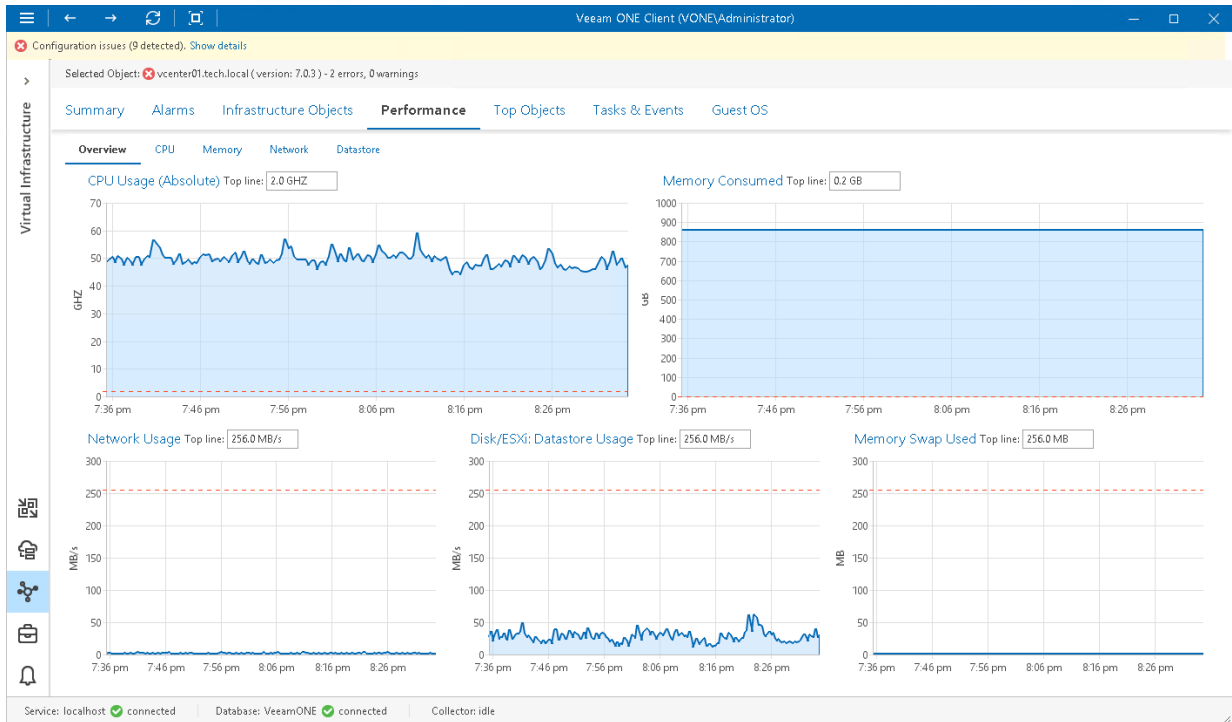
- Auto-scale enabled
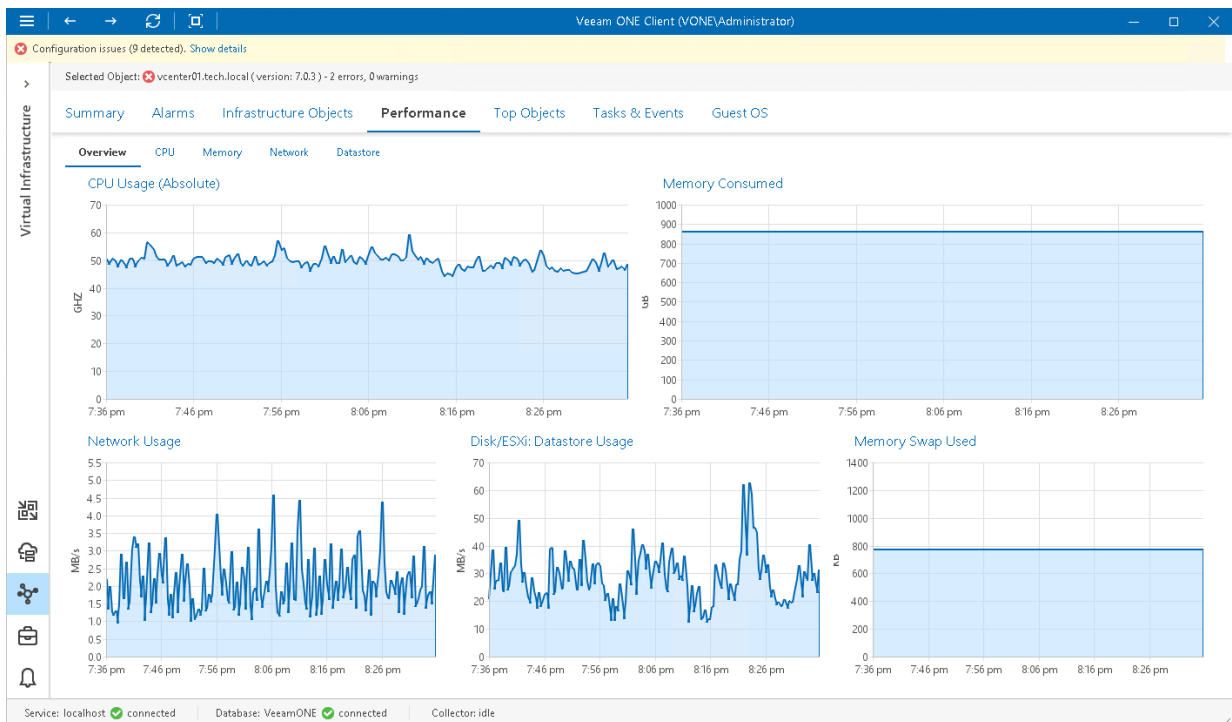
Tabs View Settings

In the tabs view settings, you can enable the automatic switching between the tabs in Veeam ONE Client.

Automatic switching is intended for screens and monitors in a network operations center (NOC). With this option enabled, Veeam ONE automatically switches between its tabs (dashboards) at a certain time interval, and displays dashboards similarly to a slideshow. An administrator can view the whole picture without interacting with Veeam ONE, and can be sure not to miss critical situations in case they occur.

If automatic switching is enabled, Veeam ONE starts switching tabs only if there is no user input from a keyboard, mouse, and so on. Once the user starts interacting with Veeam ONE Client, Veeam ONE Client stops switching tabs.

Automatic switching is disabled by default. You can enable it and create rules that Veeam ONE will use to switch tabs.

There are two types of rules for the automatic switching of tabs:

- You can choose to switch tabs for an object that is selected in the navigation tree. This rule will be useful if you want to monitor the state of one critical object.

- You can choose to switch specific tabs for a predefined scope of objects. This view will be useful if you want to monitor certain aspects of a critical infrastructure segment.

Switching Tabs for One Infrastructure Object

To enable automatic switching of tabs and create a rule that switches tabs for one infrastructure object:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the inventory pane, click the necessary view — Veeam Backup & Replication, Veeam Backup for Microsoft 365, Virtual Infrastructure, VMware Cloud Director, or Business View.

3. In the inventory pane, select the necessary infrastructure object.

4. In the main menu, click **Settings** > **Client Settings**.

   Alternatively, press `[CTRL + O]` on the keyboard.

5. In the **Client Settings** window, navigate to the **Tabs View** tab.

6. In the **Automatic tab switching rule** section, select **Switch tabs for an object selected in the navigation tree**.

7. In the **Switch tabs every <time interval>** section, specify a time interval at which tabs must be switched.

   You can specify an interval in seconds, minutes, or hours.

8. Click **OK**.
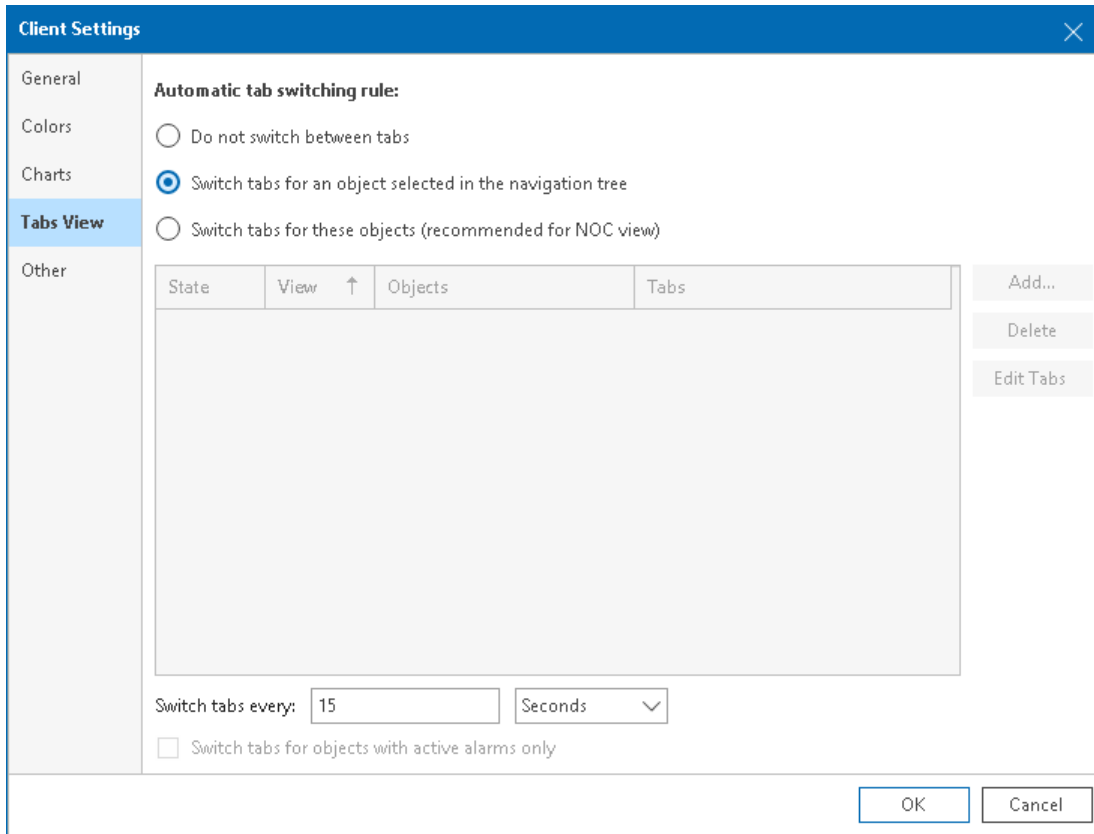
Switching Tabs for Multiple Infrastructure Objects

To enable automatic switching of tabs and create a rule that switches tabs for specific objects:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the main menu, click **Settings** > **Client Settings**.

   Alternatively, press `[CTRL + O]` on the keyboard.

3. In the **Client Settings** window, navigate to the **Tabs View** tab.

4. In the **Automatic tab switching rule** section, select **Switch tabs for these objects (recommended for NOC view)**.

5. Choose objects to include in the scope, and specify tabs that must be displayed.

   a. Click **Add** and choose the type of infrastructure objects to add — Veeam Backup & Replication, Veeam Backup for Microsoft 365, Virtual Infrastructure, VMware Cloud Director, or Business View.

   b. In the **Select scope** window, select check boxes next to objects you want to add to the scope and click **OK**.

   To select an object together with its child objects, click it with the left mouse button.

   If you select several objects of different types, Veeam ONE will create a new rule for each object type. For example, if you select a resource pool with VMs, Veeam ONE will add a rule for the resource pool, and a rule for VMs inside it.

c. Select the added object in the list and click **Edit Tabs**.

Alternatively, you can click the **All tabs** link next to the added object.

d. In the **Select tabs** window, select check boxes next to tabs that must be displayed for an object and click **OK**.

e. Make sure that the **State** check box is selected for the newly added object. If the check box is cleared, the object will not be added to the scope of automatic tab switching.

f. Repeat steps **a–e** for all objects that you want to add to the scope.

6. In the **Switch tabs every <time interval>** section, specify a time interval at which tabs must be switched.

You can specify an interval in seconds, minutes, or hours.

7. Select the **Switch tabs for objects with active alarms only** check box if Veeam ONE must switch tabs for infrastructure objects that have unresolved alarms — that is, only for objects that have potential problems and that may need your attention.

8. Click **OK**.

Other Settings

To specify miscellaneous client settings:
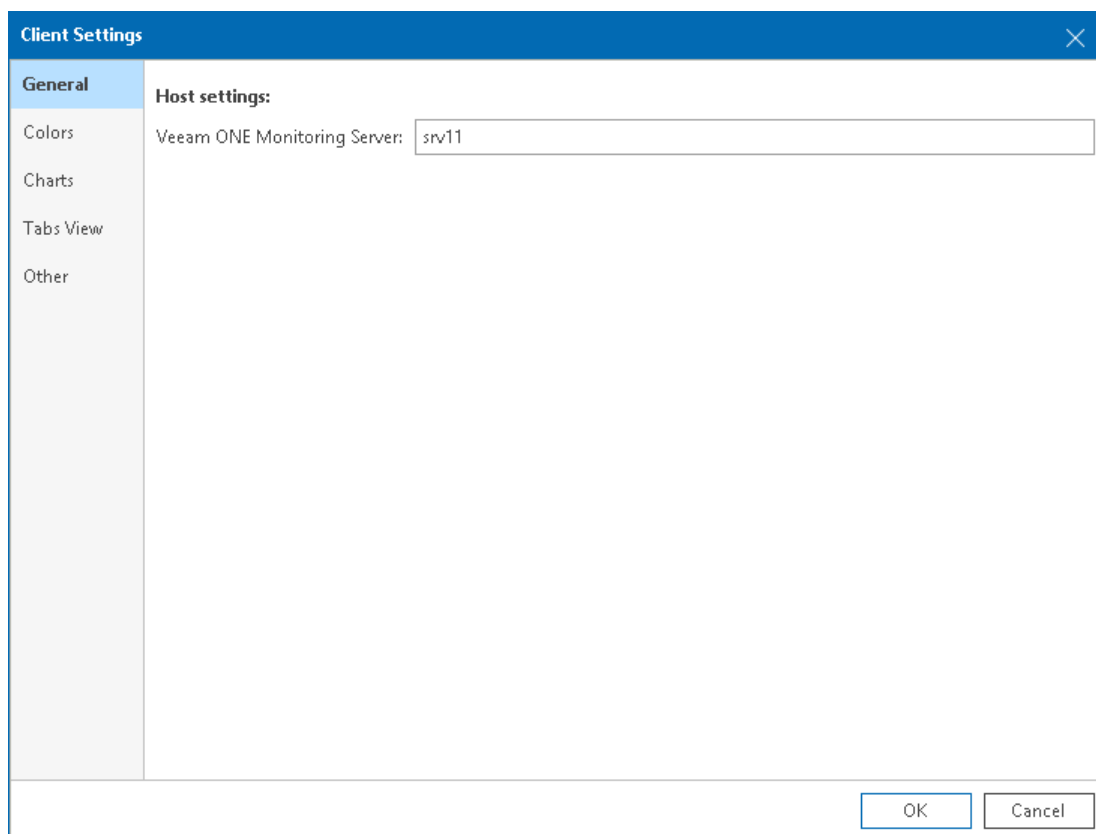
1. Open Veeam ONE Client.

    For details, see Accessing Veeam ONE Client.

2. In the main menu, click **Options** > **Client Settings**.

    Alternatively, press `[CTRL + O]` on the keyboard.

3. In the **Client Settings** window, navigate to the **Other** tab.

4. In the **Miscellaneous** section, specify the following settings:

    o   From the **Logging level** list, choose the level of detail for logging:

    -   **High** — includes events with the *Info*, *Warning* and *Error* status.

    -   **Low** — includes events with the *Warning* and *Error* status.

    -   **Off** — disables logging.

    o   Select the **Minimize to tray** check box if you want to hide Veeam ONE Client to a system tray icon when the Veeam ONE Client window is minimized.

    o   Clear the **Show child object status on a parent node in the Infrastructure tree** check box if every object in the inventory tree must reflect its own state only.

    If this check box is cleared, the state of child objects with errors and warnings will not be reflected on parent nodes. If this check box is selected, Veeam ONE will show downward arrows on parent nodes to reflect the problematic state of child objects. For more information on displaying the infrastructure inventory tree, see Inventory Pane.

5. In the **Remote access** section, specify the path to the `PuTTy.exe` file.

    Veeam ONE requires PuTTy to provide easy access to consoles of Linux VMs.

    For more information on PuTTY, see PuTTY Documentation Page.

    For more information on accessing VM console for VMware vSphere, see VMware Remote Console (VMRC).

For more information on accessing VM console for Microsoft Hyper-V, see Microsoft Hyper-V VM Console.

Veeam ONE Server Settings

Veeam ONE server settings include:

- Mail Server Settings
- Notification Policy
- SNMP Traps
- Guest OS Credentials
- Monitored Datastores
- Monitored VMs
- Business View
- Login Sessions
- Audit Log
- Banners
- Other Settings

Mail Server Settings

In mail server settings, you can configure email settings that will be used for sending alarm notifications, dashboards and reports by email.

To specify SMTP server settings:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, press [CTRL + S] on the keyboard.

3. In the **Server Settings** window, open the **Mail Server Settings** tab.

4. To configure email notification settings, select the **Enable email notifications** check box.

   For more information on configuring mail server settings, see section Configuring Notification Settings of the Veeam ONE Deployment Guide.

5. In the **Email format** section, choose the format of email messages notifying about Veeam ONE alarms.

   For more information on configuring format of alarm email notifications, see Configuring Email Notifications.

Notification Policy

In notification policy settings, you can configure the default email notification group, set the necessary notification policies, and specify other notification settings.

To specify notification policy settings:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Notification Policy** tab.

4. Configure email notifications:

   a. In the **Default email notification group** section, configure a list of recipients who must receive email notifications about Veeam ONE alarms.

   b. In the **Email notification policies** section, specify how often email notifications about Veeam ONE alarms must be sent.

   c. In the **Miscellaneous** section, choose whether you want to send email notifications when conditions that triggered alarms return to normal.

For more information on configuring alarm notification options, see Configuring Email Notifications.

SNMP Traps

In SNMP settings, you can specify trap notification settings for sending notifications about alarms.

To specify SNMP settings:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **SNMP Traps** tab.

4. Configure SNMP settings for sending trap notifications about alarms.

For more information on configuring SNMP notification options, see Configuring SNMP Traps.
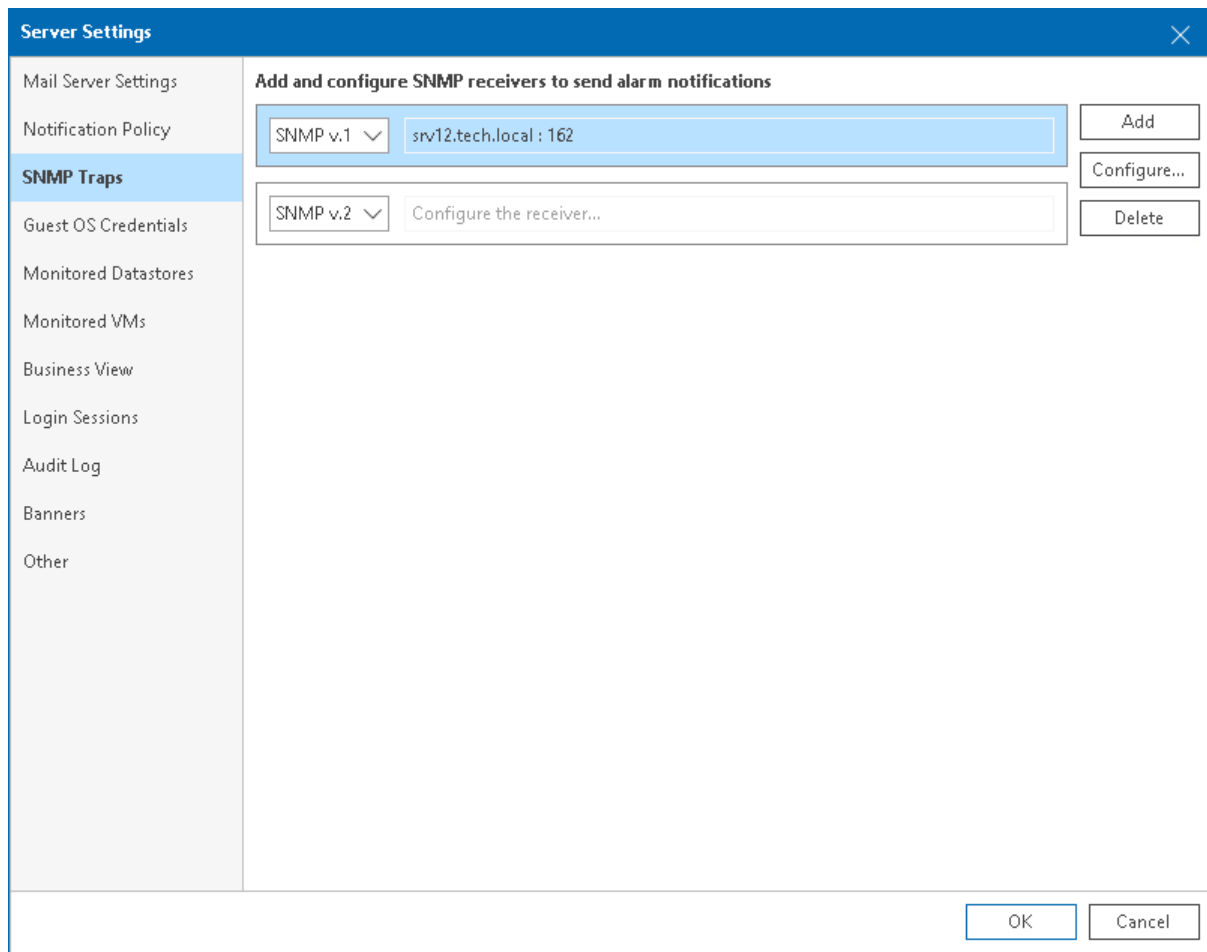
Guest OS Credentials

In guest OS credentials settings, you can set an account that will be used to collect data from the guest OS of Windows and Linux-based VMs.

To access **Guest OS Credentials** settings:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, press [CTRL + S] on the keyboard.

3. In the **Server Settings** window, open the **Guest OS Credentials** tab.

4. Specify guest OS credentials:

   a. In the **Microsoft Windows** section, select credentials of an account that will be used to collect data from the guest OS of Windows-based VMs. To create a new credentials record, click **Add**.

   b. In the **Linux** section, select credentials of an account that will be used to collect data from the guest OS of Linux-based VMs. To create a new credentials record, click **Add** and select **Standard account** or **Linux private key**.

   In the **SSH Port** field, change the default connection port if required.

   To disable fingerprint validation for Linux VMs, select **Skip fingerprint check**.

To access credentials manager, click the **Manage Credentials** link. For more information on working with credentials, see Credentials Manager.

Server Settings

Mail Server Settings
Notification Policy
SNMP Traps
Guest OS Credentials
Monitored Datastores
Monitored VMs
Business View
Login Sessions
Audit Log
Banners
Other

Configure default credentials for connecting to the guest OS of VMs

Microsoft Windows

Credentials: tech\john.smith (Last edited: 28 days ago)   ✚ Add   ✖ Clear

Linux

Credentials: admin (Last edited: 28 days ago)   ✚ Add ⌄   ✖ Clear

SSH port: 22

☐ Skip fingerprint check

🔑 Manage Credentials...

ℹ To set different credentials on individual objects right-click on the object and choose "Guest OS credentials..."

OK   Cancel

TIP:

You can set guest OS credentials on individual VMs. To do this, right-click a VM and choose **Guest OS Credentials** from the shortcut menu.

Monitored Datastores

You can manage the list of datastores that must be included in the reporting scope:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Monitored Datastores** tab.

4. Expand the virtual infrastructure tree and select check boxes next to datastores that you want to include in reporting.

For more information on choosing datastores to report on, see section Choosing Datastores to Report On of the Veeam ONE Deployment Guide.
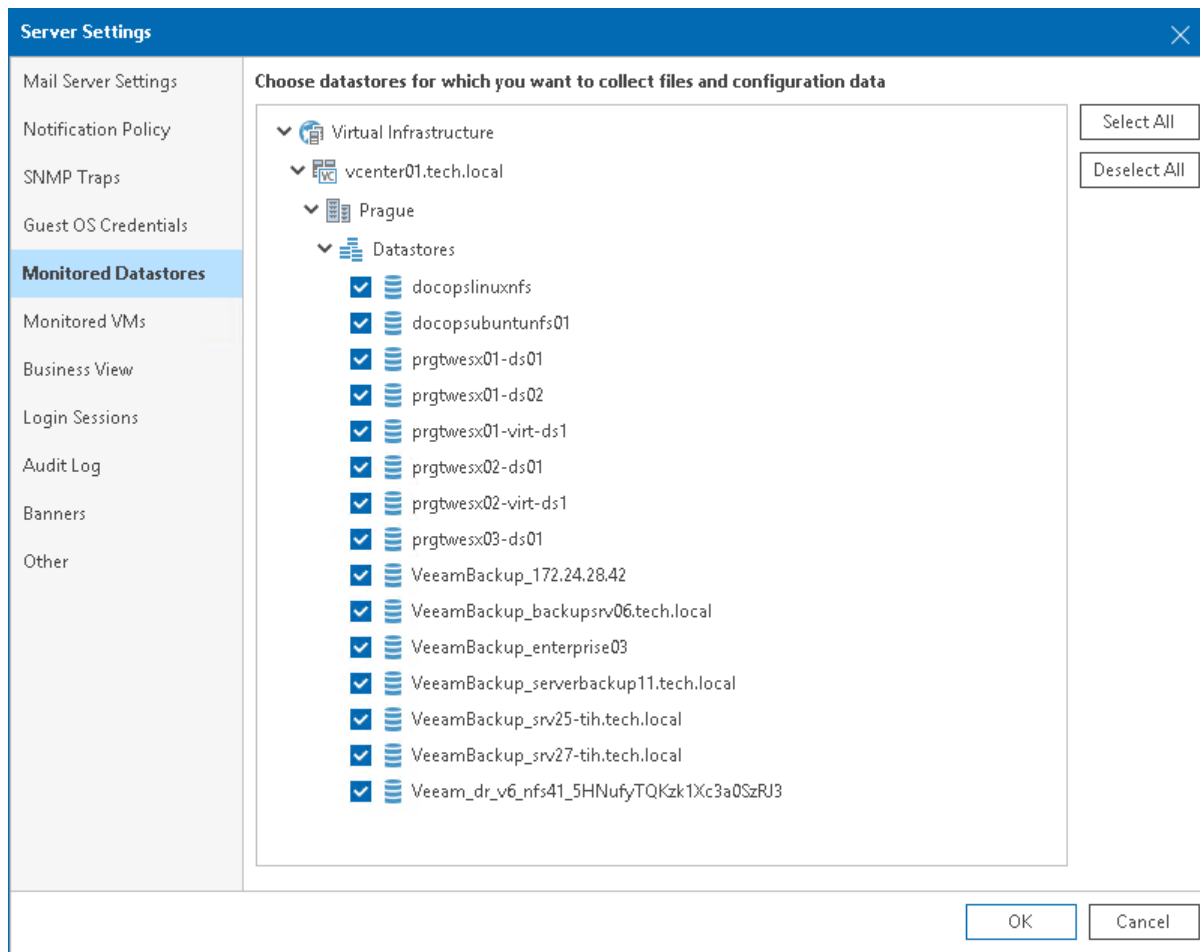
Monitored VMs

On the **Monitored VMs** tab, you can manage the list of VMs and VM containers (hosts, clusters, datastores and so on) that must be included in the monitoring and reporting scope.

To choose what VMs and VM containers must be included in the monitoring and reporting scope:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Monitor.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Monitored VMs** tab.

4. Create rules that will be used to include VMs and VM containers to and exclude VMs and VM containers from monitoring and reporting.

For more information on choosing objects to monitor and report on, see section Choosing VMs and VM Containers to Monitor and Report On of the Veeam ONE Deployment Guide.

Business View

On the **Business View** tab, you can define the following settings:

- Categorization model — choose whether you want to import an existing categorization model or create your own categories and groups.

- Ungrouped objects — hide ungrouped objects from the Business View inventory tree.

- Exclusions — define objects that must be excluded from categorization.

For more information on Business View categorization, see Business View.

Selecting Categorization Model

To select a categorization model:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Business View** tab.

4. Select one of the following categorization options:

   o **From vCenter Server and System Center Virtual Machine Manager** — select this option if you have vCenter Server tags or System Center Virtual Machine Manager properties assigned to virtual infrastructure objects, and you want to use these tags and properties to categorize objects in Veeam ONE Client.

   o **From CSV file** — select this option if you want to synchronize categorization data between Business View and a 3rd party application using a CSV file.

   For more information on configuring data synchronization, see Importing Categorization Data Automatically.

   o **Do not import** — select this option if you want to create a custom categorization model in Business View.

   For more information on creating Business View categories, see Creating Business View Categories and Groups.

   o **Import categorization model from CSV file once** — select this option if you want to map categorization data from a 3rd party application to Business View groups using a CSV file.

   For more information on manual import from, see Importing Categorization Data Manually.

NOTE:
- You cannot enable synchronization with vCenter Server and System Center Virtual Machine Manager tags and properties and a CSV file at the same time. When you switch between these options or disable import, Veeam ONE Client deletes all previously imported categories.
- Categorization model settings do not affect tags collection. For example, if you select the **Do not import** option, Veeam ONE will still collect vCenter Server tags or System Center Virtual Machine Manager properties, but will not use them for building categories and groups.

Hiding Ungrouped Objects

To hide ungrouped objects from the Business View inventory tree:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Business View** tab.

4. In the **Ungrouped objects** section, select **Hide ungrouped objects from Business View tree**.

   If you select **Hide ungrouped objects from Business View tree** check box, Veeam ONE Client will hide the Uncategorized group and all objects within this group from the Business View inventory tree.

For more information on displaying the Business View inventory tree, see Business View.

Defining Exclusions

To exclude objects from Business View categorization:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Business View** tab.

4. In the **Exclusion rules** section, select an object type and click **Edit**.

5. [For virtual infrastructure objects] Choose platform for which you want to define exclusions (*VMware*, *Hyper-V*).

6. In the **Edit Global Exclusion Rule** window, click **Add Condition** and specify exclusion conditions:

   o From the **Property** drop-down list, select an object property.

   The list contains all object properties that Veeam ONE collects from virtual and backup infrastructure servers.

   o From the **Operator** drop-down list, select a conditional operator.

   The list contains the following operators: *Equals*, *Does not equal*, *Starts with*, *Ends with*, *Contains*, *Does not contain, Wildcard*.

   o In the **Value** field, specify a value that will be checked in the condition.

   The condition will be evaluated against discovered objects. To add another condition, click **Add Condition**.

   By default, conditions are linked by the **AND** operator. That is, an object is excluded when all specified conditions are met. You can change this behavior by linking conditions with the **OR** operator. In this case, Veeam ONE will exclude an object from categorization when a condition for any of the linked rules is met.

For example, you can exclude VMs based on their power state, datacenter name, and guest OS. If you want to exclude all powered on VMs that reside in datacenter Atlanta or run Linux as their guest OS, you must link these conditions. The second and the third conditions will be linked to each other with the OR operator. The first condition will be linked to them with the AND operator.

To link conditions:

a. Select check boxes next to the necessary conditions and click **Link**.

b. In the **Rule Condition** window, select a link operator and click **OK**.

Linking supports 3 levels of nesting.

6. Click **Save**.

Server Settings				✕
Mail Server Settings	**Configure import settings to periodically synchronize Business View categorization model with external sources**			
Notification Policy	◯ From vCenter Server and System Center Virtual Machine Manager			Tags...
SNMP Traps	◯ From CSV file			File...
Guest OS Credentials	◉ Do not import			
Monitored Datastores				
Monitored VMs	a,b Import categorization model from CSV file once			
Business View	**Ungrouped objects**			
Login Sessions	☑ Hide ungrouped objects from Business View tree			
Audit Log	**Exclusion rules:**			
Banners	Object Type	Monitored Objects	Excluded Objects	Edit...
Other	🖳 Virtual Machine	220	0	
	🗄 Host	6	0	
	🗄 Datastore	16	6	
	🗄 Cluster	1	0	
	🆅 Computer	1	0	
	🗄 Enterprise Application	4	0	
	a,b Export current categorization model to CSV file			
			OK	Cancel

Login Sessions

On the **Login Sessions** tab, you can define user session settings and timeouts.

To configure Veeam ONE Client login sessions settings:

1. Open Veeam ONE Client.

    For details, see Accessing Veeam ONE Client.

2. In the main menu, click **Settings** > **Server Settings**.

    Alternatively, press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Login Sessions** tab.

4. To limit the duration of an idle session:

    o [For users included in the *Veeam ONE Power Users* and *Veeam ONE Read-Only Users* security groups] specify the value in the **Idle user login session timeout, minutes** field.

    o [For users included in the *Veeam ONE Administrators* security group] specify the value in the **Idle administrator login session timeout, minutes** field.

    For more information on Veeam ONE security groups, see section Security Groups of the Veeam ONE Deployment Guide.

5. To limit the number of simultaneous login sessions under the same user credentials, specify the value in the **Maximum number of concurrent login sessions per user** field.

    To allow unlimited number of login sessions, specify 0.

6. To display date and time of the last successful or failed authentication to a user, select the **Show previous login attempts after logging in** check box.

Server Settings ✕

Mail Server Settings	**Configure idle login session timeout for user and administrator security groups to end login sessions automatically**
Notification Policy	Idle user login session timeout, minutes: `5`
SNMP Traps	Idle administrator login session timeout, minutes: `10`
Guest OS Credentials	Maximum number of concurrent login sessions per user: `2`
Monitored Datastores	Show previous login attempts after logging in: ☑
Monitored VMs	
Business View	
Login Sessions	
Audit Log	
Banners	
Other	

OK   Cancel

Audit Log

In the audit log settings, you can select which user activities in Veeam ONE Client and Veeam ONE Web Client must be logged and enable automatic shutdown of Veeam ONE services.

To configure audit log settings:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Audit Log** tab.

4. Select which events you want to log:

   o **Access to data** — fill this check box to log data access events, for example, switching tabs or opening dialogs.

   o **Changes to data** — fill this check box to log data modification events, for example, changing Veeam ONE Server settings, report parameters or modifying tree view settings.

   o **Privileged activities** — fill this check box to log administrative events, for example, managing Veeam ONE agent, updating a license or starting data collection.

   o **Login sessions** — fill this check box to log user sessions in Veeam ONE Client and Veeam ONE Web Client.

5. If you want to shut down Veeam ONE services in case Veeam ONE is unable to write audit logs, fill the **Stop Veeam ONE services upon audit log failure** check box.

If events cannot be written to Windows Event Log, Veeam ONE will trigger the *Audit log failure* alarm and gracefully shut down Veeam ONE services.

Banners

On the **Banners** tab, you can configure consent and classified data banners to comply with data protection policies and regulations.

To configure banners:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Banners** tab.

4. Select **Enable consent banner** and specify banner title and text.

   The banner will be shown to all users who log in to Veeam ONE Client and Veeam ONE Web Client. A user must click **I Agree** to continue working with Veeam ONE.

5. Select **Enable classified content banner** and specify text that will be shown to all users in Veeam ONE Client, Veeam ONE Web Client and generated reports.

   In the **Classified content banner color** field, specify banner color in HEX format.

Other Settings

To specify miscellaneous server settings:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, you can press [CTRL + S] on the keyboard.

3. In the **Server Settings** window, open the **Other** tab.

4. In the **VMware Cloud Director** section, choose whether VMware Cloud Director VMs must be shown in the Virtual Infrastructure inventory tree:

   o If you select the **Hide VMware Cloud Director VMs from Virtual Infrastructure tree** check box, VMware Cloud Director VMs will be shown in the VMware Cloud Director inventory tree only.

   o If you select the **Hide expired VMware Cloud Director vApps from Cloud Infrastructure tree** check box, expired VMware Cloud Director vApps will not be shown in the VMware Cloud Director inventory tree.

   For more information on displaying the virtual infrastructure inventory tree, see Virtual Infrastructure.

5. In the **Notifications** section, you can disable and enable notification messages about support contract expiration.

   If you select the **Disable support contract expiration notifications** check box, Veeam ONE will not display notification messages in the UI and notification emails.

   > **NOTE:**
   >
   > This option does not disable internal alarms notifying about support expiration. It only controls whether notification messages must be displayed in the UI and notification emails. For more information on working with internal alarms, see Working with Internal Alarms.

6. In the **Support utility** section, click **Launch**, to run the Veeam ONE Settings Utility.

   The utility allows you to change configuration settings of the Veeam ONE software components. For more information on working with Veeam ONE Settings Utility, see Appendix. Veeam ONE Settings Utility.

   > **IMPORTANT!**
   >
   > The Veeam ONE Settings utility must be used only under the guidance of Veeam Support. It is strongly recommended that you obtain detailed instructions from the Veeam Support team before changing any configuration settings in your Veeam ONE deployment.

7. In the **Intelligent Diagnostics** section, you can disable and enable automatic update of Veeam Intelligent Diagnostics signatures:

   If you fill the **Update signatures automatically** check box, Veeam ONE will connect to the Veeam Technical Support web server and update signatures once a day. For more information on working with signatures, see Managing Signatures.

8. In the **Multi-tenant monitoring and reporting** section, fill the **Disable multi-tenant access** check box to restrict access to Veeam ONE Client and Veeam ONE Web Client for users who have permissions on monitored infrastructure, but not included in Veeam ONE security groups. For more information on multi-user access, see section Multi-Tenant Monitoring and Reporting of the Veeam ONE Reporting Guide.

Veeam Backup & Replication Monitoring

Veeam ONE Client offers advanced functionality for monitoring Veeam Backup & Replication infrastructure and data protection operations in the managed virtual environment.

With Veeam ONE Client, you can:

1. **Analyze Veeam Backup & Replication logs to find potential issues.**

   Configure Veeam ONE to perform automatic diagnostics of backup infrastructure to facilitate troubleshooting and avoid data protection problems.

   Veeam Intelligent Diagnostics feature allows you to receive alarms with recommendations and knowledge base articles on configuration of backup infrastructure and jobs.

2. **Monitor the overall state of the backup infrastructure**.

   Check the **Summary** dashboards to reveal hotspots in the Veeam Backup & Replication infrastructure.

   Quickly review the latest status of backup, replication and SureBackup jobs, examine configuration and performance of your backup infrastructure components, detect the most loaded proxies, repositories, WAN accelerators, tape servers, cloud gateways and cloud repositories, and check whether your jobs complete within the backup window.

   Summary dashboards help you quickly reveal issues that can lead to job failure, and cause loss of valuable data.

3. **View triggered alarms**.

   Go to the **Alarms** dashboard to see details on issues and problems in your backup infrastructure.

   Data protection alarms allow you to instantaneously react to potentially dangerous situations with ongoing data protection and take immediate actions to eliminate the risk of data loss.

4. **Check the latest job status**.

   Track the status of your backup, replication, SureBackup, backup copy, SQL database transaction log backup, Oracle database backup jobs, backup to tape, file to tape, VM copy and file copy jobs.

   Get up-to-date information on the efficiency of data protection in your virtual environment and address problems with jobs as soon as they appear.

5. **Work with performance charts**.

   Drill down to performance charts to diagnose performance problems with backup infrastructure components and identify bottlenecks.

   Track CPU, memory, disk and network performance for backup servers, proxies, repositories and WAN accelerators to make sure the backup data flow is efficient, and all resources engaged in the backup process are optimally used.

6. **View the list of events**.

   View the full list of events that triggered Veeam Backup & Replication alarms, and events notifying about connection problems with Veeam Backup & Replication servers or Veeam Backup Enterprise Manager.

Prerequisites

Before you start monitoring the Veeam Backup & Replication infrastructure, make sure you have configured connections to Veeam Backup & Replication servers from which Veeam ONE will collect data. For more information on configuring server connections, see section Connecting Veeam Backup & Replication Servers of the Veeam ONE Deployment Guide.

Veeam Intelligent Diagnostics

Veeam Intelligent Diagnostics is a feature that allows you to automatically detect known issues in configuration and performance of backup infrastructure. It enables Veeam ONE to parse logs from Veeam Backup & Replication servers and trigger alarms with recommendations based on the results of log analysis. This allows you to eliminate configuration issues without the necessity to address Veeam Technical Support.

Veeam Intelligent Diagnostics process involves the following components:

- **Signatures** — problem definitions that are based on common issues investigated by Veeam Technical Support.

  Signatures are stored in Veeam ONE database and displayed as Intelligent Diagnostics alarms in the **Alarm Management** view.

  Signatures can be updated manually or automatically. For more information on updating and importing signatures, see Managing Signatures.

- **Veeam ONE agent** — a component that enables communication with Veeam Backup & Replication servers, performs collection of logs, and sends remediation commands.

  Veeam ONE agent can work in the following modes:

  - **Server**

    In this mode, Veeam ONE agent is responsible for analyzing log data and signature updates.

    Veeam ONE agent server is included into Veeam ONE installation package and deployed on the machine running Veeam ONE Client server during product installation.

  - **Client**

    In this mode, Veeam ONE agent is responsible for collecting logs and executing remediation actions on Veeam Backup & Replication servers.

    Veeam ONE agent client is deployed on Veeam Backup & Replication servers when you connect these servers to Veeam ONE. You can also deploy client agents from Veeam ONE Client. For more information on managing client Veeam ONE agents, see Managing Veeam ONE Agents.

> **NOTE:**
>
> For proper operation of Veeam Intelligent Diagnostics feature, Veeam Backup & Replication servers on which you deploy Veeam ONE agents must have a PowerShell module deployed. For more information on Veeam Backup PowerShell module, see Veeam PowerShell Reference.

How Veeam Intelligent Diagnostics Works

Veeam Intelligent Diagnostics works in the following way:

1. When Veeam Intelligent Diagnostics session starts, Veeam ONE Client sends a command to Veeam ONE agent client to collect logs from Veeam Backup & Replication.

2. Veeam ONE agent client creates a compressed log file and sends it to Veeam ONE agent server.

3. Veeam ONE agent server parses Veeam Backup & Replication logs for known exceptions and error messages by comparing logs with signatures.

4. If any known issues found, Veeam ONE Client triggers an alarm with recommendations and knowledge base articles from Veeam Technical Support.
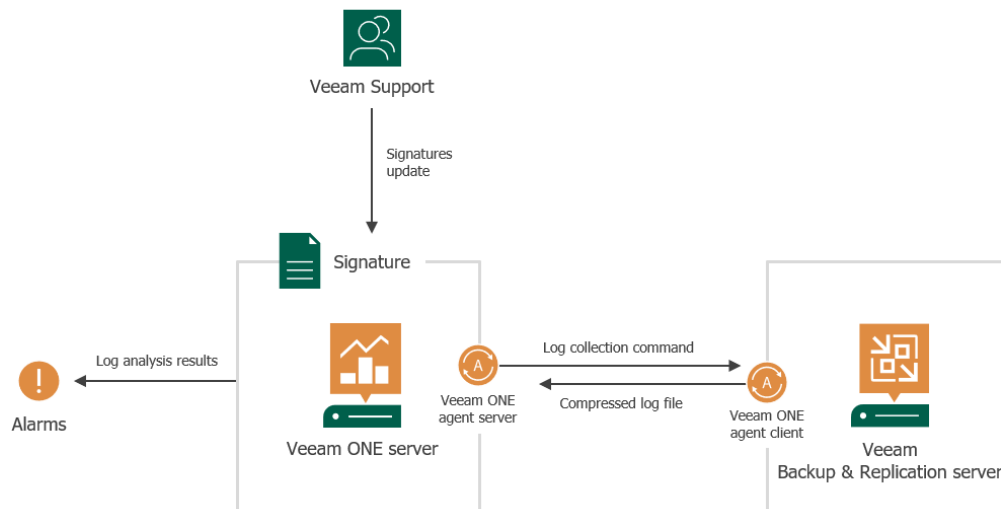
How to Configure Veeam Intelligent Diagnostics

To configure Veeam Intelligent Diagnostics, perform the following steps:

1. Install Veeam ONE agents on Veeam Backup & Replication servers connected to Veeam ONE and configure agent settings.

   For details, see Managing Veeam ONE Agents.

2. Obtain an up-to-date version of signatures.

   For details, see Managing Signatures.

3. Configure log analysis schedule or start log analysis session manually.

   For details, see Performing Log Analysis.

Managing Veeam ONE Agents

In Veeam ONE Client you can install, remove, repair and configure Veeam ONE agents.

Installing Veeam ONE Agents

By default, Veeam ONE Client installs Veeam ONE agent when you connect Veeam Backup & Replication or Veeam Backup Enterprise Manager servers in Veeam ONE Client. If you skipped Veeam ONE agent installation, you can install it later.

To install Veeam ONE agent on Veeam Backup & Replication:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the main node.

4. Open the **Veeam ONE Agents** tab.

5. From the list of connected Veeam Backup & Replication servers, select servers on which you want to install Veeam ONE agent and do either of the following:

   o Right-click the selected server and choose **Install agent** from the shortcut menu.

   o In the **Actions** pane, click **Install**.

   Press and hold the `[CRTL]` or `[SHIFT]` key to select multiple servers.

Configuring Veeam ONE Agent Settings

You can configure settings of Veeam ONE agents installed on Veeam Backup & Replication servers:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the main node.

4. Open the **Veeam ONE Agents** tab.

5. From the list of connected Veeam Backup & Replication servers, select servers for which you want to configure Veeam ONE agent settings and do either of the following:

   o Right-click the selection and choose **Agent settings** from the shortcut menu.

   o In the Actions pane, click **Settings**.

   Press and hold the `[CRTL]` or `[SHIFT]` key to select multiple agents.

6. In the **Veeam ONE Agent Settings** window, specify the required settings:

   o **Remediation actions** — keep this check box selected if you want to allow Veeam ONE agent perform remediation actions on alarms.

   For more information on alarm remediation actions, see Alarm Remediation Actions.

- o **Backup log analysis** — keep this this check box selected if you want to allow Veeam ONE agent perform analysis of Veeam Backup & Replication logs.

  For more information on log analysis, see Performing Log Analysis.

- o In the **Port number** field, specify the number of the port that Veeam ONE Client will use to communicate with Veeam ONE agent installed on Veeam Backup & Replication server.

  If you change the port number, Veeam ONE will automatically repair Veeam ONE agent to re-establish connection. For details, see Repairing Veeam ONE Agents.

7. Click **Save**.

Repairing Veeam ONE Agents

If the connection to Veeam ONE agent is lost, you may try to perform a repair. When you repair Veeam ONE agent, Veeam ONE Client re-installs the agent on Veeam Backup & Replication server and re-establishes connection.

To repair Veeam ONE agent:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the main node.

4. Open the **Veeam ONE Agents** tab.

5. From the list of connected Veeam Backup & Replication servers, select servers on which you want to repair Veeam ONE agent and do either of the following:

   - o Right-click the selected server and choose **Repair agent** from the shortcut menu.

   - o In the **Actions** pane, click **Repair**.

   Press and hold the `[CRTL]` or `[SHIFT]` key to select multiple servers.

Removing Veeam ONE Agents

If you no longer want to analyze logs and perform remediation actions for Veeam Backup & Replication, you can uninstall Veeam ONE agents:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the main node.

4. Open the **Veeam ONE Agents** tab.

5. From the list of connected Veeam Backup & Replication servers, select servers from which you want to uninstall Veeam ONE agent and do either of the following:

   o Right-click the selected server and choose **Remove agent** from the shortcut menu.

   o In the **Actions** pane, click **Remove**.

   Press and hold the `[CRTL]` or `[SHIFT]` key to select multiple servers.

Managing Signatures

If automatic signature update is enabled, and Veeam ONE Client server is connected to the Internet, it will connect to the Veeam Technical Support web server and update signatures automatically on a daily basis.

For more information on enabling automatic signature update, see Other Settings.

Alternatively, you can manually check for an available update of signatures or import signatures from file provided by Veeam Technical Support.

Updating Signatures

To update diagnostic signatures:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the main node.

4. Open the **Veeam ONE Agents** tab.

5. At the top of the page, click **Update Signatures**.

Veeam ONE Client will connect to Veeam Technical Support server over the Internet, check if an update is available, and download the latest version of signatures.

Importing Signatures

If Veeam ONE Client server has no Internet connection, you can manually import the file with the latest version of signatures:

1. Obtain the `.package` file from Veeam website.

2. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

3. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

4. In the inventory pane, select the main node.

5. Open the **Veeam ONE Agents** tab.

6. At the top of the page, click **Import Signatures**.

7. Specify a path to the `.package` file downloaded from Veeam website and click **Open**.

Performing Log Analysis

Veeam ONE Client allows you to perform log analysis according to the defined schedule or manually:

- When a scheduled log analysis session starts, Veeam ONE Client analyzes Veeam Backup & Replication logs for the last 48 hours or since the last successful log analysis session (whichever is later).

  By default, Veeam ONE agent is set to perform log analysis daily at 7:00 AM. To change the default log analysis schedule, see Scheduling Automated Log Analysis.

- When you start a log analysis session manually, Veeam ONE Client analyzes Veeam Backup & Replication logs for the last 24 hours or since the last successful log analysis session (whichever is later).

  For more information on starting log analysis manually, see Starting Log Analysis Manually.

Scheduling Automated Log Analysis

To set up daily schedule for automated log analysis:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the main node.

4. Open the **Veeam ONE Agents** tab.

5. From the list of Veeam Backup & Replication servers with installed Veeam ONE agent, select servers for which you want to configure log analysis schedule and do either of the following:

   o Right-click the selection and choose **Log analysis schedule** from the shortcut menu.

   o In the Actions pane, click **Schedule**.

   Press and hold the `[CRTL]` or `[SHIFT]` key to select multiple agents.

6. In the **Log Analysis Schedule** window, specify the time at which log analysis must start daily.

   To disable a scheduled start, select **Manually**.

7. Click **Save**.

Starting Log Analysis Manually

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the main node.

4. Open the **Veeam ONE Agents** tab.

5. From the list of Veeam Backup & Replication servers with installed Veeam ONE agent, select servers for which you want to perform log analysis and do either of the following:

   o Right-click the selection and choose **Start log analysis** from the shortcut menu.

- In the Actions pane, click **Start**.

Press and hold the `[CRTL]` or `[SHIFT]` key to select multiple agents.

6. To check the log analysis session history, click a link in the **Log Analysis Session State** column.

Stopping Log Analysis

You can stop a session, for example, if log analysis is about to take long, and you do not want to produce workload on the production environment during business hours.

To stop log analysis:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the main node.

4. Open the **Veeam ONE Agents** tab.

5. From the list of Veeam Backup & Replication servers with installed Veeam ONE agent, select servers for which you want to stop log analysis session and do either of the following:

   - Right-click the selection and choose **Stop log analysis** from the shortcut menu.

   - In the Actions pane, click **Stop**.

   Press and hold the `[CRTL]` or `[SHIFT]` key to select multiple agents.

Veeam Backup & Replication Summary Dashboards

Veeam Backup & Replication summary dashboards serve as the 'launch point' for monitoring the backup infrastructure and data protection operations in the virtual environment. The dashboards reflect the latest state of backup, replication and SureBackup jobs, and help you analyze the performance and configuration of backup infrastructure components.

Veeam ONE Client offers the following types of summary dashboards for Veeam Backup & Replication infrastructure components:

- Backup Infrastructure Summary

- Backup Repositories Overview

- Backup Repository Summary

- Proxy Servers Overview

- Proxy Server Summary

- WAN Accelerators Overview

- WAN Accelerator Summary

- Tape Servers Overview

- Tape Server Summary

- Cloud Repositories Overview

- Cloud Repository Summary

- Cloud Gateways Overview

- Cloud Gateway Pool Summary

- Cloud Gateway Summary

To view summary details for a specific backup infrastructure object or segment:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the necessary infrastructure level.

4. Open the **Summary** tab.

> **NOTE:**
>
> For proxy servers, repositories, WAN accelerators and tape servers, there are two summary dashboards:
>
> - **Summary** dashboards aggregate performance details for the previous week.
> - **Monthly Summary** dashboards aggregate performance details for the previous month.

Backup Infrastructure Summary

The backup infrastructure summary dashboard shows the latest state of data protection operations in the virtual environment and indicates the most intensively used resources in the backup infrastructure.

The dashboard is available for the following nodes:

- Backup Infrastructure

- Veeam Backup Enterprise Manager

- Veeam Backup & Replication server
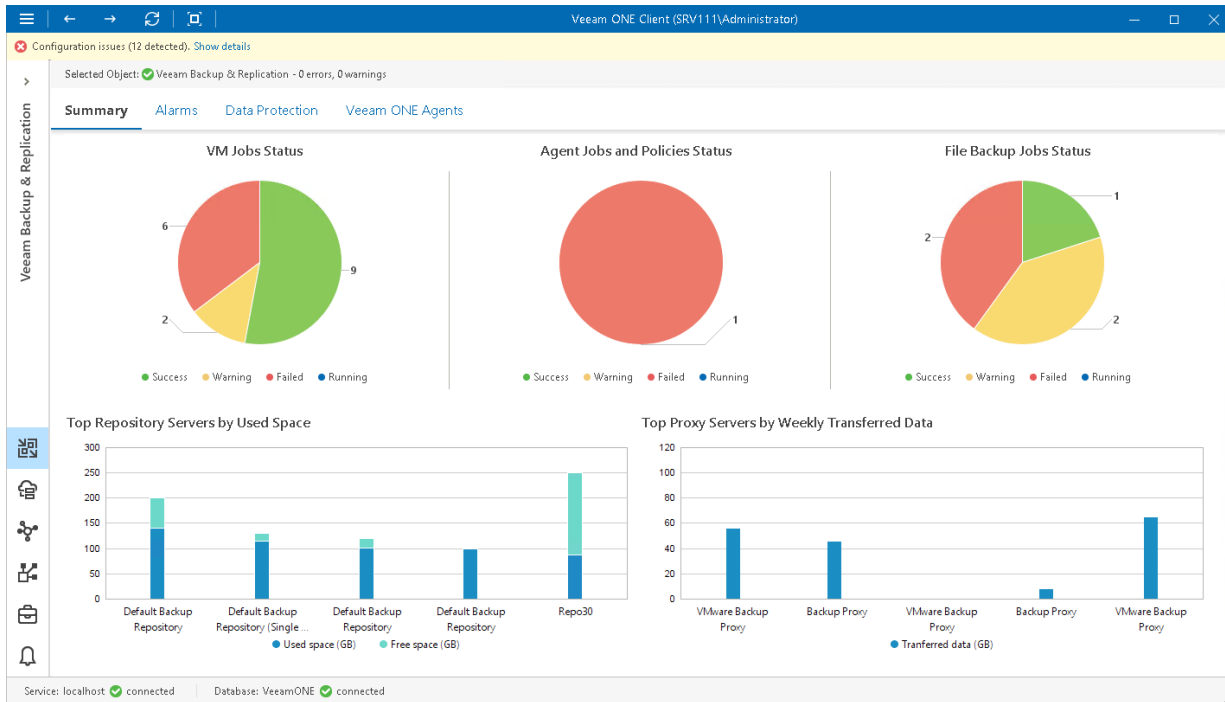
VM Jobs Status, Agent Jobs and Policies Status, File Backup Jobs Status

The charts reflect the latest status of VM protection jobs, agent protection jobs and policies, and file protection jobs for the selected level of the backup infrastructure hierarchy.

Every chart segment shows how many jobs ended with a specific status — failed jobs (red), jobs that ended with warnings (yellow), successfully performed jobs (green), and jobs that are currently running (blue). Click the necessary chart segment or a legend label to drill down to the list of jobs that ended up with the corresponding status.

For more information on Veeam Backup & Replication VM job details, see Virtual Machines.

For more information on Veeam Backup & Replication file job details, see File Shares.

For more information on Veeam Agent for Windows, Veeam Agent for Linux, Veeam Agent for Mac and Veeam Agent for Unix jobs and policies managed by Veeam Backup & Replication servers, see Computers.

Top Repository Servers by Used Space

The chart shows 5 backup repositories with the greatest amount of used storage space.

For every repository in the chart, you can track the amount of used storage space against the amount of available space. If free space on the repository is running low, you may need to free up storage space, revise your backup retention policy or even move your backups from the repository and point backup jobs to a new location.

Top Proxy Servers by Weekly Transferred Data

The chart shows 5 backup proxies that processed the greatest amount of data over the past 7 days.

To draw the chart, Veeam ONE analyzes how many VM disk and file share processing tasks were successfully performed by every proxy; failed tasks are not taken into account.

The chart helps you detect the most heavily loaded VM and file proxies and optimize the performance of your backup infrastructure. If specific proxies are overloaded with processing tasks, and the jobs often need to wait for proxy resources, you may need to deploy additional proxies or balance the processing load by assigning jobs to other proxies.

Backup Repositories Overview

The summary dashboard for the **Repositories** node provides a configuration overview and performance analysis for backup repositories managed by a backup server.
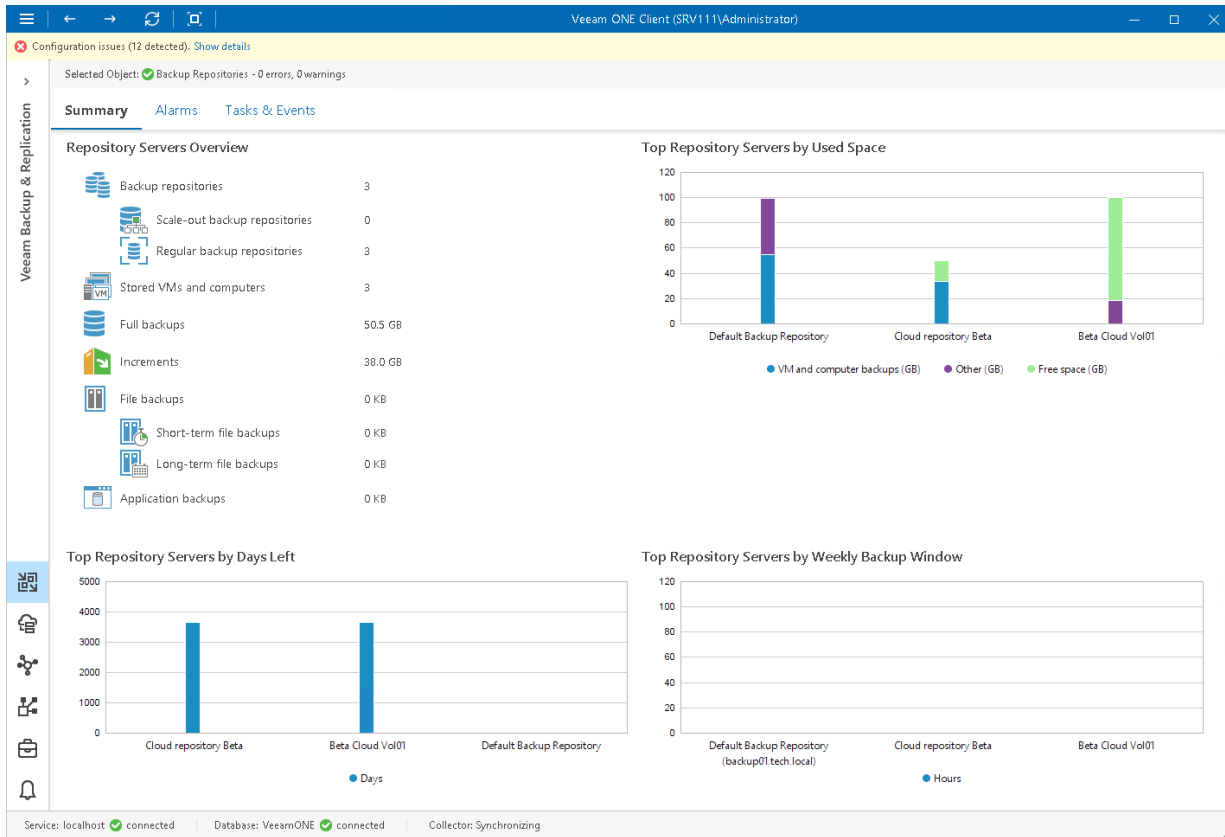
Repository Servers Overview

The section provides the following details:

- Number of repositories managed by the backup server

- Number of scale-out backup repositories

- Number of external repositories

- Number of object storage repositories

- Number of regular backup repositories

- Number of VMs and computers whose data is stored in backups on repositories

- Cumulative amount of storage space occupied by full VM and computer backups

- Cumulative amount of storage space occupied by incremental VM and computer backups

- Amount of space occupied by short-term and long-term file backups

- Amount of space occupied by application backups

Top Repository Servers by Used Space

The chart shows 5 backup repositories with the greatest amount of used storage space.

For every repository in the chart, you can see the amount of storage space used by VM, agent, file and application backups against the amount of available space. If free space on the repository is running low, you may need to free up storage space on the repository or revise your backup retention policy.

Top Repository Servers by Days Left

The chart shows 5 backup repositories that can run low on storage space sooner than others.

To draw the chart, Veeam ONE analyzes historical data and checks how fast free space on repositories has been decreasing in the past. Veeam ONE uses historical statistics to forecast how soon the repository will run out of space.

Top Repository Servers by Weekly Backup Window

The chart allows you to detect the most 'busy' repositories over the past 7 days.

For every repository, the chart shows the cumulative amount of time that the repository was busy with backup, backup copy and file backup job tasks.

Backup Repository Summary

Veeam ONE Client offers the following types of summary dashboards for backup repositories:

- Regular backup repository summary
- Scale-out backup repository summary
- Object storage repository summary
- External repository summary

Regular Backup Repository Summary

The regular repository summary dashboard provides overview details, capacity planning information and performance analysis for a chosen backup repository for the last week or month.
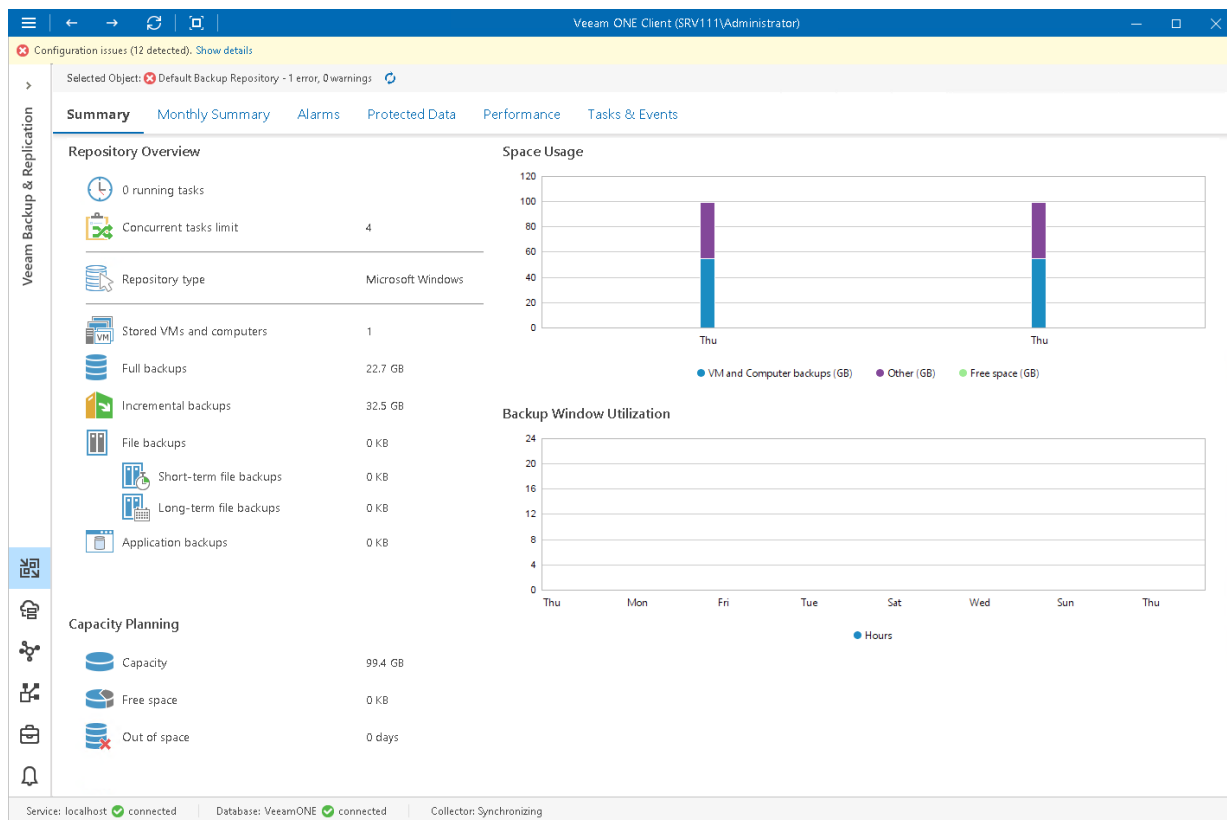
Repository Overview

The section provides the following details:

- Number of tasks that are currently running on the repository
- Maximum number of concurrent tasks allowed for the repository
- Repository type
- [For Linux repositories] Immutability feature state (Enabled, Disabled, N/A)
- Number of VMs and computers whose data is stored in backups on the repository
- Cumulative amount of storage space occupied by full VM and computer backups

- Cumulative amount of storage space occupied by incremental VM and computer backups

- Cumulative amount of storage space occupied by short- and long-term file backups

- Cumulative amount of storage space occupied by enterprise application backups

Capacity Planning

The section provides the following details:

- Storage capacity of the repository

- Amount of free space on the repository

- Number of days before the repository runs out of free space

To forecast the value, Veeam ONE uses a trend that is calculated based on historical statistics — it analyzes how fast the amount of free space on the repository was decreasing in the past and uses historical statistics to forecast how soon the repository will run out of space.

Space Usage

The chart shows the amount of used storage space against the amount of available space on the repository.

If free space on the repository is running low, you may need to free up storage space on the repository, revise your backup retention policy, or consider pointing jobs to a scale-out backup repository.

Backup Window Utilization

The chart shows the cumulative amount of time that the repository was busy with backup job tasks and backup copy job tasks during the past week or month.

The chart can help you reveal possible resource bottlenecks on the repository side. If the backup window on the chart is abnormally large, this may evidence that the required I/O operations cannot complete fast enough, and your target is presenting a bottleneck for the whole backup data processing conveyor. To identify performance bottlenecks, you can switch to repository Veeam Backup & Replication Performance Charts.

Scale-Out Backup Repository Summary

The scale-out repository summary dashboard provides overview details, capacity planning information and performance analysis for a chosen scale-out backup repository for the last week or month. You can select underlying scale-out repository extents to see details of performance, capacity and archive tiers. For more information on scale-out repository configuration, see section Scale-Out Backup Repository of the Veeam Backup & Replication User Guide.
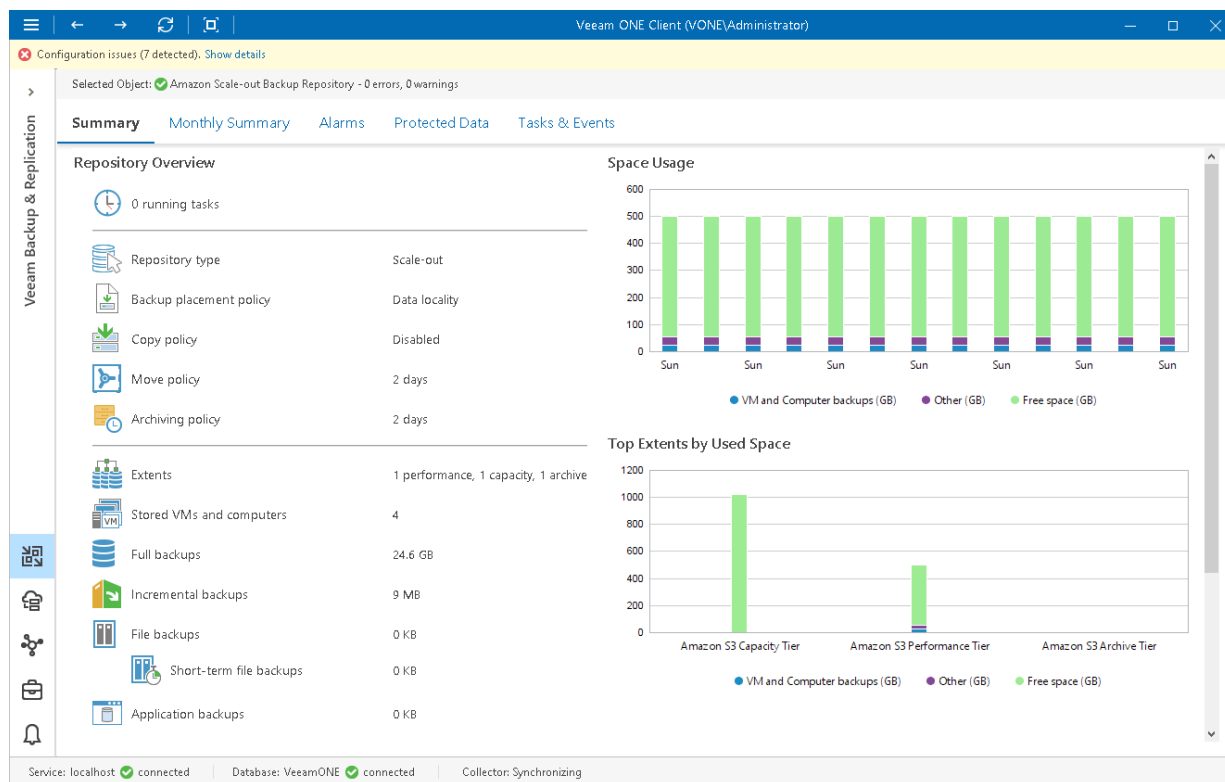
Repository Overview

The section provides the following details:

- Number of tasks that are currently running on the repository

- Repository type (Scale-out backup repository)

- Backup placement policy (as configured in the scale-out repository settings)

- Copy policy (as configured in the capacity tier settings)

- Move policy (as configured in the capacity tier settings)

- Archiving policy (as configured in the archive tier settings)

- Number of performance, capacity and archive tier extents that make up the scale-out backup repository

- Number of VMs and computers whose data is stored in backups on the repository

- Cumulative amount of storage space occupied by full VM and computer backups

- Cumulative amount of storage space occupied by incremental VM and computer backups

- Cumulative amount of storage space occupied by short- and long-term file backups

- Cumulative amount of storage space occupied by enterprise application backups

Capacity Planning

The section provides the following details:

- Storage capacity of the repository

- Amount of free storage space on the repository

- Number of days before the repository runs out of free space.

To forecast the value, Veeam ONE uses a trend that is calculated based on historical statistics — it analyzes how fast the amount of free space on the repository was decreasing in the past and uses historical statistics to forecast how soon the repository will run out of space.

Space Usage

The chart shows the amount of used storage space against the amount of available space on the repository.

If free space on the repository is running low, you may need to free up storage space on the repository, revise your backup retention policy, or consider pointing jobs to another repository.

Top Extents by Used Space

The chart shows extents with the greatest amount of used storage space.

For every extent in the chart, you can see the amount of used storage space against the amount of available space.

Object Storage Repository Summary

The object storage repository summary dashboard provides overview details and performance analysis for a chosen object storage repository added as a Capacity Tier for the last week or month.
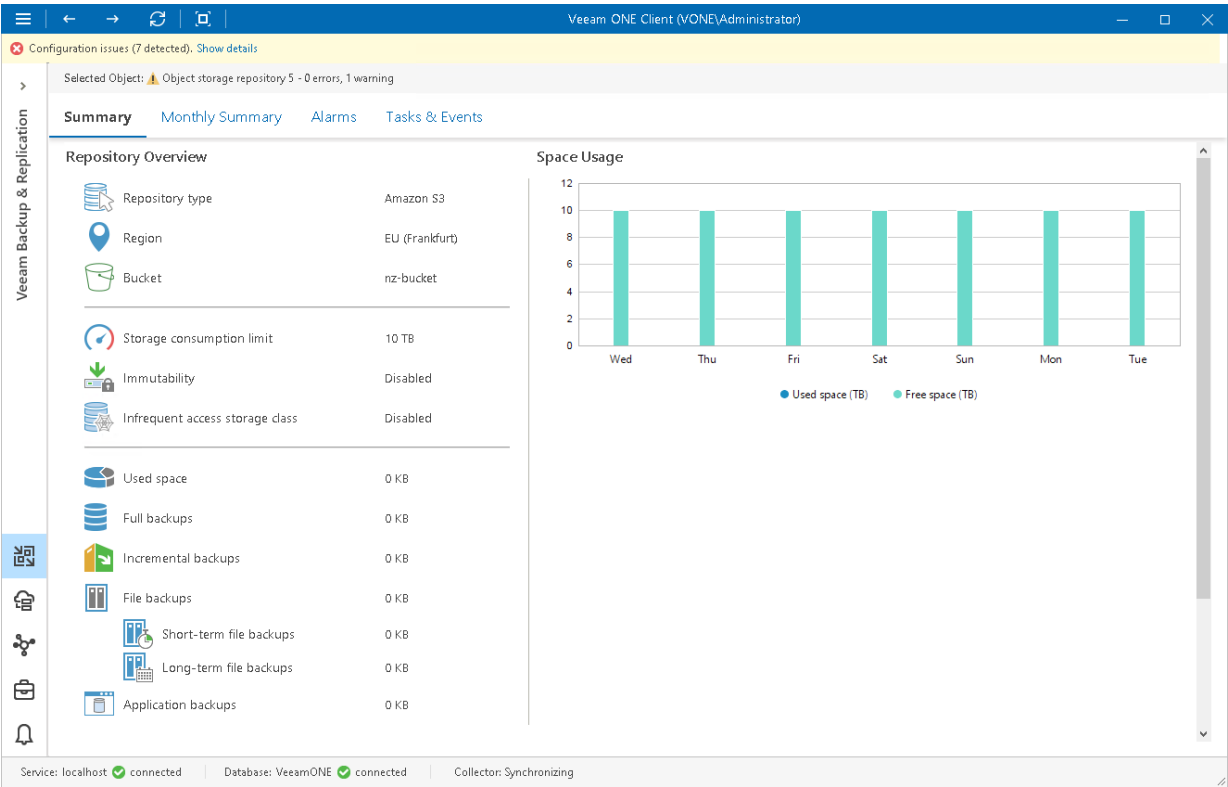
Repository Overview

The section provides the following details:

- Repository type

- Region at which the repository is located

- Name of bucket or container

- Limit of storage consumption

- Immutability feature state (Enabled, Disabled, N/A)

- Class of the infrequent access storage

- Cumulative amount of storage space occupied by full and incremental VM and computer backups

- Cumulative amount of storage space occupied by short- and long-term file backups

Capacity Planning

The section provides the following details:

- Storage capacity of the repository

- Amount of free storage space on the repository

- Number of days before the repository runs out of free space.

To forecast the value, Veeam ONE uses a trend that is calculated based on historical statistics — it analyzes how fast the amount of free space on the repository was decreasing in the past and uses historical statistics to forecast how soon the repository will run out of space.

Space Usage

The chart shows the amount of used storage space against the amount of available space on the repository.

If free space on the repository is running low, you may need to free up storage space on the repository, revise your backup retention policy, or consider pointing jobs to another repository.

External Repository Summary

The external repository summary dashboard provides overview details and performance analysis for a chosen external repository for the last week or month.
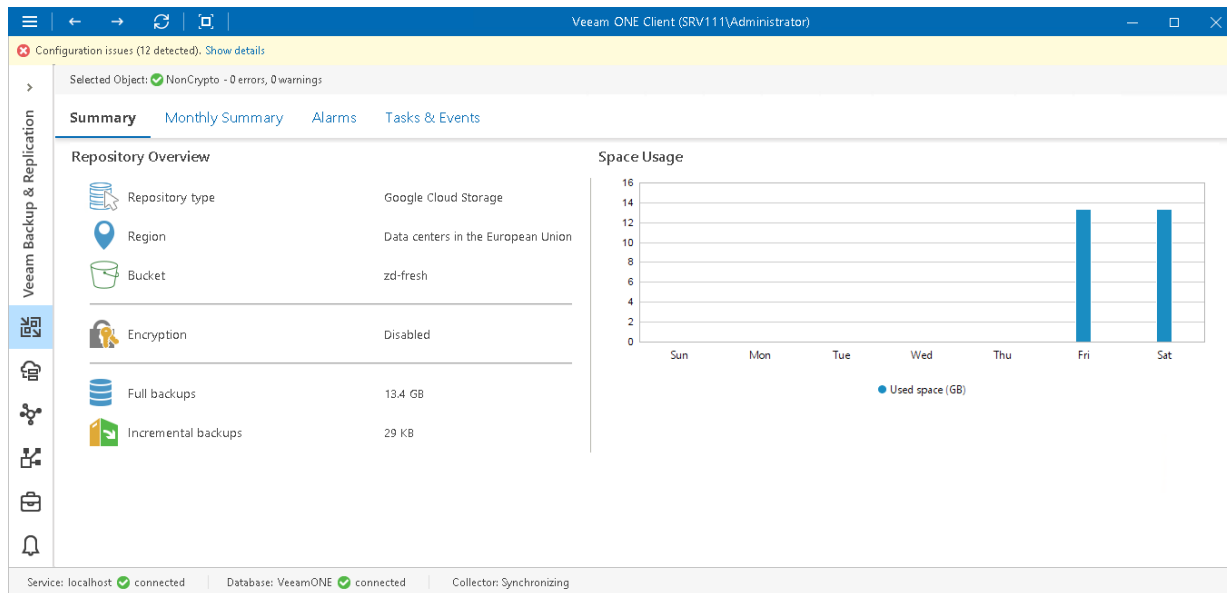
Repository Overview

The section provides the following details:

- Repository type

- Region at which the repository is located

- Name of a bucket or container

- Number of cloud VMs whose data is stored in backups on the repository

- Cumulative amount of storage space occupied by full cloud VM backups

- Cumulative amount of storage space occupied by incremental cloud VM backups

- Encryption settings (as configured in the external repository settings)

Space Usage

The chart shows the amount of storage space used by the files on the repository.

If the space consumed on the repository is running high, you may need to free up storage space on the repository, revise your backup retention policy, or consider using another repository.

Backup Proxies Overview

The summary dashboard for the **Proxies** node provides a configuration overview and performance analysis for VM, file and CDP proxies managed by a backup server.

This dashboard can help you detect configuration inefficiencies in your data protection infrastructure. If the same proxy server appears to process a great number of disks, transfer the greatest amount of backup data and use the largest backup window, you may need to re-balance the processing load across your backup proxies. The charts may also help you reveal 'lazy' proxies that you may decide to decommission.
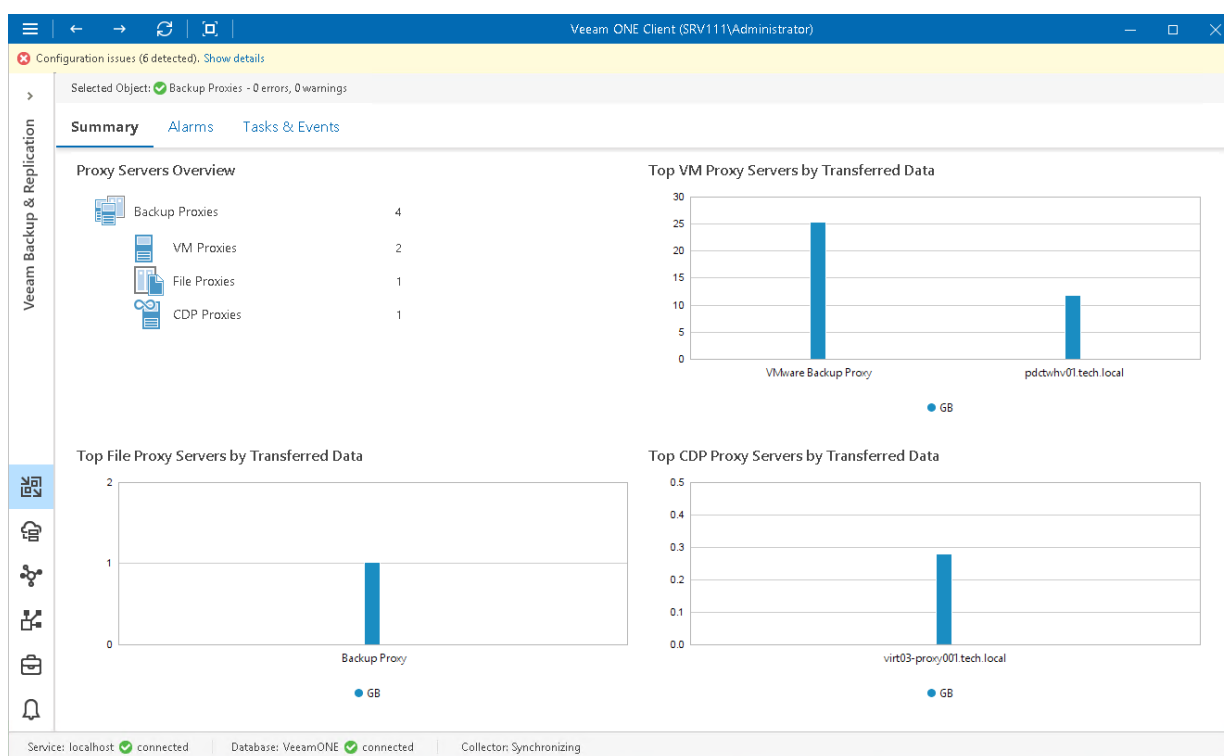
Proxy Servers Overview

The section shows the breakdown of backup proxies by the proxy type (*VM Proxies*, *File Proxies*, *CDP Proxies*).

Top VM Proxy Servers by Transferred Data

The chart shows 5 backup proxies that transferred the greatest amount of backup data to the target destination (backup repository or replica datastore/volume) over the past 7 days.

For every backup proxy, the chart shows the total amount of data that the proxy transferred over the network after the source-side deduplication and compression. The chart can help you detect backup proxies that transfer the greatest amount of backup data and estimate the load that backup and replication jobs impose on the network.

Top File Proxy Servers by Transferred Data

The chart shows 5 file proxies that transferred the greatest amount of backup data to the target destination (backup repository) over the last 7 days.

For every backup proxy, the chart shows the total amount of data that the proxy transferred over the network after the source-side deduplication and compression. The chart can help you detect backup proxies that transfer the greatest amount of backup data and estimate the load that file backup jobs impose on the network.

Top CDP Proxy Servers by Transferred Data

The chart shows 5 CDP proxies that transferred the greatest amount of VM data to the target host over the last 7 days.

For every proxy, the chart shows the total amount of data that the proxy transferred over the network after the source-side deduplication and compression. The chart can help you detect proxies that transfer the greatest amount of data and estimate the load that CDP sessions impose on the network.

VM Proxy Servers Overview

The summary dashboard for the **VM Proxies** node provides a configuration overview and performance analysis for VM proxies and file proxies managed by a backup server.

> **NOTE:**
>
> Veeam Cloud Connect service providers cannot see performance data for proxies used by tenant data protection jobs.
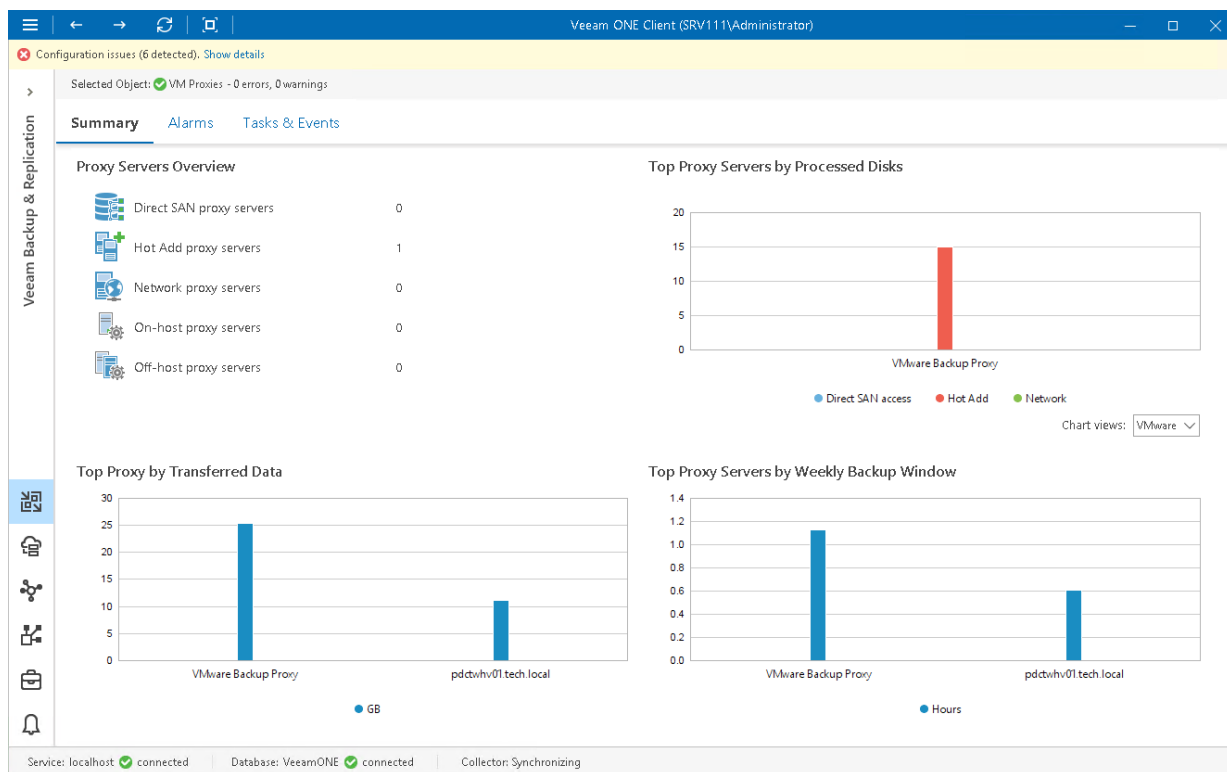
Proxy Servers Overview

The section shows the breakdown of backup proxies by the transport or backup mode:

- [VMware vSphere] You can see how many VMware backup proxies retrieve VM data from source datastores using the Direct SAN Access, Hot Add or Network transport mode.

  If a backup proxy uses different modes to retrieve VM data from various source datastores, Veeam ONE will detect its primary transport mode quantitatively, based on the number of processed VM disks. For example, if a backup proxy processed 10 VM disks using the Hot Add mode and 20 VM disks using the Network mode, the proxy would be reported as a 'Network proxy server'.

- [Microsoft Hyper-V] You can see how many Hyper-V proxies retrieve and process VM data in the on-host and off-host backup modes.

Top Proxy Servers by Processed Disks

The chart shows 5 backup proxies that processed the greatest number of VMs over the past 7 days.

To draw the chart, Veeam ONE analyzes how many VM processing tasks were successfully performed by every proxy; failed tasks are not taken into account.

The chart helps you detect the most heavily loaded backup proxies and optimize the performance of your backup infrastructure. If specific proxies are overloaded with VM processing tasks, and the tasks often need to wait for proxy resources, you may need to deploy additional proxies or balance the processing load by assigning jobs to other proxies.

You can use the **Chart views** list to view the number of VMs processed by VMware and Hyper-V backup proxies.

Top Proxy by Transferred Data

The chart shows 5 backup proxies that transferred the greatest amount of backup data to the target destination (backup repository or replica datastore/volume) over the past 7 days.

For every backup proxy, the chart shows the total amount of data that the proxy transferred over the network after the source-side deduplication and compression. The chart can help you detect backup proxies that transfer the greatest amount of backup data and estimate the load that backup and replication jobs impose on the network.

Top Proxy Servers by Weekly Backup Window

The chart allows you to detect the most 'busy' proxy servers over the past 7 days.

For every proxy, the chart shows the cumulative amount of time that the proxy was retrieving, processing and transferring VM data.

The chart can help you reveal possible resource bottlenecks. If the backup window on the chart is abnormally large, this can evidence of low source data retrieval speed, high proxy CPU load or insufficient network throughput.

File Proxy Servers Overview

The summary dashboard for the **File Proxies** node provides a configuration overview and performance analysis for file proxies managed by a backup server.
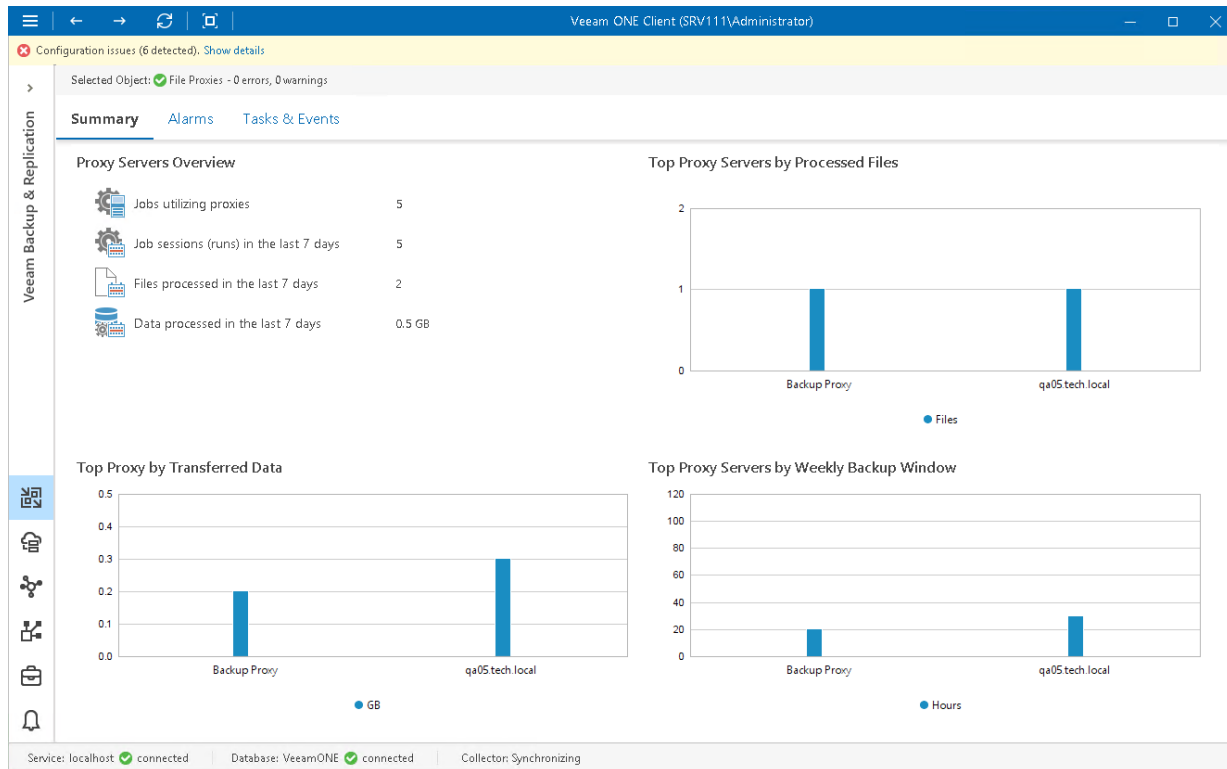
Proxy Servers Overview

The section provides the following details:

- Number of file backup jobs configured to use file proxies

- Number of job sessions that the proxies have processed during the last 7 days

- Number of files that the proxies have processed during the last 7 days

- Total amount of data that the proxy has processed during the last 7 days

Top Proxy Servers by Processed Files

The chart shows 5 file proxies that processed the greatest number of files over the last 7 days.

To draw the chart, Veeam ONE analyzes how many files were successfully processed by every proxy.

The chart helps you detect the most heavily loaded file proxies and optimize the performance of your backup infrastructure. If specific proxies are overloaded with file processing tasks, and the tasks often need to wait for proxy resources, you may need to deploy additional proxies or balance the processing load by assigning jobs to other proxies.

Top Proxy by Transferred Data

The chart shows 5 file proxies that transferred the greatest amount of backup data to the target destination (backup repository) over the last 7 days.

For every backup proxy, the chart shows the total amount of data that the proxy transferred over the network after the source-side deduplication and compression. The chart can help you detect backup proxies that transfer the greatest amount of backup data and estimate the load that file backup jobs impose on the network.

Top Proxy Servers by Weekly Backup Window

The chart allows you to detect the most 'busy' proxy servers over the last 7 days.

For every proxy, the chart shows the cumulative amount of time that the proxy was retrieving, processing and transferring file share data.

The chart can help you reveal possible resource bottlenecks. If the backup window on the chart is abnormally large, this can evidence of low source data retrieval speed, high proxy CPU load or insufficient network throughput.

CDP Proxy Servers Overview

The summary dashboard for the **CDP Proxies** node provides a configuration overview and performance analysis for CDP proxies managed by a backup server.
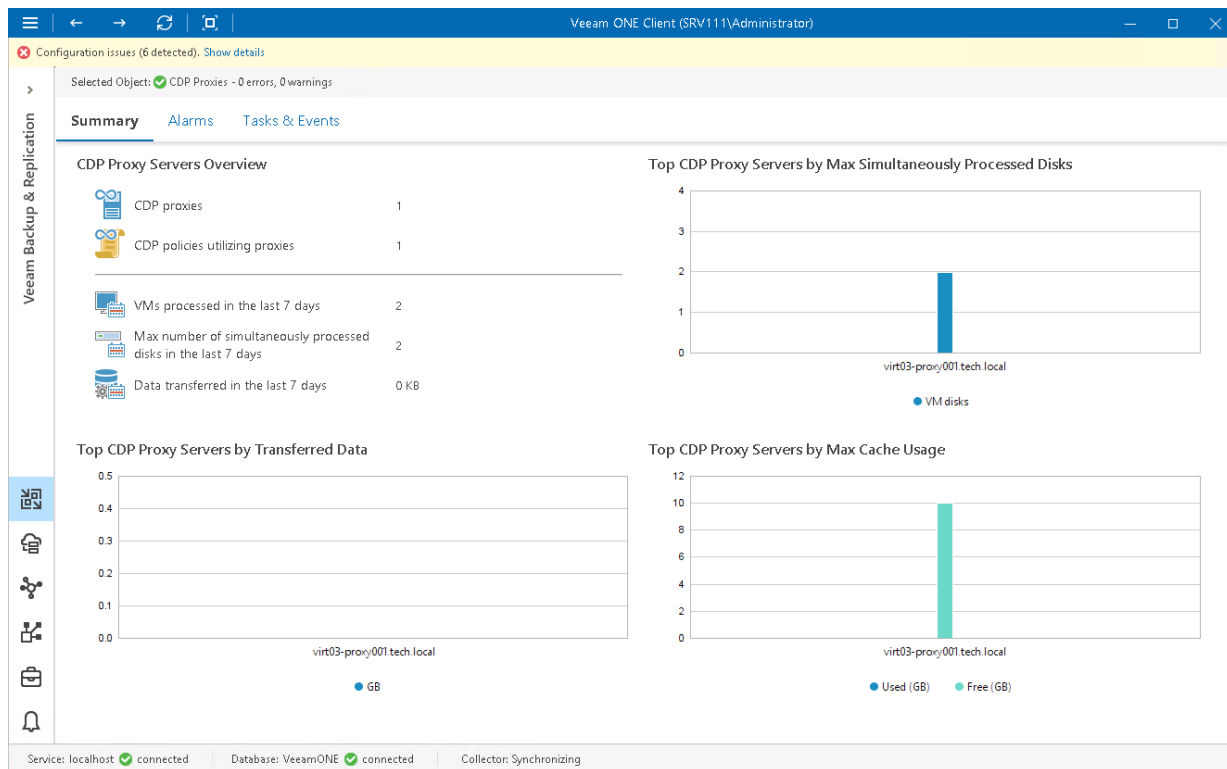
CDP Proxy Servers Overview

The section provides the following details:

- Number of CDP proxies configured on the backup server.

- Number of CDP policies configured to use proxies

- Number of VMs that CDP proxies have processed in the last 7 days

- Maximum number of VM disks that proxies have simultaneously processed in the last 7 days

- Total amount of data that proxies have processed during the last 7 days

Top CDP Proxy Servers by Max Simultaneously Processed Disks

The chart shows 5 CDP proxies that simultaneously processed the greatest number of VM disks over the last 7 days.

To draw the chart, Veeam ONE analyzes how many disks were successfully processed by every proxy.

The chart helps you detect the most heavily loaded CDP proxies and optimize the performance of your backup infrastructure. If specific proxies are overloaded with disk processing tasks, and the tasks often need to wait for proxy resources, you may need to deploy additional proxies or balance the processing load by assigning policies to other proxies.

Top CDP Proxy Servers by Transferred Data

The chart shows 5 CDP proxies that transferred the greatest amount of VM data to the target host over the last 7 days.

For every proxy, the chart shows the total amount of data that the proxy transferred over the network after the source-side deduplication and compression. The chart can help you detect proxies that transfer the greatest amount of data and estimate the load that CDP sessions impose on the network.

Top CDP Proxy Servers by Max Cache Usage

The chart shows 5 CDP proxies that used the maximum amount of space allocated for storing cache over the last 7 days.

For every proxy, the chart shows the amount of free and used space allocated for cache storage. The chart can help you detect proxies that store the greatest amount of temporary cached data and estimate which proxies require allocating more storage space.

Backup Proxy Summary

Veeam ONE Client offers the following types of summary dashboards for proxy servers:

- VM proxy summary

- File proxy summary

- CDP proxy summary

VM Proxy Summary

The VM proxy summary dashboard provides overview details and performance analysis for a chosen VM backup proxy for the last week or month.

> **NOTE:**
>
> Veeam Cloud Connect service providers cannot see performance data for proxies used by tenant data protection jobs.
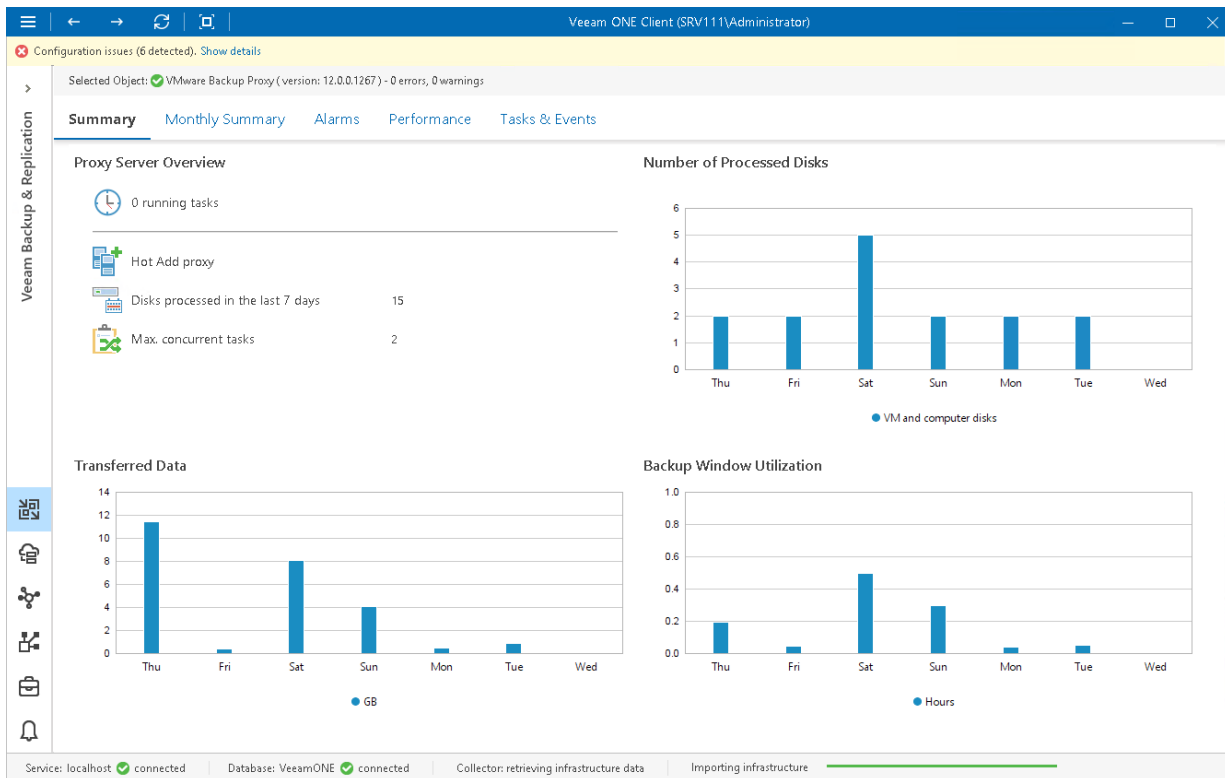
Proxy Server Overview

The section provides the following details:

- Number of tasks that the proxy is currently processing

- Mode that the proxy uses to process VM disks (Direct SAN Access, Hot Add or Network for VMware backup proxies; on-host or off-host for Hyper-V proxies)

- Number of VM disks that the proxy has processed during the last 7 days

- Number of concurrent VM disk processing tasks that can be assigned to the proxy (as configured in proxy settings)

Number of Processed Disks

The chart shows how many VM disks the proxy processed over the last 7 days.

To draw the chart, Veeam ONE Client analyzes how many disk processing tasks were successfully performed by the proxy; failed tasks are not taken into account.

The chart helps you to analyze workload on the proxy and optimize the performance of your backup infrastructure. If the proxy is overloaded with processing tasks, and the tasks often need to wait for the proxy resources, you may need to deploy additional proxies or balance the processing load by assigning jobs to other proxies.

Transferred Data

The chart shows the amount of backup data that the proxy transferred to the target destination (backup repository or replica, datastore/volume) over the last 7 days.

The chart shows the total amount of data that the proxy transferred over the network after the source-side deduplication and compression. The chart can help you measure the amount of backup traffic coming from the proxy.

Backup Window Utilization

The chart allows you to estimate how 'busy' the proxy was during the last 7 days. The chart shows the cumulative amount of time that the proxy was retrieving, processing and transferring VM data.

The chart can help you reveal possible resource bottlenecks. If the backup window on the chart is abnormally large, this can evidence of low source data retrieval speed, high proxy CPU load or insufficient network throughput. To identify performance bottlenecks, you can switch to proxy Veeam Backup & Replication Performance Charts.

File Proxy Summary

The file proxy summary dashboard provides overview details and performance analysis for a chosen file backup proxy for the last week or month.
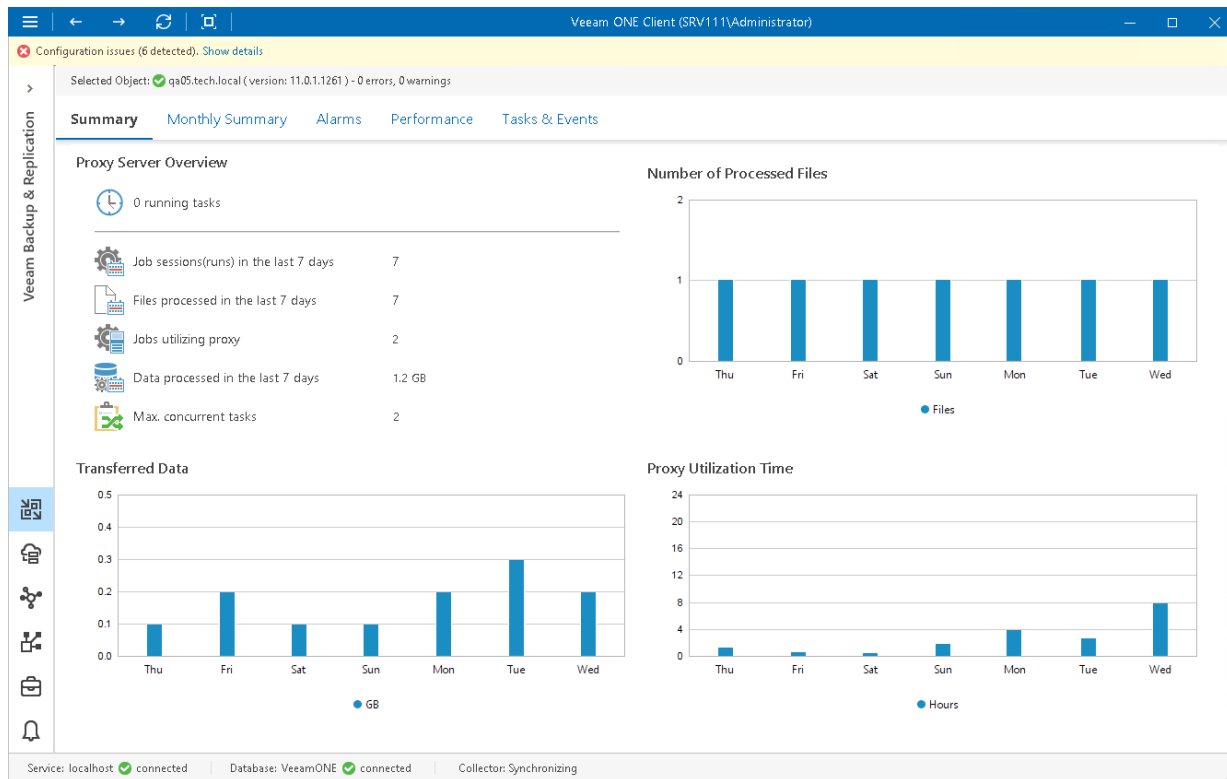
Proxy Server Overview

The section provides the following details:

- Number of tasks that the proxy is currently processing

- Number of job sessions that the proxy has processed during the last 7 days

- Number of files that the proxy has processed during the last 7 days

- Number of file backup jobs configured to use the proxy

- Total amount of data that the proxy has processed during the last 7 days

- Number of concurrent file processing tasks that can be assigned to the proxy (as configured in proxy settings)

Number of Processed Files

The chart shows how many files the proxy processed over the last 7 days.

To draw the chart, Veeam ONE Client analyzes how many files were successfully processed by the proxy.

The chart helps you to analyze workload on the proxy and optimize the performance of your backup infrastructure. If the proxy is overloaded with processing tasks, and the tasks often need to wait for the proxy resources, you may need to deploy additional proxies or balance the processing load by assigning jobs to other proxies.

Transferred Data

The chart shows the amount of backup data that the file proxy transferred to the target destination (backup repository) over the last 7 days.

The chart shows the total amount of data that the proxy transferred over the network after the source-side deduplication and compression. The chart can help you measure the amount of backup traffic coming from the proxy.

Proxy Utilization Time

The chart allows you to estimate how 'busy' the proxy was during the last 7 days. The chart shows the cumulative amount of time that the proxy was retrieving, processing and transferring file share data.

The chart can help you reveal possible resource bottlenecks. If the utilization time on the chart is abnormally large, this can evidence of low source data retrieval speed, high proxy CPU load or insufficient network throughput. To identify performance bottlenecks, you can switch to proxy Veeam Backup & Replication Performance Charts.

CDP Proxy Summary

The CDP proxy summary dashboard provides overview details and performance analysis for a chosen CDP proxy for the last week or month.
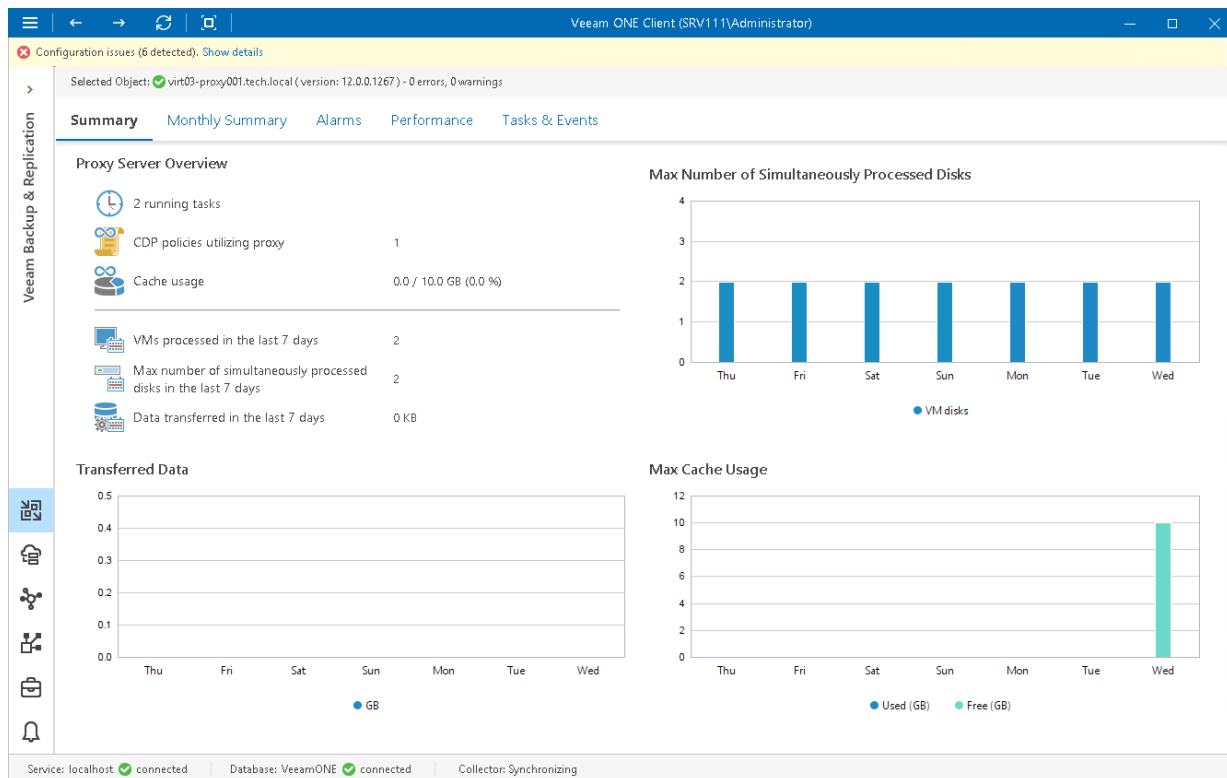
Proxy Server Overview

The section provides the following details:

- Number of tasks that the proxy is currently processing

- Number of CDP policies configured to use the proxy

- Total amount of cache data used by the proxy

- Number of VMs that the proxy has processed in the last 7 days

- Maximum number of VM disks that the proxy has simultaneously processed in the last 7 days

- Total amount of data that the proxy has processed during the last 7 days

Max Number of Simultaneously Processed Disks

The chart shows how many VM disks the proxy processed over the last 7 days.

To draw the chart, Veeam ONE Client analyzes how many VM disks were successfully processed by the proxy.

The chart helps you to analyze workload on the proxy and optimize the performance of your backup infrastructure. If the proxy is overloaded with processing tasks, and the tasks often need to wait for the proxy resources, you may need to deploy additional proxies or balance the processing load by assigning jobs to other proxies.

Transferred Data

The chart shows the amount of VM data that the proxy transferred to the target host over the last 7 days.

The chart shows the total amount of data that the proxy transferred over the network after the source-side deduplication and compression. The chart can help you measure the amount of traffic coming from the proxy.

Max Cache Usage

The chart shows the amount of temporary cached data that the proxy offloaded to the cache folder and the amount of free space in this folder over the last 7 days. If the size of the offloaded cache changed during the day, the chart will show the maximum size.

The chart can help you analyze how data blocks of continuously replicated VMs change during the week and estimate if the proxy require allocating more storage space.

WAN Accelerators Overview

The summary dashboard for the **WAN Accelerators** node provides a configuration overview and performance analysis for WAN accelerators managed by a backup server.

> **NOTE:**
>
> For WAN accelerators used in Veeam Cloud Connect jobs, performance data is available only if the target WAN accelerator is present in the Veeam ONE infrastructure.

Charts in this dashboard can help you estimate the efficiency of VM and computer data transfer over WAN links. Comparing the amount of transferred and saved traffic, you can measure how the amount of VM and computer traffic was reduced by means of Veeam WAN acceleration.
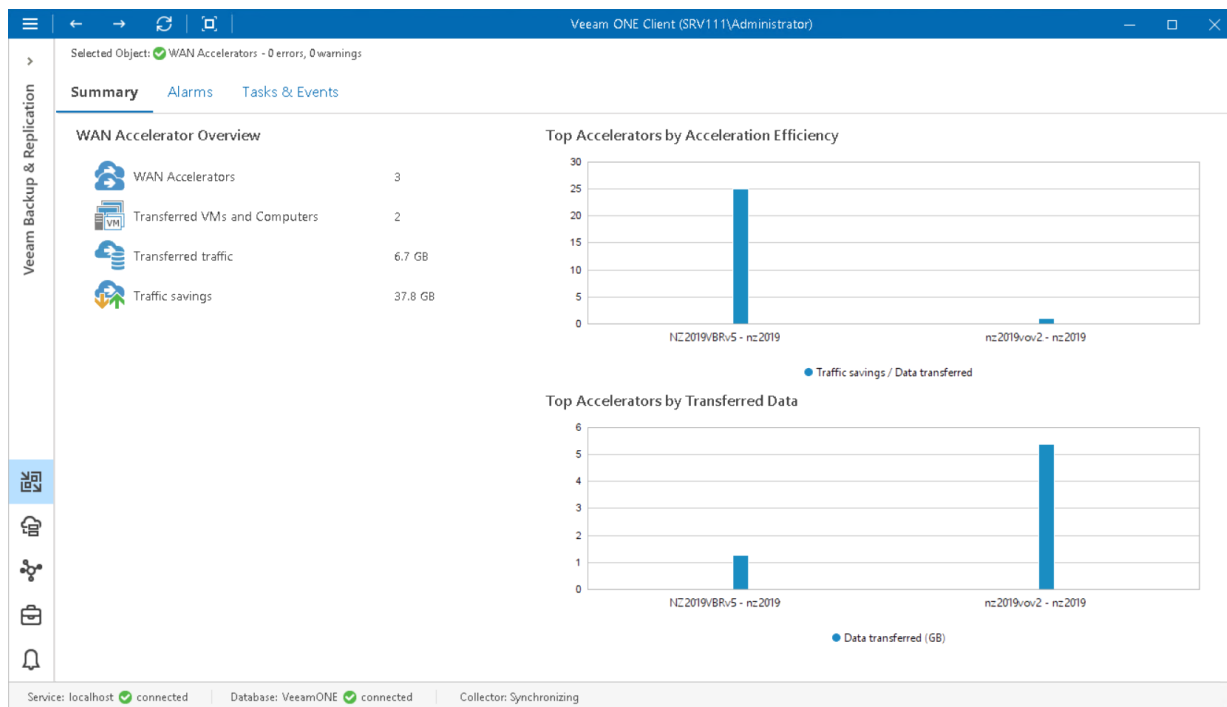
WAN Accelerator Overview

The section provides the following details:

- Number of WAN accelerators managed by the backup server

- Number of VMs and computers stored in restore points transferred by WAN accelerators during backup copy job and replication job sessions

- Cumulative amount of network traffic transferred by WAN accelerators to the target destination (secondary repositories or replica datastore/volume)

- Cumulative amount of saved traffic — that is, the difference between the amount of VM or computer data that was read from the source location (source repository or datastore/volume) and the amount of data that was actually transferred to the target destination (secondary repository or replica datastore/volume)

Top Accelerators by Acceleration Efficiency

The chart shows 5 pairs of WAN accelerators that saved the greatest amount of traffic over the past 7 days.

To draw the chart, Veeam ONE analyzes the difference between the amount of VM or computer data read from the source location (source repository or datastore/volume) and the amount of data that was actually transferred to the target destination (secondary repository or replica datastore/volume) over the past 7 days.

Top Accelerators by Transferred Data

The chart shows 5 pairs of WAN accelerators that transferred the greatest amount of VM and computer data over the past 7 days.

Every graph in the chart shows the total amount of VM and computer data that was sent from the source-side accelerator to the target-side accelerator over the network.

WAN Accelerator Summary

The WAN accelerator summary dashboard presents overview details and performance analysis for the chosen WAN accelerator.

> **NOTE:**
>
> For WAN accelerators used in Veeam Cloud Connect jobs, performance data is available only if the target WAN accelerator is present in the Veeam ONE infrastructure.
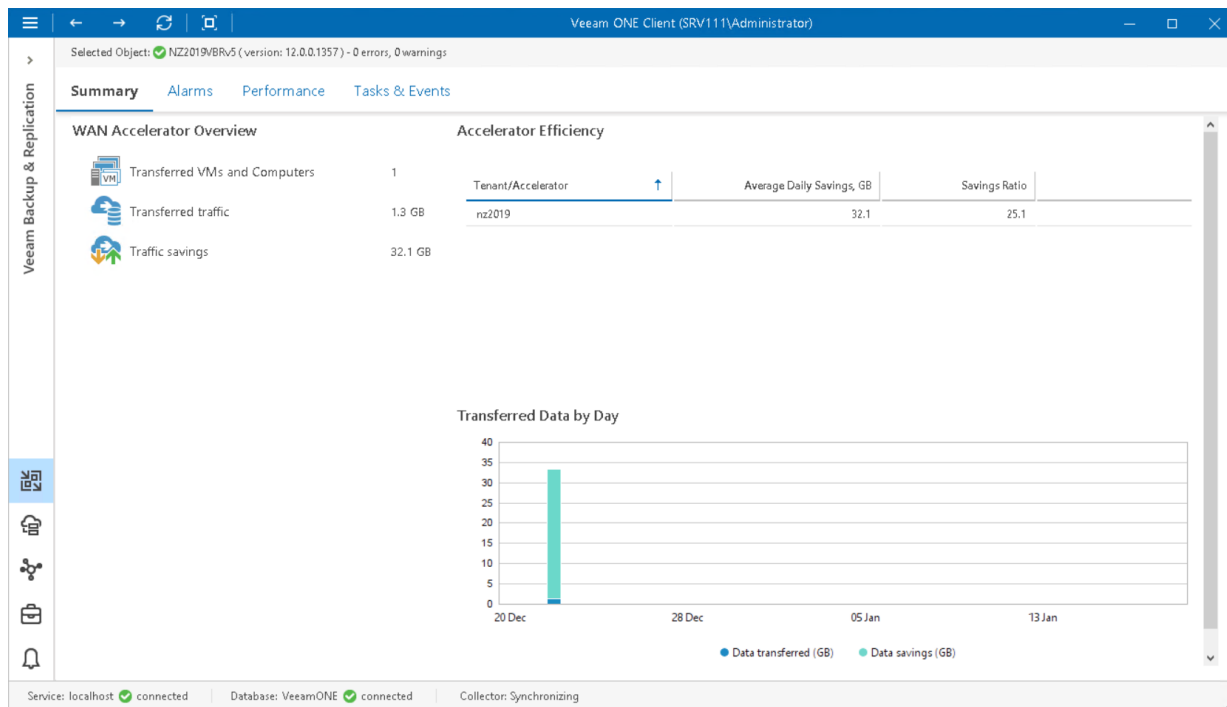
WAN Accelerator Overview

The section provides the following details:

- Number of VMs and computers stored in restore points transferred or received by the WAN accelerator during backup copy job or replication job sessions.

  If the same server acts as a target- and source-side accelerator at the same time, the dashboard will show aggregate values for transferred and received restore points.

- Amount of network traffic transferred from the accelerator to target.

- Amount of saved traffic — the difference between the amount of VM and computer data that was read from the source location (source repository or datastore/volume) and the amount of data that was actually transferred to the target destination (secondary repository or replica datastore/volume).

Accelerator Efficiency

The chart shows WAN accelerators that saved the greatest amount of traffic over the past period.

The chart lists tenant or accelerator IP, the average amount of traffic the accelerator saves daily in GB, and the ratio between the amount of VM and computer data read from the source location and the amount of data that was transferred to the destination.

Transferred Data by Day

The chart shows the amount of VM and computer data that was read from the source location (source repository or datastore/volume) and the amount of data that was actually transferred to the target destination (secondary repository or replica datastore/volume) over the past period.

Tape Servers Overview

The summary dashboard for the **Tape Servers** node presents a configuration overview and performance analysis for tape servers managed by a backup server.
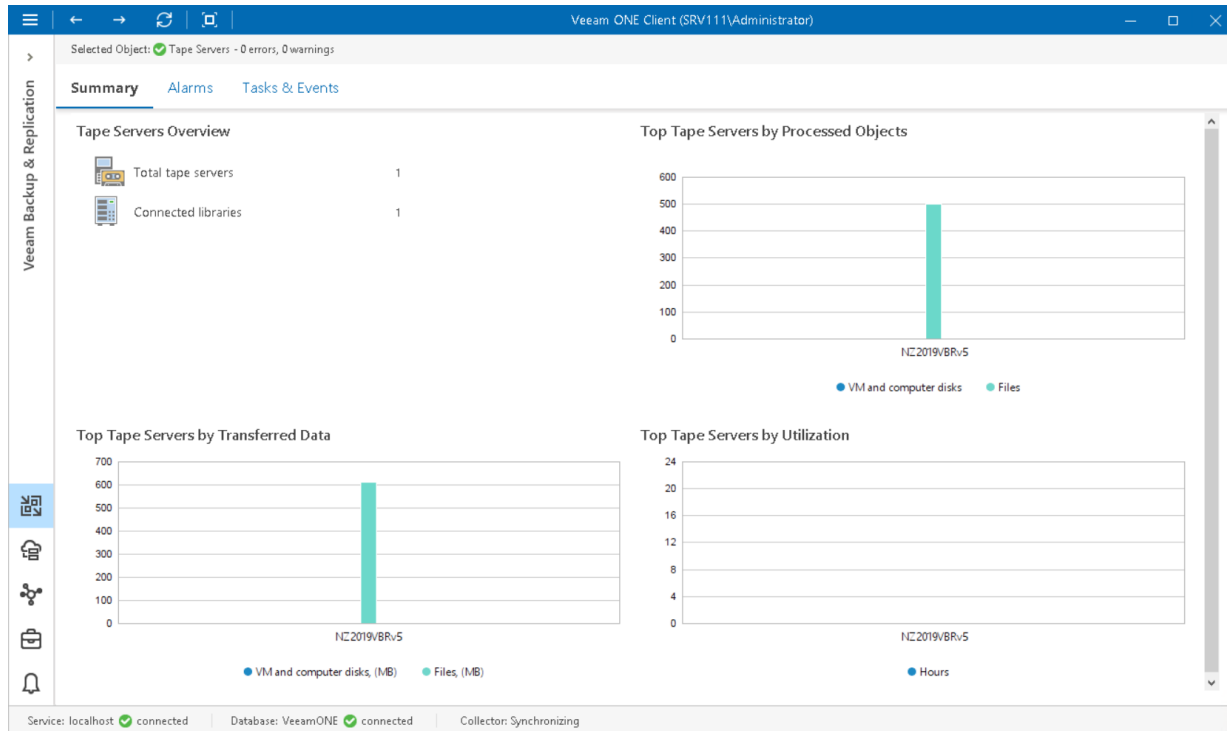
Tape Servers Overview

The section shows the number of tape servers managed by a Veeam Backup & Replication server, and tape libraries connected to these servers.

Top Tape Servers by Processed Objects

The chart shows 5 tape servers that processed and archived to tape the greatest number of VM and computer disks and files over the past 7 days. To draw the chart, Veeam ONE calculates the total number of VM and computer disks and files in all backup restore points archived to tape.

Top Tape Servers by Transferred Data

The chart shows 5 tape servers that transferred the greatest amount of data to tape devices over the past 7 days.

Top Tape Servers Utilization

The chart allows you to detect the most 'busy' tape servers over the past 7 days. For every tape server, the chart shows the cumulative amount of time that the server was retrieving, processing and transferring data.

The chart can help you reveal possible resource bottlenecks. If the graph on the chart is abnormally large, this can evidence of low data retrieval speed, high CPU load or insufficient network throughput.

Tape Server Summary

The tape server summary dashboard provides overview information and performance analysis for the chosen tape server.
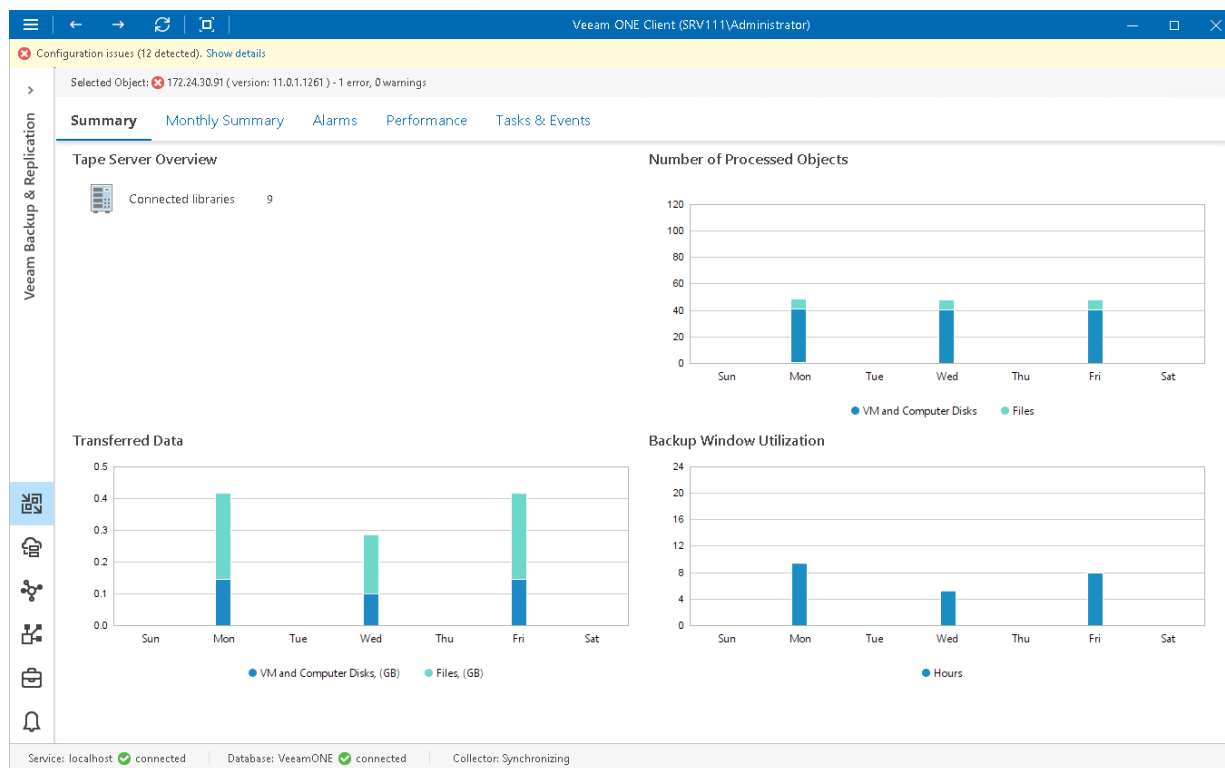
Tape Server Overview

The section outlines the number of tape libraries connected to the tape server.

Number of Processed Objects

The chart shows how many VM and computer disks and files the tape server processed and archived to tape over the past 7 days. To draw the chart, Veeam ONE calculates the total number of VM and computer disks and files in all backup restore points archived to tape.

Transferred Data

The chart shows the amount of data that the tape server transferred to tape devices over the past 7 days. The chart can help you measure the amount of traffic coming from the tape server.

Backup Window Utilization

The chart allows you to estimate how 'busy' the tape server was during the past 7 days. The chart shows the cumulative amount of time that the tape server was retrieving, processing and transferring data.

The chart can help you reveal possible resource bottlenecks. If the backup window on the chart is abnormally large, this can evidence of low source data retrieval speed, high CPU load or insufficient network throughput.

Cloud Repositories Overview

The summary dashboard for the **Cloud Repositories** node presents a configuration overview and storage utilization analysis for cloud repositories (repositories allocated for users by Veeam Cloud Connect Service Providers).
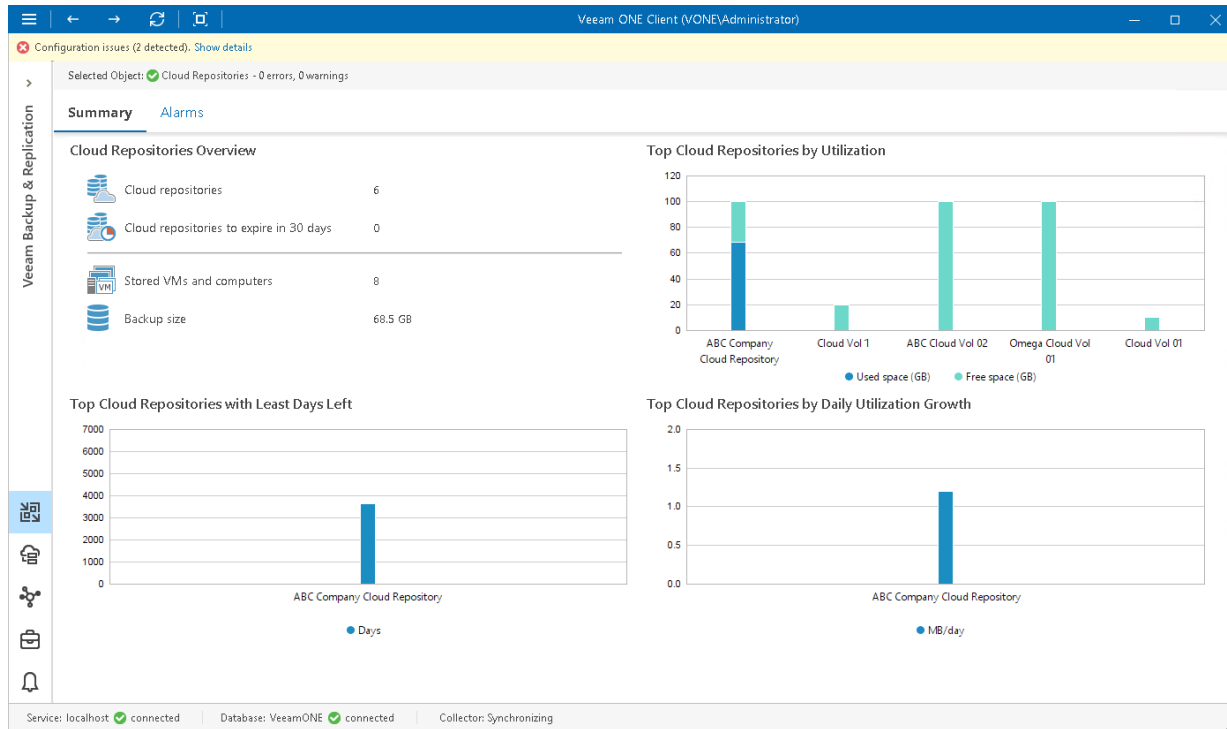
Cloud Repositories Overview

The section provides the following details:

- Number of cloud repositories created for Veeam Cloud Connect users

- Number of cloud repository leases that will expire within 30 days

- Number of VMs and computers whose data is stored in backups on cloud repositories

- Cumulative amount of storage space occupied by VM and computer backups on all managed cloud repositories

Top Cloud Repositories by Utilization

The chart shows 5 cloud repositories with the greatest amount of used storage space.

For every repository in the chart, you can see the amount of used storage space against the amount of available space. If free space on the repository is running low, you may need to increase the repository quota.

Top Cloud Repositories with Least Days Left

The chart shows 5 cloud repositories that can run low on storage space sooner than others. To draw the chart, Veeam ONE analyzes historical data and checks how fast free space on repositories has been decreasing in the past. Veeam ONE uses historical statistics to forecast how soon the repository will run out of space.

Top Cloud Repositories by Daily Utilization Growth

The chart allows you to detect how fast the amount of used space on repositories increased over the past 7 days. For every repository, the chart shows the daily disk space growth usage rate (the average increase in GB per day).

Cloud Repository Summary

The cloud repository summary dashboard provides overview details and space utilization analysis for the chosen cloud repository (repository allocated for a user by a Veeam Cloud Connect Service Provider).
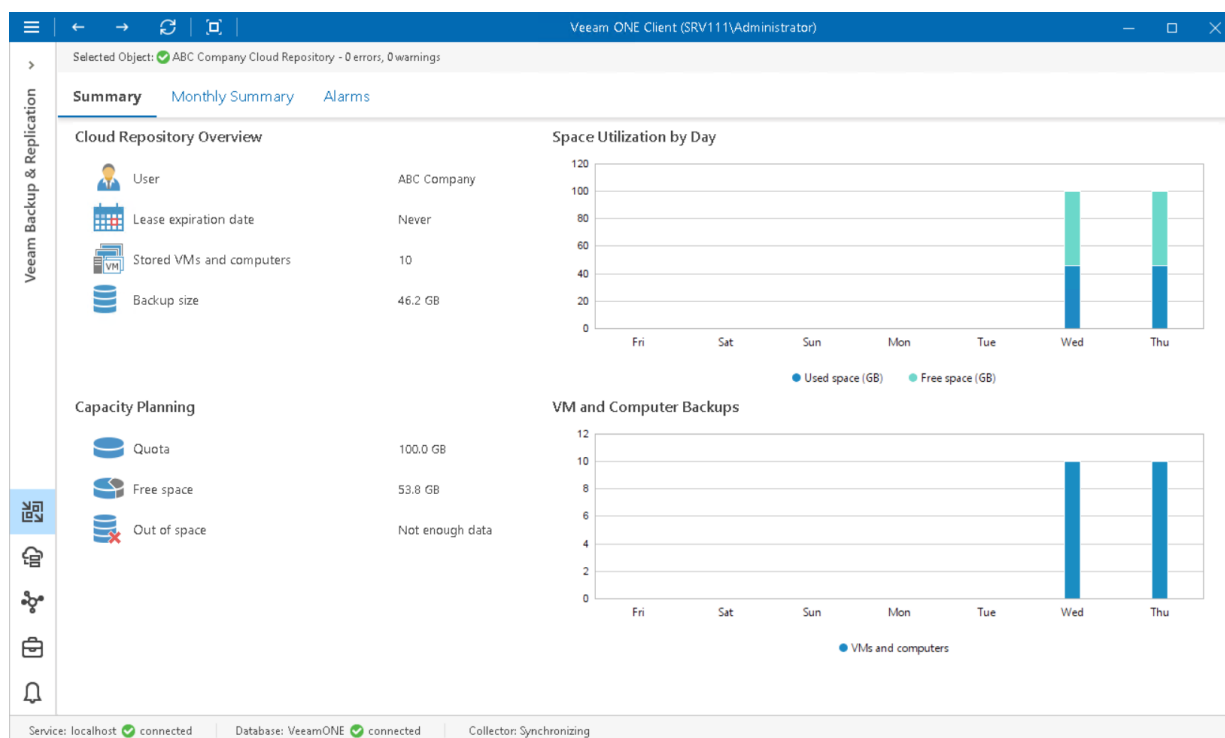
Cloud Repository Overview

The section provides the following details:

- Name of the user that owns the cloud repository

- Date when the repository lease is set to expire

- Number of VMs and computers whose data is stored in backups stored on the cloud repository

- Cumulative amount of storage space occupied by VM and computer backups on the cloud repository

Capacity Planning

The section outlines the following details:

- User quota, that is the amount of space allocated to a user

- Amount of free storage space on the cloud repository

- Number of days before the cloud repository runs out of free space

To forecast the value, Veeam ONE uses a trend that is calculated based on historical statistics — it analyzes how fast the amount of free space on the repository was decreasing in the past and uses historical statistics to forecast how soon the repository will run out of space.

Space Utilization by Day

The chart shows the amount of used storage space against the amount of available space on the cloud repository. If free space on the repository is running low, you may need to increase the repository quota.

VM and Computer Backups

The chart shows the number of VMs and computers whose backups were written to the repository during the past period.

Cloud Gateways Overview

The summary dashboard for the **Cloud Gateways** node presents a configuration overview and performance analysis for cloud gateways managed by a backup server.
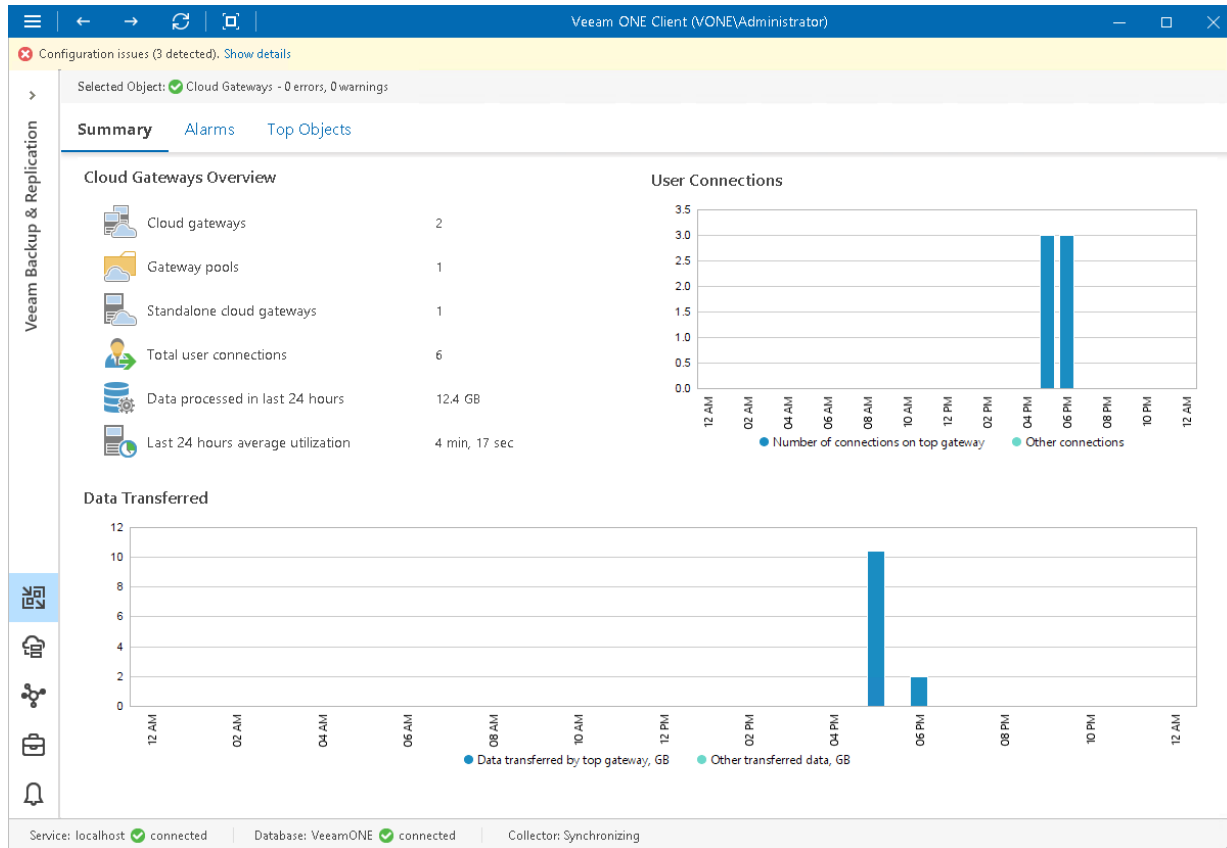
Cloud Gateways Overview

The section provides the following details:

- Number of cloud gateways managed by the backup server

- Number of gateway pools configured on the backup server

- Number of standalone cloud gateways configured on the backup server

- Number of connections to the gateways over the past 24 hours

- Amount of backup data that was transferred through all cloud gateways

- Average amount of time during which the gateways were utilized over the past 24 hours

User Connections

The chart shows the most loaded cloud gateways in terms of user connections. The chart shows the number of connections to the most utilized gateways, as well as connections to other gateways.

To draw the chart, Veeam ONE calculates how many connections were established to each cloud gateway over the past 24 hours.

Data Transferred

The chart shows the amount of data transferred by the most utilized gateways, as well as data transferred by other gateways.

The chart can help you detect cloud gateways that transfer the greatest amount of backup data and estimate the load on gateways.

Cloud Gateway Pool Summary

The cloud gateway pool summary dashboard provides overview information and performance analysis for the chosen gateway pool over the past day, week or month.
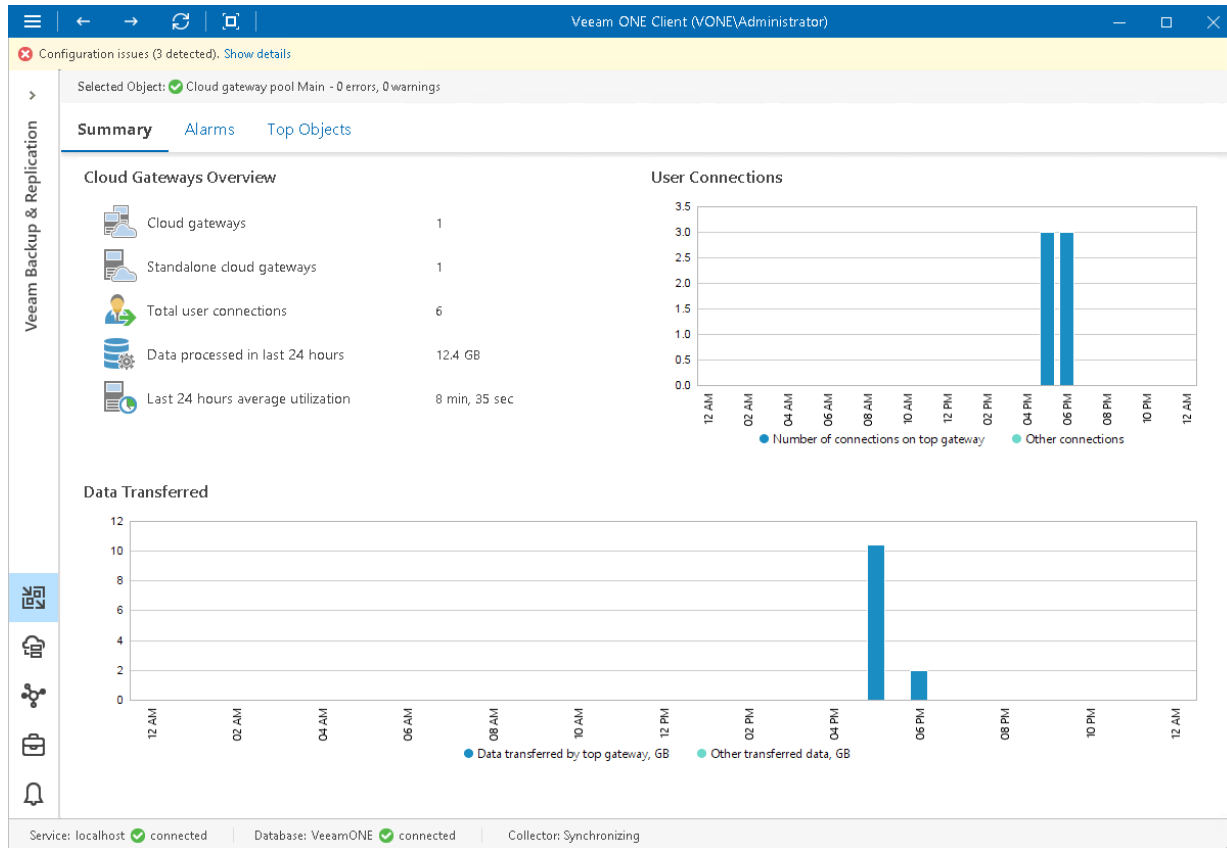
Cloud Gateways Overview

The section outlines the following details:

- Number of cloud gateways in a pool

- Number of users that connected to the gateways in the pool over the last 24 hours

- Amount of backup data that the cloud gateways in a pool processed over the last 24 hours

- Amount of time that the cloud gateways in the pool were retrieving, processing and transferring data

User Connections

The chart shows how many times the connection to the top cloud gateway and other gateways in a pool was established to transfer backup traffic over the past period.

Data Transferred

The chart shows the amount of backup data that the to the top cloud gateway and other gateways in a pool transferred to the cloud repository over the past period. The chart can help you measure the total amount of backup traffic coming through the cloud gateways in a pool.

Cloud Gateway Summary

The cloud gateway summary dashboard provides overview information and performance analysis for the chosen gateway over the past day, week or month.
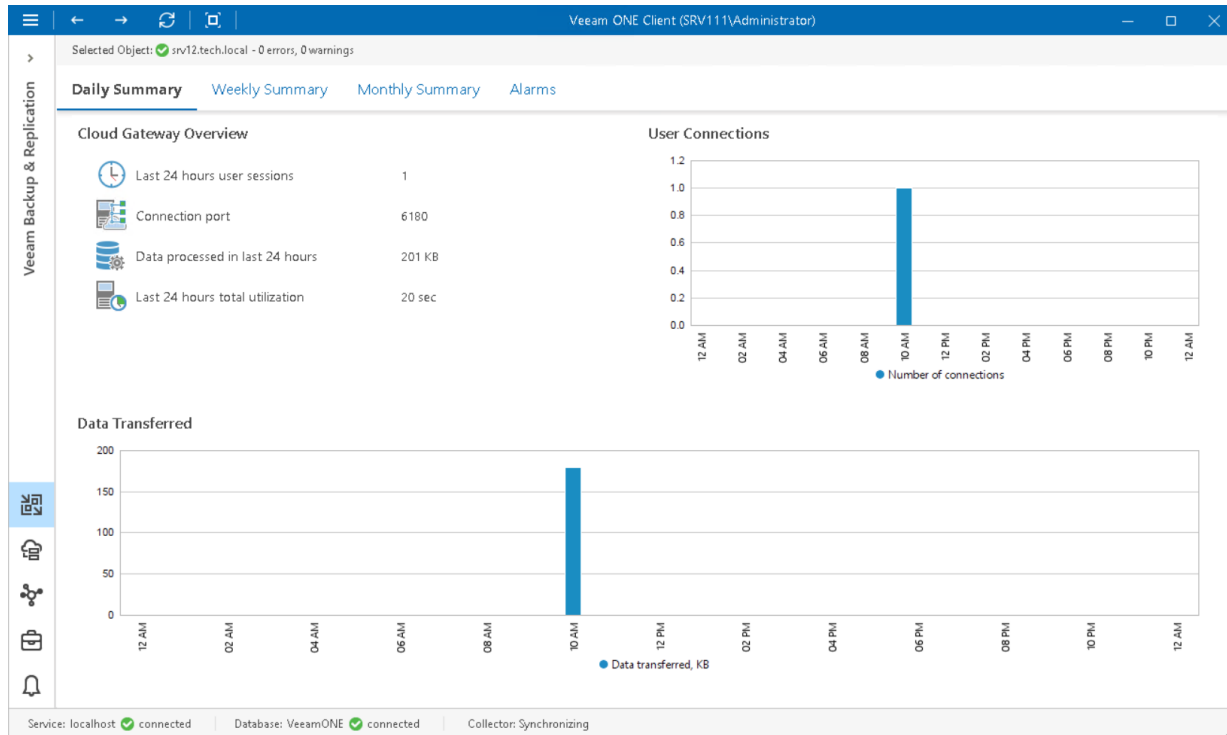
Cloud Gateway Overview

The section outlines the following details:

- Number of users that connected to the gateway over the past day, week or month

- Port configured for external connections on the cloud gateway

- Amount of backup data that the cloud gateway processed over the last 24 hours, 7 days or month

- Amount of time that the cloud gateway was retrieving, processing and transferring data

User Connections/Sessions

The chart shows how many times the connection to the cloud gateway was established to transfer backup traffic over the past period.

Data Transferred/Processed Data

The chart shows the amount of backup data that the cloud gateway transferred to the cloud repository over the past period. The chart can help you measure the total amount of backup traffic coming through the cloud gateway.

[Weekly/Monthly Summary] Utilization

The chart allows you to estimate how 'busy' the cloud gateway was during the past period. The chart shows the cumulative amount of time that the cloud gateway was retrieving, processing and transferring backup data.

The chart can help you reveal possible resource bottlenecks. If the utilization graph on the chart is abnormally large, this can evidence of high CPU load or insufficient throughput.

Veeam Backup & Replication Alarms

Veeam ONE includes a set of alarms monitor the efficiency of Veeam Backup & Replication data protection in the virtual environment.

Predefined data protection alarms are configured to warn you about events or issues that can cause loss of data or prevent Veeam Backup & Replication infrastructure from functioning properly:

- Connectivity issues and inability of backup infrastructure components to communicate with each other

- State of Veeam Backup & Replication software installed on backup infrastructure components

- Failing jobs or jobs finished with warnings

- Configuration issues, such as fast decreasing space on backup repositories or cloud repositories

- Long-running jobs that exceed the backup window

- Product license and prepaid support contract

To view the list of data protection alarms:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the necessary backup infrastructure node.

4. Open the **Alarms** tab.

On the **Alarms** dashboard, you can view triggered alarms, track alarm history, resolve and acknowledge alarms and perform other actions. For more information on available actions, see Working with Triggered Alarms.

Data Protection

Veeam ONE Client allows you to track jobs and policies configured to protect the following workloads:

- Virtual Machines

- Computers

- File Shares

- Databases

- Networks

By analyzing job details, you can reveal potential problems with the efficiency of data protection operations.

For example, if job duration has significantly increased in comparison with the average monthly duration value, while there are no noticeable changes to the amount of transferred data, you may need to investigate the root cause. Such a behavior may evidence that the job has to wait for proxy resources, which increases the backup window.

Virtual Machines

Veeam ONE Client allows you to track jobs and policies configured to protect on-premises virtual machines and cloud virtual machines and instances with Veeam Backup & Replication.

You can track real-time job and policy statistics at different levels of your backup infrastructure:

- Jobs on a specific backup server

- Jobs on all backup servers controlled by Veeam Backup Enterprise Manager

- All jobs across the entire backup infrastructure

Viewing VM Job Details

To view the list of VM jobs at the necessary backup infrastructure level:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the necessary backup infrastructure node.

4. Open the **Data Protection** tab and navigate to **Virtual Machines > On-premises**.

5. To find the necessary job, you can use filters at the top of the job list:

   o To show or hide jobs that ended with a specific status, use the status buttons at the top of the list (*Show all jobs*, *Show failed jobs*, *Show jobs with warnings*, *Show successful jobs*, *Show running jobs* or *Show jobs with no status*).

   o To show or hide jobs of a specific type, use the job type filter at the top of the list (*Backup*, *Replication*, *Backup copy*, *Backup to tape*, *CDP policy*, *VM copy*, *SureBackup*, *Microsoft SQL database transaction log backup*, *Oracle Database transaction log backup*, *PostgreSQL transaction log backup*, or *Snapshot-only*).

   o To show or hide jobs that protect VMs residing on a specific hypervisor, use the platform filter at the top of the list (*VMware vSphere*, *VMware Cloud Director*, *Microsoft Hyper-V*, *Nutanix AHV*).

   o To set the time interval when jobs ran for the last time, use the **Filter jobs by time period** button. Release the button to discard the time period filter.

   o To find jobs by name, use the search field at the top of the list.

The list of jobs shows all types of VM jobs for the backup infrastructure level that you selected in the inventory pane.

Each job in the list is described with a set of properties. To show or hide properties, right-click the list header and choose properties that must be displayed.

- **Job Status** — latest status of the job session (*Success*, *Warning*, *Failed*, *Running*, or jobs with no status).

- **Job Name** — name of the job.

- **Backup Server** — name of the backup server on which the job is configured. Click the server name link to drill down to the list of alarms for a chosen backup server.

- **Job Type** — type of the job (*Backup*, *Replication*, *Backup copy*, *Backup to tape*, *CDP policy*, *VM copy*, *SureBackup*, *Microsoft SQL database transaction log backup*, *Oracle Database transaction log backup*, *PostgreSQL transaction log backup*, or *Snapshot-only*).

- **Last Run** — date and time of the latest job run.

- **Duration** — time taken to complete the job during its latest run.

- **Avg. Duration (Last Month)** — average time taken to complete the job (total job duration time for the previous month divided by the number of times the job ran).

- **Transferred Data (GB)** — amount of backup data that was transferred to the target destination (backup repository or replication target datastore/volume) during the latest job run.

> **NOTE:**
>
> The "*No info*" label indicates that no information is available for the job because data has not been collected yet.

Viewing Cloud VM Job Details

To view the list of cloud VM policies and jobs at the necessary backup infrastructure level:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the necessary backup infrastructure node.

4. Open the **Data Protection** tab and navigate to **Virtual Machines > Cloud**.

5. To find the necessary job or policy, you can use filters at the top of the policies list:

   o To show or hide jobs and policies whose sessions ended with a specific status, use the status buttons at the top of the list (*Show all jobs*, *Show jobs with errors*, *Show jobs with warnings*, *Show successful jobs*).

   o To show or hide jobs and policies of a specific type, use the job type filter at the top of the list (*Backup policy*, *Backup copy*, *Backup to tape*).

   o To show or hide jobs and policies configured for a specific platform, use the platform type filter at the top of the list (*AWS*, *Microsoft Azure*, *Google Cloud Platform*).

   o To set the time interval when jobs and policies ran for the last time, use the **Filter jobs by time period** button. Release the button to discard the time period filter.

   o To find jobs and policies by name, use the search field at the top of the list.

The list of jobs shows all Veeam Backup for Microsoft Azure, Veeam Backup for AWS and Veeam Backup for Google Cloud Platform policies and jobs for the backup infrastructure level that you selected in the inventory pane.

Each job in the list is described with a set of properties. To show or hide properties, right-click the list header and choose properties that must be displayed.

- **Job State** — state of the cloud policy or job schedule (*Enabled*, *Disabled*).

  Click the > icon to show details of the last cloud protection sessions based on a specific policy.

- **Job Status** — latest status of the cloud policy or job session (*Success*, *Warning*, *Failed*, *Running*, or jobs with no status).

- **Job Name** — name of the cloud policy or job.

- **Platform** — name of the cloud platform for which the policy or job is configured.

- **Job Type** — backup job or policy type (*Backup policy*, *Backup copy*, *Backup to tape*).

- **Instance Type** — type of a protected instance.

- **Backup Server** — name of a backup server to which external repository with cloud backups is connected.

  Click the server name link to drill down to the list of alarms for a chosen backup server.

- **Instances Count** — number of Microsoft Azure VMs, AWS EC2 or Google Cloud instances processed during the last cloud protection session.

- **Last Snapshot** — date and time when the latest cloud-native snapshot was created for a Microsoft Azure VM, AWS EC2 or Google Cloud instance.

- **Last Backup** — date and time of the latest backup restore point was created for a Microsoft Azure VM, AWS EC2 or Google Cloud instance.

- **Last Replication** — date and time of the latest replication restore point was created for AWS EC2 instance.

- **Last Archive** — date and time of the latest archive restore point was created for a cloud instance.

- **Last Run** — date and time of the latest policy run.

- **Instance ID** — id of a Microsoft Azure VM, AWS EC2 or Google Cloud instance.

- **Duration** — time taken to complete the job during its latest run.

- **Avg. Duration (Last Month)** — average time taken to complete the job (total job duration time for the previous month divided by the number of times the job ran).

- **Transferred Data (GB)** — amount of backup data that was transferred to the target destination during the latest job run.

NOTE:

The "*No info*" label indicates that no information is available for the job because data has not been collected yet.

Computers

Veeam ONE Client allows you to track Veeam backup agent jobs and policies managed by Veeam Backup & Replication servers connected to Veeam ONE.

You can view real-time job statistics at different levels of your backup infrastructure:

- Jobs managed by a specific backup server

- Jobs managed by all backup servers controlled by Veeam Backup Enterprise Manager

- All jobs across the entire backup infrastructure

Viewing Job Details

To view the list of Veeam backup agent jobs and policies at the necessary backup infrastructure level:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the necessary backup infrastructure node.

4. Open the **Data Protection** tab and navigate to **Computers**.

5. To find the necessary job or policy, you can use filters at the top of the job list:

   o To show or hide jobs that ended with a specific status, use the status buttons at the top of the list (*Show all jobs*, *Show failed jobs*, *Show jobs with warnings*, *Show successful jobs*, *Show running jobs* or *Show jobs with no status*).

   o To show or hide jobs and policies by type, use the filters at the top of the list (*Agent backup*, *Agent backup policy*, *Backup copy*, *Backup to tape*, *SureBackup*, *Microsoft SQL transaction log backup*, *Oracle Database transaction log backup*, *PostgreSQL transaction log backup*).

   o To show or hide jobs and policies by platform of Veeam backup agent, use the filters at the top of the list (*Microsoft Windows*, *Linux*, *masOS*, *IBM AIX*, *Oracle Solaris*).

   o To set the time interval when jobs ran for the last time, use the **Filter jobs by time period** button. Release the button to discard the time period filter.

   o To find jobs and policies by name, use the search field at the top of the list.

The list of jobs shows all Veeam backup agent jobs and policies for the backup infrastructure level that you selected in the inventory pane.

Each job in the list is described with a set of properties. To show or hide properties, right-click the list header and choose properties that must be displayed.

- **Job Name** — name of the job or policy.

  Click the > icon to show details of agent job sessions based on a specific backup policy.

- **Job Status** — the latest status of the job or policy session (*Success*, *Warning*, *Failed*, *Running*, or jobs with no status).

- **Backup Server** — name of the backup server on which the job or policy is configured. Click the server name link to drill down to the list of alarms for a chosen backup server.

- **Job Type** — backup job type (*Agent backup*, *Agent backup policy*, *Backup copy*, *Backup to tape*, *SureBackup*, *Microsoft SQL transaction log backup*, *Oracle Database transaction log backup*, *PostgreSQL transaction log backup*).

- **Computer** — name of the computer for which the job or policy is configured.

- **Last Run** — date and time when the backup job was performed for the last time.

- **Duration** — time taken to complete the backup job during its latest run.

- **Computer Count** — number of computers included in the backup job.

- **IP Address** — IP addresses of computers to which the backup policy was applied.

- **Transferred Data (GB)** — amount of backup data that was transferred to the target destination during the latest job run.

- **Avg. Duration (Last Month)** — average time taken to complete the backup job (total job duration time for the previous month divided by the number of times the job ran).

NOTE:

The "*No info*" label indicates that no information is available for the job because data has not been collected yet.

File Shares

Veeam ONE Client allows you to track file backup, file backup copy, file to tape and file copy jobs configured to protect on-premises and cloud file shares.

You can track real-time job statistics at different levels of your backup infrastructure:

- Jobs managed by a specific backup server

- Jobs on all backup servers controlled by Veeam Backup Enterprise Manager

- All jobs across the entire backup infrastructure

Viewing File Share Job Details

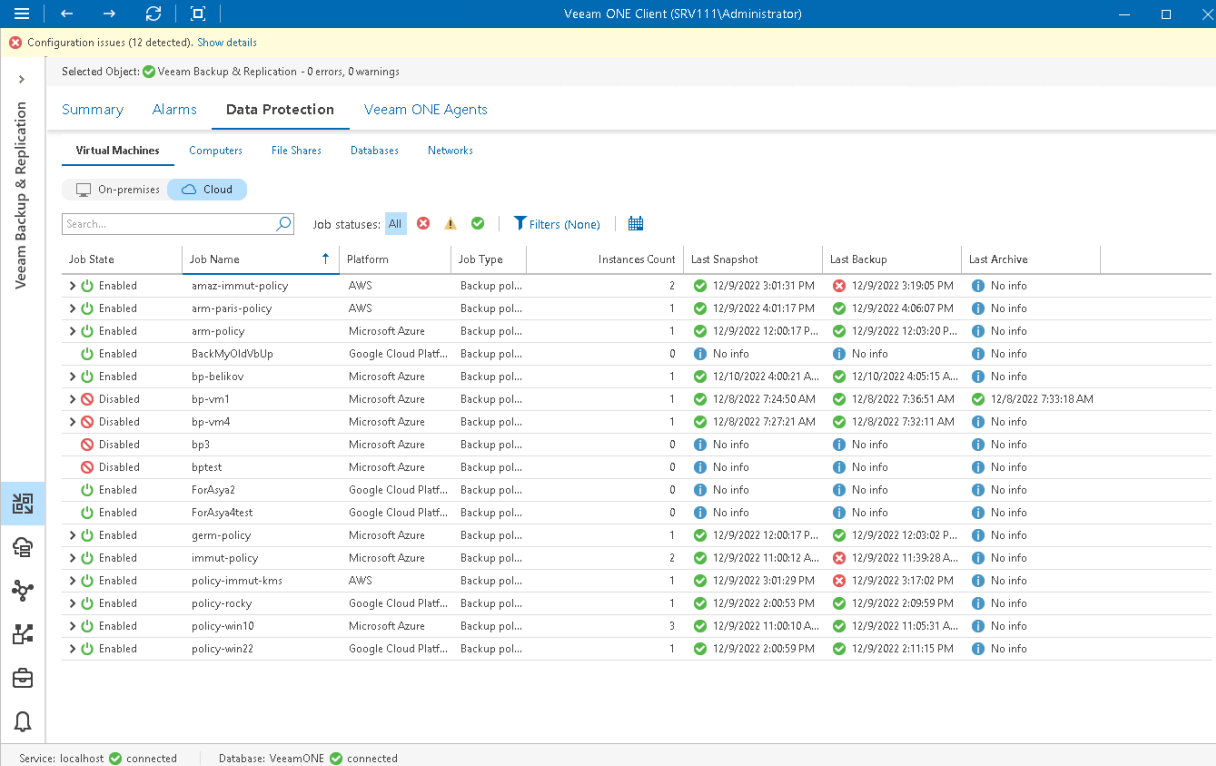To view the list of file jobs at the necessary backup infrastructure level:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the necessary backup infrastructure node.

4. Open the **Data Protection** tab and navigate to **File Shares > On-premises**.

5. To find the necessary job, you can use filters at the top of the job list:

   o To show or hide jobs that ended with a specific status, use the status buttons at the top of the list (*Show all jobs*, *Show failed jobs*, *Show jobs with warnings*, *Show successful jobs*, *Show running jobs* or *Show jobs with no status*).

   o To show or hide jobs of a specific type, use the job type filter at the top of the list (*File backup*, *Backup copy*, *Backup to tape*, *File to tape* or *File copy*).

   o To set the time interval when jobs ran for the last time, use the **Filter jobs by time period** button. Release the button to discard the time period filter.

   o To find jobs by name, use the search field at the top of the list.

The list of jobs shows all file backup, file backup copy, file to tape and file copy jobs for the backup infrastructure level that you selected in the inventory pane.

Each job in the list is described with a set of properties. To show or hide properties, right-click the list header and choose properties that must be displayed.

- **Job Status** — the latest status of the job session (*Success*, *Warning*, *Failed*, *Running*, or jobs with no status).

- **Job Name** — name of a file share job.

- **Backup Server** — name of a backup server on which the job is configured. Click the server name link to drill down to the list of alarms for the chosen backup server.

- **Job Type** — job type (*File backup*, *Backup copy*, *Backup to tape*, *File to tape* or *File copy*).

- **Last Run** — date and time of the latest job run.

- **Duration** — time taken to complete the job during its latest run.

- **Avg. Duration (Last Month)** — average time taken to complete the job (total job duration time for the previous month divided by the number of times the job ran).

- **Transferred Data (GB)** — amount of backup data that was transferred to the target destination (backup repository or tape) during the latest job run.

NOTE:

The "*No info*" label indicates that no information is available for the job because data has not been collected yet.

Viewing Cloud File Share Job Details

To view the list of file jobs at the necessary backup infrastructure level:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the necessary backup infrastructure node.

4. Open the **Data Protection** tab and navigate to **File Shares > Cloud**.

5. To find the necessary job, you can use filters at the top of the job list:

   o To show or hide jobs that ended with a specific status, use the status buttons at the top of the list (*Show all jobs*, *Show jobs with errors*, *Show jobs with warnings*, *Show successful jobs*).

   o To show or hide jobs for a specific platform, use the job type filter at the top of the list (*AWS* or *Microsoft Azure*).

   o To set the time interval when jobs ran for the last time, use the **Filter jobs by time period** button. Release the button to discard the time period filter.

   o To find jobs by name, use the search field at the top of the list.

The list of jobs shows all file backup policies for the backup infrastructure level that you selected in the inventory pane.

Each job in the list is described with a set of properties. To show or hide properties, right-click the list header and choose properties that must be displayed.

- **Job State** — the latest status of the job session (*Success*, *Warning*, *Failed*, *Running*, or jobs with no status).

- **Job Name** — name of the file share job.

- **Platform** — name of the cloud platform for which file job is configured.

- **Instance Type** — type of the protected instance.

- **Backup Server** — name of the backup server on which the job is configured. Click the server name link to drill down to the list of alarms for a chosen backup server.

- **Instances Count** — number of Microsoft Azure Files or AWS EFS instances processed during the last cloud protection session.

- **Last Snapshot** — date and time when the latest cloud-native snapshot was created for a Microsoft Azure Files or AWS EFS instance.

- **Last Backup** — date and time of the latest backup restore point was created for a Microsoft Azure Files or AWS EFS instance.

- **Last Backup Copy** — date and time of the latest backup copy restore point was created for a Microsoft Azure Files or AWS EFS instance.

- **Instance ID** — id of the Microsoft Azure Files or AWS EFS instance.

NOTE:

The "*No info*" label indicates that no information is available for the job because data has not been collected yet.

Databases

Veeam ONE Client allows you to track database jobs and policies configured to protect on-premises and cloud databases.

You can track real-time job statistics at different levels of your backup infrastructure:

- Jobs managed by a specific backup server

- Jobs on all backup servers controlled by Veeam Backup Enterprise Manager

- All jobs across the entire backup infrastructure

Viewing Database Job Details

To view the list of database protection jobs at the necessary backup infrastructure level:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the necessary backup infrastructure node.

4. Open the **Data Protection** tab and navigate to **Databases > On-premises**.

5. To find the necessary job, you can use filters at the top of the job list:

   o To show or hide jobs that ended with a specific status, use the status buttons at the top of the list (*Show all jobs*, *Show disabled jobs*, *Show failed jobs*, *Show jobs with warnings*, *Show successful jobs*, *Show running jobs* or *Show jobs with no status*).

   o To show or hide jobs of a specific type, use the job type filter at the top of the list (*Backup policy*, *Backup copy*, *Transaction log backup*).

   o To show or hide jobs for a specific platform, use the platform filter at the top of the list (*Oracle Database*, *SAP HANA*, *SAP on Oracle Database*)

   o To set the time interval when jobs ran for the last time, use the **Filter jobs by time period** button. Release the button to discard the time period filter.

   o To find jobs by name, use the search field at the top of the list.

The list of jobs shows all policies, backup copy and transaction log backup jobs for the backup infrastructure level that you selected in the inventory pane.
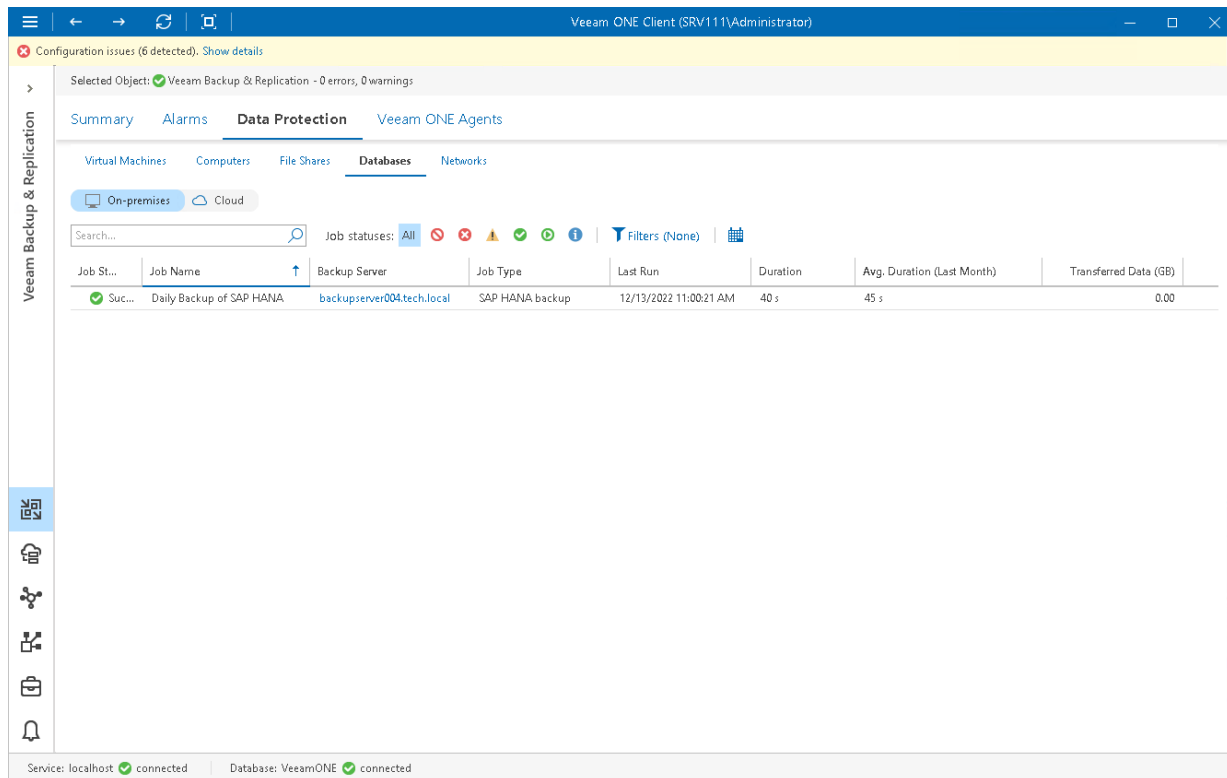
Each job in the list is described with a set of properties. To show or hide properties, right-click the list header and choose properties that must be displayed.

- **Job Status** — the latest status of the job session (*Success*, *Warning*, *Failed*, *Running*, or *jobs with no status*).

- **Job Name** — name of the database protection job.

- **Backup Server** — name of a backup server on which the job is configured. Click the server name link to drill down to the list of alarms for the chosen backup server.

- **Job Type** — type of the database protection job (*Backup policy*, *Backup copy*, *Transaction log backup*)

- **Last Run** — date and time of the latest job run.

- **Duration** — time taken to complete the job during its latest run.

- **Avg. Duration (Last Month)** — average time taken to complete the job (total job duration time for the previous month divided by the number of times the job ran).

- **Transferred Data (GB)** — amount of backup data that was transferred to the target destination during the latest job run.

NOTE:
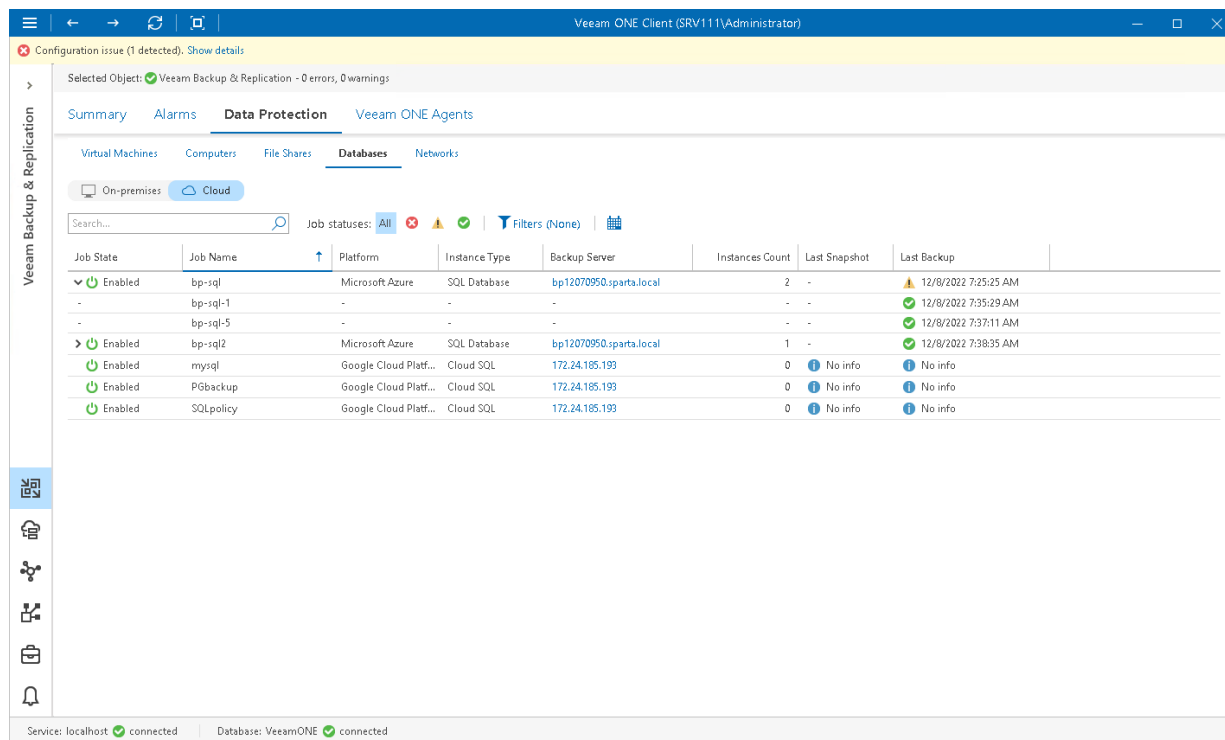
The "*No info*" label indicates that no information is available for the job because data has not been collected yet.

Viewing Cloud Database Job Details

To view the list of database protection jobs at the necessary backup infrastructure level:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the necessary backup infrastructure node.

4. Open the **Data Protection** tab and navigate to **Databases > Cloud**.

5. To find the necessary job, you can use filters at the top of the job list:

   o To show or hide jobs that ended with a specific status, use the status buttons at the top of the list (*Show all jobs*, *Show jobs with errors*, *Show jobs with warnings*, *Show successful jobs*).

   o To show or hide jobs for a specific platform, use the platform filter at the top of the list (*AWS*, *Microsoft Azure*, *Google Cloud Platform*)

   o To set the time interval when jobs ran for the last time, use the **Filter jobs by time period** button. Release the button to discard the time period filter.

   o To find jobs by name, use the search field at the top of the list.

The list of jobs shows all database protection jobs for the backup infrastructure level that you selected in the inventory pane.

Each job in the list is described with a set of properties. To show or hide properties, right-click the list header and choose properties that must be displayed.

- **Job State** — state of the Microsoft Azure SQL Database, AWS RDS or Google Cloud SQL policy schedule (*Enabled*, *Disabled*).

  Click the > icon to show details of the last cloud protection sessions based on a specific policy.

- **Job Name** — name of the Microsoft Azure SQL Database, AWS RDS or Google Cloud SQL policy.

- **Platform** — name of the cloud platform for which policy is configured.

- **Instance Type** — type of the protected instance.

- **Backup Server** — name of a backup server to which external repository with cloud backups is connected.

  Click the server name link to drill down to the list of alarms for a chosen backup server.

- **Instances Count** — number of Microsoft Azure SQL Database, AWS RDS or Google Cloud SQL instances processed during the last cloud protection session.

- **Last Snapshot** — date and time when the latest cloud-native snapshot was created for the AWS RDS or Google Cloud SQL instance.

- **Last Backup** — date and time of the latest backup restore point was created for the Microsoft Azure SQL Database or Google Cloud SQL instance.

- **Last Replication** — date and time of the latest replication restore point was created for the AWS RDS instance.

- **Last Archive** — date and time of the latest archive restore point was created for the Microsoft Azure SQL Database or Google Cloud SQL instance.

- **Instance ID** — id of the Microsoft Azure SQL Database, AWS RDS or Google Cloud SQL instance.

NOTE:

The "*No info*" label indicates that no information is available for the job because data has not been collected yet.

Networks

Veeam ONE Client allows you to track AWS policies configured to protect cloud networks.

You can track real-time job statistics at different levels of your backup infrastructure:

- Jobs managed by a specific backup server

- Jobs on all backup servers controlled by Veeam Backup Enterprise Manager

- All jobs across the entire backup infrastructure

To view the list of network protection policies at the necessary backup infrastructure level:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the necessary backup infrastructure node.

4. Open the **Data Protection** tab and navigate to **Networks**.

5. To find the necessary job, you can use filters at the top of the job list:

   o To show or hide jobs that ended with a specific status, use the status buttons at the top of the list (*Show all policies*, *Show policies with errors*, *Show policies with warnings*, *Show successful policies*).

   o To set the time interval when jobs ran for the last time, use the **Filter jobs by time period** button. Release the button to discard the time period filter.

   o To find jobs by name, use the search field at the top of the list.

The list of jobs shows all policies for the backup infrastructure level that you selected in the inventory pane.
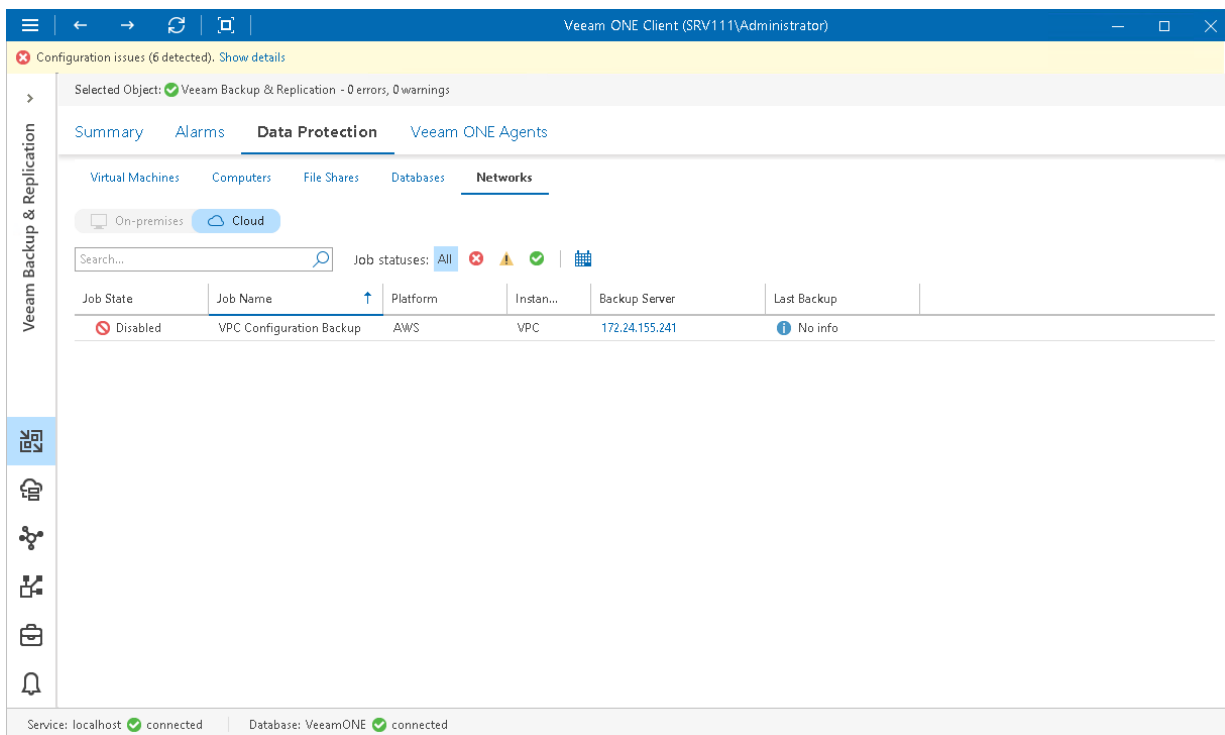
Each job in the list is described with a set of properties. To show or hide properties, right-click the list header and choose properties that must be displayed.

- **Job State** — state of the cloud policy schedule (*Enabled*, *Disabled*).

  Click the > icon to show details of the last cloud protection sessions based on a specific policy.

- **Job Name** — name of the cloud backup policy.

- **Platform** — name of the cloud platform for which policy is configured.

- **Instance Type** — type of the protected instance.

- **Backup Server** — name of the backup server to which external repository with cloud backups is connected.

  Click the server name link to drill down to the list of alarms for a chosen backup server.

- **Last Backup** — date and time when the latest backup restore point was created for a cloud instance.

NOTE:

The "*No info*" label indicates that no information is available for the job because data has not been collected yet.
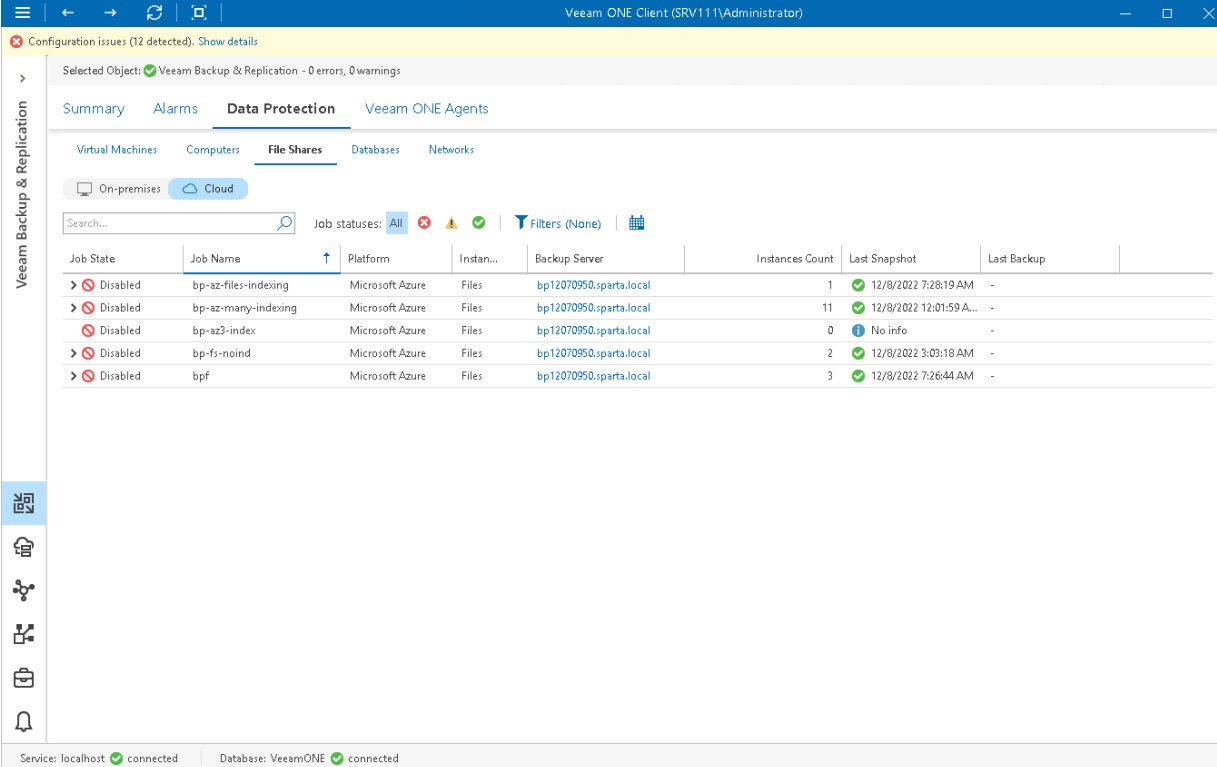
Veeam ONE Agents

You can monitor the state of Veeam ONE agents installed on the Veeam Backup & Replication servers that are connected to Veeam ONE.

Viewing Veeam ONE Agent Details

To view the list of Veeam ONE agents installed in the backup infrastructure:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the **Veeam Backup & Replication** node.

4. Open the **Veeam ONE Agents** tab.

The list of agents shows all Veeam ONE agents installed on connected Veeam Backup & Replication servers.

For every agent, the following details are available:

- **Backup Server** — name of a Veeam Backup & Replication server connected to Veeam ONE.

- **Agent Status** — the latest status of Veeam ONE agent connection.

- **Remediation Actions** — displays if remediation actions for alarms are enabled for a Veeam Backup & Replication server.

- **Log Analysis** — displays if log analysis is enabled for a Veeam Backup & Replication server.

- **Log Analysis Start Time** — scheduled time to start log analysis session.

- **Log Analysis Session State** — state of the latest log analysis session.

  Click a link in this column to see log analysis session history details.

- **Port Number** — port number used for communication with Veeam ONE agent installed on the Veeam Backup & Replication server.

Veeam Backup & Replication Performance Charts

To identify performance bottlenecks within the backup data flow, you can drill down to the following performance charts:

- CPU Performance Chart

- Memory Performance Chart

- Disk Performance Chart

- Network Performance Chart

- Cache Performance Chart

To draw the charts, Veeam ONE gathers Windows Performance Monitor metrics from the guest OS of backup infrastructure components (for this reason, performance charts for Linux-based repositories are not available). You can track performance metrics for physical and virtual backup servers, proxies, repositories, WAN accelerators or Enterprise Manager servers.

To drill down to a performance chart for a backup infrastructure component:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. Select the necessary backup infrastructure component.

4. Open the necessary performance chart tab.

For performance charts in the **Veeam Backup & Replication**, you can change chart views and set time intervals, define objects to show on charts or select custom metrics.

CPU Performance Chart

The **CPU** chart shows the amount of used processor resources on a machine where a backup infrastructure component runs. Graphs in the **CPU** chart illustrate the level of processor usage for every separate CPU on the machine. The **Total** graph shows the cumulative processor utilization for all CPUs.

Memory Performance Chart

The **Memory** chart shows the amount of used memory resources on a machine where a backup infrastructure component runs. Graphs in the **Memory** chart illustrate the amount of total available memory and memory that is currently used on the machine.

Disk Performance Chart

The **Disk** chart shows the rate at which the disk is transferring data during read and write operations. Disk usage is shown as an average for all physical disks on a machine where a backup infrastructure component runs.

Network Performance Chart

The **Network** chart shows the throughput for NICs on a machine where a backup infrastructure component runs. Graphs in the **Network** chart illustrate the rate at which data is sent on the network interface for each separate NIC. A separate graph shows the cumulative rate for all NICs on the machine.

Cache Performance Chart

The **Cache** chart shows the amount of space consumed by the data processed during CDP operations. Graphs in the chart display how much data is stored in the cache folder on the machine where CDP Proxy component runs and the percentage of allocated cache space consumed by this data.
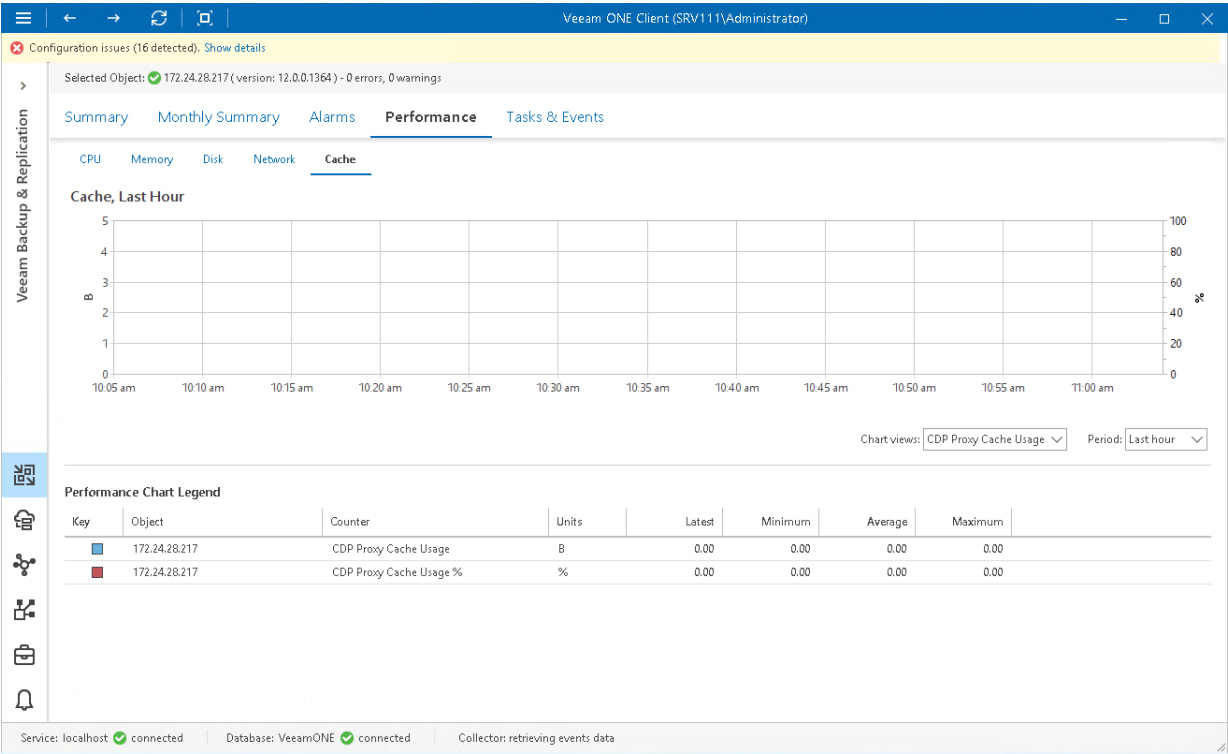
Data Transfer

The **Data Transfer** dashboard provides detailed information on data transfer sessions for the chosen scale-out backup repository and helps to monitor the amount of data transferred between the repository extents.

To view data transfer details for a specific repository:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the necessary scale-out backup repository.

4. Open the **Data Transfer** tab.
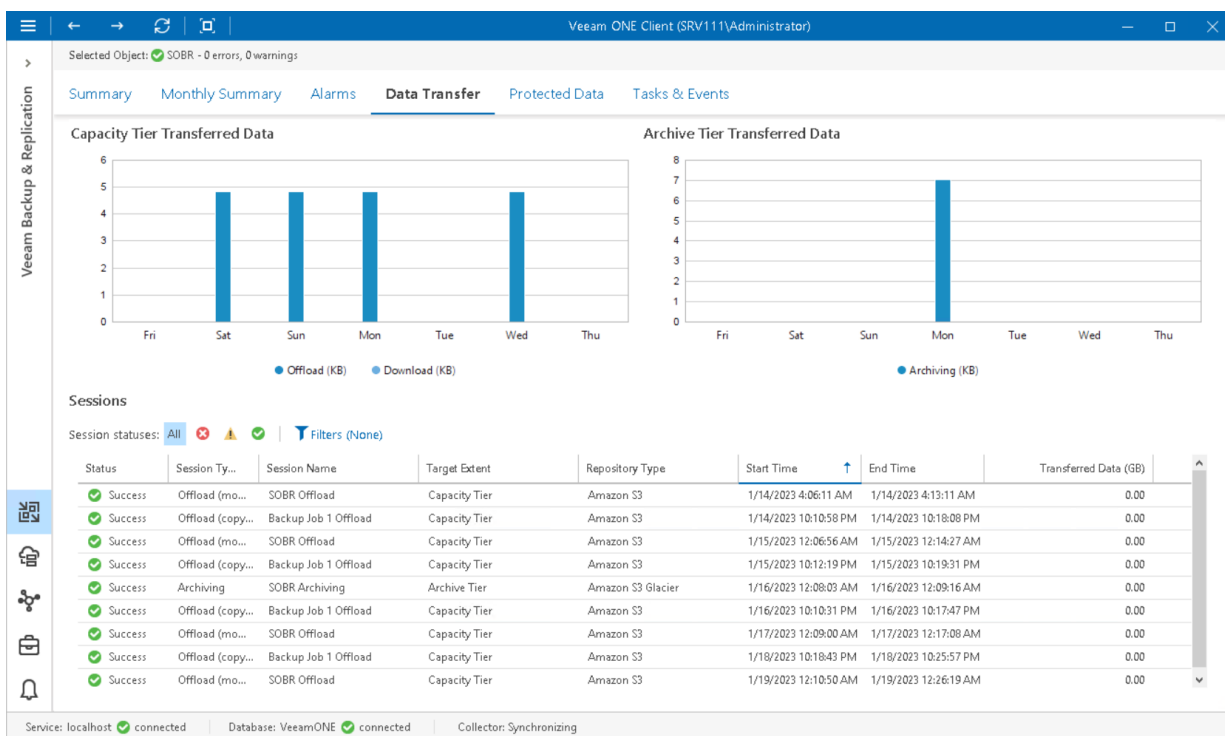
Capacity Tier Transferred Data

The chart shows the amount of data transferred during capacity tier offload and download sessions.

Archive Tier Transferred Data

The chart shows the amount of data transferred during archive tier data transfer sessions.

Sessions

The list of sessions shows all types of data transfer sessions for the scale-out backup repository that you selected in the inventory pane. Each session in the list is described with a set of properties. To show or hide properties, right-click the list header and choose properties that must be displayed. To quickly find the necessary session, use the session status and session type filters at the top of the list.

- **Status** — latest status of the data transfer session (*Success*, *Warning*, *Failed*).

- **Session Type** — type of the data transfer session (*Offload (copy policy)*, *Offload (move policy)*, *Download*, *Archiving*, *Retrieval*).

- **Session Name** — name of the data transfer session.

- **Target Extent** — type of extent to which data transfer session is targeted (*Archive Tier*, *Capacity Tier*).

- **Repository Type** — type of the object storage repository used as the scale-out backup repository tier.

- **Start Time** — date and time when the data transfer session started.

- **End Time** — date and time when the data transfer session completed.

- **Transferred Data (GB)** — amount of data transferred between the tiers during the session.

Protected Data
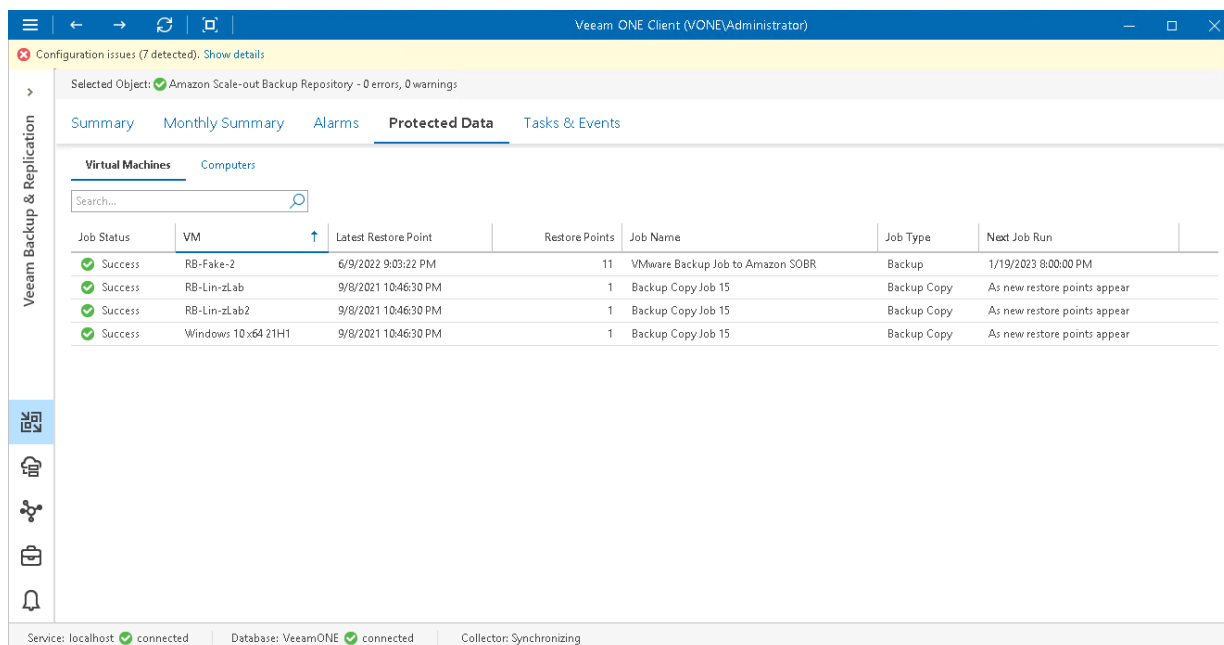
The **Protected Data** tab allows you to view backups on repositories for the following workloads:

- Virtual Machines
- Computers
- File Shares

Virtual Machines

To view the list of VMs stored in backups on repositories:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the necessary repository.

4. Open the **Protected Data** tab and navigate to **Virtual Machines**.

5. To quickly find VMs by name, use the **Search** field at the top of the list.

For every VM in the list, the following details are shown:

- **Job Status** — the latest status of the job that created the VM backup (*Success*, *Warning*, *Failed* or *Running*).

- **VM** — name of the VM stored in a backup on the repository.

- **Latest Restore Point** — date and time when the latest restore point was created for the VM.

- **Restore Points** — number of restore points created for the VM.

- **Job Name** — name of a backup or backup copy job that created VM backup.

- **Job Type** — type of the job that created the VM backup (*Backup job* or *Copy job*).

- **Next Job Run** — schedule according to which the job will start next time.

You can click column names to sort VMs by a specific parameter. For example, to view what VMs do not have recent backups, you can sort VMs in the list by **Latest Restore Point**.

Computers

To view the list of computers stored in backups on repositories:

1. Open Veeam ONE Client.

    For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the necessary repository.

4. Open the **Protected Data** tab and navigate to **Computers**.

5. To quickly find computers by name, use the filters and **Search** field at the top of the list.
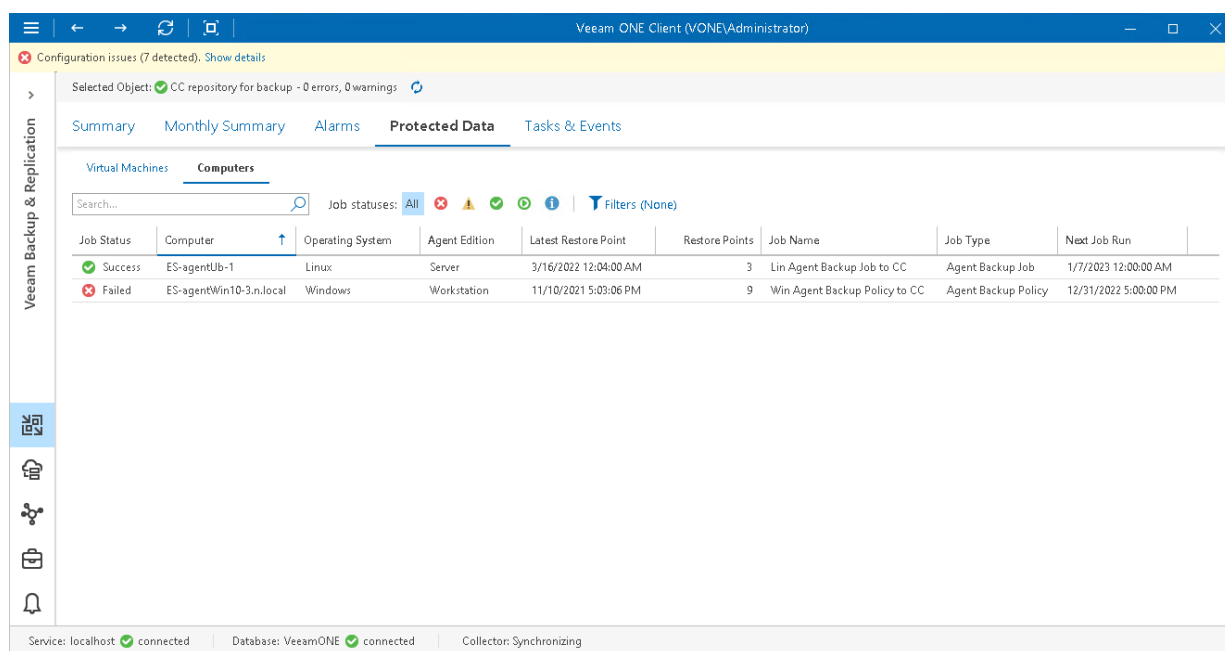
For every computer in the list, the following details are shown:

*   **Job Status** — the latest status of the job session that created the computer backup (*Success*, *Warning*, *Failed* or *Running*).

*   **Computer** — name of the computer stored in a backup on the repository.

*   **Operating System** — type of computer operating system (*Windows*, *Linux*, *Mac*, *AIX*, *Solaris*).

*   **Agent Edition** — mode in which the backup agent job or policy operates (*Server*, *Workstation*, *Free*).

*   **Latest Restore Point** — date and time when the latest restore point was created for the computer.

*   **Restore Points** — number of restore points created for the computer.

*   **Job Name** — name of the backup policy, backup or backup copy job that created computer backup.

*   **Job Type** — type of the job that created the VM backup (*Agent Backup Policy*, *Agent Backup Job*, *Backup Copy*).

*   **Next Job Run** — schedule according to which the job or policy will start next time.

You can click column names to sort computers by a specific parameter. For example, to view what computers do not have recent backups, you can sort computers in the list by **Latest Restore Point**.

File Shares

To view the list of source file shares stored in backups on repositories:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the necessary repository.

4. Open the **Protected Data** tab and navigate to **File Shares**.

5. To quickly find file shares by name, use the **Search** field at the top of the list.
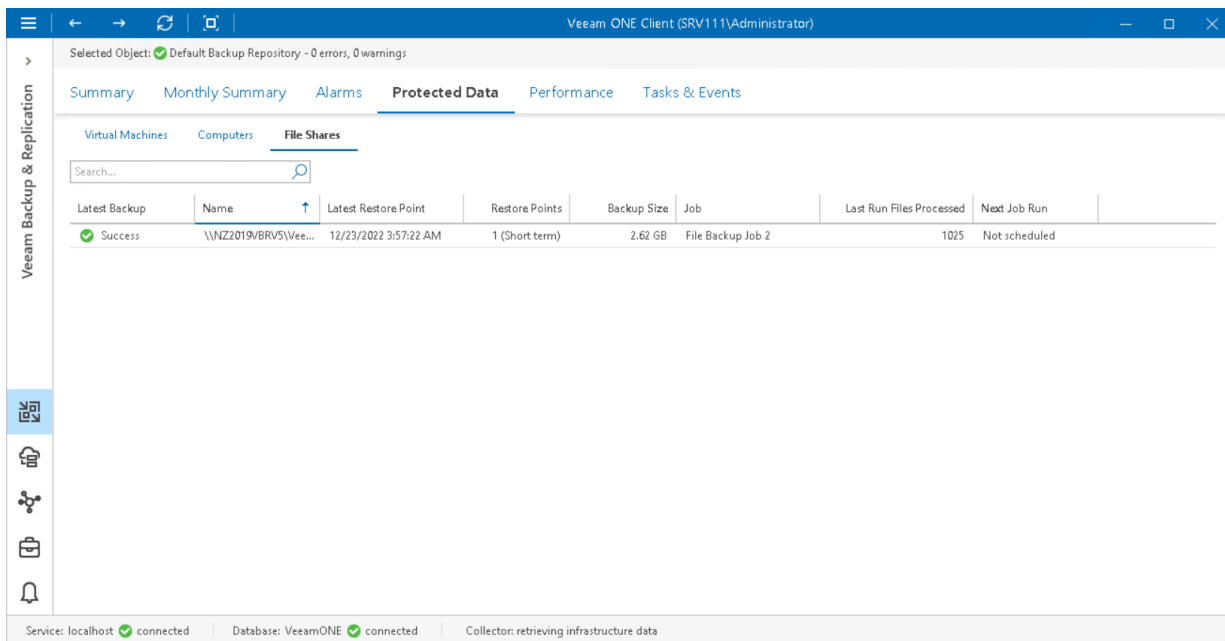
For every file share in the list, the following details are shown:

- **Latest Backup** — the latest status of the job that created the file share backup (*Success*, *Warning*, *Failed* or *Running*).

- **Name** — name of the file share stored in a backup on the repository.

- **Latest Restore Point** — date and time when the latest restore point was created for the file share.

- **Restore Points** — number of short term and long term restore points stored on the repository.

- **Backup Size** — total size of file backups on the repository.

- **Job** — name of the backup or backup copy job that created file share backup.

- **Last Run Files Processed** — number of files processed during the last file backup job session.

- **Next Job Run** — schedule according to which the job will start next time.

You can click column names to sort file shares by a specific parameter. For example, to view what file shares do not have recent backups, you can sort file shares in the list by **Latest Restore Point**.

Veeam Backup & Replication Events

The **Tasks & Events** dashboard shows the history of events that triggered Veeam Backup & Replication alarms. For the list and detailed description of data protection alarms, see section Veeam Backup & Replication Alarms of the Veeam ONE Working with Alarms Guide.

To view the list of events for a specific level:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the necessary backup infrastructure node.

4. Open the **Tasks & Events** tab.

5. The **Tasks & Events** list can display up to 1000 tasks and events at a time. To find the necessary task or event, you can use the following controls:

   o To display tasks or events for a specific period, select the necessary time interval from the **Events from** list.

   o To show or hide tasks or events, use filter buttons at the top of the list — *Show all events*, *Show errors*, *Show warnings*, *Show info messages*, *Show user events*, *Show tasks*.

   o To find the necessary tasks or events by description, use the **Search** field at the top of the list.

6. To view the detailed description of an event, click it in the list.

   The event description will be shown in the **Event Details** pane at the bottom.

   When you choose a virtual infrastructure container in the inventory pane, you can view events for the selected object and events for its child objects. To hide events related to child objects, clear the **Include events from child objects** check box at the bottom of the **Event Details** section.

7. To export displayed events to a CSV file, click **Export to CSV** at the top of the list and specify the location where the file will be saved.

Top Cloud Tenants

The **Top Objects** dashboard helps you detect top Veeam Cloud Connect users.

The dashboard displays top users in terms of transmitted data, used cloud storage space, number of connections, amount of gateway utilization time, traffic savings, peak transmission rate, number of failovers, number of replicated VMs and so on. By default, the dashboard displays top 3 user accounts ranged by consumed cloud repository space. You can change the number of displayed used accounts in the dashboard settings:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, select the necessary backup server.

4. Open the **Top Objects** tab.

5. Click the **Change Options** link in the top left corner of the dashboard and select the necessary number of tenants to display.

6. Click **OK**.

Top Cloud Gateways

The **Top Objects** dashboard provides performance data of the most utilized cloud gateways for the selected server or gateway pool over the last week. The dashboard shows the most 'busy' cloud gateways for the last 7 days in terms of:

- Amount of data transferred to cloud repositories

- Number unique users connected to each cloud gateway

- Maximum number of user connections to the gateway

- Total amount of time the gateway was utilized

To view the list of the most loaded cloud gateways:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Monitor.

2. At the bottom of the inventory pane, click **Veeam Backup & Replication**.

3. In the inventory pane, expand select the necessary node:

   o To view the most utilized standalone gateways, select the **Cloud Gateways** node under the necessary backup server.

   o To view the most utilized gateways from a gateway pool, select the necessary gateway pool under the **Cloud Gateways** node.

4. Open the **Top Objects** tab.

Veeam Backup for Microsoft 365 Monitoring

Veeam ONE Client offers advanced functionality for monitoring Veeam Backup for Microsoft 365 infrastructure and data protection operations in the managed virtual environment.

With Veeam ONE Client, you can:

1. **Monitor the overall state of the backup infrastructure**.

   Check the **Summary** dashboards to reveal hotspots in the Veeam Backup for Microsoft 365 infrastructure.

   Quickly review the latest status of data protection jobs, examine configuration and performance of your backup infrastructure components, detect the most loaded proxies and repositories and check whether your jobs complete within the backup window.

   Summary dashboards help you quickly reveal issues that can lead to job failure, and cause loss of valuable data.

2. **View triggered alarms**.

   Go to the **Alarms** dashboard to see details on issues and problems in your backup infrastructure.

   Data protection alarms allow you to instantaneously react to potentially dangerous situations with ongoing data protection and take immediate actions to eliminate the risk of data loss.

3. **Check the latest job status**.

   Track the status of your backup jobs.

   Get up-to-date information on the efficiency of data protection in your virtual environment and address problems with jobs as soon as they appear.

4. **Work with performance charts**.

   Drill down to performance charts to diagnose performance problems with backup infrastructure components and identify bottlenecks.

   Track CPU, memory, disk and network performance for Veeam Backup for Microsoft 365 servers and proxies to make sure the backup data flow is efficient, and all resources engaged in the backup process are optimally used.

5. **View the list of events**.

   View the full list of events that triggered Veeam Backup for Microsoft 365 alarms, and events notifying about connection problems with Veeam Backup for Microsoft 365 servers.

Prerequisites

Before you start monitoring the Veeam Backup for Microsoft 365 infrastructure, make sure you have configured connections to Veeam Backup for Microsoft 365 servers from which Veeam ONE will collect data. For more information on configuring server connections, see section Connecting Veeam Backup for Microsoft 365 Servers of the Veeam ONE Deployment Guide.

> **NOTE:**
>
> Veeam ONE monitors cloud Organizations protection only, monitoring of hybrid and on-premise (Exchange) platform protection is not supported.

In This Section

- Veeam Backup for Microsoft 365 Summary Dashboards

- Veeam Backup for Microsoft 365 Alarms

- Veeam Backup for Microsoft 365 Data Protection

- Veeam Backup for Microsoft 365 Performance Charts

- Veeam Backup for Microsoft 365 Protected Data

- Veeam Backup for Microsoft 365 Events

Veeam Backup for Microsoft 365 Summary Dashboards

Veeam Backup & Replication summary dashboards serve as the 'launch point' for monitoring the backup infrastructure and data protection operations. The dashboards reflect the latest state of backup jobs, and help you analyze the performance and configuration of backup infrastructure components.

Veeam ONE Client offers the following types of summary dashboards for Veeam Backup & Replication infrastructure components:

- Veeam Backup for Microsoft 365 Infrastructure Summary

- Veeam Backup for Microsoft 365 Repositories Overview

- Veeam Backup for Microsoft 365 Repository Summary

- Veeam Backup for Microsoft 365 Proxies Overview

- Veeam Backup for Microsoft 365 Proxy Summary

Veeam Backup for Microsoft 365 Infrastructure Summary

The Veeam Backup for Microsoft 365 infrastructure summary dashboard shows the latest state of data protection operations and indicates the most intensively used resources in the infrastructure.

The dashboard is available for the following nodes:

- Veeam Backup for Microsoft 365 Infrastructure

- Veeam Backup for Microsoft 365 server
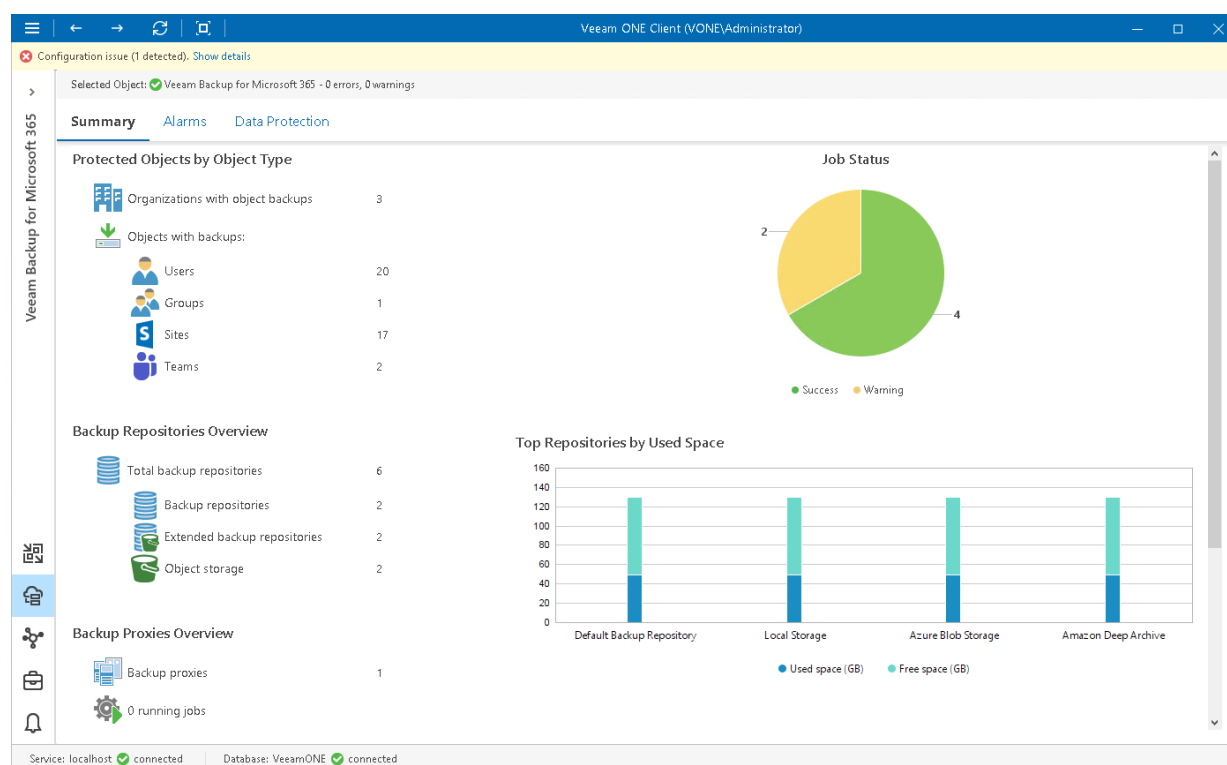
Protected Objects by Object Type

The section provides the following details:

- Number of organizations with object backups

- Number of objects (*Users*, *Groups*, *Sites*, *Teams*) with backups

Job Status

The charts reflect the latest status of Veeam Backup for Microsoft 365 protection jobs for the selected level of the infrastructure hierarchy.

Every chart segment shows how many jobs ended with a specific status — failed jobs (red), jobs that ended with warnings (yellow), successfully performed jobs (green), and jobs that are currently running (blue). Click the necessary chart segment or a legend label to drill down to the list of jobs that ended up with the corresponding status.

Backup Repositories Overview

The section provides the following details:

- Total number of backup repositories for the selected infrastructure node

- Number of repositories extended with an object storage

- Number of object storage repositories

Backup Proxies Overview

The section provides the following details:

- Number of proxies for the selected infrastructure node

- Number of jobs that the proxies are currently processing

- Number of jobs queued for processing

Top Repositories by Used Space

The chart shows 5 backup repositories with the greatest amount of used storage space.

For every repository in the chart, you can track the amount of used storage space against the amount of available space. If free space on the repository is running low, you may need to free up storage space, revise your backup retention policy or even move your backups from the repository and point backup jobs to a new location.

Top Backup Proxies by Weekly Transferred Data

The chart shows 5 backup proxies that processed the greatest amount of data over the past 7 days.

To draw the chart, Veeam ONE analyzes how many object processing tasks were successfully performed by every proxy; failed tasks are not taken into account.

The chart helps you detect the most heavily loaded proxies and optimize the performance of your backup infrastructure. If specific proxies are overloaded with processing tasks, and the jobs often need to wait for proxy resources, you may need to deploy additional proxies or balance the processing load by assigning jobs to other proxies.

Veeam Backup for Microsoft 365 Repositories Overview

The summary dashboard for the **Repositories** node provides a configuration overview and performance analysis for backup repositories and object storage extents managed by Veeam Backup for Microsoft 365 server.

Backup Repositories
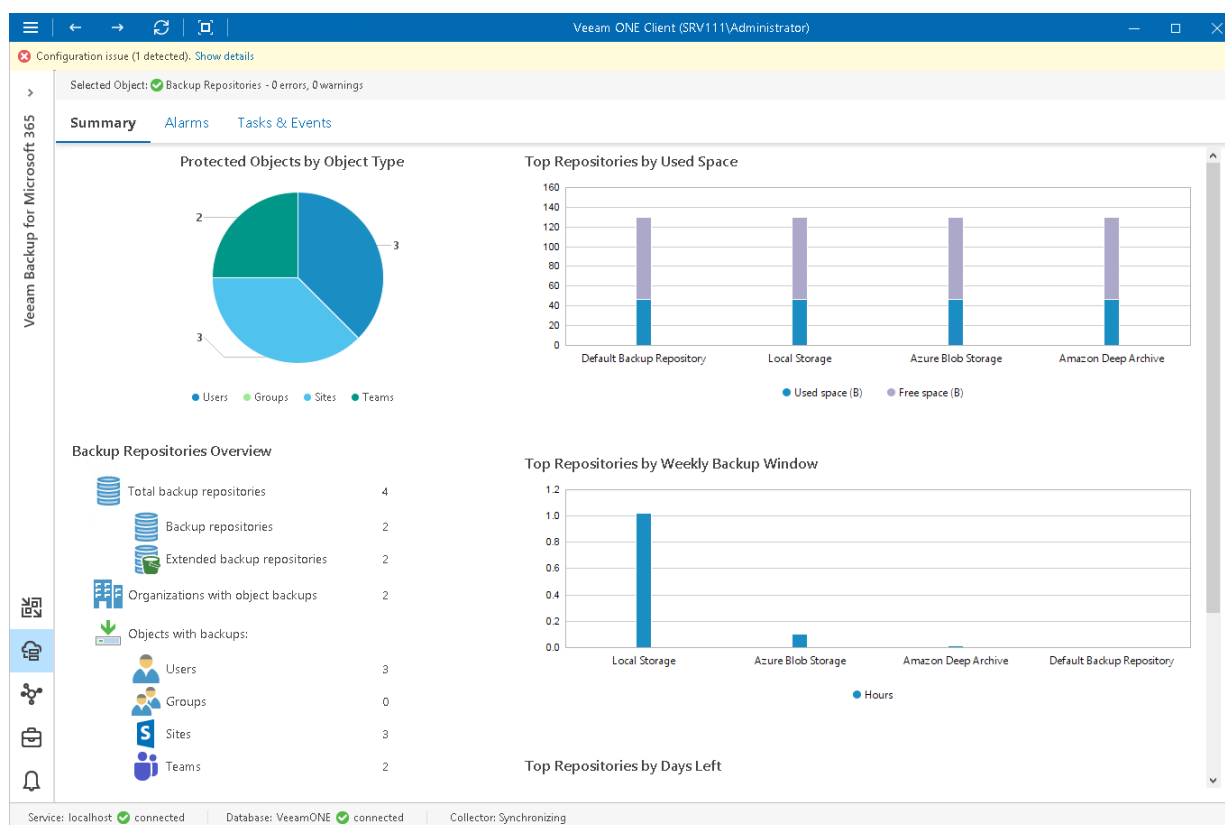
Protected Objects by Object Type

The chart displays types of objects protected with Veeam Backup for Microsoft 365 jobs and policies.

Every chart segment shows the number of objects of a specific type — the number of protected Users, Groups, Sites or Teams.

Backup Repositories Overview

The section provides the following details:

- Total number of repositories managed by Veeam Backup for Microsoft 365 server

- Number of backup repositories and repositories extended with object storage

- Number of organizations with object backups that reside on backup repositories

- Number of Users, Groups, Sites and Teams backups that reside on backup repositories

Top Repositories by Used Space

The chart shows backup repositories with the greatest amount of used storage space.

For every repository in the chart, you can see the amount of storage space used by Microsoft 365 object backups against the amount of available space. If free space on the repository is running low, you may need to free up storage space on the repository or revise your backup retention policy.

Top Repositories by Weekly Backup Window

The chart allows you to detect the most 'busy' repositories over the past 7 days.

For every repository, the chart shows the cumulative amount of time that the repository was busy with backup job tasks.

Top Repositories by Days Left

The chart shows backup repositories that can run low on storage space sooner than others.

To draw the chart, Veeam ONE analyzes historical data and checks how fast free space on repositories has been decreasing in the past. Veeam ONE uses historical statistics to forecast how soon the repository will run out of space.

Object Storage

Protected Objects by Object Type

The chart displays types of objects protected with Veeam Backup for Microsoft 365 jobs and policies.

Every chart segment shows the number of objects of a specific type — the number of protected Users, Groups, Sites or Teams.

Object Storage Overview

The section provides the following details:

- Total number of object storage extents

- Number of organizations with object backups that reside on object storage extents

- Number of Users, Groups, Sites and Teams backups that reside on object storage extents

Space Usage

The chart shows the amount of used storage space in object storage.

If free space in the object storage is running low, you may need to free up storage space, revise your backup retention policy, or consider pointing jobs to another repository.

Top Object Storage by Used Space

The chart shows object storage extents with the greatest amount of used storage space.

For every object storage in the chart, you can see the amount of storage space used by Microsoft 365 object backups. If free space in the object storage is running low, you may need to free up storage space or revise your backup retention policy.

Top Object Storage by Weekly Backup Window

The chart allows you to detect the most 'busy' object storage extents over the past 7 days.

For every repository, the chart shows the cumulative amount of time that the repository was busy with backup job tasks.
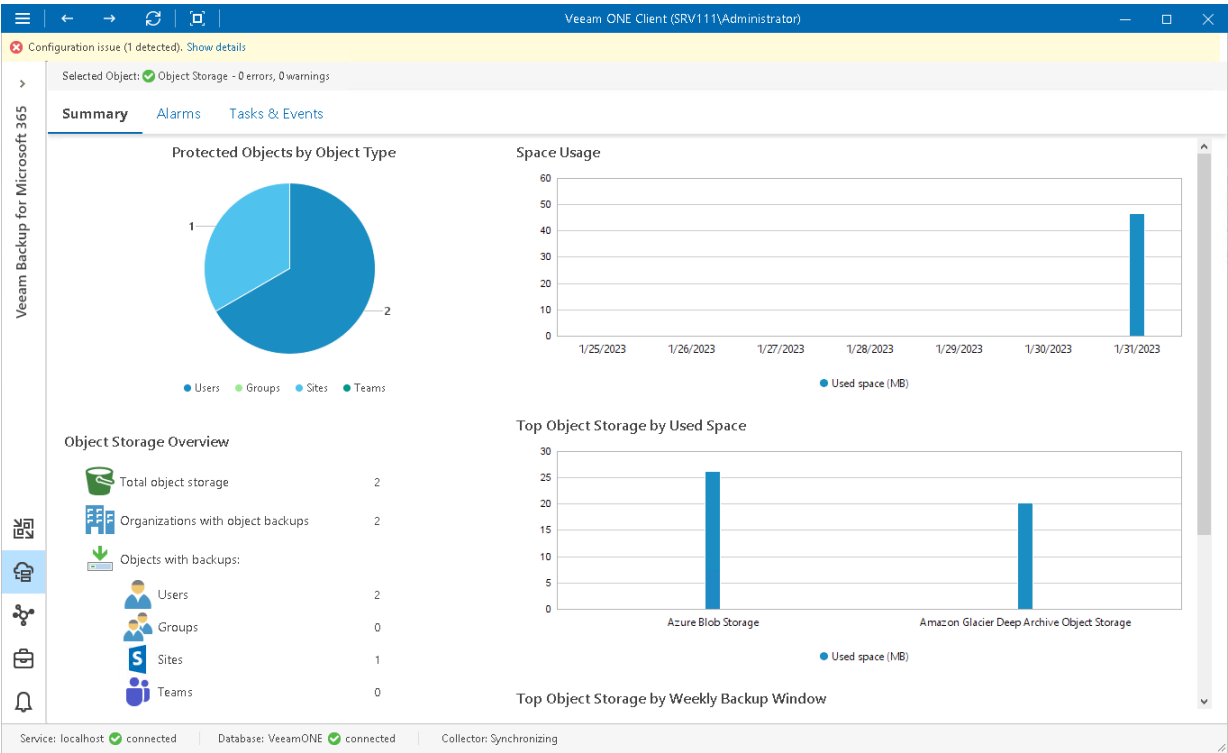
Veeam Backup for Microsoft 365 Repository Summary

Veeam ONE Client offers the following types of summary dashboards for backup repositories and object storage extents managed by Veeam Backup for Microsoft 365 server.

Backup Repository

The backup repository summary dashboard provides overview details, capacity planning information and performance analysis for a chosen backup repository for the last week or month.
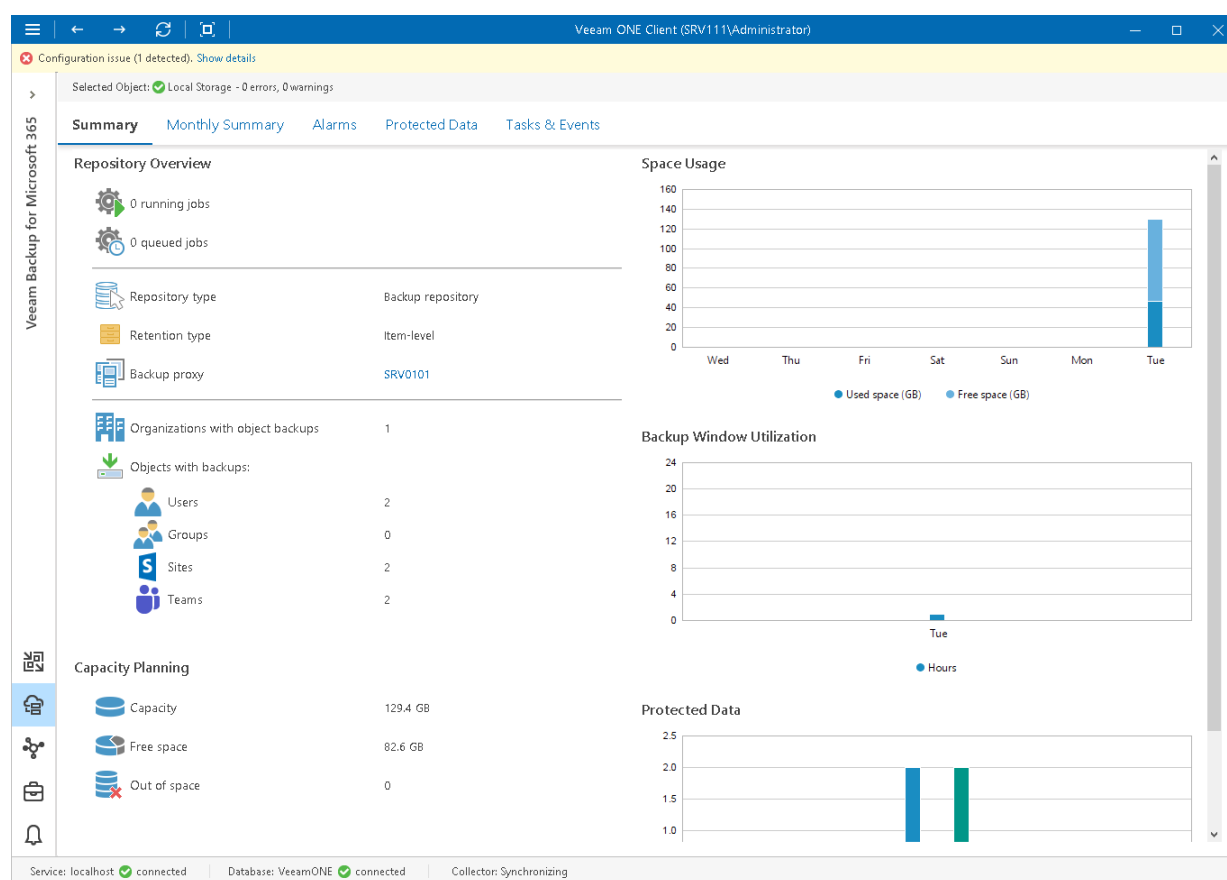
Repository Overview

The section provides the following details:

- Number of jobs that are currently running and queued on the repository

- Repository type: Backup repository or Extended with object storage

- Type of retention configured in the repository settings

- Backup proxy that processes jobs targeted to the repository

- [For extended repository] Object storage used as the repository extent

- Number of organizations with object backups that reside on the repository

- Number of Users, Groups, Sites and Teams backups that reside on the repository

Capacity Planning

The section provides the following details:

- Storage capacity of the repository

- Amount of free space on the repository

- Number of days before the repository runs out of free space

To forecast the value, Veeam ONE uses a trend that is calculated based on historical statistics — it analyzes how fast the amount of free space on the repository was decreasing in the past and uses historical statistics to forecast how soon the repository will run out of space.

Space Usage

The chart shows the amount of used storage space on the repository.

If free space on the repository is running low, you may need to free up storage space, revise your backup retention policy, or consider pointing jobs to another repository.

Backup Window Utilization

The chart shows the cumulative amount of time that the repository was busy with backup job tasks during the past week or month.

The chart can help you reveal possible resource bottlenecks on the repository side. If the backup window on the chart is abnormally large, this may evidence that the required I/O operations cannot complete fast enough, and your target is presenting a bottleneck for the whole backup data processing conveyor. To identify performance bottlenecks, you can switch to repository Veeam Backup for Microsoft 365 Performance Charts.

Protected Data

The chart shows the number of Microsoft 365 objects (Users, Groups, Sites, Teams) whose data was backed up to the repository during the past week or month.

Object Storage

The object storage summary dashboard provides overview details, capacity planning information and performance analysis for a chosen backup repository for the last week or month.
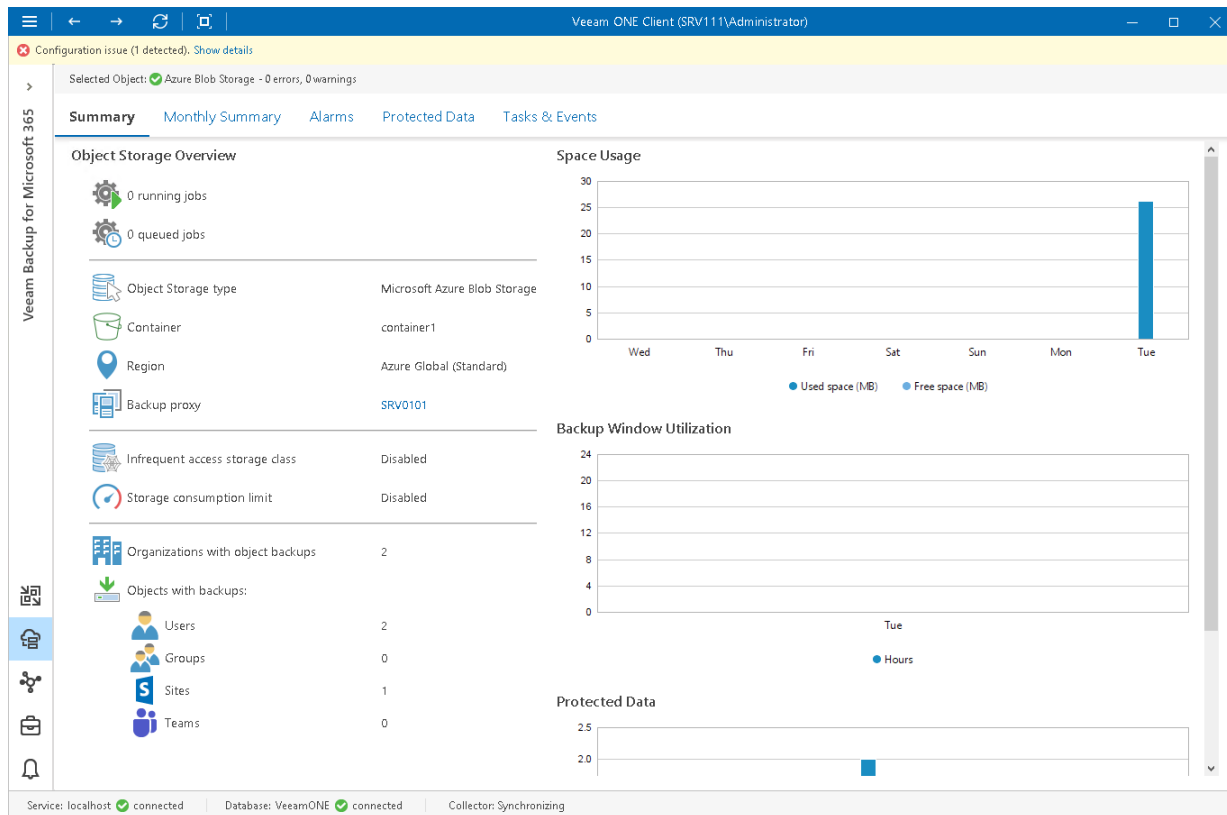
Object Storage Overview

The section provides the following details:

- Number of jobs that are currently running and queued on the object storage

- Object storage type

- Region at which the storage is located

- Name of bucket or container

- Limit of storage consumption

- Class of the infrequent access storage

- Number of organizations with object backups that reside on the repository

- Number of Users, Groups, Sites and Teams backups that reside on the repository

Capacity Planning

The section provides the following details:

- Amount of used space in the object storage

- Number of days before the object storage runs out of free space

To forecast the value, Veeam ONE uses a trend that is calculated based on historical statistics — it analyzes how fast the amount of used space in the object storage was increasing in the past and uses historical statistics to forecast how soon the object storage will run out of space.

Space Usage

The chart shows the amount of used space in the object storage.

If free space in the object storage is running low, you may need to free up storage space, revise your backup retention policy, or consider pointing jobs to another repository.

Backup Window Utilization

The chart shows the cumulative amount of time that the object storage was busy with backup job tasks during the past week or month.

The chart can help you reveal possible resource bottlenecks on the object storage side. If the backup window on the chart is abnormally large, this may evidence that the required I/O operations cannot complete fast enough, and your target is presenting a bottleneck for the whole backup data processing conveyor.

Protected Data

The chart shows the number of Microsoft 365 objects (Users, Groups, Sites, Teams) whose data was backed up to the repository during the past week or month.

Veeam Backup for Microsoft 365 Proxies Overview

The summary dashboard for the **Backup Proxies** node provides a configuration overview and performance analysis for backup proxies managed by a Veeam Backup for Microsoft 365 server.

This dashboard can help you detect configuration inefficiencies in your data protection infrastructure. If the same proxy server appears to process a great number of objects, transfer the greatest amount of backup data and use the largest backup window, you may need to re-balance the processing load across your backup proxies. The charts may also help you reveal 'lazy' proxies that you may decide to decommission.
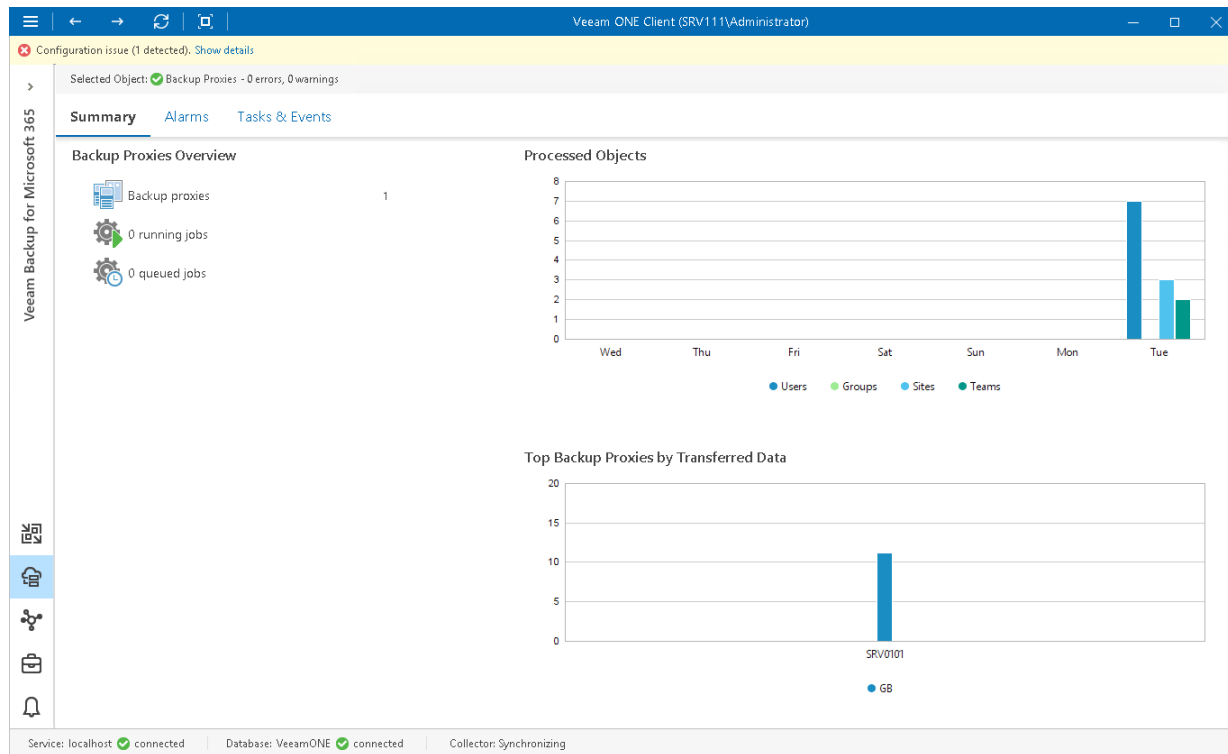
Backup Proxies Overview

The section provides the total number of backup proxies for the chosen Veeam Backup for Microsoft 365 infrastructure node and the total number of running and queued jobs that these proxies process.

Processed Objects

The chart shows the number of Microsoft 365 objects (Users, Groups, Sites, Teams) whose data the proxies processed during the past week.

Top Backup Proxies by Transferred Data

The chart shows backup proxies that transferred the greatest amount of backup data to the target destination over the past 7 days.

For every proxy, the chart shows the total amount of data that the proxy transferred over the network after the source-side deduplication and compression. The chart can help you detect backup proxies that transfer the greatest amount of backup data and estimate the load that backup jobs impose on the network.

Veeam Backup for Microsoft 365 Proxy Summary

The proxy summary dashboard provides overview details and performance analysis for a chosen backup proxy for the last week or month.
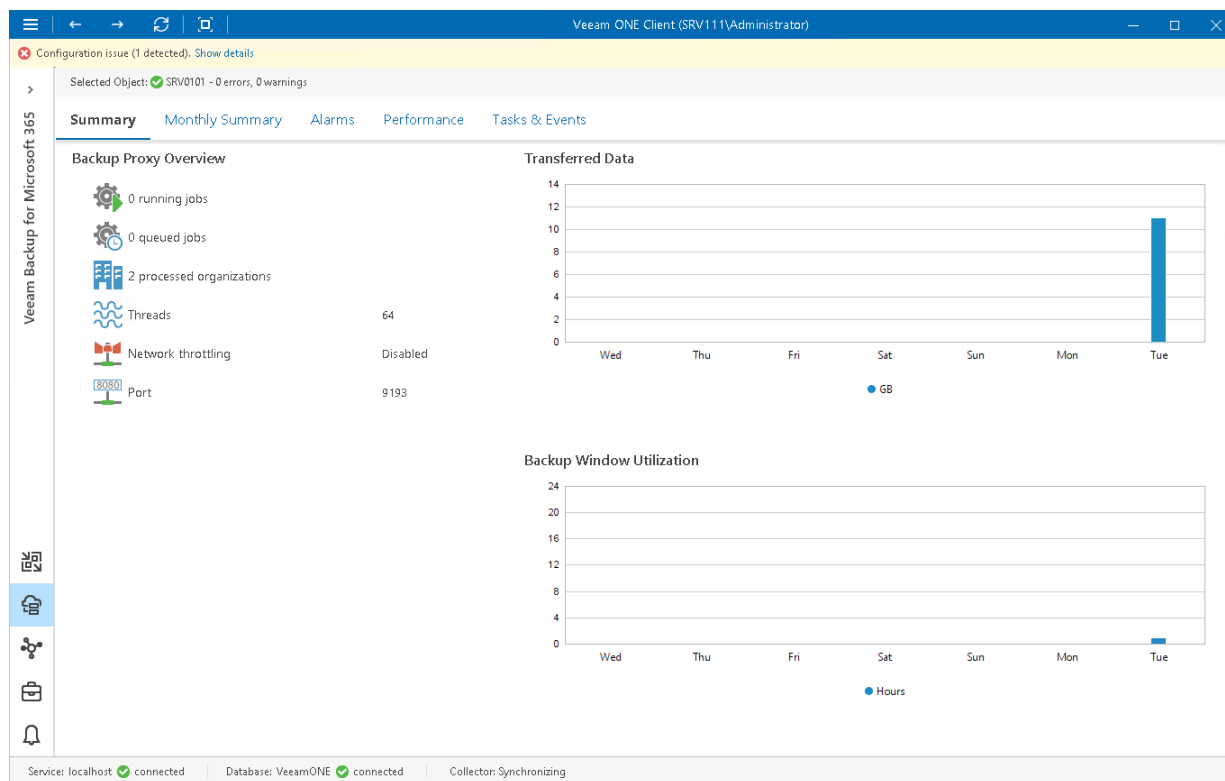
Backup Proxy Overview

The section provides the following details:

- Number of jobs that the proxy is currently processing

- Number of jobs queued for processing

- Number of Microsoft 365 organizations

- Number of threads configured in the backup proxy settings

- State of network throttling settings

- Port through which the proxy communicates with Veeam Backup for Microsoft 365 server

Transferred Data

The chart shows the amount of backup data that the proxy transferred to the target destination (backup repository or object storage) over the last 7 days.

The chart shows the total amount of data that the proxy transferred over the network after the source-side deduplication and compression. The chart can help you measure the amount of backup traffic coming from the proxy.

Backup Window Utilization

The chart allows you to estimate how 'busy' the proxy was during the last 7 days. The chart shows the cumulative amount of time that the proxy was retrieving, processing and transferring Veeam Backup for Microsoft 365 data.

The chart can help you reveal possible resource bottlenecks. If the backup window on the chart is abnormally large, this can evidence of low source data retrieval speed, high proxy CPU load or insufficient network throughput. To identify performance bottlenecks, you can switch to proxy Performance Charts.

Veeam Backup for Microsoft 365 Alarms

Veeam ONE includes a set of alarms monitor the efficiency of Veeam Backup for Microsoft 365 data protection in the virtual environment.

Predefined data protection alarms are configured to warn you about events or issues that can cause loss of data or prevent Veeam Backup for Microsoft 365 infrastructure from functioning properly:

- Connectivity issues and inability of backup infrastructure components to communicate with each other

- State of Veeam Backup for Microsoft 365 software installed on backup infrastructure components

- Failing jobs or jobs finished with warnings

- Configuration issues, such as fast decreasing space on backup repositories

- Long-running jobs that exceed the backup window

- Product license and prepaid support contract

To view the list of data protection alarms:

1. Open Veeam ONE Client.

    For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup for Microsoft 365**.

3. In the inventory pane, select the necessary backup infrastructure node.

4. Open the **Alarms** tab.

On the **Alarms** dashboard, you can view triggered alarms, track alarm history, resolve and acknowledge alarms and perform other actions. For more information on available actions, see Working with Triggered Alarms.

Veeam Backup for Microsoft 365 Data Protection

Veeam ONE Client allows you to track jobs configured to protect Microsoft 365 objects with Veeam Backup for Microsoft 365.

You can track real-time job statistics at different levels of your infrastructure:

- Jobs on a specific Veeam Backup for Microsoft 365 server

- All jobs across the entire Veeam Backup for Microsoft 365 infrastructure

To view the list of jobs at the necessary backup infrastructure level:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup for Microsoft 365**.

3. In the inventory pane, select the necessary infrastructure node.

4. Open the **Data Protection** tab.

5. To find the necessary job, you can use filters at the top of the job list:

   o To show or hide jobs that ended with a specific status, use the status buttons at the top of the list (*Show failed jobs*, *Show jobs with warnings*, *Show successful jobs*, *Show running jobs* or *Show jobs with no status*).

   o To show or hide jobs of a specific type, use the job type filter at the top of the list (*Backup*, *Backup copy*).

   o To show or hide jobs that protect specific object types, use the objects filter at the top of the list (*Entire organization, Users, Groups, Sites, Teams*).

   o To set the time interval when jobs ran for the last time, use the **Filter jobs by time period** button. Release the button to discard the time period filter.

   o To find jobs by name, use the search field at the top of the list.

The list of jobs shows all types of VM jobs for the backup infrastructure level that you selected in the inventory pane.

For every job, the following details are available:

- **Status** — the latest status of the job session (*Success*, *Warning*, *Failed*, *Running*, or jobs with no status).

- **Job Name** — name of a job.

- **Objects to Protect** — list of objects included in the job.

- **Organization** — name of Microsoft organization to which protected objects belong.

- **Last Run** — date and time of the latest job run.

- **Duration** — time taken to complete the job during its latest run.

- **Backup Proxy** — name of the backup proxy configured in job settings.

- **Backup Repository** — name of the target backup repository.

- **Transferred Data (GB)** — amount of backup data that was transferred to the target destination during the latest job run.

Veeam Backup for Microsoft 365 Performance Charts

To identify performance bottlenecks within the backup data flow, you can drill down to the following performance charts:

- CPU Performance Chart

- Memory Performance Chart

- Disk Performance Chart

- Network Performance Chart

To draw the charts, Veeam ONE gathers Windows Performance Monitor metrics from the guest OS of Veeam Backup for Microsoft 365 infrastructure components (for this reason, performance charts for Linux-based repositories are not available). You can track performance metrics for Veeam Backup for Microsoft 365 servers and proxies.

To drill down to a performance chart for a backup infrastructure component:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click Veeam Backup for Microsoft 365.

3. Select the necessary backup infrastructure component.

4. Open the necessary performance chart tab.

For Veeam Backup for Microsoft 365 performance charts, you can change chart views and set time intervals, define objects to show on charts or select custom metrics.

CPU Performance Chart

The **CPU** chart shows the amount of used processor resources on a machine where a backup infrastructure component runs. Graphs in the **CPU** chart illustrate the level of processor usage for every separate CPU on the machine. The **Total** graph shows the cumulative processor utilization for all CPUs.

Memory Performance Chart

The **Memory** chart shows the amount of used memory resources on a machine where a backup infrastructure component runs. Graphs in the **Memory** chart illustrate the amount of total available memory and memory that is currently used on the machine.

Disk Performance Chart

The **Disk** chart shows the rate at which the disk is transferring data during read and write operations. Disk usage is shown as an average for all physical disks on a machine where a backup infrastructure component runs.

Network Performance Chart

The **Network** chart shows the throughput for NICs on a machine where a backup infrastructure component runs. Graphs in the **Network** chart illustrate the rate at which data is sent on the network interface for each separate NIC. A separate graph shows the cumulative rate for all NICs on the machine.

Veeam Backup for Microsoft 365 Protected Data

The **Protected Data** tab allows you to view the list of protected Microsoft 365 objects stored in backups on backup and object storage repositories:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup for Microsoft 365**.

3. In the inventory pane, select the necessary repository.

4. Open the **Protected Data** tab.

5. To quickly find the necessary object, use the **Search** field and object type filter at the top of the list.

For every object in the list, the following details are shown:

- **Object** — name of the Microsoft 365 object stored in a backup on the repository.

- **Object Type** — type of Microsoft 365 object (*Users*, *Groups*, *Sites*, *Teams*).

- **Email Address** — address of the Microsoft 365 object.

- **Organization** — name of the Microsoft 365 to which the object belongs.

- **Last Job Run** — date and time of the latest job session.

- **Last Job Status** — status of the latest job session.

- **Job Name** — name of the data protection job to which the object is included.

- **Restore Points** — number of restore points stored on the backup repository.

Veeam Backup for Microsoft 365 Events

The **Tasks & Events** dashboard shows the history of events that triggered Veeam Backup for Microsoft 365 alarms. For the list and detailed description of data protection alarms, see Veeam Backup for Microsoft 365 Alarms.

To view the list of events for a specific level:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Veeam Backup for Microsoft 365**.

3. In the inventory pane, select the necessary backup infrastructure node.

4. Open the **Tasks & Events** tab.

5. The **Tasks & Events** list can display up to 1000 tasks and events at a time. To find the necessary task or event, you can use the following controls:

   o To display tasks or events for a specific period, select the necessary time interval from the **Events from** list.

   o To show or hide tasks or events, use filter buttons at the top of the list — *Show all events*, *Show errors*, *Show warnings*, *Show info messages*, *Show user events*, *Show tasks*.

   o To find the necessary tasks or events by description, use the **Search** field at the top of the list.

6. To view the detailed description of an event, click it in the list.

   The event description will be shown in the **Event Details** pane at the bottom.

   When you choose a virtual infrastructure container in the inventory pane, you can view events for the selected object and events for its child objects. To hide events related to child objects, clear the **Include events from child objects** check box at the bottom of the **Event Details** section.

7. To export displayed events to a CSV file, click **Export to CSV** at the top of the list and specify the location where the file will be saved.

VMware vSphere Monitoring

Veeam ONE Client offers a variety of tools for monitoring the VMware vSphere environment from any perspective and with any level of detail.

With Veeam ONE Client, you can:

1. **Monitor health status of the virtual environment.**

   o Start with the **Summary** dashboards to check the overall health status of the virtual environment and reveal hotspots.

     Quickly review the state of virtual infrastructure components, see the latest alarms, detect the most problematic objects and drill down to the problem source for further investigation.

   o Use the **Virtual Machines** dashboard to view the list of VMs in a virtual infrastructure container and check additional details for every VM — VM current state, parent host, IP address, DNS name and the amount of resources currently consumed by the VM.

   o Use the **Top Objects** dashboard to detect the most and less loaded components in the virtual environment.

     Detect what virtual infrastructure objects are consuming the most and the least amount of CPU, memory, disk, network, and swap resources, or select additional counters to detect resource consumers in other areas.

2. **View triggered alarms.**

   Switch to the **Alarms** dashboard to see details on breached thresholds, events and problems that occurred in the virtual environment.

   Use the **Actions** pane on the alarms dashboard to detect root causes — drill down to performance charts, open VM console or view the list of in-guest processes.

3. **Work with performance charts and track events.**

   Drill down to performance charts to diagnose performance problems. You can change predefined views, quickly switch between charts and view events occurring in your environment to get all-round statistics.

4. **Investigate problems from within the guest OS.**

   Open the VM console or view the list of in-guest processes to diagnose problems related to a specific service, module or application.

Prerequisites

Before you start monitoring your virtual environment, make sure you have configured connections to virtual servers from which Veeam ONE will collect data. For more information on configuring server connections, see section Connecting VMware vSphere Servers of the Veeam ONE Deployment Guide.

VMware vSphere Summary Dashboards

VMware vSphere infrastructure summary dashboards serve as the starting point for monitoring and troubleshooting. Summary dashboards reflect the health status of the selected infrastructure object or infrastructure segment.

The following types of summary dashboards are available for virtual infrastructure objects:

- VMware vSphere Infrastructure Summary

- Host Summary

- Virtual Machine Summary

- Datastore Summary

To access a summary dashboard for a virtual infrastructure object or virtual infrastructure segment:

1. Open Veeam ONE Client.

    For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure object or segment.

4. Open the **Summary** tab.

VMware vSphere Infrastructure Summary

The VMware vSphere infrastructure summary dashboard provides the health status overview for the selected virtual environment segment.

The dashboard is available for the following infrastructure levels:

- Virtual infrastructure (root node)

- Virtual infrastructure container (such as folder, resource pool, host, cluster, datacenter or vCenter Server)

Host Status, Datastores Status, Virtual Machines Status

The charts reflect the status of virtual infrastructure objects.

Every chart segment represents the number of objects in a certain state — objects with errors (red), objects with warnings (yellow) and healthy objects (green). Click a chart segment or a legend label to drill down to the list of alarms with the corresponding status for the selected type of virtual infrastructure objects.

Latest Alarms

The list displays the latest 15 alarms that were triggered for objects in the selected virtual environment segment. Click a link in the **Source** column to drill down to the list of alarms triggered for a specific virtual infrastructure object.

Alarms by Object

The list displays 15 objects with the highest number of alarms.

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 error alarms and 1 warning alarm triggered for the object. Click a link in the **Source** column to drill down to the list of alarms related to a specific virtual infrastructure object.

For more information, see Working with Triggered Alarms.

Host Summary

The host summary dashboard provides the health status and performance overview for the selected ESXi host and its child objects.
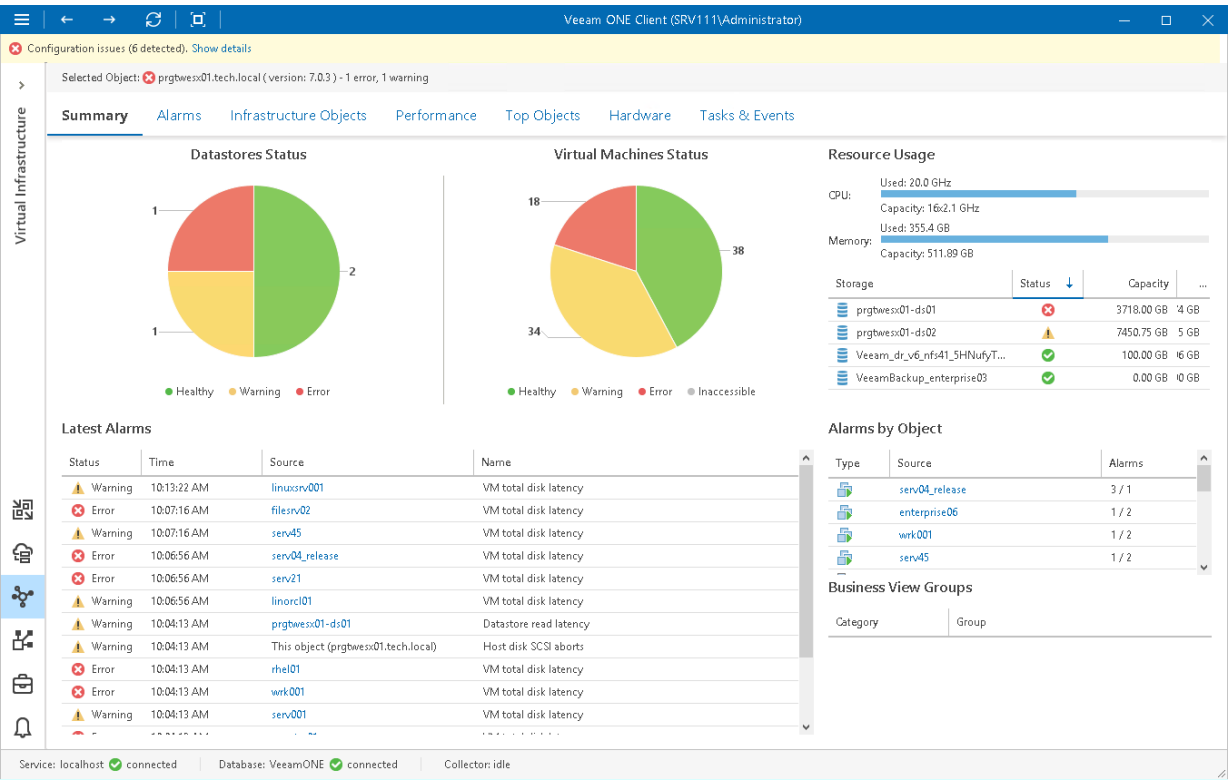
Datastores Status, Virtual Machines Status

The charts reflect the status of datastores connected to the host and the state of VMs running on the host.

Every chart segment represents the number of objects with a certain status — objects with errors (red), objects with warnings (yellow) and healthy objects (green). Click a chart segment or a legend label to drill down to the list of alarms with the corresponding status for host child objects.

Resource Usage

The section displays capacity and performance summary for host CPU and memory. It also shows an overview for datastores connected to the host — status of the datastore, its capacity and the amount of free space on the datastore.

Latest Alarms

The list displays the latest 15 alarms triggered for the host and its child objects. Click a link in the **Source** column to drill down to the list of alarms for the host and its child objects.

Alarms by Object

The list displays 15 objects with the greatest number of alarms (including the host and its child objects).

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 error alarms and 1 warning alarm triggered for the object. Click a link in the **Source** column to drill down to the list of alarms related to the host and its child objects.

For more information, see Working with Triggered Alarms.

Business View Groups

The section displays the list of categories and groups to which the host is included.

Virtual Machine Summary

The VM summary dashboard provides the health status and performance overview for the selected VM. In addition, this dashboard shows the state of objects that can affect the VM performance — the parent host and the datastores where VM files are located.

Selected Object

The section at the top of the dashboard shows the VM health status (number of warnings and errors) and the date when the latest backup or replica restore point was created for the VM with Veeam Backup & Replication.

CPU Usage, Memory Usage

The charts display the amount of CPU and memory resources currently consumed by the VM.

Guest Disk Usage

The chart displays the amount of available and used guest disk space with a breakdown by disks. By default, 5 guest disks with the greatest amount of used space are displayed.

Use the **Disks to show** list to change the number of disks to display on the chart. Click the **View all disks** link to view details for all guest disks. In the **Guests Disks** window, you can suppress *Guest disk space* alarms for specific disks. To suppress alarms for a disk, select the **Suppress alarms** check boxes next to the disk name.

> **NOTE:**
>
> Details on the guest disk usage are available only for VMs with VMware Tools installed.

Parent Object Health Status

The section displays the current state of the host where the VM resides and the state of datastores that host VMs files. Information available in this section may help you estimate how the state of parent objects impacts the VM performance. Click the host or datastore link to drill down to the list of alarms for the host or datastore.

Latest Alarms

The list displays the latest 15 alarms for the VM.

For more information, see Working with Triggered Alarms.

Business View Groups

The section displays the list of categories and groups to which the VM is included.

Datastore Summary

The datastore summary dashboard provides the health status and performance overview for the selected datastore. In addition, it shows the status of objects that can affect the datastore performance — hosts that work with the datastore and VMs whose files reside on the datastore.
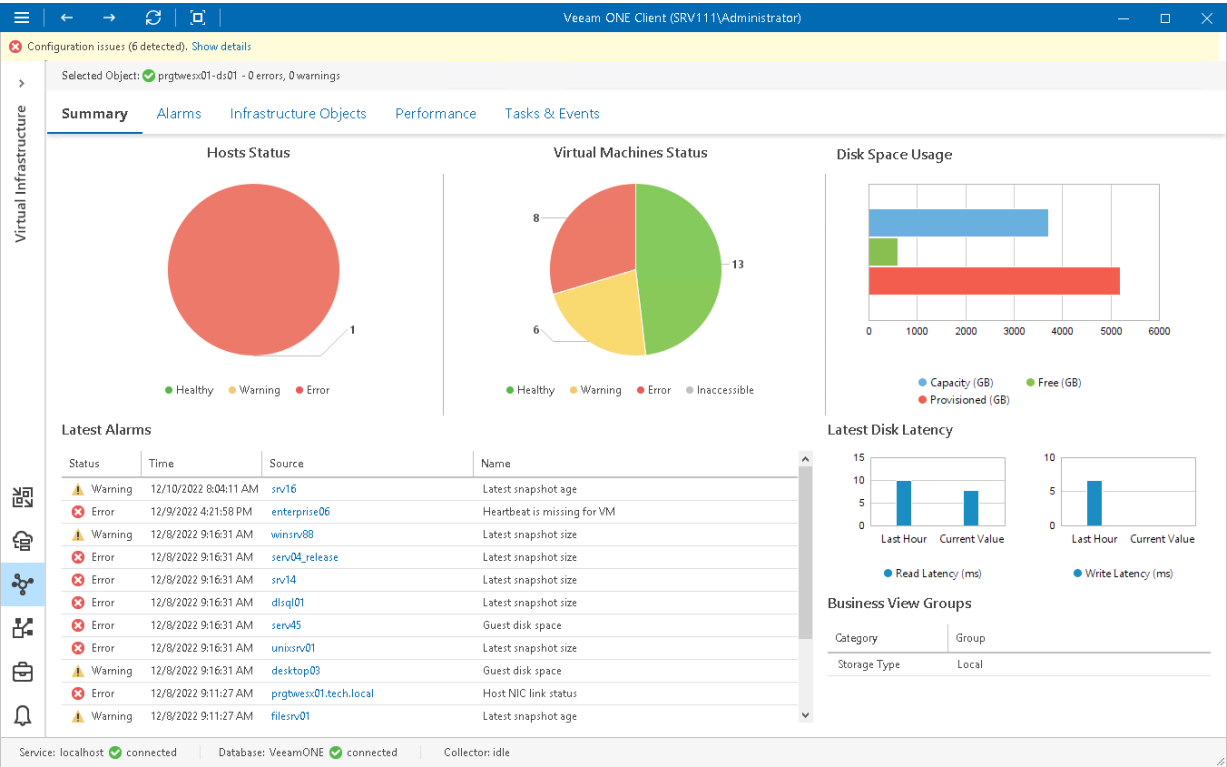
Hosts Status, Virtual Machines Status

The charts reflect the health status of hosts that work with the datastore and VMs whose files reside on the datastore.

Every chart segment represents the number of objects with a certain status — objects with errors (red), objects with warnings (yellow) and healthy objects (green). Click a chart segment or a legend label to drill down to the list of alarms with the corresponding status for hosts or VMs.

Disk Space Usage

The chart shows the amount of available, used and provisioned disk space on the datastore.

Latest Disk Latency

The section displays the current read and write latency values as well as the average latency values for the past hour.

Latest Alarms

The list displays the latest 15 alarms for the datastore and for objects that work with this datastore. Click a link in the **Source** column to drill down to the list of alarms for the selected object.

For more information, see Working with Triggered Alarms.

Business View Groups

The section displays the list of categories and groups to which the datastore is included.

VMware vSphere Alarms

Veeam ONE includes a set of alarms for monitoring VMware vSphere virtual environment. These alarms warn you about events or changes that can affect performance of operations and services in the virtual environment.

To view the list of triggered VMware vSphere alarms:

1. Open Veeam ONE Client.

    For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary virtual infrastructure node.

4. Go to the **Alarms** tab.

On the **Alarms** dashboard, you can view triggered alarms, track alarm history, resolve and acknowledge alarms and perform other actions. For more information on available actions, see Working with Triggered Alarms.

VMware vSphere Performance Charts

Performance charts show how key performance counters have been changing over time to help you diagnose performance issues and perform root cause analysis.

Performance charts include the following elements:

- **Axes**

  Performance charts display data for a particular time period (the horizontal axis) using two scales of measurement units (vertical axes). The measurement units may vary depending on selected performance counters. However, the number of units is always limited to two.

- **Graphs**

  Performance charts include one or more graphs. Every graph on a performance chart visualizes a specific counter for an infrastructure object or a container of infrastructure objects.

- **Legend**

  The chart legend shows details about objects and counters displayed in the chart. The details include key color, object name, list of counters and units of measurement, the latest, minimum, average, and maximum counter values.

- **Chart views**

  Performance charts come with a number of predefined chart views. Every view logically groups related counters to display the most valuable data and help you speed up troubleshooting and root cause analysis of performance problems.

Performance charts can be easily customized. For more information on customization options, see Customizing VMware vSphere Performance Charts.

Accessing Performance Charts

To access a performance chart for an infrastructure object or infrastructure segment:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure object or segment.

4. Open the **Performance** tab.

Overview

The **Overview** page shows aggregated performance data for the selected infrastructure object or segment: CPU usage, memory usage, memory swapped, network and datastore usage. Performance data is shown for the previous 60 minutes.

In the **Top line** field, you can set a threshold value. The top line is displayed as the red dotted line in the chart to help you monitor whether resource usage exceeds the healthy value range. If you do not need to display the top line, enter '0' (zero) in the **Top line** field or disable top lines in Veeam ONE Client chart settings. With the top line disabled, the Y-axis will scale automatically to match the range of the displayed data.

To drill down to performance chart details, click the counter link above a performance widget. A corresponding performance chart for the selected virtual infrastructure object will open.

CPU Performance Chart

The **CPU** chart displays historical statistics on CPU utilization for the selected infrastructure object.

Host

The following table provides information on predefined views and counters that apply to hosts.

Chat View	Counter	Measurement Unit	Description
CPU Usage	CPU Usage	Percent	CPU actively used on a host, as a percentage of total available CPU.
	CPU Usage (Absolute)	GHZ	Sum of actively used CPU for all powered on VMs on a host.
CPU Bottlenecks	Average CPU Ready	Percent	Average CPU Ready value for all VMs on a host.

Virtual Machine

The following table provides information on predefined views and counters that apply to VMs.

Chat View	Counter	Measurement Unit	Description
CPU Usage	CPU Usage	Percent	Amount of actively used virtual CPU resources, as a percentage of total available CPU (this is the host view, not the guest OS view).
	CPU usage (Absolute)	GHZ	Amount of actively used virtual CPU resources (this is the host view, not the guest OS view).
CPU Bottlenecks	Average CPU Idle All cores	Percent	Average amount of time all CPU cores spent in an idle state.
	Average CPU Ready All cores	Percent	Average CPU Ready value across all cores on a host.
	Average CPU Standstill All cores	Percent	Average amount of time all CPU cores spent in a standstill state.
	Average CPU Wait All cores	Percent	Time spent waiting for hardware or VMKernel lock thread locks.
	CPU Co-stop all cores	Percent	Average amount of time a VM was ready but unable to run due to co-scheduling constraints.

For objects that are parent to ESXi hosts and VMs, Veeam ONE displays rollup values.
Charts for folders, clusters, datacenters, vCenter Servers display rollup values for all hosts in the container. Chart for a resource pool displays rollup values for all VMs in the resource pool.

Memory Performance Chart

The **Memory** chart displays historical statistics on memory utilization for the selected infrastructure object.
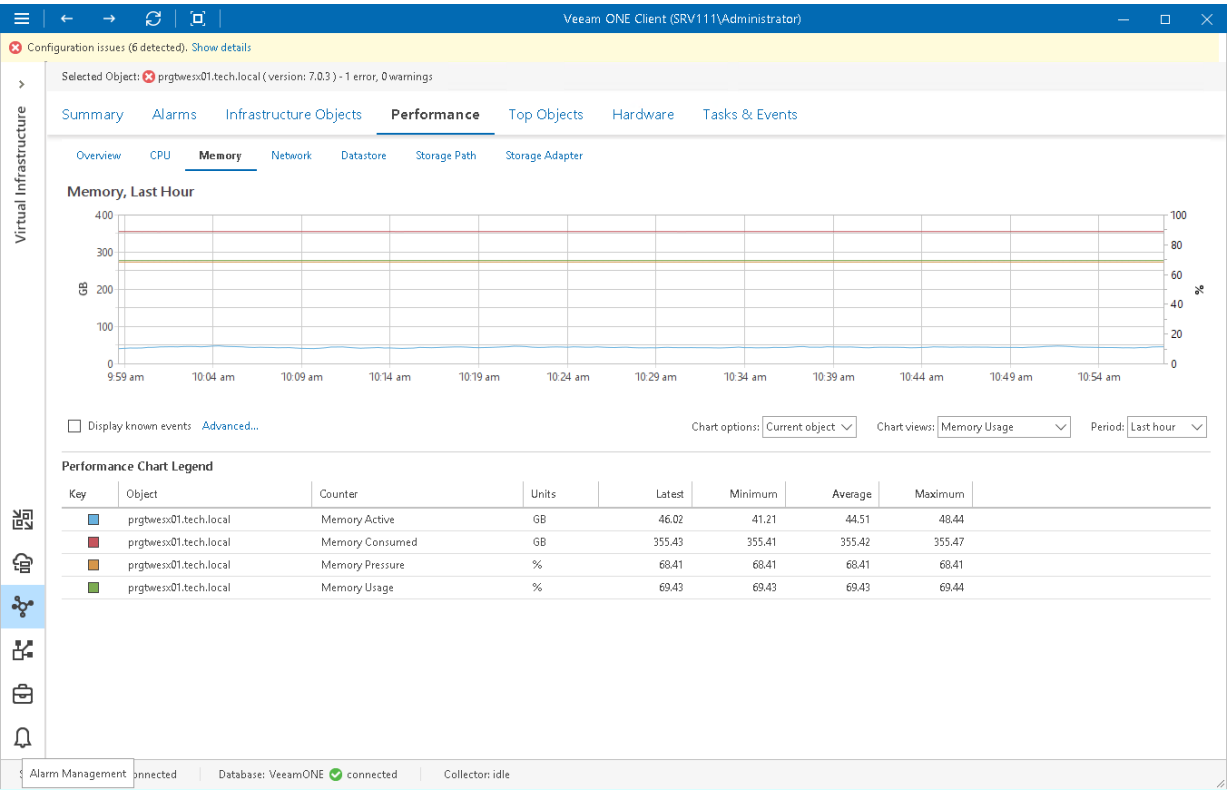
Host

The following table provides information on predefined views and counters that apply to hosts.

Chart View	Counter	Measurement Unit	Description
Memory Usage	Memory Active	GB	Sum of all active memory metrics for all powered-on VMs and vSphere services (such as COS, vpxa) on a host, as estimated by VMkernel based on recently touched memory pages.
	Memory Consumed	GB	Amount of physical memory used on a host, including memory used by the Service Console, VMkernel, vSphere services and total memory consumed by running VMs.
	Memory Pressure	Percent	Potential memory demand that is based on total allocated memory for running VMs, memory overhead, effects of memory Transparent Page Sharing and total available memory.

Chart View	Counter	Measurement Unit	Description
	Memory Usage	Percent	Memory usage as percentage of available machine memory.
Memory Swap Rate	Memory Swap Used	B	Amount of memory swapped to disk: sum of memory swapped for all powered on VMs and vSphere services on a host.
	Swap In Rate	B/s	Rate at which memory is swapped from disk into host active memory during the current interval.
	Swap Out Rate	B/s	Rate at which memory is swapped from host active memory to disk during the current interval.
Memory Management	Memory Balloon	B	Amount of memory allocated by the VM memory control driver (vmmemctl).
	Memory Compressed	B	Amount of RAM pages memory compressed by a host instead of swapping to disk.
	Memory Overhead	B	Total amount of memory overhead metrics for all powered-on VMs, plus memory overhead of running vSphere services on a host.
Memory Sharing	Memory Shared	MB	Sum of memory shared metrics for all powered-on VMs, and memory consumed by vSphere services on a host.
	Memory Shared Common	MB	Amount of memory shared by all powered-on VMs and vSphere services on a host.
Memory Latency	Memory Latency	Percent	Percentage of time a VM is waiting to access swapped or compressed memory.

Virtual Machine

The following table provides information on predefined views and counters that apply to VMs.

Chart View	Counter	Measurement Unit	Description
Memory Usage	Memory Active	GB	Amount of guest physical memory actively used, as estimated by VMkernel based on recently touched memory pages.
	Memory Consumed	GB	Amount of guest physical memory consumed by a VM. The value includes the shared and memory that might be reserved but not actually used; overhead memory is not taken into account.
	Memory Entitlement	GB	Amount of host physical memory a VM is entitled to, as determined by the ESXi scheduler.
	Memory Usage	Percent	Memory usage as percentage of configured physical memory for a VM.
Memory Swap Rate	Memory Swapped	B	Amount of guest physical memory swapped out to the VM swap file by the VMkernel. The metrics refers to VMkernel swapping, not to guest OS swapping.
	Swap In Rate	B/s	Rate at which memory is swapped from disk into active memory during the current interval.
	Swap Out Rate	B/s	Rate at which memory is swapped from active memory to disk during the current interval.
Memory Management	Memory Balloon	MB	Amount of memory allocated by the VM memory control driver (vmmemctl).
	Memory Compressed	MB	Amount of RAM pages compressed by a host instead of swapping to disk.
	Memory Overhead	MB	Amount of machine memory used by VMkernel to run a VM.
	Memory Saved by Zipping	MB	Amount of memory saved by memory zipping.

Chart View	Counter	Measurement Unit	Description
Memory Sharing	Memory Shared	B	Amount of guest physical memory that a VM shares with other virtual machines (through VMkernel Transparent Page Sharing and RAM deduplication).
Memory Latency	Memory Latency	Percent	Percentage of time a VM is waiting to access swapped or compressed memory.

For objects that are parent to ESXi hosts and VMs, Veeam ONE Client displays rollup values.

Charts for folders, clusters, datacenters, vCenter Servers display rollup values for all hosts in the container. Chart for a resource pool displays rollup values for all VMs in the resource pool.

Network Performance Chart

The **Network** chart displays historical statistics on network usage for the selected infrastructure object.
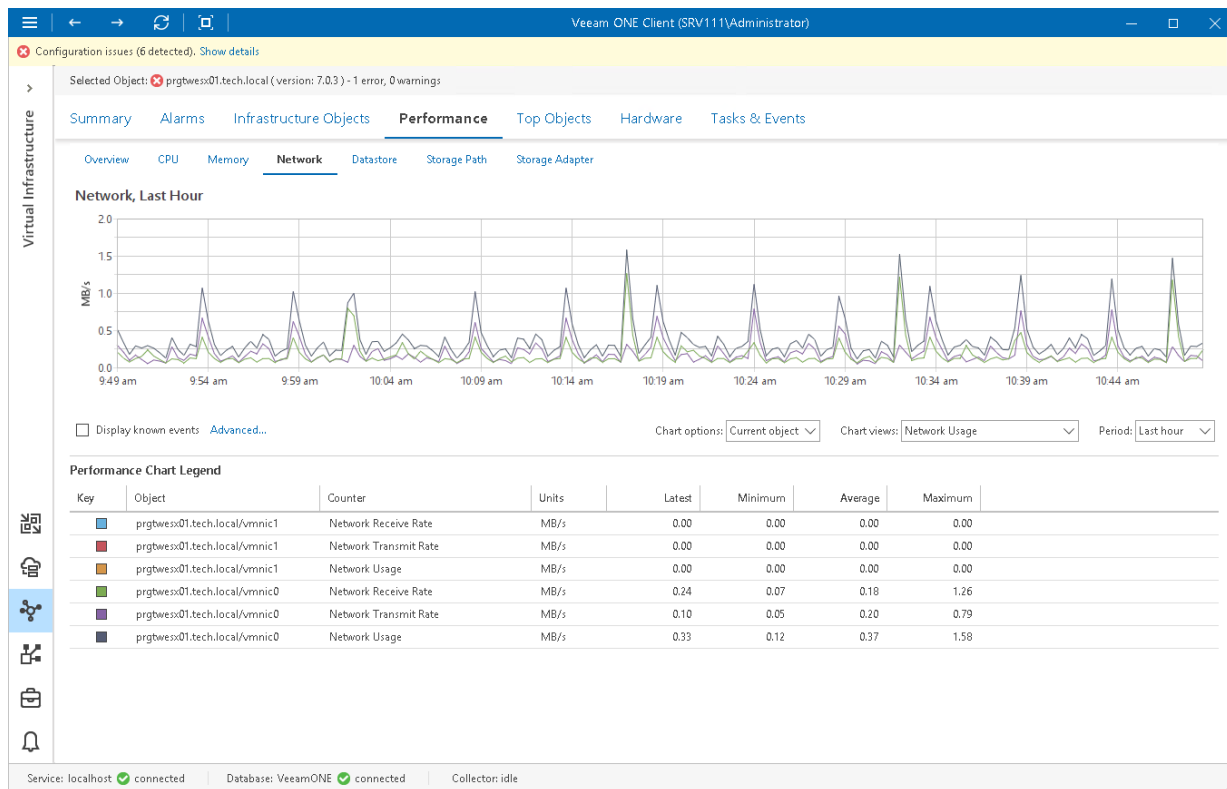
Host

The following table provides information on predefined views and counters that apply to hosts.

Chart View	Counter	Measurement Unit	Description
Network Usage	Network Receive Rate	KB/s	Rate at which data is received across each physical NIC instance on a host. The counter represents the bandwidth of the network.
	Network Transmit Rate	KB/s	Rate at which data is transmitted across each physical NIC instance on a host.
	Network Usage	KB/s	Network utilization, sum of data received and transmitted across all physical NIC instances connected to a host.
	Received Packets per Second	Number	Average number of packets received per second across each physical NIC instance on a host.

Chart View	Counter	Measurement Unit	Description
Network Transfer Rate (Packets)	Transmitted Packets per Second	Number	Average number of packets transmitted per second across each physical NIC instance on a host.
Dropped and Error Packets	Packet Receive Errors	Number	Number of packets with errors received.
	Packet Transmit Errors	Number	Number of packets with errors transmitted.
	Receive Packets Dropped	Number	Number of receives dropped.
	Total Errors	Number	Total number of packets with errors received and transmitted.
	Total Packets Dropped	Number	Total number of dropped packets.
	Transmit Packets Dropped	Number	Number of transmits dropped.

Virtual Machine

The following table provides information on predefined views and counters that apply to VMs.

Chart View	Counter	Measurement Unit	Description
Network Usage	Network Receive Rate	KB/s	Rate at which data is received across the vNIC instance on a VM. The counter represents the bandwidth of the network.
	Network Transmit Rate	KB/s	Rate at which data is transmitted across the vNIC instance on a VM.
	Network Usage	KB/s	Network utilization, sum of data received and transmitted across all vNIC instances on a VM.
	Received Packets per Second	Number	Average number of packets received per second by each vNIC instance on a VM.

Chart View	Counter	Measurement Unit	Description
Network Transfer Rate (Packets)	Transmitted Packets per Second	Number	Average number of packets transmitted per second by each vNIC instance on a VM.

For objects that are parent to ESXi hosts and VMs, Veeam ONE Client displays rollup values.

Charts for folders, clusters, datacenters, vCenter Servers display rollup values for all hosts in the container. Chart for a resource pool displays rollup values for all VMs in the resource pool.

Datastore Performance Chart

The **Datastore** chart displays historical statistics for all datastores (including vSAN datastores) used by the selected infrastructure component and its child objects.
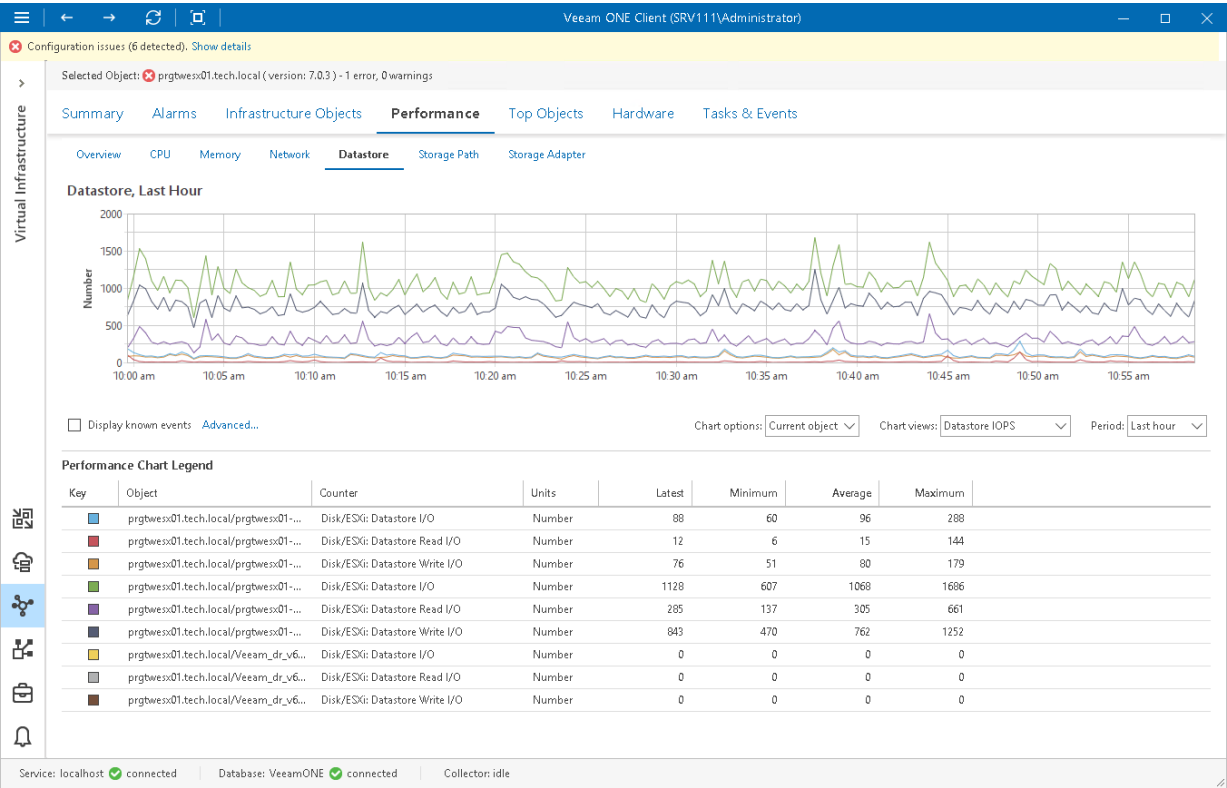
Host

The following table provides information on predefined views and counters that apply to hosts.

Chart View	Counter	Measurement Unit	Description
Datastore IOPS	Disk/ESXi: Datastore I/O	Number	Aggregate number of I/O operations on a datastore.
	Disk/ESXi: Datastore Read I/O	Number	Average number of read commands per second to a datastore.
	Disk/ESXi: Datastore Write I/O	Number	Average number of write commands per second to a datastore.
Datastore Usage Rates	Disk/ESXi: Datastore Read Rate	MB/s	Rate at which data is read from a datastore.

Chart View	Counter	Measurement Unit	Description
	Disk/ESXi: Datastore Usage	MB/s	Sum of read and write rates to a datastore.
	Disk/ESXi: Datastore Write Rate	MB/s	Rate at which data is written to a datastore.
Datastore Latency	Disk/ESXi: Datastore Highest Latency	Millisecond	Highest latency value across all datastores used by a host.
	Disk/ESXi: Datastore Latency Observed by VMs	Millisecond	Average datastore latency as seen by VMs.
	Disk/ESXi: Datastore Read Latency	Millisecond	Average amount of time that a read from the datastore takes.
	Disk/ESXi: Datastore Write Latency	Millisecond	Average amount of time that a write operation to a datastore takes.
Datastore Issues	Disk/ESXi: Datastore Bus Resets	Number	Number of SCSI bus reset commands.
	Disk/ESXi: Datastore Command Aborts	Number	Number of aborted SCSI commands.
	Disk/ESXi: Datastore Maximum Queue Depth	Number	Number of outstanding requests to a storage device.

Virtual Machine

The following table provides information on predefined views and counters that apply to VMs.

Chart View	Counter	Measurement Unit	Description
Datastore IOPS	Datastore I/O	Number	Aggregate number of I/O operations on a datastore.
	Datastore Read I/O	Number	Average number of read commands per second to a datastore.

Chart View	Counter	Measurement Unit	Description
	Datastore Write I/O	Number	Average number of write commands per second to a datastore.
	Disk/vSAN: Recovery Write I/O	Number	Average number of write commands per second to a vSAN datastore disk that contains copy of VM data.
Datastore Usage Rates	Datastore Read Rate	MB/s	Rate at which data is read from a datastore.
	Datastore Usage	MB/s	Sum of read and write rates for a datastore.
	Datastore Write Rate	MB/s	Rate at which data is written to a datastore.
	Disk/vSAN: Recovery Write Rate	MB/s	Rate of writing data to a vSAN datastore disk that stores copy of VM data.
Datastore Latency	Datastore Highest Latency	Millisecond	Highest latency value across all datastores used by a host.
	Datastore Read Latency	Millisecond	Average amount of time that a read operation from a datastore takes.
	Datastore Write Latency	Millisecond	Average amount of time that a write operation to a datastore takes.
	Disk/vSAN: Recovery Write Latency	Millisecond	Average amount of time that a write operation to a vSAN datastore disk storing copy of VM data takes.
Datastore Issues	Datastore Bus Resets	Number	Number of SCSI bus reset commands.
	Datastore Command Aborts	Number	Number of aborted SCSI commands.

For objects that are parent to ESXi hosts and VMs, Veeam ONE Monitor displays rollup values.
Charts for folders, clusters, datacenters, vCenter Servers display rollup values for all hosts in the container. Chart for a resource pool displays rollup values for all VMs in the resource pool.

Virtual Disks Performance Chart

The **Virtual Disks** chart displays historical statistics for partitions of all disks on the selected VM.
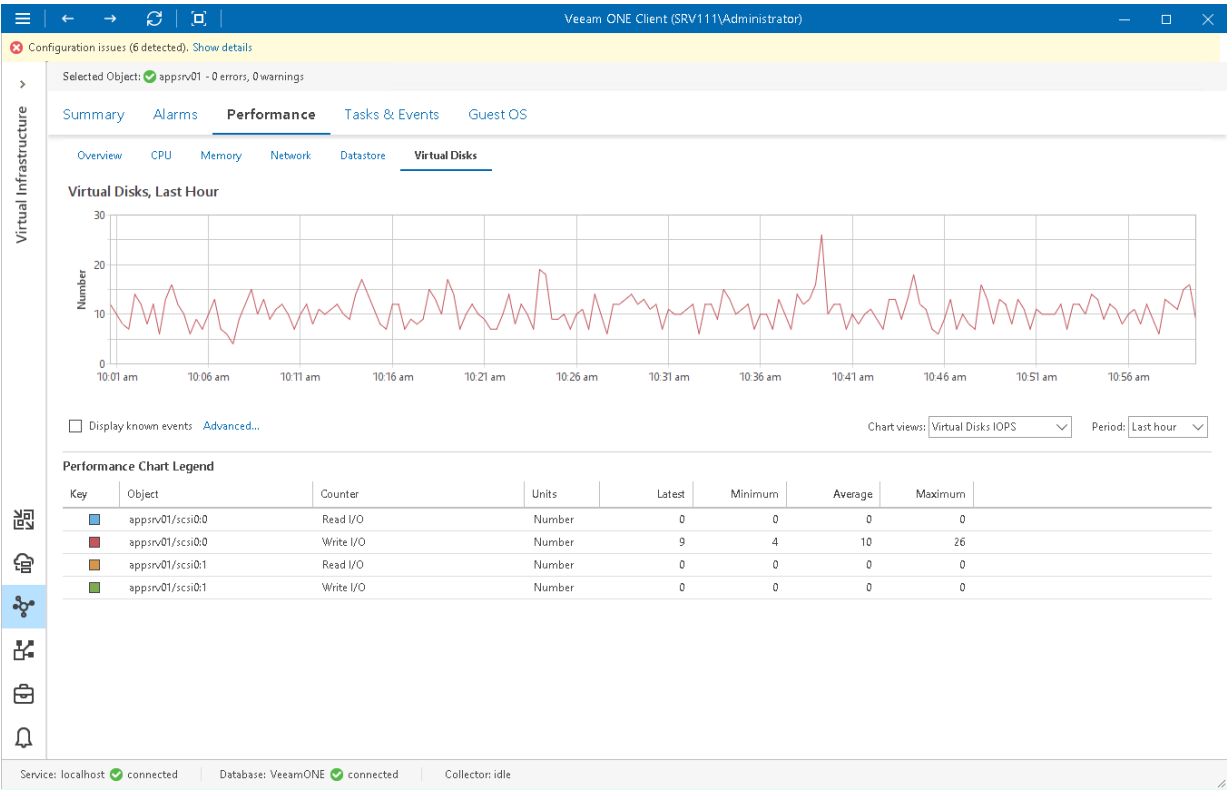
The following table provides information on predefined views and counters.

Chat View	Counter	Measurement Unit	Description
Virtual Disks IOPS	Read I/O	Number	Average number of read operations issued per second to a virtual disk.
	Write I/O	Number	Average number of write operations issued per second to a virtual disk.
Virtual Disks Usage Rates	Read Rate	MB/s	Rate at which data is read from a virtual disk.
	Write Rate	MB/s	Rate at which data is written to a virtual disk.
Virtual Disks Latency	Read Latency	Millisecond	Average amount of time that a read operation from a virtual disk takes.
	Write Latency	Millisecond	Average amount of time that a write operation to a virtual disk takes.

Storage Path Performance Chart

The **Storage Path** chart displays historical statistics for paths used by the storage adapter on the selected host.
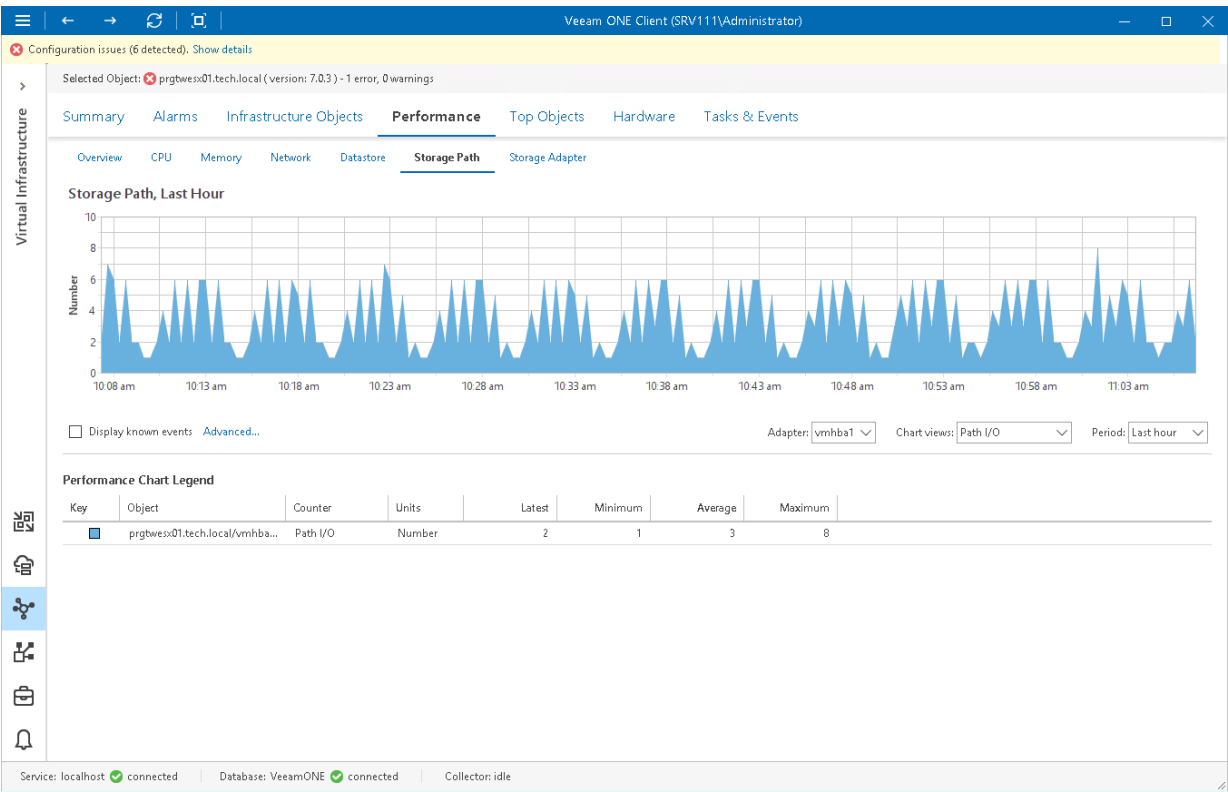
You can switch between adapters using the **Adapter** list below the performance chart.

The name of each storage device connected to the storage adapter through the selected path is specified after the host address (separated by a forward slash). It has the following format: *<HBA>:<SCSI target>:<SCSI LUN>:<disk partition>*

The following table provides information on predefined views and counters.

Chart View	Measurement Unit	Description
Path I/O	Number	Average number of commands issued per second through a path.
Path Read I/O	Number	Average number of read commands issued per second through a path.
Path Write I/O	Number	Average number of write commands issued per second through a path.
Path Read Rate	MB/s	Rate at which data is read through a path.
Path Write Rate	MB/s	Rate at which data is written through a path.

Chart View	Measurement Unit	Description
Path Read Latency	Millisecond	Average amount of time taken for a read operation through a path.
Path Write Latency	Millisecond	Average amount of time that a write operation through a path takes.

Storage Adapter Performance Chart

The **Storage Adapter** chart displays historical statistics for the storage adapters on the selected host.
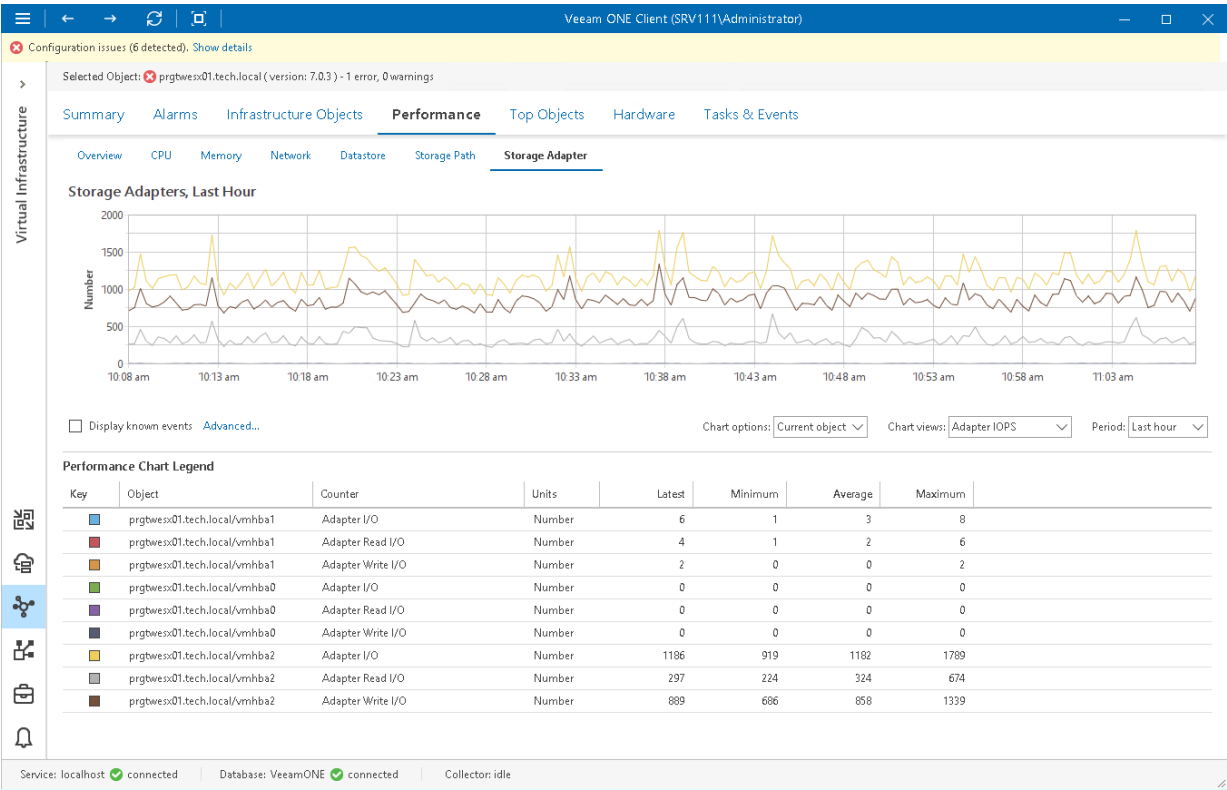
The following table provides information on predefined views and counters.

Chart View	Counter	Measurement Unit	Description
Adapter IOPS	Adapter I/O	Number	Average number of commands issued per second on a storage path during the collection interval.
	Adapter Read I/O	Number	Average number of read commands issued per second on a storage path during the collection interval.
	Adapter Write I/O	Number	Average number of write commands issued per second on a storage path during the collection interval.
Adapter Usage Rates	Adapter Read Rate	MB/s	Rate at which data is read on a storage path.
	Adapter Write Rate	MB/s	Rate at which data is written on a storage path.
Adapter Latency	Adapter Read Latency	Millisecond	Average amount of time that a read operation on a storage path takes.

Chart View	Counter	Measurement Unit	Description
	Adapter Write Latency	Millisecond	Average amount of time that a write operation on a storage path takes.

Disk Space Chart

The **Disk Space** chart is available for datastores and datastore clusters. It displays historical statistics on disk space resources and usage for the selected datastore or datastore cluster.
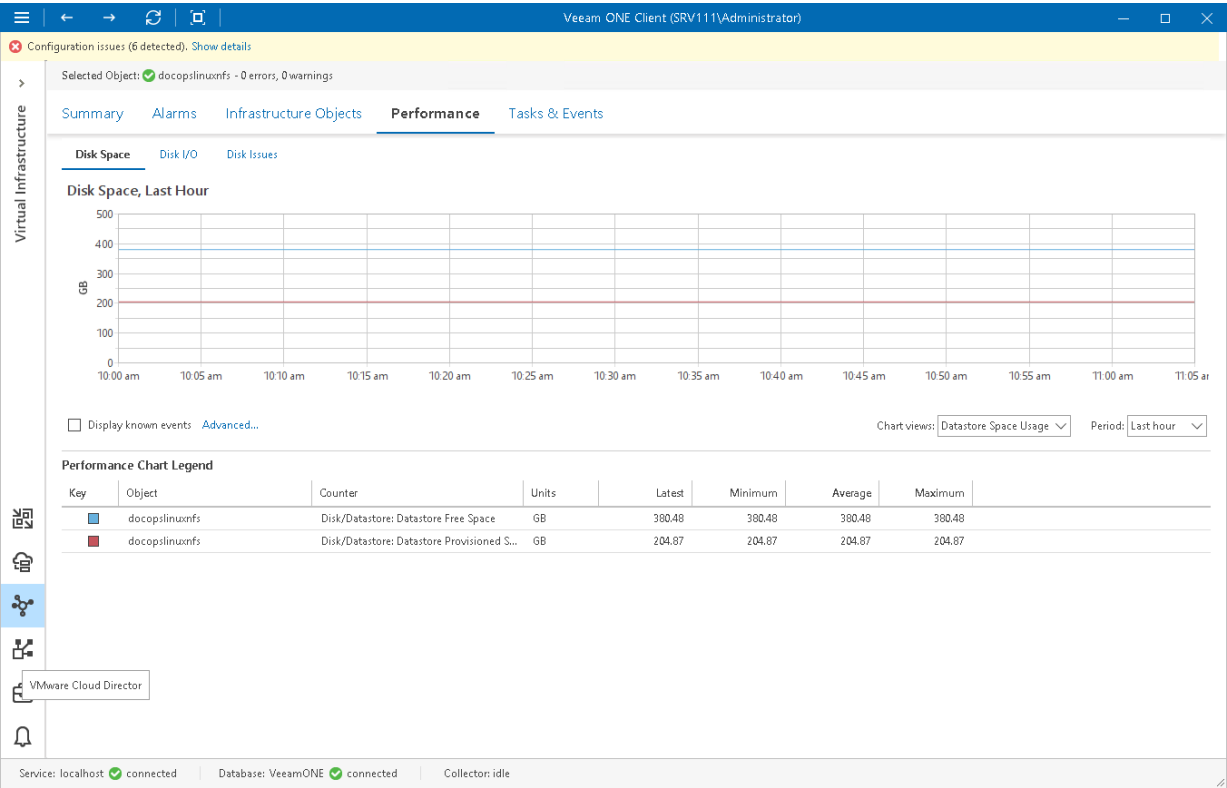
The following table provides information on predefined views and counters.

Chart View	Counter	Measurement Unit	Description
Datastore Space Usage	Disk/Datastore: Datastore Free Space	TB/GB	Amount of free space on a datastore.
	Disk/Datastore: Datastore Provisioned Space	TB/GB	Amount of storage allocated for a datastore. Size of files on the datastore cannot exceed this value.

Disk I/O Chart

The **Disk I/O** chart is available for datastores and datastore clusters. It displays historical statistics on the read and write load.
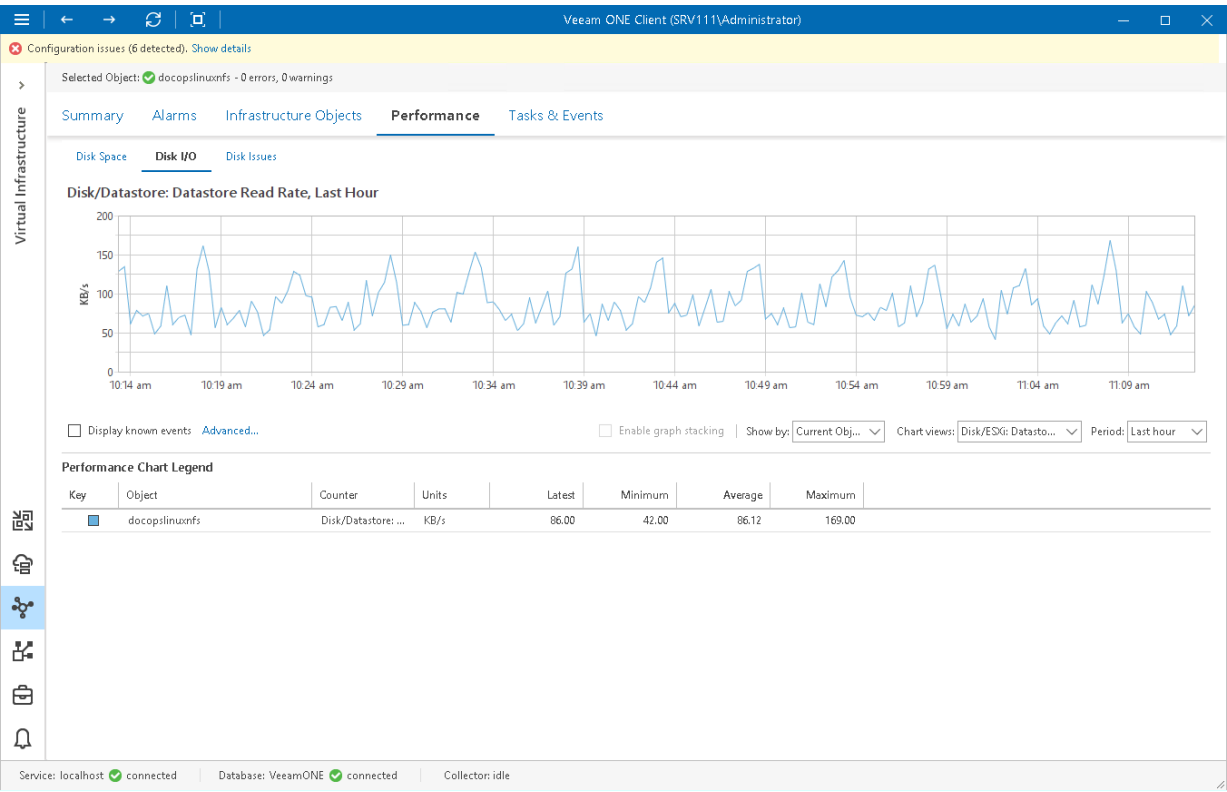
Use the **Chart options** list to display graphs for the current object (for example, a specific datastore or a virtual infrastructure container), for VMs or hosts that work with the selected datastore. For VMs or for hosts, this chart displays stacked graphs to let you see actual cumulative load on a particular datastore. If you choose to view the chart for the top **Datastore** parent object, you will also be able to stack graphs by all available datastores.

The following table provides information on predefined views and counters.

Chart View	Measurement Unit	Description
Disk/ESXi: Datastore Read Rate	MB/s	Rate at which data is read from a datastore.
Disk/ESXi: Datastore Write Rate	MB/s	Rate at which data is written to a datastore.
Disk/ESXi: Datastore Usage	MB/s	Sum of read and write rates for a datastore.
Disk/ESXi: Datastore Read I/O	Number	Number of times data was read from the disk by all VMs residing on a datastore.

Chart View	Measurement Unit	Description
Disk/ESXi: Datastore Write I/O	Number	Number of times data was written to the disk by all VMs residing on a datastore.
Disk/ESXi: Datastore I/O	Number	Average number of commands issued per second to a storage device by the adapter.
Disk/ESXi: Datastore Read Latency	Millisecond	Average amount of time that a read operation from a datastore takes (from the perspective of an ESXi host).
Disk/ESXi: Datastore Write Latency	Millisecond	Average amount of time that a write operation to a datastore takes (from the perspective of an ESXi host).

Disk Issues Chart

The **Disk Issues** chart displays historical statistics on the number of disk bus resets and disk command aborts that have occurred in the defined interval. This chart is available for datastores and datastore clusters.
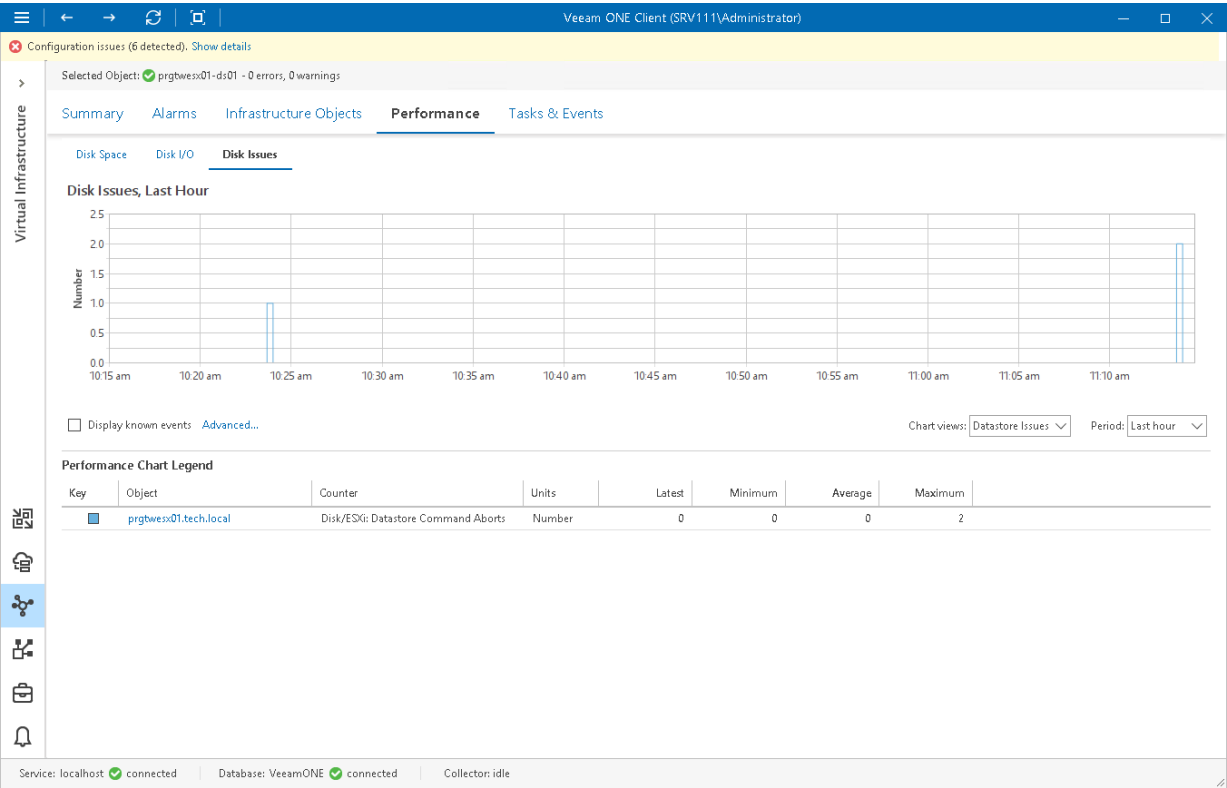
The following table provides information on predefined views and counters.

Chart View	Measurement Unit	Counter	Description
Datastore Issues	Disk/ESXi: Datastore Bus Resets	Number	Number of aborted SCSI commands.
	Disk/ESXi: Datastore Command Aborts	Number	Number of SCSI bus reset commands.

Customizing VMware vSphere Performance Charts

You can customize performance charts to select specific objects, time intervals or performance counters to display on the charts.

Selecting Objects to Chart

By default, all performance charts display data for an infrastructure object selected in the inventory pane. You can also choose to display performance data on charts for:

- Child components or objects of the selected virtual infrastructure object (for example, all hosts in the cluster)

- Child VMs for the selected virtual infrastructure object or segment

To display performance data for direct children of the selected virtual infrastructure object:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure object.

4. Open the necessary performance chart tab.

5. From the **Chart options** list, select *Custom*.

6. In the **Customize Chart Options** window, choose **Show performance data for these child objects**.

7. Select check boxes next to child objects that should be included in the chart scope.

8. Click **OK**.

To display performance data for a set of VMs in the selected infrastructure segment:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the inventory pane, select the necessary infrastructure object.

3. Open the necessary performance chart tab.

4. From the **Chart options** list, select *Custom*.

5. In the **Customize Chart Options** window, choose **Show performance data for these VMs**.

   You can select both direct and indirect children (children of children) of the selected virtual infrastructure object.

6. Select check boxes next to VMs that should be included in the chart scope.

7. Click **OK**.

NOTE:

The legend pane displays objects for which data is available for the selected time interval.

Selecting Chart Views and Performance Counters

Performance charts come with a set of predefined chart views that logically group related performance counters. You can switch between chart views using the **Chart view** list at the top of the chart legend.

Instead of using predefined views, you can choose a custom set of performance counters to show on the chart:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure object.

4. Open the necessary performance chart tab.

5. From the **Chart views** list, select the *Custom* option to open the **Select Devices and Counters** window.

6. From the **Devices** list, select the necessary resource device(s).

   Select *Total* to display all available devices on the chart.

NOTE:

The list of devices is not available for some performance charts. For example, for the **CPU** or **Memory** performance chart, you can only choose counters to display.

7. From the **Counters** list, select counters to display on the chart.

   When you select a counter, its description appears in the **Counter description** section of the window.

8. Click **OK**.

Selecting Time Interval

You can choose the time interval for which performance data on the chart will be displayed. Available options are:

* Last hour (real-time information)

* Last day

* Last week

* Last month

* Last year

* Custom time range (you can choose any time interval within the specified number of hours, days, or weeks, or specify any from/to period)

To specify a time interval for which performance data should be displayed:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure object.

4. Open the necessary performance chart tab.

5. From the **Period** list, select _Last hour_, _Last day_, _Last week_, _Last month_ or _Last year_.

   To define a custom time range, select _Custom_. In the **Select Custom Time Interval** window, define the necessary interval and click **OK**.

When you change the time interval, the time scale (X-axis) of the performance chart and the chart will change respectively.

VMware vSphere Tasks & Events

You can view information about tasks and events that occur in the virtual environment within the selected time interval. Veeam ONE loads tasks and events from vCenter Server. For each loaded task, it creates two events — one informs you when the task starts and the other informs you when the task ends.

To view the list of tasks and events:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure object.

4. Open the **Tasks & Events** tab.

5. The **Tasks & Events** list can display up to 1000 tasks and events at a time. To find the necessary task or event, you can use the following controls:

   o To display tasks or events for a specific period, select the necessary time interval from the **Events from** list.

   o To show or hide tasks or events, use filter buttons at the top of the list — *Show all events*, *Show errors*, *Show warnings*, *Show info messages*, *Show user events*, *Show tasks*.

   o To find the necessary tasks or events by description, use the **Search** field at the top of the list.

6. To view the detailed description of an event, click it in the **Tasks & Events** list.

   The event description will be shown in the **Event Details** pane at the bottom.

   When you choose a virtual infrastructure container in the inventory pane, you can view events for the selected object and events for its child objects. To hide events related to child objects, clear the **Include events from child objects** check box at the bottom of the **Event Details** section.

7. To export displayed events to a CSV file, click **Export to CSV** at the top of the list and specify the location where the file will be saved.

For every task or event in the list, the following details are available:

- Event type (*User*, *Task*, *Info*, *Warning* or *Error*)

- Short description

- Time of occurrence

- Object to which the task or event relates

- Object or user that caused or initiated the event

Viewing Events on Performance Charts

Performance charts for VMware vSphere infrastructure objects allow you to display the following resource-consuming events:

- Live Migration (vMotion)

- Snapshot creation events

- Snapshot removal events

- Veeam Backup & Replication events

This option can help you detect events that caused performance degradation. For example, you can see what was the reason for a steep increase in the network resources usage.

To display events on a performance chart:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure object.

4. Open the necessary performance chart tab.

5. At the bottom of the performance chart, select the **Display known events** check box.

6. To choose what type of events to show on the performance chart, click the **Advanced** link next to the **Display known events** check box, and select the necessary events.
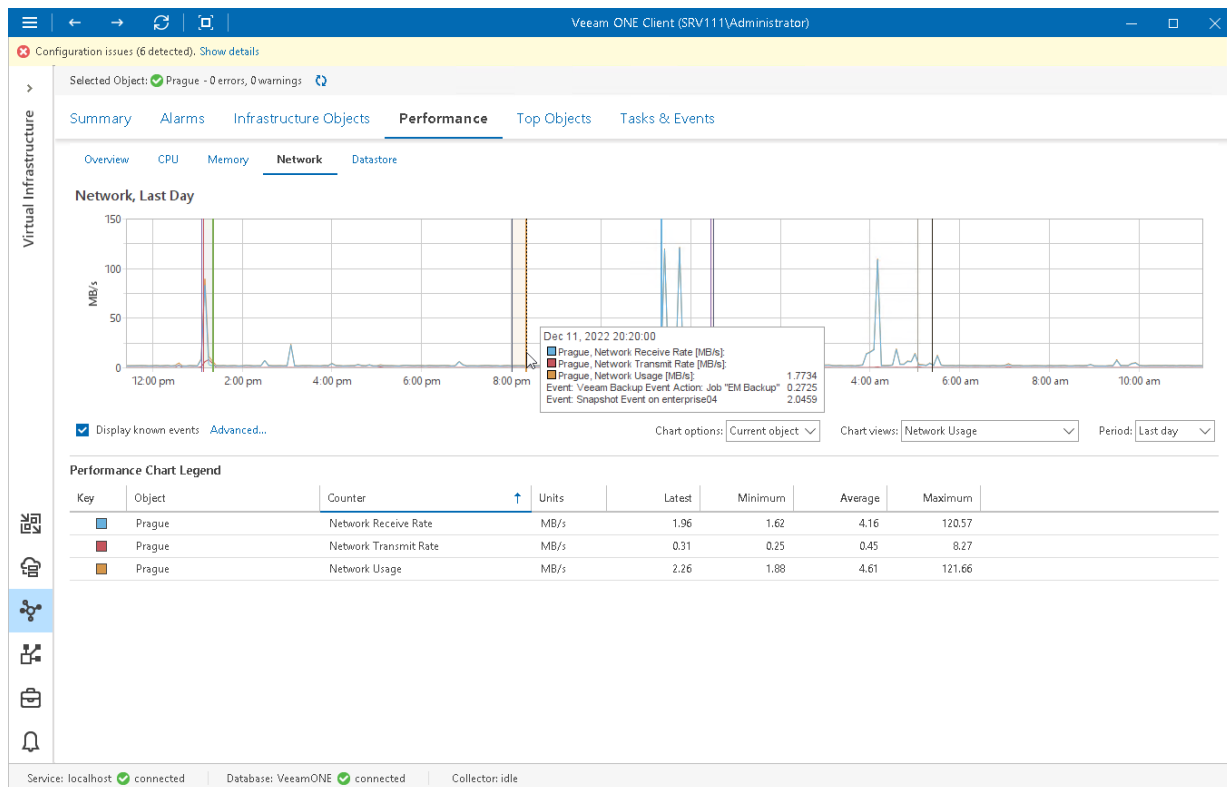
Events are shown as vertical lines crossing the performance graphs. To learn more about an event, hover the mouse cursor over it to see a tooltip, or click the line in the graph. The **Events Description** window will provide detailed information about the event.
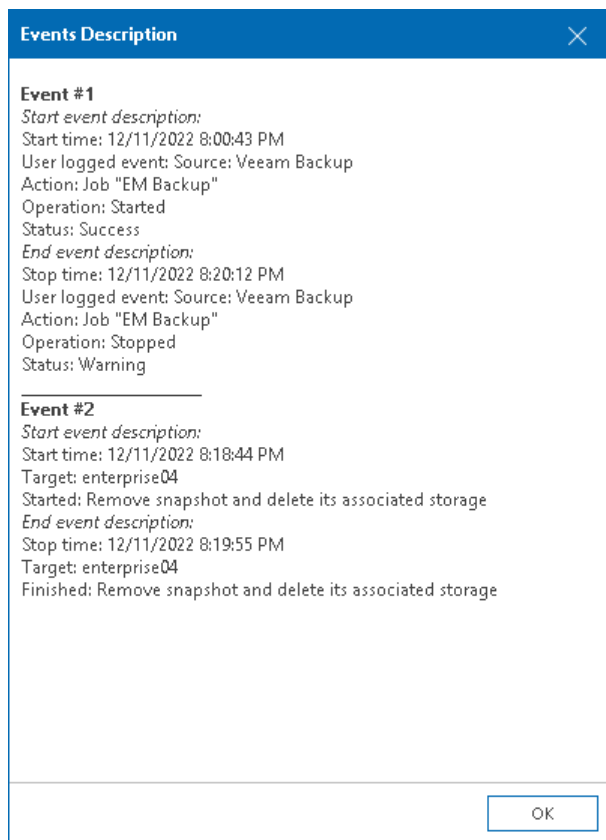
> **NOTE:**
>
> The **Display known events** option is available only for time intervals not greater than 3 days. You will not be able to view events on the performance chart if a longer time interval is selected.
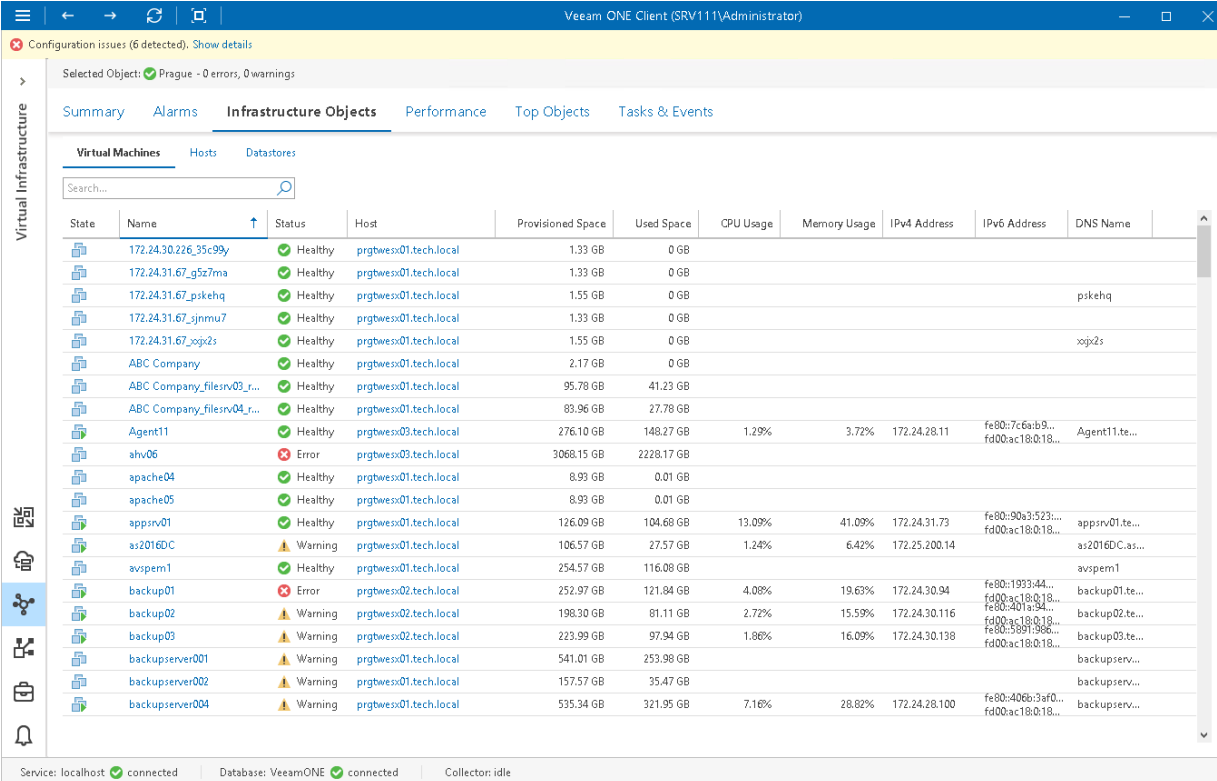
VMware vSphere Virtual Machines

You can view the list of VMs within a virtual infrastructure container — on a host, on a datastore, in a folder and so on.

To view the list of VMs:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure container.

4. Open the **Infrastructure Objects** tab and navigate to **Virtual Machines**.

5. To find the necessary VM by name, use the **Search** field at the top of the list.

6. Click column names to sort VMs by a specific parameter.

   For example, to view what VMs are consuming the greatest amount of memory, you can sort VMs in the list by **Memory Usage**.

For every VM in the list, the following details are available:

- **State** — state of the VM (*powered on*, *powered off*, *suspended*)

- **Name** — name of the VM

- **Status** — current status of the VM in terms of alarms (*healthy*, *warning* or *error*)

- **Host** — name of the host on which the VM resides

- **Provisioned Space** — amount of storage space provisioned for the VM

- **Used Space** — amount of storage space actually used for storing VM files (for VMs with thin provisioned disks, this value is normally less than *Provisioned Space*)

- **CPU Usage** — amount of actively used virtual CPU as a percentage of total available CPU resources

- **Memory Usage** — amount of actively used memory resources as a percentage of configured VM memory

- **IP V4 Address** — IP v4 address assigned to the VM

- **IP V6 Address** — IP v6 address assigned to the VM

- **DNS Name** — DNS name of the VM

- **vCPU** — number of virtual CPUs configured for the VM

- **Assigned Memory** — amount of virtual memory allocated for the VM

- **Guest OS** — guest operating system installed in the VM

- **VMware Tools** — state of VMware Tools

- **Hardware Version** — hardware version of the VM

You can choose what columns to show or hide in the **Virtual Machines** table:

- To hide one or more columns, right-click the table header, and clear check boxes next to the corresponding data fields.

- To make hidden columns visible, right-click the table header, and select check boxes next to the corresponding data fields.

VMware vSphere Hosts

You can view the list of ESXi hosts in your VMware vSphere infrastructure — on vCenter Server or in a datacenter.

To view the list of hosts:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure container.

4. Open the **Infrastructure Objects** tab and navigate to **Hosts**.

5. To find the necessary host by name, use the **Search** field at the top of the list.

6. Click column names to sort hosts by a specific parameter.

   For example, to view hosts with the greatest number of VMs, you can sort VMs in the list by **VM Count**.

For every host in the list, the following details are available:

- **Object** — name of the host

- **Parent Object** — name of the parent infrastructure object

- **CPU Count** — number of CPU cores on the host

- **CPU Frequency** — frequency of the host CPU core in GHz

- **Memory Size** — amount of physical memory available on the host

- **VM Count** — number of VMs that reside on the host

You can choose what columns to show or hide in the **Hosts** table:

- To hide one or more columns, right-click the table header, and clear check boxes next to the corresponding data fields.

- To make hidden columns visible, right-click the table header, and select check boxes next to the corresponding data fields.

VMware vSphere Datastores

You can view the list of datastores in your VMware vSphere infrastructure — on vCenter Server or in a datacenter.

To view the list of datastores:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure container.

4. Open the **Infrastructure Objects** tab and navigate to **Datastores**.

5. To find the necessary datastore by name, use the **Search** field at the top of the list.

6. Click column names to sort datastores by a specific parameter.

   For example, to view what datastores have the greatest amount of free space, you can sort datastores in the list by **Free Space**.

For every host in the list, the following details are available:

- **Object** — name of the datastore

- **Parent Object** — name of the parent object in the infrastructure

- **File System** — type of the file system on the datastore

- **Capacity** — total capacity of the datastore

- **Free Space** — amount of available free space on the datastore

- **VM Count** — number of VMs that reside on the datastore

You can choose what columns to show or hide in the **Hosts** table:

- To hide one or more columns, right-click the table header, and clear check boxes next to the corresponding data fields.

- To make hidden columns visible, right-click the table header, and select check boxes next to the corresponding data fields.

VMware vSphere Top Objects

The Top Objects dashboards help you detect VMs and hosts consuming the most and the least amount of resources in the selected virtual infrastructure segment:

- **Top vSphere VMs** dashboard displays top VM consumers in terms of CPU, memory, datastore, network usage, memory swapped, active snapshot size, active snapshot age and the number of existing snapshots.

- **Top vSphere Hosts** dashboard displays top host consumers in terms of CPU, memory, datastore, network usage and swapped memory.

- **Bottom vSphere Hosts** dashboard displays least loaded hosts in terms of CPU, memory, datastore, network and memory swap used.

  You can use this dashboard to choose hosts where you can deploy new VMs or to which you can move existing VMs.

To detect the most and the least loaded hosts or VMs:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Monitor.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure container.

4. Open the **Top Objects** tab and switch to the necessary dashboard — **Top vSphere VMs**, **Top vSphere Hosts** or **Bottom vSphere Hosts**.

5. At the top left corner of the dashboard, click the **Change Options** link.

   a. In the **Interval** field, set the time interval for which resource utilization statistics must be analyzed.

   b. In the **VMs to display/Hosts to display** field, specify the number of objects to display on the dashboard.

6. At the top left corner of the dashboard, click the **Select Counters** link.

   a. In the **Select Counters** window, choose metrics that must be included in the dashboard.

      Press and hold the `[SHIFT]` or `[CTRL]` key on the keyboard to select multiple counters.

b. Click **OK**.

Host Hardware State

You can monitor the health of ESXi host hardware components. Veeam ONE collects sensor details for chassis, memory, power, processors, software components, storage, system, watchdog, fan, temperature, voltage and other components.

To monitor the health status of host hardware components:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary host.

4. Open the **Hardware** tab.
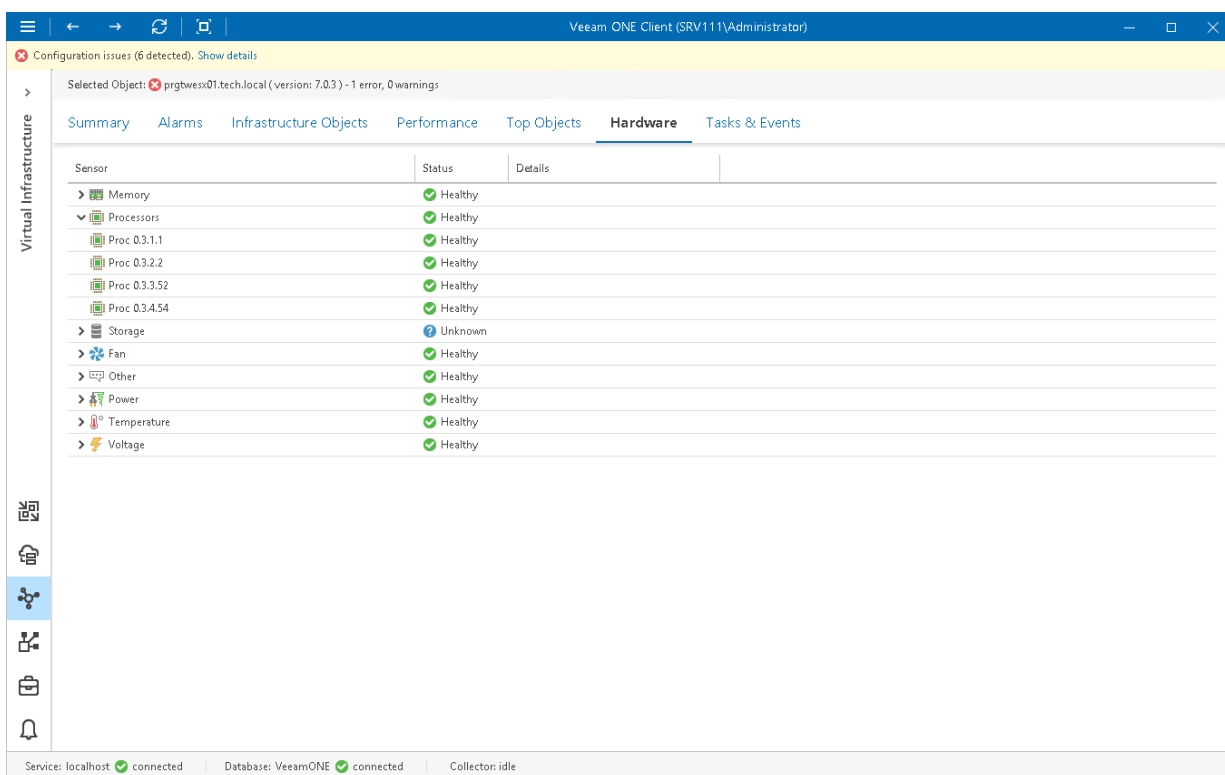
The color of the status indicator changes depending on the state of the corresponding component for a standalone host and on the status of a triggered vCenter Server alarm:

- *Green* — the subsystem is functioning properly.

- *Yellow* and *Red* — the performance threshold is exceeded, performance has gone down or the subsystem has stopped operating.

VMware Remote Console (VMRC)

You can access the VMware Remote Console (VMRC) right from the Veeam ONE Client interface. From within the VMware Remote Console, you can isolate the root cause of VM performance problems and perform management tasks — for example, restart an unresponsive VM.

This option requires no additional software installed on the Veeam ONE server and is available for both Window-based and Linux-based OS's.

Accessing VMware Remote Console

To access the VMware Remote Console:

1. Open Veeam ONE Client.

    For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, right-click the necessary VM and select **Open Console** from the shortcut menu.
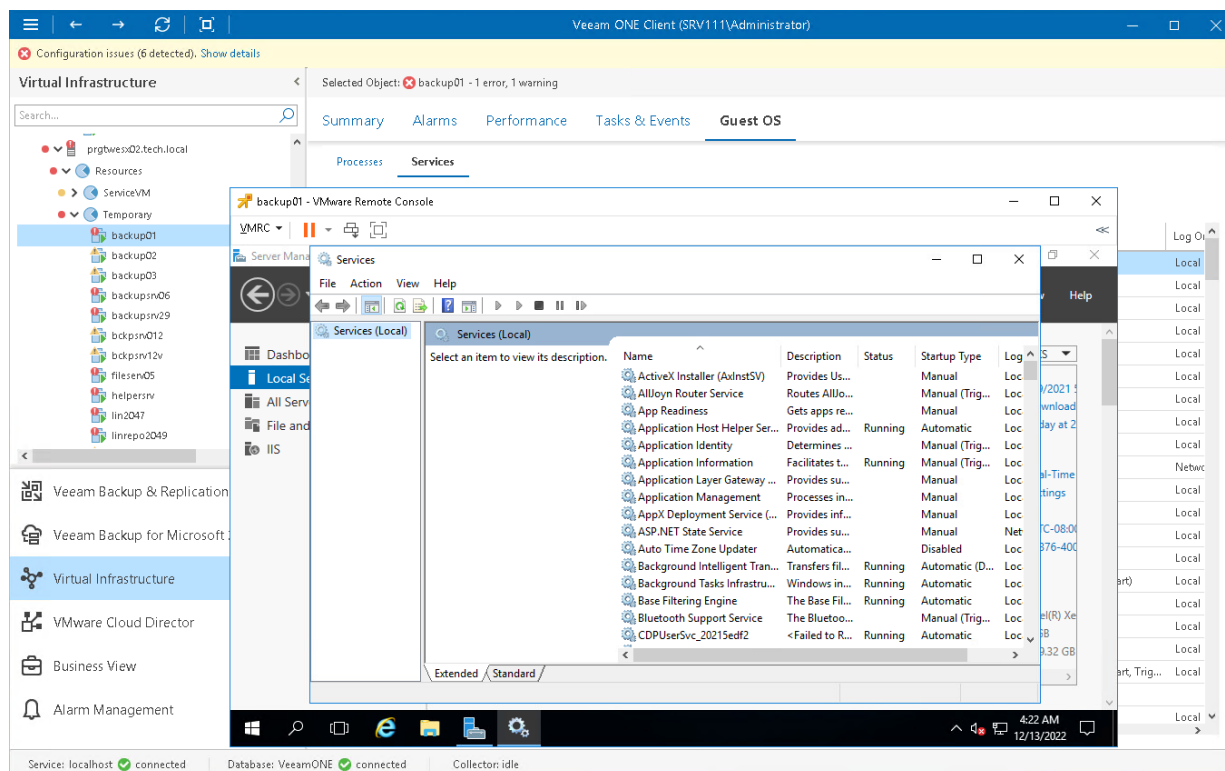
You can use buttons at the top of the VMware Remote Console to manage the VM and change its power state.

To connect to a VM or change the VM power state, you can also right-click the VM in the inventory pane and use one of the following shortcut menu commands:

*   To access the VM using Windows Remote Desktop Connection, choose **Remote Management > Connect to VM**.

*   To change the VM power state, choose **Remote Management** and choose the necessary command.

VMware vSphere In-Guest Processes

You can view and control processes currently running inside a VM or vCenter Server.

- For Windows-based machines, you can view, end or restart processes.

- For Linux-based machines, you can view or end daemons.

Prerequisites

Before viewing in-guest processes, check the following prerequisites:

- For VMs, make sure that VMware Tools are installed.

- For Linux-based machines, make sure that the SSH Server is started.

Viewing In-Guest Processes

To view the list of processes:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure object.

4. Open the **Guest OS** tab and navigate to **Processes**.

5. Provide OS authentication credentials (user name and password) to access the list of running processes.

Every process is described with a set of counters that are presented as column headings. You can add or remove counters to monitor running processes:

1. In the upper right corner of the **Processes** dashboard, click the **Select Columns** link.

2. In the **Select Columns** window, select check boxes next to counters you want to display.

3. To view the detailed description of a counter, click it in the **Counters** list. The description will be displayed in the lower pane of the window.

You can end unwanted processes running on the VM or create an alarm based on the process state or object performance:

- [For Windows-based machines] To end a process, select it in the list and click the **Kill Process** button, or right-click a necessary process and select **Kill Process** from the shortcut menu.

- [For Linux-based machines] To end a daemon, select it in the list and click the **Kill Process** button and choose one of the following options:

  o **Hangup** — to send the `SIGHUP` signal

  o **Kill** — to send the `SIGKILL` signal

  o **Terminate** — to send the `SIGTERM` signal

  You can also right-click a necessary process and select **Kill Process** and choose the necessary option from the shortcut menu.

- [For Windows-based machines] To create an alarm, select one or more processes in the list, click the **Create Alarm** button, and select the type of rule on which the alarm must be based. For more information on alarm rules, see section Alarm Rules of the Veeam ONE Working with Alarms Guide.

VMware vSphere In-Guest Services

You can view and control services currently running inside a VM or vCenter Server.

- For Windows-based machines, you can view, start, stop and restart services, and create alarms based on retrieved services.

- For Linux-based machines, you can view or end services.

Prerequisites

Before viewing in-guest services, check the following prerequisites:

- For VMs, make sure that VMware Tools are installed.

- For Linux-based machines, make sure that the SSH Server is started.

Viewing In-Guest Services

To view the list of services:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure object.

4. Open the **Guest OS** tab and navigate to **Services**.

5. Provide OS authentication credentials (user name and password) to access the list of running services.

You can start, stop and restart a running service, or create an alarm based on the service state or object performance:

- To restart a service, click the **Restart** button, or right-click a necessary service and select **Restart** from the shortcut menu.

- To disconnect from guest OS, click the **Disconnect** button.

- [For Windows-based machines] To create an alarm, select a service in the list, click the **Create Alarm** button, and select the type of rule on which the alarm must be based. For details on alarm rules, see section Alarm Rules.

Launching vSphere Client

You can launch vSphere Client or vSphere Web Client from within Veeam ONE Client.

Prerequisites

Before launching vSphere Client, check the following prerequisites:

- The **Open with vSphere Client** option is available only if vSphere Client is installed on the machine where the Veeam ONE Client runs.

- To launch vSphere Client from Veeam ONE Client, you must have the **x86** version of Veeam ONE Client installed.

Launching vSphere Client

To launch the vSphere Client from Veeam ONE Client:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, right-click a vCenter Server or ESXi host and choose **Open with vSphere Client** or **Open with vSphere Web Client** from the shortcut menu.

VMware Cloud Director Monitoring

Veeam ONE Client offers a comprehensive view for the logical and physical layers of the VMware Cloud Director infrastructure. Veeam ONE collects real-time statistics from connected VMware Cloud Director servers and underlying vCenter Servers to help you track provider capacities, monitor resource usage and identify issues that may potentially result in SLA breaches.

With Veeam ONE Client, you can:

1. **Monitor health status of the VMware Cloud Director infrastructure**.

   Start with the **Summary** dashboards to check the health status of the VMware Cloud Director infrastructure and supporting VMware vSphere components.

   View the latest alarms, track pending blocking tasks and expired leases and review the overall state of vApps and VMs provisioned by Cloud Director tenants.

2. **View triggered alarms**.

   Switch to the **Alarms** dashboard to see details on issues and problems occurred in the VMware Cloud Director infrastructure. VMware Cloud Director alarms will notify you on increasing resource usage for provider and organization VDCs, expiring vApp runtime and storage leases, blocking tasks left with no response, and the health status of Cloud Director infrastructure components.

3. **Work with performance charts**.

   Drill down to performance charts to diagnose performance problems and identify resource bottlenecks.

   Track CPU, memory, disk and network performance for underlying hosts, VMs, VM containers, organizations, organization VDCs and vApps.

4. **Monitor Cloud Director capacities and resource usage**.

   Monitor available, allocated and consumed resources to make sure that VMs and vApps have enough allocated CPU, memory and storage resources, and Cloud Director tenants have enough capacities to run their workloads.

5. **Investigate problems from within the guest OS**.

   View the list of in-guest processes to diagnose problems related to a specific service, module or application within the guest OS.

Prerequisites

Before you start monitoring the VMware Cloud Director environment, make sure you have configured connections to Cloud Director servers from which Veeam ONE will collect data. For more information on configuring server connections, see section Connecting VMware Cloud Director Servers of the Veeam ONE Deployment Guide.

VMware Cloud Director Summary Dashboards

VMware Cloud Director summary dashboards serve as the 'launch point' for monitoring the VMware Cloud Director infrastructure state. The dashboards reflect the health status of all VMware Cloud Director infrastructure levels — from VMware Cloud Director cells to separate vApps and VMs.

The following types of summary dashboards are available for VMware Cloud Director infrastructure objects:

- VMware Cloud Director Infrastructure Summary
- Provider VDCs Overview
- Provider VDC Summary
- Organizations Overview
- Organization Summary
- Organization VDC Summary
- vApp Summary
- Virtual Machine Summary

To access a summary dashboard for a VMware Cloud Director infrastructure object or segment:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **VMware Cloud Director**.

3. In the inventory pane, select the necessary infrastructure object or segment.

4. Open the **Summary** tab.

VMware Cloud Director Infrastructure Summary

The VMware Cloud Director infrastructure summary dashboard provides the health status overview for all organizations and child VMware Cloud Director objects.

The dashboard is available for the following infrastructure levels:

- VMware Cloud Director Infrastructure (root node)
- VMware Cloud Director cell
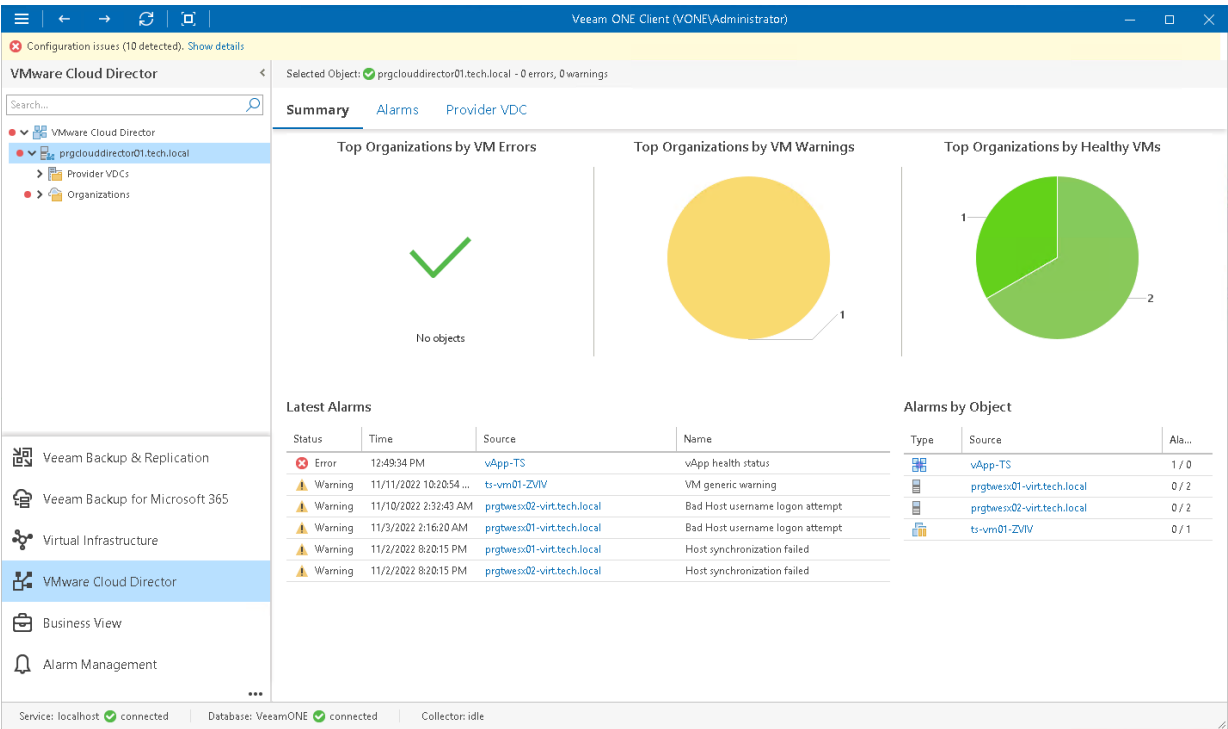
Top Organizations by VM Errors, Top Organizations by VM Warnings, Top Organizations by Healthy VMs

The charts represent organizations with the greatest number of errors, warnings and organizations with no registered alarms. Click a chart segment or a legend label to drill down to the list of alarms with the corresponding status for the selected organization.

Latest Alarms

The list displays the latest 15 alarms for the selected VMware Cloud Director segment. Click a link in the **Source** column to drill down to the list of alarms triggered for a specific VMware Cloud Director infrastructure object.

Alarms by Object

The list displays 15 objects with the greatest number of alarms.

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 error alarms and 1 warning alarm triggered for the object. Click a link in the **Source** column to drill down to the list of alarms related to a specific VMware Cloud Director infrastructure object.

For more information on alarms, see Working with Triggered Alarms.

Provider VDCs Overview

The summary dashboard for the **Provider VDCs** node displays the health status overview for provider virtual datacenters under a VMware Cloud Director cell.
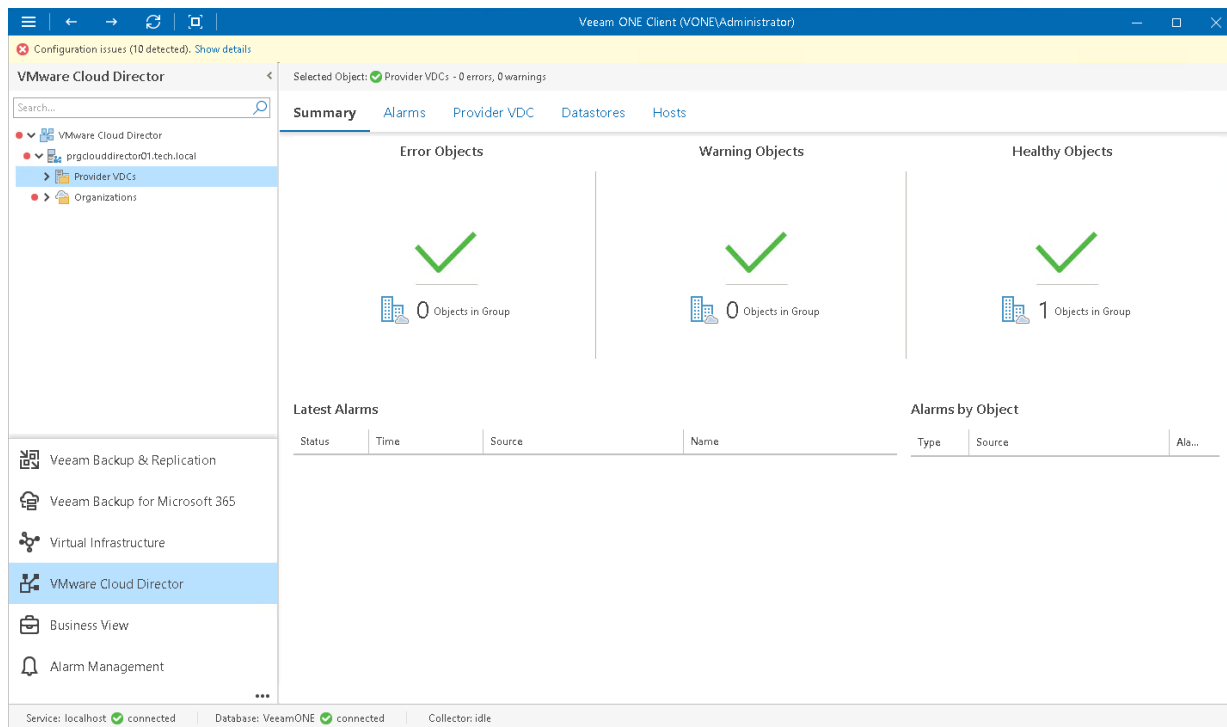
Error Objects, Warning Objects, Healthy Objects

The charts group provider VDCs by their health status.

Every chart reflects the number of provider VDCs with a specific state — provider VDCs with errors (red), provider VDCs with warnings (yellow) and healthy provider VDCs (green). Click the problematic chart to drill down to the list of alarms for VDCs with the chosen health status.

Latest Alarms

The list displays the latest 15 alarms that were triggered for provider VDCs and underlying virtual infrastructure objects (datastores and hosts). Click a link in the **Source** column to drill down to the list of alarms triggered for a specific object.

Alarms by Object

The list displays 15 objects with the greatest number of alarms.

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 error alarms and 1 warning alarm triggered for the object. Click a link in the **Source** column to drill down to the list of alarms related to a specific object.

For more information on alarms, see Working with Triggered Alarms.

Provider VDC Summary

The provider VDC summary dashboard reflects resource utilization analysis results and the health status overview for the chosen provider virtual datacenter and VMware vSphere resources.
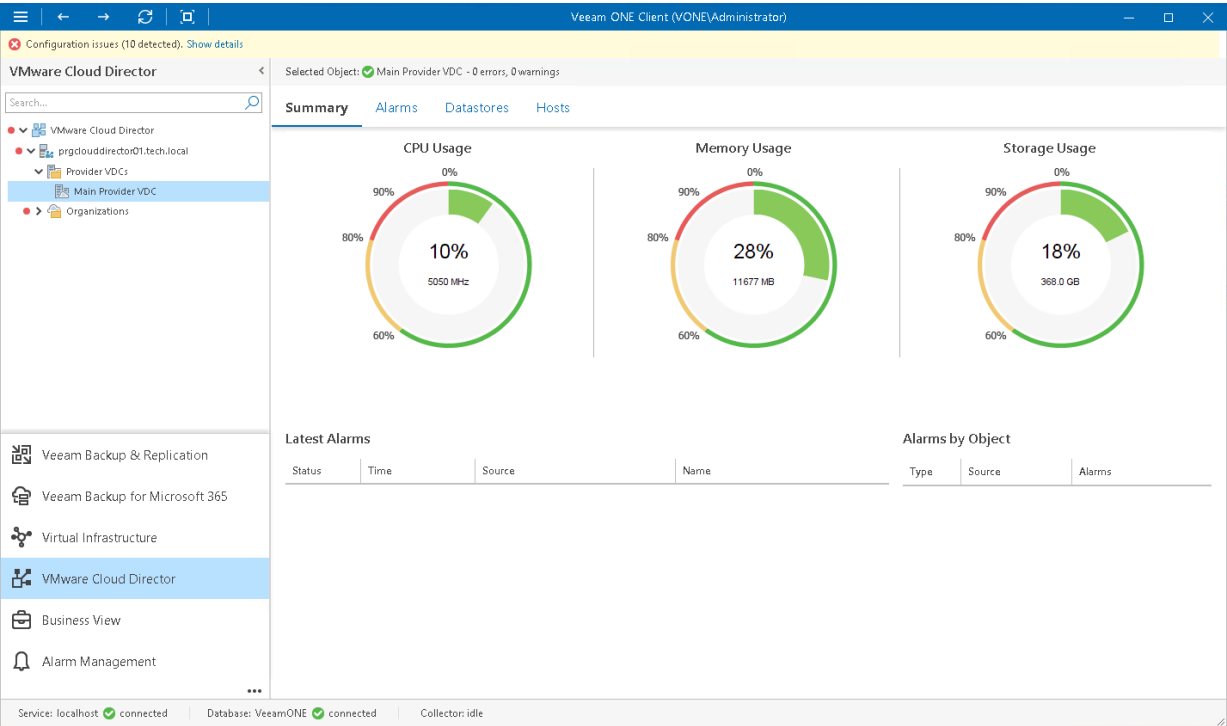
CPU Usage, Memory Usage, Storage Usage

The charts reflect the amount of currently consumed CPU, memory and storage resources for the chosen provider virtual datacenter.

Latest Alarms

The list displays the latest 15 alarms for the provider VDC and underlying virtual infrastructure objects (datastores and hosts). Click a link in the **Source** column to drill down to the list of alarms triggered for a specific object.

Alarms by Object

The section displays the current state of hosts and datastores that provide compute and storage resources for the provider VDC. Information in this section may help you estimate the impact of underlying VMware vSphere objects on the provider VDC and speed up root cause analysis.

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 error alarms and 1 warning alarm triggered for the object. Click a link in the **Source** column to drill down to the list of alarms related to a specific object.

For more information on alarms, see Working with Triggered Alarms.

Organizations Overview

The summary dashboard for the **Organizations** node provides an overview for organizations under the selected VMware Cloud Director cell.
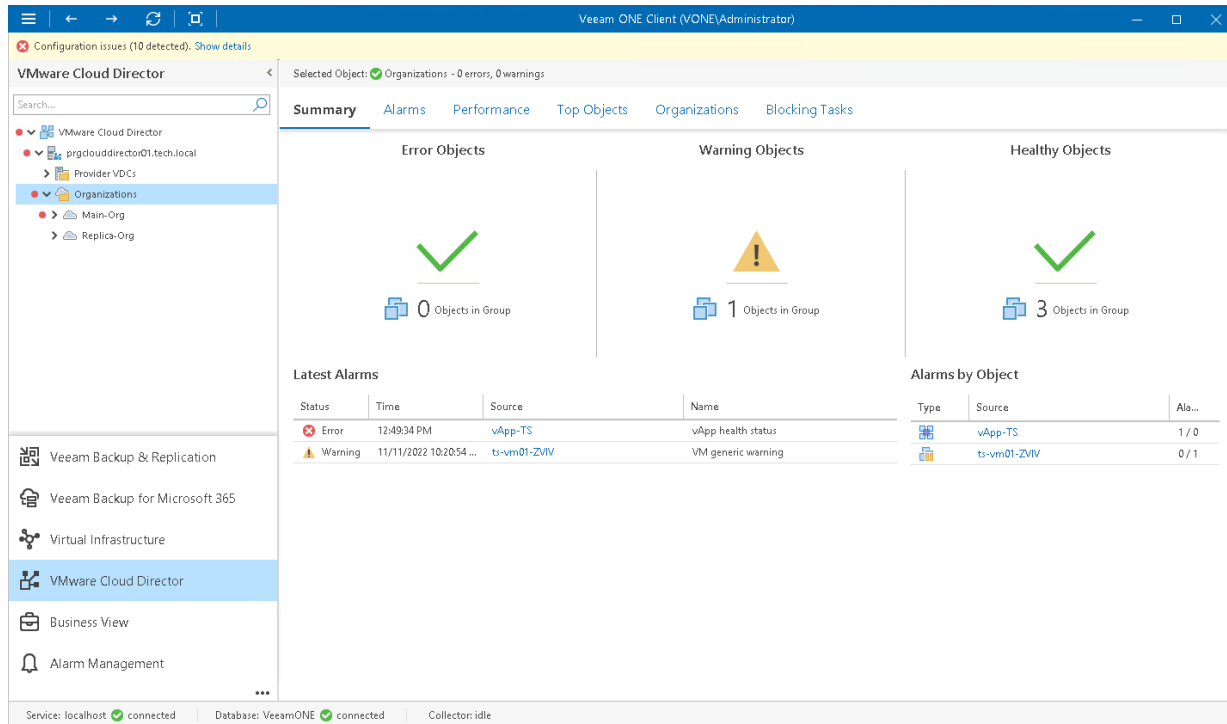
Error Objects, Warning Objects, Healthy Objects

The charts group VMs in organizations by their health status.

Every chart reflects the number of organization VMs with a specific state — VMs with errors (red), VMs with warnings (yellow) and healthy VMs (green). Click the problematic chart to drill down to the list of alarms for VMs with the chosen health status.

Latest Alarms

The list displays the latest 15 alarms that were triggered for organizations, organization VDCs, as well as for VMs and vApps within these organizations. Click a link in the **Source** column to drill down to the list of alarms triggered for a specific object.

Alarms by Object

The list displays 15 objects with the greatest number of alarms.

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 error alarms and 1 warning alarm triggered for the object. Click a link in the **Source** column to drill down to the list of alarms related to a specific object.

For more information on alarms, see Working with Triggered Alarms.

Organization Summary

The organization summary dashboard presents the health status overview for the chosen organization and its child objects.
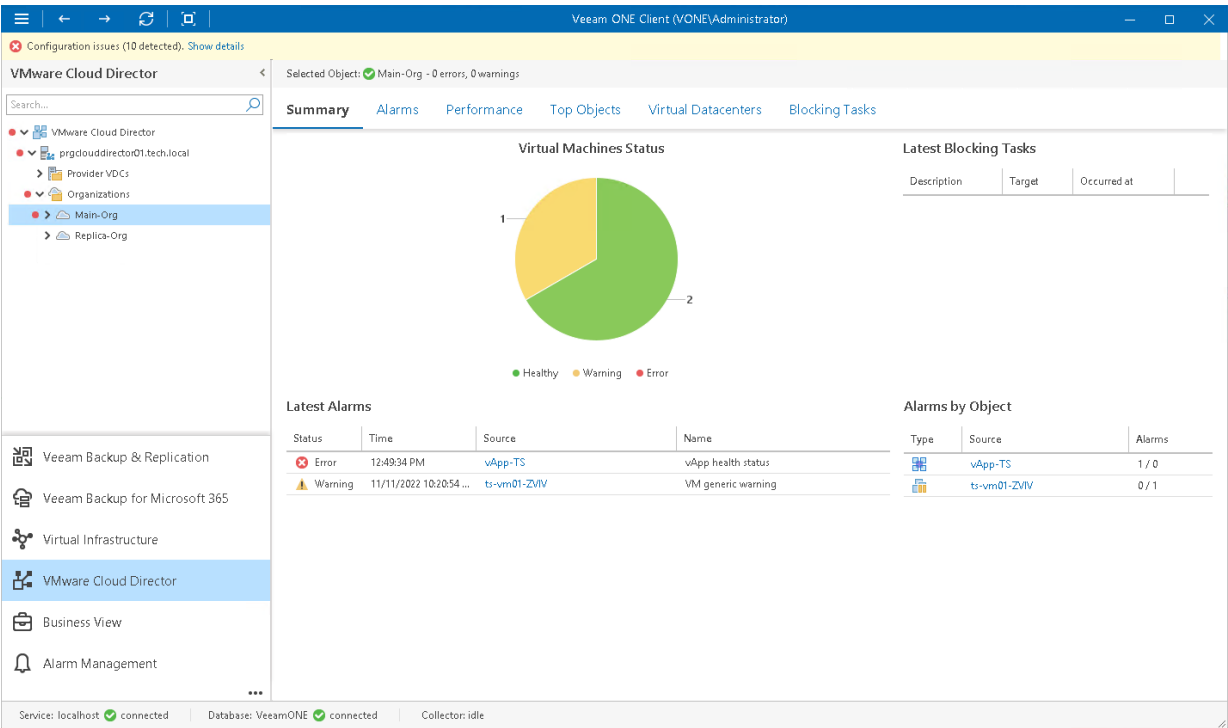
Virtual Machines by State

The chart reflects the summary health status of VMs in the organization.

Every colored segment represents the number of VMs in a certain state — VMs with errors (red), VMs with warnings (yellow) and healthy VMs (green). Click the chart segment or a legend label to drill down to the list of alarms triggered for organization VMs with the chosen health status.

Latest Blocking Tasks

The list displays the latest 15 suspended operations that require approval before the operation will resume.

For each pending operation, Veeam ONE Client provides a description, the organization for which the operation was initiated and the time when the operation was initiated by an organization user. Blocking tasks that expired with timeout are not included in the list.

Latest Alarms

The list displays the latest 15 alarms for the organizations, organization VDCs, as well as for VMs and vApps within these organizations. Click a link in the **Source** column to drill down to the list of alarms triggered for a specific object.

Alarms by Object

The list displays 15 objects with the greatest number of alarms.

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 error alarms and 1 warning alarm triggered for the object. Click a link in the **Source** column to drill down to the list of alarms related to a specific object.

For more information on alarms, see Working with Triggered Alarms.

Organization VDC Summary

The organization VDC summary dashboard presents resource utilization analysis and the health status overview for the chosen organization virtual datacenter.
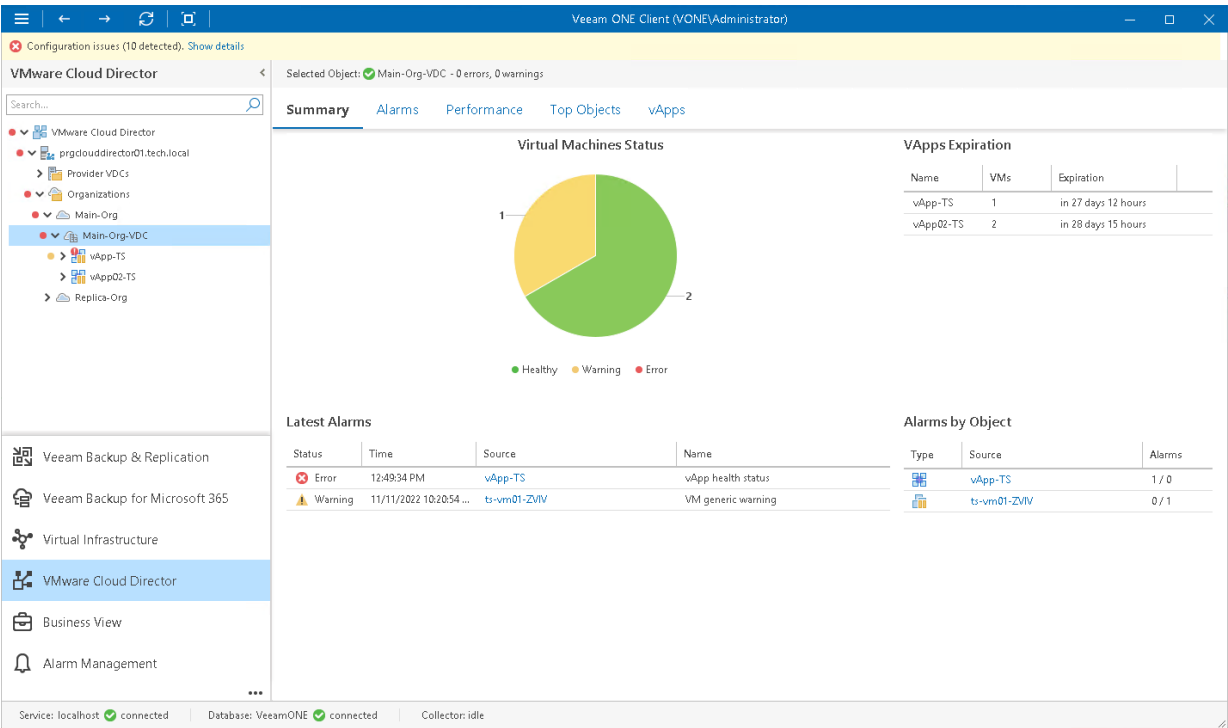
Virtual Machines by State

The chart reflects the summary health status of VMs in the organization virtual datacenter.

Every colored segment represents the number of VMs in a certain state — VMs with errors (red), VMs with warnings (yellow) and healthy VMs (green). Click a chart segment or legend label to drill down to the list of alarms triggered for VMs with the chosen health status.

VApps Expiration

The list displays vApps whose runtime lease or storage lease has expired. The list shows 15 items with the recently expired lease, and is only populated if the storage lease cleanup policy for the organization is set to **Move to Expired Items**.

Latest Alarms

The list displays the latest 15 alarms for the organization VDC and its child objects (vApps and VMs). Click a link in the **Source** column to drill down to the list of alarms triggered for a specific object.

Alarms by Object

The list displays 15 objects with the greatest number of alarms.

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 error alarms and 1 warning alarm triggered for the object. Click a link in the **Source** column to drill down to the list of alarms related to a specific object.

For more information on alarms, see Working with Triggered Alarms.

vApp Summary

The vApp summary dashboard provides a health status overview for the chosen vApp and VMs in this vApp.
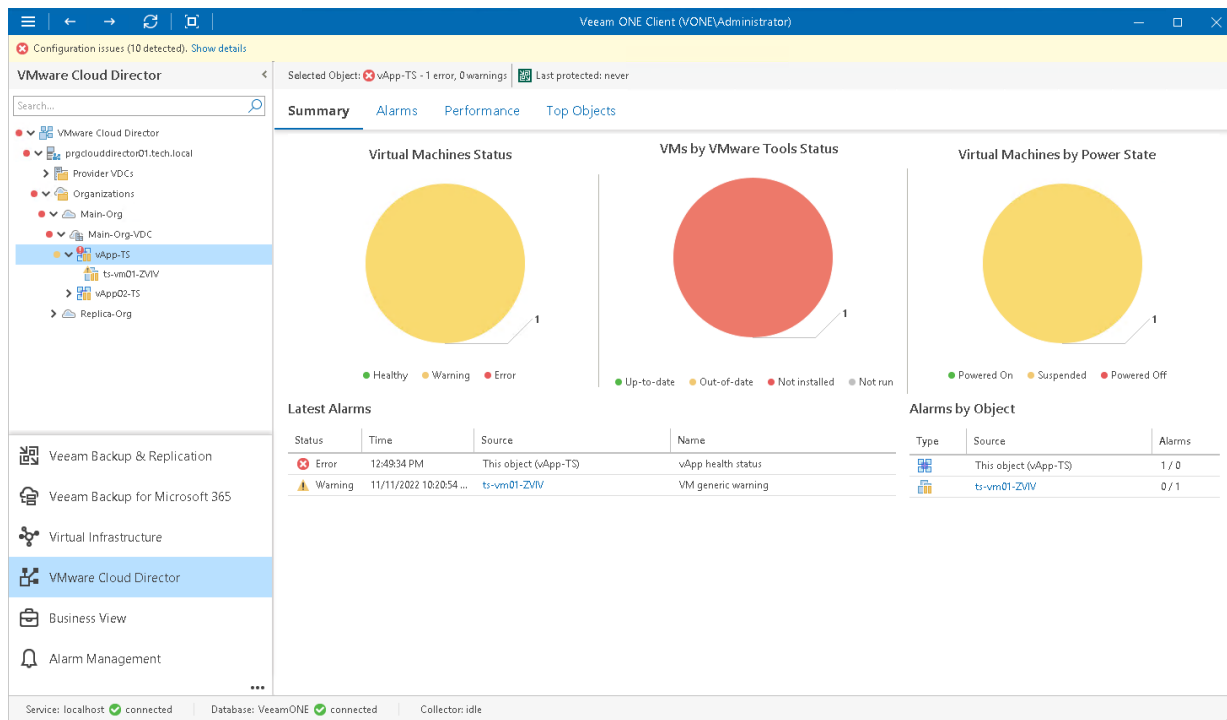
Virtual Machines by State

The chart groups VMs in the vApp by health status.

Every colored segment represents the number of VMs in a certain state — VMs with errors (red), VMs with warnings (yellow) and healthy VMs (green). Click a chart segment or a legend label to drill down to the list of alarms triggered for VMs with the chosen health status.

VMs by VMware Tools Status

The chart groups VMs in the vApp by VMware Tools status.

Every colored segment reflects the number of VMs with a specific state — VMware Tools not installed (red), VMware Tools need to be updated to the latest version (yellow), VMware Tools up-to-date and running (green) and VMware Tools installed but not running for some reason (grey).

Virtual Machines by Power State

The chart groups VMs in the vApp by power state. Every colored segment reflects the number of VMs with a specific power state — powered off VMs (red), suspended VMs (yellow) and powered on VMs (green).

Latest Alarms

The list displays the latest 15 alarms triggered for the vApp and VMs that belong to it. Click a link in the **Source** column to drill down to the list of alarms triggered for a specific object.

Alarms by Object

The list displays 15 objects with the greatest number of alarms.

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 error alarms and 1 warning alarm triggered for the object. Click a link in the **Source** column to drill down to the list of alarms related to a specific object.

For more information on alarms, see Working with Triggered Alarms.

Virtual Machine Summary

The VM summary dashboard provides the health status and performance overview for the selected VM. In addition, this dashboard shows the state of objects that can affect the VM performance — the parent host and the datastores where VM files are located.
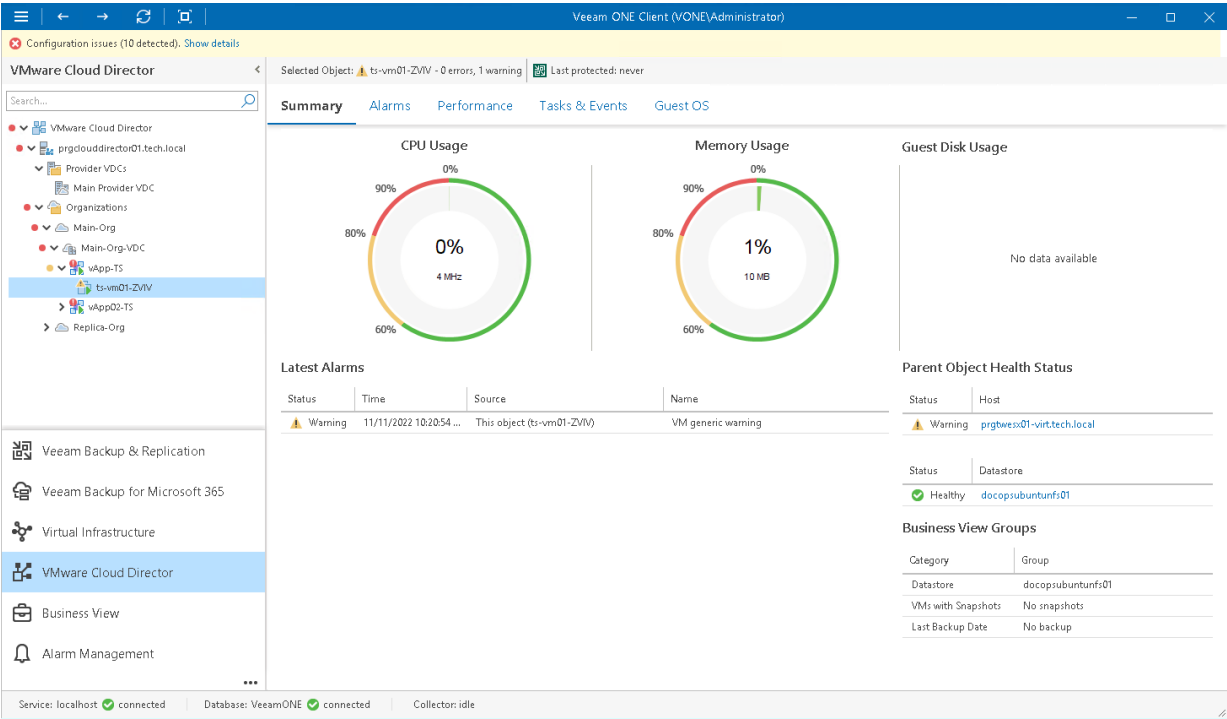
Selected Object

The section at the top of the dashboard shows the VM health status (number of triggered warnings and errors) and the date when the latest backup or replica restore point was created for the VM with Veeam Backup & Replication.

CPU Usage, Memory Usage

The charts display the amount of CPU and memory resources currently consumed by the VM.

Guest Disk Usage

The chart displays the amount of available and used guest disk space with a breakdown by disks. By default, 5 guest disks with the greatest amount of used space are displayed.

Use the **Disks to show** list to change the number of disks to display on the chart. Click the **View all disks** link to view details for all guest disks. In the **Guests Disks** window, you can suppress *Guest disk space* alarms for specific disks. To suppress alarms for a disk, select the **Suppress alarms** check boxes next to the disk name.

> **NOTE:**
>
> Details on the guest disk usage are available only for VMs with VMware Tools installed.

Latest Alarms

The list displays the latest 15 alarms for the VM.

Parent Object Health Status

The section displays the current state of the host where the VM resides and the state of datastores that host VMs files. Information available in this section may help you estimate how the state of parent objects impacts VM performance. Click the host or datastore link to drill down to the list of alarms for the host or datastore.

For more information on alarms, see Working with Triggered Alarms.

Business View Groups

The section displays the list of categories and groups to which the VM is included.

VMware Cloud Director Alarms

Veeam ONE includes a set of alarms for monitoring VMware Cloud Director health status and resource usage. Predefined VMware Cloud Director alarms are configured to warn you about events or issues that can cause disruptions in cloud service availability:

- Expiring runtime and storage leases for customers' vApps

- Pending blocking tasks left without timely response

- Breached thresholds for compute, storage and network resource utilization at various layers of the VMware Cloud Director infrastructure

- Changes in health status of VMware Cloud Director components

To view the list of alarms for VMware Cloud Director infrastructure:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **VMware Cloud Director**.

3. In the inventory pane, select the necessary infrastructure node.

4. Open the **Alarms** tab.

In addition to Cloud Director-specific alarms, the dashboard displays alarms triggered for VMware vSphere infrastructure components. Thus you can monitor both the logical cloud layer and the state of underlying VMware vSphere infrastructure components.

For more information on alarms, see Working with Triggered Alarms.

VMware Cloud Director Performance Charts

To facilitate the troubleshooting process and quickly identify resource bottlenecks, you can drill down to performance charts right from the VMware Cloud Director view:

- Overall Chart

- CPU Performance Chart

- Memory Performance Chart

- Datastore Performance Chart

- Network Performance Chart

- Virtual Disks Performance Chart

You can track performance metrics for separate VMs within an organization, for a VM container (such as vApp, organization or organization VDC) and for hosts that support provider VDCs.

To drill down to a performance chart from the VMware Cloud Director view, do one of the following:

- In the VMware Cloud Director inventory, select an infrastructure object (VM or VM container) and go to the necessary performance chart tab in the information pane.

- Open the **Alarms** dashboard. In the list of alarms, select an alarm for the necessary VM or host. Click **Performance** in the **Actions** pane on the right and choose the required performance chart.

- Open the **Alarms** dashboard. In the list of alarms, select an alarm for the necessary VM or host. Right-click the alarm, choose **Performance** and select necessary performance chart from the shortcut menu.

> **NOTE:**
>
> When you open a performance chart for a host, Veeam ONE Client automatically switches to the Virtual Infrastructure.

For performance charts in the VMware Cloud Director view, Veeam ONE supports a similar set of actions as for virtual infrastructure performance charts: you can change chart views and set time intervals, define objects to show on charts or select custom metrics. For more information on customizing performance charts, see Customizing VMware vSphere Performance Charts.

VMware Cloud Director Resources

Veeam ONE Client includes a set of dashboards for monitoring resource allocation and utilization at the VMware Cloud Director infrastructure and service layers. These dashboards help you compare VMware Cloud Director capacities to the current level of resource usage and estimate the size of virtual datacenter capacities required to maintain customer workloads.

Provider VDCs

You can view a list of provider virtual datacenters configured within a Cloud Director cell:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **VMware Cloud Director**.

3. In the inventory pane, select a VMware Cloud Director cell or the **Provider VDCs** node.

4. Open the **Provider VDC** tab.
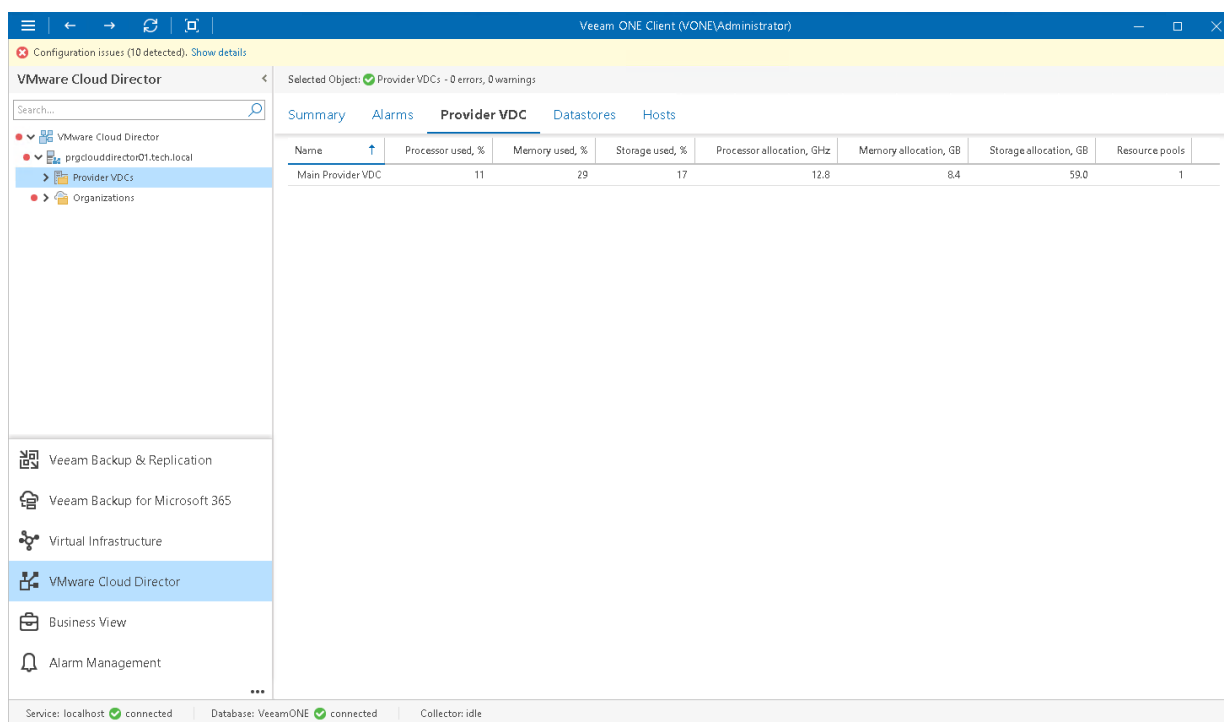
For every provider VDC in the list, the following details are shown:

- **Name** — name of the provider virtual datacenter

- **Processor used, %** — amount of provider VDC CPU resources that is currently used by organizations

- **Memory used, %** — amount of provider VDC memory resources that is currently used by organizations

- **Storage used, %** — amount of provider VDC storage resources that is currently used by organizations

- **Processor allocation, GHz** — amount of provider VDC CPU resources that is committed to organization VDCs

- **Memory allocation, GB** — amount of provider VDC memory resources that is committed to organization VDCs

- **Storage allocation, GB** — amount of provider VDC storage resources that is committed to organization VDCs

- **Resource pools** — number of resource pools that are backing compute resources of the provider VDC

You can click column names to sort provider VDCs by a specific parameter. For example, to identify what provider VDCs are running out of storage resources, you can sort provider VDCs in the list by **Storage used, %**.

Datastore Resources

You can view a list of datastores attached to provider virtual datacenters:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **VMware Cloud Director**.

3. In the inventory pane, select a provider VDC node to view datastores attached to this provider VDC. Select the **Provider VDCs** node to view datastores attached to all provider VDCs within the VMware Cloud Director cell.

4. Open the **Datastores** tab.

For every datastore in the list, the following details are shown:

- **Name** — name of the datastore (you can click the name to switch to the summary dashboard for the datastore)

- **Type** — datastore file system (*VMFS* or *NFS*)

- **Used Storage, GB** — amount of storage resources currently consumed on the datastore

- **Provisioned Storage, GB** — amount of space provisioned to VMs. If VMs are created using thin provisioning, some of the provisioned space might not be used

- **Requested Storage, GB** — amount of provisioned storage used by Cloud Director-managed objects. If thin provisioning is enabled on Cloud Director, some of the requested space might not be used

- **Provider VDC** — number of provider VDCs to which the datastore is attached

- **vCenter** — name of the vCenter Server that manages the datastore

Host Resources

You can view a list of hosts that are backing a provider virtual datacenter:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **VMware Cloud Director**.

3. In the inventory pane, select a provider VDC node.

4. Open the **Hosts** tab.
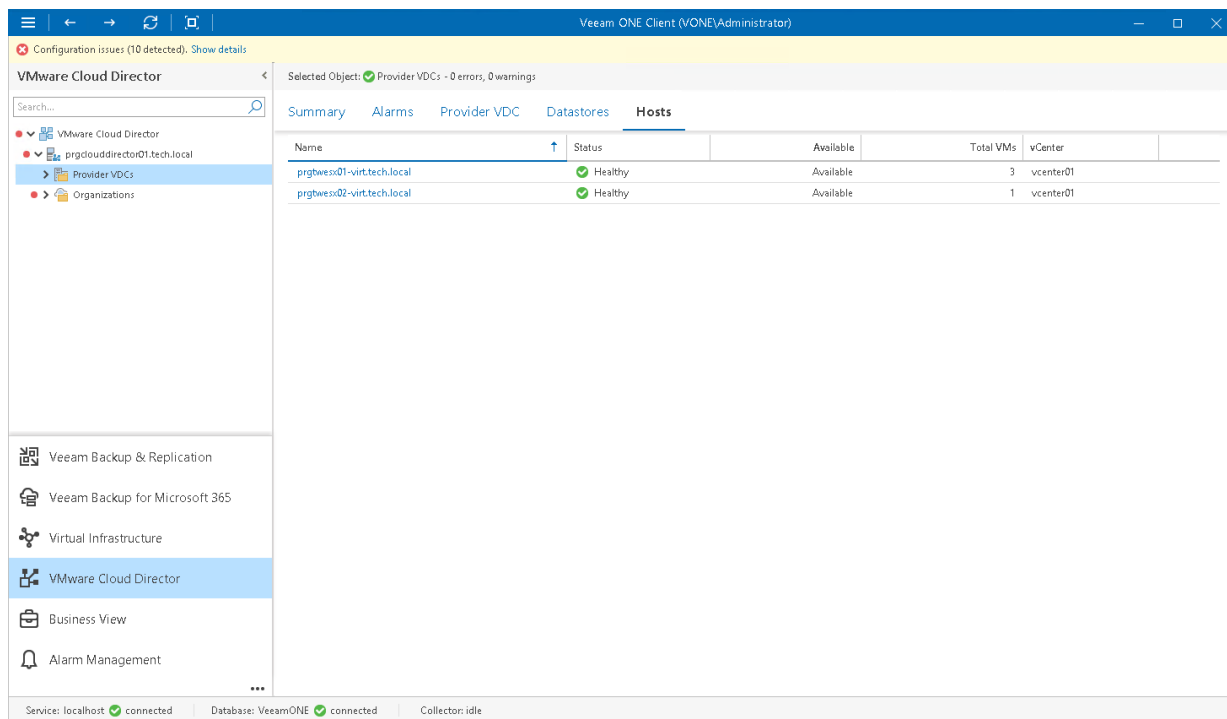
For every host in the list, the following details are shown:

- **Name** — name of the host (you can click the name to switch to the summary dashboard for the host)

- **Status** — health status of the host (*Healthy*, *Warning* or *Error*)

- **Available** — flag indicating whether the host is available to VMware Cloud Director

- **Total VMs** — number of VMs currently registered on the host

- **vCenter** — name of the vCenter Server that manages the host

Organizations

You can view a list of organizations within the VMware Cloud Director cell:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **VMware Cloud Director**.

3. In the inventory pane, select the **Organizations** node.

4. Open the **Organizations** tab.
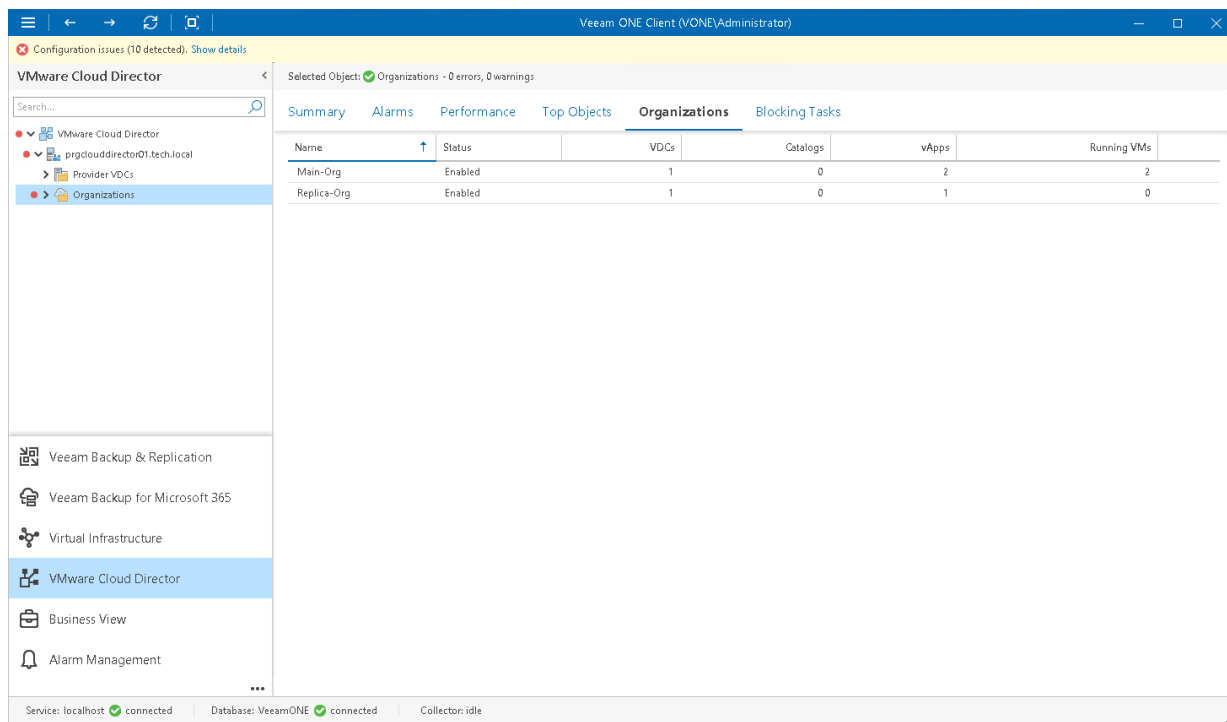
For every organization in the list, the following details are shown:

- **Name** — name of the organization

- **Status** — status of the organization indicating whether the organization is enabled (that is, users can log in to the organization and the current user sessions can run)

- **VDCs** — number of virtual datacenters configured for the organization

- **Catalogs** — number of organization's catalogs, both shared and non-shared

- **vApps** — number of vApps configured for the organization (including expired vApps)

- **Running VMs** — number of VMs currently running within this organization

Organization VDCs

You can view a list of VDCs configured for a specific organization:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **VMware Cloud Director**.

3. In the inventory pane, select an organization node.

4. Open the **Virtual Datacenters** tab.
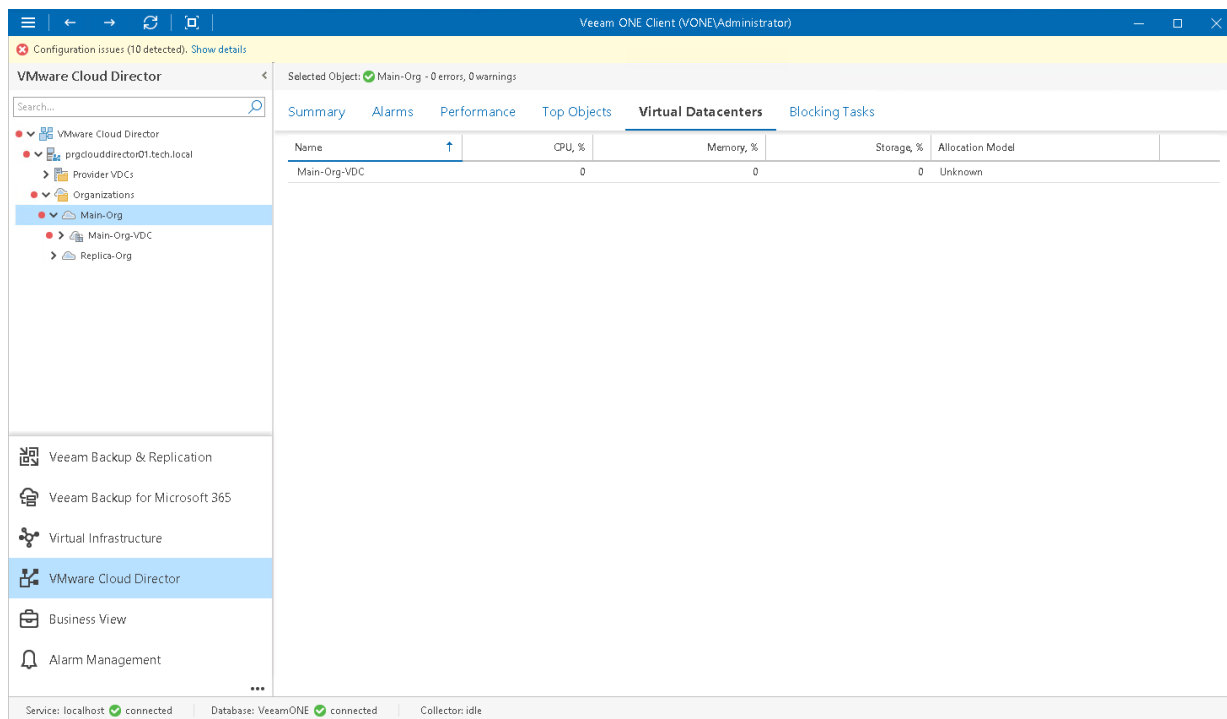
For every virtual datacenter in the list, the following details are shown:

- **Name** — name of the organization VDC

- **CPU, %** — amount of CPU resources currently used by the organization (as a percentage of resources allocated to the organization within this virtual datacenter)

- **Memory, %** — amount of memory resources currently used by the organization (as a percentage of resources allocated to the organization within this virtual datacenter)

- **Storage, %** — amount of storage resources currently used by the organization (as a percentage of resources allocated to the organization within this virtual datacenter)

- **Allocation Model** — allocation model for the virtual datacenter (*Allocation Pool*, *Reservation Pool*, *Pay-as-you-go*, *Flex*)

vApps

You can view a list of virtual applications created within a specific organization VDC:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **VMware Cloud Director**.

3. In the inventory pane, select an organization VDC node.

4. Open the **vApps** tab.
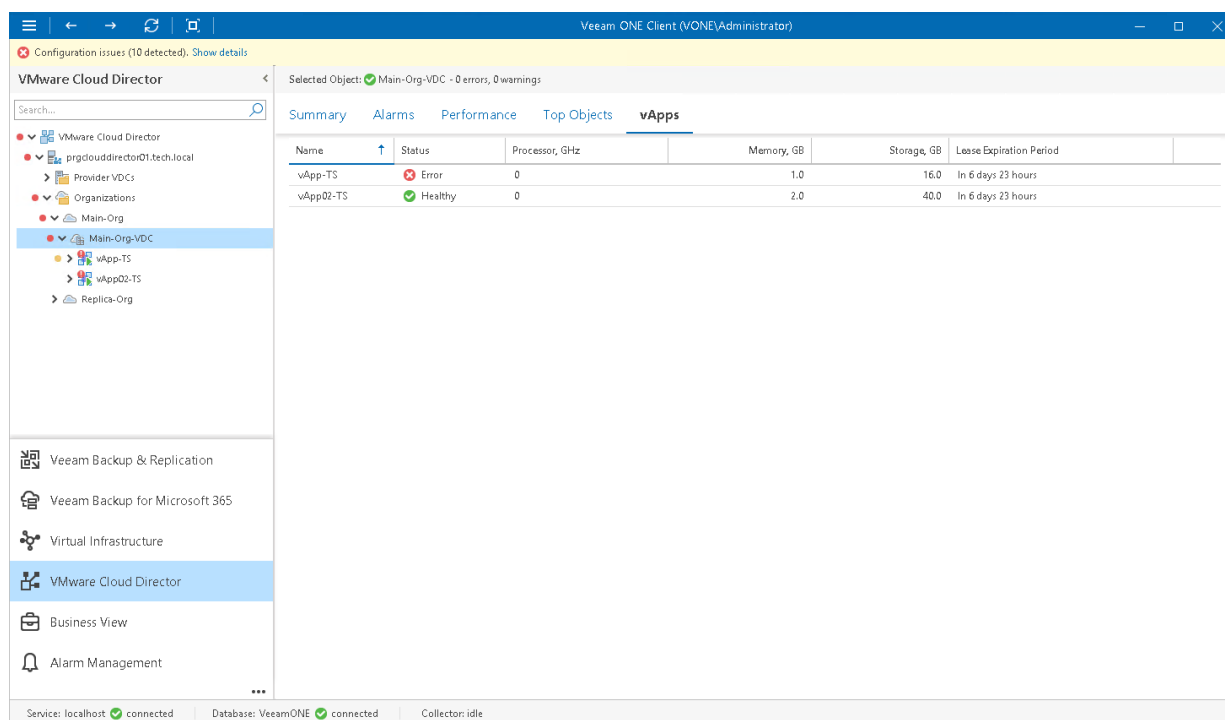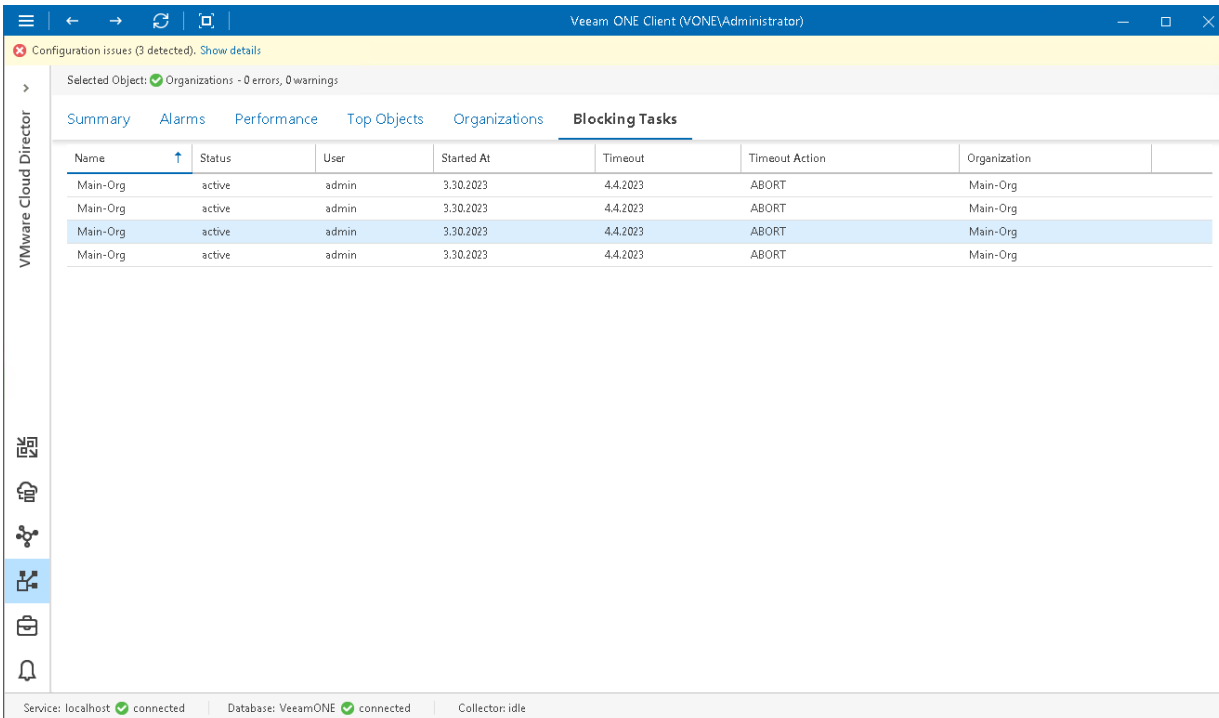
For every vApp in the list, the following details are shown:

- **Name** — name of the vApp

- **Status** — health status of the vApp

- **Processor, GHz** — amount of CPU resources currently consumed by the vApp and all its VMs

- **Memory, GB** — amount of memory resources currently consumed by the vApp and all its VMs

- **Storage, GB** — amount of storage resources currently consumed by the vApp and all its VMs

- **Lease Expiration Period** — amount of time left before the vApp runtime lease expires (for running vApps), or amount of time left before the vApp storage lease expires (for inactive vApps and templates)

Tracking Blocking Tasks

You can track pending blocking task requests for a specific organization or all organizations at once:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **VMware Cloud Director**.

3. In the inventory pane, select an organization node to view blocking tasks pending for this organization.

   Select the **Organizations** node to view blocking tasks pending for all organizations within this VMware Cloud Director cell.

4. Open the **Blocking Tasks** tab.

For every blocking task in the list, the following details are shown:

- **Name** — name of the organization

- **Status** — current status of the blocking task

- **User** — name of the user who initiated the task

- **Started At** — date and time when the task was initiated

- **Timeout** — default timeout set for blocking tasks

- **Timeout Action** — the action that will be triggered upon the task after the timeout expires

- **Organization** — name of the organization

Troubleshooting Virtual Machine Performance

Veeam ONE Client includes a set of dashboards that give you enhanced control over VMs provisioned in the VMware Cloud Director environment, and help you facilitate the troubleshooting process:

- **Top VMs** dashboard displays the top resource consumers for CPU, memory, datastore, network usage, snapshot size and snapshot age.

  To view VMs that consume the greatest amount of compute, network and storage resources, select the necessary VM container in the inventory pane and go to the **Top VMs** tab. For more information, see VMware vSphere Top and Lowest Load.

- **Tasks & Events** dashboard shows VMware vSphere tasks and events targeted at a specific VM.

  To view the list of tasks and events for a VM, select it in the inventory pane and go to the **Tasks & Events** tab. For more information, see VMware vSphere Tasks & Events.

- **Processes** dashboard provides control over processes currently running inside the guest OS of a VM. You can view, end and restart processes on Windows- based machines. You can also view and end daemons on Linux-based machines.

  To view the list of processes, select the necessary VM in the inventory pane and go to the **Processes** tab. For more information, see VMware vSphere In-Guest Processes.

- **Services** dashboard provides control over services currently running inside the guest OS of a VM. You can view, start, stop and restart services on VMs. For Windows-based machines, you can also create alarms based on the service state or object performance.

  To view the list of processes, select the necessary VM in the inventory pane and go to the **Services** tab. For more information, see VMware vSphere In-Guest Services.

- **Console** dashboard lists running in-guest processes and helps you diagnose problems related to a specific service, module or application.

  To access a VM console, select the necessary VM in the inventory pane and go to the **Console** tab. For more information, see VMware vSphere VM Console.

Hyper-V Monitoring

Veeam ONE offers a variety of tools for monitoring the Microsoft Hyper-V environment from any perspective and with any level of detail.

With Veeam ONE Client, you can:

1. Monitor health status of the virtual environment.

   o Start with the **Summary** dashboards to check the overall health status of the virtual environment and reveal hotspots.

     Quickly review the state of virtual infrastructure components, see the latest alarms, detect the most problematic objects and drill down to the problem source for further investigation.

   o Use the **Virtual Machines** dashboard to view the list of VMs in a virtual infrastructure container and check additional details for every VM — such as VM current status, parent host, IP address, DNS name and the amount of resources currently consumed by the VM.

   o Use the **Top Objects** dashboard to detect the most and less loaded components in the virtual environment.

     Detect what virtual infrastructure objects are consuming the most and the least amount of CPU, memory, disk, network, and swap resources, or select additional counters to detect resource consumers in other areas.

2. View triggered alarms.

   Switch to the **Alarms** dashboard to see details on breached thresholds, events and problems that occurred in the virtual environment.

   Use the **Actions** pane on the alarms dashboard to detect root causes — drill down to performance charts, open VM console or view the list of in-guest processes.

3. Work with performance charts and track events.

   Drill down to performance charts to diagnose performance problems. You can change predefined views, quickly switch between charts and view events that occur in your environment to get all-round statistics.

4. Investigate problems from within the guest OS.

   Open VM console or view the list of running in-guest processes to diagnose problems related to a specific service, module or application.

Prerequisites

Before you start monitoring your virtual environment, make sure you have configured connections to virtual servers from which Veeam ONE will collect data. For more information on configuring server connections, see section Connecting Microsoft Hyper-V Servers of the Veeam ONE Deployment Guide.

Microsoft Hyper-V Summary Dashboards

Microsoft Hyper-V infrastructure summary dashboards serve as the starting point for monitoring and troubleshooting. Summary dashboards reflect the health status of the selected infrastructure object or infrastructure segment.

The following types of summary dashboards are available for virtual infrastructure objects:

- Infrastructure Summary

- Host Summary

- Virtual Machine Summary

- Local Storage Summary

- SMB Share Summary

- Cluster Shared Volume Summary

To access a summary dashboard for a virtual infrastructure object or virtual infrastructure segment:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure object or segment.

4. Open the **Summary** tab.

Microsoft Hyper-V Infrastructure Summary

The Hyper-V infrastructure summary dashboard provides the health status overview for the selected virtual environment segment.

The dashboard is available for the following infrastructure levels:

- Virtual infrastructure (root node)

- Virtual infrastructure container (such as SCVMM, cluster or storage container)

Hosts Status, Datastores Status, Virtual Machines Status

The charts reflect the status of virtual infrastructure objects.

Every chart segment represents the number of objects with a certain status — objects with errors (red), objects with warnings (yellow) and healthy objects (green). Click a chart segment or a legend label to drill down to the list of alarms with the corresponding status for the selected type of virtual infrastructure objects.

Latest Alarms

The list displays the latest 15 alarms that were triggered for objects in the selected virtual environment segment. Click a link in the **Source** column to drill down to the list of alarms triggered for a specific virtual infrastructure object.

Alarms by Object

The list displays 15 objects with the highest number of alarms.

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 error alarms and 1 warning alarm triggered for the object. Click a link in the **Source** column to drill down to the list of alarms related to a specific virtual infrastructure object.

For more information, see Working with Triggered Alarms.

Business View Groups

The section displays the list of categories and groups to which the cluster is included.

Host Summary

The host summary dashboard provides the health status and performance overview for the selected Microsoft Hyper-V host and its child objects.
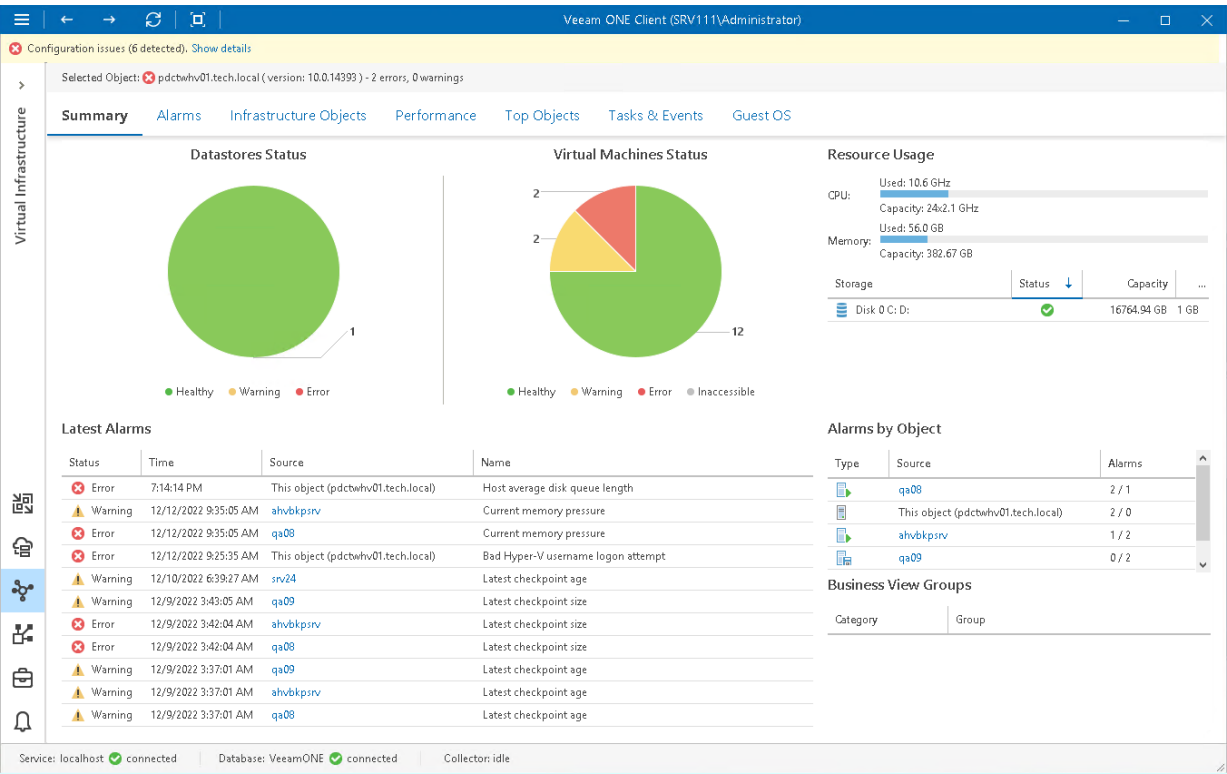
Datastores Status, Virtual Machines Status

The charts reflect the status of volumes connected to the host and the status of VMs running on the host.

Every chart segment represents the number of objects with a certain status — objects with errors (red), objects with warnings (yellow) and healthy objects (green). Click a chart segment or a legend label to drill down to the list of alarms with the corresponding status for host child objects.

Resource Usage

The section displays capacity and usage summary for host CPU and memory. It also shows an overview for volumes connected to the host — state of the volume, its capacity and the amount of free space on the volume.

Latest Alarms

The list displays the latest 15 alarms triggered for the host and its child objects. Click a link in the **Source** column to drill down to the list of alarms for the host and its child objects.

Alarms by Object

The list displays 15 objects with the greatest number of alarms (including the host and its child objects).

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 error alarms and 1 warning alarm triggered for the object. Click a link in the **Source** column to drill down to the list of alarms related to the host and its child objects.

For more information, see Working with Triggered Alarms.

Business View Groups

The section displays the list of categories and groups to which the host is included.

Virtual Machine Summary

The VM summary dashboard provides the health status and performance overview for the selected VM. In addition, this dashboard shows the status of objects that can affect the VM performance — the parent host and the volumes where VM files are located.
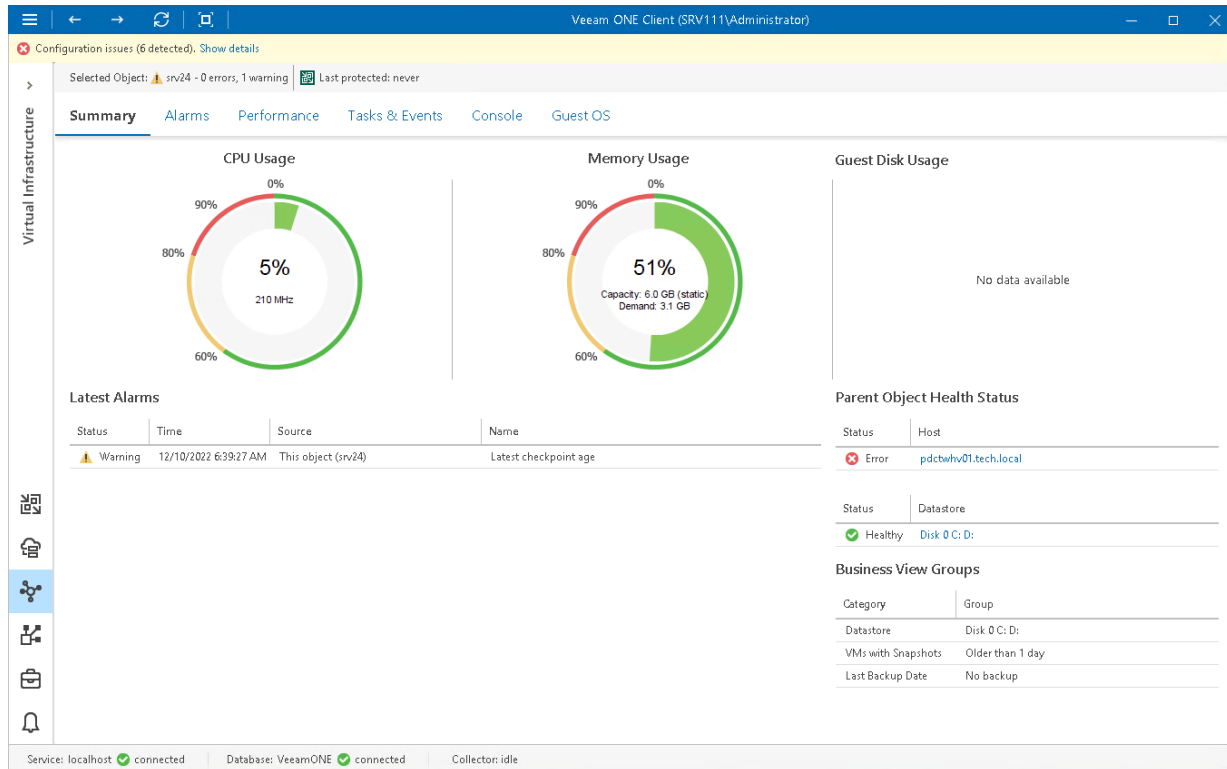
Selected Object

The section at the top of the dashboard shows the VM health status (number of warnings and errors) and the date when the latest backup or replica restore point was created for the VM with Veeam Backup & Replication.

CPU Usage, Memory Usage

The charts display the amount of CPU and memory resources currently consumed by the VM.

> **NOTE:**
> - On Hyper-V hosts prior to version 2016, memory usage is shown as 100% for VMs with Static Memory.
> - For Microsoft SQL Server or Exchange VMs running on Hyper-V 2016 hosts, memory usage can be shown to exceed 100%.

Guest Disk Usage

The chart displays the amount of available and used guest disk space with a breakdown by disks. By default, 5 guest disks with the greatest amount of used space are displayed.

Use the **Disks to show** list to change the number of disks to display on the chart. Click the **View all disks** link to view details for all guest disks. In the **Guests Disks** window, you can suppress *Guest disk space* alarms for specific disks. To suppress alarms for a disk, select the **Suppress alarms** check boxes next to the disk name.

Parent Object Health Status

The section displays the current state of the host where the VM resides and the state of volumes that host VMs files. Information in this section may help you to estimate the impact of parent objects on the VM performance. Click the host or volume name link to drill down to the list of alarms for the host or volume.

Latest Alarms

The list displays the latest 15 alarms for the VM.

For more information, see Working with Triggered Alarms.

Business View Groups

The section displays the list of categories and groups to which the VM is included.

Local Storage Summary

The local storage summary dashboard provides the health status and performance overview for the selected host local storage. In addition, it shows the state of objects that can affect the storage performance — the parent host and VMs on the local storage.
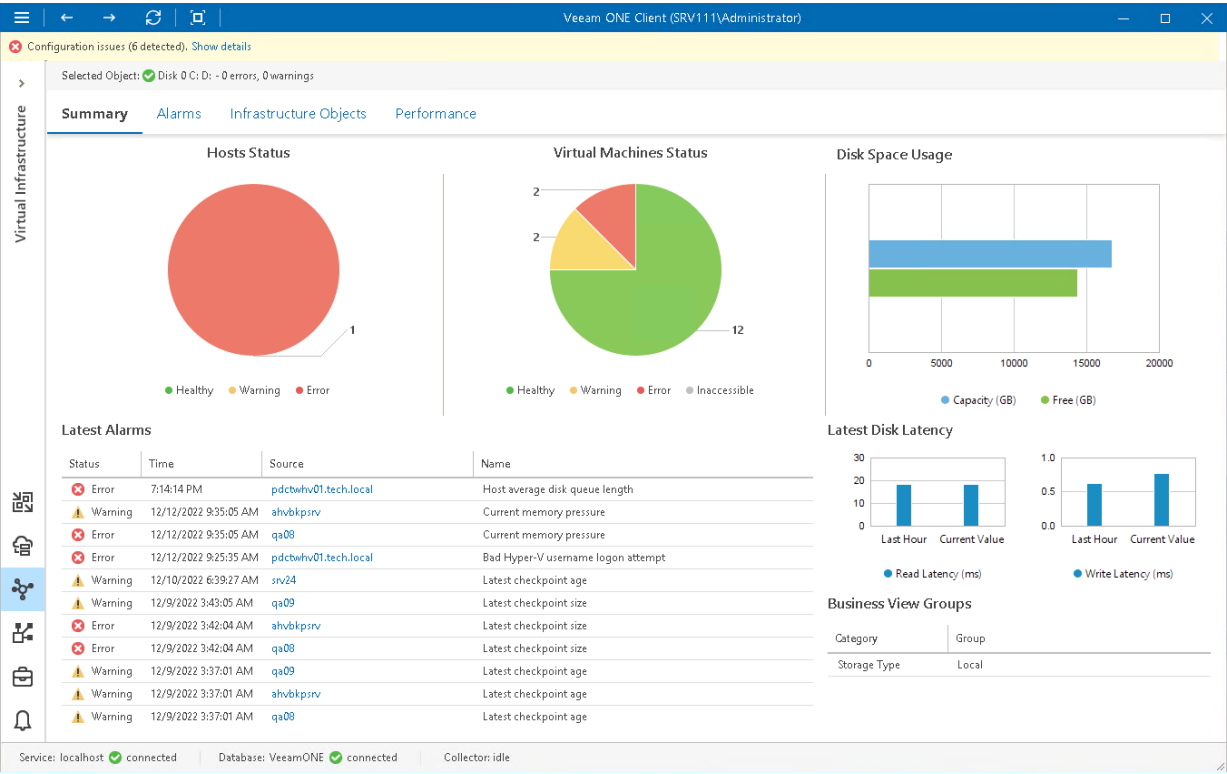
Hosts Status, Virtual Machines Status

The charts reflect the health status of the host and VMs that work with the local storage.

Every chart segment represents the number of objects in a certain state — objects with errors (red), objects with warnings (yellow) and healthy objects (green). Click a chart segment or a legend label to drill down to the list of alarms with the corresponding status for hosts or VMs.

Disk Space Usage

The chart reflects the amount of available and used disk space on the local storage.

Latest Alarms

The list displays the latest 15 for the local storage and objects that work with the local storage. Click a link in the **Source** column to drill down to the list of alarms for the selected object.

For more information, see Working with Triggered Alarms.

Latest Disk Latency

The section displays the current read and write latency values as well as the average latency values for the past hour.

Business View Groups

The section displays the list of categories and groups to which the storage is included.

SMB Share Summary

The SMB shares summary dashboard provides the health status and performance overview for the selected SMB share. In addition, it shows the state of objects that can affect SMB share performance — hosts that work with SMB shares and VMs residing on the shares.
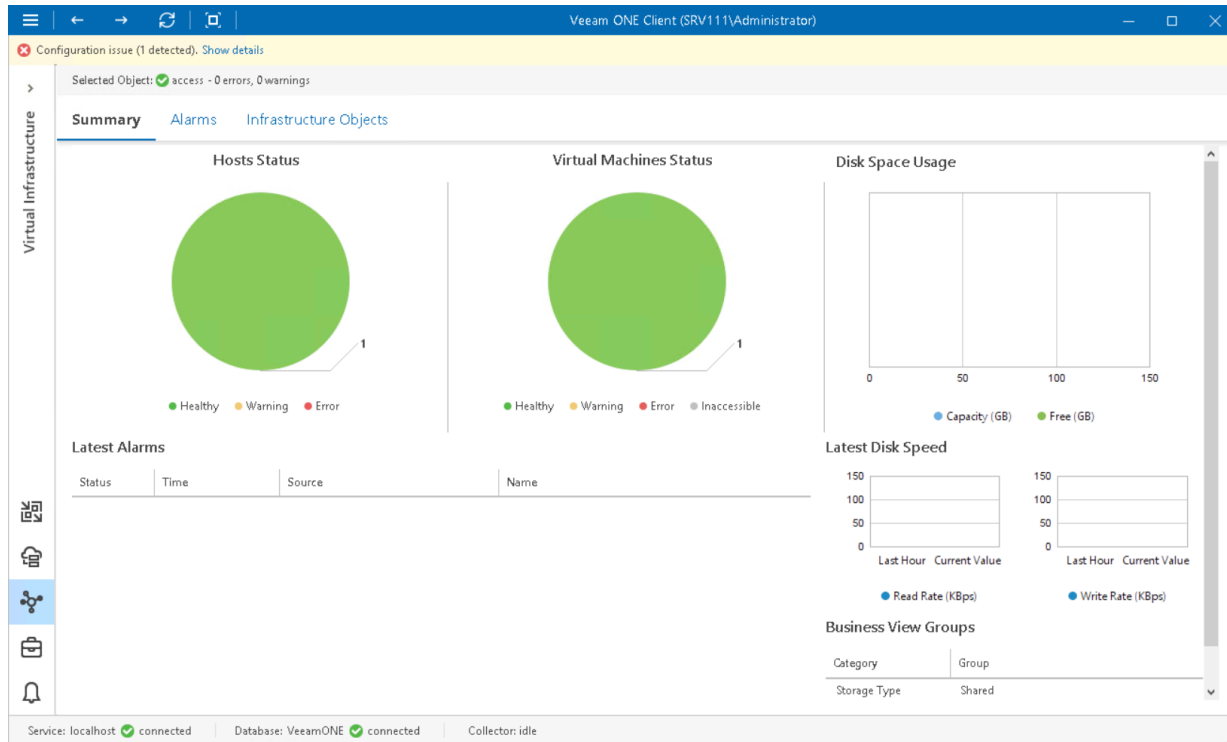
Hosts Status, Virtual Machines Status

The charts reflect the health status of the hosts that work with the SMB share and VMs located on the share.

Every chart segment represents the number of objects with a certain status — objects with errors (red), objects with warnings (yellow) and healthy objects (green). Click a chart segment or a legend label to drill down to the list of alarms with the corresponding status for hosts or VMs.

Disk Space Usage

The chart reflects the amount of available and used disk space on the SMB share.

Latest Alarms

The list displays the latest 15 alarms for the SMB share and alarms for hosts that work with the file share and for VMs located on the share. Click a link in the **Source** column to drill down to the list of alarms for the selected object.

For more information, see Working with Triggered Alarms.

Latest Disk Speed

The section displays the current read and write rate as well as the average read and write rate values for the past hour.

Cluster Shared Volume Summary

The CSV summary dashboard provides the health status and performance overview for the selected Cluster Shared Volume. In addition, it shows the state of objects that can affect the volume performance — hosts that work with the CSV and VMs residing on the CSV.
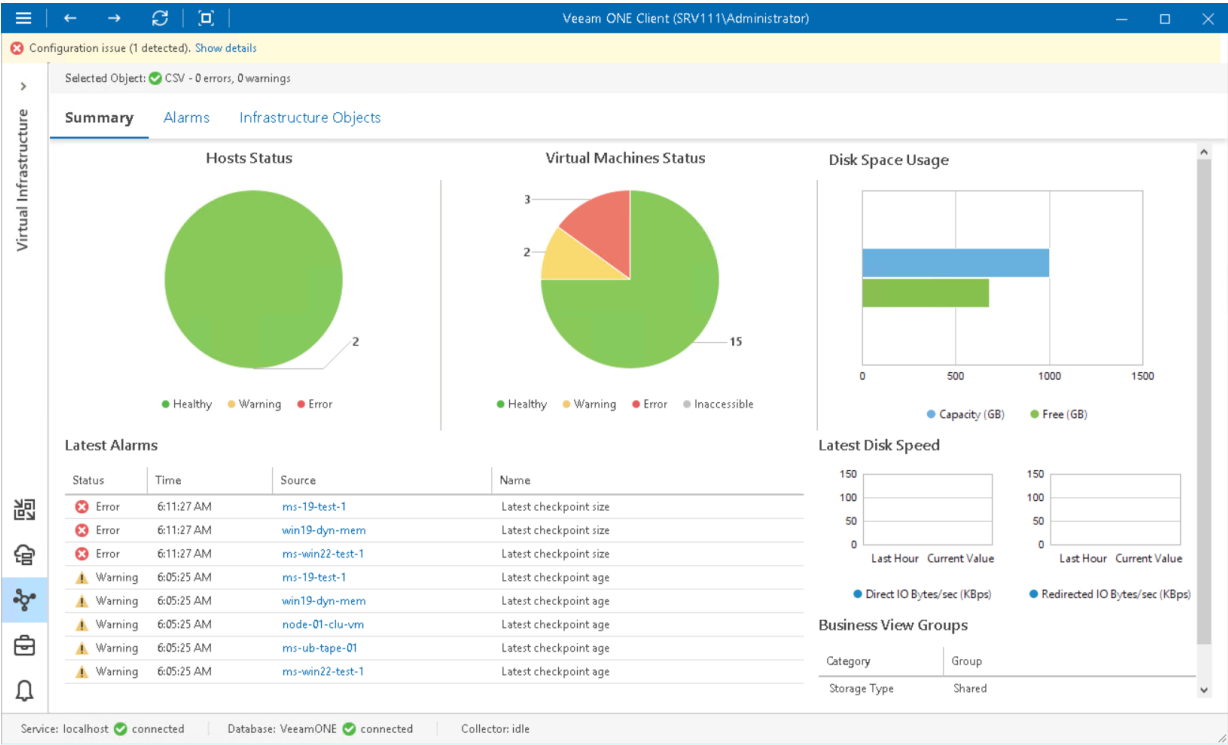
Hosts Status, Virtual Machines Status

The charts reflect the health status of hosts that work with the volume and the state of VMs stored on the volume.

Every colored segment represents the number of objects with a certain status — objects with errors (red), objects with warnings (yellow) and healthy objects (green). Click a chart segment or a legend label to drill down to the list of alarms with the corresponding status for hosts or VMs.

Disk Space Usage

The chart reflects the amount of available and used disk space on the Cluster Shared Volumes.

Latest Alarms

The list displays the latest 15 alarms for the Cluster Shared Volumes and objects that work with the volumes. Click a link in the **Source** column to drill down to the list of alarms for the selected object.

For more information, see Working with Triggered Alarms.

Latest Disk Speed

The section displays the current direct and redirected I/O values as well as the average values for the past hour.

Microsoft Hyper-V Alarms

Veeam ONE includes a set of alarms for monitoring Microsoft Hyper-V virtual environment. These alarms warn you about events or changes that can affect performance of operations and services in the virtual environment.

To view the list of triggered Microsoft Hyper-V alarms:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary virtual infrastructure node.

4. Open the **Alarms** tab.

On the **Alarms** dashboard, you can view triggered alarms, track alarm history, resolve and acknowledge alarms and perform other actions. For more information on available actions, see Working with Triggered Alarms.

Microsoft Hyper-V Performance Charts

Performance charts show how key performance counters have been changing over time to help you diagnose performance issues and perform root cause analysis.

Performance charts include the following elements:

- **Axes**

  Performance charts display data for a particular time period (the horizontal axis) using two scales of measurement units (vertical axes). The measurement units may vary depending on selected performance counters. However, the number of units is always limited to two.

- **Graphs**

  Performance charts include one or more graphs. Every graph on a performance chart visualizes a specific counter for an infrastructure object or a container of infrastructure objects.

- **Legend**

  The chart legend shows details about objects and counters displayed in the chart. The details include key color, object name, list of counters and units of measurement, the latest, minimum, average, and maximum counter values.

- **Chart views**

  Performance charts come with a number of predefined chart views. Every view logically groups related counters to display the most valuable data and help you speed up troubleshooting and root cause analysis of performance problems.

Performance charts can be easily customized. For more information on customization options, see Customizing Microsoft Hyper-V Performance Charts.

Accessing Performance Charts

To access a performance chart for an infrastructure object or infrastructure segment:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure object or segment.

4. Open the **Performance** tab.

Overview

The **Overview** page shows aggregated performance data for the selected virtual infrastructure object or segment: total run time, memory usage, network, disk/host read and write speed. Performance data is shown for the previous 15 minutes.

In the **Top line** field, you can set a threshold value. The top line is displayed as the red dotted line on the chart to help you monitor whether resource usage exceeds the healthy value range. If you do not need to display the top line, enter '0' (zero) in the **Top line** field or disable top lines in Veeam ONE Client chart settings. With the top line disabled, the Y-axis will scale automatically to match the range of the displayed data.

To drill down to performance chart details, click the counter link above a performance widget. A corresponding performance chart for the selected virtual infrastructure object will open.

CPU Performance Chart

The **CPU** chart displays historical statistics on CPU utilization for the selected virtual infrastructure object.

Host

The following table provides information on predefined views and counters that apply to hosts.

Chart View	Counter	Measurement Unit	Description
CPU Usage	Total Run Time	Percent	Percentage of time a physical processor required to run both VMs and the hypervisor itself.
	Total Run Time	GHz	Amount of time physical processor required to run both VMs and the hypervisor itself.
CPU Usage by Host/VMs	Guest Run Time	Percent	Percentage of time a physical processor required to run VMs.
	Hypervisor Run Time	Percent	Percentage of time a physical processor required to run a hypervisor.
	vCPU Total Run Time	Percent	Percentage of time vCPUs were used by all VMs on a host.

Chart View	Counter	Measurement Unit	Description
CPU Idle Time	Idle Time	Percent	Percentage of time a physical processor spent in an idle state.
CPU Interrupts	Total Interrupts/sec	Number	Number of interrupts to which a processor was asked to respond. Interrupts are generated from hardware components like hard disk controller adapters and network interface cards. A sustained value over 1000 usually indicates of a problem.
CPU Bottlenecks	Host CPU Wait Time	Microsecond	Average amount of time that VMs on a host spend waiting for their virtual processors to be dispatched onto a logical processor.

Virtual Machine

The following table provides information on predefined views and counters that apply to VMs.

Chart View	Counter	Measurement Unit	Description
CPU Usage	Guest Run Time	Percent	Percentage of time a physical processor required to run a VM.
	Guest vCPU Run Time	MHz	Amount of virtual CPU resources used by a VM.
CPU Usage by Host	Hypervisor Run Time	Percent	Percentage of physical processor time consumed by Hyper-V host for a VM.
	Total Run Time	Percent	Percentage of time a Hyper-V host required to run a VM, plus time consumed by the VM itself.
	vCPU Total Run Time	MHz	Amount of vCPU resources consumed by all VMs on a host.
CPU Bottlenecks	CPU Wait Time	Microsecond	Amount of time that a virtual processor spends waiting to be dispatched onto a logical processor.

For objects that are parent to hosts and VMs, Veeam ONE Client displays rollup values.
Charts for folders and clusters display rollup values for all hosts in the container. Chart for a resource displays rollup values for all VMs registered as shared resources.

Memory Performance Chart

The **Memory** chart displays historical statistics on memory utilization for the selected virtual infrastructure object.
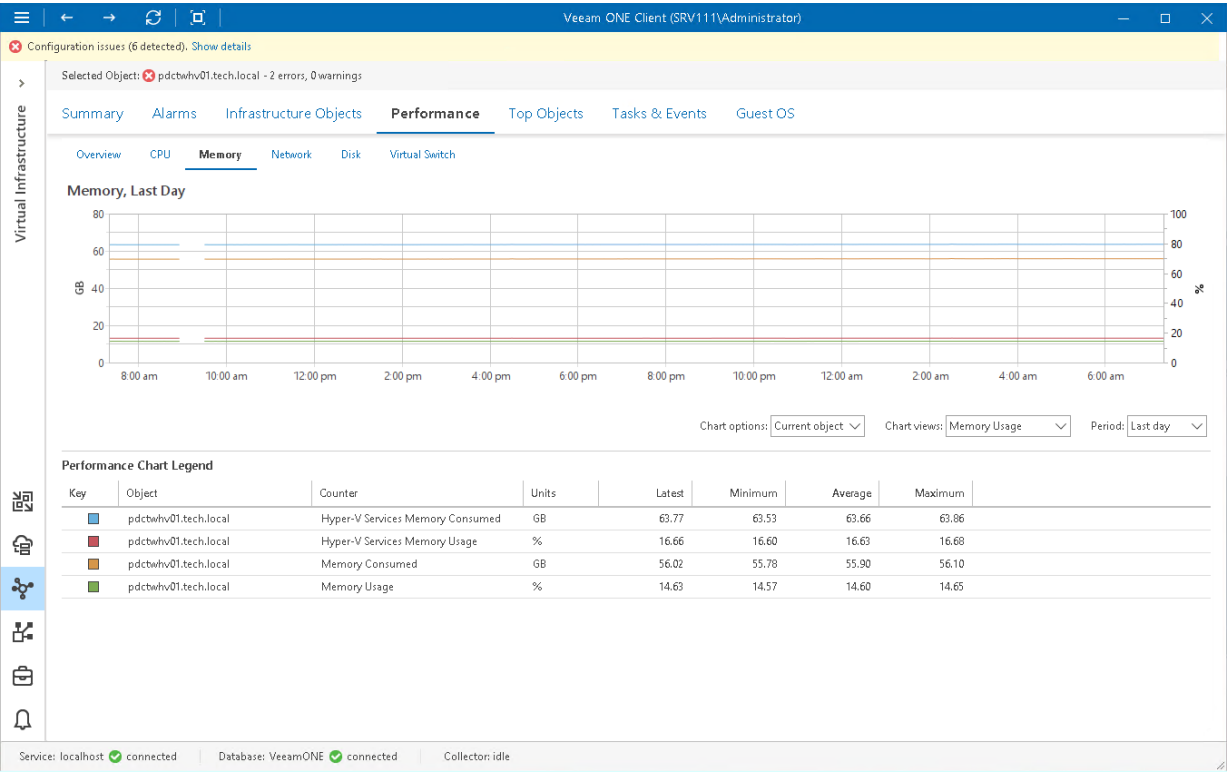
Host

The following table provides information on predefined views and counters that apply to hosts.

Chart View	Counter	Measurement Unit	Description
Memory Usage	Hyper-V Services Memory Consumed	GB	Amount of memory currently consumed by Hyper-V services.
	Hyper-V Services Memory Usage	Percent	Amount of memory resources currently used by Hyper-V services.
	Memory Consumed	GB	Amount of physical memory resources used on a host.

Chart View	Counter	Measurement Unit	Description
	Memory Usage	Percent	Memory usage as percentage of available machine memory.
Memory Pressure	Average Pressure	Percent	Amount of memory resources available on a host.
Committed Memory	Committed	GB	Demand for virtual memory. The counter shows how much memory were allocated for processes and to which processes the OS has committed a RAM page frame or a page slot in the pagefile (or both). As the Committed counter grows above the available RAM, paging increases and the amount of the pagefile in use increases as well. At some point, paging activity starts to affect perceived performance significantly.
Memory Swap Faults	Page Faults/sec	Number	Page faults that occur when any process attempts to read from a virtual memory location that is marked as 'not present'. The best counter value is zero. The counter displays both hard page and soft page faults.
Memory Swap Rate	Page Reads/sec	Number	Lack of memory resources. The counter shows how often the system reads from disk because of hard page faults. The counter shows the number of read operations, not taking into account the number of pages retrieved in each operation. The counter can reveal different kinds of faults that cause system delays.
	Page Writes/sec	Number	Number of attempts taken by running the write command/operation to clear unused items out of memory. Pages are written to disk only if they change while in physical memory, so they are likely to hold data, not code. The counter shows write operations, not taking into account the number of pages written in each operation.
	Pages Input/sec	Number	Rate at which memory pages are read from disk.
	Pages Output/sec	Number	Rate at which memory pages are written to disk.
	Pages/sec	Number	Sum of Pages Input/sec and Pages Output/sec counters. The counter indicates how often the system uses a hard drive to store and retrieve memory-associated data.

Virtual Machine

The following table provides information on predefined views and counters that apply to VMs.

Chart View	Counter	Measurement Unit	Description
Memory Usage	Guest Visible Physical Memory	GB	Amount of memory visible to the guest OS running inside a VM.
	Physical Memory	GB	Amount of memory currently used by a VM.
Memory Pressure	Demand	B	Amount of memory a VM requires to run all active processes. The counter represents the total committed memory based on data obtained from other performance counters.
	Current Pressure	Percent	Current pressure in a VM. To calculate the counter, Microsoft Hyper-V analyzes the VM total committed memory and calculates the pressure as the following ratio: the amount of memory the VM wants / the amount of memory the VM has.

For objects that are parent to hosts and VMs, Veeam ONE Client displays rollup values.

Charts for folders and clusters display rollup values for all hosts in the container. Chart for a resource displays rollup values for all VMs registered as shared resources.

Network Performance Chart

The **Network** chart displays historical statistics on network usage for the selected virtual infrastructure object.

Host

The following table provides information on predefined views and counters that apply to hosts.

Chart View	Counter	Measurement Unit	Description
Network Transfer Rate	Network Bytes Received/sec	KB/s	Rate at which data is received across each network adapter on a host. The counter represents the bandwidth of the network.
	Network Bytes Sent/sec	KB/s	Rate at which data is sent across each network adapter on a host.
	Network Bytes Total/sec	KB/s	Rate at which data is sent and received across a network interface.
Network Output Queue Length	Network Output Queue Length	Number	Length of the output queue, in packets. If the Output Queue Length value exceeds 2, it can be an indicator of delays across the network. In this case, you should find and eliminate the bottleneck to improve performance.

Chart View	Counter	Measurement Unit	Description
Network Connections	Network Offloaded Connections	Number	Number of TCP connections (over both IPv4 and IPv6) currently handled by a TCP Chimney Offload network adapter.
Network Errors	Network Outbound Errors	Number	Number of outbound packets that could not be transmitted because of errors.
	Network Received Errors	Number	Number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Network Transfer Rate (Packets)	Network Packets Received/sec	Number	Rate at which packets are received on the network interface.
	Network Packets Sent/sec	Number	Rate at which packets are sent on the network interface.
	Network Packets/sec	Number	Rate at which packets are sent and received on the network interface.

Virtual Machine

The following table provides information on predefined views and counters that apply to VMs.

Chart View	Counter	Measurement Unit	Description
Virtual Network Usage	Virtual Network Bytes Received/sec	KB/s	Rate at which data is received across the vNIC instance on a VM. The counter represents the bandwidth of the network.
	Virtual Network Bytes Sent/sec	KB/s	Rate at which data is sent across the vNIC instance on a VM.
	Virtual Network Bytes/sec	KB/s	Network utilization, sum of data received and sent across all vNIC instances on a VM.
Virtual Network Usage (Packets)	Virtual Network Packets Received/sec	Number	Total number of packets received per second by the network adapter.
	Virtual Network Packets Sent/sec	Number	Total number of packets sent per second by the network adapter.

Chart View	Counter	Measurement Unit	Description
Legacy Network Bytes Dropped	Legacy Network Bytes Dropped	B	Amount of data dropped on the network adapter.
Legacy Network Usage	Legacy Network Bytes Received/sec	B/s	Amount of data received by the network adapter.
	Legacy Network Bytes Sent/sec	B/s	Amount of data sent by the network adapter.

For objects that are parent to hosts and VMs, Veeam ONE Client displays rollup values.

Charts for folders and clusters display rollup values for all hosts in the container. Chart for a resource displays rollup values for all VMs registered as shared resources.

Virtual Switch Performance Chart

The **Virtual Switch** chart displays historical statistics on virtual switch usage for Microsoft Hyper-V hosts.
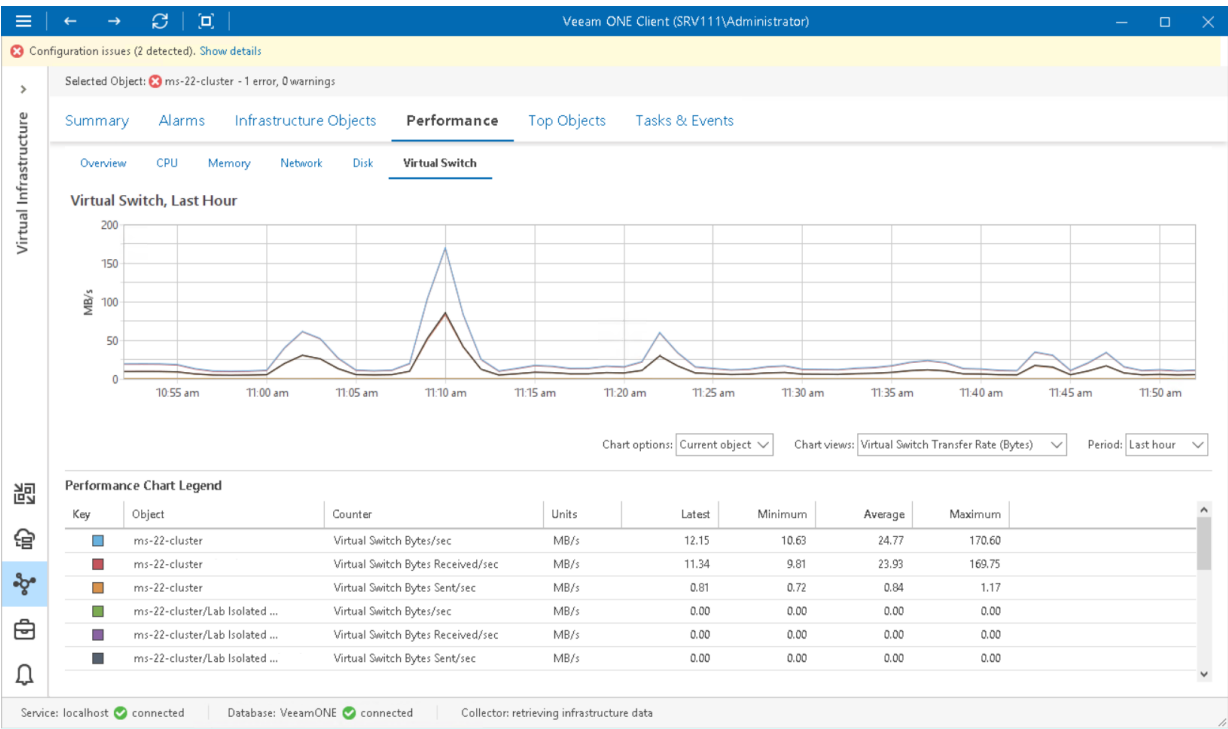
The following table provides information on predefined views and counters.

Chart View	Counter	Measurement Unit	Description
Virtual Switch Transfer Rate (Bytes)	Virtual Switch Bytes Received/sec	KB/s	Amount of data received per second by a virtual switch.
	Virtual Switch Bytes Sent/sec	KB/s	Amount of data sent per second by a virtual switch.
	Virtual Switch Bytes/sec	KB/s	Amount of data received and sent per second by a virtual switch.
Virtual Switch Transfer Rate (Packets)	Virtual Switch Packets Received/sec	Number	Total number of packets received per second by a virtual switch.
	Virtual Switch Packets Sent/sec	Number	Total number of packets sent per second by a virtual switch.
	Virtual Switch Packets/sec	Number	Total number of packets received and sent per second by a virtual switch.

Cluster/Host Disk Performance Chart

The **Disk** chart is available for Microsoft Hyper-V clusters and hosts. The chart displays historical statistics on disk usage for the selected cluster or host.
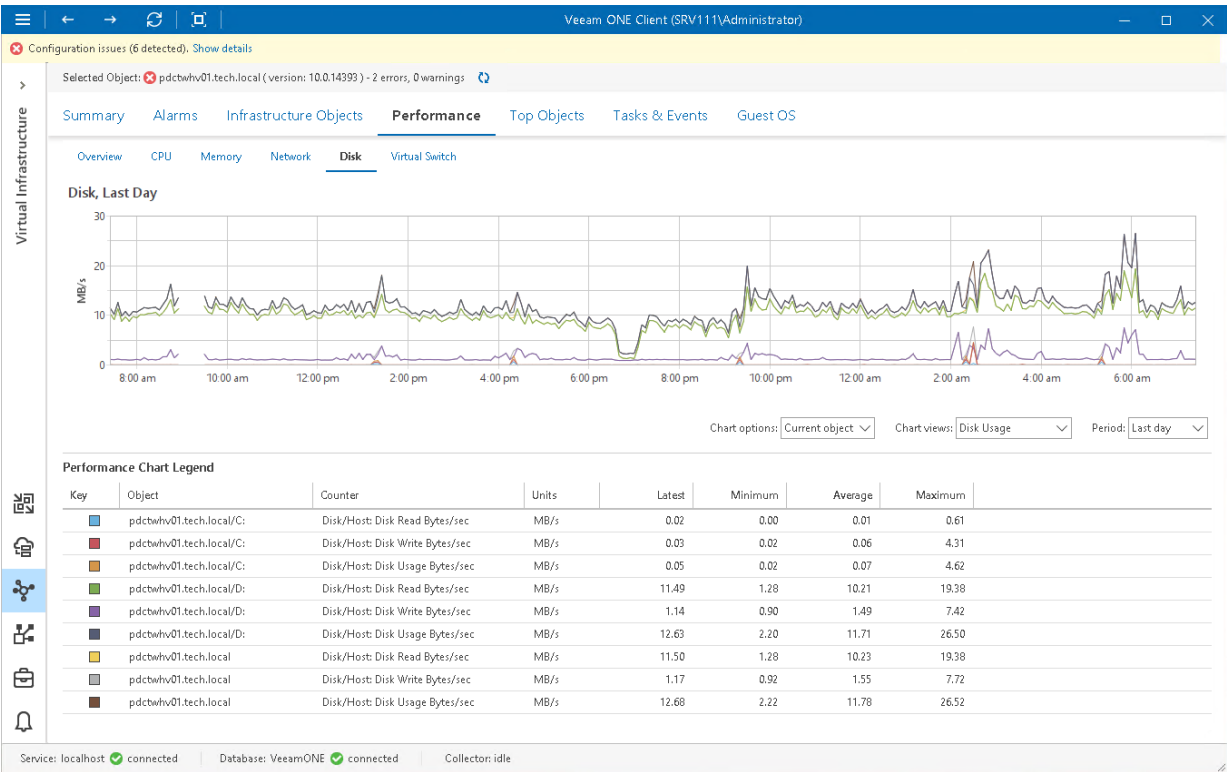
The following table provides information on predefined views and counters.

Chart View	Counter	Measurement Unit	Description
Disk Usage	Disk/Host: Disk Read	MB/s	Rate at which bytes are transferred from a disk during read operations.
	Disk/Host: Disk Write	MB/s	Rate at which bytes are transferred from a disk during write operations.
	Disk/Host: Disk Usage	MB/s	Rate at which bytes are transferred to and from a disk during read and write operations.
Disk Queue Length	Disk/Host: Avg Disk Queue Length	Number	Average number of read and write requests that were queued for a disk during the sample interval.
Disk Latency	Disk/Host: Avg Disk sec/Read	Millisecond	Average amount of time that a read operation from a disk takes.

Chart View	Counter	Measurement Unit	Description
	Disk/Host: Avg Disk sec/Write	Millisecond	Average amount of time that a write operation to a disk takes.

VM Disk Performance Chart

The **Disk** chart for VMs displays historical statistics for partitions of all disks on the selected VM.

The following table provides information on predefined views and counters.

Chart View	Counter	Measurement Unit	Description
Virtual Storage Issues	Errors/min	Number	Number of virtual storage errors per minute.
	Flushes/min	Number	Number of virtual storage flush operations per minute.
Virtual Storage Usage	Virtual Storage Read	KB/s	Total number of bytes that have been read per second on a virtual storage.
	Virtual Storage Write	KB/s	Total number of bytes that have been written per second on a virtual storage.
	Virtual Storage Usage	KB/s	Rate at which bytes have been read and written per second on a virtual storage.
Virtual Storage IOPS	IOPS	Number	Average number of read and write operations per second to a virtual storage.

Chart View	Counter	Measurement Unit	Description
	Reads/sec	Number	Total number of read operations issued per second to a virtual storage.
	Writes/sec	Number	Total number of write operations issued per second to a virtual storage.

Disk Space Chart

The **Disk Space** chart it displays historical statistics on disk space resources and usage for the selected disk.
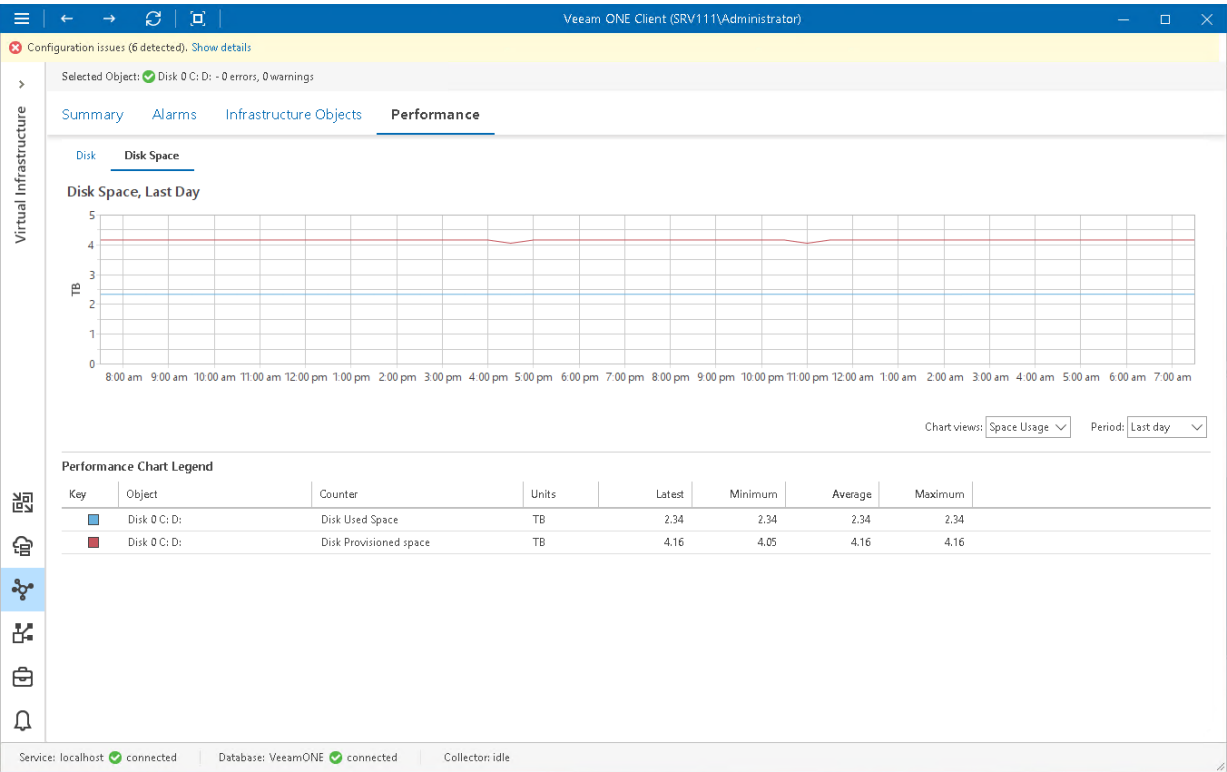
The following table provides information on predefined views and counters.

Chart View	Counter	Measurement Unit	Description
Space Usage	Disk Free Space	TB	Amount of free space on a disk.
	Disk Provisioned Space	TB	Amount of disk space provisioned to VMs.
	Disk Used Space	TB	Amount of used space on a disk.

Local Volume Performance Chart

The **Disk** chart displays historical statistics on disk usage for the selected local volume.

The following table provides information on predefined views and counters.

Chart View	Counter	Measurement Unit	Description
Datastore Usage	Disk/Physical Disk: Disk Read	MB/s	Rate at which data is read from a volume.
	Disk/Physical Disk: Disk Write	MB/s	Rate at which data is written to a volume.
	Disk/Physical Disk: Disk	MB/s	Sum of read and write rates for a volume.
Datastore Queue Length	Disk/Physical Disk: Avg. Disk Queue Length	Number	Average number of read and write operations queued for a volume.
Datastore IOPS	Disk/Physical Disk: Disk Transfers/sec	Number	Number of read and write operations completed per second, regardless of how much data they involve. This counter measures disk utilization. If the value exceeds 50, it can be an indicator of a bottleneck.

Chart View	Counter	Measurement Unit	Description
Datastore Latency	Disk/Physical Disk: Avg Disk sec/Read	Millisecond	Average time that a read operation from a volume takes.
	Disk/Physical Disk: Avg Disk sec/Write	Millisecond	Average time that a write operation to a volume takes.

Cluster Shared Volume Disk Performance Chart

The **Disk** chart displays historical statistics on disk usage for the selected Cluster Shared Volume.
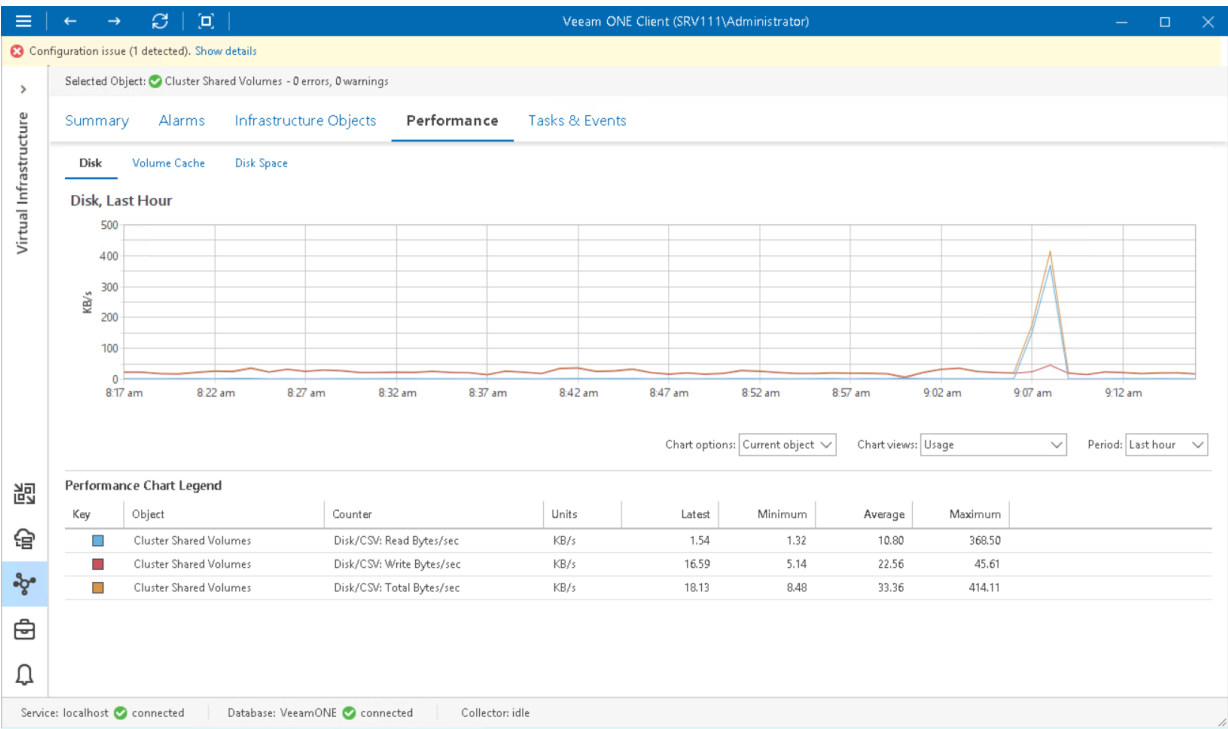
The following table provides information on predefined views and counters.

Chart View	Counter	Measurement Unit	Description
Usage	Disk/CSV: Read Bytes/sec	KB/s	Rate at which data is read from the volume in the Direct Access or Redirected Access mode.
	Disk/CSV: Write Bytes/sec	KB/s	Rate at which data is written to the volume in the Direct Access or Redirected Access mode.
	Disk/CSV: Total Bytes/sec	KB/s	Rate at which data is read from and written to the volume in the Direct Access or Redirected Access mode.
IOPS	Disk/CSV: Reads/sec	Number	Rate at which read operations were performed directly on a volume.
	Disk/CSV: Writes/sec	Number	Rate at which write operations were performed directly on a volume.

Chart View	Counter	Measurement Unit	Description
	Disk/CSV2012: IOPS	Number	Rate at which read and write operations were performed directly on a volume.
Latency	Disk/CSV: Read Latency	Millisecond	Average latency between the time a read request arrived to a file system and the time when it was completed.
	Disk/CSV: Write Latency	Millisecond	Average latency between the time a write request arrived to a file system and the time when it was completed.
	Disk/CSV: Latency	Millisecond	Average latency required to complete read and write operations on a volume.
Datastore Queue Length	Disk/CSV: Read Queue Length	Number	Number of read operations queued for a volume.
	Disk/CSV: Write Queue Length	Number	Number of write operations queued for a volume.
	Disk/CSV: Queue Length	Number	Number of read and write operations that were queued for a volume during the sample interval.
Direct/Redirected Usage	Disk/CSV: Redirected Bytes/sec	KB/s	Average amount of data transferred to or from a disk during write or read operations over the network stack.
	Disk/CSV: Direct Bytes/sec	KB/s	Average amount of data transferred to or from a disk during write or read operations.
Direct/Redirected Latency	Disk/CSV: Direct Latency	Millisecond	Average latency required to for complete read and write operations on a volume in the Direct Access mode.
	Disk/CSV: Redirected Latency	Millisecond	Average latency required to complete read and write requests on a volume in the Redirected Access mode.
Direct/Redirected IOPS	Disk/CSV: Direct IOPS	Number	Rate at which read and write operations were performed directly on a disk.

Chart View	Counter	Measurement Unit	Description
	Disk/CSV: Redirected IOPS	Number	Rate at which read and write operations were redirected to a volume through the network.

SMB Share Disk Performance Chart

The **Disk** chart displays historical statistics on disk usage for the selected SMB file share.

The following table provides information on predefined views and counters.

Chart View	Counter	Measurement Unit	Description
Virtual Storage Issues	Errors/min	Number	Number of virtual storage errors per minute.
	Flushes/min	Number	Number of virtual storage flush operations per minute.
Virtual Storage Usage	Virtual Storage Read	KB/s	Total amount of data that have been read per second on the virtual storage.
	Virtual Storage Write	KB/s	Total amount of data that have been written per second on the virtual storage.
	Virtual Storage Usage	KB/s	Rate at which data is read and written per second on the virtual storage.
Virtual Storage IOPS	Reads/sec	Number	Total number of read operations that have occurred on the virtual storage.
	Writes/sec	Number	Total number of write operations that have occurred on the virtual storage.
	IOPS	Number	Average number of read and write operations per second during collection interval.

HA SMB Performance Chart

The **HA Disk** chart displays historical statistics on disk usage for the selected Highly Available SMB share created on Cluster Shared Volumes.

The following table provides information on predefined views and counters.

Chart View	Counter	Measurement Unit	Description
Usage	Disk/CSV: Read	KB/s	Rate at which data was read from a volume in the Direct Access or Redirected Access mode.
	Disk/CSV: Write	KB/s	Rate at which data was written to a volume in the Direct Access or Redirected Access mode.
	Disk/CSV: Total	KB/s	Rate at which data was read from and written to a volume in the Direct Access or Redirected Access mode.
IOPS	Disk/CSV: Read/sec	Number	Rate at which read operations were performed directly on a volume.
	Disk/CSV: Writes/sec	Number	Rate at which write operations were performed directly on a volume.
	Disk/CSV: IOPS	Number	Rate at which read and write operations were performed directly on a volume.
Latency	Disk/CSV: Read Latency	Millisecond	Average latency between the time a read request arrived to a file system and the time when it was completed.
	Disk/CSV: Write Latency	Millisecond	Average latency between the time a write request arrived to the file system and the time when it was completed.
	Disk/CSV: Latency	Millisecond	Average latency required to complete read and write operations on a volume.
Datastore Queue Length	Disk/CSV: Read Queue Length	Number	Number of read operations queued for a volume.
	Disk/CSV: Write Queue Length	Number	Number of write operations queued for a volume.

Chart View	Counter	Measurement Unit	Description
	Disk/CSV: Queue Length	Number	Total number of read and write operations queued for a volume during the sample interval.
Direct/Redirected Usage	Disk/CSV: Redirected Bytes/sec	KB/s	Average amount of data transferred to or from the disk during write or read operations over the network stack.
	Disk/CSV: Direct Bytes/sec	KB/s	Average amount of data transferred to or from the disk during write or read operations.
Direct/Redirected Latency	Disk/CSV: Direct Latency	Millisecond	Average latency required to complete read and write operations on a volume in the Direct Access mode.
	Disk/CSV: Redirected Latency	Millisecond	Average latency required to complete read and write operations on a volume in the Redirected Access mode.
Direct/Redirected IOPS	Disk/CSV: Direct IOPS	Number	Rate at which read and write operations were performed directly on a disk.
	Disk/CSV: Redirected IOPS	Number	Rate at which read and write operations were redirected to a volume through the network.

Volume Cache Performance Chart

The **Volume Cache** chart displays historical statistics on read requests from the cache for the selected Cluster Shared Volume with enabled CSV Cache.
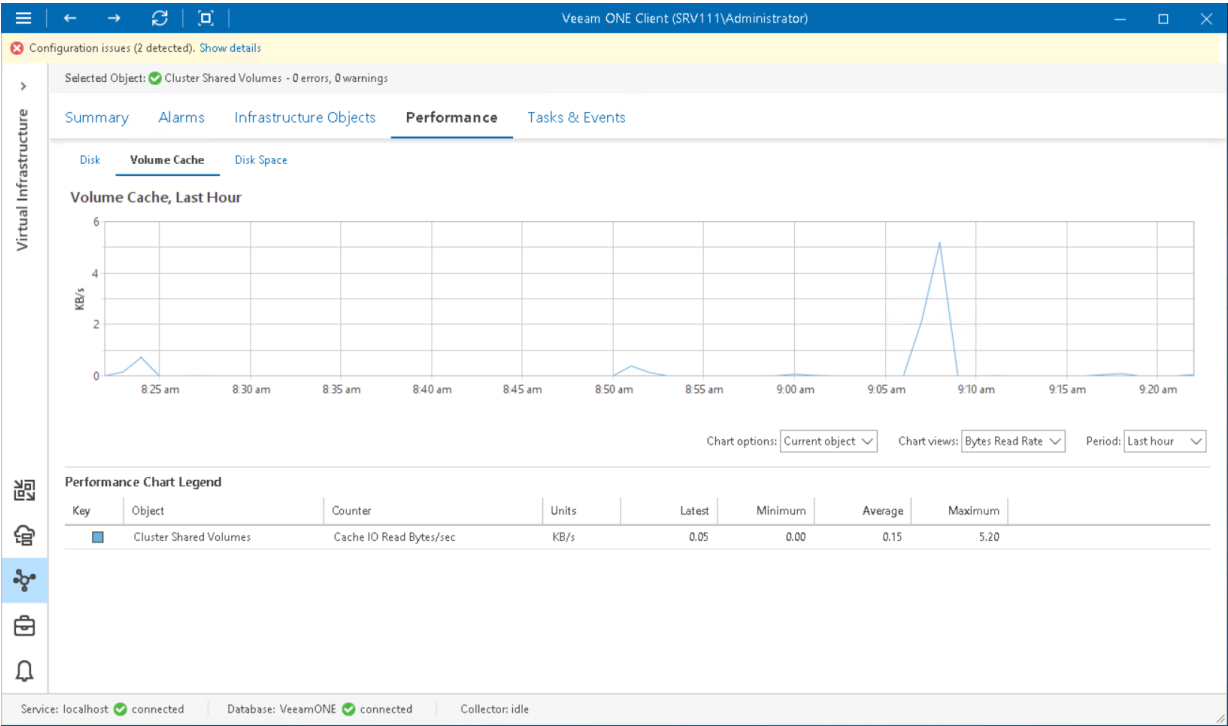
The following table includes information on predefined views and counters.

Chart View	Counter	Measurement Unit	Description
Bytes Read Rate	Cache IO Read	MB/s	Rate at which data is transferred from the volume cache during read operations.
Total Read	Cache Reads/sec	Number	Number of read operations performed in the volume cache per second.

Customizing Microsoft Hyper-V Performance Charts

You can customize performance charts to select specific objects, time intervals or performance counters to display on the charts.

Selecting Objects to Chart

By default, all performance charts display data for an infrastructure object selected in the inventory pane. You can also choose to display performance data on charts for:

- Child components or objects of the selected virtual infrastructure object (for example, all hosts in the cluster)

- Child VMs for the selected virtual infrastructure object or segment

To display performance data for direct children of the selected virtual infrastructure object:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure object.

4. Open the necessary performance chart tab.

5. From the **Chart options** list, select *Custom*.

6. In the **Customize Chart Options** window, choose **Show performance data for these child objects**.

7. Select check boxes next to child objects that should be included in the chart scope.

8. Click **OK**.

To display performance data for a set of VMs in the selected virtual infrastructure segment:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the inventory pane, select the necessary infrastructure object.

3. Open the necessary performance chart tab.

4. From the **Chart options** list, select *Custom*.

5. In the **Customize Chart Options** window, choose **Show performance data for these VMs**.

   You can select both direct and indirect children (children of children) of the selected virtual infrastructure object.

6. Select check boxes next to VMs that should be included in the chart scope.

7. Click **OK**.

NOTE:

The legend pane displays objects for which data is available for the selected time interval.

Selecting Chart Views and Performance Counters

Performance charts come with a set of predefined chart views that logically group related performance counters. You can switch between chart views using the **Chart view** list at the top of the chart legend.

Instead of using predefined views, you can choose a custom set of performance counters to show on the chart:

1. Open Veeam ONE Client.

    For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure object.

4. Open the necessary performance chart.

5. In the **Chart views** list, select the *Custom* option to open the **Select Devices and Counters** window.

6. From the **Devices** list, select the necessary device(s).

    Select *Total* to display all available devices on the chart.

NOTE:

The list of devices is not available for some performance charts. For example, for the **CPU** or **Memory** performance chart, you can only choose counters to display.

7. From the **Counters** list, select counters to display on the chart.

   When you select a counter, its description appears in the **Counter description** section of the window.

8. Click **OK**.

Selecting Time Interval

You can choose the time interval for which performance data on the chart will be displayed. Available options are:

- Real-time information (last hour)

- Last day

- Last week

- Last month

- Last year

- Custom time range (you can choose any time interval within the specified number of hours, days, or weeks, or specify any from/to period)

To specify a time interval for which performance data should be displayed:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure object.

4. Open the necessary performance chart.

5. From the **Period** list, select *Last hour*, *Last day*, *Last week*, *Last month* or *Last year*.

   To define a custom time range, select *Custom*. In the **Select Custom Time Interval** window, define the necessary interval and click **OK**.

When you change the time interval, the time scale (X-axis) of the performance chart and the chart will change respectively.

Microsoft Hyper-V Tasks & Events

You can view information about events that occur in your virtual environment within the selected time interval. Veeam ONE loads information about events through the Event Viewer.

To view the list of events:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure object.

4. Open the **Tasks & Events** tab.

5. The **Tasks & Events** list can display up to 1000 tasks and events at a time. To find the necessary task or event, you can use the following controls:

   o To display tasks or events for a specific period, select the necessary time interval from the **Events from** list.

   o To show or hide tasks or events, use filter buttons at the top of the list — *Show all events*, *Show errors*, *Show warnings*, *Show info messages*, *Show user events*, *Show tasks*.

   o To find the necessary tasks or events by description, use the **Search** field at the top of the list.

6. To view the detailed description of an event, click it in the list.

   The event description will be shown in the **Event Details** pane at the bottom.

   When you choose a virtual infrastructure container in the inventory pane, you can view events for the selected object and events for its child objects. To hide events related to child objects, clear the **Include events from child objects** check box at the bottom of the **Event Details** section.

7. To export displayed events to a CSV file, click the **Export to CSV** at the top of the list and specify the location where the file will be saved.

For every event in the list, the following details are available:

- Event type (*User*, *Info*, *Warning* or *Error*)

- Short event description

- Time of occurrence

- Event target

- Object that caused or initiated the event
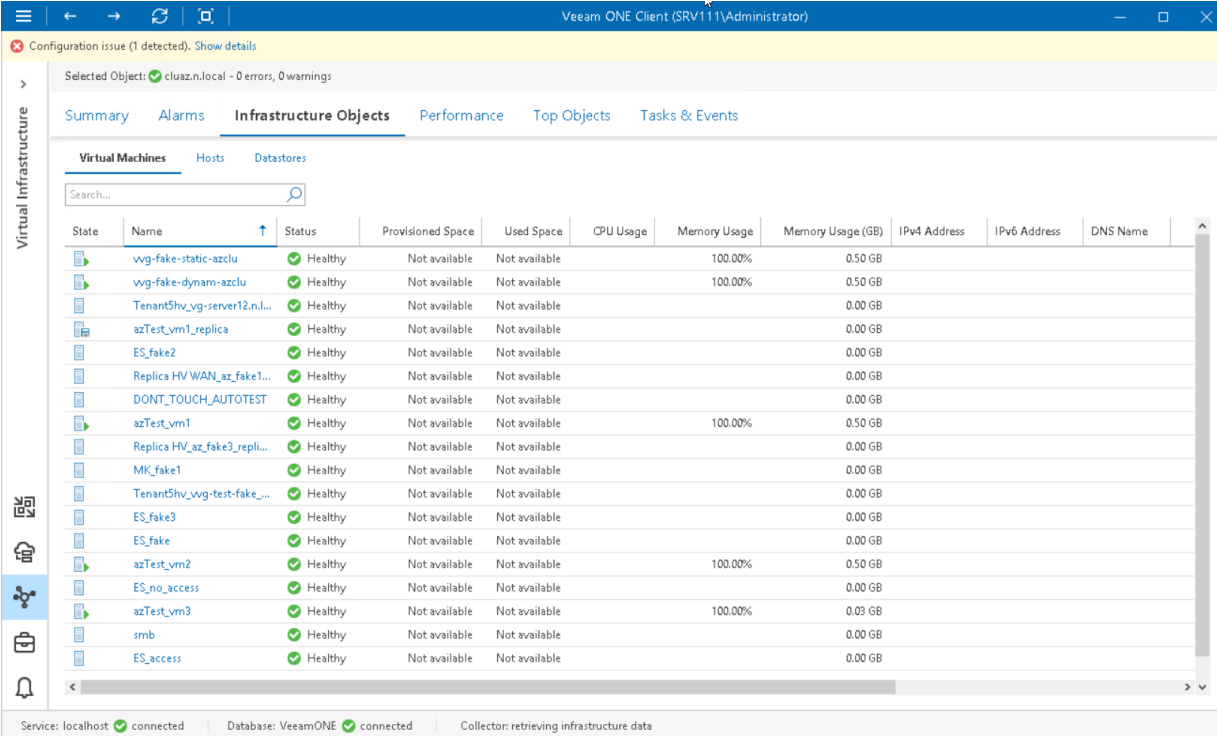
Microsoft Hyper-V Virtual Machines

You can view the list of VMs within a virtual infrastructure container — on a host, on a volume, in a folder and so on.

To view the list of VMs:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure container.

4. Open the **Infrastructure Objects** tab and navigate to **Virtual Machines**.

5. To find the necessary VM by name, use the **Search** field at the top of the list.

6. Click column names to sort VMs by a specific parameter.

   For example, to view what VMs are consuming the greatest amount of memory, you can sort VMs in the list by **Memory Usage**.

For every virtual machine in the list, the following details are available:

- **State** — state of the virtual machine (*powered on*, *powered off*, *saved*, *paused*)

- **Name** — name of the virtual machine

- **Status** — current status of the virtual machine in terms of alarms (*healthy*, *warning* or *error*)

- **Host** — name of the host where the virtual machine resides

- **Provisioned Space** — amount of storage space provisioned for the virtual machine

- **Used Space** — amount of storage space actually used for storing virtual machine files (for VMs with thin provisioned disks, this value is normally less than Provisioned Space)

- **CPU Usage** — amount of actively used virtual CPU as a percentage of total available CPU resources

- **Memory Usage** — amount of actively used memory resources as a percentage of configured VM memory

- **Memory Usage (GB)** — amount of actively used memory resources in GB

- **IP V4 Address** — IP V4 address assigned to the virtual machine

- **IP V6 Address** — IP V6 address assigned to the virtual machine

- **DNS Name** — DNS name of the virtual machine

- **vCPU** — number of virtual CPUs configured for the virtual machine

- **Assigned Memory** — amount of virtual memory allocated for the virtual machine

- **Guest OS** — guest operating system installed in the virtual machine

- **Integration Services** — number and state of Hyper-V Integration Services installed in the guest OS

You can choose what columns to show or hide in the **Virtual Machines** table:

- To hide one or more columns, right-click the table header and clear check boxes for corresponding data fields.

- To make hidden columns visible, right-click the table header and select check boxes for corresponding data fields.

Microsoft Hyper-V Hosts

You can view the list of Microsoft Hyper-V hosts in your virtual infrastructure — on System Center Virtual Machine Manager or in a cluster.

To view the list of hosts:

1. Open Veeam ONE Client.

    For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure container.

4. Open the **Infrastructure Objects** tab and navigate to **Hosts**.

5. To find the necessary host by name, use the **Search** field at the top of the list.

6. Click column names to sort hosts by a specific parameter.

    For example, to view hosts with the greatest number of VMs, you can sort VMs in the list by **VM Count**.

For every host in the list, the following details are available:

- **Name** — name of the host

- **Parent Object** — name of the parent object in the infrastructure

- **CPU Count** — number of CPU cores on a host

- **CPU Frequency** — frequency of a host CPU core in GHz

- **Memory Size** — amount of physical memory available on a host

- **VM Count** — number of VMs that reside on a host

You can choose what columns to show or hide in the **Hosts** table:

- To hide one or more columns, right-click the table header, and clear check boxes next to the corresponding data fields.

- To make hidden columns visible, right-click the table header, and select check boxes next to the corresponding data fields.
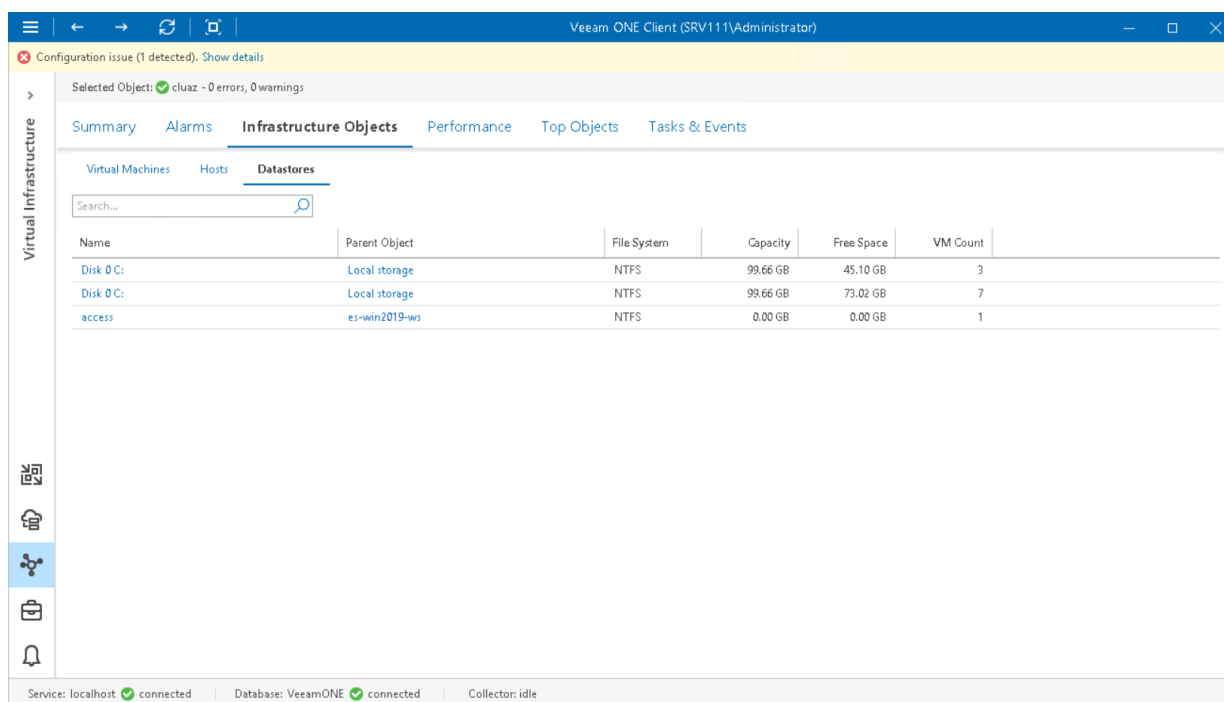
Microsoft Hyper-V Datastores

You can view the list of datastores in your Microsoft Hyper-V infrastructure — on System Center Virtual Machine Manager or in a cluster.

To view the list of datastores:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure container.

4. Open the **Infrastructure Objects** tab and navigate to **Datastores**.

5. To find the necessary datastore by name, use the **Search** field at the top of the list.

6. Click column names to sort datastores by a specific parameter.

   For example, to view what datastores have the greatest amount of free space, you can sort datastores in the list by **Free Space**.

For every datastore in the list, the following details are available:

- **Name** — name of a datastore

- **Parent Object** — name of the parent object in the infrastructure

- **File System** — type of the file system on the datastore

- **Capacity** — total capacity of a datastore

- **Free Space** — amount of available free space on a datastore

- **VM Count** — number of VMs that reside on a datastore

You can choose what columns to show or hide in the **Datastores** table:

- To hide one or more columns, right-click the table header, and clear check boxes next to the corresponding data fields.

- To make hidden columns visible, right-click the table header, and select check boxes next to the corresponding data fields.

Microsoft Hyper-V Top Objects

The top and lowest load dashboards help you detect VMs and hosts consuming the greatest or the smallest amount of resources in the selected virtual infrastructure segment.

- **Top Hyper-V VMs** dashboard displays top VM consumers in terms of CPU, memory, storage, network usage, snapshot age and size.

- **Top Hyper-V Hosts** dashboard displays top hosts in terms of CPU, memory, disk and network usage.

- **Bottom Hyper-V Hosts** dashboard displays least loaded hosts in terms of CPU, memory, disk and network resource usage.

  You can use this dashboard to choose hosts where you can deploy new VMs or to which you can move existing VMs.

To detect the most or least loaded hosts or VMs:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure container.

4. Open the **Top Objects** tab and navigate to necessary dashboard — **Top Hyper-V VMs**, **Top Hyper-V Hosts** or **Bottom Hyper-V Hosts**.

5. Click the **Change Options** link in the top left corner of the dashboard.

   o In the **Interval** field, set the time interval for which resource utilization statistics must be analyzed.

   o In the **VMs to display/Hosts to display** field, define the number of objects to display on the dashboard.

6. Click the **Select Counters** link in the top left right corner of the dashboard.

   a. In the **Select counters** window, choose metrics that must be included in the dashboard. Press and hold the `[SHIFT]` or `[CTRL]` key on the keyboard to select multiple counters.

b. Click **OK**.

Microsoft Hyper-V VM Console

From within the VM console, you can easily isolate the root cause of VM performance problems and execute management tasks — for example, restart an unresponsive VM.

This option requires no additional software installed on the Veeam ONE server and is available for both Window-based and Linux-based OS's.

Prerequisites

To access the console of a Linux-based VM, you must download PuTTY.exe and provide path to it in Veeam ONE Client client settings.

Accessing VM Console

You can access the VM console right from the Veeam ONE Client interface:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary VM.

4. Open the **Console** tab.
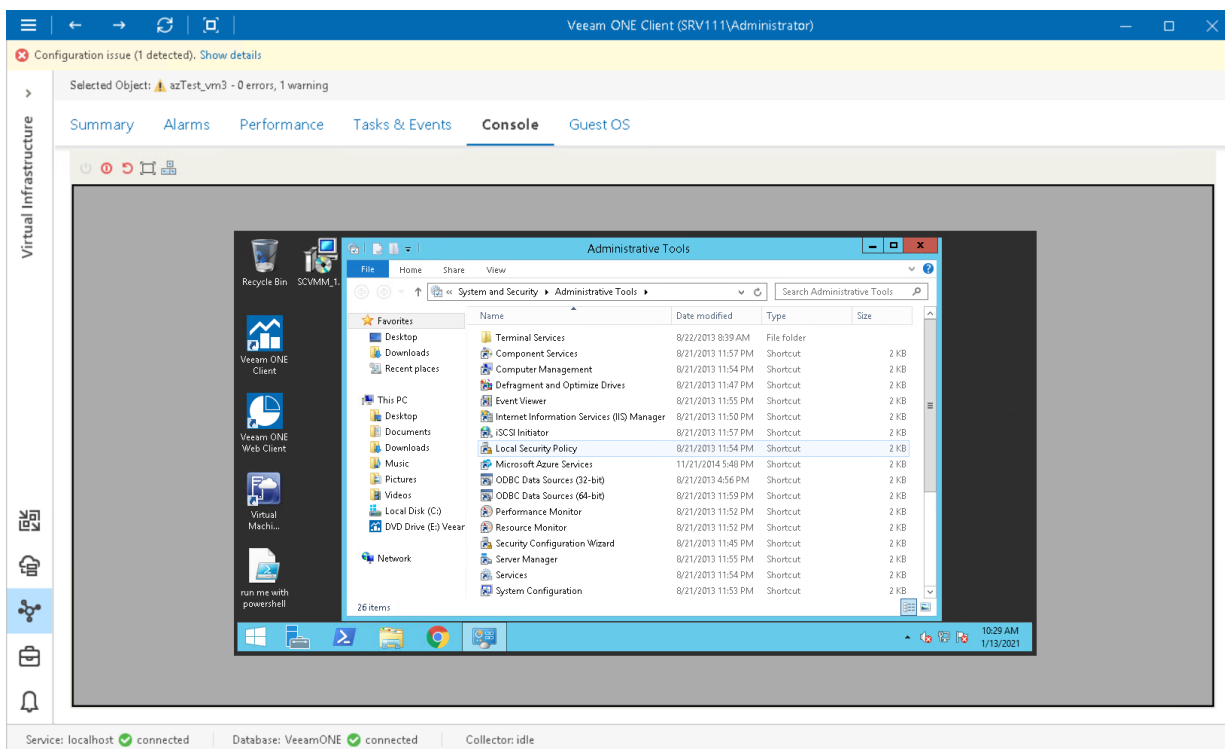
You can use buttons at the top of the **Console** tab to change the VM power state:

- **Power on** — powers on a VM if it is powered off. Resumes a VM if it is paused.

- **Power off** — shuts down the guest OS and powers off a VM.

- **Hard reset** — resets a VM without waiting for the guest OS and VM processes to stop. It is recommended to use this option only if you want to reboot a stuck or unresponsive VM.

- **Full screen** — switches between the full screen mode and a separate window running the VM console.

- **Send Ctrl+Alt+Del** — sends the **[Ctrl+Alt+Del]** command to a VM.

To access the VM console or change the VM power state, you can also right-click the VM in the inventory pane and use one of the following shortcut menu commands:

- To access the VM using Windows Remote Desktop Connection, choose **Remote Management > Connect to VM**.

- To change the VM power state, choose **Remote Management** and click the necessary command.

- To send the [Ctrl+Alt+Del] command to the VM, choose **Send Ctrl+Alt+Del**. Note that this command is only available if the **VM Console** tab is active.

Microsoft Hyper-V In-Guest Processes

You can view and control processes that are currently running inside a virtual machine or host.

- On Windows-based machines, you can view, end or restart processes.

- On Linux-based machines, you can view or end daemons.

Prerequisites

For Linux-based machines, make sure that the SSH Server is started.

Viewing In-Guest Processes

To view the list of processes:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure object.

4. Open the **Processes** tab.

5. Provide OS authentication credentials (user name and password) to access the list of running processes.

Every process is described with a set of counters that are presented as column headings. You can add or remove counters to monitor running processes:

1. In the upper right corner of the **Processes** dashboard, click the **Select columns** link.

2. In the **Select Columns** window, select check boxes next to counters you want to display.

3. To view a detailed description of a counter, click it in the **Counters** list, and the description will be displayed in the lower pane of the window.
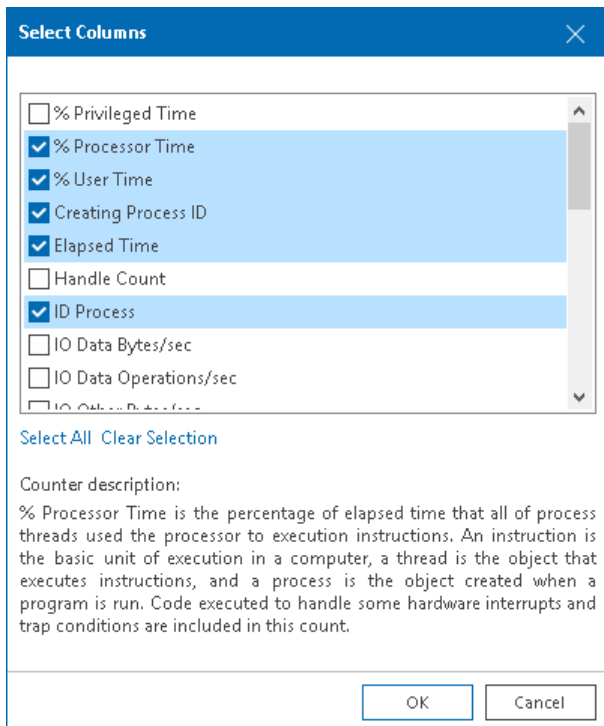
You can end unwanted processes running on the VM or create an alarm based on the process state or object performance:

- [For Windows-based machines] To end a process, select it in the list and click the **Kill Process** button, or right-click a necessary process and select **Kill Process** from the shortcut menu.

- [For Linux-based machines] To end a daemon, select it in the list and click the **Kill Process** button and choose one of the following options:

  - **Hangup** — to send the `SIGHUP` signal

  - **Kill** — to send the `SIGKILL` signal

  - **Terminate** — to send the `SIGTERM` signal

  You can also right-click a necessary process and select **Kill Process** and choose the necessary option from the shortcut menu.

- [For Windows-based machines] To create an alarm, select one or more processes in the list, click the **Create Alarm** button, and select the type of rule on which the alarm must be based. For more information, see Alarm Rules.

Microsoft Hyper-V In-Guest Services

You can view and control services currently running inside a VM.

- For Windows-based machines, you can view, start, stop and restart services, and create alarms based on retrieved services.

- For Linux-based machines, you can view, start, stop and restart services.

Prerequisites

For Linux-based machines, make sure that the SSH Server is started.

Viewing In-Guest Services

To view the list of services:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Virtual Infrastructure**.

3. In the inventory pane, select the necessary infrastructure object.

4. Open the **Services** tab.

5. Provide OS authentication credentials (user name and password) to access the list of running services.

You can start, stop and restart a running service, or create an alarm based on the service state or object performance:

- To restart a service, click the **Restart** button, or right-click a necessary service and select **Restart** from the shortcut menu.

- To disconnect from guest OS, click the **Disconnect** button.

- [For Windows-based machines] To create an alarm, select a service in the list, click the **Create Alarm** button, and select the type of rule on which the alarm must be based. For more information, see Alarm Rules.

Business View

Veeam ONE Client can present your virtual infrastructure from the technical perspective (in terms of VMware vSphere or Microsoft Hyper-V inventory), and from the business perspective (based on your company needs and priorities). Veeam ONE Client presents infrastructure objects from the business perspective using categorization capabilities provided by the embedded Business View component.

Business View allows you categorize virtual and backup infrastructure objects — VMs, hosts, clusters, datastores, enterprise applications and computers protected with Veeam backup agents — according to constructs of your business. You can categorize virtual infrastructure objects by such criteria as business unit, department, purpose, SLA and others. Categorization data is continuously synchronized with Veeam ONE Client and Veeam ONE Web Client, and enables you to monitor, troubleshoot, resolve issues and report on business groups of infrastructure objects. For more information on creating categories and groups for the objects in your infrastructure, see Configuring Business View Categorization.

To work with the business view of your infrastructure in Veeam ONE Client, click **Business View** at the bottom of the inventory pane. In this view, you can use monitoring capabilities for business groups created for your virtual environment. For more information on monitoring capabilities for Business View groups, see Business View Monitoring.
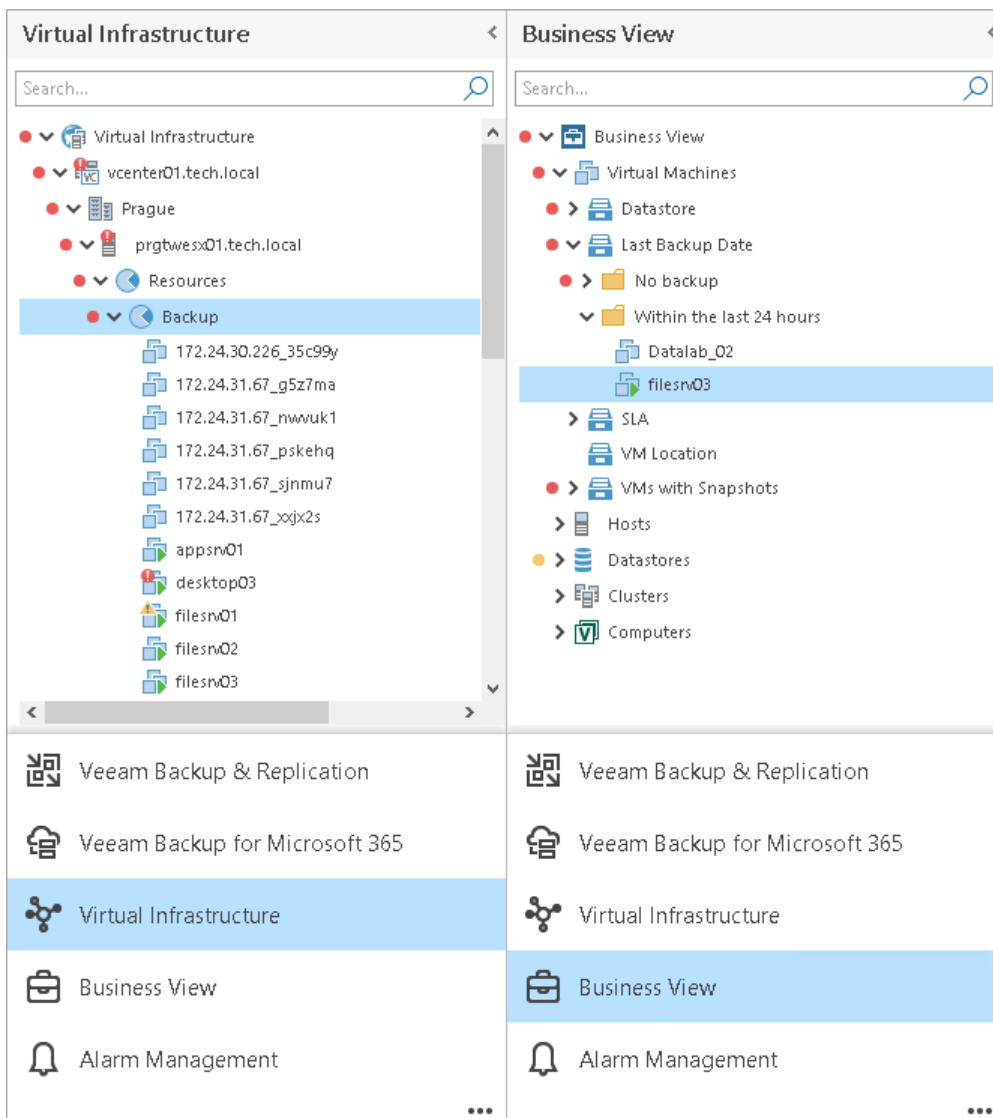
Configuring Categorization Model

To present the virtual infrastructure, Veeam ONE Client uses the model that includes categories, groups and objects:

- **Category** is a logical division or a sector of the infrastructure. Each category includes one or more groups.

  Categories can be static or dynamic:

  - **Static** categories include a user-defined number of groups. You can manually create groups that Veeam ONE will populate each time data collection runs.

  - **Dynamic** categories can include one or more groups that Veeam ONE creates and populates automatically each time data collection runs.

- **Group** is a collection of infrastructure objects that share same characteristics, or match same criteria. You can think of a group as a tag assigned to an object.

  Each group includes one or more objects.

- **Objects** are categorized elements of the infrastructure.

  In Veeam ONE Client you can categorize the following types of objects: clusters, hosts, storage objects, VMs, computers protected with Veeam backup agents and enterprise applications. You can include an object into one or more groups within a category.

The following picture illustrates an example of Veeam ONE categorization model.
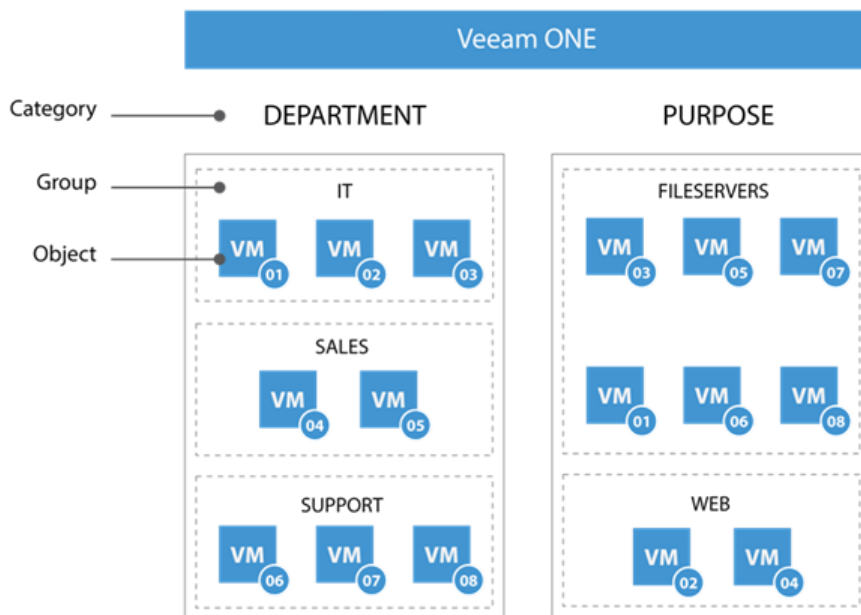
In the example above, the categorization model includes categories *Department* and *Purpose*.

- *Department* category includes groups *IT*, *Sales* and *Support*

- *Purpose* category includes groups *Fileservers* and *Web*

Virtual machines numbered 1-8 are included in groups within both categories.

Predefined Categories

Out of the box, Veeam ONE Client comes with a number of predefined categories:

- **Datastore** — dynamically groups VMs by datastore where VM files reside.

- **Location** — dynamically groups by location computers managed by Veeam Backup & Replication.

- **Last Backup Date** — dynamically groups VMs, computers and enterprise applications by the age of the latest restore point.

- **SLA** — category with static groups for all types of virtual infrastructure objects. Includes two predefined groups: *Mission Critical* and *Other*.

- **Storage Type** — dynamically groups storage objects by type.

- **VM Location** — dynamically groups by location VMs protected with Veeam Backup & Replication.

- **VMs with Snapshots** — dynamically groups VMs with snapshots by the snapshot age.

You can use predefined categories for your categorization model. If predefined categories are not enough, you can create custom categories and edit predefined categories or import an existing categorization model.

Creating Business View Categories and Groups

To categorize objects into groups automatically, you can use the following methods:

- Single-Parameter Categorization — the method that allows you to configure dynamic categories. Veeam ONE will create groups automatically based on the values of a single property of an object.

- Multiple-Condition Categorization — the method that allows you to configure static categories and create groups manually by combining multiple object properties and logical operators.

- Grouping Expressions — the method that allows you to configure dynamic categories. Veeam ONE will create groups automatically based on object properties, operators and methods included into expression.

Configuring Single-Parameter Categorization

Single-parameter categorization is based on object properties specified within a hypervisor and Veeam Backup & Replication server. When you select a property as a categorization condition, Veeam ONE automatically creates a group for each unique value of the selected property. All objects with the same property value will fall into one group.

Groups created using the single property method have dynamic membership. If the property value changes, the object can be moved into another group or excluded from categorization when the next data collection runs.

For example, you can categorize VMs based on their power state. After data collection, Veeam ONE will create three groups: **Powered On**, **Powered Off** and **Suspended**. If a VM power state changes, this VM will be moved into another group next time data collection runs.

To categorize objects using a single property:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the inventory pane, navigate to the **Business View** node.

3. Launch the **Categorization Wizard**:

   a. In the information pane, switch to the **Categories** tab.

b. In the **Actions** pane, click **Add Category**.

Alternatively, in the **Business View** tree, right-click the main node and select **Add Category**.

4. At the **Name and Object Type** step of the wizard, enter a category name and select an object type.

You can select the following types of objects: *Virtual Machine*, *Host*, *Cluster*, *Storage*, *Computer*, *Enterprise Application*.

If you select the *Computer* or *Enterprise Application* object type, continue with step 6 of this procedure.

5. At the **Platform** step of the wizard, select the platform for which you want to categorize objects: *VMware vSphere* or *Microsoft Hyper-V*.

6. At the **Categorization Method** step of the wizard, select *Single parameter*.

7. At the **Grouping Criteria** step of the **Categorization Wizard,** select an object property.

   If you selected the *Computer* or *Enterprise Application* object type, click **Save** to finish working with the wizard.

8. At the **Export** step of the wizard, choose whether you want to export Business View categorization data:

   o [For VMware vSphere objects] Select **Create vSphere tags** if you want to display Business View categories and groups in vCenter Server.

   Veeam ONE will export categories as tag categories and groups as tags.

   o [For Microsoft Hyper-V objects] Select **Create Hyper-V custom properties** if you want to display Business View categories and groups in System Center Virtual Machine Manager.

   Veeam ONE will export categories as custom properties and groups as property values.

   Veeam ONE will periodically overwrite created tags and custom properties to keep categorization data in synchronization with vCenter Server and System Center Virtual Machine Manager.

> **NOTE:**
>
> This step is not available if you enable import of categorization data from vCenter Server, System Center Virtual Machine Manager. For more information on importing categorization model, see Selecting Categorization Model.

9. Click **Save**.

   Veeam ONE will create an individual group for each unique value of the selected property.

Configuring Multiple-Condition Categorization

Multiple-condition categorization allows you to combine multiple conditions that evaluate object properties for creating groups. This method makes categories highly customizable, as each group within a category can have its own condition. Conditions can be based on different object properties and logical operators. For one group, you can specify one or more conditions and link them with the **AND** and **OR** operators.

Groups created with the multiple-condition method have dynamic membership. If the property value changes, the object can be moved into another group or excluded from categorization after the next data collection.

For example, you can categorize VMs based on their power state, datacenter name and guest OS at the same time. If any of these properties change, the VM will be moved into another group or excluded from categorization.

To create groups using multiple conditions:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the inventory pane, navigate to the **Business View** node.

3. Launch the **Categorization Wizard**:

   a. In the information pane, switch to the **Categories** tab.

b. In the **Actions** pane, click **Add Category**.

Alternatively, in the **Business View** tree, right-click the main node and select *Add Category*.

4. At the **Name and Object Type** step of the `wizard,` enter a category name and select an object type.

You can select the following types of objects: *Virtual Machine*, *Host*, *Cluster*, *Storage*, *Computer*, *Enterprise Application*.

If you select the *Computer* or *Enterprise Application* object type, continue with step 6 of this procedure.

5. At the **Platform** step of the wizard, select the platform for which you want to categorize objects.

6. At the **Categorization Method** step of the **wizard,** select *Multiple conditions*.

7. At the **Grouping Criteria** step of the **wizard,** click **Add** to create groups based on multiple conditions.

The **Add Group** wizard will open.

8. At the **Group Name** step of the wizard, specify a group name and description.

9. At the **Grouping Conditions** step of the **Add Group** wizard, set up categorization conditions:

   o From the **Property** drop-down list, select an object property.

   The list contains all object properties that Veeam ONE collects from a hypervisor and Veeam Backup & Replication servers.

   o From the **Operator** drop-down list, select a conditional operator.

   The list contains the following operators: *Equals, Does not equal, Starts with, Contains, Does not contain*.

o   In the `Value` field, specify a value that will be checked in the condition.

The condition will be evaluated against discovered objects. To add another condition, click **Add Condition**.

By default, conditions are linked by the **AND** operator. That is, an object falls into a group when all specified conditions are met. You can change this behavior by linking conditions with the **OR** operator. In this case, an object will fall into a group when a condition for any of the linked rules is met.

For example, you can create a group which will include VMs based on their power state, datacenter name and guest OS. If you want the group to include all powered on VMs that reside in datacenter Atlanta or run Linux as their guest OS, you must link these conditions. The second and the third conditions will be linked to each other with the **OR** operator. The first condition will be linked to them with the **AND** operator.

> **NOTE:**
>
> Linking supports 3 levels of nesting.

To link conditions:

a. Select check boxes next to the necessary conditions and click **Link**.

b. In the **Rule condition** window, select a link operator and click **OK**.

10. [Optional] At the **Notifications** step of the wizard, specify notification settings:

a. Select the **Email address** check box and specify an email address of a person who will receive notifications about alarms triggered for the objects in a group (group owner).

To receive alarm notifications, enable the **Send email to Business View group owner** option in alarm settings. For more information on configuring alarm notification settings, see Specify Alarm Notification Options.

b. Choose the notification policy:

- **Send email notification on every alarm** — select this option if you want to send an email notification every time a new alarm is triggered or the status of an existing alarm changes.

- **Send periodical summary every** — select this option and if you want to accumulate information about alarms and send an email notification once within a specific time interval. You can specify the time interval in minutes or hours.

11. Click **Save** to save a group configuration and close the **Add Group** wizard.

Group settings will appear in the **Categorization Wizard**.

12. Repeat steps **7-11** for each group you want to configure in the category.

If you selected the *Computer* or *Enterprise Application* object type, click **Save** to finish working with the wizard.

13. At the **Export** step of the wizard, choose whether you want to export Business View categorization data:

   o [For VMware vSphere objects] Select **Create vSphere tags** if you want to display Business View categories and groups in vCenter Server.

   Veeam ONE will export categories as tag categories and groups as tags.

   o [For Microsoft Hyper-V objects] Select **Create Hyper-V custom properties** if you want to display Business View categories and groups in System Center Virtual Machine Manager.

   Veeam ONE will export categories as custom properties and groups as property values.

   Veeam ONE will periodically overwrite created tags and custom properties to keep categorization data in synchronization with vCenter Server and System Center Virtual Machine Manager.

> **NOTE:**
>
> This step is not available if you enable import of categorization data from vCenter Server, System Center Virtual Machine Manager. For more information on importing categorization model, see Selecting Categorization Model.

14. Click **Save**.

Configuring Categorization Using Grouping Expressions

Grouping expressions are used to find objects that share common properties. When you configure categorization with grouping expression, Veeam ONE creates a set of groups, and includes objects with matching attributes into these groups.

Groups created with grouping expressions have dynamic membership. If the property value changes, the object can be moved into another group or excluded from categorization after the next data collection.

For example, you can create an expression that will divide VMs into groups by the guest OS name. Veeam ONE will create groups with the names of guest OSes that VMs in your infrastructure run. Each group will include VMs with the same guest OS.

To create groups using expressions:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the inventory pane, navigate to the **Business View** node.

3. Launch the **Categorization Wizard**:

   a. In the information pane, switch to the **Categories** tab.

   b. In the **Actions** pane, click **Add Category**.

   Alternatively, in the **Business View** tree, right-click the main node and select *Add Category*.
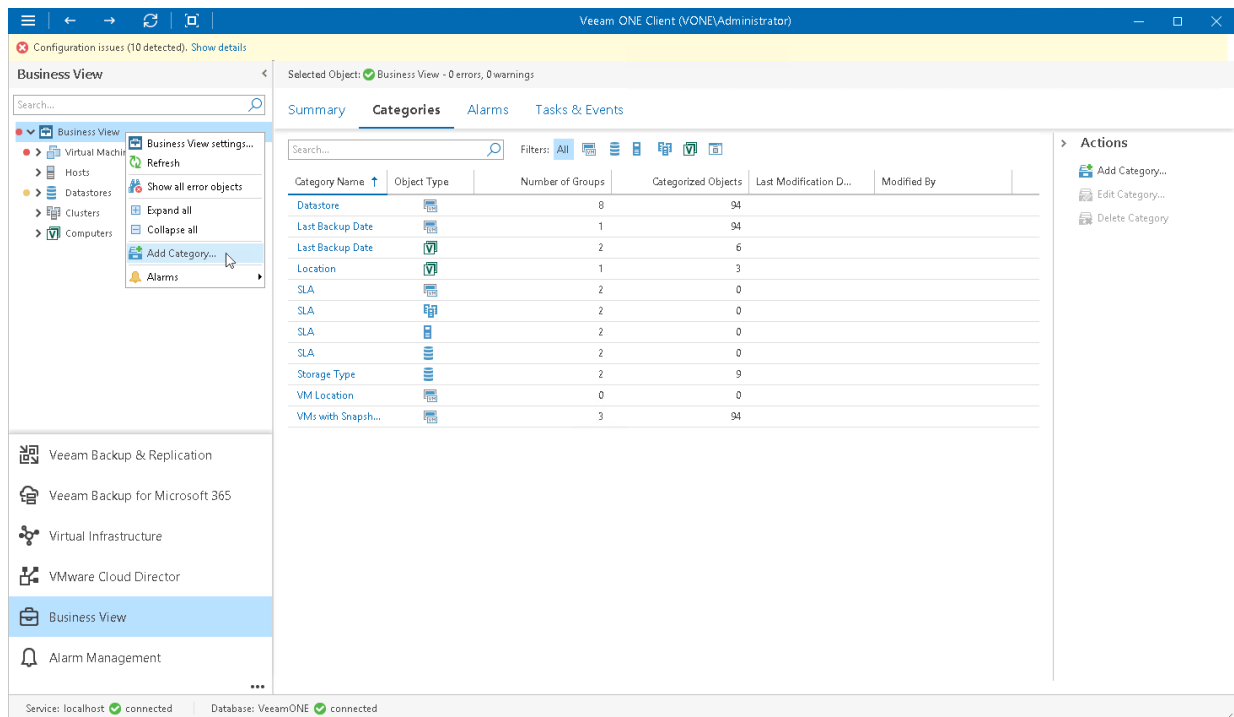
4. At the **Name and Object Type** step, enter category name, select object type and click **Next**.

   You can select the following types of objects: *Virtual Machine*, *Host*, *Cluster*, *Storage*, *Computer*, *Enterprise Application*.

If you select the *Computer* or *Enterprise Application* object type, continue with step 6 of this procedure.

5. At the **Platform** step of the wizard, select the platform for which you want to categorize objects.

6. At the **Categorization Method** step of the wizard, select *Grouping expression*.

7. At the **Grouping Criteria** step of the wizard, specify an expression that Veeam ONE must use to create groups and distribute infrastructure objects in these groups:

   a. Click the **Editor** button to open the **Grouping Expression Editor**.

   b. In the menu on the left, double click an item to add it to the **Expression** field.

   c. Click **Save** to save the expression and exit the editor.

To check the created script, click the **Verify** button.

For more information on the syntax of grouping expressions, see Appendix B. Grouping Expressions Syntax.

If you selected the *Computer* or *Enterprise Application* object type, click **Save** to finish working with the wizard.

8. At the **Export** step of the wizard, choose whether you want to export Business View categorization data:

   o [For VMware vSphere objects] Select **Create vSphere tags** if you want to display Business View categories and groups in vCenter Server.

   Veeam ONE will export categories as tag categories and groups as tags.

   o [For Microsoft Hyper-V objects] Select **Create Hyper-V custom properties** if you want to display Business View categories and groups in System Center Virtual Machine Manager.

   Veeam ONE will export categories as custom properties and groups as property values.

> **NOTE:**
>
> This step is not available if you enable import of categorization data from vCenter Server, System Center Virtual Machine Manager or a 3rd party application. For more information on importing categorization model, see Selecting Categorization Model.

9. Click **Save**.

Adding Objects to Groups Manually

You can manually add objects to groups in static categories — categories created with multiple-condition method and imported manually from a CSV file. When you map an object to a group, Veeam ONE adds the **Manual selection** condition to the group configuration. The name of an object acts as condition value. Mapped objects have static group membership, that is, they remain in the group until you manually reset categorization values. For more information on resetting, see Resetting Categorization Values.

> **TIP:**
>
> To add objects to groups within multiple categories in a batch, you can describe these objects and groups in a CSV file and import this file to Veeam ONE Client. For more information on importing categorization data from a CSV file, see Importing and Exporting Using CSV File.

Mapping Objects to Groups

To add objects to a group:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the inventory pane, navigate to the **Business View** node.

3. In the **Business View** tree, select the necessary object type — Virtual Machines, Hosts, Datastores, Clusters, Computers or Enterprise Applications.

4. Open the tab with the name of the object: *Virtual Machines*, *Hosts*, *Datastores*, *Clusters*, *Computers*, *Enterprise Applications*.

5. Select objects that you want to add to a group.

   To quickly find necessary objects, use the scope drop-down list and search field at the top of the objects list.

   Press and hold the `[CTRL]` or `[SHIFT]` key on the keyboard to select multiple objects.

6. In the **Actions** pane, click **Manual Categorization**.

7. In the **Edit Categories** window, select a category and groups to which you want to add objects.

   The **Categories** section lists static categories to which you can add objects. To display all categories for the selected object type, select the **Show dynamic categories** check box.

8. Click **OK** to save the settings.
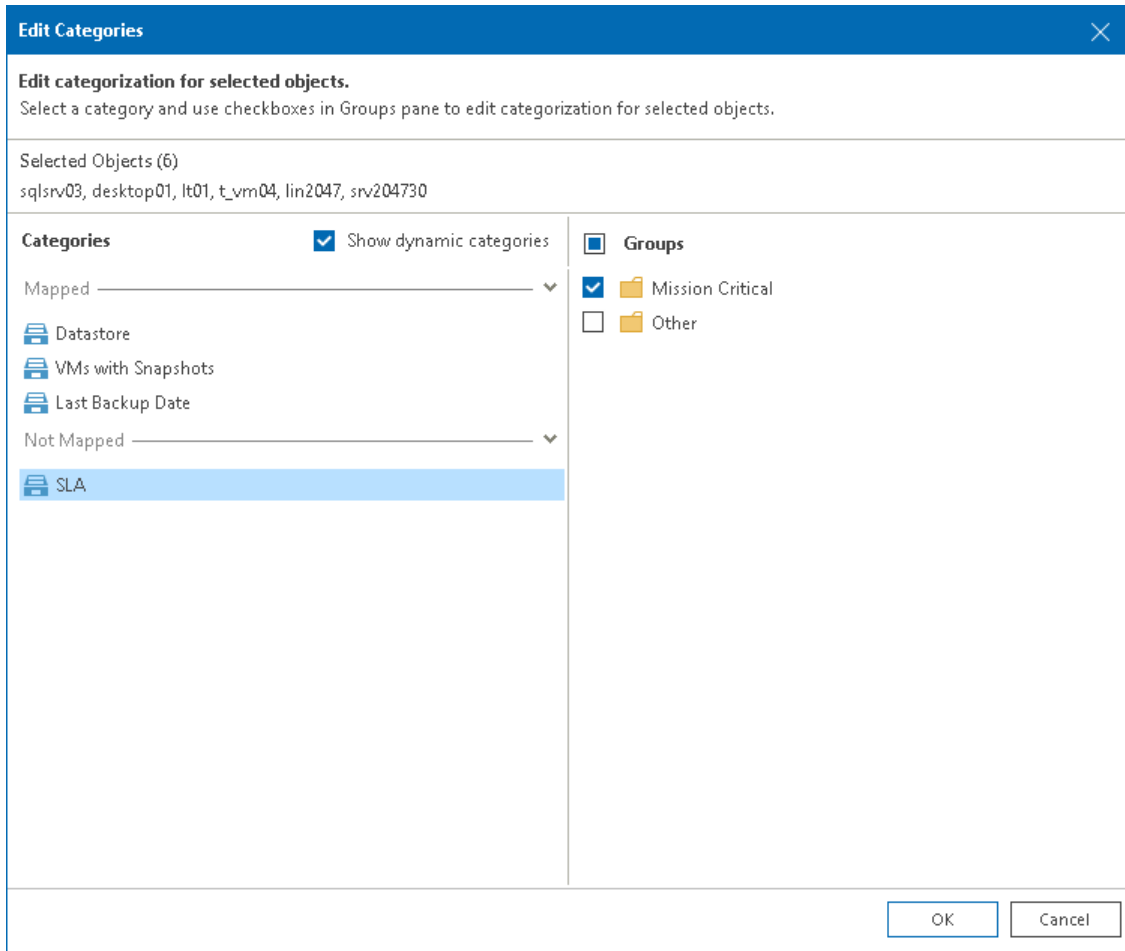
Resetting Categorization Values

You can remove objects from categories and groups to which you manually added these objects.

To remove objects from groups:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the inventory pane, navigate to the **Business View** node.

3. In the **Business View** tree, select the necessary object type — *Virtual Machines*, *Hosts*, *Datastores*, *Clusters*, *Computers* or *Enterprise Applications*.

4. Open the tab with the name of the object: *Virtual Machines*, *Hosts*, *Datastores*, *Clusters*, *Computers*, *Enterprise Applications*.

5. Select objects for which you want to reset categorization.

   To quickly find necessary objects, use the scope drop-down list and search field at the top of the objects list.

   Press and hold the `[CTRL]` or `[SHIFT]` key on the keyboard to select multiple objects.

6. In the **Actions** pane, click **Reset Categorization**.

7. In the **Reset Manual Categorization** window, click **OK** to confirm object removal.

Importing and Exporting Categorization Data

You can import and export categorization data and synchronize it with other applications. Veeam ONE offers the following synchronization possibilities:

- Importing Categorization Model from vCenter Server and System Center Virtual Machine Manager

  If you use vCenter Server tags and System Center Virtual Machine Manager custom properties to categorize virtual infrastructure objects on the vCenter Server or Microsoft Hyper-V side, you can import these tags and properties to create Business View groups in Veeam ONE. Each time data collection runs, tag categories and custom properties are imported as Business View categories, tags and property values are assigned to groups within these categories.

- Importing and Exporting Using CSV File

  You can synchronize Business View categorization data with categorization data from 3rd party software. In Veeam ONE, you can import categorization data from and export categorization data to a CSV file that acts as a medium between the two systems.

Importing Categorization Model from vCenter Server and System Center Virtual Machine Manager

You can import categorization model from vCenter Server and System Center Virtual Machine Manager.

When you enable synchronization of categorization data from virtualization servers, Veeam ONE Client imports tags and custom properties and creates categories and groups according to the values of imported tags and properties. Every time data collection runs, Veeam ONE Client overwrites created categories and groups to keep categorization data in synchronization with vCenter Server and System Center Virtual Machine Manager.

> **NOTE:**
>
> Consider the following:
>
> - Categories imported from vCenter Server and System Center Virtual Machine Manager are read-only, you cannot edit or delete them. To remove such categories from Business View tree, disable the option in Server Settings. For more information on Business View Server Settings, see Business View.
> - If Veeam ONE detects tags and custom properties with names that are already assigned to categories in Business View, it will exclude such tags and properties from synchronization.
> - While in categorization model imported from vCenter Server and System Center Virtual Machine Manager, if you create a new category, you will not be able to export it to tags.

To import tags and custom properties:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the main menu, click **Settings > Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Business View** tab.

4. Select **From vCenter Server and System Center Virtual Machine Manager**.

By default, Veeam ONE Client imports all tags and custom properties available on the vCenter Server and System Center Virtual Machine Manager side.

To select which tags and properties to import:

a. Click the **Tags** button.

b. Clear the check boxes next to tags that you want to exclude from import.
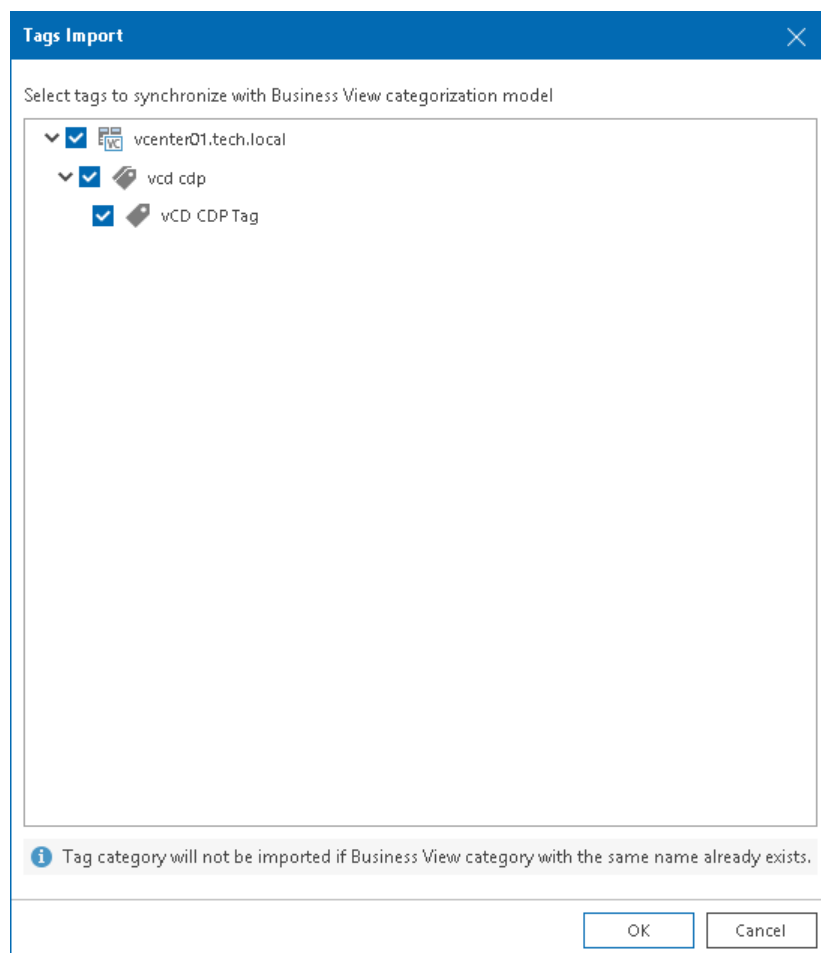
c. Click **OK** to save settings.

5. Click **OK** to close the **Server Settings** window.

Veeam ONE will import selected vCenter Server tags and System Center Virtual Machine Manager properties to create Business View categories and groups.

Importing and Exporting Using CSV File

In Veeam ONE, you can import and export categorization model using a CSV file.

Importing Categorization Data Manually

If you already categorized the virtual infrastructure objects outside Veeam ONE, you can describe categorization model using a CSV file and then import this file to Veeam ONE.

When you import a CSV file manually, Veeam ONE creates categories and groups specified in the file and maps objects to these groups. If Veeam ONE detects in the imported CSV file categories and groups that already exist in Business View, it will map objects specified in the CSV file to existing groups. Imported objects have static membership, that is, they remain in the group until you manually reset categorization values. For more information on manual mapping and resetting categorization values, see Adding Objects to Groups Manually.

> **NOTE:**
>
> To make sure that Veeam ONE will process the CSV file without errors, check the file structure. For more information on CSV file structure, see CSV File Structure.

To import categorization data from a CSV file:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the main menu, click **Settings > Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Business View** tab.

4. Click the **Import categorization model from CSV file once** link.

5. In the **Categorization Import** window, specify the path to the CSV file with the categorization data you want to import.

6. Click **Import**.
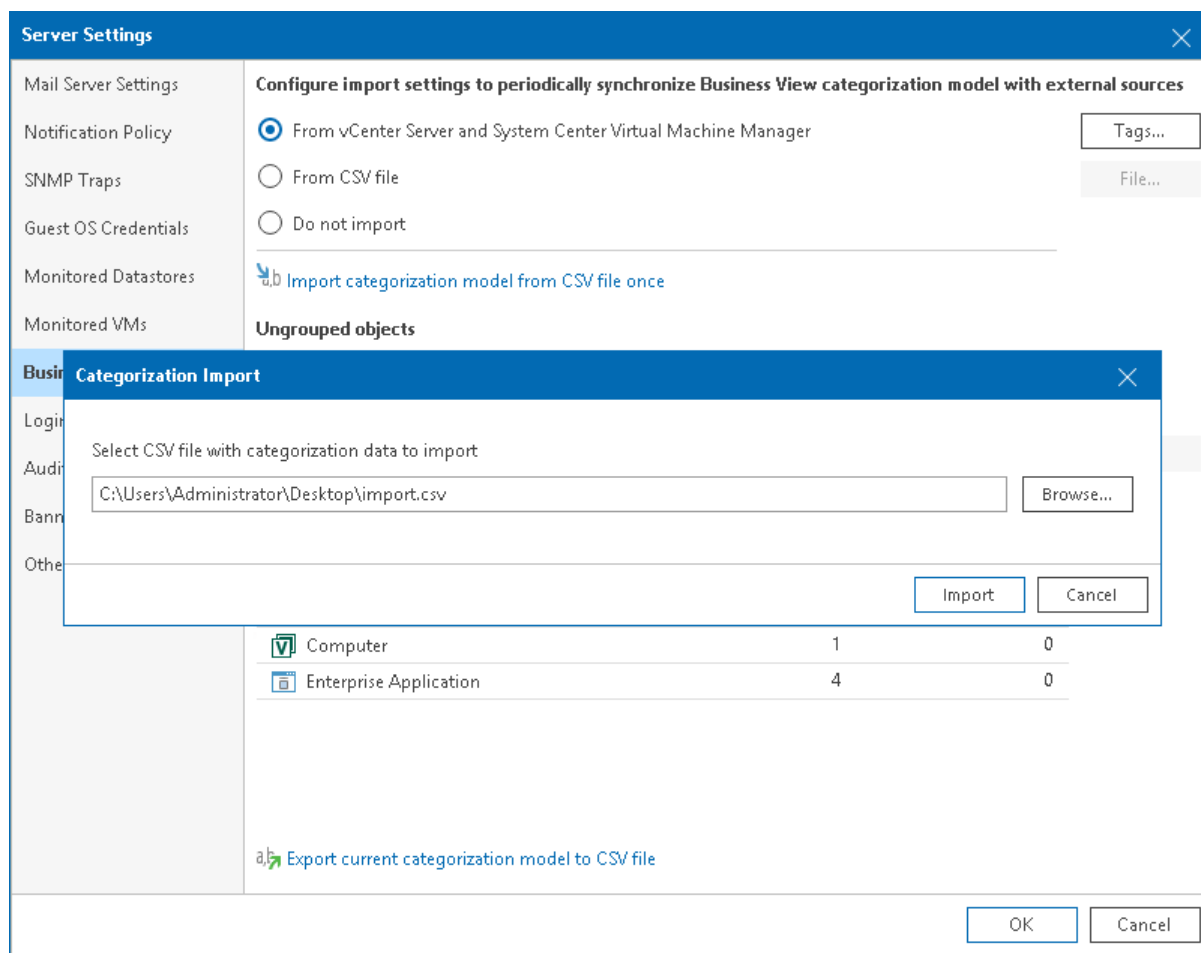
Importing Categorization Data Automatically

You can synchronize categorization data between Veeam ONE and a 3rd party application every time data collection runs. To do this, you can specify a path to a CSV file with the categorization data exported from a 3rd party application. Veeam ONE will import data from this file during every data collection session.

Additionally, you can specify a path to a script that must be triggered before data from the CSV file is imported. This can be a script that creates the CSV file based on data from a 3rd party application, or updates the file. For more information on structuring the file, see CSV File Structure.

> **NOTE:**
>
> If Veeam ONE detects in the specified CSV file categories that already exist in Business View, it will exclude such categories from synchronization.

To configure periodic synchronization of categorization data between Veeam ONE and a 3rd party application:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the main menu, click **Settings > Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Business View** tab.

4. Select **From CSV file** and click the **File** button.

5. In the **Categorization File** window, specify the path to the CSV file with the categorization data you want to synchronize.

6. If you want to trigger a custom script before data synchronization, select the **Execute this script before synchronizing with a CSV file** check box and specify a path to the script file.

> **NOTE:**
>
> The CSV and script files must reside in a folder that is accessible by *Veeam ONE Monitoring Service*. The account under which the service runs must have read permissions on the files.

7. Click **Save**.
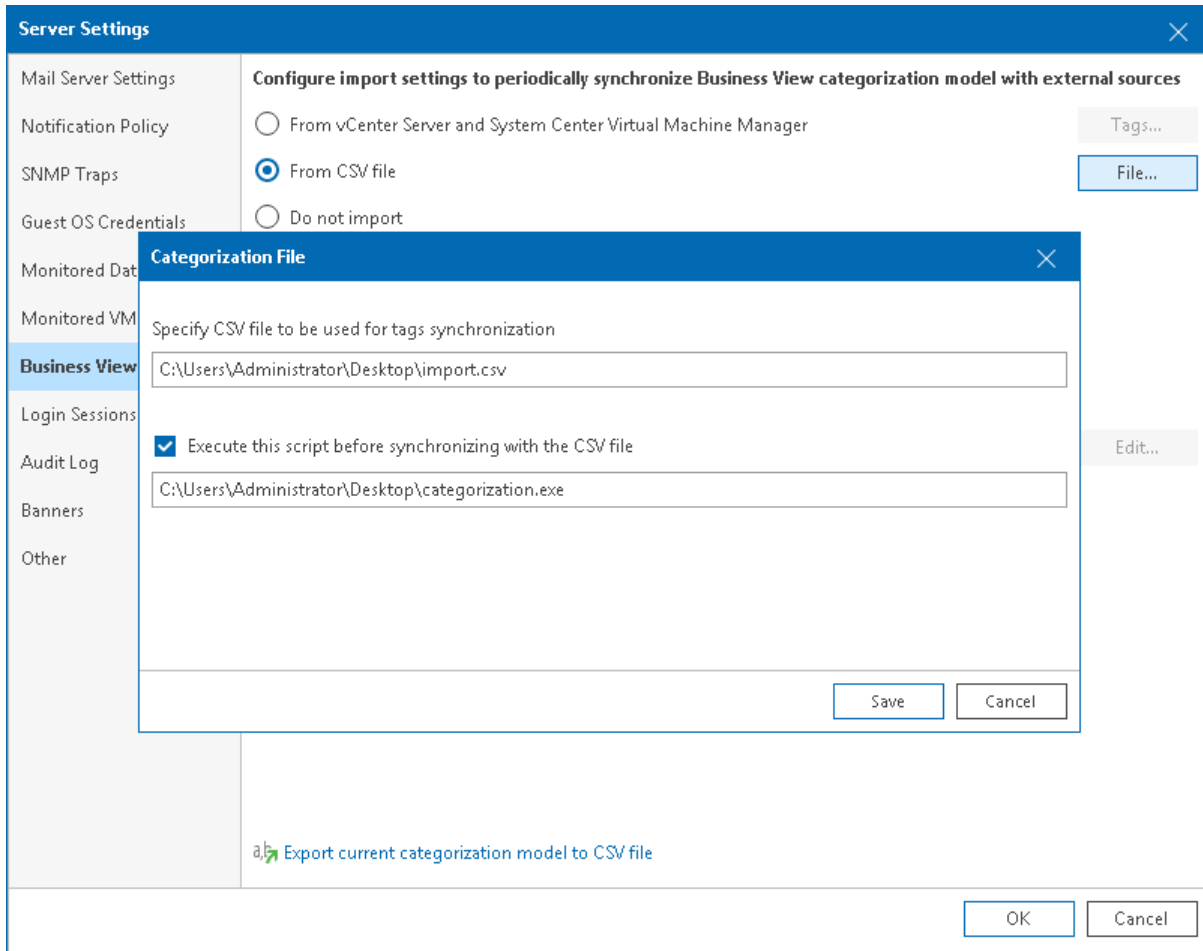
Exporting Categorization Data

To export Business View categorization data to a CSV file:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the main menu, click **Settings > Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Business View** tab.

4. At the bottom of the window, click the **Export current categorization model to CSV file** link, specify the location where the file must be saved and click **Save**.

5. In the **Veeam ONE Client** window, click **OK** to acknowledge export results.
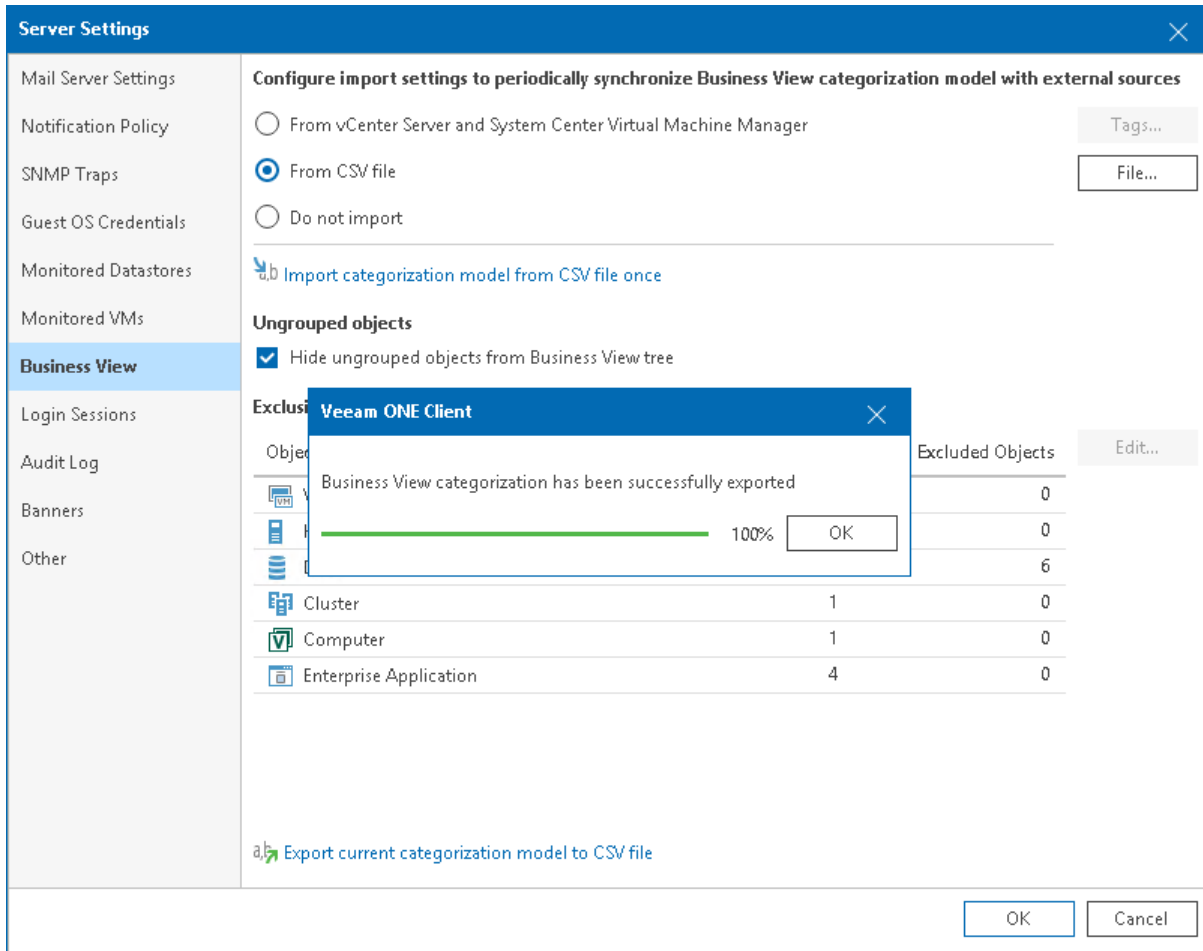
CSV File Structure

You can create a CSV file with categorization data from scratch. Every new record (row) in the file must describe an infrastructure object and its categorization data.

The following columns are mandatory for every record:

- **Server** — name of the managed virtual infrastructure or backup server to which object belongs.

- **ObjectType** — type of object (possible values are *VirtualMachine*, *HostSystem*, *Storage*, *ClusterComputerResource*, *HvCluster*, *HvCsvDisk*, *HvHost*, *HvPhysicalDisk*, *HvVirtualMachine*, *VeeamBpAgent*, *SMBShare*).

- **MoRef** — reference number of the object (for VMware vSphere), UUID or ID of the object (for Microsoft Hyper-V).

Other columns in the CSV file must be named as Business View categories. Category fields accept the following types of values:

- Name of a group within the category to which an infrastructure object belongs

- Empty field, if the object does not belong to any group within the category

- *Excluded*, if the object must be excluded from categorization

The following table shown as example of a CSV file for VMware vSphere VMs.

Server	ObjectType	MoRef	Category1
server.local	VirtualMachine	vm-01	Group1
server.local	VirtualMachine	vm-02	Excluded

Editing Business View Categories

You can edit Business View categories created in Veeam ONE Client as well as predefined categories and categories imported manually from a `csv` file.

To edit a category:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the inventory pane, navigate to the **Business View** node.

3. Open the **Categories** tab.

4. Select a category that you want to edit.

   To quickly find the necessary category, use filters and the search field at the top of the **Categories** list.

5. In the **Actions** pane, click **Edit Category**.

   Alternatively, right-click the category and select **Edit Category** from the shortcut menu.

6. Change the required category settings.

   For more information on category settings, see Creating Business View Categories.

Deleting Business View Categories

You can delete Business View categories created in Veeam ONE Client as well as predefined categories and categories imported manually from a `csv` file. When you delete a category, objects from this category remain in your infrastructure.

To delete a category:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the inventory pane, navigate to the **Business View** node.

3. Open the **Categories** tab.

4. Select a category that you want to delete.

   To quickly find the necessary category, use filters and the search field at the top of the **Categories** list.

5. In the **Actions** pane, click **Delete Category**.

   Alternatively, right-click the category and select **Delete Category** from the shortcut menu.

Business View Monitoring

Veeam ONE Client allows you to monitor infrastructure presented from the business perspective — that is, based on Business View categories and groups of VMs, hosts, datastores, clusters, computers and enterprise applications.

With Veeam ONE, you can:

- Monitor the overall state of the categorized infrastructure

- View triggered alarms

- View objects included in categories and groups

- Work with performance charts

- View the list of events

Business View Summary Dashboards

Veeam ONE Client comes with a set of summary dashboards for business view groups that include infrastructure objects. These dashboards allow you to:

- Review the summary details for all VMs, hosts, datastores, clusters, computers and enterprise applications in custom groups

- View latest alarms

- Troubleshoot issues by drilling down to specific objects in groups

To access a summary dashboard for a virtual infrastructure object or virtual infrastructure segment:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Business View**.

3. In the inventory pane, select the necessary node.

4. Open the **Summary** tab.

Business View Summary

The Business View summary dashboard presents the health status overview for objects in all available Business View groups.
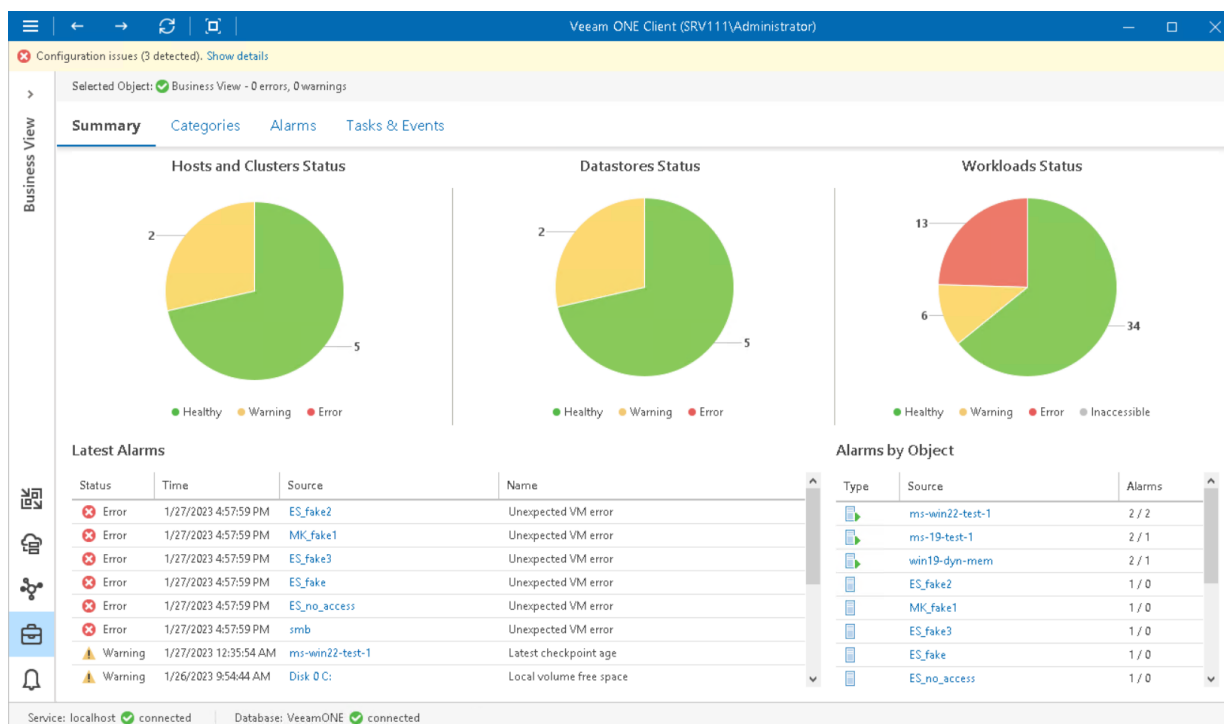
Host and Clusters Status, Datastores Status, Workloads Status

The charts reflect the health status of virtual infrastructure objects in Business View groups.

Every chart segment represents the number of objects in a certain state — objects with errors (red), objects with warnings (yellow) and healthy objects (green). Click a chart segment or a legend label to drill down to the list of alarms with the corresponding status for the selected type of virtual infrastructure objects.

Latest Alarms

The list displays the latest 15 alarms for objects in available Business View groups. Click a link in the **Source** column to drill down to the list of alarms triggered for a specific virtual infrastructure object.

Alarms by Object

The list displays 15 objects with the greatest number of alarms.

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 errors and 1 warning triggered for the object. Click a link in the **Source** column to drill down to the list of alarms triggered for a specific virtual infrastructure object.

For more information, see Working with Triggered Alarms.

Category Summary

The category summary dashboard provides an overview of the health status and performance for categorized infrastructure objects.
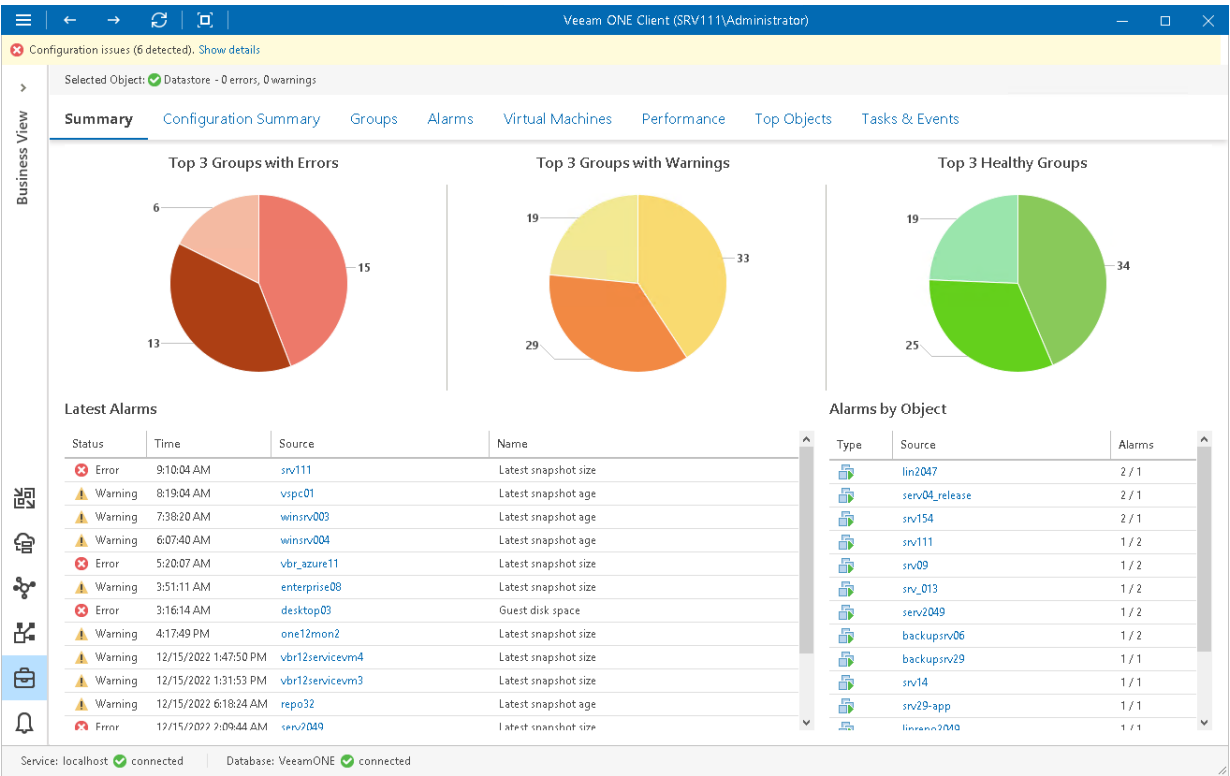
Top 3 Groups with Errors, Top 3 Groups with Warnings, Top 3 Healthy Groups

The charts reflect the health status of all groups within the chosen category.

Every chart segment represents groups in a certain state — groups with the greatest number of infrastructure objects with errors (red), groups with the greatest number of infrastructure objects with warnings (yellow) and groups with healthy infrastructure objects (green).

Click a chart segment to drill down to the list of alarms with the corresponding status for the selected Business View group.

Latest Alarms

The list displays the latest 15 alarms for the selected category. Click a link in the **Source** column to drill down to the list of alarms triggered for a specific infrastructure object.

Alarms by Object

The list displays 15 objects with the greatest number of alarms.

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 errors and 1 warning triggered for the object. Click a link in the **Source** column to drill down to the list of alarms triggered for a specific infrastructure object.

For more information, see Working with Triggered Alarms.

Category Configuration Summary

The **Configuration Summary** dashboard displays categorization details for different types of virtual infrastructure objects.

The dashboard acts as detailed monitoring panel: it presents virtual infrastructure objects from the perspective of business view categories. For each category, **Configuration Summary** provides information on the groups included in the category, shows how many objects belong to these groups, and provides information on the total number of objects in a group of their vCPU, memory and storage resources.

At the top of the dashboard, Veeam ONE Client displays information on the total number of objects included in a category.

> **NOTE:**
>
> This dashboard is not available for the *Computers* and *Enterprise Applications* categories.
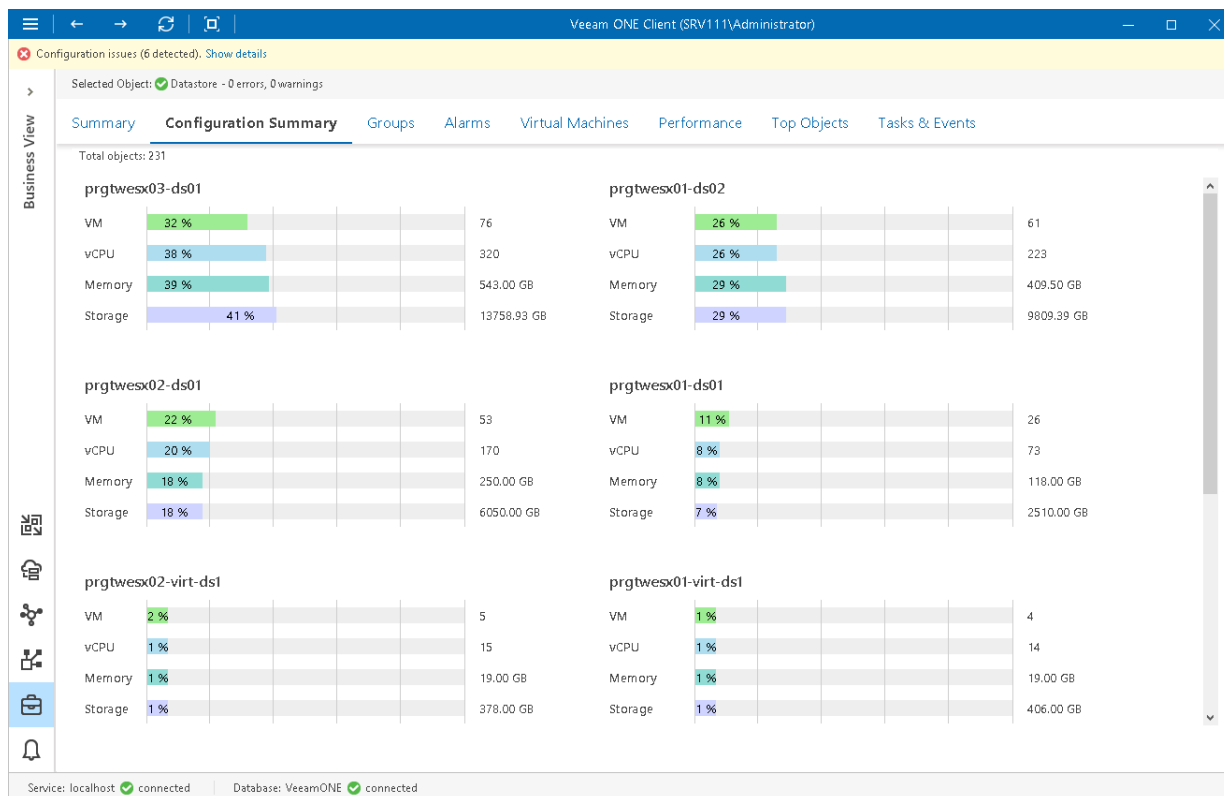
Group Summary

The group summary dashboard provides an overview of the health status and performance for the virtual infrastructure objects that belong to the chosen group.
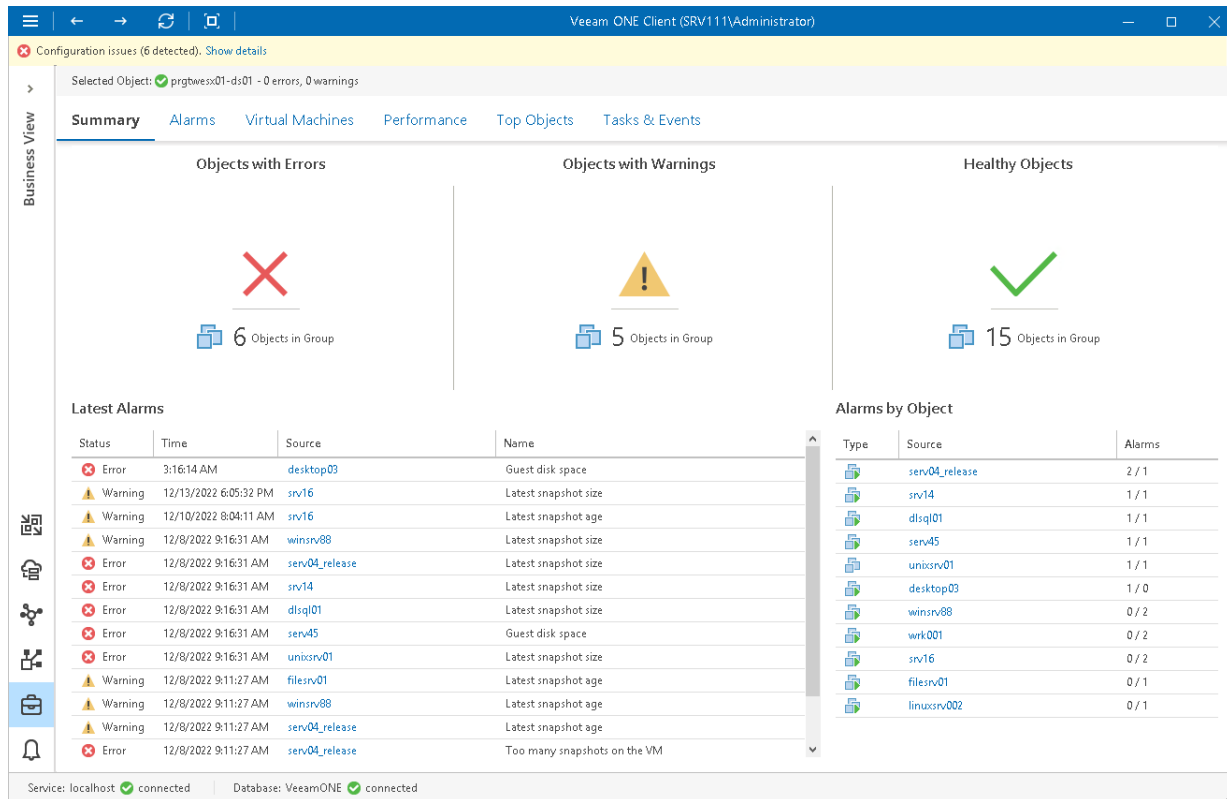
Error Objects, Warning Objects, Healthy Objects

The charts reflect the health status of virtual infrastructure objects in the group — objects with errors (red), objects with warnings (yellow) and healthy objects (green). Click the problematic chart to drill down to the list of alarms for objects with the chosen health status.

Latest Alarms

The list displays the latest 15 alarms for virtual infrastructure objects in the selected group. Click a link in the **Source** column to drill down to the list of alarms triggered for a specific virtual infrastructure object.

Alarms by Object

The list displays 15 objects with the greatest number of alarms.

The value in the **Alarms** column shows the number of errors and warnings for an object. For example, 3/1 means that there are 3 errors and 1 warning triggered for the object. Click a link in the **Source** column to drill down to the list of alarms triggered for a specific virtual infrastructure object.

For more information, see Working with Triggered Alarms.

Virtual Infrastructure Objects Summary

Veeam ONE allows you not only to view category and group summary, but also to monitor the summary state of categorized virtual infrastructure objects — VMs, hosts, clusters and datastores. To view a summary dashboard for a specific virtual infrastructure object:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Business View**.

3. In the inventory pane, select the necessary categorized object.

4. Open the **Summary** tab.

For more information on virtual infrastructure summary dashboards, see VMware vSphere Summary Dashboards and Microsoft Hyper-V Summary Dashboards.

Computers Summary

The **Computers** summary dashboard presents the health status overview for computers protected with Veeam Agent for Windows, Veeam Agent for Linux, Veeam Agent for Mac and Veeam Agent for Unix. The dashboard scope includes computers whose backups are managed by Veeam Backup & Replication servers that you monitor in Veeam ONE.

The dashboard is available for different levels of the categorization model:

- For the **Computers** node, the dashboard presents all computers from the monitored infrastructure

- For the category node, the dashboard to presents computers included in groups within the selected category
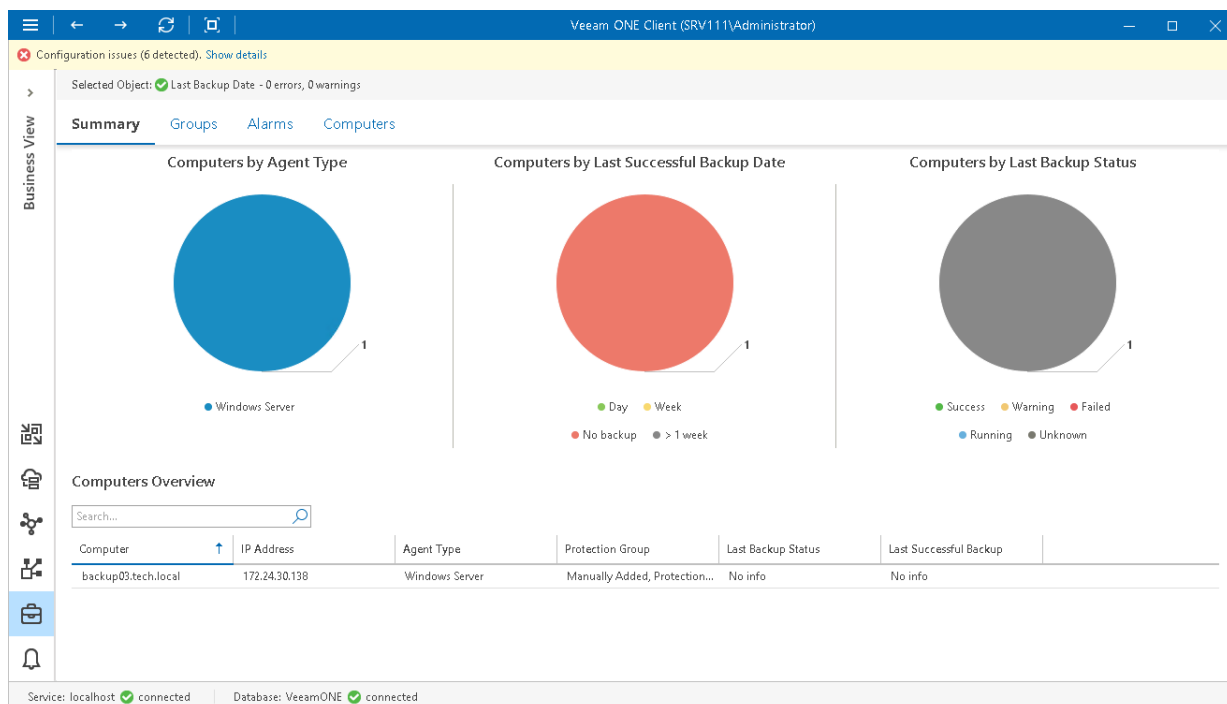
Computers by Agent Type

The chart displays types of computers protected with Veeam Agent for Windows, Veeam Agent for Linux, Veeam Agent for Mac and Veeam Agent for Unix.

Every chart segment shows the number of computers of a specific platform and type — the number of managed Windows servers, the number of managed Windows workstations, the number of managed Linux servers, the number of managed Linux workstations, the number of managed Mac servers, the number of managed Mac workstations, the number of managed AIX servers, the number of managed Solaris servers.

Computers by Last Successful Backup Date

The chart displays the time interval when the latest successful backup was created for computers running Veeam Agent for Windows, Veeam Agent for Linux, Veeam Agent for Mac and Veeam Agent for Unix.

Every chart segment shows the number of computers with last successful backups created within a specific interval — the number of computers with backups created not older than a day ago, computers with backups created not older than a week ago, computers with backups older than a week, and computers with no backups.

Computers by Last Backup Status

The chart displays the latest status of backup jobs for computers running Veeam Agent for Windows, Veeam Agent for Linux, Veeam Agent for Mac and Veeam Agent for Unix.

Every chart segment shows how many jobs ended with a specific status — failed jobs, jobs that ended with warnings, successfully performed jobs, jobs that are currently running, and jobs whose status is unknown.

Computers Overview

The table provides details on computers running Veeam Agent for Windows, Veeam Agent for Linux, Veeam Agent for Mac and Veeam Agent for Unix:

- **Computer** — computer name.

- **IP Address** — computer IP address.

- **Agent Type** — operation mode of a backup agent on the computer *(Windows server, Windows workstation, Linux Server, Linux Workstation, Mac Server, Mac Workstation, AIX Server, Solaris Server)*.

- **Protection Group** — name of a protection group in which the computer is included.

- **Last Backup State** — the latest status of a backup job (*Success, Warning, Failed, Running, No Info*).

- **Last Successful Backup** — date and time when the latest successful backup was created for the computer.

Computer Details

The **Summary** dashboard for a single computer node presents an overview and protection status details for computers running Veeam Agent for Windows, Veeam Agent for Linux, Veeam Agent for Mac and Veeam Agent for Unix.
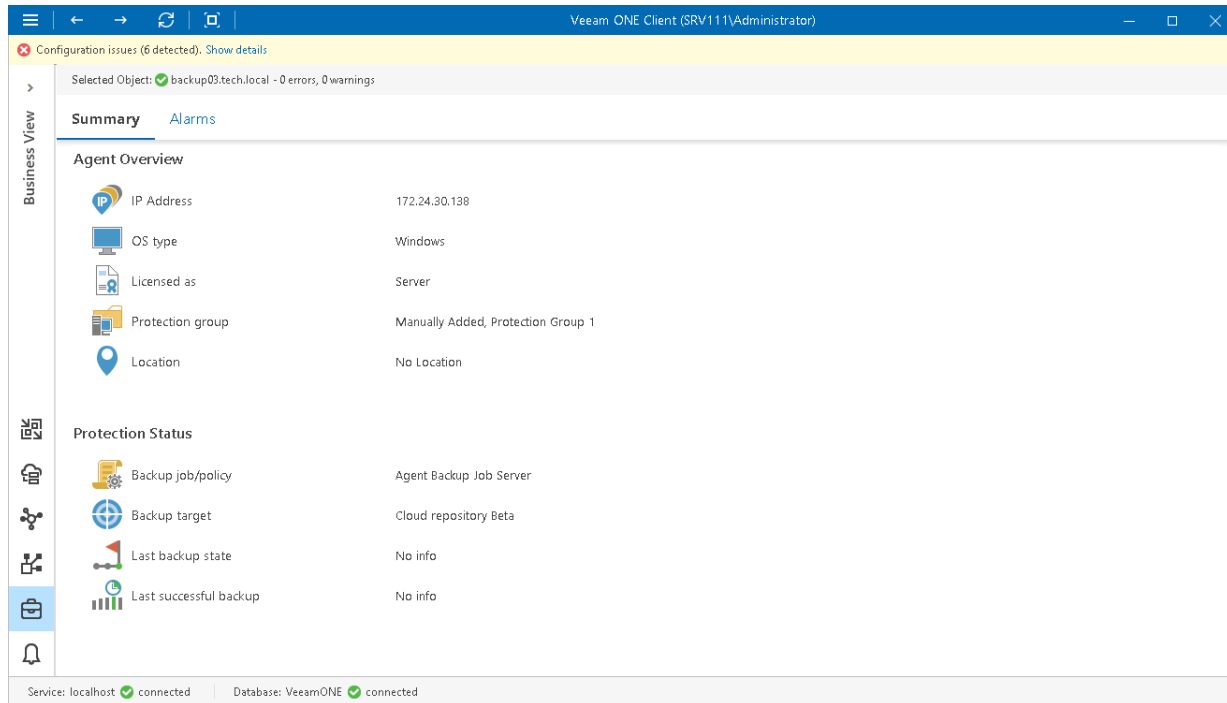
Agent Overview

The section provides the following details:

- IP address of the computer running Veeam Agent for Windows, Veeam Agent for Linux, Veeam Agent for Mac or Veeam Agent for Unix

- Type of an OS installed on the computer (*Windows*, *Linux*, *macOS*, *UNIX*)

- Operation mode in which the computer is licensed

- Name of the protection group in which the computer is included

- Location of the computer, as specified in Veeam Backup & Replication

Protection Status

The section provides the following details:

- Name of the backup policy applied to the computer, or the backup job in which a computer is included

- Target location in which computer backups are stored

- The latest status of the backup job session (*Success*, *Warning*, *Failed*, *Running*, *No Info*)

- Date and time when the latest successful backup was created for the computer

Enterprise Applications Summary

The **Enterprise Applications** summary dashboard presents the health status overview for applications protected with Veeam plug-ins for SAP HANA, SAP on Oracle and Oracle RMAN. The dashboard scope includes applications whose backups are managed by Veeam Backup & Replication servers that you monitor in Veeam ONE.
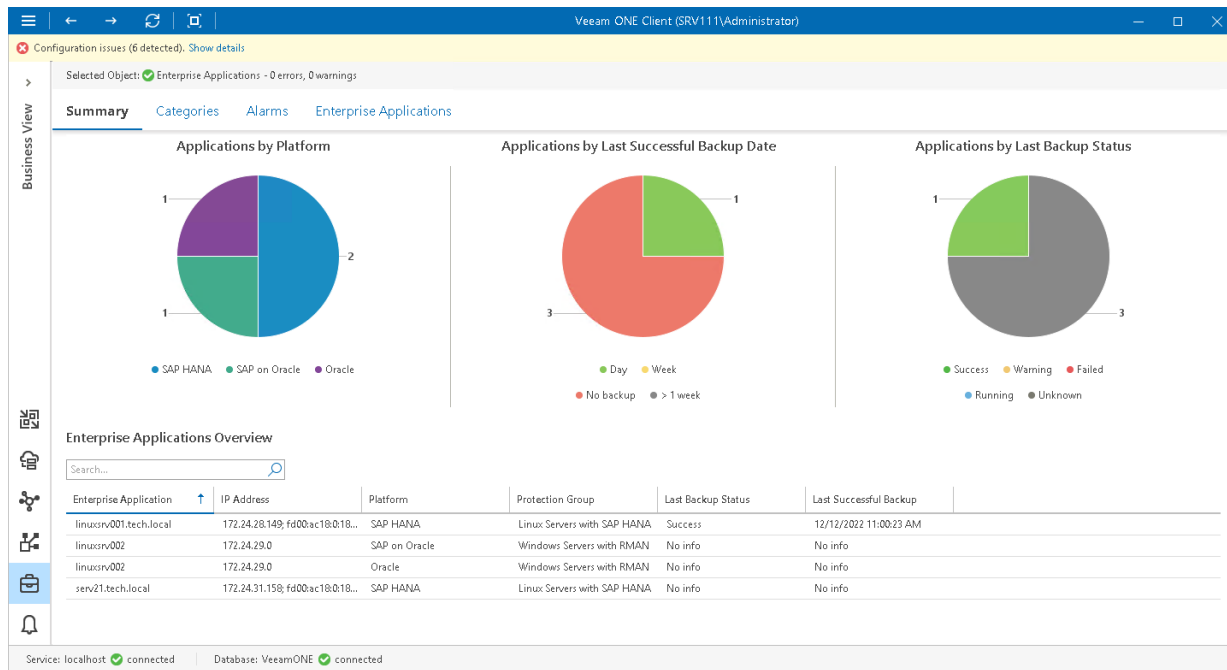
Applications by Platform

The chart displays types of application protected with enterprise application plug-ins.

Every chart segment shows the number of applications of a specific platform — the number of protected SAP HANA, SAP on Oracle and Oracle RMAN applications.

Applications by Last Successful Backup Date

The chart displays the time interval when the latest successful backup was created for enterprise applications.

Every chart segment shows the number of computers with last successful backups created within a specific interval — the number of applications with backups created not older than a day ago, applications with backups created not older than a week ago, applications with backups older than a week, and applications with no backups.

Applications by Last Backup Status

The chart displays the latest status of backup jobs for enterprise applications.

Every chart segment shows how many jobs ended with a specific status — failed jobs, jobs that ended with warnings, successfully performed jobs, jobs that are currently running, and jobs whose status is unknown.

Enterprise Applications Overview

The table provides details on protected enterprise applications:

- **Enterprise Application** — name of the machine on which the enterprise application is installed.

- **IP Address** — IP address of the machine on which the enterprise application is installed.

- **Platform** — enterprise application platform (*SAP HANA*, *SAP on Oracle*, *Oracle*).

- **Protection Group** — name of a protection group in which an application is included.

- **Last Backup Status** — the latest status of a backup job (*Success*, *Warning*, *Failed*, *Running*, *No Info*).

- **Last Successful Backup** — date and time when the latest successful backup was created for the enterprise application.

Enterprise Application Details

The **Summary** dashboard for a single application node presents an overview and protection status details for applications protected with Veeam plug-ins for SAP HANA, SAP on Oracle and Oracle RMAN.
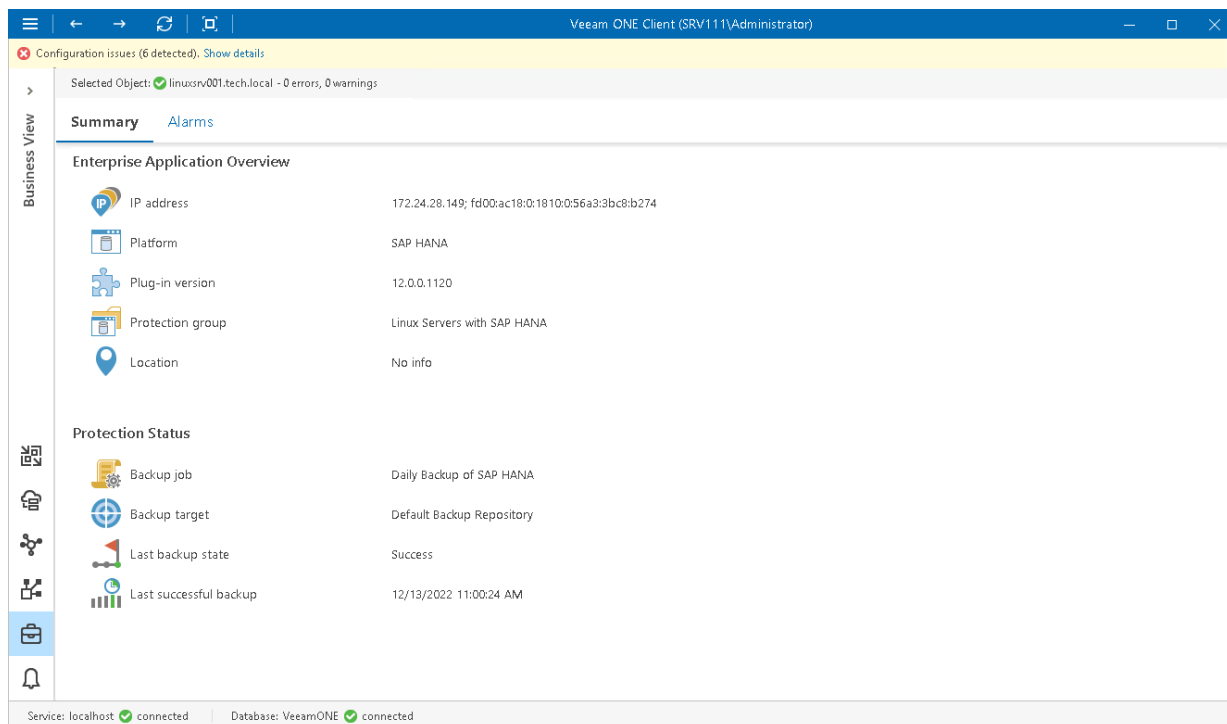
Enterprise Application Overview

The section provides the following details:

- IP address of a machine on which the enterprise application is installed

- Enterprise application platform (*SAP HANA*, *SAP on Oracle*, *Oracle*)

- Version of the enterprise application plug-in

- Name of the protection group in which the enterprise application is included

- Location of the enterprise application, as specified in Veeam Backup & Replication

Protection Status

The section provides the following details:

- Name of the backup job in which the enterprise application is included

- Target location in which enterprise application backups are stored

- The latest status of the backup job session (*Success*, *Warning*, *Failed*, *Running*, *No Info*)

- Date and time when the latest successful backup was created for the enterprise application

Business View Alarms

You can create and manage alarms for virtual infrastructure objects organized into Business View groups. For example, you can group your virtual infrastructure objects by a department to which these objects belong. For each group, you can configure alarms with severity levels and thresholds corresponding to requirements of a specific department.

For Business View, Veeam ONE supports all alarms that apply to categorized objects — VMs, hosts, clusters, datastores, computers and enterprise applications.

To view the list of alarms for categorized objects:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Business View**.

3. In the inventory pane, select the necessary category, group or object.

4. Open the **Alarms** tab.

For more information, see Working with Triggered Alarms.

Business View Objects

You can view the list of infrastructure objects within the Business View node — object type, platform, category and group.

To view the list of objects:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Business View**.

3. In the inventory pane, select the necessary node.

4. Open the tab with the name of the object: *Virtual Machines*, *Hosts*, *Datastores*, *Clusters*, *Computers*, *Enterprise Applications*.

5. To find the necessary object by name, use the **Search** field at the top of the list.

   To display objects of a specific virtual infrastructure node, select the necessary node in the **Scope** field at the top of the list.

6. Click column names to sort objects by a specific parameter.

For every object in the list, the following details are available.

Virtual Machines

- **State** — state of the VM (*powered on*, *powered off*, *suspended*)

- **Name** — name of the VM

- **Parent Object** — name of the parent object for the VM

  Click a link in this column to switch to the **Virtual Infrastructure** for the parent object.

- **vCPUs** — number of virtual CPUs configured for the virtual machine

- **Memory Size** — amount of memory resources allocated to the VM

- **Guest OS** — guest operating system installed on the VM

- **Virtual Disk Size** — size of the VM virtual disk

- **Categories** — number of categories to which the VM is included

  Click a link in this column to see all categories and groups in which the VM is included.

Hosts

- **Name** — name of the host

- **Parent Object** — name of the parent object for the host

  Click a link in this column to switch to the **Virtual Infrastructure** for the parent object.

- **CPU Count** — number of CPU cores on the host

- **CPU Speed** — frequency of CPU cores on the host

- **Memory Size** — total capacity of the host

- **VM Count** — number of VMs residing on the host

- **Categories** — number of categories to which the host is included

  Click a link in this column to see all categories and groups in which the host is included.

Datastores

- **Datastores** — name of the datastore

- **Parent Object** — name of the parent object for the datastore

  Click a link in this column to switch to the **Virtual Infrastructure** for the parent object.

- **File System** — type of the file system on the datastore

- **Capacity** — total capacity of the datastore

- **Free Space** — free space remaining on the datastore

- **VM Count** — number of VMs residing on the datastore

- **Categories** — number of categories to which the datastore is included

  Click a link in this column to see all categories and groups in which the datastore is included.

Clusters

- **Clusters** — name of the cluster

- **Parent Object** — name of the parent object for the cluster

  Click a link in this column to switch to the **Virtual Infrastructure** for the parent object.

- **CPU Count** — number of CPU cores in the cluster

- **CPU Speed** — total frequency of all CPU cores in the cluster

- **Memory Size** — total size of memory available for the cluster

- **Host Count** — number of hosts in the cluster

- **VM Count** — number of VMs residing on the cluster

- **Categories** — number of categories to which the cluster is included

  Click a link in this column to see all categories and groups in which the cluster is included.

Computers

- **Name** — name of the computer on which Veeam backup agent is installed

- **IP Address** — IP address of the computer on which Veeam backup agent is installed

- **Cluster** — name of a failover cluster added to a protection group

- **Agent Type** — type of the computer OS and mode in which Veeam backup agent job runs (*Windows Server*, *Windows Workstation*, *Linux Server*, *Linux Workstation*, *Mac Server*, *Mac Workstation*, *Solaris Server* or *AIX Server*)

- **Location** — location assigned to the computer in Veeam Backup & Replication

- **Agent Version** — version of the Veeam backup agent

- **Protection Group** — name of the protection group to which the computer is included

- **Backup Server** — name of the Veeam Backup & Replication server that manages the Veeam backup agent

- **Backup Job / Policy** — name of the backup job or policy assigned to the Veeam backup agent on the computer

- **Last Backup State** — state of the latest job session

- **Last Successful Backup** — date and time when the latest restore point was created

- **Categories** — number of categories to which the computer is included

  Click a link in this column to see all categories and groups in which a computer is included.

Enterprise Applications

- **Name** — name of the machine on which the enterprise application plug-in is installed

- **IP Address** — IP address of the machine on which the enterprise application plug-in is installed

- **Platform** — enterprise application platform

- **Location** — location assigned to the application in Veeam Backup & Replication

- **Plug-in Version** — version of the Veeam Plug-in

- **Protection Group** — name of the protection group to which the application is included

- **Backup Server** — name of the Veeam Backup & Replication server that manages the Veeam Plug-in

- **Backup Policy** — name of the backup job or policy assigned to the Veeam Plug-in

- **Last Backup State** — state of the latest job session

- **Last Successful Backup** — date and time when the latest restore point was created

- **Categories** — number of categories to which the application is included

  Click a link in this column to see all categories and groups in which a computer is included.

You can choose what columns to show or hide in the objects table:

- To hide one or more columns, right-click the table header, and clear check boxes next to the corresponding data fields.

- To make hidden columns visible, right-click the table header, and select check boxes next to the corresponding data fields.

Exporting Object Details to CSV

You can export categorization data to a CSV file and save it for documenting purposes:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Business View**.

3. In the inventory pane, select the necessary node.

4. Open the tab with the name of the object: *Virtual Machines*, *Hosts*, *Datastores*, *Clusters*, *Computers*, *Enterprise Applications*.

5. To find the necessary object by name, use the **Search** field at the top of the list.

6. At the top of the list, click **Export to CSV** and save the file.

Business View Performance Charts

You can launch performance charts for infrastructure objects organized into business groups. You can view the performance of objects in custom groups, and identify whether there are enough resources allocated to these objects.

For Business View, Veeam ONE supports all dashboards that apply to categorized virtual infrastructure objects — VMs, hosts, clusters and datastores.

To access a performance chart for a categorized virtual infrastructure object:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Business View**.

3. In the inventory pane, select the necessary object.

4. Open the necessary performance chart tab.

For more information on performance charts, see VMware vSphere Performance Charts and Microsoft Hyper-V Performance Charts.
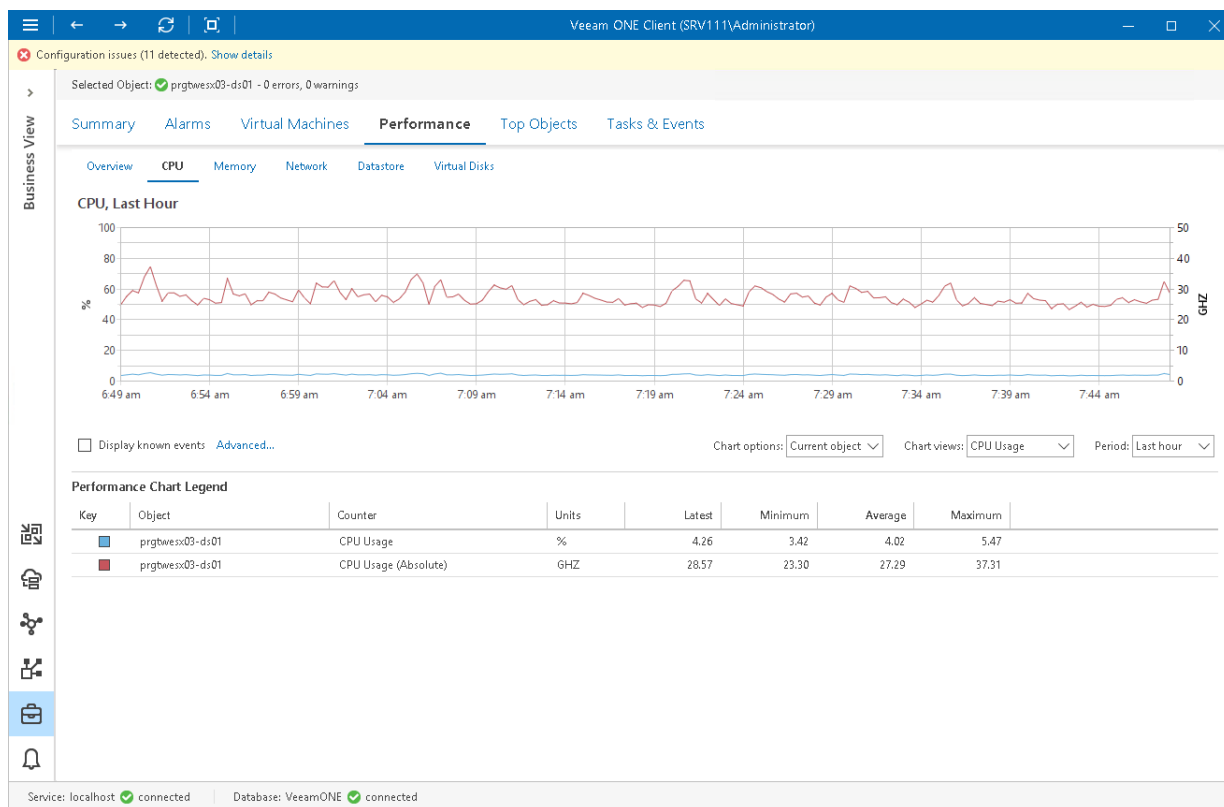
Troubleshooting Performance of Categorized Objects

Veeam ONE Client includes a set of dashboards that give you enhanced control over categorized virtual infrastructure objects and facilitate the troubleshooting process:

- Top N dashboards display top and bottom resource consumers in a group:

  - To view VMs that consume the greatest amount of compute, network and storage resources, choose the necessary VM group in the inventory pane and go to the **Top Objects** tab.

  - To view the most loaded hosts, choose the necessary host group in the inventory pane and navigate to **Top Objects** > **Top Hosts**.

  - To view the least loaded hosts, choose the necessary host group in the inventory pane and navigate to **Top Objects** > **Bottom Hosts**.

  For more information on the **Top and Lowest Load** dashboards, see VMware vSphere Top Objects and Microsoft Hyper-V Top Objects.

- **Tasks & Events** dashboard shows tasks and events targeted for categorized objects.

  To view the list of tasks and events for a categorized virtual infrastructure object, select it in the inventory pane and go to the **Tasks & Events** tab.

- **Processes** dashboard provides control over processes and services running inside the guest OS of a VM.

  - For Windows- based machines, you can view, end or restart processes.

  - You can view or end daemons on Linux-based machines.

  To view the list of processes, select the necessary VM in the inventory pane and go to the **Processes** tab.

  For more information on VM processes, see VMware vSphere In-Guest Processes and Microsoft Hyper-V In-Guest Processes.

- **Console** view allows you to access the VM guest OS right from the Veeam ONE Client interface.

  To access a VM console, select the necessary VM in the inventory pane and go to the **Console** tab.

  For more information on working with VM console, see VMware vSphere VM Console and Microsoft Hyper-V VM Console.

Generating Reports

To obtain a point-in-time view of your virtual infrastructure and data protection operations, you can create reports from the Veeam ONE Client:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click the necessary view — Veeam Backup & Replication, Veeam Backup for Microsoft 365, Virtual Infrastructure, VMware Cloud Director, or Business View.

3. Do one of the following:

   o In the main menu, click **Reports** and choose the necessary report from the list.

   o Right-click the necessary infrastructure object or a node in the inventory tree, click **Reports** and choose the necessary report from the list.

4. On the Veeam ONE Web Client login page, specify user credentials.

5. On the report details page, specify the report parameters.

6. Click **Preview**.

You can quickly generate any other reports supplied by Veeam ONE Web Client. To do that, select the necessary report on the **Report Templates** tab pane on the left.

For more information on available reports, see Veeam ONE Reporting Guide.

veeam

Host Configuration Chargeback

Description

This report helps to make infrastructure costs audit and identify the most and least expensive VMs based on the hardware price and current VMs configuration.

Report Parameters

Hosts:	10 Hosts
Hosts cost:	110.50 USD
Host expenses distribution:	CPU: 22% / RAM: 78%
Datastores cost:	2605.50 USD
Include powered-off VMs in the calculation:	True
Show VM details:	True
Calculate VM storage costs based on:	Provisioned space

Summary

Hosts:	10	Processor core avg. cost:	0.42	Virtual CPU avg. cost:	0.08
Datastores:	22	Physical memory, GB avg. cost:	0.22	Virtual Memory, GB avg. cost:	0.33
Virtual Machines:	414	Datastore, TB avg. cost:	31.49	Virtual Storage, TB avg. cost:	46.31
Average VM cost:	33.35				
Total hardware cost, USD:	2,716.00				

Cost Distribution
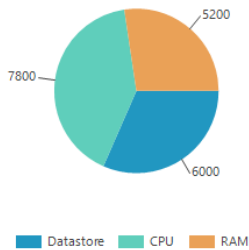
VM Power Status
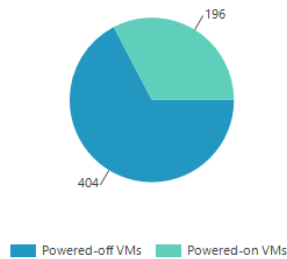
Top 10 Most Expensive VMs
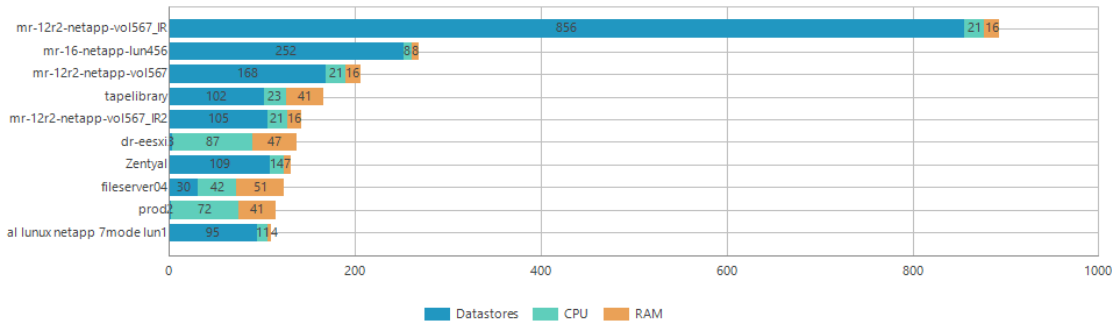
Working with Alarms

Veeam ONE alarms notify users about important events, changes and potential problems in the managed virtual and backup environment. Alarms speed up the process of identifying, troubleshooting and reacting to issues that may affect mission-critical services and business operations.

Out of the box, Veeam ONE comes with a set of predefined alarms so that you can start monitoring your environment immediately after deploying the solution. Predefined alarms include:

- Veeam Backup & Replication alarms

- Veeam Backup for Microsoft 365 alarms

- VMware vSphere and VMware Cloud Director alarms

- Microsoft Hyper-V alarms

- Internal alarms for monitoring issues with Veeam ONE

Predefined alarms are based on best practices and include an extensive knowledge base. When a problem occurs, you will not only receive an alert but will also have all the necessary information for troubleshooting and finding the root cause of the issue.

About Alarms

Veeam ONE offers an extensive set of tools that will help you develop your own alarm model. Depending on your requirements for the virtual and backup environment, you can customize predefined alarms, or create new alarms. This section describes various aspects of alarms in Veeam ONE, including alarm rules, severity levels, assignment options, response actions and other.

How Alarms Work

After you connect virtual or backup servers, Veeam ONE starts collecting data about objects in your environment and their health state, and checks this data against alarm configuration in real time. If Veeam ONE detects that behavior or state of an infrastructure object meets alarm criteria, or that a specific event occurs, it triggers an alarm with the defined severity level.

After an alarm is triggered, Veeam ONE Client will display alarm details and information about the affected object. You can view, acknowledge or resolve the alarm.

If an alarm is configured to perform an action, Veeam ONE performs a response action after the alarm is triggered — sends an email notification, SNMP trap, or runs a predefined or custom script.

If the event, state or condition that triggered the alarm is resolved, Veeam ONE updates the alarm status in the console.

Alarm Rules

Every alarm has one or more associated rules that define conditions to trigger the alarm, severity of the alarm and rule suppression settings.

There are the following types of alarm rules:

- **Event-based rules** are rules for alerting about specific events that occur in the backup or virtual infrastructure. These can be events issued by the hypervisor or Veeam Backup & Replication events.

- **Rules for a specific condition or state** are rules for alerting about important conditions or changed state of infrastructure objects.

- **Rules based on existing alarms** are rules for alerting about other alarms triggered in Veeam ONE.

- **Rules based on resource usage counters** are rules for alerting about abnormal resource usage of infrastructure objects.

For the full list of available rule types, see Appendix B. Alarm Rules.

Aggregation Type

An aggregation type defines how Veeam ONE analyzes performance data collected for a specified period of time, and compares it to the threshold.

The following table explains how Veeam ONE alarms trigger depending on the aggregation type and rule condition:

Aggregation Type	Condition	
	Above	**Below**
Min	Veeam ONE takes the **minimum** value across the collected performance parameters and compares it to the specified threshold. If the value is above the threshold, Veeam ONE triggers an alarm. That means that the alarm triggers only if all the values are above the threshold.	Veeam ONE takes the **minimum** value across the collected performance parameters and compares it to the specified threshold. If the value is below the threshold, Veeam ONE triggers an alarm. That means that the alarm triggers if at least one of the collected values is below the threshold.
Avg	Veeam ONE takes the **average** value across the collected performance parameters. The alarm triggers if this value is above the threshold.	Veeam ONE takes the **average** value across the collected performance parameters. The alarm triggers if this value is below the threshold.
Max	Veeam ONE takes the **maximum** value across the collected performance parameters and compares it to the specified threshold. If the value is above the threshold, Veeam ONE triggers an alarm. That means that the alarm triggers if at least one of the collected values is above the threshold.	Veeam ONE takes the **maximum** value across the collected performance parameters and compares it to the specified threshold. If the value is below the threshold, Veeam ONE triggers an alarm. That means that the alarm triggers only if all the values are below the threshold.

To learn how to configure rules based on performance counters, see Adding Rules Based on Resource Usage Counters.

Analysis Depth

Alarm rules may include the **Analysis depth** parameter. This parameter defines the number of latest performance data values among which an average value is calculated. Each newly collected value is compared to the average value. If the new value is above or below the average value according to severity levels, Veeam ONE triggers the alarm.

Linking Rules

You can link two or more rules using Boolean operators:

- **AND** — if rules are joined with this operator, an alarm is triggered when conditions for all linked rules are met.

- **OR** — if rules are joined with this operator, an alarm is triggered when a condition for any of the linked rules is met.

You can form several groups of linked rules and join them with different operators. To learn how to link rules, see Linking Rules.

Alarm Severity

Every alarm rule is associated with a specific severity level. The severity level defines how serious the state or event is and how badly it can affect an object health state.

There are four severity levels that are color-coded as follows:

- **Error (red)** indicates a critical situation or a major problem that requires immediate action.

- **Warning (yellow)** indicates a potential problem or non-critical issue that needs your attention. If the issue is left without attention, it can potentially cause a major problem.

- **Resolved (green)** indicates that the issue was eliminated because of the changed conditions, or shows that the alarm was resolved manually.

- **Information (blue)** indicates general information about a specific condition or health state of an object.

You can define different severity levels for conditions of different intensity. For example, if the level of memory usage must not exceed 75%, you can create the following alarm rules:

- If the memory usage is over 70%, an alarm with the *Warning* severity level must be triggered.

- If the memory usage is over 75%, an alarm with the *Error* severity level must be triggered.

In such situation, if the memory usage level is constantly growing and exceeds 70%, Veeam ONE will trigger a warning alarm, notifying about a potentially dangerous situation. If the memory usage level keeps on growing and exceeds the level of 75%, Veeam ONE will trigger an error alarm notifying about the severe danger.

Alarm Assignment Options

You can assign Veeam ONE alarms to objects of the backup or virtual infrastructure. There are several options to assign alarms:

- **Object-level assignment** — you can assign an alarm to a single object.

  This type of assignment can be useful if you need to customize alarms for specific objects, like separate hosts, VMs or backup infrastructure components.

- **Group-level assignment** — you can assign an alarm to a group of objects (for example, to an infrastructure container or Business View group).

  This type of assignment can be useful if you need to assign an alarm to all objects under a specific parent entity. For example, to all VMs residing on a host or to all backup proxies connected to a backup server.

- **Infrastructure-level assignment** — you can assign an alarm to all objects of a particular type in the entire managed environment.

  This is the default type of assignment used for all predefined alarms.

You can combine various assignment options. For example, you can assign an alarm to all VMs running on a chosen host, to all VMs in a Business View group and to a few single VMs at the same time.

In addition to flexible alarm assignment options, Veeam ONE offers a possibility to exclude specific objects or object groups from the assignment scope. Thus, you can easily point out what part of your environment the alarm must ignore.

Alarm Notification Options

You can configure Veeam ONE to send notifications when alarms are triggered or change their status. Depending on alarm configuration, Veeam ONE can:

- Send email notifications to the default notification group or to specific recipients

- Send SNMP traps to third-party consoles

Alarm notification options are defined in alarm settings. You can specify when Veeam ONE must notify you about alarm status change:

- Alarm severity changes to *Error*

- Alarm severity changes to *Error* or *Warning*

- Alarm is resolved

- Alarm severity changes to any level (*Error*, *Warning* or *Resolved*)

By default, all predefined alarms are configured to send email notifications to the default notification group when the alarm severity changes to any level. You can change alarm notification settings and define conditions when notifications must be sent.

Alarm Remediation Actions

To automate virtual and backup infrastructure troubleshooting, you can configure Veeam ONE to run remediation actions as soon as alarms are triggered.

> **NOTE:**
>
> To run remediation actions for the backup infrastructure, you must have Veeam ONE agents installed on connected Veeam Backup & Replication servers. For more information on installing and configuring Veeam ONE agents, see Managing Veeam ONE Agents.

Veeam ONE offers the following types of remediation for alarms:

- Predefined actions that are configured for the most commonly used out-of-the-box alarms. For each alarm severity level, Veeam ONE can run only one predefined action.

  For the list of alarms with predefined remediation actions, see Appendix C. Remediation Actions.

- Custom scripts that you can specify in the settings of any alarm. For each severity level, Veeam ONE can run one or more custom scripts.

You can select the resolution type for alarm remediation actions:

- **Manual** — when an alarm is triggered, you must approve the remediation action manually. This type of resolution is default for alarms with predefined remediation actions.

- **Automatic** — when an alarm is triggered, Veeam ONE will automatically run a predefined remediation action or custom script.

Veeam ONE makes 3 attempts to run a remediation action or script. If the remediation is successful, the alarm status will change to Acknowledged. If for some reason Veeam ONE fails to run an action or script, the alarm will remain active.

Advanced Alarm Options

To avoid alarm storms and ensure that critical issues are not overlooked, you can use advanced alarm configuration options — alarm suppression and alarm modeling.

- **Alarm suppression** is used to disregard events and prevent sending alarms when specific activities are performed. For example, during backup Veeam ONE may send a great number of alarms informing about potential problems or increased resource pressure. Alarm suppressing allows you to pause specific alarms during such activities, or at a specific period of time when you plan to perform resource-consuming operations.

- **Alarm modeling** is used to verify the created alarm scheme and estimate the need for adjusting alarm settings. During alarm modeling, Veeam ONE applies alarm settings to collected historical data and produces a forecast on the number of alarms that will be sent over a specific period of time. If the number of alarms is too high, alarm thresholds may need to be changed to avoid numerous useless alarms. If the number is too low, the sensitivity of alarms may need to be increased so that you do not miss important issues.

Alarm Reports

In addition to receiving alarms in real-time, Veeam ONE allows you to analyze alarm statistics. You can use Veeam ONE Web Client dashboards and reports to track how the number of alarms is changing over time, identify short- and long-term alarm trends, detect the most affected infrastructure objects, troubleshoot commonly encountered issues and ensure that your infrastructure stays fully reliable and productive.

You can use the following dashboards and reports for analyzing alarms:

- **Alarms Dashboard** analyzes alarms triggered over the previous week. The dashboard provides information on the general health state of virtual infrastructure objects, shows daily roll-ups for errors and warnings, enumerates typical problems and helps to detect the most affected VMs, clusters, hosts and datastores.

- **Alarms Overview Report** provides an overview of the current health state of the virtual infrastructure, details the most common alarms and identifies the most affected infrastructure objects. The report consolidates information about raised alarms and provides a summary for the selected time interval.

- **Alarms Current State Overview Report** provides information about all currently unresolved alarms (alarms with the *Error* or *Warning* severity level) and displays reasons why these alarms were triggered.

For details on Veeam ONE reports and dashboards, see Veeam ONE Reporting Guide.

Configuring Alarms

Veeam ONE comes with a set of predefined alarms that cover most common monitoring scenarios. You can customize predefined alarms or create new alarms to meet specific monitoring conditions.

To access the list of alarms:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Alarm Management**.

3. To limit the list of displayed alarms, you can use filter buttons — *Show predefined alarms only*, *Show custom alarms only*, *All*.

The Alarm Management view comprises the following panes — the inventory pane, information pane, and actions pane.

- The **inventory pane** on the left shows the alarm management tree with alarm object types: virtual infrastructure components to which alarms can be applied, VMware Cloud Director components, Veeam Backup & Replication and Veeam Backup for Microsoft 365 infrastructure components, and internal alarms.

- The **information pane** contains the list of predefined and custom alarms for the type of object that is selected in the alarm management tree. Every alarm is described with the following details: type, name, source (*Predefined* or *Custom*), state (*Enabled* or *Disabled*), assignment scope and resolve action (*Automatic* or *Manual*). The bottom section of the information pane displays information on the selected alarm, such as summary, cause, resolution and external resources.

- The **Actions** pane on the right displays a list of links that you can use to perform actions with alarms.

Creating Alarms

If predefined alarms do not cover all important events, conditions or state changes about which you need to be notified, you can create custom alarms.

To create a new alarm, perform the following steps.

Step 1. Select Alarm Object Type

All alarms are applied to a certain level of the monitored infrastructure. The **Type** attribute of an alarm defines to what kind of infrastructure objects this alarm applies. The list of available alarm types is displayed in the inventory pane of the **Alarm Management** view.

To create a new alarm, select its type first:

1. Open Veeam ONE Client.

    For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Alarm Management**.

3. In the alarm management tree, select the necessary object type.

4. In the **Actions** pane on the right, click the **New** link.

    You can also right-click anywhere in the information pane and choose **New** from the shortcut menu.

> **NOTE:**
>
> Mind that you will not be able to change the alarm type later.

Creating Alarms from Tasks or Events

You can create an alarm that is based on a task or event that occurred in the monitored infrastructure. Veeam ONE will add the **Event-based** rule type to the alarm configuration, and will trigger this alarm for all events with the same name. For details on the Event-based rules, see Adding Event-Based Rules.

To create an alarm from a task or event:

1. Open Veeam ONE Client.

    For details, see Accessing Veeam ONE Client.

2. Select the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the information pane, navigate to the **Tasks & Events** tab.

4. Right-click a task or event for which you want to create an alarm, select **Create new alarm** from the shortcut menu and then choose an object type.

Creating Alarms from Performance Chart Counters

You can create an alarm from a performance counter. Veeam ONE will add to the alarm configuration a rule based on resource usage counter, and will trigger this alarm every time the counter reaches the specified values. For details on the rules based on resource usage counters, see Adding Rules Based on Resource Usage Counters.

1. Open Veeam ONE Client.

    For details, see Accessing Veeam ONE Client.

2. Select the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the object tree, select an object for which you want to create an alarm.

4. Open a tab with performance parameters for which you want to create an alarm (for example, *Network*, *Memory*, *CPU*, and so on).

5. At the bottom of the performance chart, right-click the necessary counter and select **Create new alarm** from the shortcut menu.

Creating Alarms from In-Guest Processes and Services

You can create an alarm from a process or service. For details on the rules based on specific condition or state, see Adding State-Based Rules.

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. Select the necessary view (*Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the object tree, select an object for which you want to create an alarm.

4. Open the **Processes** or **Services** tab.

5. Select one or more processes or services in the list.

6. Click the **Create Alarm** button.

   Alternatively, you can right-click the necessary process or service.

7. Select the type of rule on which the alarm must be based.

Step 2. Specify General Alarm Settings

On the **General** tab of the **Alarm Settings** window, specify general alarm settings:

1. In the **Alarm name** field, specify the name of the new alarm.

2. If you want to enable the alarm immediately after you save its settings, make sure that the **Enable this alarm** check box is selected.

    If you unselect this check box, the alarm settings will be saved, but the alarm will be disabled and will not raise any notifications.

Step 3. Specify Alarm Rules

On the **Rules** tab of the **Alarm Settings** window, specify rules for triggering the alarm. You can add up to 8 rules of different type and link them to each other.

Adding State-Based Rules

Alarms with state or condition-based rules alert about the important condition or state changes.

To add a rule for a specific condition or state change:

1. On the **Rules** tab, click **Add**.

2. At the **Choose Rule Type** step of the wizard, select the necessary trigger type.

3. Click **Next** and select the necessary rule condition.

   Available options depend on the alarm type. For the full list of alarm rules, see Appendix B. Alarm Rules.

4. At the **Define Rule** step of the wizard, specify conditions (or other settings, as applicable) for the alarm rule.

5. Specify alarm severity.

   For details, see Alarm Severity.

6. If you want to put the rule in action for the alarm, make sure that the **Enable this rule** check box is selected.

   If you clear this check box, the rule settings will be saved, but the rule will be disregarded.

7. Click **Finish**.

8. Repeat steps **1–7** for every state-based rule you want to add to an alarm.

Adding Event-Based Rules

Alarms with event-based rules alert about specific events that occur in your backup or virtual infrastructure. These can be events issued by the hypervisor or Veeam Backup & Replication events.

To add an event-based rule:

1. On the **Rules** tab, click **Add**.

2. At the **Choose Rule Type** step of the wizard, select **Event-based rule**.

3. At the **Define Rule** step of the wizard, specify rule settings:

    a. In the **Event name** field, specify the name of the event that must trigger the alarm.

    For the list of Veeam Backup & Replication events, see the Appendix A. Alarms section. For the list of virtual infrastructure events, see VMware vSphere Documentation or Microsoft TechNet library.

    Note that for VMware vSphere events, you must provide their names without prefixes. For example, for the *vim.event.VmReconfiguredEvent* event, you must specify only the *VmReconfiguredEvent* part.

    b. In the **Event text** field, specify one or more keywords that an event description must contain. This can be a name of a user who initiated an action, a name of a changed object, or a specific action.

    You can use the '*' (asterisk) and '?' (question) wildcards in the **Event name** and **Event text** fields. The '*' (asterisk) character stands for zero or more characters. The '?' (question mark) stands for a single character.

For example, if you want to receive notifications when users reconfigure VMs on the *host.domain.local* host, in the **Event name** field, specify *VmReconfiguredEvent*, and in the **Event text** field, specify '*reconfigured * on host.domain.local*'. Here the '*' (asterisk) replaces a name of a reconfigured VM. As a result, the alarm will be triggered each time any user reconfigures any VM on the host.

c. Specify the alarm severity level for the rule.

For details, see Alarm Severity.

d. In the **Ignore after** field, enter the number of times the alarm for the same event or condition must be triggered. All further repetitive alarms are suppressed.

For example, an alarm is configured to fire when a host loses its network connection, and the **Ignore after** value is set to 1. If a host loses its network connection, an event informing about connection loss will be raised by the hypervisor, and Veeam ONE will trigger an alarm. All further events informing about problems with host network connectivity will be ignored until you resolve the alarm that has already been triggered.

If you want the alarm to trigger every time an event or condition occurs, set the **Ignore after** value to 0.

e. In the **Trigger after** field, enter the number of times an event must repeat before Veeam ONE must trigger an alarm.

By default, this value is set to 0, which means that Veeam ONE must trigger an alarm after the first event occurrence.

f. If you want to put the rule in action for the alarm, make sure that the **Enable this rule** check box is selected.

If you clear this check box, the rule settings will be saved, but the rule will be disregarded.

4. Click **Finish**.

5. Repeat steps **1–4** for every event-based rule you want to add.

Adding Rules Based on Existing Alarms

You can add to an alarm rules that are based on existing alarms. These rules alert if the specified alarms trigger or change their status.

To add a rule based on existing alarm:

1. On the **Rules** tab, click **Add**.

2. At the **Choose Rule Type** step of the wizard, select **Existing alarm**.

3. At the **Define Rule** step of the wizard, specify rule settings:

   a. In the **Alarm name** field, specify the name of the existing alarm that must trigger an alarm.

   This can be a predefined or custom alarm. For a list of predefined alarms, see the Appendix A. Alarms section.

   b. In the **Delay time** field, specify the period that must pass between triggering the source and the target alarm.

   You can specify the delay time in minutes, hours, or days.

   c. If you want to put the rule in action for the alarm, make sure that the **Enable this rule** check box is selected.

   If you unselect this check box, the rule settings will be saved, but the rule will be disregarded.

4. Click **Finish**.

5. Repeat steps **1–4** for every alarm-based rule you want to add.

Adding Rules Based on Resource Usage Counters

Alarms with rules resource usage counters alert about the important changes in the performance of objects from the monitored infrastructure.

To add a rule based on resource usage counters:

1. On the **Rules** tab, click **Add**.

2. At the **Choose Rule Type** step of the wizard, select **Resource usage**.

3. At the **Define Rule** step of the wizard, specify conditions (or other settings, as applicable) for the alarm rule.

   If you want to put the rule in action for the alarm, make sure that the **Enable this rule** check box is selected. If you unselect this check box, the rule settings will be saved, but the rule will be disregarded.

4. [Optional] Exclude specific objects from the alarm scope.

   By default, counter-based rules apply to all storage objects in the alarm scope. For example, if you create an alarm rule for a host and select a datastore usage counter, this rule will apply to all datastores connected to the host.

   For some counter-based rules, you can exclude specific storage objects from the alarm scope. Excluded objects will not be monitored by the alarm. To exclude one or more storage objects, specify their names in the **Exclude instances** field. Separate object names with a semicolon (;).

> **NOTE:**
> - When you specify objects to exclude, use object display names. To learn the exact display name of an object, navigate to a performance chart for the necessary object in Veeam ONE Client, and choose a chart view with the necessary counter. You can check the object display name either in the chart legend or in the **Select Devices and Counters** window > **Devices** list. For details, see section Selecting Chart Views and Performance Counters of the Veeam ONE Monitoring Guide.
> - Names of drives must be specified with the backward slash, for example, `C:\; Z:\`.

5. Click **Finish**.

6. Repeat steps **1–5** for every alarm-based rule you want to add.

Linking Rules

If you add multiple rules to one alarm, Veeam ONE will trigger the alarm when conditions for at least one rule are met. You can change the default way of evaluating alarm rules and link rules using Boolean AND or OR operators. For example, if an alarm must be triggered when conditions for two rules are met simultaneously, you can link these rules with Boolean AND.

To link alarm rules:

1. Choose the rules you want to link and place them one after another. You cannot link rules that do not follow one another in the list. For example, you cannot link the first and the fifth rule.

   To move a rule one position up, select the check box next to the rule and click **Move up**. To move a rule one position down, select the check box next to the rule and click **Move down**.

2. Select check boxes next to rules you want to link, and click **Link** on the right.

3. In the **Rule condition** window, select a condition:

   o **AND** — if rules are linked with this operator, the alarm is triggered when conditions for all linked rules are met.

   o **OR** — if rules are linked with this operator, the alarm is triggered when a condition for any of the linked rules is met.

4. Click **Apply**.

   After you link two or more rules, Veeam ONE will display a dotted line and a linking condition between the rules. Linking supports 3 levels of nesting.

To unlink rules:

1. Select the check box next to the linked rules.

2. On the right, click **Unlink**.

If you unlink rules, the alarm will be triggered each time when conditions for any alarm rule are met.

Removing Rules

To remove a rule from an alarm:

1. Select the check box next to a rule you want to remove.

2. On the right, click **Remove**.

Duplicating Rules

To duplicate a rule:

1. Select the check box next to a rule you want to duplicate.

2. On the right, click **Duplicate**.

Step 4. Specify Alarm Assignment Scope

On the **Assignment tab** of the **Alarm settings** window, specify one or more infrastructure objects to which the alarm must be assigned.

Adding Objects to Alarm Assignment Scope

To add one or more objects to alarm assignment scope:

1. On the **Assignment** tab, in the **Assignment for alarm** section, click **Add** and select the necessary node (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

2. In the **Assign Alarm** window, select check boxes next to objects to which you want to assign the alarm.

3. Click **Assign**.
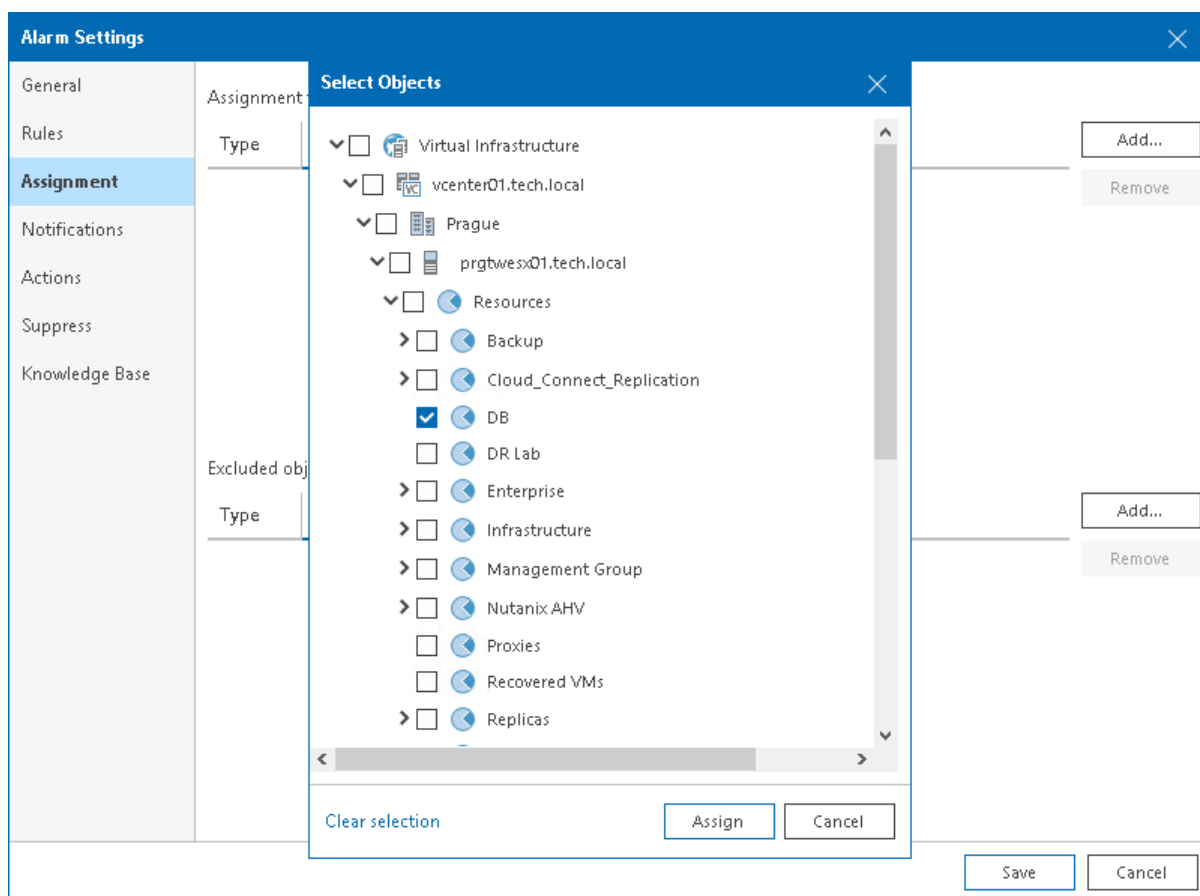
To remove an object from the alarm assignment:

1. On the **Assignment** tab, in the **Assignment for alarm** section, select an object you want to remove from the assignment.

2. On the right, click **Remove**.

Excluding Objects from Alarm Assignment Scope

You can exclude objects from alarm assignment scope:

1. On the **Assignment** tab, in the **Excluded objects** section, click **Add** and select the necessary node (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

2. In the **Exclude Alarm** window, select check boxes next to objects you want to exclude from alarm assignment.

3. Click **Exclude**.
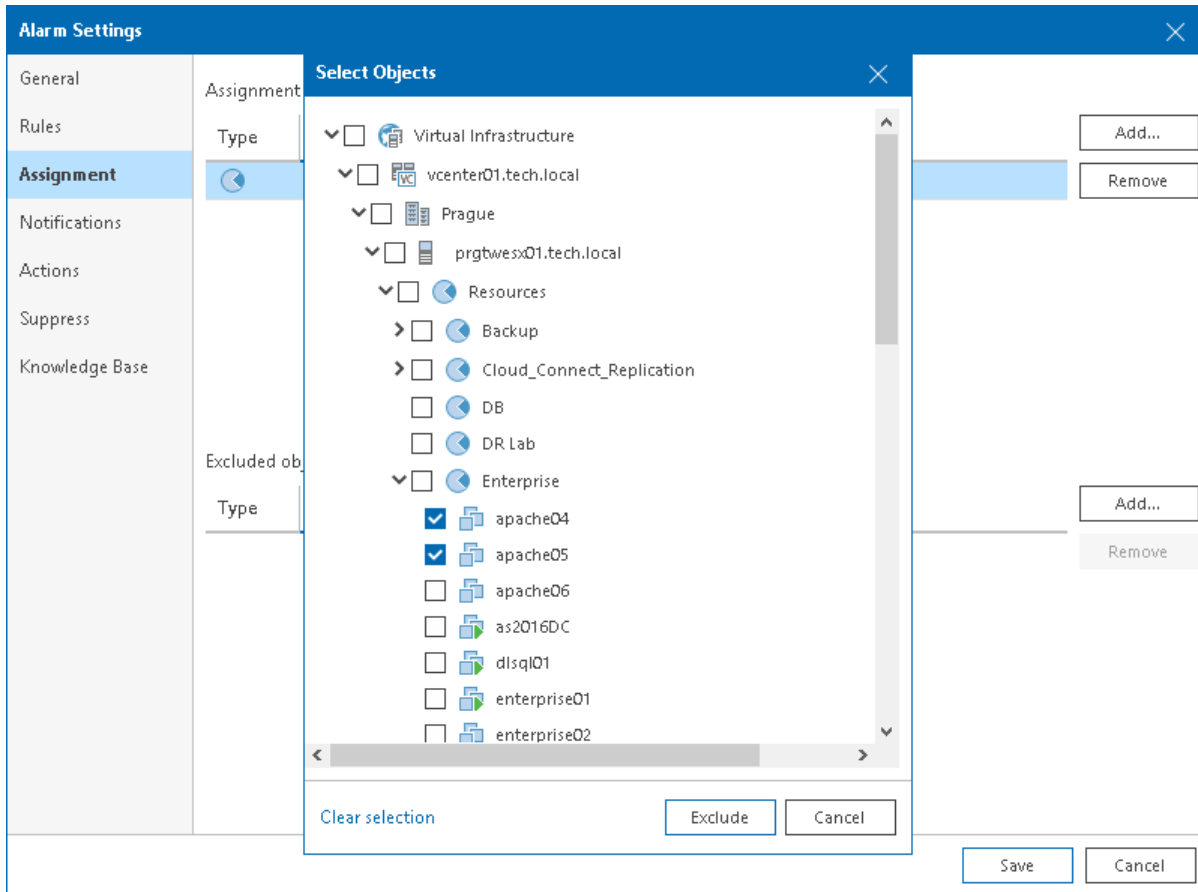
Step 5. Specify Alarm Notification Options

On the **Notifications** tab of the **Alarm settings** window, you can specify what actions must be performed after the alarm is triggered, or after the alarm status changes. You can choose to notify virtual infrastructure administrators by email, send SNMP traps or run a custom script.

> **NOTE:**
>
> To receive email and trap notifications, you must first configure email and trap notification settings in the Veeam ONE Client Configuration Wizard or in Veeam ONE Client server settings. To learn how to configure notification settings for alarms, see Configuring Alarm Notification Settings.

To define alarm response actions:

1. From the **Action** list, select the action you want to perform:

   o **Send email to a default group** — select this option if you want to send an email notification to all recipients included in the *default email notification group* when the alarm is triggered or when the alarm status changes. This is the default action that applies to all new and predefined alarms.

   For details, see Email Notifications.

   o **Send email to Business View group owner** — select this option if you want to send an email notification an owner of a Business View group to which the object is included.

   To receive notifications, you must specify an email address of a group owner in the Business View group settings. For details, see Configuring Multiple-Condition Categorization.

   o **Send email notification** — select this option if you want to send an email notification to specific recipients when the alarm is triggered or when the alarm status changes. In the **Value** field, enter recipients email addresses. If you want to specify several recipients, separate email addresses with a semicolon (;), comma (,) or space ( ).

   For more information, see Email Notifications.

   o **Send SNMP trap** — select this option if you want to send a Simple Network Management Protocol (SNMP) trap when the alarm is triggered or when the alarm status changes.

   For details, see SNMP Traps.

   o **Run script** — select this option if you want to run a custom script when the alarm is triggered or when the alarm status changes. By running a script, you can automate routine tasks that you normally perform when specific alarms fire. For example, if a critical system is affected, you may need to immediately open a ticket with the in-house support or perform corrective actions that will eliminate the problem.

   In the **Value** field, specify the path to the executable file. The executable file must be located on the machine running the Veeam ONE Server component. You can use the following parameters in the command line for running the script: *%1* — alarm name; *%2* — affected node name; *%3* — alarm summary; *%4* — date and time of alarm trigger; *%5* — alarm status; *%6* — previous alarm status; *%7* — ID assigned to a combination of an affected node and an alarm; *%8* — type of a child alarm object.

2. In the **Condition** field, specify when the action must be performed:

   o **Errors and warnings** — select this option if the action must be performed every time when the alarm status changes to *Error* or *Warning*.

   o **Errors only** — select this option if the action must be performed every time when the alarm status changes to *Error*.

o **Resolved** — select this option if the action must be performed every time when the alarm status changes to *Resolved*.

o **Any state** — select this option if the action must be performed every time when the alarm status changes to *Error*, *Warning* or *Resolved*.

You can specify multiple response actions for the same alarm. To add a new action, click the **Add** button and repeat steps **1-2** for every new action.

Step 6. Specify Alarm Remediation Actions

On the **Actions** tab of the **Alarm settings** window, you can specify what actions must be performed after the alarm is triggered, or after the alarm status changes:

1. Click **Add**.

2. From the **Action** list, select **Run Script**.

   In the **Path to script** field, specify the path to the script that must be executed after the alarm is triggered, or after the alarm status changes. The executable file must be placed at the location accessible for the Veeam ONE service account. The script is executed on the machine running Veeam ONE Server component. You can use the following parameters in the command line for running the script: *%1* — alarm name; *%2* — affected node name; *%3* — date and time of alarm trigger; *%4* — alarm status; *%5* — affected object name; *%6* — ID assigned to a combination of an affected node and an alarm.

> **NOTE:**
>
> Predefined remediation actions are available for a number of out-of-the-box alarms only. For the list of alarms with predefined remediation actions, see Appendix C. Remediation Actions.

3. From the **Severity** list, select alarm severity level at which an action must be taken.

4. From the **Resolution Type** list, select resolution type — manual or automatic.

   For details, see Alarm Remediation Actions.

5. Repeat steps **1–4** for every action you want to add to an alarm.

To change the position of an action relative to other actions, select the action and click **Move up** or **Move down**.

Step 7. Configure Alarm Suppression Settings

To automatically suppress alarms that occur under specific conditions or during a specific time interval, you can configure alarm suppression settings. For example, alarms informing about high resource utilization may need to be suppressed if these alarms occur during a scheduled resource-consuming operation (such as backup performed with Veeam Backup & Replication or other operations).

For suppressed alarms, Veeam ONE does not show any notifications and does not perform any response actions. If the object stays affected by the end of the suppression period, Veeam ONE will trigger the alarm and perform the alarm response actions.

On the **Suppress tab** of the **Alarm settings** window, specify alarm suppression settings.

Suppressing Alarms During Events

To suppress the alarm under specific conditions or when a specific event occurs, choose one of the following options:

- **Veeam Backup activity** — suppresses the alarm when Veeam Backup & Replication jobs are running. Veeam ONE detects which VMs are being processed and does not trigger alarms for these VMs and associated hosts and datastores.

  For example, if you select **Veeam Backup activity** check box for the *VM CPU Usage* alarm, this alarm will be suppressed for all VMs that are being backed up or replicated — until the jobs finish processing these VMs.

  If you select the **Veeam Backup activity** check box for the *Host CPU Usage* alarm, this alarm will be suppressed for the entire host where at least one VM is being backed up or replicated — until the jobs are finished.

- **Snapshot creation** — suppresses the alarm during snapshot creation for the object itself or its parent objects.

  For example, if you create an alarm for a VM, the alarm will be suppressed for a VM while a hypervisor creates a snapshot. If you create an alarm for a host, the alarm will be suppressed for the host while a snapshot is being created for any VM on this host.

- **Snapshot deletion** — suppresses the alarm during snapshot deletion for the object itself or its parent objects.

  For example, if you create an alarm for a VM, the alarm will be suppressed for a VM while a hypervisor deletes a snapshot. If you create an alarm for a host, the alarm will be suppressed for the host while a snapshot is being deleted for any VM on this host.

NOTE:
- The **Veeam Backup activity** suppression option apply to VMware vSphere and Microsoft Hyper-V alarms only. To enable the **Veeam Backup activity** option, make sure that you connected a Veeam Backup & Replication server to Veeam ONE. Otherwise, alarms will not be suppressed during Veeam Backup & Replication activity.
- **Snapshot creation** and **Snapshot deletion** suppression options apply to VMware vSphere alarms only.

Scheduled Alarm Suppression

To suppress the alarm according to a specific schedule during the week:

1. Select the **Suppress alarm based on schedule** option.

2. Specify time intervals on specific weekdays during which the alarm must be suppressed.

You can add more than one record for one weekday. Note that the time intervals specified for the same day must not intersect.

Step 8. Specify Alarm Details

On the **Knowledge base** tab of the **Alarm settings** window, specify alarm details. Alarm details are displayed when you select the alarm in the **Alarm Management** view or on the **Alarms** monitoring dashboard in Veeam ONE Client, and included in alarm email notifications.

1. In the **Knowledge**, **Cause** and **Resolution** fields, specify alarm details, what could cause the alarm, and steps to resolve the alarm.

2. In the **External** field, provide links to external resources containing reference information, such as VMware vSphere Documentation or Microsoft TechNet Library.

3. In the **Custom** field, specify additional information, such as comments or additional instructions.

Step 9. Save Alarm Settings

Review the specified alarm settings and click **Save** to save the alarm.

Modifying Alarms

Veeam ONE allows you to modify settings of predefined or custom alarms.

To modify alarm settings:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Alarm Management**.

3. Select an alarm from the list and do either of the following:

   o Double click the alarm.

   o Right-click the alarm and choose **Edit** from the shortcut menu.

   o In the **Actions** pane, click **Edit**.

4. Change the necessary alarm settings.

   For details on alarm settings, see Creating Alarms.

Other Ways to Modify Alarms

You can also modify alarms on the **Alarms** tab of the Veeam Backup & Replication view, Veeam Backup for Microsoft 365 view, Virtual Infrastructure view, VMware Cloud Director view, Business View view.

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the inventory pane, select the necessary infrastructure object.

4. In the information pane, open the **Alarms** tab.

5. To open the **Alarm settings** window, do either of the following:

   o Right-click the alarm and select **Edit alarm** from the shortcut menu.

   o Select the alarm in the list and click **Edit alarm** in the **Actions** pane on the right.

6. Change the necessary alarm settings.

   For details, see Creating Alarms.

Modifying Multiple Alarms

Veeam ONE supports batch alarm editing. In the batch editing mode, you can change only the **Assignment**, **Notifications**, **Actions** and **Suppression** alarm settings.

To modify settings of several alarms in batch:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Alarm Management**.

3. Select the necessary alarms in the list using the `[CTRL]` or `[SHIFT]` key on the keyboard and do either of the following:

   o Right-click the selected alarms and click **Edit** in the shortcut menu.

   o Click **Edit** in the **Actions** pane on the right.

4. Change the **Actions** or **Suppression** settings.

   For details, see Creating Alarms.

Adding Alarm Rule from Task or Event

You can add to an alarm a new rule based on a task or event that occurred in the managed environment. For example, you can create a rule that monitors the *Create virtual machine* event and notifies you whenever a new VM is created.

To create a new rule from a task or event:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the inventory pane on the left, select the necessary object.

4. In the information pane, open the **Tasks & Events** tab.

5. Right-click a task or event about which you want to be notified, select **Add this event to the existing alarm** from the shortcut menu, and click the necessary infrastructure object type.

6. In the **Select Alarms** window, select an alarm to which the rule must be added and click **Add**.

7. In the **Alarm Settings** window, change the rule settings, and click **Save**.

   For details on working with alarm rules, see Step 3. Specify Alarm Rules and Severity.

8. In the **Select Alarms** window, click **Close**.

Adding Alarm Rules from Performance Counters

You can add to an alarm a new rule based on a performance counter.

> **NOTE:**
>
> You can use this option with objects for which Veeam ONE collects performance data. For objects that do not have any performance data, such as datacenters and clusters, this option is not available.

To create a new rule from a performance counter:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the inventory pane on the left, select the necessary object.

4. Open a tab with performance parameters for which you want to create an alarm (for example, *Network, Memory, CPU, and so on*).

5. At the bottom of the performance chart, right-click the necessary counter and select **Add this counter to the existing alarm** from the shortcut menu.

6. In the **Select Alarms** window, select an alarm to which the rule must be added and click **Add**.

7. In the **Alarm Settings** window, change the rule settings, and click **Save**.

   For details on alarm rules, see Step 3. Specify Alarm Rules and Severity.

8. In the **Select Alarms** window, click **Close**.

Changing Alarm Assignment Scope

By default, all predefined alarms are assigned to the root level of the managed infrastructure. Alarms for monitoring the virtual environment apply to the root level of the virtual infrastructure — connected vCenter Server, SCVMM, failover cluster, or host. VMware Cloud Director alarms apply to the root VMware Cloud Director level. Veeam Backup & Replication alarms apply to the root level of the backup infrastructure — connected Veeam Backup & Replication server or Veeam Backup Enterprise Manager. Veeam Backup for Microsoft 365 alarms apply to the connected Veeam Backup for Microsoft 365 server.

You can change the alarm assignment scope for predefined and custom alarms, exclude one or more objects from the alarm scope, or even exclude an object from the scope of multiple alarms at once.

Modifying Alarm Assignment Scope

To modify the assignment scope of one or more alarms:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Alarm Management**.

3. In the alarm management tree, select the necessary type of infrastructure objects.

4. Select one or more alarms in the list and do either of the following:

   o Right-click the alarm and select **Edit assignment** from the shortcut menu.

   o In the **Actions** pane on the right, click **Edit assignment**.

5. In the **Edit** assignment window, select the effective assignment rules and click **Remove**.

6. Click **Add** and choose one of the following options:

   o **Virtual Infrastructure tree** — choose this option if you want to assign the alarm to specific levels of the virtual infrastructure.

   You can select infrastructure objects that match the alarm type or choose containers from the virtual infrastructure hierarchy. For example, you can assign an alarm of the *Virtual Machine* type to a specific VM, resource pool, host, cluster, datacenter, or vCenter Server or SCVMM server.

   o **Business View** — choose this option if you want to assign the alarm to custom categorization groups that you have configured in Business View.

   For example, if VMs in your environment are divided into SLA groups, you can create a set of alarms that correspond to specific service level requirements and assign these alarms to the necessary SLA group.

   o **VMware Cloud Director View** — choose this option if you want to assign the alarm to a certain level of your VMware Cloud Director infrastructure.

   You can select infrastructure objects that match the alarm type or select containers from the VMware Cloud Director hierarchy. For example, you can assign an alarm of the VMware Cloud Director vApp type to a specific vApp, organization VDC, organization or vCloud Director cell.

- o **Veeam Backup for Microsoft 365 View** — choose this option if you want to assign the alarm to a certain level of the Veeam Backup for Microsoft 365 infrastructure.

  You can select Veeam Backup for Microsoft 365 infrastructure objects that match the alarm type or select containers from the infrastructure hierarchy. For example, you can assign an alarm of the *Repository* type to a specific repository or Veeam Backup for Microsoft 365 server.

- o **Veeam Backup & Replication View** — choose this option if you want to assign the alarm to a certain level of the Veeam Backup & Replication infrastructure.

  You can select backup infrastructure objects that match the alarm type or select containers from the backup infrastructure hierarchy. For example, you can assign an alarm of the *Repository* type to a specific repository, Veeam Backup & Replication servers or Veeam Backup Enterprise Manager.

You can combine various types of alarm assignment options for the same alarm. The type of options you can combine depends on the alarm type. For example, if an alarm has the *Virtual machine* type, you can include in the assignment scope virtual infrastructure, VMware Cloud Director and Business View objects.

7. Repeat steps **3–6** for all virtual and backup infrastructure objects or categorization groups to which the alarms must be assigned.

NOTE:

Mind the following restrictions for alarm assignment:

- Alarm can be assigned to infrastructure objects that correspond to the alarm type. For example, alarm of the VM type can be assigned to VMs or to a container that includes VMs.
- The same applies to Business View groups: the alarm type must match the Business View category type. You cannot assign an alarm of the Host type to a Business View group that is used to categorize VMs.

Excluding Single Objects from Alarm Assignment Scope

You can exclude a single infrastructure object from alarm assignment:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the information pane, open the **Alarms** tab.

4. Select the necessary alarm in the list and do either of the following:

   - o Right-click the alarm and select **Edit Exclusions** from the shortcut menu.

   - o In the **Actions** pane on the right, click **Edit Exclusions**.

   If you select a container object and choose an alarm that was triggered for its child object, Veeam ONE will provide two exclusion choices — exclude the child object only or exclude the whole container from the alarm assignment scope.

   For example, if in the inventory pane you select a cluster, the list of alarms will contain alarms on the cluster and alarms on the hosts in this cluster. If you select an alarm that was triggered for a host, you can exclude either the host (child object) or the whole cluster (container).

5. Click **OK** in the dialog box to confirm exclusion.

> **NOTE:**
>
> When you exclude an object from an alarm, all unresolved *Warning* or *Error* notifications that were triggered by this alarm for the object will change their status to *Resolved*.

Excluding Multiple Objects from Alarm Assignment Scope

You can exclude multiple infrastructure objects from the alarm assignment scope:

1. Open Veeam ONE Client.

    For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Alarm Management**.

3. Select the necessary alarm in the list and do either of the following:

    o Right-click the alarm and select **Edit exclusions** from the shortcut menu.

    o In the **Actions** pane on the right, click **Edit exclusions**.

4. In the **Edit exclusions** window, click **Add** and select objects that you want to exclude from the assignment scope:

    o **Virtual Infrastructure tree** — select this option if you want to assign the alarm to specific levels of the virtual infrastructure.

    You can select infrastructure objects that match the alarm type or choose containers from the virtual infrastructure hierarchy. For example, you can assign an alarm of the *Virtual Machine* type to a specific VM, resource pool, host, cluster, datacenter, or vCenter Server or SCVMM server.

    o **Business View** — select this option if you want to assign the alarm to custom categorization groups that you have configured in Business View.

    For example, if VMs in your environment are divided into SLA groups, you can create a set of alarms that correspond to specific service level requirements and assign these alarms to the necessary SLA group.

    o **VMware Cloud Director View** — select this option if you want to assign the alarm to a certain level of your vCloud Director infrastructure.

    You can select infrastructure objects that match the alarm type or select containers from the vCloud Director hierarchy. For example, you can assign an alarm of the vCloud Director vApp type to a specific vApp, organization VDC, organization or vCloud Director cell.

    o **Veeam Backup for Microsoft 365 View** — select this option if you want to assign the alarm to a certain level of the Veeam Backup for Microsoft 365 infrastructure.

    You can select Veeam Backup for Microsoft 365 infrastructure objects that match the alarm type or select containers from the infrastructure hierarchy. For example, you can assign an alarm of the *Repository* type to a specific repository or Veeam Backup for Microsoft 365 server.

    o **Veeam Backup & Replication View** — select this option if you want to assign the alarm to a certain level of the Veeam Backup & Replication infrastructure.

    You can select backup infrastructure objects that match the alarm type or select containers from the backup infrastructure hierarchy. For example, you can assign an alarm of the *Repository* type to a specific repository, Veeam Backup & Replication servers or Veeam Backup Enterprise Manager.

You can combine various types of alarm assignment options for the same alarm. The type of options you can combine depends on the alarm type. For example, if an alarm has the *Virtual machine* type, you can include in the assignment scope virtual infrastructure, vCloud Director and Business View objects.

5. Repeat steps **3–4** for all virtual and backup infrastructure objects or categorization groups you want to exclude.

6. In the **Edit exclusions** window, click **OK**.

Other Ways to Exclude Multiple Objects from Alarm Assignment

You can also exclude objects from the alarm assignment scope on the **Alarms** tab of the Virtual Infrastructure view, Business View, VMware Cloud Director view, Veeam Backup for Microsoft 365 view or Veeam Backup & Replication view.

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the inventory pane, select the necessary infrastructure object.

4. In the information pane, open the **Alarms** tab.

5. Repeat steps **3–5** of the procedure above.

Excluding Objects from Multiple Alarms

You can exclude a single infrastructure object from the scope of multiple alarms:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the inventory pane, select the necessary infrastructure object.

4. In the information pane, open the **Alarms** tab.

5. Select an alarm and do either of the following:

   o Right-click the alarm and select **Define alarms** in the shortcut menu.

   o In the **Actions** pane on the right, click **Define Alarms**.

6. In the **Define Alarms** window, select check boxes next to alarms from which you want to exclude the object.

7. Click **OK**.

Other Ways to Exclude Objects from Multiple Alarms

You can also exclude an object from multiple alarms using the object tree in the inventory pane.

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the inventory pane, right-click the necessary object in the inventory pane and select **Alarms** > **Define alarms** from the shortcut menu.

4. In the **Define Alarms** window, select check boxes next to alarms from which you want to exclude the object.

5. Click **OK**.

Viewing Alarm Exclusions

You can view the list of excluded objects for an alarm:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Alarm Management**.

3. Select the necessary alarm in the list and click **Show All Exclusions** in the **Actions** pane on the right.
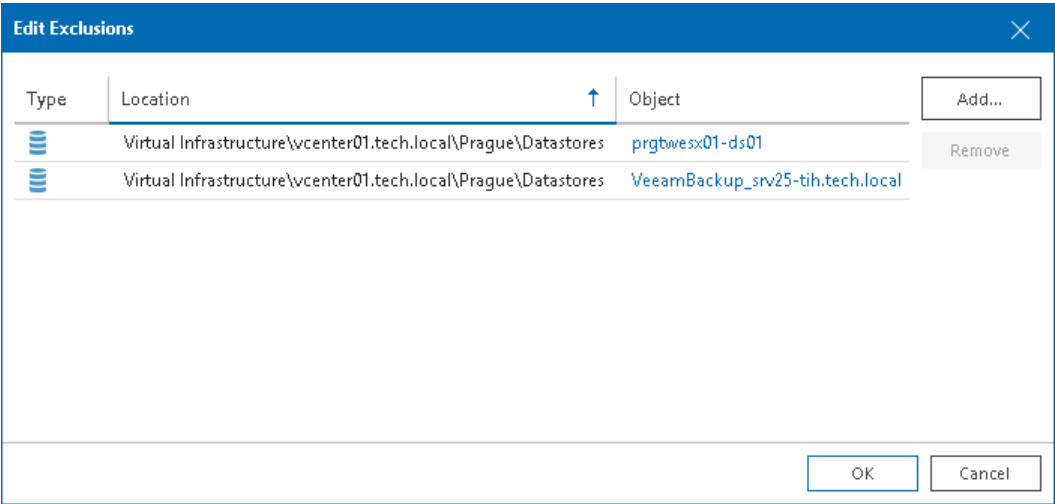
Copying Alarms

Instead of creating a new alarm from scratch, you can create a copy of an existing alarm and modify its settings.

An alarm copy keeps the same settings as the original alarm, except the alarm assignment. Initially, an alarm copy is not assigned to any virtual infrastructure, VMware Cloud Director objects, Business View groups, or Veeam Backup & Replication and Veeam Backup for Microsoft 365 infrastructure components.

To copy an alarm:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Alarm Management**.

3. Select the necessary alarm in the list.

   Press and hold the `[CTRL]` or `[SHIFT]` key on the keyboard to select multiple alarms.

4. Do either of the following:

   o Right-click the selection and click **Copy** from the shortcut menu.

   o In the **Actions** pane on the right, click **Copy**.

What You Can Do Next

After you create an alarm copy, you can change its settings and assignment scope:

1. Select the alarm copy from the list of alarms.

   Veeam ONE uses the following pattern for names of alarm copies: *Copy of <alarm name>*.

2. Change alarm settings and alarm assignment scope.

   For details on alarm settings, see Creating Alarms.

Disabling and Enabling Alarms

You can disable and enable predefined and custom alarms.

Disabling Alarms

You can disable alarms that you do not use for monitoring:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the information pane, click **Alarm Management**.

3. In the information pane, select the necessary alarm.

   Press and hold the `[CTRL]` or `[SHIFT]` key on the keyboard to select multiple alarms.

4. Do either of the following:

   o Right-click the selection and select **Disable** from the shortcut menu.

   o In the **Actions** pane on the right, click **Disable**.

> **NOTE:**
>
> After you disable an alarm, all unresolved *Warning* or *Error* notifications that were triggered by this alarm will change their status to *Resolved*.

Enabling Alarms

To enable alarms that were previously disabled:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the information pane, click **Alarm Management**.

3. In the information pane, select the necessary alarm.

   Press and hold the `[CTRL]` or `[SHIFT]` key on the keyboard to select multiple alarms.

4. Do either of the following:

   o Right-click the selection and select **Enable** from the shortcut menu.

   o In the **Actions** pane on the right, click **Enable**.

Deleting Alarms

You can delete alarms you no longer need for monitoring:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Alarm Management**.

3. In the information pane, select the necessary alarm.

   Press and hold the `[CTRL]` or `[SHIFT]` key on the keyboard to select multiple alarms.

4. Do either of the following:

   o Right-click the selection and choose **Delete** from the shortcut menu.

   o In the **Actions** pane on the right, click **Delete**.

5. In the displayed dialog box, click **OK** to confirm deletion.

> **NOTE:**
>
> When you delete an alarm in the Alarm Management view, Veeam ONE retains the alarm history. All triggered alarms and alarm status changes will be available on the **Alarms** view.
>
> The status of a deleted alarm is changed to *Resolved*. To view the history of a deleted alarm, you need to apply the *Show resolved alarms* filter. For details on working with triggered alarms, see Viewing Triggered Alarms.

Exporting and Importing Alarms

You can export alarms to an `XML` file and import alarms from an `XML` file. Exporting and importing alarms can be useful if you need to back up your alarm settings, or if you want to copy alarm settings from one Veeam ONE deployment to another.

You can use export and import options to copy alarm settings between different Veeam ONE versions. Veeam ONE 12 supports import of alarm settings that were exported from Veeam ONE version 8.0 and later.

Exporting Alarms

To export alarms to an `XML` file:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Alarm Management**.

3. In the alarm management tree, select the type of infrastructure object for which you want to export alarms.

4. Right-click the object and choose **Export Alarms** from the shortcut menu.

5. Save the `XML` file with alarm settings.

Importing Alarms

To import alarms from an `XML` file:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Alarm Management**.

3. In the alarm management tree, right-click any object and choose **Import Alarms** from the shortcut menu.

4. In the **Alarms Import** window:

   o Specify a path to an `XML` file with alarm settings.

   o Select the **Import assignment** check box if you want to import a list of alarms together with their assignment settings.

   o Select the **Replace all existing alarms** check box if you want to replace existing alarms with imported alarms.

     If you do not select this check box, but during import Veeam ONE detects alarms with matching names, Veeam ONE will suggest you to update settings of the existing alarm with data from the `XML` file. You can either replace the existing alarm with the alarm from the `XML` file, or leave the existing alarm without any changes.

     If an alarm in the `XML` file does not match any existing alarm by name, Veeam ONE will create a new alarm.

5. When the import is finished, the **Alarms Import** window will display a report with the import status, the total number of added, replaced, and skipped alarms, and the number of alarms that were imported with errors.

    Review the report and click **Close** to close the **Alarms Import** window.
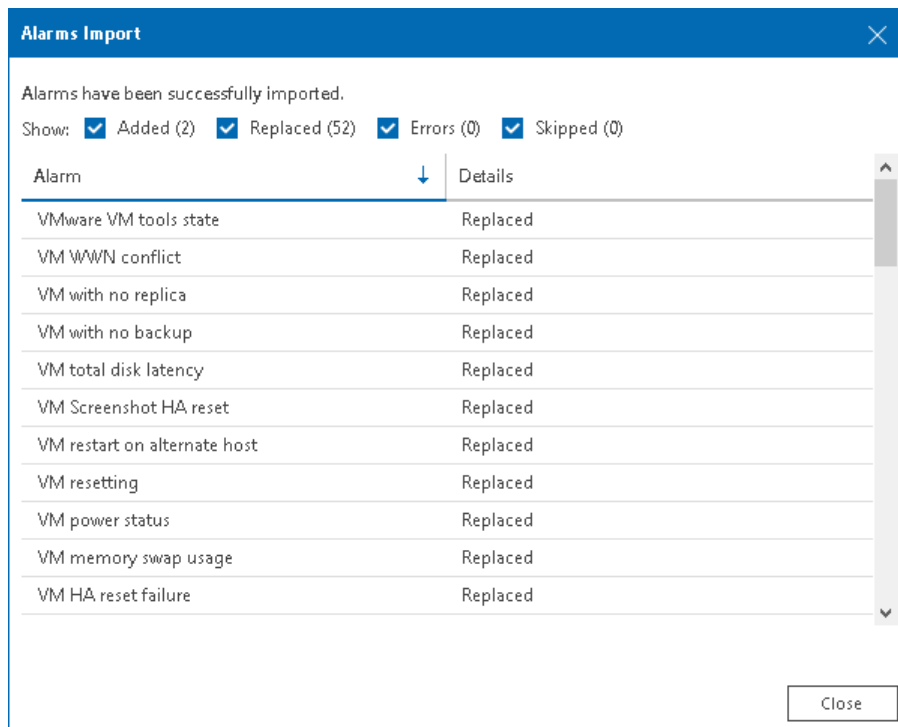
Suppressing Alarms

During resource-consuming operations, such as backup, Veeam ONE may send a great number of alarms informing about potential problems or increased resource pressure. If you do not want to receive notifications during specific activities or at a specific period of time, you can disable alarms for an object in your infrastructure. When alarms are suppressed, Veeam ONE disregards events and state changes to which the alarms react and does not trigger any alarms.

To suppress alarms, you can use one of the following options:

- Maintenance mode

- Alarm-specific suppression settings

- Suppression of guest disk space alarms

Maintenance Mode

Maintenance mode is an option used to suppress alarms for specific infrastructure objects during planned maintenance operations. After you switch an infrastructure object to the maintenance mode, Veeam ONE will suppress all alarms on this object.

You can enable the maintenance mode for single infrastructure objects or containers. When you enable the maintenance mode for a container, you can choose to propagate alarm suppression to its child objects. For example, if you want to perform maintenance on a host, you can enable the maintenance mode for the host itself and for all VMs on this host.

You can enable the maintenance mode manually or set a maintenance schedule.

Enabling Maintenance Mode Manually

You can enable the maintenance mode for an infrastructure object manually. After you switch an infrastructure object to the maintenance mode manually, Veeam ONE will stop triggering alarms for this object until you manually disable the maintenance mode.

To enable the maintenance mode for an infrastructure object manually:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the inventory pane, right-click an infrastructure object and select **Maintenance Mode** from the shortcut menu.

   If you select an object container, you can select the scope of objects for which you want to enable the maintenance mode:

   o If you select **For this object**, the maintenance mode will be enabled for the selected object only. Alarms on its child objects will not be suppressed.

   o If you select **For this and all contained objects**, the maintenance mode will be enabled for the container and its child objects.

After you enable the maintenance mode for an infrastructure object, Veeam ONE will change the infrastructure object icon, and will display the *Maintenance mode* label next to the object name in the inventory pane.

Scheduling Maintenance Mode

You can configure a maintenance schedule for infrastructure objects. When a schedule is set, the maintenance mode will be enabled and disabled automatically according to the schedule.

To configure a maintenance schedule:

1. Open Veeam ONE Client.

    For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the inventory pane, right-click an infrastructure object and choose **Schedule Maintenance Mode** from the shortcut menu.

4. In the **Schedule Maintenance Mode** window, configure the maintenance schedule.

    a. Click **Add**.

    b. In the **Type** field, specify how often the object must be placed into the maintenance mode (*once*, *monthly*, *weekly*, *daily*).

    c. In the **Day/Date** field, specify a day when the maintenance mode must be enabled.

    d. In the **Start time** and **End time** fields, specify the start and end time of the maintenance period.

    e. Select the **Apply to child objects** check box if you want to enable the maintenance mode on the object itself and its child objects.

    f. In the **Comment** field, provide additional information about the planned maintenance. You can enter up to 512 characters in this field.

    g. Select the **Enabled** check box to enable the maintenance schedule.

    h. Repeat steps **a–g** for each schedule entry you want to add.

5. Click **OK**.

To disable a maintenance schedule:

1. In the **Schedule Maintenance** window, clear the **Enabled** check box next to the necessary schedule entry.

2. Click **OK**.

The disabled schedule will remain on the list, but it will not be applied to the object.

To delete a schedule:

1. In the **Schedule Maintenance** window, select the check box next to the schedule entry you want to remove.

2. Click **Delete**.

3. Click **OK**.

Disabling Maintenance Mode

To exit a scheduled or manual maintenance mode:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the inventory pane, right-click an object in the maintenance mode and select **Exit Maintenance Mode**.

After you exit the maintenance mode, Veeam ONE will resume triggering alarms.

Alarm-Specific Suppression Settings

For each alarm, you can configure individual suppression settings to disable the alarm during specific resource-consuming operations. For details on configuring alarm suppression settings, see Step 7. Configure Alarm Suppression Settings.

Suppressing Guest Disk Space Alarms

You can suppress *Guest disk space* alarms for specific VM guest OS disks:

1. Open Veeam ONE Client.

    For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click the necessary view (*Virtual Infrastructure*, *Business View*).

3. In the inventory pane, select the necessary VM.

4. In the information pane, open the **Summary** tab.

5. In the **Guest Disk Usage** section, click the **View all disks** link.

6. In the **Guest disks** list, select check boxes next to guest OS disks for which alarms must be suppressed.

7. Click **OK**.
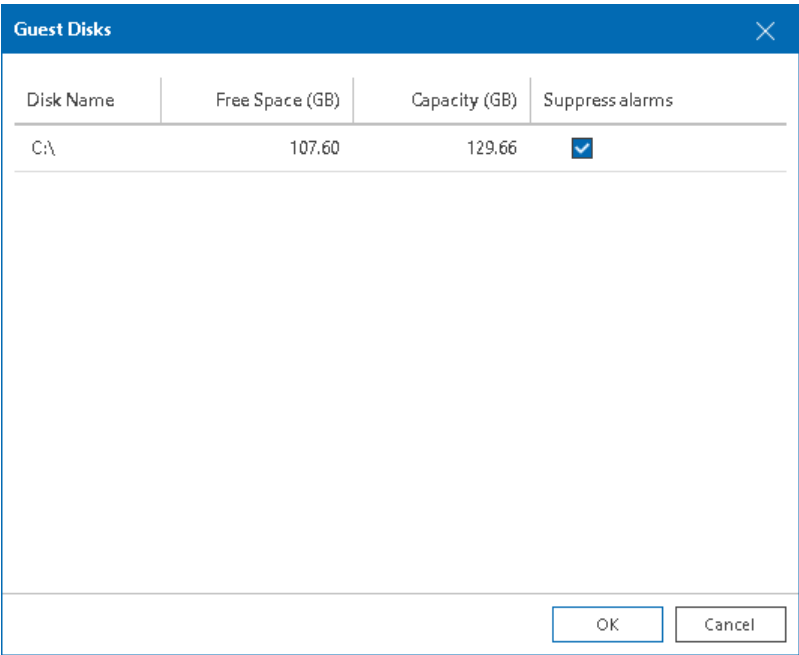
Modeling Alarm Number

Alarm modeling allows you to forecast the number and type of alarms that will be sent for a specific infrastructure object within a specified time interval. To model the alarm number, Veeam ONE applies the current alarm settings to historical data collected for the selected infrastructure object, and calculates the approximate number of alarms that will be sent within the specified time interval in future.

Alarm modeling can help you avoid receiving non-significant alarms, or conversely missing important events. After you change alarm settings, you can perform alarm modeling to estimate how many alarms will be triggered for an infrastructure object if you keep the effective alarm settings. Taking into consideration the modeled number of alarms, you can consider changing alarm settings. For example, if the number is too high, you can adjust alarm rule conditions.

To forecast the number of alarms that will be sent for a specific infrastructure object:

1. Open Veeam ONE Client.

    For details, see Accessing Veeam ONE Client.

2. In the main menu, click **Modeling**.

3. In the **Alarm Modeling** window, click **Select** and choose the necessary type of infrastructure objects (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

4. In the **Select Node** window, select check box next to an infrastructure object for which you want to model the number of alarms and click **Select**.

5. From the **Interval** drop-down list, select the period for which historical data must be analyzed (week, month or year).

6. In the list of alarms, select check boxes next to alarms for which you want to perform modeling.

7. Click **Start Modeling**.

Veeam ONE will forecast the number of alarms of different severity that will be sent within the selected period of time.
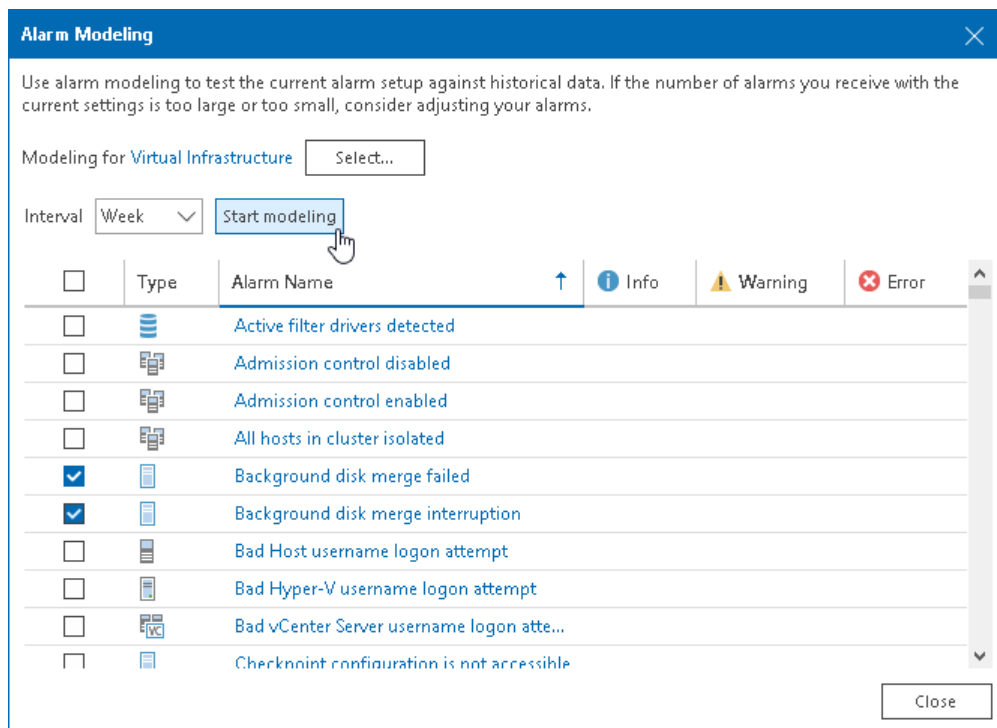
Other Ways to Perform Alarm Modeling

To perform alarm modeling for a selected infrastructure object:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the inventory pane, right-click an infrastructure object and select **Alarms** > **Modeling** from the shortcut menu.

4. From the **Interval** drop-down list, select the period for which historical data must be analyzed (week, month or year).

5. In the list of alarms, select check boxes next to alarms for which you want to perform modeling.

6. Click **Start Modeling**.

To perform alarm modeling for selected alarms:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Alarm Management**.

3. Select the one or more alarms in the list, right-click the selection and select **Modeling** from the shortcut menu.

4. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

5. In the **Select Node** window, select check box next to an infrastructure object for which you want to model the number of alarms and click **Select**.

6. From the **Interval** drop-down list, select the period for which historical data must be analyzed (week, month or year).

7. Click **Start Modeling**.

Configuring Alarm Notifications

To ensure you do not miss critical events or state changes in the managed infrastructure, you can configure Veeam ONE to send notifications when alarms are triggered. Veeam ONE supports the following types of alarm notifications:

- Email Notifications

- SNMP Traps

Configuring Email Notifications

To stay informed about potential problems, state changes, events, and tasks performed by users in your infrastructure, you can configure Veeam ONE to send email notifications about alarms. Email notifications contain basic information that helps to find the root cause of an issue and resolve it.

An email notification can be sent when a new alarm is triggered or when an existing alarm changes its status.

To configure alarm email notifications, perform the following steps:

1. Configure SMTP server settings.

2. Configure notification frequency.

3. Customize the email template.

4. Configure email recipients.

5. [Optional] Disable notifications about resolved alarms.

Step 1. Configure SMTP Server Settings

To deliver email notifications, Veeam ONE needs an SMTP server.

To configure SMTP settings:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, you can press `[CTRL + S]` on the keyboard.

3. In the **Server Settings** window, open the **Mail Server Settings** tab.

4. Select the **Enable email notifications** check box.

5. From the drop-down list, select **Custom SMTP (Basic authentication)**.

6. In the **SMTP server** field, specify DNS name or IP address of the SMTP server that must be used for sending email notifications.

   The default SMTP port number is `25`.

7. In the **From** field, enter an email address of the notification sender.

   This email address will be displayed in the **From** field of the email header.

8. To configure additional settings, click Advanced:

   a. In the **Timeout** field, specify server connection timeout in milliseconds.

   b. In the **Port** field, change the default SMTP communication port if required.

   c. For SMTP server with SSL support, select **Connect using SSL** to enable SSL data encryption.

   d. If your SMTP server requires authentication, select the **Use authentication** check box and specify authentication credentials in the **Login** and **Password** fields.

e. Click **OK**.

Sending Test Email

To check whether you have specified SMTP settings correctly, you can send out a test email:

1. Click **Send Test Email**.

2. In the **Test Email Settings** window, specify an email address to which a test notification must be sent.

3. Click **OK**.

The test email will be sent to the specified email address. Veeam ONE will notify you whether the message was successfully sent.

Step 2. Configure Notification Frequency

Veeam ONE sends an email notification when a new alarm is created or when the status of an existing alarm is changed. If you do not want to receive an email message each time a new alarm is triggered or alarm status changes, you can change the notification frequency.

The frequency with which Veeam ONE sends email notifications is defined by *notification policy*. There are two types of notification policies:

- Mission Critical

- Other

You can apply different types of notification policies to different infrastructure objects.

Enabling Mission Critical Notifications

Mission Critical notification policy is the default policy that is enabled for all infrastructure objects. This policy prescribes Veeam ONE to send an email notification every time a new alarm is created or the status of an existing alarm changes. An email notification contains details on the triggered alarm and affected object.

The following image shows an example of an email notification for the *Mission Critical* policy.

To apply the **Mission Critical** notification policy to an infrastructure object:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. On the toolbar, click **Options** and select **Server Settings**.

   Alternatively, you can press [CTRL + S] on the keyboard.

3. In the **Server Settings** window, open the **Notification Policy** tab.

4. In the **Email notification policies** section, select **Mission Critical** and click **Edit**.

5. In the **Edit Email Policy** window, click **Select** and choose one of the infrastructure types.

6. In the **Select Objects** window, click **Select**.

7. In the **Edit Email Policy** window, Click **OK**.
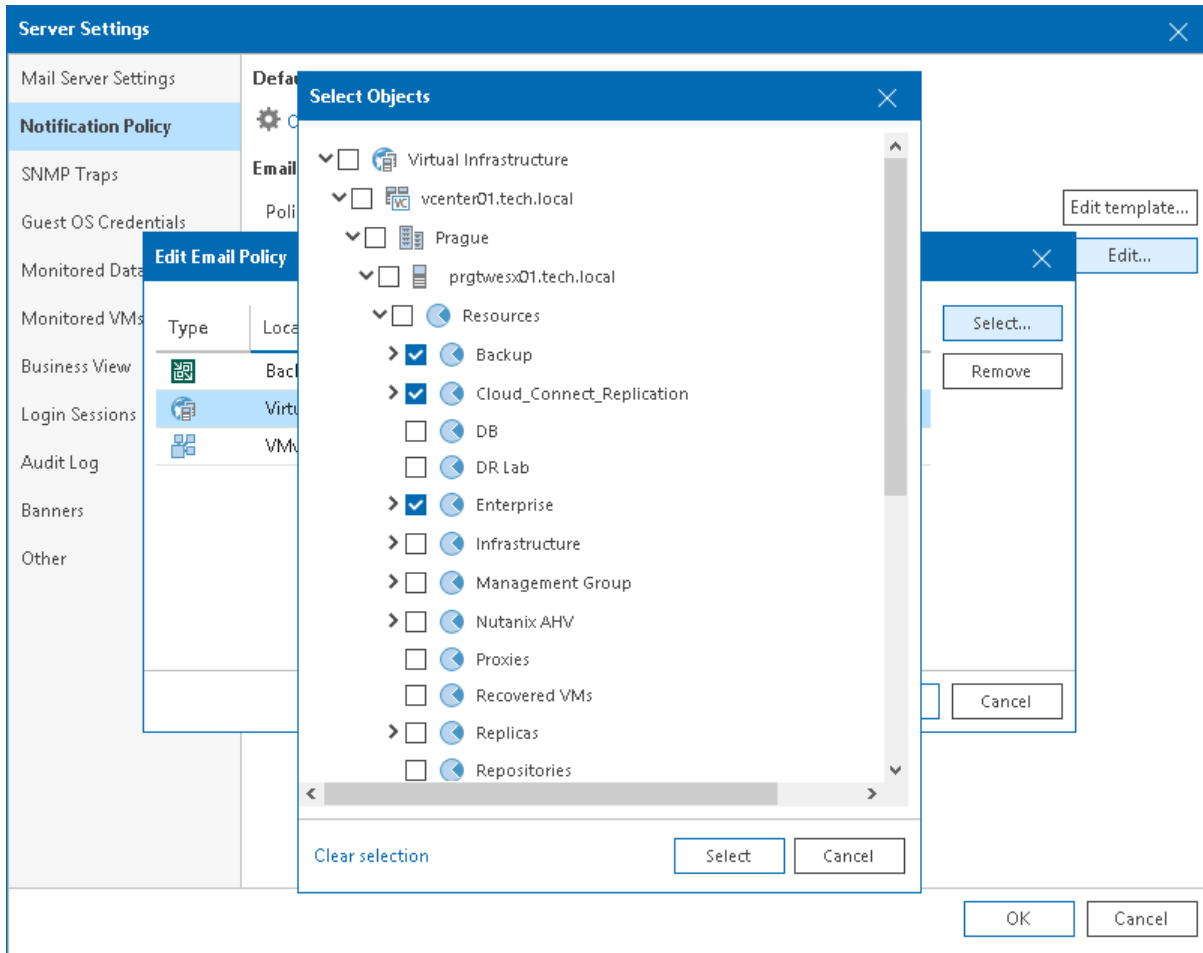
Enabling Summary Notifications

Other notification policy prescribes Veeam ONE to accumulate information about alarms and send an email notification once within a specific time interval (by default, a notification is sent once every 30 minutes). You do not receive a notification on every triggered alarm. Instead, Veeam ONE generates a message with a list of all alarms triggered over the past period.

You can choose how often you want to receive summary email notifications. For example, if you specify the time interval of 15 minutes, you will receive notifications with the list of alarms triggered over the past 15 minutes. If no alarms are triggered over the past 15 minutes, you will not receive a summary email notification.

The following image shows an example of a summary email notification for the *Other* policy.

By default, all infrastructure objects have the *Mission Critical* policy assigned. Before you apply the *Other* notification policy to an object, you must remove the default *Mission Critical* policy assignment:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. On the toolbar, click **Options** and select **Server Settings**.

   Alternatively, you can press [CTRL + S] on the keyboard.

3. In the **Server Settings** window, open the **Notification Policy** tab.

4. In the **Email notification policies** section, select the *Mission Critical* policy and click **Edit**.

5. In the **Edit Email Policy** window, select the necessary type of infrastructure objects and click **Remove**.

6. In the **Edit Email Policy** window, click **OK**.

To apply the *Other* notification policy to one or more infrastructure objects:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. On the toolbar, click **Options** and select **Server Settings**.

   Alternatively, you can press [CTRL + S] on the keyboard.

3. In the **Server Settings** window, open the **Notification Policy** tab.

4. In the **Email notification policies** section, select *Other* and click **Edit**.

5. In the **Edit Email Policy** window, click **Select** and choose one of the infrastructure types.

6. In the **Select Objects** window, click **Select**.

7. In the **Time interval to send summary email (minutes)** field, specify how often Veeam ONE must send out a summary email informing about triggered alarms. The default time interval is 30 minutes.

8. In the **Edit Email Policy** window, click **OK**.
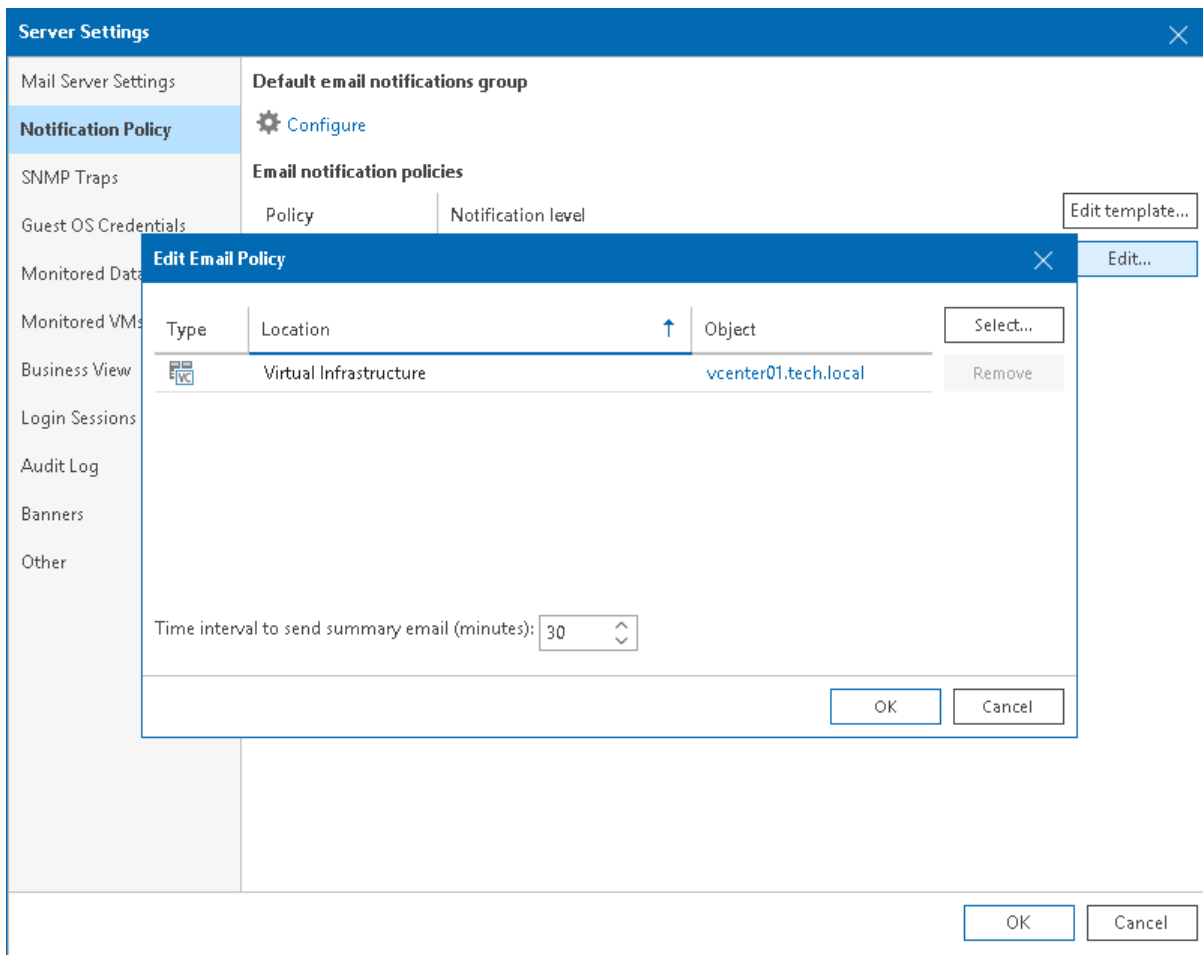
Step 3. Customize Email Template

You can customize the email template used for alarm notifications. In the template, you can change the following items:

- Email subject and body

- Email format

> **NOTE:**
>
> You can customize the email template for *Mission Critical* notifications only. You cannot modify the template for alarm summary notifications sent in accordance with the *Other* notification policy. For more information on notification policies, see Step 2. Configure Notification Frequency.

Configuring Email Subject and Body

You can customize the email notification subject:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. On the toolbar, click **Options** and select **Server Settings**.

   Alternatively, you can press [CTRL + S] on the keyboard.

3. In the **Server Settings** window, open the **Notification Policy** tab.

4. In the **Email notification policies** section, select *Mission Critical* and click **Edit template**.

5. In the **Email subject template** field, specify the subject of the notification.

   You can use the following variables in the subject text:

   - *%ALARM_NAME%* — name of the alarm

   - *%TIME%* — date and time when the alarm was triggered or when the alarm status changed

   - *%STATUS%* — current alarm status

   - *%OLD_STATUS%* — status of the alarm before its status was changed

   - *%OBJECT%* — affected infrastructure object

   - *%OBJECT_TYPE%* — type of the affected infrastructure object

   - *%SOURCE%* — affected child object

   - *%LOCATION%* — location of the object in the infrastructure tree

   - *%HOST%* — name of a vCenter Server, SCVMM server, or Veeam Backup & Replication server

6. In the **Select additional fields to include to the email notifications** section, select check boxes next to options you want to include in the body of the email message.

   General options apply to email notification for all types of alarms.

   - **KB article** — select this check box if an email notification must include a knowledge base article.

- o **Business View group** — select this check box if an email notification must include a category assigned to the object in Business View.

VM options apply to email notifications for VM alarms.

- o **Guest OS IP address** — select this check box if an email notification must include IP and MAC addresses of the affected VM.

- o **Guest OS type** — select this check box if an email notification must include information about the guest OS of the affected VM.

- o **Guest OS hostname** — select this check box if an email notification must include a DNS name of the affected VM.

- o **Notes** — select this check box if an email notification must include custom notes that can be specified in alarm details.

7. Click **OK**.
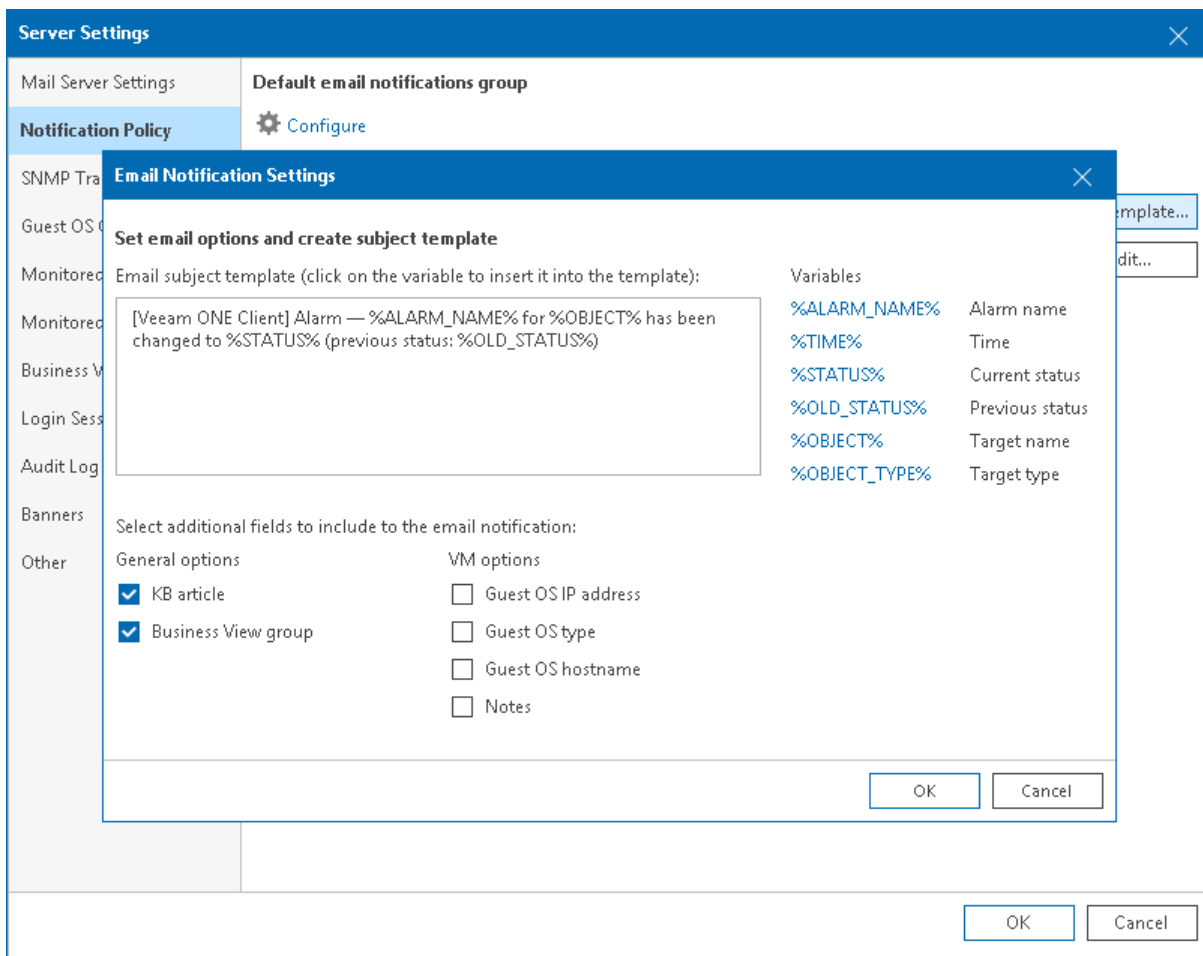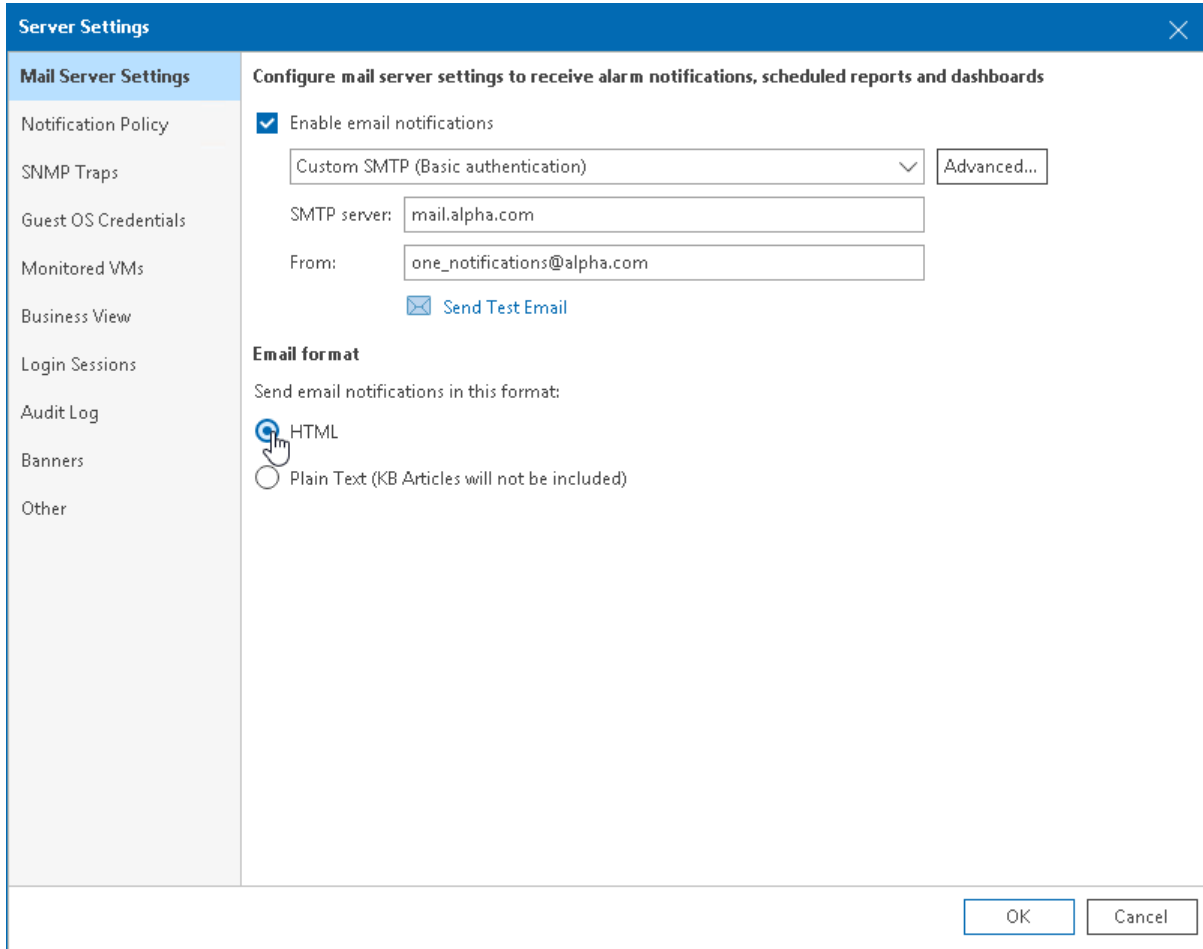
Configuring Email Format

By default, Veeam ONE sends email notifications in the HTML format. You can change notification format to *plain text*. Note that plain text notifications do not support HTML elements, formatted text, colors or graphics. Plain text notifications also do not include knowledge base articles.

To choose the email notification format:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. On the toolbar, click **Options** and select **Server Settings**.

   Alternatively, you can press [CTRL + S] on the keyboard.

3. On the **SMTP Settings** tab, in the **Email format** section, choose a format: *HTML* or *Plain Text*.

4. Click **OK**.

Step 4. Configure Email Recipients

To report about triggered alarms by email, Veeam ONE must know where to deliver messages. When you configure alarm notifications, you must specify email addresses of users who will receive these notifications.

Veeam ONE offers the following options for configuring email notification recipients:

- You can add recipients to the default email notification group.

  This option can be useful if you want to notify responsible personnel when alarms are triggered or when alarms change their statuses.

- You can configure recipients for individual alarms.

  This option can be useful if you want to notify responsible personnel when a specific event occurs in the managed infrastructure.

Configuring Default Email Notification Group

The default email notification group includes a list of recipients who must be notified about alarms by email. All predefined alarms are configured to send email notifications to the default notification group. You can also configure custom alarms to send notifications to the default notification group.

To add recipients to the default email notification group:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. On the toolbar, click **Options** and select **Server Settings**.

   Alternatively, you can press [CTRL + S] on the keyboard.

3. Open the **Notification Policy** tab.

4. In the **Default email notifications group** section, click **Configure**.

5. In the **Default Email Notification Group** window, specify email addresses of notification recipients.

   To add a recipient, in the **Add this recipient** field enter recipient email address and click **Add**. If you want to specify several recipients, separate email addresses with ";" (semicolon), "," (comma) or ", " (comma with space).

6. From the **Notification Level** list, choose the severity of alarms about which recipients must be notified:

   - **Any state** — an email notification will be sent every time when an alarm status changes to *Error*, *Warning* or *Info*.

   - **Errors and warnings** — an email notification will be sent every time when an alarm status changes to *Error* or *Warning*.

   - **Errors only** — an email notification will be sent every time when an alarm status changes to *Error*.

7. Click **OK**.
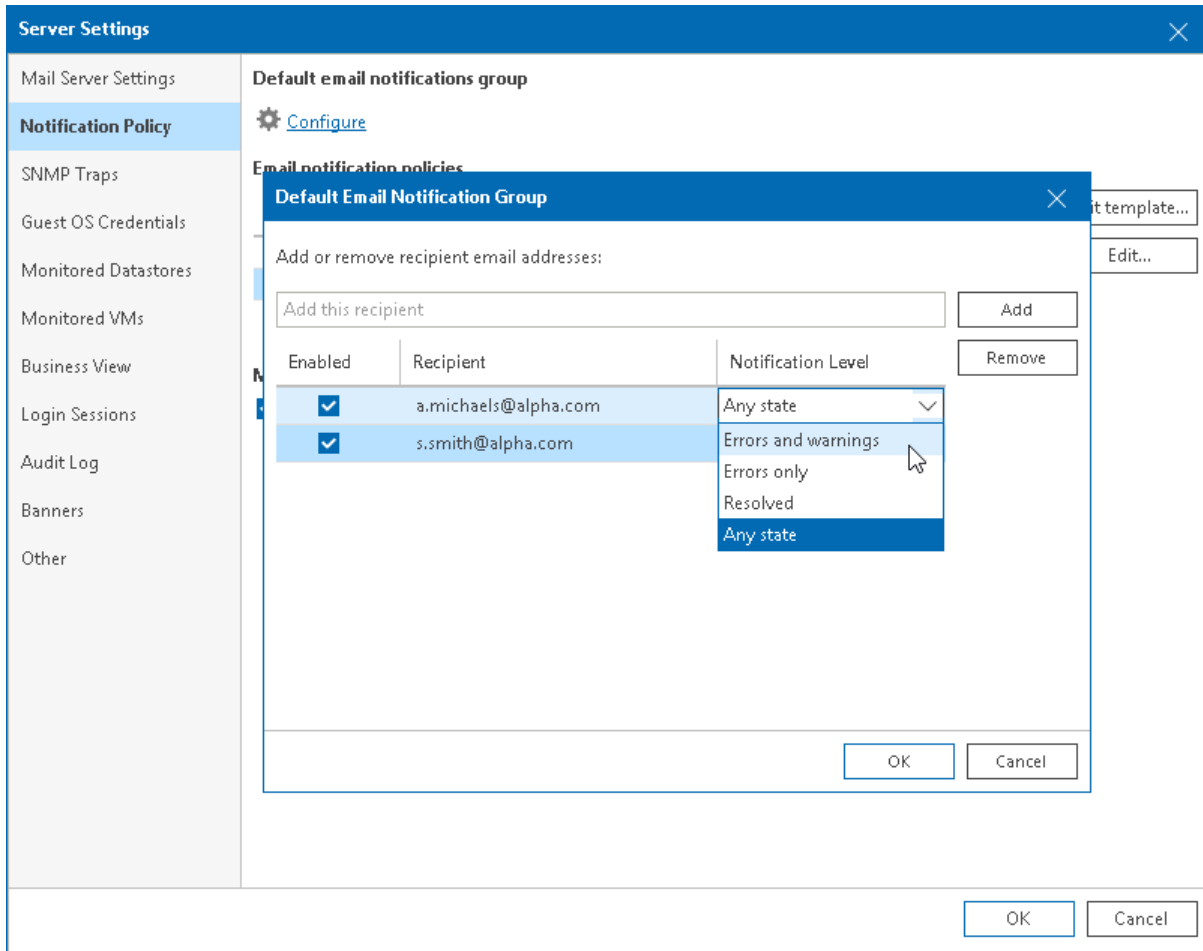
You can temporarily disable email notifications for specific recipients in the default email notification group. The recipients will remain on the list, but they will no longer receive email notifications on triggered alarms.

1. In the **Default Email Notification Group** window, clear the check box next to recipient email address.

2. Click **OK**.

To permanently remove a recipient from the default email notification group:

1. In the **Default Email Notification Group** window, select an email address you want to delete and click **Remove**.

2. Click **OK**.

Configuring Recipients for Specific Alarms

You can add email notification recipients to each alarm individually and specify alarm severity about which the recipients must be notified.

To add one or more recipients to a specific alarm:

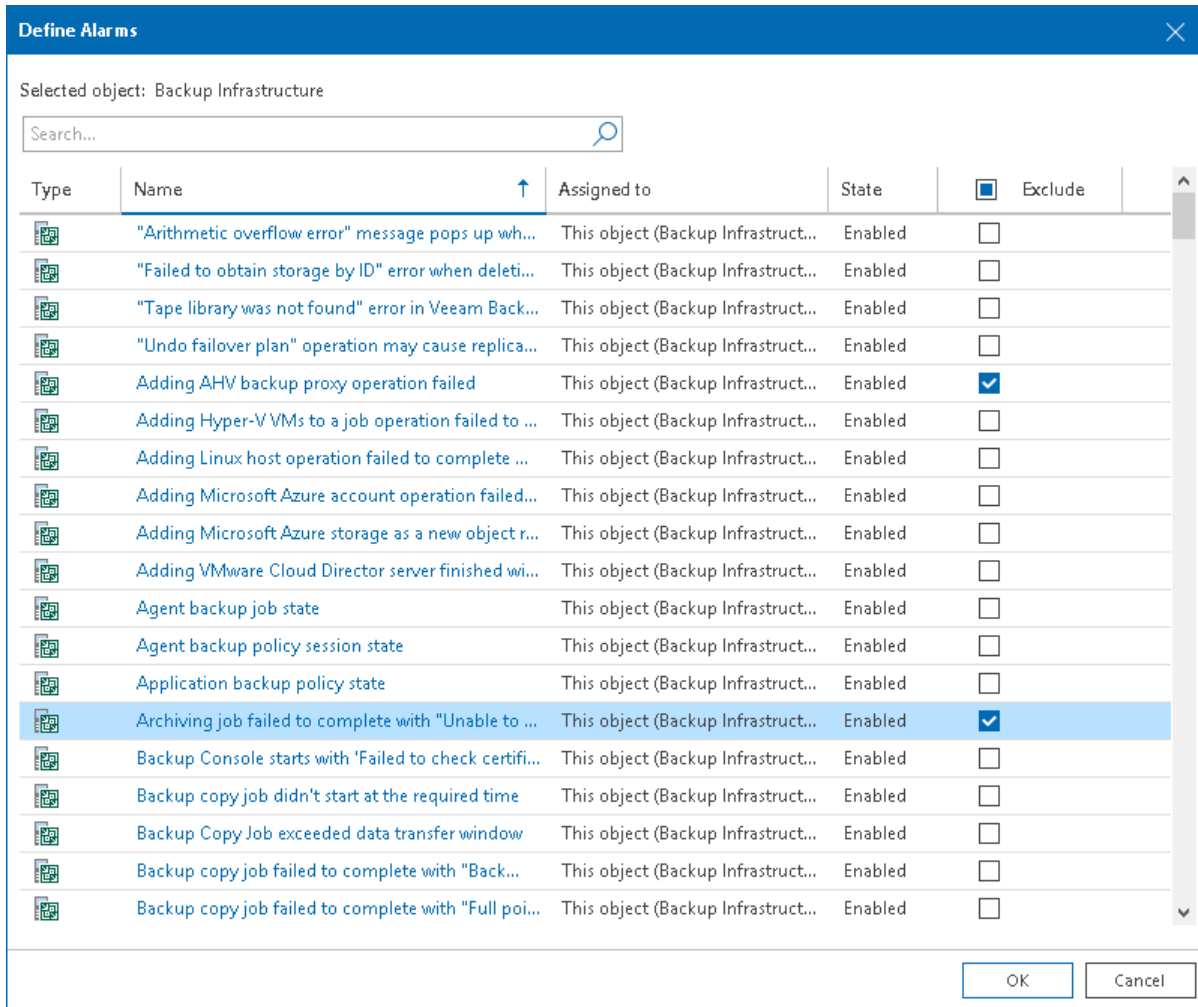1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Alarm Management**.

3. To open the **Alarm Settings** window for the necessary alarm, do either of the following:

    ○ Double click the alarm in the list.

    ○ Right-click the alarm and choose `Edit` from the shortcut menu.

    ○ Select the alarm in the list and click `Edit` in the **Actions** pane on the right.

4. In the **Alarm Settings** window, open the **Notifications** tab.

5. On the **Notifications** tab, click `Add`.

6. From the **Action** list, select the **Send alarm notification** option.

7. In the `Value` field, specify an email address of the recipient.

    If you want to specify several recipients, separate email addresses with ";" (semicolon), "," (comma) or ", " (comma with space).

8. From the **Condition** list, choose the severity of alarms about which the recipient must be notified:

    ○ **Any state** — an email notification will be sent every time when an alarm status changes to *Error*, *Warning* or *Info*.

    ○ **Errors and warnings** — an email notification will be sent every time when an alarm status changes to *Error* or *Warning*.

    ○ **Resolved** — an email notification will be sent every time when an alarm status changes to *Resolved.*

    ○ **Errors only** — an email notification will be sent every time when an alarm status changes to *Error*.

9. Click `Save`.

Step 5. Disable Notifications About Resolved and Acknowledged Alarms

By default, Veeam ONE sends an email notification when an alarm is triggered, when its status changes to *Error* or *Warning,* when an alarm is resolved and acknowledged. If you do not want to receive notifications on resolved and acknowledged alarms, you can disable them.

To disable email notifications on resolved and acknowledged alarms:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. On the toolbar, click **Options** and select **Server Settings**.

   Alternatively, you can press [CTRL + S] on the keyboard.

3. In the **Server Settings** window, open the **Notification Policy** tab.

4. In the **Miscellaneous** section, clear the **Send notification when alarm metrics are back to normal** check box.

5. Click **OK**.
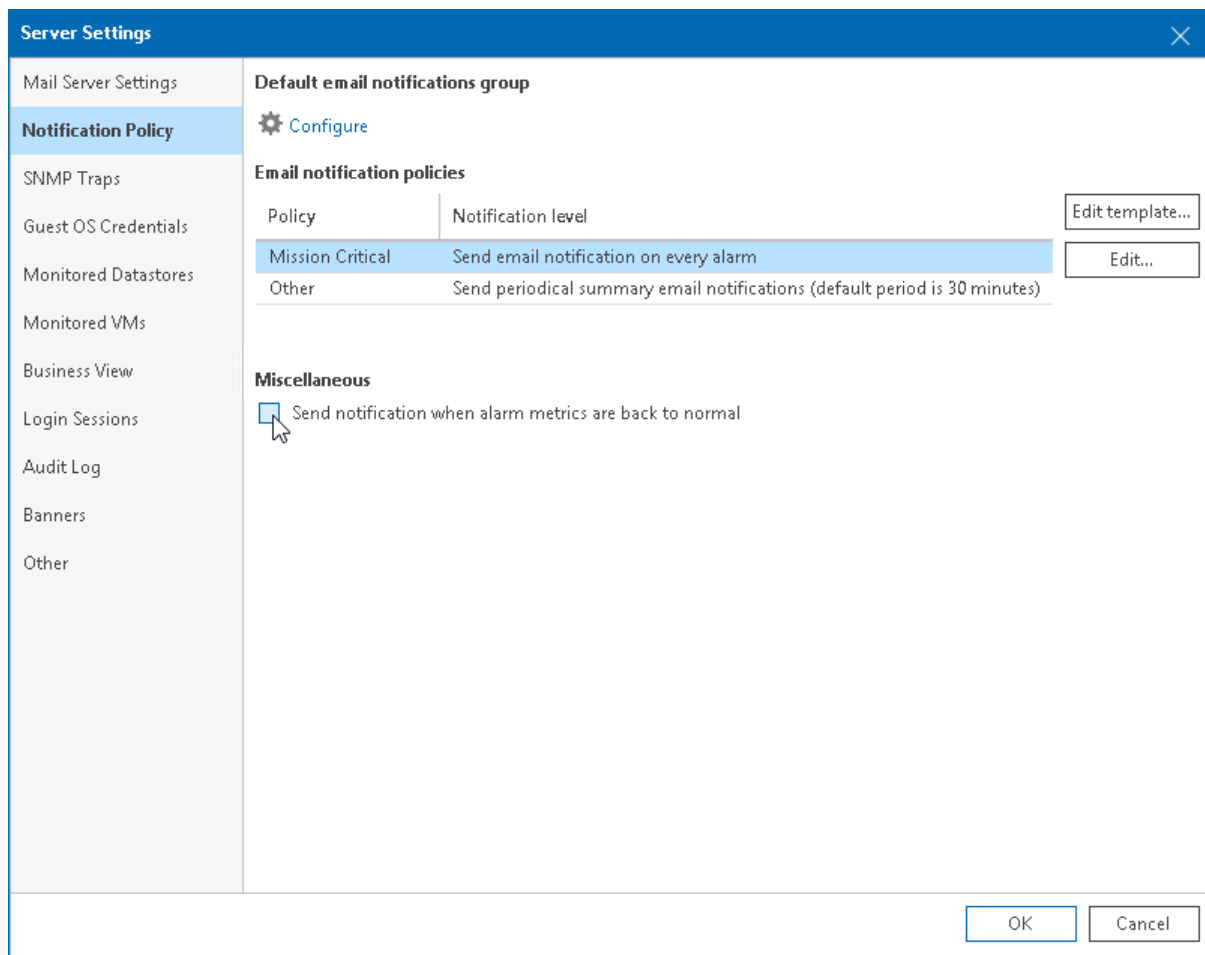
Configuring SNMP Traps

If you use SNMP to monitor applications and devices in the managed infrastructure, you can configure Veeam ONE to report about triggered alarms by means of SNMP traps. When SNMP trap notifications are enabled, Veeam ONE acts as an agent. It generates trap messages when an alarm is triggered, and sends them to SNMP receivers. SNMP receivers can then forward the traps to a management application.

Veeam ONE sends SNMP traps with the following information:

- Date and time the alarm was triggered

- Name of the affected node

- Old alarm status

- New alarm status

- Alarm name

- Alarm summary

Veeam ONE supports SNMP versions 1, 2, and 3. For version 3, Veeam ONE sends traps based on CISCO-SNMP-USM-OIDS-MIB that complies with RFC 3414.

To configure SNMP traps, perform the following steps:

1. Configure SNMP receivers and manager.

2. Configure SNMP settings in Veeam ONE.

3. Change alarm action settings to enable SNMP traps for the necessary alarms.

Step 1. Configure SNMP Receivers and Manager

To receive and process SNMP traps generated by Veeam ONE, you must install and configure the following components:

1. SNMP receivers that will listen for traps.

2. SNMP management application that will obtain and process traps from receivers.

The configuration procedure depends on the SNMP processing solution you use to handle traps. To learn how to configure an SNMP receiver with Net-SNMP, see SNMPTRAPD.

Step 2. Configure SNMP Settings in Veeam ONE

To send SNMP traps, Veeam ONE must know trap destinations. You must specify a list of receivers to which Veeam ONE must send traps, and ports that SNMP receivers will listen.

To configure SNMP trap destination settings in Veeam ONE:

1. Open Veeam ONE Client.

    For details, see Accessing Veeam ONE Client.

2. On the toolbar, click **Options** and select **Server Settings**.

    Alternatively, you can press [CTRL + S] on the keyboard.

3. In the **Server Settings** window, open the **SNMP** tab.

4. Click **Add**

5. From the drop-down list on the left, select the preferable SNMP version.

6. Configure receiver settings. To do that:

    o For SNMP v.1 and v.2

        i. Double-click the added entry in the list.

            Alternatively, you can select the receiver entry and click **Configure**.

        ii. In the **Receiver** field, specify FQDN or IP address of the SNMP receiver.

        iii. In the **Port** field, specify the port number.

        iv. In the **Community string** field, specify the community identifier.

        v. Click **OK**.

vi. To add a new receiver to the list, click **Add** and repeat steps a-e.
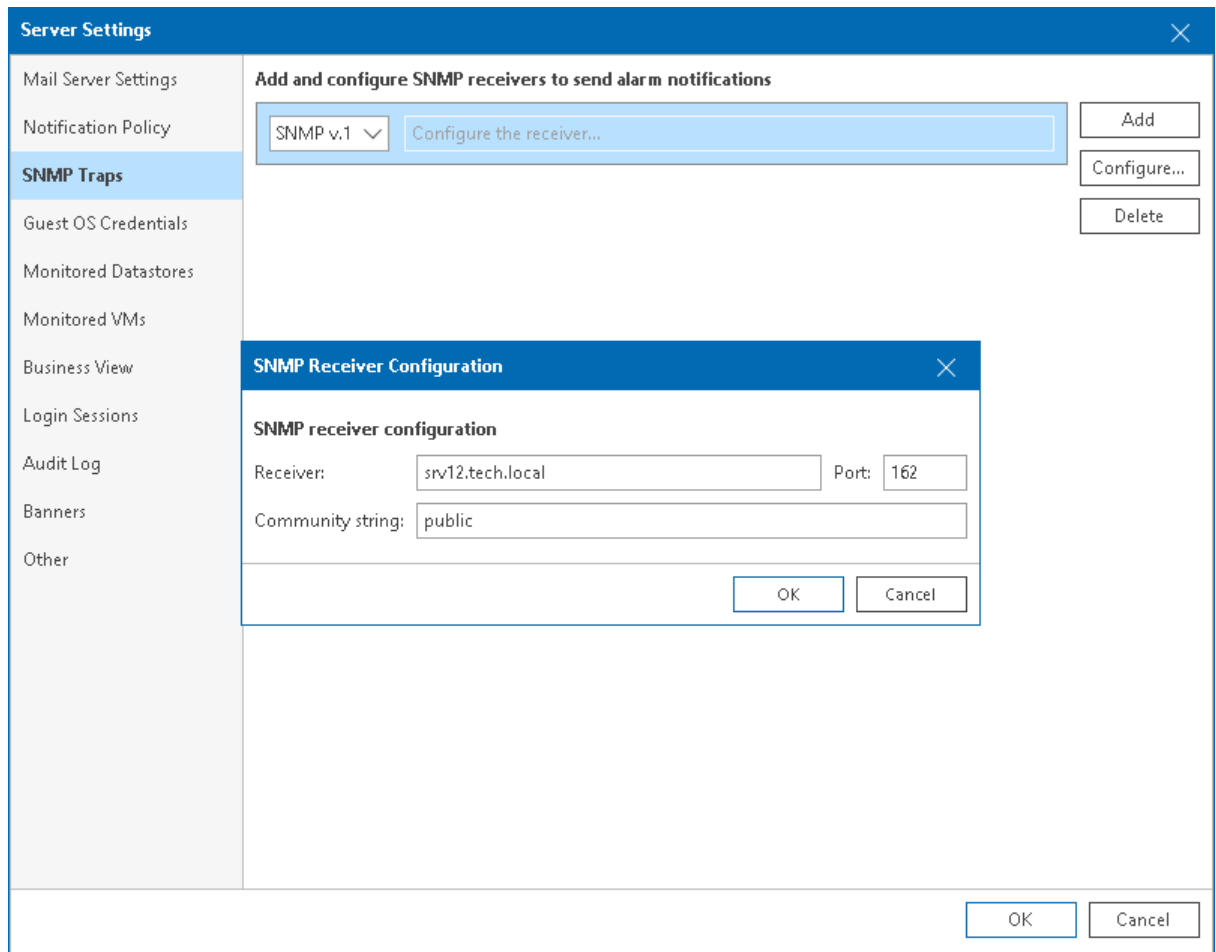
o For SNMP v.3

   i. Double-click the added entry in the list.

   Alternatively, you can select the receiver entry and click **Configure**.

   ii. In the **Receiver** field, specify FQDN or IP address of the SNMP receiver.

   iii. In the **Port** field, specify the port number.

   iv. In the **Engine ID** field, specify an ID for an SNMP remote agent.

   v. In the **Username** and **Password** fields, specify credentials for SNMP receiver user account.

   vi. From the **Authentication model** list, select the authentication algorithm for SNMP receiver user.

   vii. From the **Privacy protocol** list, select encryption method for SNMP messages.

   viii.   In the **Privacy password** field, specify a password that an SNMP receiver will use for private access.

   ix. Click **OK**.

x. To add a new receiver to the list, click **Add** and repeat steps a-i.

7. Click **OK**.

Step 3. Enable SNMP Notification for Alarms

To receive SNMP traps when an alarm is triggered, you must set SNMP notification as a response action for every alarm manually.

To configure SNMP traps for an alarm:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Alarm Management**.

3. To open the **Alarm Settings** window for the necessary alarm, do either of the following:

   o Double click the necessary alarm in the list.

   o Right-click the alarm and choose **Edit** from the shortcut menu.

   o Select the alarm in the list and click **Edit** in the **Actions** pane on the right.

4. In the **Alarm Settings** window, open the **Actions** tab.

5. On the **Actions** tab, click **Add**.

6. From the new **Action** list, select **Send SNMP trap**.

7. In the **Condition** field, specify at which state Veeam ONE must send trap messages.

8. Click **Save**.

Working with Triggered Alarms

You can perform the following actions with alarms that were triggered by Veeam ONE:

- View triggered alarms

- Resolve alarms

- Acknowledge alarms

- Approve alarm remediation action

- View alarm history

- Export triggered alarms

Viewing Triggered Alarms

To view alarms triggered for a specific infrastructure object:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the inventory pane, select the necessary object.

4. In the information pane, open the **Alarms** tab.

The list of alarms shows alarms triggered for the selected infrastructure object and alarms for child objects.

For every alarm, the following details are available:

- **Status** — current status of the alarm (*Warning*, *Error*, *Resolved*, *Info* or *Acknowledged*). If an alarm was triggered multiple times, its latest state will be displayed in the list.

- **Time** — date and time when the alarm was triggered. If the alarm was triggered multiple times, the latest date time when the alarm was triggered will be displayed in the list.

- **Source** — name of the infrastructure object that caused the alarm. To view all alarms related to the infrastructure object, click the source link.

- **Type** — type of the infrastructure object that caused the alarm.

- **Name** — alarm name. Click the name link to open alarm details in the **Alarm Management** section.

  If the alarm has been already deleted and not available in the **Alarm Management** section, the alarm name is shown as plain text.

- **Repeat count** — the number of times the alarm was triggered or changed its status. Click the repeat count link to view the alarm history.

  For more details, see Viewing Alarm History.

- **Remediation** — remediation action and resolution type configured for an alarm.

  For more information on remediation actions, see Alarm Remediation Actions.

The **Alarm details** section of the information pane displays knowledge base for the selected alarm — description of the problem, possible causes, instructions for resolution, links to external resources, and other details.

The **Actions** pane on the right displays links to actions that you can perform against triggered alarms, as well as navigation links.

Searching for Alarms

To quickly find the necessary alarms, you can use filters and controls at the top of the **Alarms** list.

You can limit the list of alarms by the following criteria:

- To find alarms by alarm name, use the search field.

- To display or hide alarms with a specific severity, click the **Status** icons — *Show alarms with all statuses*, *Show alarms with status "Error"*, *Show alarms with status "Warning"*, *Show alarms with status "Resolved"*, *Show informational alarms,* and *Show alarms with status "Acknowledged"*.

- To display alarms with configured remediation actions, click the **Show alarms with available Remediation Actions** icon.

- To display or hide alarms for a specific type of infrastructure objects, click the object type icons — *Show alarms for all types of objects* or *Show [object type] alarms*.

- To display alarms that are related to the selected infrastructure object, use the **This object** icon. Release the icon to display alarms for the selected infrastructure object and alarms for its child objects. Press the icon to display alarms for the selected object only.

- To set the time interval within which alarms were triggered, use the **Filter alarms by time period** icon and set the necessary time interval. Release the icon to discard the time interval filter.

You can click column names to sort alarms by a specific parameter. For example, to view repetitive alarms, you can sort alarms in the list by **Repeat Count** in the descending order.

Resolving Alarms

Veeam ONE alarms can be resolved automatically or manually.

Alarms are resolved automatically in the following cases:

- When an alarm is disabled or deleted.

- When an object that caused the alarm is deleted or excluded from the alarm assignment scope.

- When conditions that caused the alarm are eliminated, and the alarm is configured to react to this (the alarm resolve action is automatic).

  For example, some alarms are configured to change the alarm severity to **Resolved** in specific cases or during events that occur in the managed infrastructure. Other alarms — such as alarms that are triggered when resource usage is above a certain threshold — are resolved automatically when the resource usage level is back to normal.

You can manually resolve alarms if the state of the monitored object is back to normal, or if the alarm requires no further investigation and no corrective actions should be taken.

Resolving Individual Alarms

To resolve individual alarms:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the inventory pane, select the necessary object.

4. In the information pane, open the **Alarms** tab.

5. In the list of alarms, select one or more alarms and do either of the following:

   o Right-click the selection and choose **Resolve** from the shortcut menu.

   o In the **Actions** pane, click **Resolve**.

   Press and hold the `[CRTL]` or `[SHIFT]` key to select multiple alarms.

6. In the **Resolve Alarm** window, specify a reason for changing the alarm status, or provide any other additional information.

   The message you specify will appear in the **Comment** field of the alarm history details, and in the email notification on resolved alarms. For details, see Viewing Alarm History and Notifications on Resolved Alarms.

7. Click **OK**.

Resolving Multiple Alarms

To resolve all displayed alarms at once:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the inventory pane, select the necessary object.

4. In the information pane, open the **Alarms** tab.

5. Use the filters and the search field at the top of the list to display the alarms that you want to resolve.

   For details on alarm filters, see Searching for Alarms.

6. Do either of the following:

   o Right-click anywhere in the list of alarms and choose **Resolve all alarms** from the shortcut menu.

   o In the **Actions** pane, click **Resolve All**.

7. In the **Resolve All Alarms** window, specify a reason for changing the alarm status, or provide any other additional information.

   The message you specify will appear in the **Comment** field of the alarm history details, and in the email notification on resolved alarms. For details, see Viewing Alarm History and Notifications on Resolved Alarms.

8. Click **OK**.

Notifications on Resolved Alarms

When one or more alarms are resolved, Veeam ONE sends an email notification to users who monitor the affected object. The notification includes information about the number of alarms resolved, resolve action, time and reason, as well as the list of resolved alarms.

To receive notifications about resolved alarms, make sure that:

- You have configured SMTP server settings.

  For details, see Step 1. Configure SMTP Server Settings.

- Your email address is included either in the default notification group, or in the list of notification recipients specified in the alarm action settings, and the notification level is set to *Any state*.

  For details, see Step 4. Configure Email Recipients.

- Notifications about resolved and acknowledged alarms are enabled.

  For details, see Step 5. Configure Notifications About Resolved and Acknowledged Alarms.

The following image shows an example of a notification about a resolved alarm.

Acknowledging Alarms

By acknowledging an alarm you let other administrators know that an issue is being investigated or resolved, so no attention is required from their side.

You can acknowledge alarms that have the *Error* or *Warning* status. When you acknowledge an alarm, its status is changed to *Acknowledged*, and no response actions are performed on it. Additionally, Veeam ONE notifies users who monitor the affected object that the alarm is acknowledged.

Acknowledging Individual Alarms

To acknowledge individual alarms:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the inventory pane, select the necessary object.

4. In the information pane, open the **Alarms** tab.

5. In the list of alarms, select one or more alarms and do either of the following:

   o Right-click the selection and choose **Acknowledge**.

   o In the **Actions** pane, click **Acknowledge**.

   Press and hold the `[CTRL]` or `[SHIFT]` key to select multiple alarms.

6. In the **Acknowledge Alarm** window, specify a comment or a reason for acknowledging the alarms.

   The message you specify will appear in the **Comment** field of the alarm history details, and in the email notification on acknowledged alarms. For details, see Viewing Alarm History and Notifications on Acknowledged Alarms.

7. Click **OK**.

Acknowledging Multiple Alarms

To acknowledge all displayed alarms at once:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the inventory pane, select the necessary object.

4. In the information pane, open the **Alarms** tab.

5. Use the filters and the search field at the top of the list to display the alarms that you want to acknowledge.

   For details on alarm filters, see Searching for Alarms.

6. Do either of the following:

   o Right-click anywhere in the list of alarms and choose **Acknowledge all alarms** from the shortcut menu.

   o In the **Actions** pane, click **Acknowledge All**.

7. In the **Acknowledge All Alarms** window, specify a reason for changing the alarm status, or add any other information.

   The message you specify will appear in the **Comment** field of the alarm history details, and in the email notification on acknowledged alarms. For details, see Viewing Alarm History and Notifications on Acknowledged Alarms.

8. Click **OK**.

Notifications on Acknowledged Alarms

When one or more alarms are acknowledged, Veeam ONE sends a notification to users who monitor the affected object. The notification includes information about the number of alarms acknowledged, time when the alarms were acknowledged and reason, as well as the list of acknowledged alarms.

To receive a notification about acknowledged alarms, make sure that:

- You have configured SMTP Server settings.

  For details, see Step 1. Configure SMTP Server Settings.

- Your email address is included either in the default notification group, or in the list of notification recipients specified in the alarm action settings, and the notification level is set to *Any state*.

  For details, see Step 4. Configure Email Recipients.

- Notifications about resolved and acknowledged alarms are enabled.

  For details, see Step 5. Configure Notifications About Resolved and Acknowledged Alarms.

The following image shows an example of a notification about acknowledged alarms.

Approving Alarm Remediation Actions

Veeam ONE can run alarm remediation actions automatically or after manual approval.

Veeam ONE runs an alarm action automatically if the resolution type of the alarm remediation action is set to *Automatic*. If the alarm remediation action requires manual approval, you can approve such actions in Veeam ONE Client.

Approving Actions for Individual Alarms

To approve actions for individual alarms:

1. Open Veeam ONE Client.

    For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the inventory pane, select the necessary object.

4. In the information pane, open the **Alarms** tab.

5. At the top of the alarms list, click the **Show alarms with available Remediation Actions** icon.

6. In the list of alarms, select one or more alarms and do either of the following:

    o Right-click the selection and choose **Approve action** from the shortcut menu.

    o In the **Actions** pane, click **Approve Action**.

    Press and hold the `[CRTL]` or `[SHIFT]` key to select multiple alarms.

7. In the **Approve Action** window, specify a reason or a comment for approving the alarm actions.

    The message you specify will appear in the **Comment** field of the alarm history details, and in the email notification on acknowledged alarms. For details, see Viewing Alarm History and Notifications on Acknowledged Alarms.

8. Click **OK**.

Approving Actions for Multiple Alarms

To approve actions for all displayed alarms at once:

1. Open Veeam ONE Client.

    For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the inventory pane, select the necessary object.

4. In the information pane, open the **Alarms** tab.

5. Use the filters and the search field at the top of the list to display the alarms for which you want to approve actions.

    For details on alarm filters, see Searching for Alarms.

6. Do either of the following:

   o Right-click anywhere in the list of alarms and choose **Approve all actions** from the shortcut menu.

   o In the **Actions** pane, click **Approve All Actions**.

7. In the **Approve All Actions** window, specify a reason or a comment for approving the alarm actions.

   The message you specify will appear in the **Comment** field of the alarm history details, and in the email notification on acknowledged alarms. For details, see Viewing Alarm History and Notifications on Acknowledged Alarms.

8. Click **OK**.

Viewing Alarm History

Veeam ONE keeps the history of alarm status changes for every triggered alarm. You can track the number of times the alarm changed its status and view alarm history details: assigned status, time, rule that triggered the alarm or changed its state, and comments for resolved, remediated, or acknowledged alarms.

To view alarm history:

1. Open Veeam ONE Client.

    For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the information pane, open the **Alarms** tab.

4. Select the necessary alarm and do either of the following:

    o Click the **Repeat Count** link in the list of alarms.

    o Double-click the alarm in the list.

    o Right-click the alarm and select **Show History** from the shortcut menu.

    o In the **Actions** pane, click **Show History**.

Exporting Triggered Alarms

You can export information about triggered alarms to a CSV file. The file contains the following details for each exported alarm:

- Alarm status

- Alarm name

- Date and time when the alarm was triggered

- Name of the affected object

- Repeat count

To export one or more triggered alarms to a CSV file:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click the necessary view (*Veeam Backup & Replication*, *Veeam Backup for Microsoft 365*, *Virtual Infrastructure*, *VMware Cloud Director*, *Business View*).

3. In the inventory pane, select the necessary object.

4. In the information pane, open the **Alarms** tab.

5. Use the filters and the search field at the top of the list to display the alarms that you want to export.

   For details on alarm filters, see Searching for Alarms.

6. In the **Actions** pane on the right, click **Export Alarms**.

7. Save the CSV file with exported data.

8. Click **OK**.

The following image shows an example of alarm details exported to a CSV file.
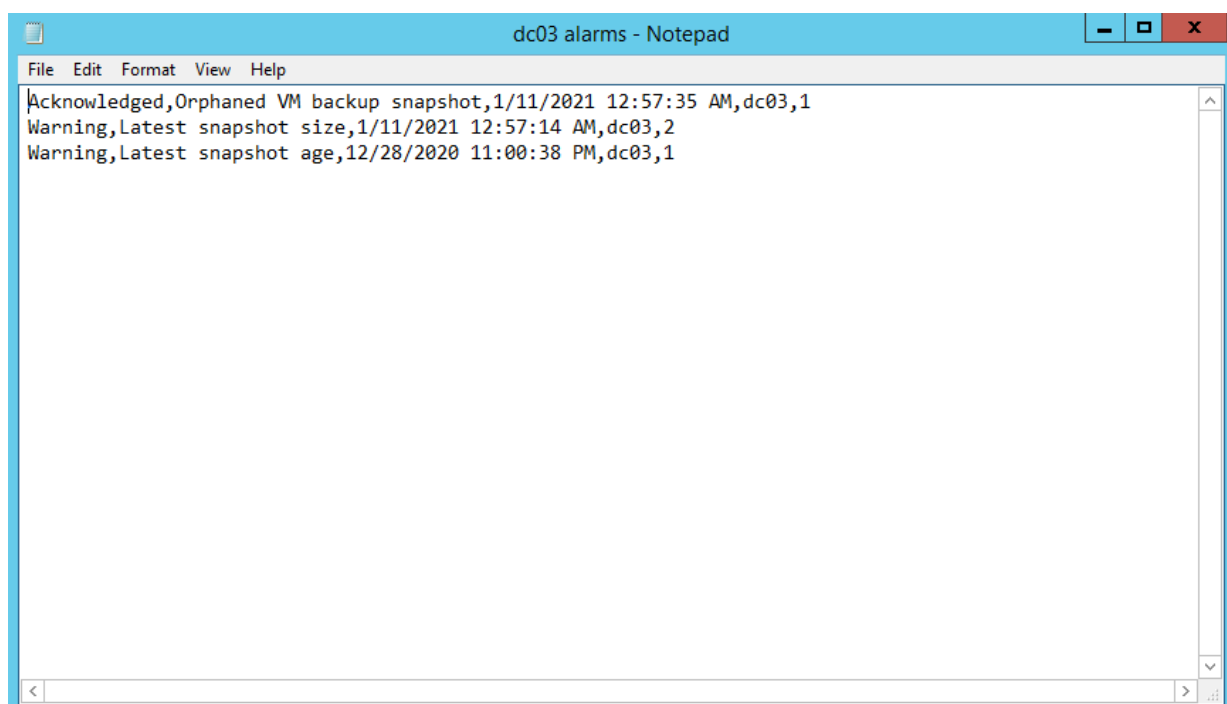
Working with Internal Alarms

In addition to alarms for monitoring the virtual and backup infrastructure, Veeam ONE includes a set of predefined alarms to monitor internal Veeam ONE problems — such as data collection, connection problems, or license issues. For the list and description of internal alarms, see Internal Alarms.

Viewing Internal Alarms

To view Veeam ONE internal alarms:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. In the **Configuration issues** pane, click the **Show details** link.

3. Click the object name to drill down to the list of alarms for the selected object.

Configuring Internal Alarms

You can configure internal alarms similarly to regular alarms:

1. Open Veeam ONE Client.

   For details, see Accessing Veeam ONE Client.

2. At the bottom of the inventory pane, click **Alarm Management**.

3. In the alarm management three, select the **Internal** node.

4. Select an alarm in the list and do either of the following:

   o Double click the alarm.

   o Right-click the alarm and choose **Edit** from the shortcut menu.

   o In the **Actions** pane, click **Edit**.

5. Change the necessary alarm settings.

   For details on working with alarm settings, see Creating Alarms.
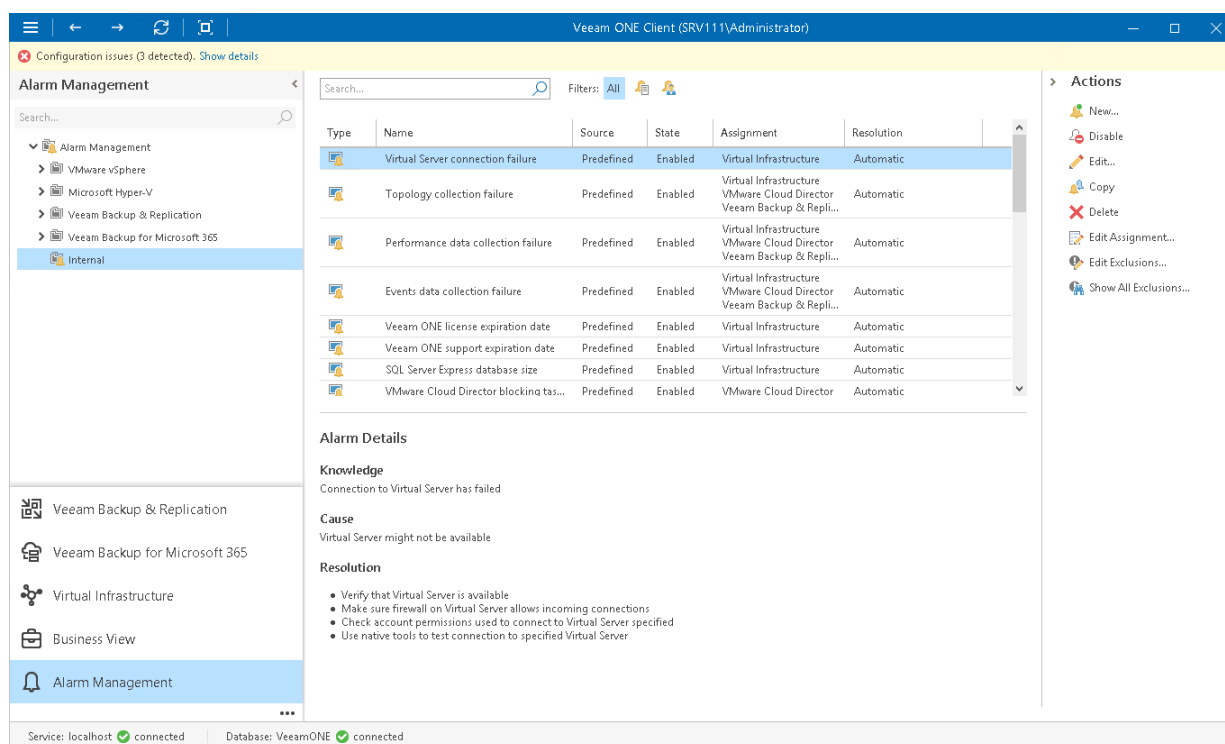
Predefined Alarms

This section lists predefined Veeam ONE alarms.

Veeam Backup & Replication Alarms

This section describes predefined alarms for Veeam Backup & Replication infrastructure components.

Enterprise Manager

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Veeam Backup Enterprise Manager connection failure	State does not equal *Connected*.	Error	Automatic	Veeam ONE failed to connect to Veeam Backup Enterprise Manager.

Veeam Backup & Replication Server

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Agent backup job state	State of an agent backup job equals *Warning*.	Warning	Automatic	One or more computers failed to back up successfully.
	State of an agent backup job equals *Failed*.	Error		
Agent backup policy session state	State of a backup policy session equals *Warning*.	Warning	Automatic	One or more computers failed to back up successfully.
	State of a backup policy session equals *Failed*.	Error		
Application backup policy state	State of a backup policy session equals *Warning*.	Warning	Automatic	One or more application databases failed to back up successfully.
	State of a backup policy session equals *Failed*.	Error		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Backup Copy Job exceeded data transfer window	Based on event VeeamBpCopyJobNetworkWindowExceededEvent.	Error	Manual	One or more backup copy jobs exceeded defined window, and data transfer between source and target backup repositories has been stopped.
Backup Copy job state	State of an backup copy job equals *Warning*.	Warning	Automatic	One or more objects could not be successfully copied from the backup repository.
	State of an backup copy job equals *Failed*.	Error		
Backup Copy RPO	Restore point copy is missing according to job schedule.	Error	Automatic	One or more backups was not successfully copied to the secondary repository within the defined RPO interval.
Job disabled	Job is disabled for more than 12 hours.	Warning	Automatic	Job stays in the disabled state for a longer time than configured in the alarm threshold.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Backup job failed to create storage snapshot	Based on event VeeamBpJobFailedToCreateStorageSnapshotEvent.	Warning	Manual	Integrated storage failed to create storage snapshot initiated by Veeam backup job.
Backup job state	State of a backup job equals *Warning*.	Warning	Automatic	Backup job reported either an error or a warning.
	State of a backup job equals *Failed*.	Error		
	State of a Nutanix backup job equals *Warning*.	Warning		
	State of a Nutanix backup job equals *Failed*.	Error		
CDP SLA Compliance	SLA decreases to 95% for 5 minutes	Warning	Automatic	SLA % of one or more workloads processed by CDP policy has dropped below threshold.
	SLA decreases to 75% for 5 minutes	Error		
Cloud backup policy session state	Status of a cloud backup policy session equals *Warning*.	Warning	Automatic	Policy finished with warning or error.
	Status of a cloud backup policy session equals *Error*.	Error		
File backup job state	State of a file backup job equals *Warning.*	Warning	Automatic	File backup job finished with warning or error.
	State of a file backup job equals *Failed.*	Error		
File copy job state	State of a file copy job equals *Warning.*	Warning	Manual	One or more files failed to be transferred to the destination folder.
	State of a file copy job equals *Failed.*	Error		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Job exceeded backup window	Based on event VeeamBpJobWindowExceededEvent.	Error	Manual	One or more jobs exceeded allowed backup window and has been terminated.
License expiration date	Based on event VeeamBackupServerLicenseExpiration.	Warning	Automatic	Veeam Backup & Replication license expired.
	Based on event VeeamBackupServerLicenseChanged.	Resolve		
	Based on event VeeamBackupServerLicenseExpirationResolve.	Resolve		
Maximum allowed job duration	Job duration is more than 480 minutes.	Error	Manual	Job has exceeded its maximum allowed execution time.
	Job duration is more than 120 minutes.	Warning		
Plug-in backup data collection failure	Plug-in backup data collection failed due to connection loss for more than 5 minutes.	Error	Automatic	Veeam ONE server failed to collect plug-in backup data provided by Veeam Backup & Replication.
Quick Migration job state	Based on event VeeamBpQMigrationSessionWarningEvent.	Warning	Automatic	One or more VMs failed to migrate to another host.
	Based on event VeeamBpQMigrationSessionErrorEvent.	Error		
Replication job state	State of a replication job equals *Warning.*	Warning	Automatic	One or more VMs failed to replicate successfully.
	State of a replication job equals *Failed.*	Error		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Restore activity	Based on event 290 Veeam MP.	Information	Automatic	Restore session initiated.
	Based on event 40290 Veeam MP.			
Support expiration date	Based on event VeeamBackupServerLicenseSupportExpiration.	Warning	Automatic	Veeam Backup & Replication prepaid support contract expired.
	Based on event VeeamBackupServerLicenseChanged.	Resolve		
	Based on event VeeamBackupServerLicenseSupportExpirationResolved.	Resolve		
SureBackup job state	State of a SureBackup job equals *Warning.*	Warning	Automatic	One or more VMs could not be successfully verified.
	State of a SureBackup job equals *Failed.*	Error		
Suspicious incremental backup size	One of 3 last job increment sizes is above 150% of configured threshold.	Warning	Automatic	The size of the recently created incremental restore point is significantly different from the previously created ones. For Oracle RMAN backup jobs, Veeam ONE analyzes only the differential level 1 backups.
	One of 3 last job increment sizes is above 200% of configured threshold.	Error		
	One of 3 last job increment sizes is below 80% of configured threshold.	Warning		
	One of 3 last job increment sizes is below 70% of configured threshold.	Error		
	Status of the file to tape backup job equals *Warning.*	Warning	Manual	

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Tape job state	Status of the file to tape backup job equals *Failed*.	Error		One or more VMs or files failed to be transferred to the tape device.
	Status of the backup to tape job equals *Warning*.	Warning		
	Status of the backup to tape job equals *Failed*.	Error		
Database log backup job state	Microsoft SQL server log backup job completed with warning	Warning	Automatic	Database transaction logs have not been backed up successfully.
	Microsoft SQL server log backup job failed	Error		
	Oracle Database log backup job completed with warning	Warning		
	Oracle Database log backup job failed	Error		
	PostgreSQL log backup job completed with warning	Warning		
	PostgreSQL log backup job failed	Error		
	Enterprise application log backup job completed with warning	Warning		
	Enterprise application log backup job failed	Error		
Unusual job duration	Job duration is above 150% of average time interval	Warning	Automatic	Job duration is above usual values among the set of job sessions.
	Job duration is above 200% of average time interval	Error		
Veeam Backup & Replication Server connection failure	State does not equal *Connected*.	Error	Automatic	Connection to Veeam Backup & Replication server failed.
Veeam Broker	Based on event VeeamBackupServerBrokerServiceDownEvent.	Warning	Automatic	Veeam Broker

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Service state	Based on event VeeamBackupServerBrokerServiceDownEvent.	Resolve		Service that interacts with virtual infrastructure to collect and cache its topology is not started and not working properly.
	Based on event VeeamBackupServerBrokerServiceDownEvent.	Resolve		

Repository

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Backup repository connection failure	State equals *Not accessible* for more than 5 minutes.	Error	Automatic	Veeam Backup & Replication server lost connection to the Microsoft Windows backup repository.
	State equals *Partially accessible* for more than 5 minutes.	Warning		
Backup repository free space	Free space is below 5%.	Error	Automatic	Backup repository is low on free space.
	Free space is below 10%.	Warning		
Backup repository version is out-of-date	Component version mismatch.	Warning	Automatic	Veeam backup repository version does not match the version of Veeam Backup & Replication server.
Backup repository ReFS data integrity issue	Based on event 133 ReFS	Warning	Manual	ReFS-formatted volume of a backup repository experienced a data integrity issue.
	Based on event 135 ReFS			
	Based on event 136 ReFS			

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Immutability state	Immutability is disabled.	Warning	Automatic	The immutability setting is turned off on one or several backup repositories or scale-out backup repository extents.
Immutability change tracking	Based on event VeeamImmutabilityIntervalDaysDecreased.	Warning	Manual	The configured immutability period has been changed on one or several backup repositories or scale-out backup repository extents.
	Based on event VeeamImmutabilityIntervalDaysIncreased.			
	Based on event VeeamImmutabilityIntervalDaysEnabled.			
Scale-out backup repository data transfer session state	Scale-out backup repository data transfer session completed with warning	Warning	Automatic	Scale-out backup repository offload, download, archiving or retrieval data transfer session finished with warning or failed.
	Scale-out backup repository data transfer session failed	Error		

Proxy

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Backup proxy connection failure	State does not equal *Accessible* for more than 5 minutes.	Error	Automatic	Veeam Backup & Replication server lost connection to the backup proxy server.
Backup proxy version is out-of-date	Component version mismatch.	Warning	Automatic	Veeam backup proxy version does not match the version of Veeam Backup & Replication server.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
CDP proxy cache usage	CDP cache usage is above 50%	Warning	Automatic	CDP proxy cache usage has reached the configured threshold.
	CDP cache usage is above 75%	Error		

WAN Accelerator

Alarm Name	Event/Condition	Severity	Resolve Action	Description
WAN accelerator connection state	State does not equal *Accessible* for more than 5 minutes.	Error	Automatic	Veeam Backup & Replication server lost connection to the WAN accelerator
WAN accelerator version is out-of-date	Component version mismatch.	Warning	Automatic	Veeam WAN accelerator version does not match the version of Veeam Backup & Replication server.

Tape Server

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Tape server connection state	State does not equal *Accessible* for more than 5 minutes.	Error	Automatic	Veeam Backup & Replication server lost connection to the tape server.
Tape server version is out-of-date	Component version mismatch.	Warning	Automatic	Veeam tape server version does not match the version of Veeam Backup & Replication server.

Cloud Repository

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Cloud repository free space	Free space is below 10%.	Warning	Automatic	Cloud repository is low on available free space.
	Free space is below 5%.	Error		
Cloud repository lease expiration date	14 days to lease expiration.	Warning	Automatic	Cloud repository lease time is about to expire.
	0 days to lease expiration.	Error		
VM backups in cloud repository	Number of stored VMs is above the specified threshold.	Warning	Automatic	Number of VMs stored in the cloud repository is above the defined threshold.

Cloud Gateway

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Cloud gateway connection state	State does not equal *Accessible* for more than 5 minutes.	Error	Automatic	Veeam Backup & Replication server lost connection to the cloud gateway.
Cloud gateway version is out-of-date	Component version mismatch.	Warning	Automatic	Veeam cloud gateway version does not match the version of Veeam Backup & Replication server.

Computer

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Computer with no backup	No computer backups were created for more than 24 hours	Warning	Automatic	This computer has not been backed up within the configured RPO (Recovery Point Objective) period.

Enterprise Application

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Application with no recent data backup sessions	No backup jobs protecting application database finished successfully or with warnings for more than 24 hours	Warning	Automatic	One or several databases on an application server or application cluster are not protected with a backup job that finished successfully or with warnings within the configured RPO (Recovery Point Objective) period.

Intelligent Diagnostics

List of intelligent diagnostics alarms depends on the set of installed signatures. For details, see Veeam Intelligent Diagnostics.

Veeam Backup for Microsoft 365 Alarms

This section describes predefined alarms for Veeam Backup for Microsoft 365 infrastructure components.

Veeam Backup for Microsoft 365 Server

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Backup copy job state (Veeam Backup for Microsoft 365)	State of an backup copy job equals *Warning*.	Warning	Automatic	Backup copy job reported either an error or a warning.
	State of an backup copy job equals *Failed*.	Error		
Backup job state (Veeam Backup for Microsoft 365)	State of an backup job equals *Warning*.	Warning	Automatic	Backup job reported either an error or a warning.
	State of an backup job equals *Failed*.	Error		
Job disabled (Veeam Backup for Microsoft 365)	Job is disabled for more than 12 hours.	Warning	Automatic	Job stays in the disabled state for a longer time than configured in the alarm threshold.
License exceeded (Veeam Backup for Microsoft 365)	Based on event VeeamVbmServerLicenseCapacityDepleting.	Warning	Automatic	Number of protected user accounts exceeds the license limit.
	Based on event VeeamVbmServerLicenseCapacityDepletingResolved.	Resolve		
	Based on event VeeamMonitorServicesStartedEvent.	Resolve		
License expiration date	Based on event VeeamVbmServerLicenseExpiration.	Warning	Automatic	Veeam Backup for Microsoft 365 license expired.
	Based on event VeeamVbmServerLicenseExpirationResolved.	Resolve		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
	Based on event VeeamMonitorServicesStartedEvent.	Resolve		
Organization with no backup	Microsoft 365 organization has no restore points created within the last 24 hours.	Warning	Automatic	Microsoft 365 organization was not backed up during the configured RPO period.
Unusual job duration (Veeam Backup for Microsoft 365)	Job duration is above 150% of average time interval	Warning	Automatic	Job duration is above usual values among the set of job sessions.
	Job duration is above 200% of average time interval	Error		
Veeam Backup for Microsoft 365 server connection failure	State does not equal *Connected* for more than 5 minutes.	Error	Automatic	Connection to Veeam Backup for Microsoft 365 server failed.
Veeam Backup for Microsoft 365 service state	Veeam Backup for Microsoft 365 service status does not equal *Running* for more than 5 minutes.	Error	Automatic	Veeam Backup for Microsoft 365 service is not running on the Veeam Backup for Microsoft 365 server.

Backup Proxy

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Backup proxy connection failure (Veeam Backup for Microsoft 365)	Backup proxy status does not equal *Online* for more than 5 minutes.	Error	Automatic	Veeam Backup for Microsoft 365 server lost connection to the proxy server.

Backup Repository

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Backup repository free space (Veeam Backup for Microsoft 365)	Free space is below 5%.	Error	Automatic	Backup repository is low on free space.
	Free space is below 10%.	Warning		

VMware vSphere Alarms

This section describes predefined alarms for VMware vSphere infrastructure components.

vCenter Server

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Bad vCenter Server username logon attempt	Based on event BadUsernameSessionEvent.	Error	Manual	This event records a failed user logon. The combination of username, password, and permissions is the mechanism by which vCenter Server authenticate a user for access and authorize the user to perform activities.
Insufficient user access permissions	Based on event NoAccessUserEvent.	Error	Manual	This event records a failed user logon due to insufficient access permission.
Invalid license edition	Based on event InvalidEditionEvent.	Error	Manual	This event records if the license edition is set to an invalid value.
License expired	Based on event LicenseExpiredEvent.	Error	Manual	This event records the expiration of a license.
License file restricted	Based on event LicenseRestrictedEvent.	Error	Manual	This event records if the required licenses could not be reserved because of a restriction in the option file.
License is not compliant	Based on event LicenseNonComplianceEvent.	Error	Manual	This event records that the inventory is not license compliant.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Maximum host connections reached	Based on event HostInventoryFullEvent.	Error	Manual	This event records if the inventory of hosts has reached capacity.
No license reservation	Based on event NoLicenseEvent.	Error	Manual	These are events reported by License Manager. A NoLicenseEvent is reported if the required licenses could not be reserved. Each feature that is not fully licensed is reported.
Non VI workload detected	Based on event NonVIWorkloadDetectedOnDatastoreEvent.	Error	Manual	A potential misconfiguration or I/O performance issue caused by a non-ESX workload has been detected. This alarm is triggered when Storage I/O Control (SIOC) detects that a workload that is not managed by SIOC is contributing to I/O congestion on a datastore that is managed by SIOC.
vCenter Server agent uninstall failure	Based on event VcAgentUninstallFailedEvent.	Error	Manual	This event records when the vCenter Server agent on a host failed to uninstall.
vCenter Server agent upgrade failure	Based on event VcAgentUpgradeFailedEvent.	Error	Manual	This event records when the vCenter Server agent on a host failed to upgrade.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
vCenter Server license expired	Based on event ServerLicenseExpiredEvent.	Error	Manual	This event records an expired vCenter Server license.

Cluster

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Admission control disabled	Based on event DasAdmissionControlDisabledEvent.	Information	Automatic	This event records when admission control checks have been disabled in a HA cluster.
Admission control enabled	Based on event DasAdmissionControlEnabledEvent.	Information	Automatic	This event records when admission control checks have been enabled in a HA cluster.
All hosts in cluster isolated	Based on event DasClusterIsolatedEvent.	Error	Manual	This event records that all hosts have been isolated from the network in a HA cluster.
DRS invocation failure	Based on event DrsInvocationFailedEvent.	Error	Manual	This event records DRS invocation failure. DRS invocation not completed.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
HA disabled for cluster	Based on event DasDisabledEvent.	Information	Automatic	This event records when a cluster has been disabled for HA.
HA enabled for cluster	Based on event DasEnabledEvent.	Information	Automatic	This event records when a cluster has been enabled for HA.
Host cluster capacity overcommitted	Based on event ClusterOvercommittedEvent.	Error	Manual	This event records when a cluster's host capacity cannot satisfy resource configuration constraints.
vSphere cluster warning	Based on event com.vmware.vc.HA.ClusterContainsIncompatibleHosts. Based on event com.vmware.vc.HA.DasFailoverHostIsolatedEvent. Based on event com.vmware.vc.HA.DasFailoverHostPartitionedEvent. Based on event com.vmware.vc.HA.DasFailoverHostUnreachableEvent. Based on event com.vmware.vc.HA.DasHostIsolatedEvent.	Warning	Manual	One of the hosts in an HA cluster has been isolated.

Host

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Bad Host username logon attempt	Based on event BadUsernameSessionEvent.	Warning	Manual	This event records a failed user logon. The combination of username, password, and permissions is the mechanism by which hosts authenticate a user for access and authorize the user to perform activities.
Connection to iSCSI storage target failure	Based on event esx.problem.storage.iscsi.discovery.connect.error.	Error	Manual	The iSCSI initiator is unable to establish a connection to the target.
	Based on event esx.problem.storage.iscsi.discovery.login.error.			
	Based on event esx.problem.storage.iscsi.target.connect.error.			
	Based on event esx.problem.storage.iscsi.target.login.error.			
DPM failed to bring host out of standby mode	Based on event DrsExitStandbyModeFailedEvent.	Error	Automatic	This event records that Distributed Power Management tried to bring a host out of standby mode, but failed. Standby Mode powers off a host and allows it to be powered back on again through the Wake-on-LAN protocol. It can be triggered either manually or automatically by vCenter Server.
	Based on event DrsExitedStandbyMode.	Resolve		
	Based on event ExitedStandbyMode.	Resolve		
DRS host standby mode entrance	Based on event DrsEnteredStandbyModeEvent.	Information	Automatic	This event records that the host has successfully entered standby mode initiated by Distributed Power Management. A host in this mode has no running virtual machines and no provisioning operations are occurring.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
DRS host standby mode exit	Based on event DrsExitedStandbyModeEvent.	Information	Automatic	This event records that Distributed Power Management brings this host out from standby mode.
DRS synchronization failure	Based on event DrsResourceConfigureFailedEvent.	Error	Manual	This event records when resource configuration specification synchronization fails on a host.
DVS host configuration out of sync	Based on event OutOfSyncDvsHost.	Warning	Manual	The list of hosts that have the DVS configuration on the host diverged from that of the vCenter Server.
ESXi host network uplink failure	Based on event esx.problem.net.lacp.uplink.fail.duplex. Based on event esx.problem.net.lacp.uplink.fail.speed. Based on event esx.problem.net.lacp.uplink.inactive.	Error	Manual	Link Aggregation Control Protocol (LACP) is included in IEEE specification as a method to control the bundling of several physical ports together to form a single logical channel. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that also implements LACP).
ESXi host CPU hardware error	Based on event esx.problem.cpu.amd.mce.dram.disabled. Based on event esx.problem.cpu.intel.ioapic.listing.error. Based on event esx.problem.cpu.mce.invalid. Based on event esx.problem.cpu.smp.ht.invalid. Based on event esx.problem.cpu.smp.ht.numpcpus.max.	Error	Manual	ESXi host has experienced a CPU hardware error.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
ESXi host network error	Based on event esx.problem.dhclient.lease.none.	Error	Manual	DHCP client lease issue has been detected.
ESXi host network uplink problems	Based on event esx.problem.net.lacp.uplink.blocked.	Warning	Manual	Link Aggregation Control Protocol (LACP) is included in IEEE specification as a method to control the bundling of several physical ports together to form a single logical channel. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that also implements LACP).
	Based on event esx.problem.net.lacp.uplink.disconnected.			
ESXi host network warning	Based on event esx.problem.dhclient.lease.offered.error.	Warning	Manual	DHCP client lease issue has been detected.
	Based on event esx.problem.dhclient.lease.persistent.none.			
ESXi host storage error	Based on event esx.problem.scsi.device.state.permanentloss.withreservationheld.	Error	Manual	Storage device becomes permanently lost while SCSI reservation is held by ESXi.
ESXi host storage failure	Based on event esx.problem.visorfs.failure.	Error	Manual	An operation on the root file system has failed.
ESXi host storage warning	Based on event esx.problem.visorfs.inodetable.full.	Warning	Manual	One of the host's ramdisks reached the limit for the number of files it can contain.
	Based on event esx.problem.visorfs.ramdisk.full.	Warning		
	Average memory usage is for 15 minutes is above 80%.	Warning	Automatic	This host is low on available memory.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Host available memory	Average memory usage is for 15 minutes is above 90%.	Error		
Host connection failure	Host state equals *Disconnected* for 5 minutes and more.	Warning	Automatic	This alarm monitors the VMware vCenter Server API for events indicating that a host is disconnected.
	Host state equals *Not responding* for 5 minutes and more.			
Host connectivity failure	Based on event vprob.net.connectivity.lost.	Error	Automatic	This event indicates that one or more portgroups in the host have lost connectivity to the network, resulting in unavailability of all physical connections to the network from this switch.
	Based on event esx.problem.net.connectivity.lost.			
	Based on event esx.clear.net.connectivity.restored.	Resolve		
Host CPU ready	Average CPU Ready for 15 minutes is above 15%.	Warning	Automatic	This Host has exceeded the threshold for CPU Ready Percent.
	Average CPU Ready for 15 minutes is above 25%.	Error		
Host CPU usage	Average CPU usage for 15 minutes is above 75%.	Warning	Automatic	This host has exceeded the threshold for CPU usage.
	Average CPU usage for 15 minutes is above 95%.	Error		
Host disk bus resets	Average datastore bus resets for 15 minutes is above 2.	Warning	Automatic	This host disk (vmhba) has logged one or more SCSI bus resets.
	Average datastore bus resets for 15 minutes is above 4.	Error		
	Average datastore command aborts for 15 minutes is above 2.	Warning	Automatic	This host disk (vmhba) has logged one or more SCSI aborts.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Host disk SCSI aborts	Average datastore command aborts for 15 minutes is above 4.	Error		
Host failed to exit standby mode	Based on event ExitStandbyModeFailedEvent.	Error	Automatic	This event records that the host failed to exit standby mode. Standby Mode powers off a host and allows it to be powered back on again through the Wake-on-LAN protocol. It can be triggered either manually or automatically by vCenter Server.
	Based on event ExitedStandbyMode.	Resolve		
Host HA agent failure	Based on event com.vmware.vc.HA.HostAgentErrorEvent.	Error	Manual	Usually, such triggers indicate that a host has actually failed, but failure reports can sometimes be incorrect. A failed host reduces the available capacity in the cluster and, in the case of an incorrect report, prevents vSphere HA from protecting the virtual machines running on the host.
Host HA disabled	Based on event HostDasDisabledEvent.	Information	Automatic	This event records when HA has been disabled on a host.
Host HA enabled	Based on event HostDasEnabledEvent.	Information	Automatic	This event records when the HA (high-availability) agent has been enabled on a host.
Host hardware status	Hardware sensor equals *Warning.*	Warning	Automatic	One of the hosts' hardware sensors has changed its status.
	Hardware sensor equals *Alert.*	Error		
	Hardware sensor equals *Unknown.*	Warning		
Host IP inconsistent	Based on event HostIpInconsistentEvent.	Warning	Manual	This event records that the IP address resolution returned different addresses on the host.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Host IP to short name failed	Based on event HostIpToShortNameFailedEvent.	Warning	Manual	This event records that the host's IP address could not be resolved to a short name.
Host Isolation IP not available	Based on event HostIsolationIpPingFailedEvent.	Warning	Manual	This event records that the isolation address could not be pinged. The default isolation address is the service console's default gateway.
Host license expired	Based on event HostLicenseExpiredEvent.	Error	Manual	This event records an expired host license.
Host memory pressure	Average memory pressure for 15 minutes is above 150%.	Warning	Automatic	This host has exceeded the threshold for memory pressure.
	Average memory pressure for 15 minutes is above 250%.	Error		
Host NIC link status	Host NIC link status equals *Down.*	Error	Automatic	Physical NIC linkstate is down.
Host not compliant	Based on event HostNonCompliantEvent.	Warning	Manual	This event records that host went out of compliance.
Host operation cancelled	Based on event CanceledHostOperationEvent.	Information	Automatic	An operation performed on the host was canceled.
Host operation timed out	Based on event TimedOutHostOperationEvent.	Warning	Manual	This event indicates that an operation performed on the host timed out.
Host primary agent not in short name	Based on event HostPrimaryAgentNotShortNameEvent.	Warning	Manual	This event records that the primary agent specified is not a short name.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Host reconnection failed	Based on event HostConnectedEvent.	Resolve	Automatic	This event records a failed attempt to re-establish a host connection.
	Based on event HostReconnectionFailedEvent.	Error		
Host redundancy failure	Based on event vprob.net.redundancy.lost.	Warning	Automatic	The event indicates that one or more portgroups in the host has lost a redundant uplink to the physical network. Portgroups are still connected. However this may be the last redundant uplink. Check the event description and context to confirm the status.
	Based on event vprob.net.redundancy.degraded.			
	Based on event esx.problem.net.redundancy.lost.			
	Based on event esx.problem.net.redundancy.degraded.			
	Based on event esx.clear.net.redundancy.restored.	Resolve		
Host short name inconsistent	Based on event HostShortNameInconsistentEvent.	Warning	Manual	This event records that host name resolution returned different names on the host.
Host short name IP resolve failed	Based on event HostShortNameToIpFailedEvent.	Warning	Manual	This event records that the host's short name could not be resolved to an IP address.
Host swap memory	Average memory swap used for 15 minutes is above 64 MB.	Warning	Automatic	This host is swapping too much memory.
	Average memory swap used for 15 minutes is above 128 MB.	Error		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Host synchronization failed	Based on event HostSyncFailedEvent.	Warning	Manual	This event records a failure to sync up with the vCenter Server agent on the host.
Host upgrade connection failure	Based on event HostUpgradeFailedEvent.	Error	Manual	This event records a failure to connect to a host due to an installation or upgrade issue.
Incorrect host information	Based on event IncorrectHostInformationEvent.	Warning	Manual	This event records if the host did not provide the information needed to acquire the correct set of licenses.
iSCSI target storage connection failure	Based on event esx.problem.storage.iscsi.target.connected.error.	Error	Manual	The iSCSI initiator is unable to establish a connection to the target.
iSCSI targets are permanently removed from ESXi	Based on event esx.problem.storage.iscsi.target.permanently.lost.	Error	Manual	The esx.problem.storage.iscsi.target.permanently.removed message is received when an iSCSI target is no longer presented to ESXi.
Isolation addresses is missing	Based on event com.vmware.vc.HA.HostHasNoIsolationAddrsDefined.	Warning	Manual	ESXi host is missing isolation addresses for isolation detection.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Network rollback detected	Based on event NetworkRollbackEvent.	Error	Manual	In vSphere 5.1, rollback is enabled by default. However, you can enable or disable rollbacks at the vCenter Server level. Several networking events can trigger a rollback. The events are grouped into these categories: • Host networking rollbacks (virtual switches or network system) • Distributed switch rollbacks
No host network for HA available	Based on event HostNoAvailableNetworksEvent.	Warning	Manual	This event records the fact that a host does not have any available networks for HA communication.
Non VI workload detected on host	Based on event EsxProblemIormNonViWorkload.	Error	Manual	A potential misconfiguration or I/O performance issue caused by a non-ESX workload has been detected. This alarm is triggered when Storage I/O Control (SIOC) detects that a workload that is not managed by SIOC is contributing to I/O congestion on a datastore that is managed by SIOC.
SCSI unsupported plugin warning	Based on event esx.problem.scsi.unsupported.plugin.type.	Warning	Manual	An invalid storage module attempted to configure a SCSI device.
Storage connection failure	Based on event vprob.storage.connectivity.lost.	Error	Automatic	The event indicates a loss in connectivity to the specified storage device. The path indicated is the last path that went down.
	Based on event esx.problem.storage.connectivity.lost.			
	Based on event esx.clear.storage.connectivity.restored.	Resolve		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Storage connection redundancy failure	Based on event vprob.storage.redundancy.lost.	Warning	Automatic	A host has lost a path to access the specified storage and the path to storage is either degraded, or no longer redundant. Check the event description and context to confirm the status.
	Based on event vprob.storage.redundancy.degraded.			
	Based on event esx.problem.storage.redundancy.degraded.			
	Based on event esx.problem.storage.redundancy.lost.			
	Based on event esx.clear.storage.redundancy.restored.	Resolve		
Teaming mismatch error	Based on event TeamingMisMatchEvent.	Error	Manual	The teaming configuration of the uplink ports in the DVS does not match physical switch configuration.
Uplink port MTU error	Based on event UplinkPortMtuNotSupportEvent.	Error	Manual	MTU health check status of an uplink port is changed.
Uplink port VLAN error	Based on event UplinkPortVlanUntrunkedEvent.	Error	Manual	Vlans health check status of an uplink port is changed.
vCenter Server lost connection to host	Based on event HostConnectionLostEvent.	Error	Automatic	vCenter Server has lost connection to this host.
	Based on event HostCnxFailed.			
	Based on event HostConnectedEvent.	Resolve		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
vMotion license expired	Based on event VMotionLicenseExpiredEvent.	Error	Manual	This event records an expired vMotion license.
vSphere Distributed Switch MTU mismatch	Based on event MtuMismatchEvent.	Error	Manual	A larger MTU (maximum transmission unit) bring greater efficiency because each packet carries more user data while protocol overheads; the resulting higher efficiency means a slight improvement in bulk protocol throughput. A larger MTU also means processing of fewer packets for the same amount of data. However, this gain is not without some downside. Large packets can occupy a slow link for some time, causing greater delays to following packets and increasing lag and minimum latency.

Virtual Machine

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Customization unknown failure	Based on event CustomizationUnknownFailure.	Warning	Manual	The customization sequence failed unexpectedly in the guest.
Fault Tolerance VM terminated	Based on event VmFaultToleranceVmTerminatedEvent.	Warning	Manual	This event records a secondary or primary VM is terminated.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
FT VM Failover	Based on event VmPrimaryFailoverEvent.	Error	Manual	This event records a fault tolerance failover.
Guest customization failure	Based on event CustomizationFailed.	Warning	Manual	The customizatio n sequence in the guest failed. Cannot complete customizatio n of VM.
Guest disk space	Guest disk free space space is below 10%.	Warning	Automat ic	Guest OS volume is low on available guest disk space.
	Guest disk free space space is below 5%.	Error		
HA agent update failed	Based on event VmDasUpdateErrorEvent.	Error	Manual	The event records an error occurred when updating the HA agents with the current state of the VM.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Heartbeat is missing for VM	Heartbeat not detected for 15 minutes.	Error	Automatic	The heartbeat is the communication to the VMware tools heartbeat running inside the VM. Heartbeat can only be monitored when the VMware tools are installed in a VM. The heartbeat is what vCenter Server uses to determine the general health and availability of a running VM.
High balloon memory utilization	Average memory balloon percent for 15 minutes is above 10%.	Warning	Automatic	There is high utilization of the VMware Tools memory controller, also known as the 'balloon driver', within this VM.
	Average memory balloon percent for 15 minutes is above 50%.	Error		
High memory usage	Average memory usage for 15 minutes is above 90%.	Warning	Automatic	There is high utilization of

Alarm Name	Event/Condition	Severity	Resolve Action	Description
	Average memory usage for 15 minutes is above 95%.	Error		memory within this Virtual Machine. The memory active metric is the current percentage of memory active vs. memory maximum for this VM.
Latest snapshot age	VM snapshot age is 48 hour or more.	Warning	Automatic	The age of the latest snapshot for this VM has exceeded the configured threshold.
Latest snapshot size	VM snapshot size is above 10%.	Warning	Automatic	The size of the latest snapshot file for this VM has exceeded the configured threshold.
	VM snapshot size is above 20%.	Error		
Linux customization identity failure	Based on event CustomizationLinuxIdentityFailed.	Warning	Manual	Failed to set Linux identity.
Network customization setup failure	Based on event CustomizationNetworkSetupFailed.	Warning	Manual	Network setup failed in the guest during customization.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
No compatible host for Secondary VM	Based on event VmNoCompatibleHostForSecondaryEvent.	Warning	Manual	This event records that no compatible host was found to place a secondary VM. A default alarm will be triggered upon this event, which by default, triggers a SNMP trap.
No host for a virtual machine available	Based on event VmOrphanedEvent.	Warning	Manual	This event records a VM for which no host is responsible.
No maintenance mode DRS recommendation for VM	Based on event NoMaintenanceModeDrsRecommendationForVM.	Warning	Manual	This event records that DRS did not recommend a migration for a powered on VM, even though its host is going into maintenance mode.
No network access for VM migration	Based on event VmNoNetworkAccessEvent.	Warning	Manual	This event records a migration failure when the destination host is not on the same network as the source host.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Not enough resources for failover	Based on event NotEnoughResourcesToStartVmEvent.	Warning	Manual	This event records when the HA does not find sufficient resources to failover a VM.
Orphaned VM backup snapshot	Orphaned VM backup snapshot age is 60 minutes or more.	Error	Automat ic	This VM is running on the snapshot left by backup or replication job.
Possible ransomware activity	Average CPU Usage is above 70% and Datastore Write Rate is above 40 MB/s or Network Transmit Rate is above 40 MB/s for 5 minutes.	Warning	Automat ic	Veeam ONE detected suspicious activity on this VM.
	Average CPU Usage is above 80% and Datastore Write Rate is above 60 MB/s or Network Transmit Rate is above 60 MB/s for 5 minutes.	Error		
Secondary VM config update failed	Based on event VmFailedUpdatingSecondaryConfig.	Warning	Manual	This event is recorded after a failover of the new primary VM failed to update the config of the secondary VM.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Secondary VM failed to start	Based on event VmFailedStartingSecondaryEvent.	Warning	Manual	The Secondary VM cannot be powered on as there are no compatible hosts that can accommodate it.
Secondary VM start timeout	Based on event VmTimedoutStartingSecondaryEvent.	Warning	Manual	This event records timeout when starting a secondary VM.
Sysprep customization failure	Based on event CustomizationSysprepFailed.	Warning	Manual	Sysprep failed to run in the guest during customization. This can be caused by the fact that the wrong sysprep was used for the guest or errors in the sysprep file.
Too many snapshots on the VM	Number of VM snapshots is 3 or more.	Warning	Automatic	An excessive number of snapshots in a chain has been detected on the VM which may lead to decreased virtual machine and host performance.
	Number of VM snapshots is 5 or more.	Error		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Virtual disk creation failed	Based on event VmDiskFailedEvent.	Error	Manual	This event records a failure to create a virtual disk in a VM.
VM clone operation failure	Based on event VmCloneFailedEvent.	Error	Manual	This event records a failure to clone a VM.
VM configuration file missing	Based on event VmConfigMissingEvent.	Warning	Manual	This event records if the configuration file (VMX file) for a VM cannot be found.
VM connection failure	Based on event VmDisconnectedEvent.	Error	Automatic	This VM is 'Disconnected' in vCenter Server.
	Based on event VmConnectedEvent.	Resolve		
VM consolidation needed status	Based on event com.vmware.vc.VmDiskConsolidationNeeded.	Error	Automatic	When initiating Delete or DeleteAll operations on snapshots, the snapshot
	Based on event com.vmware.vc.VmDiskConsolidationNoLongerNeeded.	Resolve		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
	Based on event com.vmware.vc.VmDiskConsolidatedEvent.	Resolve		details are deleted from Snapshot Manager, then the snapshot files are consolidated and merged to another snapshot file or to the virtual machine parent disk. If the consolidation fails, there were no snapshots shown in the Snapshot Manager, but the snapshot files were still being used on the datastore. This can cause the datastore to run out of space.
VM CPU ready	Average CPU ready all cores metric for 15 minutes is above 10%.	Warning	Automatic	This VM has exceeded the threshold for CPU Ready Percent.
	Average CPU ready all cores metric for 15 minutes is above 20%.	Error		
VM CPU usage	Average CPU usage for 15 minutes is above 75%.	Warning	Automatic	This VM has exceeded the threshold for CPU usage.
	Average CPU usage for 15 minutes is above 90%.	Error		
VM disk consolidation failure	Based on event com.vmware.vc.VmDiskFailedToConsolidateEvent.	Error	Automatic	There is an issue with the disk for

Alarm Name	Event/Condition	Severity	Resolve Action	Description
	Based on event com.vmware.vc.VmDiskConsolidatedEvent.	Resolve		this virtual machine.
VM disk SCSI connection failures	Average number of datastore command aborts for 15 minutes is above 2.	Warning	Automatic	This VMGuest disk connection (LUN) has logged one or more SCSI aborts.
	Average number of datastore command aborts for 15 minutes is above 6.	Error		
VM disk SCSI connection resets	Average number of datastore bus resets for 15 minutes is above 2.	Warning	Automatic	This VMGuest disk connection (LUN) has logged one or more SCSI bus resets.
	Average number of datastore bus resets for 15 minutes is above 6.	Error		
VM generic error	Based on event VmMessageErrorEvent.	Error	Manual	This is a generic event for error messages from a VM that do not fit into any other specific vCenter Server event.
VM generic warning	Based on event VmMessageWarningEvent.	Warning	Manual	This is a generic event for warning messages from a VM that did not fit into any other specific vCenter Server event.
VM guest reboot	Based on event VmGuestRebootEvent.	Information	Automatic	This is a VM guest reboot request event.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
VM guest shutdown	Based on event VmGuestShutdownEvent.	Information	Automatic	This is a VM guest shutdown request event.
VM HA error	Based on event com.vmware.vc.HA.FailedRestartAfterIsolationEvent.	Error	Manual	vSphere HA has failed to restart after a host isolation.
VM HA reset	Based on event VmDasBeingResetEvent.	Warning	Manual	This event records when a VM is reset by HA VM Health Monitoring on hosts that do not support the create screenshot APIi or if the create screenshot API fails.
VM HA reset failure	Based on event VmDasResetFailedEvent.	Warning	Manual	This event records when HA VM health monitoring fails to reset a VM after failure.
VM memory swap usage	Average memory swapped for 15 minutes is above 64 MB.	Warning	Automatic	This VM has exceeded the threshold for memory swapping to disk within the host.
	Average memory swapped for 15 minutes is above 128 MB.	Error		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
VM power status	State not equals *Running* for 5 minutes or more.	Error	Automatic	The power state of a VM indicates whether the VM is active and functional.
VM resetting	Based on event VmResettingEvent.	Information	Automatic	This event records a VM resetting.
VM restart on alternate host	Based on event VmRestartedOnAlternateHostEvent.	Information	Automatic	This event records that the VM was restarted on a host, since its original host had failed.
VM Screenshot HA reset	Based on event VmDasBeingResetWithScreenshotEvent.	Warning	Manual	This event records when a VM is reset by HA VM health monitoring on hosts that support the create screenshot API.
VM total disk latency	Average datastore highest latency for 15 minutes is above 50 milliseconds.	Warning	Automatic	Highest latency value across all disks used by the VM.
	Average datastore highest latency for 15 minutes is above 75 milliseconds.	Error		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
VM with no backups	No backup restore points for the past 24 hours.	Warning	Automatic	This VM has not been backed up within the defined RPO (Recovery Point Objective) interval.
VM with no replica	No replica restore points for the past 24 hours.	Warning	Automatic	This VM has not been replicated within the defined RPO (Recovery Point Objective) interval.
VM WWN conflict	Based on event VmWwnConflictEvent.	Error	Manual	This event records a conflict of VM WWNs (World Wide Name).
VMware VM tools state	VMware VM tools state changes equals *Unknown.*	Warning	Automatic	There is a problem with VMware Tools in this Virtual Machine.
	VMware VM tools state changes equals *Out-of-date.*	Warning		
	VMware VM tools state changes equals *Not installed.*	Error		
	VMware VM tools state changes equals *Not running.*	Error		

Datastore

Alarm Name	Event/Condition	Severity	Resolve Action	Description
	Free space is below 10%.	Warning	Automatic	

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Datastore free space	Free space is below 5%.	Error		Datastore is low on available free space.
Datastore is inaccessible	State not equals *Accessible* for 5 minutes or more.	Error	Automatic	The event indicates a loss in connectivity to the specified storage device. The path indicated is the last path that went down.
Datastore over-allocation	Datastore provisioning rate is above 400%.	Warning	Automatic	Datastore is over-allocated.
	Datastore provisioning rate is above 600%.	Error		
Datastore read latency	Maximum datastore read latency for 15 minutes is above 100 milliseconds.	Warning	Automatic	Datastore latency has exceeded the threshold of total read latency.
	Maximum datastore read latency for 15 minutes is above 250 milliseconds.	Error		
Datastore write latency	Maximum datastore write latency for 15 minutes is above 100 milliseconds.	Warning	Automatic	Datastore latency has exceeded the threshold of total write latency.
	Maximum datastore write latency for 15 minutes is above 250 milliseconds.	Error		
Locker misconfiguration	Based on event LockerMisconfiguredEvent.	Warning	Manual	Locker has not been configured properly. Datastore which is configured to back the locker does not exist.

Any Object

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Duplicate IP address detected	Based on event DuplicateIpDetectedEvent.	Warning	Manual	This event records that a duplicate IP address has been observed, with conflict between VM, and the vMotion or IP storage interface configured on the host.
Host cluster destroyed	Based on event ClusterDestroyedEvent.	Information	Automatic	This event records when a cluster is destroyed.
Host failure detected	Based on event DasHostFailedEvent.	Error	Manual	This event records when a host failure has been detected by HA.
Host isolation in HA cluster	Based on event DasHostIsolatedEvent.	Warning	Manual	This event records that a host has been isolated from the network in a HA cluster. Since an isolated host cannot be distinguished from a failed host except by the isolated host itself, this event is logged when the isolated host regains network connectivity.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
No host redundant management network available	Based on event HostNoRedundantManagementNetworkEvent.	Warning	Manual	This event records the fact that a host does not have a redundant management network. It is recommended that host management networks be configured with redundancy.
Primary host connection re-established	Based on event DasAgentFoundEvent.	Information	Automatic	This event records that vCenter Server has re-established contact with a primary host in this HA cluster.
Primary host unavailable	Based on event DasAgentUnavailableEvent.	Error	Automatic	This event records that vCenter Server cannot contact to any primary host in this HA cluster. vCenter Server has lost contact with all primary nodes with a connected state. Attempts to configure HA on a host in this cluster will fail until a DasAgentFoundEvent is logged or unless this is the first node to be configured. For example, if all the other hosts are disconnected first.
	Based on event DasAgentFoundEvent.	Resolve		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Resource pool configuration conflict	Based on event ResourceViolatedEvent.	Error	Manual	This event records when a conflict with a resource pool's resource configuration is detected.
Storage ATS support failure	Based on event esx.problem.vmfs.ats.support.lost.	Error	Manual	In a shared storage environment, when multiple hosts access the same VMFS datastore, specific locking mechanisms are used. These locking mechanism prevent multiple hosts from concurrently writing to the metadata and ensure that no data corruption occurs. VMFS supports SCSI reservations and atomic test and set (ATS) locking. For storage devices that support hardware acceleration, VMFS uses the ATS algorithm, also called hardware assisted locking. In contrast with SCSI reservations, ATS supports discrete locking per disk sector.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Task timeout reached	Based on event TaskTimeoutEvent.	Warning	Manual	This event records when a task exceeds defined timeout in vCenter Server.
Template deployment failure	Based on event VmDeployFailedEvent.	Error	Manual	This event records a failure to deploy a VM from a template.
vCenter storage availability error	Based on event vprob.vmfs.error.volume.is.locked.	Error	Manual	The alarm indicates that a VMFS volume on the ESXi host is locked due to an I/O error.
	Based on event esx.problem.vmfs.error.volume.is.locked.	Error		
	Based on event vprob.vmfs.extent.offline.	Warning		
	Based on event esx.problem.vmfs.extent.offline.	Warning		
VM instance UUID conflict	Based on event VmInstanceUuidConflictEvent.	Warning	Automatic	This event records a conflict of VM instance UUIDs.
	Based on event VmInstanceUuidChangedEvent.	Resolve		
VM MAC address conflict	Based on event VmMacConflictEvent.	Error	Automatic	This event records a MAC address conflict for a VM.
	Based on event VmStaticMacConflictEvent.			
	Based on event VmMacChangedEvent.	Resolve		
vSphere cluster HA error	Based on event com.vmware.vc.HA.HostDasErrorEvent.	Error	Manual	There is an issue with VMware high-availability configuration for this host.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
vSphere cluster HA warning	Based on event com.vmware.vc.HA.InvalidMaster.	Warning	Manual	There is an issue with VMware high-availability protection for this cluster.
	Based on event com.vmware.vc.HA.UserHeartbeatDatastoreRemoved.			
	Based on event com.vmware.vc.HA.VcCannotFindMasterEvent.			
	Based on event com.vmware.vc.HA.HostPartitionedFromMasterEvent.			
	Based on event com.vmware.vc.HA.HostUnconfiguredWithProtectedVms.			
	Based on event com.vmware.vc.HA.HostUnconfigureError.			
	Based on event com.vmware.vc.HA.NotAllHostAddrsPingable.			

vCloud Director vApp

Alarm Name	Event/Condition	Severity	Resolve Action	Description
vApp health status	VMware Cloud Director object task status equals *Warning.*	Warning	Automatic	vApp health status has changed.
	VMware Cloud Director object task status equals *Alert.*	Error		
vApp runtime lease timeout	vApp runtime lease timeout is 14 days.	Warning	Automatic	vApp runtime lease has expired. Once a vApp is powered on for

Alarm Name	Event/Condition	Severity	Resolve Action	Description
	vApp runtime lease timeout is 7 days.	Error		the first time, the clock starts for the Maximum Runtime Lease. The Maximum Runtime Lease is how long a vApp can be powered on before its automatically suspended.
vApp storage lease timeout	vApp storage lease timeout is 14 days.	Warning	Automatic	vApp storage lease has expired. A vApp storage lease begins when a user stops the vApp. Storage leases do not affect running vApps.
	vApp storage lease timeout is 7 days.	Error		

vCloud Director Organization

Alarm Name	Rule Event	Severity	Resolve Action	Description
Organization blocking task number	Number of blocking tasks is 1 or more.	Warning	Automatic	Some tasks are in a pending state as a result of blocking.
	Number of blocking tasks is 5 or more.	Error		
Organization blocking task timeout	Blocking tasks timeout is 5 minutes.	Warning	Automatic	One or more organization blocking tasks has expired.
	Blocking tasks timeout is 10 minutes.	Error		

vCloud Director Org VDC

Alarm Name	Rule Event	Severity	Resolve Action	Description
Network pool usage	Network pool usage is above 90%.	Warning	Automatic	Network pool usage has exceeded the configured threshold.
	Network pool usage is above 95%.	Error		

Alarm Name	Rule Event	Severity	Resolve Action	Description
Org VDC CPU usage	Average CPU usage for 15 minutes is above 80%.	Warning	Automatic	Organization VDC has exceeded the CPU usage threshold.
	Average CPU usage for 15 minutes is above 90%.	Error		
Org VDC health status	VMware Cloud Director object task status equals *Warning.*	Warning	Automatic	Organization VDC health status has changed.
	VMware Cloud Director object task status equals *Alert.*	Error		
Org VDC memory usage	Average memory usage for 15 minutes is above 80%.	Warning	Automatic	Organization VDC has exceeded the memory usage threshold.
	Average memory usage for 15 minutes is above 90%.	Error		
Org VDC storage usage	Average storage usage for 15 minutes is above 80%.	Warning	Automatic	Organization VDC has exceeded the storage usage threshold.
	Average storage usage for 15 minutes is above 90%.	Error		

vCloud Director Provider VDC

Alarm Name	Rule Event	Severity	Resolve Action	Description
Provider VDC CPU usage	Average CPU usage for 15 minutes is above 80%.	Warning	Automatic	Provider VDC has exceeded the threshold for CPU Usage
	Average CPU usage for 15 minutes is above 90%.	Error		
Provider VDC health status	VMware Cloud Director object task status equals *Warning.*	Warning	Automatic	Provider VDC health status has changed.

Alarm Name	Rule Event	Severity	Resolve Action	Description
	VMware Cloud Director object task status equals *Alert.*	Error		
Provider VDC memory usage	Average memory usage for 15 minutes is above 80%.	Warning	Automatic	Provider VDC has exceeded the memory usage threshold.
	Average memory usage for 15 minutes is above 90%.	Error		
Provider VDC storage usage	Average storage usage for 15 minutes is above 80%.	Warning	Automatic	Provider VDC has exceeded the storage usage threshold.
	Average storage usage for 15 minutes is above 90%.	Error		

Microsoft Hyper-V Alarms

This section describes predefined alarms for Microsoft Hyper-V infrastructure components.

Host

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Bad Hyper-V username logon attempt	Based on event 4625 Microsoft-Windows-Security-Auditing.	Error	Manual	This event records a failed user logon attempt. The combination of username, password and permissions is the mechanism by which Hyper-V server authenticate a user for access and authorize the user to perform activities.
Cluster communication session failed	Based on event 1570 Microsoft-Windows-FailoverClustering.	Error	Manual	Host mode failed to establish a communication session while joining the cluster.
Cluster host node network connectivity error	Based on event 1554 Microsoft-Windows-FailoverClustering.	Error	Manual	This cluster node has no network connectivity. It cannot participate in the cluster until connectivity is restored.
Cluster hosts update version mismatch	Based on event 1548 Microsoft-Windows-FailoverClustering.	Error	Manual	Host node has established a communication session with another node and detected that it is running a different but compatible version of the cluster service software.
Cluster network failure	Based on event 1127 Microsoft-Windows-FailoverClustering.	Warning	Manual	Cluster network interface for cluster node has failed.
Cluster witness resource failure	Based on event 1558 Microsoft-Windows-FailoverClustering.	Error	Manual	The cluster service detected a problem with the witness resource. The witness resource will be failed over to another node within the cluster in an attempt to reestablish access to cluster configuration data.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Cluster witness resource update failure	Based on event 1557 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster service failed to update the cluster configuration data on the witness resource.
Host available memory	Average Hyper-V Services memory usage for 15 minutes is above 80%.	Warning	Automatic	This host is low on available memory.
	Average Hyper-V Services memory usage for 15 minutes is above 90%.	Error		
Host average disk queue length	Average disk queue length for 15 minutes is above 1.	Warning	Automatic	Average disk queue length on the host may report on too many I/O requests. This means that not all requests are queued. Some requests are completed and are on their way back to where the performance data is being collected.
	Average disk queue length for 15 minutes is above 2.	Error		
Host average memory pressure	Average pressure for 15 minutes is above 90%.	Warning	Automatic	This host has exceeded the threshold for memory pressure.
	Average pressure for 15 minutes is above 100%.	Error		
Host cluster membership	Based on event 1093 Microsoft-Windows-FailoverClustering.	Error	Manual	The Cluster service cannot identify host node as a member of failover cluster.
Host connection failure	State not equals *Connected* for 5 minutes or more.	Error	Automatic	This alarm monitors Hyper-V host connection state.
Host CPU time per dispatch	Average host CPU wait time for 15 minutes is 60 microseconds.	Warning	Automatic	The counter shows the average time Virtual Machines running on the host spent waiting for a virtual processor to be dispatched onto a logical processor. More vCPUs on host means more things the dispatcher has to schedule thus wait time raises.
	Average host CPU wait time for 15 minutes is 100 microseconds.	Error		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Host CPU usage	Average Total Run Time value for 15 minutes is above 75%.	Warning	Automatic	This host has exceeded the threshold for CPU usage.
	Average Total Run Time value for 15 minutes is above 85%.	Error		
Host failed to form a cluster	Based on event 1546 Microsoft-Windows-FailoverClustering.	Error	Manual	Host node failed to form a failover cluster.
Host Image Management service is not running	*Hyper-V Image Management* service is not running for 5 minutes or more.	Error	Automatic	The service required to manage virtual storage is not running. No virtual storage management operations can be performed.
Host Memory Pages Usage	Average pages/sec value for 15 minutes is above 500.	Warning	Automatic	The counter shows the rate at which pages are read from or written to disk to resolve hard page faults. This counter is a primary indicator of the types of faults that cause system-wide delays.
	Average pages/sec value for 15 minutes is above 1500.	Error		
Host network average output queue length	Average network output queue length for 15 minutes is above 1.	Warning	Automatic	This host has exceeded the threshold for the length of the queue in packets. This counter should be 0 at all times.
	Average network output queue length for 15 minutes is above 2.	Error		
Host network outbound errors number	Average network outbound errors number for 15 minutes is above 1.	Warning	Automatic	This host has exceeded the threshold for the outbound packets that couldn't be transmitted because of errors.
	Average network outbound errors number for 15 minutes is above 2.	Error		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Host Networking Management service is not running	*Hyper-V Networking Management* service is not running for 5 minutes or more.	Error	Automatic	The Hyper-V Networking Management Service is not configured to start automatically. Virtual networks cannot be managed until the service is started.
Host node failed to form a cluster	Based on event 1573 Microsoft-Windows-FailoverClustering.	Error	Manual	Host node failed to form a cluster.
Host node failed to join cluster	Based on event 1572 Microsoft-Windows-FailoverClustering.	Error	Manual	Host node failed to join the cluster because it could not send and receive failure detection network messages with other cluster nodes.
Host node was evicted from cluster	Based on event 1011 Microsoft-Windows-FailoverClustering.	Warning	Manual	Cluster host node has been evicted from the failover cluster.
Host node was removed from cluster	Based on event 1135 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster node was removed from the active failover cluster membership. If the Cluster service fails to start on a failover cluster node, the node cannot function as part of the cluster.
Host restart	Based on event 1074 User32.	Information	Automatic	Host operation system has been restarted or shut down.
Missing latest cluster configuration data	Based on event 1561 Microsoft-Windows-FailoverClustering.	Error	Manual	The cluster service has determined that this node does not have the latest copy of cluster configuration data. Therefore, the cluster service has prevented itself from starting on this node.
Network communication failure	Based on event 1592 Microsoft-Windows-FailoverClustering.	Warning	Manual	Cluster node lost communication with another cluster node. Network communication was reestablished.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Unreachable cluster network interface	Based on event 1126 Microsoft-Windows-FailoverClustering.	Warning	Manual	Cluster network interface for cluster node is unreachable by at least one other cluster node attached to the network.
Virtual Machine Management service is not running	*Hyper-V Virtual Machine Management* service is not running.	Error	Automatic	The service required to manage virtual machines is not running. No virtual machine management operations can be performed.

Virtual Machine

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Background disk merge failed	Based on event 19100 Microsoft-Windows-Hyper-V-VMMS.	Warning	Manual	The parent virtual hard disks associated with this virtual machine may be in an inconsistent state.
Background disk merge interruption	Based on event 19090 Microsoft-Windows-Hyper-V-VMMS.	Warning	Manual	The snapshot merge operation was interrupted.
Checkpoint configuration is not accessible	Based on event 16420 Microsoft-Windows-Hyper-V-VMMS.	Error	Manual	The configuration of checkpoint is no longer accessible.
Current memory pressure	Average memory pressure for 15 minutes is above 110%.	Warning	Automatic	This VM has exceeded the threshold for memory pressure.
	Average memory pressure for 15 minutes is above 125%.	Error		
Failed to assign dynamic MAC address	Based on event 12572 Microsoft-Windows-Hyper-V-SynthNic.	Error	Manual	Dynamic MAC address for VM network adapter was not assigned.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Failed to create memory contents file	Based on event 3320 Microsoft-Windows-Hyper-V-Worker.	Error	Manual	Failed to create memory contents file.
Failed to create VM saved state file	Based on event 3080 Microsoft-Windows-Hyper-V-Worker.	Error	Manual	Failed to create or access VM saved state file.
Failed to delete VM directory	Based on event 16150 Microsoft-Windows-Hyper-V-VMMS.	Warning	Manual	Cannot delete VM directory.
Failed to initialize VM memory	Based on event 3050 Microsoft-Windows-Hyper-V-Worker.	Error	Manual	Failed to initialize VM memory.
Failed to merge virtual disk	Based on event 16210 Microsoft-Windows-Hyper-V-VMMS.	Warning	Manual	Cannot merge disk file on deletion. As a result, this disk may be in an inconsistent state.
Failed to power on VM	Based on event 12010 Microsoft-Windows-Hyper-V-Worker. Based on event 12030 Microsoft-Windows-Hyper-V-Worker. Based on event 12040 Microsoft-Windows-Hyper-V-Worker. Based on event 12050 Microsoft-Windows-Hyper-V-Worker.	Error	Manual	Failed to power on VM.
Failed to restore VM	Based on event 12080 Microsoft-Windows-Hyper-V-Worker.	Error	Manual	Failed to restore a VM.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Failed to save VM	Based on event 12054 Microsoft-Windows-Hyper-V-Worker.	Error	Manual	Failed to save state for a VM.
Guest disk space	Guest disk free space is below 10%.	Warning	Automatic	Guest OS volume is low on available guest disk space.
	Guest disk free space is below 5%.	Error		
Incompatible version of integration services	Based on event 4010 Microsoft-Windows-Hyper-V-Integration.	Warning	Manual	The version of a component of integration services is incompatible with another version.
Insufficient disk space	Based on event 16050 Microsoft-Windows-Hyper-V-VMMS.	Warning	Manual	Hyper-V disk space is low on available free space.
Invalid static MAC address	Based on event 12560 Microsoft-Windows-Hyper-V-SynthNic.	Error	Manual	By default, new virtual machines in Hyper-V are created with NICs that are assigned dynamic MAC addresses.
	Based on event 12560 Microsoft-Windows-Hyper-V-Worker.			
	Based on event 12560 Microsoft-Windows-Hyper-V-VMMS.			
Latest checkpoint age	VM checkpoint age is 48 hours or more.	Warning	Automatic	The age of the latest checkpoint for this VM has exceeded the configured threshold.
Latest checkpoint size	Hyper-V VM checkpoint size is above 10% of the VM size.	Warning	Automatic	The size of the latest checkpoint file for this VM has

Alarm Name	Event/Condition	Severity	Resolve Action	Description
	Hyper-V VM checkpoint size is above 20% of the VM size.	Error		exceeded the configured threshold.
Machine remoting system failure	Based on event 12480 Microsoft-Windows-Hyper-V-Worker.	Warning	Manual	Failure in machine remoting system has been detected.
No disk space to run this VM	Based on event 16060 Microsoft-Windows-Hyper-V-VMMS.	Error	Manual	VM has been paused because it has run out of disk space.
Not enough memory to start a VM	Based on event 3122 Microsoft-Windows-Hyper-V-Worker.	Error	Manual	Hyper-V was unable to allocate RAM resources to start this VM.
	Based on event 3030 Microsoft-Windows-Hyper-V-Worker.			
Possible ransomware activity	Total Run Time is above 70% and Virtual Storage Write is above 40 MB/s or Virtual Network Bytes Sent/sec is above 40 MB/s for 5 minutes.	Warning	Automatic	Veeam ONE detected suspicious activity on this VM.
	Total Run Time is above 80% and Virtual Storage Write is above 60 MB/s or Virtual Network Bytes Sent/sec is above 60 MB/s for 5 minutes.	Error		
Static MAC address conflict	Based on event 12562 Microsoft-Windows-Hyper-V-SynthNic.	Warning	Manual	By default, new virtual machines in Hyper-V are created with NICs that are

Alarm Name	Event/Condition	Severity	Resolve Action	Description
	Based on event 12562 Microsoft-Windows-Hyper-V-Worker.			assigned dynamic MAC addresses.
Unexpected VM error	Based on event 16020 Microsoft-Windows-Hyper-V-VMMS.	Error	Manual	This VM has encountered an unexpected error.
VM configuration is not accessible	Based on event 16410 Microsoft-Windows-Hyper-V-VMMS.	Error	Manual	The configuration of virtual machine is no longer accessible.
	Based on event 16400 Microsoft-Windows-Hyper-V-VMMS.			
VM configuration module error	Based on event 4096 Microsoft-Windows-Hyper-V-Config.	Error	Manual	The VM configuration is no longer accessible.
VM CPU usage	Average guest run time for 15 minutes is above 75%.	Warning	Automatic	This VM has exceeded the threshold for CPU usage.
	Average guest run time for 15 minutes is above 85%.	Error		
VM disk errors	Average number of errors/min for 15 minutes is above 4.	Warning	Automatic	This VM has logged one or more errors that have occurred on its virtual device.
	Average number of errors/min for 15 minutes is above 8.	Error		
VM guest OS reboot	Based on event 18514 Microsoft-Windows-Hyper-V-Worker.	Information	Warning	Virtual Machine was rebooted. This warning is applied only to Windows Server 2012 and Windows Server 2012 R2.
VM initialization error	Based on event 3040 Microsoft-Windows-Hyper-V-Worker.	Error	Manual	VM initialization has failed.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
VM power status	State not equals *Running* for 5 minutes or more.	Error	Automatic	VM power state has been changed.
VM invalid switch port reference	Based on event 12570 Microsoft-Windows-Hyper-V-SynthNic.	Error	Manual	The virtual machine cannot be started.
VM restart	Based on event 18512 Microsoft-Windows-Hyper-V-Worker.	Information	Automatic	Virtual Machine was rebooted. This warning is applied only to Windows Server 2012 and Windows Server 2012 R2.
VM shutdown by guest	Based on event 18508 Microsoft-Windows-Hyper-V-Worker.	Information	Automatic	Virtual Machine was shut down. This warning is applied only to Windows Server 2012 and newer Windows server versions.
VM shutdown by host	Based on event 18504 Microsoft-Windows-Hyper-V-Worker.	Information	Automatic	Virtual Machine was shut down. This warning is applied only to Windows Server 2012 and newer Windows server versions.
VM vCPU time per dispatch	Average CPU wait time for 15 minutes is above 60 microseconds.	Warning	Automatic	The counter shows the average time spent waiting for a virtual processor to be dispatched onto a logical processor.
	Average CPU wait time for 15 minutes is above 100 microseconds.	Error		
VM with no backups	No backup restore points for the past 24 hours.	Warning	Automatic	This VM has not been backed up within the defined RPO (Recovery Point Objective) interval.
VM with no replica	No replica restore points for the past 24 hours.	Warning	Automatic	This VM has not been replicated within the defined RPO (Recovery Point Objective) interval.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
VSS checkpoint failure	Based on event 10102 Microsoft-Windows-Hyper-V-VMMS.	Error	Manual	Failed to create the backup of virtual machine.
	Based on event 15252 Microsoft-Windows-Hyper-V-VMMS.	Error		

Cluster

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Cluster configuration data is missing or corrupt	Based on event 1575 Microsoft-Windows-FailoverClustering.	Error	Manual	An attempt to forcibly start the cluster service has failed because the cluster configuration data on host node is either missing or corrupt.
Cluster configuration database cannot be unloaded	Based on event 1593 Microsoft-Windows-FailoverClustering.	Error	Manual	The failover cluster database could not be unloaded and any potentially incorrect changes in memory could not be discarded. The cluster service will attempt to repair the database by retrieving it from another cluster node.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Cluster database could not be loaded	Based on event 1057 Microsoft-Windows-FailoverClustering.	Error	Manual	The cluster database could not be loaded. Ensure that a good copy of the cluster configuration is available to the node.
Cluster memory overcommitment	Based on event VeeamHvClusterReserveStateOkEvent.	Resolve	Automatic	When placing a virtual machine in a failover cluster, the placement process calculates whether the new virtual machine will over-commit the cluster. If the action will over-commit the cluster, the alarm will trigger.
	Based on event VeeamHvClusterReserveStateErrorEvent.	Error		
Cluster network is down	Based on event 1130 Microsoft-Windows-FailoverClustering.	Warning	Manual	Cluster network is down.
Cluster resource cannot be brought online	Based on event 1207 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster network name resource cannot be brought online. The computer object associated with the resource could not be updated in domain.
Cluster resource failure	Based on event 1069 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster resource in clustered service or application has failed.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Cluster service cannot be started	Based on event 1090 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster service cannot be started. An attempt to read configuration data from the Windows registry failed.
Cluster service failed to start	Based on event 1105 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster service failed to start because it was unable to register interfaces with the RPC service.
Cluster service failed to write data to a file	Based on event 1080 Microsoft-Windows-FailoverClustering.	Warning	Manual	Cluster service could not write to a file. In a failover cluster, most clustered services or applications use at least one disk, also called a disk resource, that you assign when you configure the clustered service or application. Clients can use the clustered service or application only when the disk is functioning correctly.
Cluster service fatal error	Based on event 1000 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster service suffered an unexpected fatal error.
Cluster service interruption	Based on event 1006 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster service was halted due to incomplete connectivity with other cluster nodes.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Cluster service shut down	Based on event 1177 Microsoft-Windows-FailoverClustering.	Error	Manual	The Cluster service is shutting down because quorum was lost.
Cluster Shared Volume is not available	Based on event 5120 Microsoft-Windows-FailoverClustering.	Warning	Automatic	Cluster Shared Volume is no longer available on this node. All I/O will temporarily be queued until a path to the volume is reestablished.
	Based on event 5122 Microsoft-Windows-FailoverClustering.	Resolve		
Cluster Shared Volume is not directly accessible	Based on event 5121 Microsoft-Windows-FailoverClustering.	Warning	Automatic	Cluster Shared Volume is no longer directly accessible from this cluster node. I/O access will be redirected to the storage device over the network through the node that owns the volume. This may result in degraded performance.
	Based on event 5122 Microsoft-Windows-FailoverClustering.	Resolve		
Failed to bring cluster resource online	Based on event 1049 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster IP address resource cannot be brought online.
Failed to copy cluster configuration data file	Based on event 1581 Microsoft-Windows-FailoverClustering.	Warning	Manual	The restore request for the cluster configuration data failed to make a copy of the existing cluster configuration data file (ClusDB).

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Failed to create cluster resource name in domain	Based on event 1193 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster network name resource failed to create its associated computer object in domain.
Failed to migrate virtual machine	Based on event 22506 Microsoft-Windows-Hyper-V-High-Availability. Based on event 22505 Microsoft-Windows-Hyper-V-High-Availability. Based on event 21100 Microsoft-Windows-Hyper-V-High-Availability.	Error	Manual	Live migration for this VM did not succeed.
Failed to unload failover cluster database	Based on event 1574 Microsoft-Windows-FailoverClustering.	Error	Manual	The failover cluster database could not be unloaded.
Inconsistency within the failover cluster	Based on event 1073 Microsoft-Windows-FailoverClustering.	Error	Manual	The Cluster service was halted to prevent an inconsistency within the failover cluster.
Invalid IP address detected	Based on event 1047 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster IP address resource cannot be brought online because the address value is invalid.
Invalid IP address for cluster resource	Based on event 1360 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster IP address resource failed to come online.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Invalid subnet mask detected	Based on event 1046 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster IP address resource cannot be brought online because the subnet mask value is invalid.
Unexpected cluster service problem	Based on event 1556 Microsoft-Windows-FailoverClustering.	Error	Manual	The cluster service encountered an unexpected problem and will be shut down.

Cluster Shared Volume

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Active filter drivers detected	Based on event 5125 Microsoft-Windows-FailoverClustering.	Warning	Manual	Cluster Shared Volume has identified one or more active filter drivers on this device stack that could interfere with CSV operations. I/O access will be redirected to the storage device over the network through another Cluster node. This may result in degraded performance.
	Based on event 5126 Microsoft-Windows-FailoverClustering.			
Cluster Shared Volume read latency	Average read latency for 15 minutes is above 40 milliseconds.	Warning	Automatic	Cluster Shared Volume has exceeded the configured threshold of total read latency.
	Average read latency for 15 minutes is above 80 milliseconds.	Error		
Cluster Shared Volume write latency	Average write latency for 15 minutes is above 40 milliseconds.	Warning	Automatic	Cluster Shared Volume has exceeded the configured threshold of total write latency.
	Average write latency for 15 minutes is above 80 milliseconds.	Error		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Cluster Shared Volume free space	Free space is below 10%.	Warning	Automatic	Cluster Shared Volume is low on available free space.
	Free space is below 5%.	Error		
Redirected access was turned on	Based on event 5136 Microsoft-Windows-FailoverClustering.	Warning	Manual	Cluster Shared Volume redirected access was turned on. Access to the storage device will be redirected over the network from all cluster nodes that are accessing this volume. This may result in degraded performance.
Volume snapshot preparation error	Based on event 1584 Microsoft-Windows-FailoverClustering.	Error	Manual	A backup application initiated a VSS snapshot on Cluster Shared Volume without properly preparing the volume for snapshot. This snapshot may be invalid and the backup may not be usable for restore operations.

Local Storage

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Datastore read latency	Avg Disk sec/Read value for 15 minutes is 40 milliseconds.	Warning	Automatic	This host local disk has exceeded the threshold for total read latency. This performance monitor counter measures the amount of time that read operations take to respond to the operating system.
	Avg Disk sec/Read value for 15 minutes is 80 milliseconds.	Error		
Datastore write latency	Avg Disk sec/Write value for 15 minutes is 40 milliseconds.	Warning	Automatic	This host disk has exceeded the threshold for total write latency. This performance monitor counter measures the amount of time that write operations take to respond to the operating system.
	Avg Disk sec/Write value for 15 minutes is 80 milliseconds.	Error		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Local volume free space	Free space is below 10%.	Warning	Automatic	Local volume is low on available free space.
	Free space is below 5%.	Error		

Any Hyper-V Object

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Cluster Shared Volume is no longer accessible	Based on event 5142 Microsoft-Windows-FailoverClustering.	Error	Manual	Cluster Shared Volume is no longer accessible from this cluster node because of error.
Failed to load VM configuration	Based on event 16300 Microsoft-Windows-Hyper-V-VMMS.	Error	Manual	Cannot load a virtual machine configuration
Failed to open VM attachment	Based on event 12290 Microsoft-Windows-Hyper-V-Worker.	Error	Manual	Cannot open VM attachment.
	Based on event 12290 Microsoft-Windows-Hyper-V-SynthStor.			
	Based on event 12290 Microsoft-Windows-Hyper-V-VMMS.			
	Based on event 12140 Microsoft-Windows-Hyper-V-VMMS.			
	Based on event 12140 Microsoft-Windows-Hyper-V-Worker.			
	Based on event 12140 Microsoft-Windows-Hyper-V-SynthStor.			

Alarm Name	Event/Condition	Severity	Resolve Action	Description
	Based on event 12240 Microsoft-Windows-Hyper-V-VMMS.			
	Based on event 12240 Microsoft-Windows-Hyper-V-Worker.			
	Based on event 12240 Microsoft-Windows-Hyper-V-SynthStor.			
Failed to register VM configuration file	Based on event 20100 Microsoft-Windows-Hyper-V-VMMS.	Warning	Manual	The Hyper-V Virtual Machine Management service failed to register the configuration for the virtual machine.
Failed to revert to VSS snapshot	Based on event 10104 Microsoft-Windows-Hyper-V-VMMS.	Error	Manual	Failed to revert to VSS snapshot on one or more virtual hard disks of the virtual machine.
Failed to unregister VM configuration file	Based on event 20102 Microsoft-Windows-Hyper-V-VMMS.	Warning	Manual	The Hyper-V Virtual Machine Management service failed to unregister the configuration for the virtual machine.
Failed to verify VM configuration file	Based on event 20104 Microsoft-Windows-Hyper-V-VMMS.	Warning	Manual	The Hyper-V Virtual Machine Management service failed to verify that the configuration is registered for the virtual machine.
VM configuration file is corrupt	Based on event 16310 Microsoft-Windows-Hyper-V-VMMS.	Error	Manual	Cannot load the virtual machine because the configuration is corrupt.

Internal Alarms

The following table describes internal Veeam ONE alarms.

Alarm Name	Event/Condition	Severity	Description
Audit log failure	Based on event VeeamAuditLogFailureEvent.	Error	Veeam ONE failed to add a new record to the audit log.
	Based on event VeeamAuditLogFailureResolvedEvent.	Resolve	
Audit log free space	Amount of free space is below 25%.	Warning	Size of the audit log is reaching the maximum allocated space limit.
	Amount of free space is below 5%.	Error	
Backup performance data collection failure	Based on event VeeamBpPerfCollectionFailedEvent.	Error	Veeam ONE failed to collect performance data from the specified backup server.
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	
	Based on event VeeamBpPerfCollectionFailedResolvedEvent.	Resolve	
Backup data collection failure	Based on event VeeamNoHostConnectionEvent.	Error	Veeam ONE failed to collect data from a Veeam Backup & Replication server.
	Based on event VeeamNoHostConnectionResolvedEvent.	Resolve	
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	
Disk cache error	Based on event VeeamDPCacheEvent.	Warning	Veeam ONE failed to write performance data to the disk cache folder.
	Based on event VeeamDPCacheResolvedEvent.	Resolve	
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	

Alarm Name	Event/Condition	Severity	Description
Events data collection failure	Based on event VeeamEventCollectionFailedEvent.	Error	Veeam ONE failed to collect events data from the objects specified.
	Based on event VeeamEventCollectionFailedResolvedEvent.	Resolve	
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	
Guest services collection failure	Based on event VeeamCollectionServiceFailedEvent.	Error	Veeam ONE failed to collect guest services state information.
	Based on event VeeamCollectionServiceFailedResolvedEvent.	Resolve	
Guest processes collection failure	Based on event VeeamCollectionProcessFailedEvent.	Error	Veeam ONE failed to collect guest processes state information.
	Based on event VeeamCollectionProcessFailedResolvedEvent.	Resolve	
Hardware sensors collection failure	Based on event VeeamHardwareSensorsCollectionEvent.	Error	Veeam ONE failed to collect host hardware information.
	Based on event VeeamHardwareSensorsCollectionResolvedEvent.	Resolve	
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	
Performance data collection failure	Based on event VeeamPerfCollectionFailedEvent.	Error	Veeam ONE failed to collect performance data from the objects specified.
	Based on event VeeamPerfCollectionFailedResolvedEvent.	Resolve	
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	
Reporting data scheduling issue	Status of a report scheduling task equals *Warning*.	Warning	Veeam ONE failed to deliver a scheduled report,
	Status of a report scheduling task equals *Failed*.	Error	

Alarm Name	Event/Condition	Severity	Description
	Status of a report folder scheduling task equals *Warning*.	Warning	report folder or dashboard.
	Status of a report folder scheduling task equals *Failed*.	Error	
	Status of a dashboard scheduling task equals *Warning*.	Warning	
	Status of dashboard scheduling task equals *Failed*.	Error	
SQL Server Express database size	Based on event VeeamSqlLowDbFreeSpaceEvent.	Warning	Veeam ONE database size is close to maximum database size supported by SQL Server Express Edition.
	Based on event VeeamSqlLowDbFreeSpaceResolvedEvent.	Resolve	
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	
Staging data processing issue	Age of the oldest file that contains staging data equals 1 day.	Error	Age of the oldest file that contains staging data of Veeam ONE databases has reached the configured threshold.
Topology collection failure	Based on event VeeamInfCollectionFailedEvent.	Error	Veeam ONE failed to collect infrastructure topology.
	Based on event VeeamInfCollectionFailedResolvedEvent.	Resolve	
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	
VMware Cloud Director blocking tasks update failure	Based on event VeeamVcdBlockingTaskUpdateFailedEvent.	Error	Veeam ONE failed to update VMware Cloud Director blocking tasks list.
	Based on event VeeamVcdBlockingTaskUpdateFailedResolvedEvent.	Resolve	

Alarm Name	Event/Condition	Severity	Description
VMware Cloud Director connection failure	Based on event VeeamNoVcdHostConnectionEvent.	Error	Veeam ONE failed to collect performance and configuration data from VMware Cloud Director.
	Based on event VeeamNoVcdHostConnectionResolvedEvent.	Resolve	
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	
VMware Cloud Director stranded items update failure	Based on event VeeamVcdStrandedItemUpdateFailedEvent.	Error	Veeam ONE failed to update VMware Cloud Director stranded items list.
	Based on event VeeamVcdStrandedItemUpdateFailedResolvedEvent.	Resolve	
Veeam Backup & Replication license compatibility	Based on event VeeamBackupServerLicenseCompatibility.	Error	License installed on the backup server is not compatible with the license installed on Veeam ONE server.
	Based on event VeeamBackupServerLicenseCompatibilityResolved.	Resolve	
Veeam intelligent diagnostics failure	Based on event VeeamIntelligenceDiagnosisFailedEvent.	Error	Veeam ONE failed to analyze Veeam Backup & Replication server logs.
Veeam ONE agent server connection failure	Based on event VeeamOneAgentServerNoConnectionEvent.	Error	Veeam ONE server failed to connect to Veeam ONE agent server.
	Based on event VeeamOneAgentServerNoConnectionResolvedEvent.	Resolve	
Veeam ONE agent client connection failure	Based on event VeeamOneAgentClientNoConnectionEvent.	Error	Veeam ONE server failed to connect to Veeam ONE agent client.
	Based on event VeeamOneAgentClientNoConnectionResolvedEvent.	Resolve	
	Based on event VeeamEmailNotificationFailed.	Error	

Alarm Name	Event/Condition	Severity	Description
Veeam ONE email notification delivery failure	Based on event VeeamEmailNotificationResolved.	Resolve	Veeam ONE server failed to deliver an email notification.
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	
Veeam ONE license expiration date	Based on event VeeamLicenseExpirationWarningEvent.	Warning	Veeam ONE license is going to expire soon.
	Based on event VeeamLicenseExpirationErrorEvent.	Error	
	Based on event VeeamLicenseChangedEvent.	Resolve	
	Based on event VeeamLicenseExpirationResolvedEvent.	Resolve	
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	
Veeam ONE license update failure	Based on event VeeamLicenseUpdateErrorEvent.	Warning	License update failure can take place for a number of reasons such as connection failure, invalid identifier, expired contract, and so on. In case of a connection problem and licensing server key generation error, Veeam ONE will retry to update the license key.
	Based on event VeeamLicenseUpdateResolvedEvent.	Resolve	
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	
Veeam ONE license exceeded	Based on event VeeamVMsExceedErrorEvent.	Error	Veeam ONE license limit has been exceeded.
	Based on event VeeamVMsExceedWarningEvent.	Warning	
	Based on event VeeamSocketExceedEvent.	Error	

Alarm Name	Event/Condition	Severity	Description
	Based on event VeeamBpExceedErrorEvent.	Error	
	Based on event VeeamBpExceedWarningEvent.	Warning	
	Based on event VeeamLicenseGraceOverEvent.	Error	
	Based on event VeeamVMsExceedResolvedEvent.	Resolve	
	Based on event VeeamSocketExceedResolvedEvent.	Resolve	
	Based on event VeeamLicenseChangedEvent.	Resolve	
	Based on event VeeamVbmExceedWarningEvent.	Warning	
	Based on event VeeamVbmExceedResolvedEvent.	Resolve	
Object properties data collection failure	Job state equals *Failed*.	Error	Veeam ONE Object properties data collection job did not finish successfully.
	Job state equals *Warning*.	Warning	
Veeam ONE Reporting service state	Veeam ONE Reporting service is not running.	Error	Veeam ONE Reporting service has failed.
Veeam ONE Server Load	Veeam ONE Server CPU Usage is above 90% or Veeam ONE Server Memory Usage is above 95%.	Error	Veeam ONE Server load is too high.
	Veeam ONE Server CPU Usage is above 75% or Veeam ONE Server Memory Usage is above 85%.	Warning	

Alarm Name	Event/Condition	Severity	Description
Veeam ONE support expiration date	Based on event VeeamLicenseSupportExpirationWarningEvent.	Warning	Veeam ONE support period is going to expire soon.
	Based on event VeeamLicenseSupportExpirationErrorEvent.	Error	
	Based on event VeeamLicenseChangedEvent.	Resolve	
	Based on event VeeamLicenseSupportExpirationResolvedEvent.	Resolve	
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	
Virtual Server connection failure	Based on event VeeamNoHostConnectionEvent.	Error	Connection to virtual server has failed.
	Based on event VeeamNoHostConnectionResolvedEvent.	Resolve	
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	

Alarm Rules Reference

This section describes rules that can be used to create alarms for virtual and backup infrastructures.

Alarm Rules for VMware vSphere

Veeam ONE offers the following types of alarm rules for VMware vSphere infrastructure objects.

vCenter Server

Rule Type	Description
Event-based rule	An alarm is triggered if some vCenter-related event is generated.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Power or connection state changes	An alarm is triggered if the vCenter Server state reports to be equal or not equal to a specific state value (for example, if vCenter Server is not responding).

Cluster

Rule Type	Description
Event-based rule	An alarm is triggered if some cluster-related event is generated.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Resource usage	An alarm is triggered if the specified counter is above or below the specified threshold value (for example, if the memory usage exceeds 80%).

Host

Rule Type	Description
Event-based rule	An alarm is triggered if some host-related event is generated.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.

Rule Type	Description
Hardware sensor state changes	An alarm is triggered if the sensor state reports to be equal or not equal to a specific state value (*Normal*, *Warning*, *Alert*, *Unknown*).
Number of VMs is out of allowed range	An alarm is triggered if the number of running, powered off or suspended VMs on the ESXi host is above or below the specified threshold value. This type of alarm can be configured if it is necessary to limit the number of VMs running on the ESXi host at the same time to avoid the host overload.
Power or connection state changes	An alarm is triggered if the host state reports to be equal or not equal to a specific state value (for example, if the ESXi host is not responding).
Resource usage	An alarm is triggered if the specified counter is above or below the specified threshold value (for example, if the CPU usage exceeds 75%).

Resource Pool

Rule Type	Description
Event-based rule	An alarm is triggered if some event is generated on a resource pool.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Resource usage	An alarm is triggered if the specified counter is above or below the specified value (for example, if the CPU usage exceeds 80%).

Virtual Machine

Rule Type	Description
Event-based rule	An alarm is triggered if some VM-related event is generated (for example, if the MAC address of the VM conflicts with the MAC address of another VM existing in the virtual infrastructure).

Rule Type	Description
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Guest disk space	An alarm is triggered if available disk space on guest volumes is above or below the specified threshold value. You can choose to specify the amount of due free space as an absolute value or a relative value. For example, an alarm is triggered if free disk space falls below 1 GB or 10% of total space.
Heartbeat is missing	An alarm is triggered if a monitored virtual machine is not available or overloaded for a specific period of time (for example, if heartbeat is missing for 5 minutes).
Number of running services	[For Windows-based machines] An alarm is triggered if the number of services running on a VM is greater than the specified threshold.
Orphaned Veeam Backup & Replication snapshot	An alarm is triggered if a VM has a snapshot that Veeam Backup & Replication created (to back up, replicate or perform another data protection operation for the VM) but was unable to remove when the operation was over.
Power or connection state changes	An alarm is triggered if the state of the VM reports to be equal or not equal to the specified state value (for example, if the VM is suspended).
Process performance	[For Windows-based machines] An alarm is triggered if the specified counter for a VM process is above or below the specified value (for example, if the CPU usage by a process exceeds 15%).
Process state	[For Windows-based machines] An alarm is triggered if VM process state is equal or not equal to a specific state value (*Terminated*, *Running*).
Resource usage	An alarm is triggered if the specified counter is above or below the specified value (for example, if the CPU ready level exceeds 5%).
Service state	[For Windows-based machines] An alarm is triggered if service state is equal or not equal to a specific state value (*Running*, *Paused*, *Stopped*).

Rule Type	Description
Snapshot age for VM	An alarm is triggered if the current snapshot is older than a specified number of hours. This rule helps monitor forgotten snapshots that are consuming valuable storage space and degrading performance of virtual machines.
Snapshot size for VM	An alarm is triggered if the size of the VM snapshot is above or below the specified threshold value. You can choose to specify the size of the snapshot as an absolute value or a relative value. For example, an alarm is triggered if the snapshot size exceeds 5 GB or 10% of total available disk space.
VM snapshots number has exceeded the configured threshold	An alarm is triggered if the number of snapshots created for the VM is greater than the specified threshold.
VMware VM tools state changes	An alarm is triggered if the state of the VMware Tools reports to be equal or not equal to the specified state value (for example, if the VMware Tools is out of date).
VMs with no restore points	An alarm is triggered if the age of the latest backup or replica restore point for the VM has exceeded the threshold (that is, if there are no restore points for the specified RPO period).

Datastore

Rule Type	Description
Datastore is running out of free space	An alarm is triggered if free space on the datastore is above or below the specified threshold value. You can choose to specify the free space threshold as an absolute value or a relative value. For example, an alarm is triggered if the datastore space falls below 10 GB or 15% of total space.
Datastore performance	An alarm is triggered if a performance counter of a datastore is above or below the specified threshold value.
Datastore provisioned space	An alarm is triggered if the provisioned disk space is above or below the specified threshold value. You can select to specify the threshold as an absolute value or a relative value. For example, an alarms is triggered if the provisioned disk space exceeds 500 GB or 400% compared to the datastore capacity.

Rule Type	Description
Event-based rule	An alarm is triggered if some datastore-related event is generated.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Power or connection state changes	An alarm is triggered if the state of the datastore reports to be equal or not equal to the specified state value (for example, if the datastore is not accessible).
Resource usage	An alarm is triggered if the specified counter is above or below the specified threshold value (for example, if the datastore I\O threshold is violated).

Any Object

Rule Type	Description
Event-based rule	An alarm is triggered if some event is generated on any object in the infrastructure.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.

vCloud Director vApp

Rule Type	Description
Event-based rule	An alarm is triggered if some vApp-related event in generated.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Resource usage	An alarm is triggered if the specified counter is above or below the specified value (for example, if the storage usage exceeds 80%).
System health status change	An alarm is triggered if the object health state changes.

Rule Type	Description
vApp runtime lease timeout	An alarm is triggered in N days after the vApp runtime lease has expired.
vApp storage lease timeout	An alarm is triggered in N days after the vApp storage lease has expired.
vCloud Director object task status	An alarm is triggered if the vApp state reports to be equal or not equal to a specific state value (for example, if warnings are registered for the vApp).

vCloud Director Organization

Rule Type	Description
Event-based rule	An alarm is triggered if some event is generated on the organization.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Organization VDC blocking task number	An alarm is triggered if the number of pending blocking tasks has exceeded the specified threshold.
Organization VDC blocking task timeout	An alarm is triggered in N minutes after the blocking tasks has expired.
System health state change	An alarm is triggered if the object health state changes.
vCloud Director object task status	An alarm is triggered if the organization state reports to be equal or not equal to a specific state value (for example, if warnings are registered for the organization).

vCloud Director Org VDC

Rule Type	Description
Event-based rule	An alarm is triggered if some event is generated on the organization VDC.

Rule Type	Description
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Network pool is running out of available IP addresses	An alarm is triggered if the number of remaining IP addresses is above or below the specified threshold value. You can select to specify the threshold as an absolute value or a relative value. For example, if the number of remaining IP addresses is lower than 5 or 10% of the total number for the organization VDC network.
Resource usage	An alarm is triggered if the specified counter is above or below the specified value (for example, if the CPU ready level exceeds 5%).
System health status change	An alarm is triggered if the object health state changes.
vCloud Director object task status	An alarm is triggered if the organization VDC state reports to be equal or not equal to a specific state value (for example, if warnings are registered for the organization VDC).

vCloud Director Provider VDC

Rule Type	Description
Event-based rule	An alarm is triggered if some event is generated on the provider VDC.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Resource usage	An alarm is triggered if the specified counter is above or below the specified value (for example, if the storage usage exceeds 80%).
System health status change	An alarm is triggered if the object health state changes.
vCloud Director object task status	An alarm is triggered if the provider VDC state reports to be equal or not equal to a specific state value (for example, if warnings are registered for the provider VDC).

Alarm Rules for Microsoft Hyper-V

Veeam ONE offers the following types of alarm rules for Microsoft Hyper-V infrastructure objects.

Host

Rule Type	Description
Event-based rule	An alarm is triggered if some host-related event is generated.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Power or connection state changes	An alarm is triggered if the host state reports to be equal or not equal to a specific state value (for example, if the Hyper-V host is not responding).
Service state	An alarm is triggered if host service state is equal or not equal to a specified state value (*Running*, *Paused*, *Stopped*).
Resource usage	An alarm is triggered if the specified counter is above or below the specified threshold value (for example, if the Total Run Time exceeds 75%).
Service state	An alarm is triggered if service state is equal or not equal to a specific state value (*Running*, *Paused*, *Stopped*).

Virtual Machine

Rule Type	Description
Checkpoint age for Hyper-V VM has exceeded the configured threshold	An alarm is triggered if the current checkpoint is older than a specified number of hours. This rule helps monitor forgotten checkpoints that are consuming valuable storage space and degrading performance of virtual machines.

Rule Type	Description
Checkpoint size for Hyper-V VM is out of allowed range	An alarm is triggered if the size of the VM checkpoint is above or below the specified threshold value. You can choose to specify the size of the checkpoint as an absolute value or a relative value (for example, if the checkpoint size exceeds 10% of total available disk space). For example, if the checkpoint size exceeds 5 GB or 10% of total disk space.
Event-based rule	An alarm is triggered if some VM-related event is generated (for example, if the MAC address of the VM conflicts with the MAC address of another VM existing in the virtual infrastructure).
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Guest volumes are running out of free disk space	An alarm is triggered if available disk space on guest volumes is below the specified threshold value. You can choose to specify the amount of due free space as an absolute value or a relative value. For example, alarm triggers if free disk space falls below 1 GB or 10% of total space.
Number of running services	[For Windows-based machines] An alarm is triggered if the number of services running on a VM is greater than the specified threshold.
Process performance	[For Windows-based machines] An alarm is triggered if the specified counter for a VM process is above or below the specified value (for example, if the CPU usage by a process exceeds 15%).
Process state	[For Windows-based machines] An alarm is triggered if VM process state is equal or not equal to a specific state value (*Terminated*, *Running*).
Resource usage	An alarm is triggered if the specified counter is above or below the specified threshold value (for example, if the Guest Run Time level exceeds 5%).
Service state	[For Windows-based machines] An alarm is triggered if service state is equal or not equal to a specific state value (*Running*, *Paused*, *Stopped*).

Rule Type	Description
VMs with no restore points	An alarm is triggered if the age of the latest backup or replica restore point for the VM has exceeded the threshold (that is, if there are no restore points for the specified RPO period).
Power or connection state changes	An alarm is triggered if the VM state reports to be equal or not equal to a specific state value (for example, if the VM is not responding).

Cluster

Rule Type	Description
Event-based rule	An alarm will be triggered if some cluster-related event is generated.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.

Cluster Shared Volumes (CSV)

Rule Type	Description
CSV is running out of free space	An alarm is triggered if free space on the CSV is above or below the specified threshold value. You can choose to specify the free space threshold as an absolute value or a relative value. For example, an alarm is triggered if the CSV space is below 10 GB or 15% of total space.
Event-based rule	An alarm is triggered if some event occurs on Cluster Shared Volumes level.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Resource usage	An alarm is triggered if the specified counter is above or below the specified threshold value (for example, if read latency exceeds 40 milliseconds).

Local Storage

Rule Type	Description
Event-based rule	An alarm is triggered if some storage-related event is generated.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Hyper-V Datastore is running out of free space	An alarm is triggered if free space on the datastore is above or below the specified threshold value. You can choose to specify the free space threshold as an absolute value or a relative value. For example, an alarm is triggered if the datastore space is below 10 GB or 15% of total space.
Resource usage	An alarm will be triggered if the specified counter is above or below the specified threshold value (for example, the average time of disk read exceeds 40 milliseconds).

Any Object

Rule Type	Description
Event-based rule	An alarm is triggered if some event is generated on any object.
Existing alarm	An alarm is triggered if the status of another alarm specified in the settings is changed.
Process state	An alarm is triggered if the state of the specified process reports to be equal or not equal to a specific state value (*Terminated*, *Running*).
Service state	An alarm is triggered if the state of the specified service reports to be equal or not equal to a specific state value for a specified time (for example, if a service is paused for 10 minutes).

Alarm Rules for Veeam Backup & Replication

Veeam ONE offers the following types of alarm rules for Veeam Backup & Replication infrastructure objects.

Enterprise Manager

Rule Type	Description
Event-based rule	An alarm is triggered if some Veeam Backup & Replication event is generated for the Veeam Backup Enterprise Manager.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Power or connection state changes	An alarm is triggered if the state of Veeam Backup Enterprise Manager is equal or not equal to the specified value (for example, if connection to the Enterprise Manager is lost).

Backup Server

Rule Type	Description
CDP VM SLA %	An alarm is triggered if CDP policy SLA is below the specified threshold.
Backup Copy RPO	An alarm is triggered if no VM restore points were created during the specified period.
Incremental backup size	An alarm is triggered if size of one or more increments has exceeded the specified threshold.
Disabled job	An alarm is triggered if the time during which a job was disabled has exceeded the specified threshold.
Job/Policy status	An alarm is triggered if the job or policy status is equal or not equal to the specified value.
Plug-in backup data collection failure	An alarm is triggered if the Veeam ONE server fails to collect plug-in backup data.

Rule Type	Description
Event-based rule	An alarm is triggered if some Veeam Backup & Replication event is generated for the backup server.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Job duration exceeded the allowed time period	An alarm is triggered if duration of a job exceeds the threshold specified in minutes.
Power or connection state changes	An alarm is triggered if the state of Veeam Backup & Replication server is equal or not equal to the specified value (for example, if connection to the backup server is lost).
Unusual job duration	An alarm is triggered if duration of a job session is above specified percentage based on the set of latest job sessions.

Repository

Rule Type	Description
Event-based rule	An alarm is triggered if some Veeam Backup & Replication event is generated for the repository.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Immutability state	An alarm is triggered if immutability is disabled for repositories or repository extents.
Out-of-date state	An alarm is triggered if Veeam Backup & Replication software components installed on the repository server are out of date.
Power or connection state changes	An alarm is triggered if the state of the backup repository is equal or not equal to the specified value (for example, if connection to the repository is lost).

Rule Type	Description
Repository server is running out of free space	An alarm is triggered if free space on the repository is above or below the specified threshold value. You can select to specify the free space threshold as an absolute value or a relative value. For example, an alarm is triggered if the storage space is below 10 GB or 15% of total space.

Proxy

Rule Type	Description
CDP Proxy Cache Usage	An alarm is triggered if the CDP cache usage is above the specified threshold.
Event-based rule	An alarm is triggered if some Veeam Backup & Replication event is generated for the proxy server.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Out-of-date state	An alarm is triggered if Veeam Backup & Replication software components installed on the proxy server are out of date.
Power or connection state changes	An alarm is triggered if the state of proxy server is equal or not equal to the specified value (for example, if connection to the proxy server is lost).

WAN Accelerator

Rule Type	Description
Event-based rule	An alarm is triggered if some Veeam Backup & Replication event is generated for the WAN accelerator.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Out-of-date state	An alarm is triggered if Veeam Backup & Replication software components installed on the WAN accelerator server are out of date.

Rule Type	Description
Power or connection state changes	An alarm is triggered if the state of the WAN accelerator is equal or not equal to the specified value (for example, if connection to the WAN accelerator is lost).

Tape Server

Rule Type	Description
Event-based rule	An alarm is triggered if some Veeam Backup & Replication event is generated for the tape server.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Out-of-date state	An alarm is triggered if Veeam Backup & Replication software components installed on the tape server are out of date.
Power or connection state changes	An alarm is triggered if the state of the backup repository is equal or not equal to the specified value (for example, if connection to the server is lost).

Cloud Repository

Rule Type	Description
Cloud repository lease expiration	An alarm is triggered if cloud repository lease time will expire in the specified number of days.
Event-based rule	An alarm is triggered if some Veeam Backup & Replication event is generated for the cloud repository.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Number of VMs stored in repository	An alarm is triggered if the number of VMs stored in the backup repository has exceeded the specified threshold.

Rule Type	Description
Repository server is running out of free space	An alarm is triggered if free space on the repository is above or below the specified threshold value. You can select to specify the free space threshold as an absolute value (for example, if the storage space should not fall below 10 GB) or a relative value (for example, if the free space should not fall below 15% of total space).

Cloud Gateway

Rule Type	Description
Event-based rule	An alarm is triggered if some Veeam Backup & Replication event is generated for the cloud gateway.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Out-of-date state	An alarm is triggered if Veeam Backup & Replication software components installed on the cloud gateway server are out of date.
Power or connection state changes	An alarm is triggered if the state of the backup repository is equal or not equal to the specified value (for example, if connection to the cloud gateway is lost).

Enterprise Application

Rule Type	Description
Event-based rule	An alarm is triggered if some Veeam Backup & Replication event is generated for the application.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Application backup RPO	An alarm is triggered if no application database backups were created during the specified period.

Alarm Rules for Veeam Backup for Microsoft 365

Veeam ONE offers the following types of alarm rules for Veeam Backup for Microsoft 365 infrastructure objects.

Veeam Backup for Microsoft 365 Server

Rule Type	Description
Job disabled	An alarm is triggered if the time during which a job was disabled has exceeded the specified threshold.
Job status	An alarm is triggered if the job status is equal or not equal to the specified value.
Event-based rule	An alarm is triggered if some Veeam Backup for Microsoft 365 event is generated for the backup server.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Organization without backups	An alarm is triggered if no backups were created for a Microsoft 365 organization during the specified RPO interval.
Power or connection state changes	An alarm is triggered if the state of Veeam Backup for Microsoft 365 server is equal or not equal to the specified value (for example, if connection to the server is lost).
Unusual job duration	An alarm is triggered if duration of a job session is above specified percentage based on the set of latest job sessions.
Veeam Backup for Microsoft 365 Service state	An alarm is triggered if the Veeam Backup for Microsoft 365 Service state is equal or not equal to the specified value.

Backup Proxy

Rule Type	Description
Event-based rule	An alarm is triggered if some Veeam Backup for Microsoft 365 event is generated for the proxy server.

Rule Type	Description
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Power or connection state changes	An alarm is triggered if the state of proxy server is equal or not equal to the specified value (for example, if connection to the proxy server is lost).

Backup Repository

Rule Type	Description
Event-based rule	An alarm is triggered if some Veeam Backup & Replication event is generated for the repository.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Backup repository is running out of free space	An alarm is triggered if free space on the repository is above or below the specified threshold value. You can select to specify the free space threshold as an absolute value or a relative value. For example, an alarm is triggered if the storage space is below 10 GB or 15% of total space.

Rules for Internal Alarms

Veeam ONE offers the following types of rules for internal alarms:

Rule Type	Description
Audit log free space	An alarm is triggered if free disk space allocated to an audit log is below or beyond a specific value (for example, if free space is below 15%).
Event-based rule	An alarm is triggered if some Veeam Backup & Replication event is generated for the Veeam Backup Enterprise Manager.
Existing alarm	An alarm is triggered if the state of another selected alarm is changed.
Resource usage	An alarm is triggered if the specified counter is above or below the specified threshold value (for example, if CPU usage exceeds 90%).
Staging data processing state	An alarm is triggered if the age of the oldest staging data file reaches the specified value.
Veeam ONE Web Client task state	An alarm is triggered if Veeam ONE Web Client task state is equal or not equal to a specific state value (*Failed*, *Warning*, *Success*).

Remediation Actions

This section lists alarms with predefined remediation actions.

Alarm Name	Infrastructure	Resolve Actions	Action Type	Description
Job disabled	Veeam Backup & Replication	Enable backup job	Default action for warning severity	Veeam ONE runs the script that enables the disabled job.
Suspicious incremental backup size	Veeam Backup & Replication	Add job to SureBackup job and start verification	Extra action	Veeam ONE runs the script that starts a SureBackup job to check the restore point containing the suspicious increment.
Latest snapshot age	VMware vSphere	Delete snapshot	Default action for warning severity	Veeam ONE runs the script that deletes the latest snapshot.
		Delete all snapshots	Extra action	Veeam ONE runs the script that deletes all snapshots in the current snapshot branch.
Latest snapshot size	VMware vSphere	Delete snapshot	Default action for error severity	Veeam ONE runs the script that deletes the latest snapshot.
		Delete all snapshots	Extra action	Veeam ONE runs the script that deletes all snapshots in the current snapshot branch.
Too many snapshots on the VM	VMware vSphere	Delete snapshot	Default action for error severity	Veeam ONE runs the script that deletes the latest snapshot.
		Delete all snapshots	Extra action	Veeam ONE runs the script that deletes all snapshots in the current snapshot branch.
Orphaned VM backup snapshot	VMware vSphere	Delete orphaned snapshot	Default action for error severity	Veeam ONE runs the script that deletes the snapshot left by backup or replication job.

Alarm Name	Infrastructure	Resolve Actions	Action Type	Description
VM power status	VMware vSphere	Power on VM	Default action for error severity	Veeam ONE runs the script that powers on the VM.
VM with no backups	VMware vSphere	Add VM to backup job	Default action for warning severity	Veeam ONE runs the script that adds the VM to an existing backup job. For this action you must specify a backup server and a job to which the VM must be added. You can suppress this action if the VM and a target repository do not share location. To do that, select the Suppress if original VM location does not match target repository location check box.
		Add VM to backup job and run	Extra action	Veeam ONE runs the script that adds the VM to an existing backup job and starts that job. For this action you must specify a backup server and a job to which the VM must be added. You can suppress this action if the VM and a target repository do not share location. To do that, select the Suppress if original VM location does not match target repository location check box.
		Run parent backup job	Extra action	Veeam ONE runs the script that starts an existing backup job into which the VM is included. The latest session of the job must have the *Success* status.
		Start Quick backup	Extra action	Veeam ONE runs the script that starts a quick backup job for the VM. For this action you must specify backup server. For details on quick backup, see Quick Backup.

Alarm Name	Infrastructure	Resolve Actions	Action Type	Description
		Start VeeamZIP	Extra action	Veeam ONE runs the script that creates an independent full backup file. For this action you must specify a backup server and a backup repository. You can suppress this action if the VM and a target repository do not share location. To do that, select the Suppress if original VM location does not match target repository location check box. For details on VeeamZIP, see VeeamZIP.
VM with no replica	VMware vSphere	Add VM to replication job	Default action for warning severity	Veeam ONE runs the script that adds the VM to an existing replication job. For this action you must specify a backup server and a job to which the VM must be added. You can suppress this action if the VM and a target repository do not share location. To do that, select the Suppress if original VM location does not match target repository location check box.
		Add VM to replication job and run	Extra action	Veeam ONE runs the script that adds the VM to an existing replication job and starts that job. For this action you must specify a backup server and a job to which the VM must be added. You can suppress this action if the VM and a target repository do not share location. To do that, select the Suppress if original VM location does not match target repository location check box.
		Run parent replication job	Extra action	Veeam ONE runs the script that starts an existing replication job into which the VM is included. The latest session of the job must have the *Success* status.

Alarm Name	Infrastructure	Resolve Actions	Action Type	Description
		Start Quick backup	Extra action	Veeam ONE runs the script that starts a quick backup job for the VM. For this action you must specify backup server. For details on quick backup, see Quick Backup.
		Start VeeamZIP	Extra action	Veeam ONE runs the script that creates an independent full backup file. For this action you must specify a backup server and a backup repository. You can suppress this action if the VM and a target repository do not share location. To do that, select the Suppress if original VM location does not match target repository location check box. For details on VeeamZIP, see VeeamZIP.
Latest checkpoint age	Microsoft Hyper-V	Delete checkpoint	Default action for warning severity	Veeam ONE runs the script that deletes the latest checkpoint.
		Delete checkpoint subtree	Extra action	Veeam ONE runs the script that deletes all checkpoints in the current subtree.
Latest checkpoint size	Microsoft Hyper-V	Delete checkpoint	Default action for error severity	Veeam ONE runs the script that deletes the latest checkpoint.
		Delete checkpoint subtree	Extra action	Veeam ONE runs the script that deletes all checkpoints in the current subtree.
VM power status	Microsoft Hyper-V	Power on VM	Default action for error severity	Veeam ONE runs the script that powers on the VM.

Alarm Name	Infrastructure	Resolve Actions	Action Type	Description
VM with no backup	Microsoft Hyper-V	Add VM to backup job	Default action for warning severity	Veeam ONE runs the script that adds the VM to an existing backup job. For this action you must specify a backup server and a job to which the VM must be added. You can suppress this action if the VM and a target repository do not share location. To do that, select the Suppress if original VM location does not match target repository location check box.
		Add VM to backup job and run	Extra action	Veeam ONE runs the script that adds the VM to an existing backup job and starts that job. For this action you must specify a backup server and a job to which the VM must be added. You can suppress this action if the VM and a target repository do not share location. To do that, select the Suppress if original VM location does not match target repository location check box.
		Run parent backup job	Extra action	Veeam ONE runs the script that starts an existing backup job into which the VM is included. The latest session of the job must have the *Success* status.
		Start Quick backup	Extra action	Veeam ONE runs the script that starts a quick backup job for the VM. For this action you must specify backup server. For details on quick backup, see Quick Backup.

Alarm Name	Infrastructure	Resolve Actions	Action Type	Description
		Run VeeamZIP	Extra action	Veeam ONE runs the script that creates an independent full backup file.
				For this action you must specify a backup server and a job to which the VM must be added.
				You can suppress this action if the VM and a target repository do not share location. To do that, select the Suppress if original VM location does not match target repository location check box.
				For details on VeeamZIP, see VeeamZIP.
VM with no replica	Microsoft Hyper-V	Add VM to replication job	Default action for warning severity	Veeam ONE runs the script that adds the VM to an existing replication job.
				For this action you must specify a backup server and a job to which the VM must be added.
				You can suppress this action if the VM and a target repository do not share location. To do that, select the Suppress if original VM location does not match target repository location check box.
		Add VM to replication job and run	Extra action	Veeam ONE runs the script that adds the VM to a existing replication job and starts that job.
				For this action you must specify a backup server and a job to which the VM must be added.
				You can suppress this action if the VM and a target repository do not share location. To do that, select the Suppress if original VM location does not match target repository location check box.
		Run parent replication job	Extra action	Veeam ONE runs the script that starts an existing replication job into which the VM is included. The latest session of the job must have the *Success* status.

Alarm Name	Infrastructure	Resolve Actions	Action Type	Description
		Start Quick backup	Extra action	Veeam ONE runs the script that starts a quick backup job for the VM. For this action you must specify backup server. For details on quick backup, see Quick Backup.
		Run VeeamZIP	Extra action	Veeam ONE runs the script that creates an independent full backup file. For this action you must specify a backup server and a job to which the VM must be added. You can suppress this action if the VM and a target repository do not share location. To do that, select the Suppress if original VM location does not match target repository location check box. For details on VeeamZIP, see VeeamZIP.

Appendix A. Veeam ONE Settings Utility

The Veeam ONE Settings utility allows you to change configuration of the Veeam ONE software components.

> **NOTE:**
>
> The Veeam ONE Settings utility must be used only under the guidance of Veeam Support. It is strongly recommended that you obtain detailed instructions from the Veeam Support team before changing any configuration settings in your Veeam ONE deployment.

To run the Veeam ONE Settings utility:

1. Log in to Veeam ONE Client under account with *Local Administrator* permissions on the machine where Veeam ONE Server component is installed.

   For details, see Accessing Veeam ONE Client.

   > **NOTE:**
   >
   > If you use Microsoft Windows authentication to connect to Microsoft SQL Server, make sure that the user under which you launch Veeam ONE Settings utility has sufficient permissions to access Veeam ONE database. Otherwise the **Retention Policy Period** and **Scalability** settings in the utility will be unavailable.

2. In the main menu, click **Settings** > **Server Settings**.

   Alternatively, press `[CTRL + S]` on the keyboard.

3. Open the **Other** tab.

4. In the **Support utility** section, click **Launch**.

This section describes configuration settings that you can change using the Veeam ONE Settings utility.

General Settings

The **General** section groups configuration settings common for all Veeam ONE software components.

This section includes the following tabs:

- Database
- Retention Policy Period

Database

On the **Database** tab, you can modify connection settings for the Veeam ONE database and the Microsoft SQL Server that hosts this database. By default, the fields are populated with the values specified during Veeam ONE installation.

To change database configuration settings:

1. In the **Server name** field, specify the name of the SQL Server that hosts the Veeam ONE database.

2. In the **Database name** field, specify the name of the database that stores Veeam ONE data.

3. In the **Command time-out** field, specify the wait time in seconds for a command to execute on the Veeam ONE database.

   By default, the time-out value is set to 18000 seconds (5 hours).

   Select the **Multisubnet Failover** check box, to enable failover in a SQL Server multi-subnet failover cluster.

4. From the **Authentication** list, select the type of authentication that Veeam ONE components must use to connect to the Microsoft SQL Server that hosts the Veeam ONE database:

   o Select **Windows Authentication** to use Windows authentication credentials of the Veeam ONE service account.

   o Select **SQL Server Authentication** to use Microsoft SQL Server account credentials.

5. [For SQL Server Authentication] In the **User name/Password** fields, specify credentials of the SQL account used to connect to the Microsoft SQL Server that hosts the Veeam ONE database.

6. Click **Save** to apply settings.

7. To check if Veeam ONE can connect to the specified database using the specified connection settings, click **Test**.

To back up the Veeam ONE database to a `BAK` file, click **Create Backup** and specify the location where the database backup file must be saved.

In the **Information** section, you can view the Veeam ONE connection status and version number.

Retention Policy Period

On the **Retention Policy Period** tab, you can modify the time period during which historical data is stored in the Veeam ONE database. By default, virtual and backup infrastructure performance data is retained for 12 months, and event data is stored for 3 months.

To modify the retention period:

- In the **Virtual Infrastructure performance data retention period** field, specify the period for storing virtual infrastructure performance data, in months.

- In the **Backup Infrastructure performance data retention period** field, specify the period for storing backup infrastructure performance data, in months.

- In the **Retention period for events** field, specify the period for storing events data, in months.

  You can specify a value from 1 to 36.

Specified retention values will be applied at the end of the current week. To apply retention settings immediately, click **Delete Obsolete Data**.

Veeam ONE Server Settings

The **Server** section groups configuration settings for the Veeam ONE Server.

This section includes the following tabs:

- Monitoring Service

- Reporting Service

- Performance Cache

- Object Cleanup

- Web API Certificate

Monitoring Service

On the **Monitoring Service** tab, you can start, stop or restart the Veeam ONE Monitoring service. These operations may be required to complete Veeam ONE configuration updates.
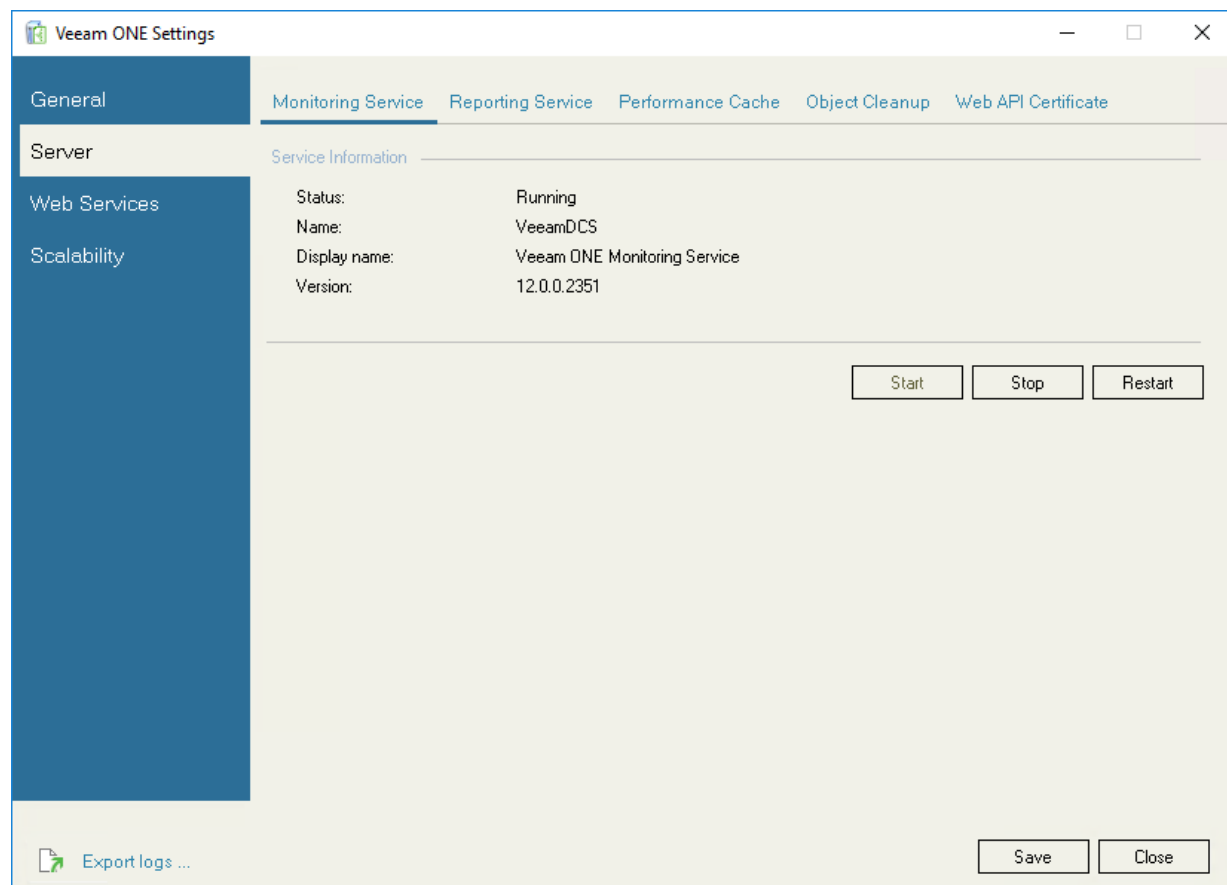
Reporting Service

On the **Reporting Service** tab, you can start, stop or restart the Veeam ONE Reporting service. These operations may be required to complete Veeam ONE configuration updates.
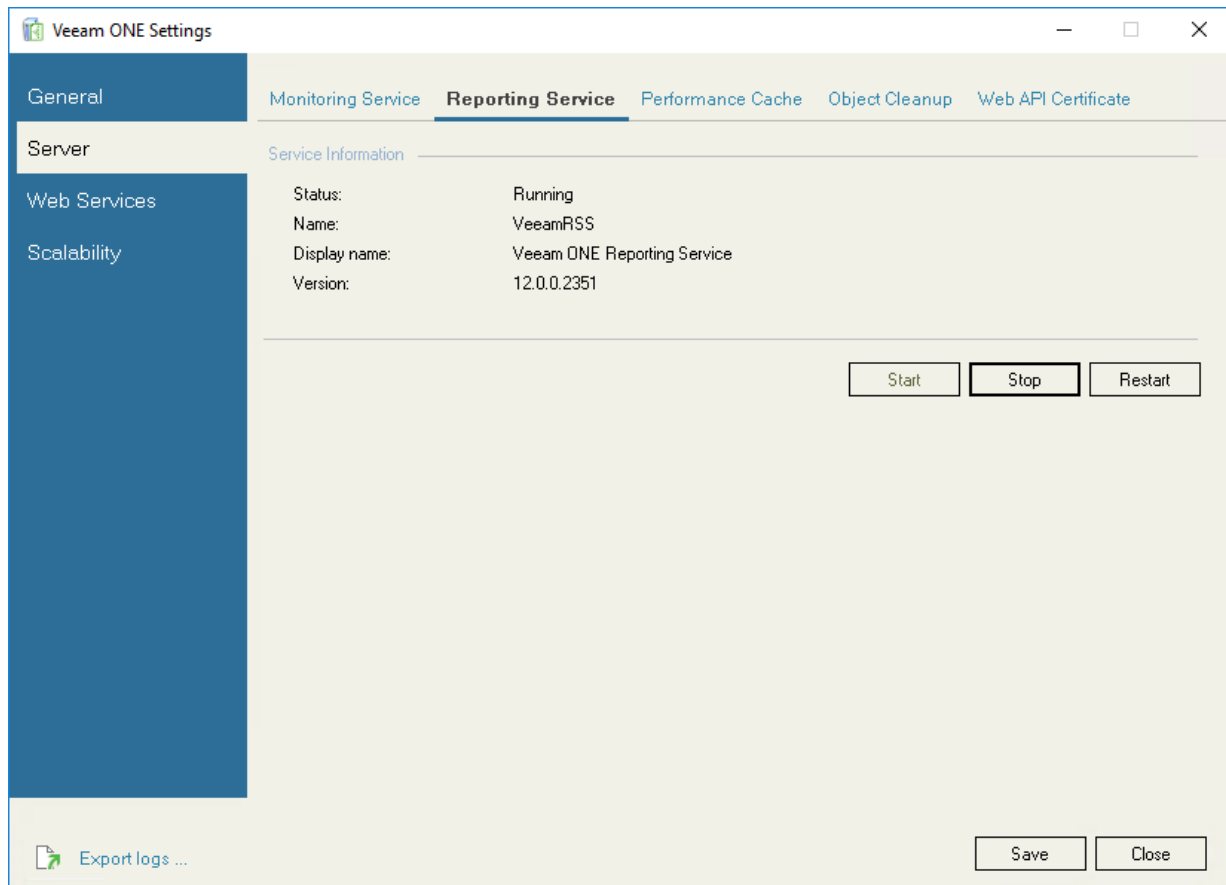
Performance Cache

On the **Performance Cache** tab, you can change the path to the directory in which performance cache is stored. After you change the directory, switch to the **Monitoring Service** tab and restart Veeam ONE Monitoring service.

The initial directory to store performance cache is specified during installation.
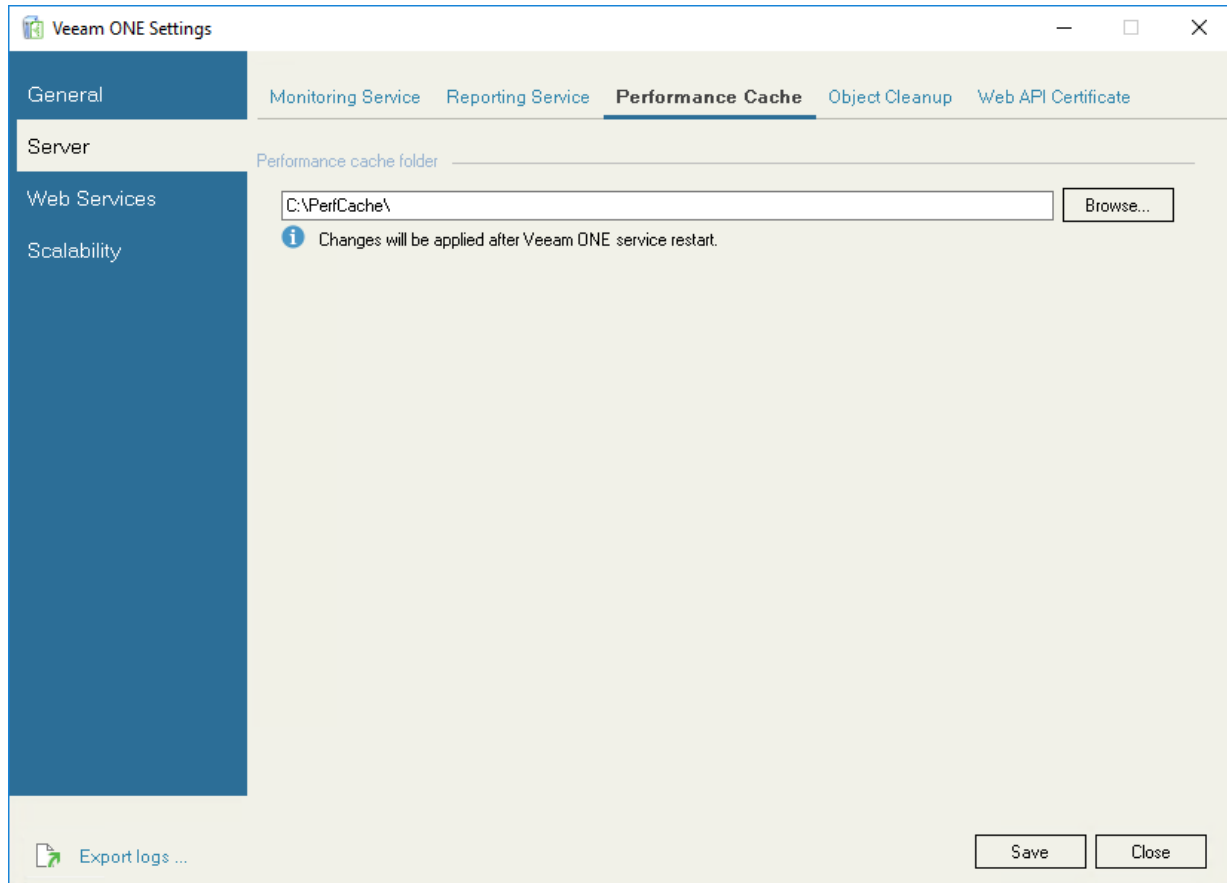
Object Cleanup

On the **Object Cleanup** tab, you can remove residual data on deleted infrastructure objects from the Veeam ONE database.

In some cases, data collected from infrastructure objects remain in the Veeam ONE database even if connections to these infrastructure objects are removed in the Veeam ONE Client. As a result, residual data may appear in Veeam ONE reports.

To clean data on obsolete infrastructure objects from the Veeam ONE database:

1. Click **Select** and choose an infrastructure object for which data must be removed.

2. Click **Remove** and wait for completion of the object data cleanup.
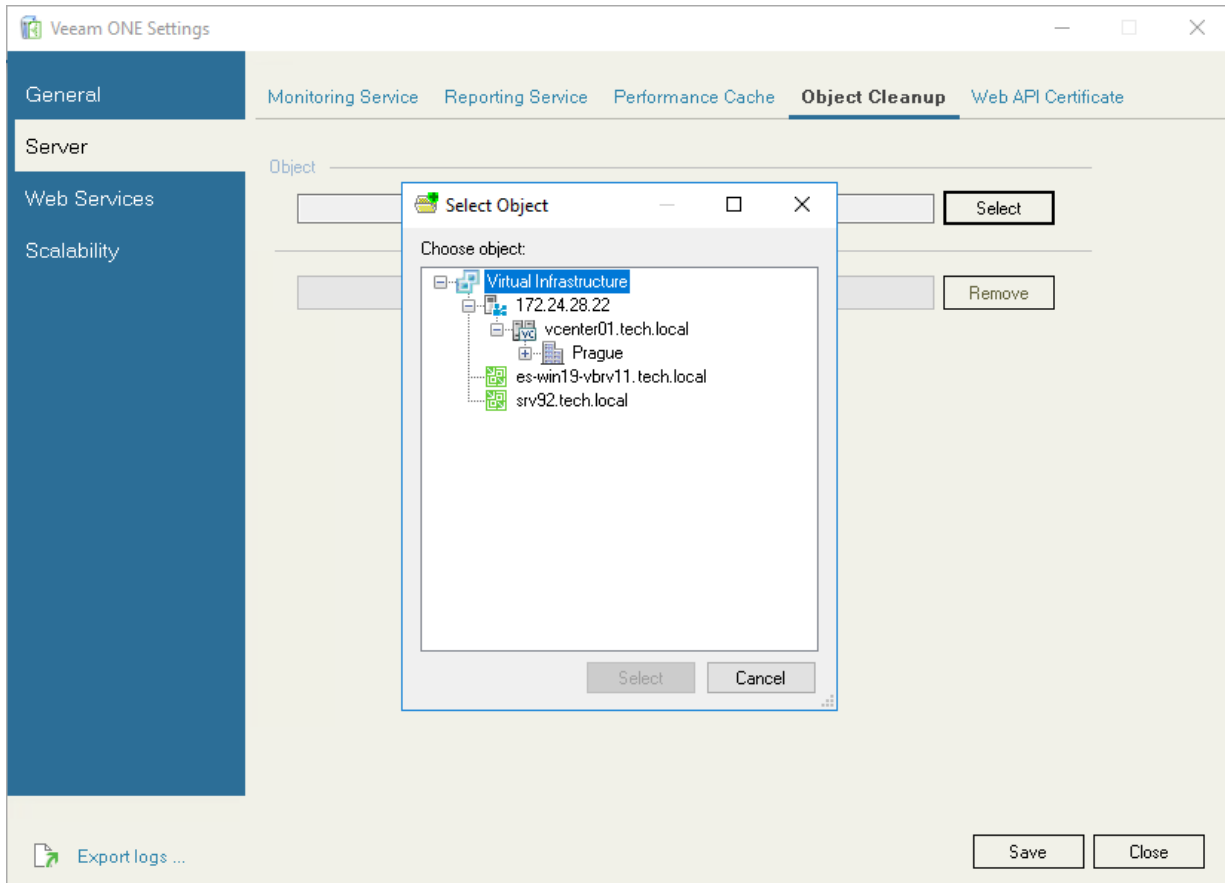
Web API Certificate

On the **Web API Certificate** tab, you can view and manage security certificate installed to protect connection to Veeam ONE REST API. By default Veeam ONE uses the certificate provided during installation.

- The **Certificate Information** section displays summary details of the currently installed certificate.

  Click **View**, to see detailed information on the certificate.

- To import the certificate on the machine where Veeam ONE server component is installed, click **Import** and browse the certificate file.

- To use the certificate from the certificate store, click **Select** and select the certificate from the certificate store.

  The certificate must be added to the **Trusted Root Certificate Authorities** store of the machine where Veeam ONE server component is installed.

- To generate a new self-signed certificate, click **Generate**.

  Veeam ONE will generate a certificate using RSA algorithm with a 2048-bit key length and SHA-2 hashing algorithm. To use a newly generated certificate, in the displayed window, click **Yes**.
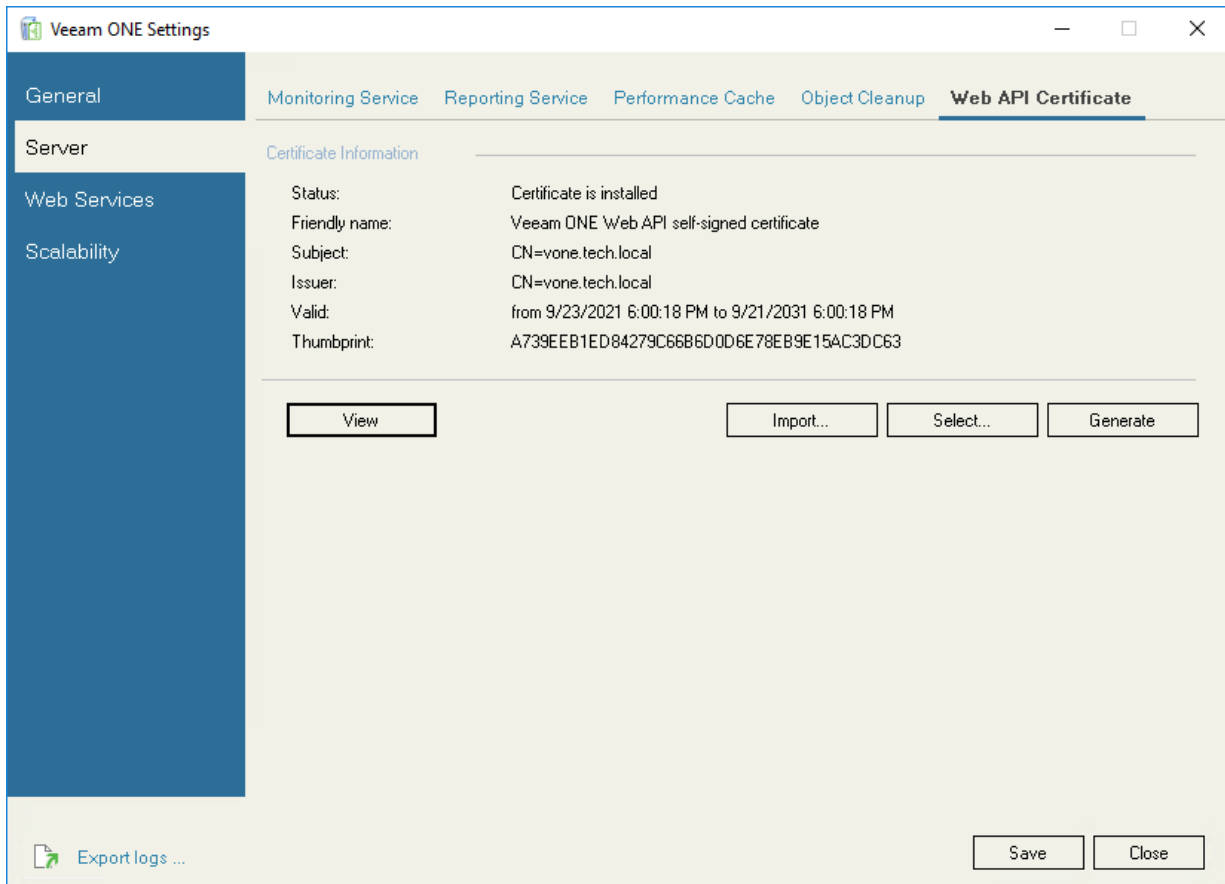
Veeam ONE Web Settings

In the **Web Services** section, you can view Veeam ONE Server connection details and configure.

Veeam ONE Server

On the **Veeam ONE Server** tab, you can review the connection details of the machine where Veeam ONE Server components are installed. This may be required if you installed Veeam ONE using the distributed deployment scenario. Click **Test**, to check connection between Veeam ONE Server and Web Services.
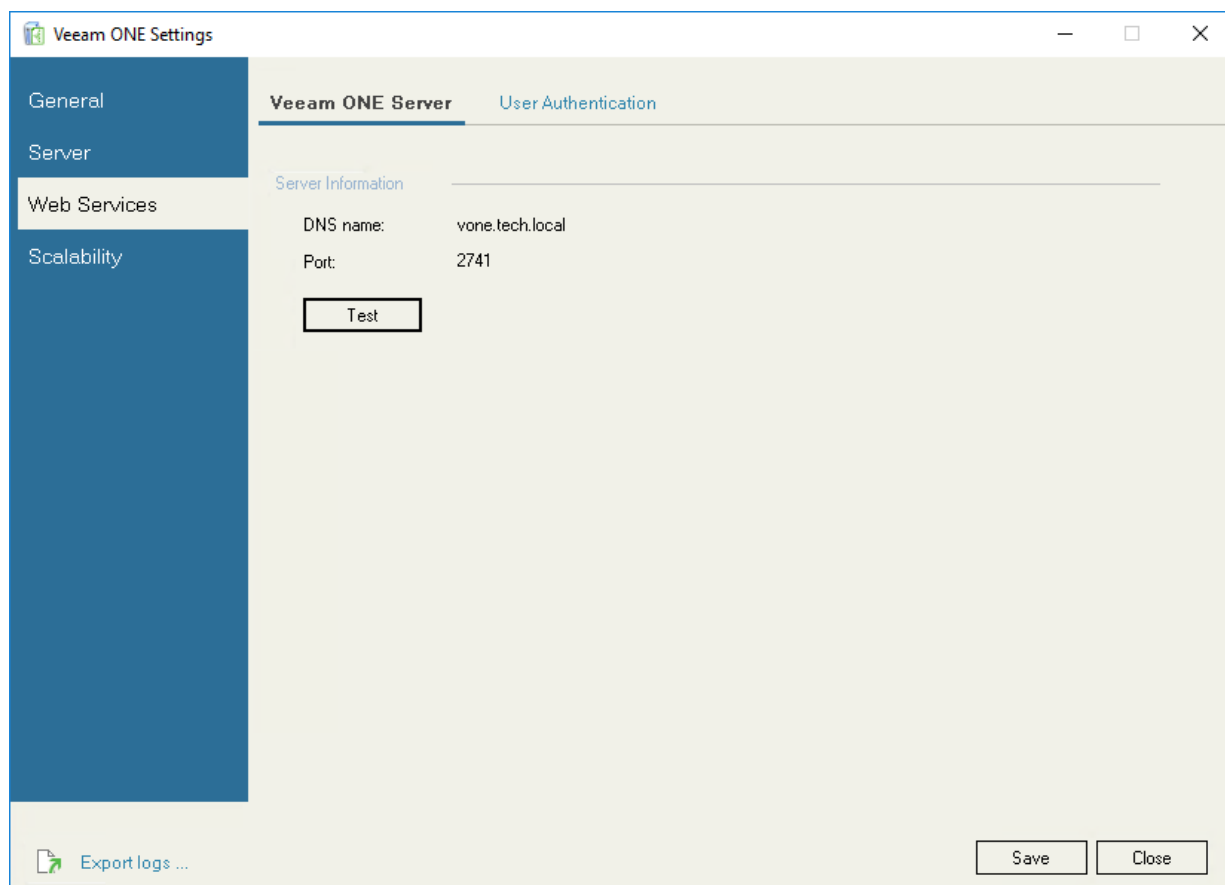
User Authentication

On the **User Authentication** tab, you can select which methods are allowed to authenticate users in Veeam ONE Web Client:

- **Basic authentication** — select this method to allow users to log in with user name and password.

- **Windows authentication** — select this method to allow users to log in with credentials of a Windows user account under which the user is logged on to the machine.

- **Client Certificate Mapping authentication** — select this method to allow users to log in with a client certificate.

  For more information, see Configuring Client Certificate Mapping Authentication.
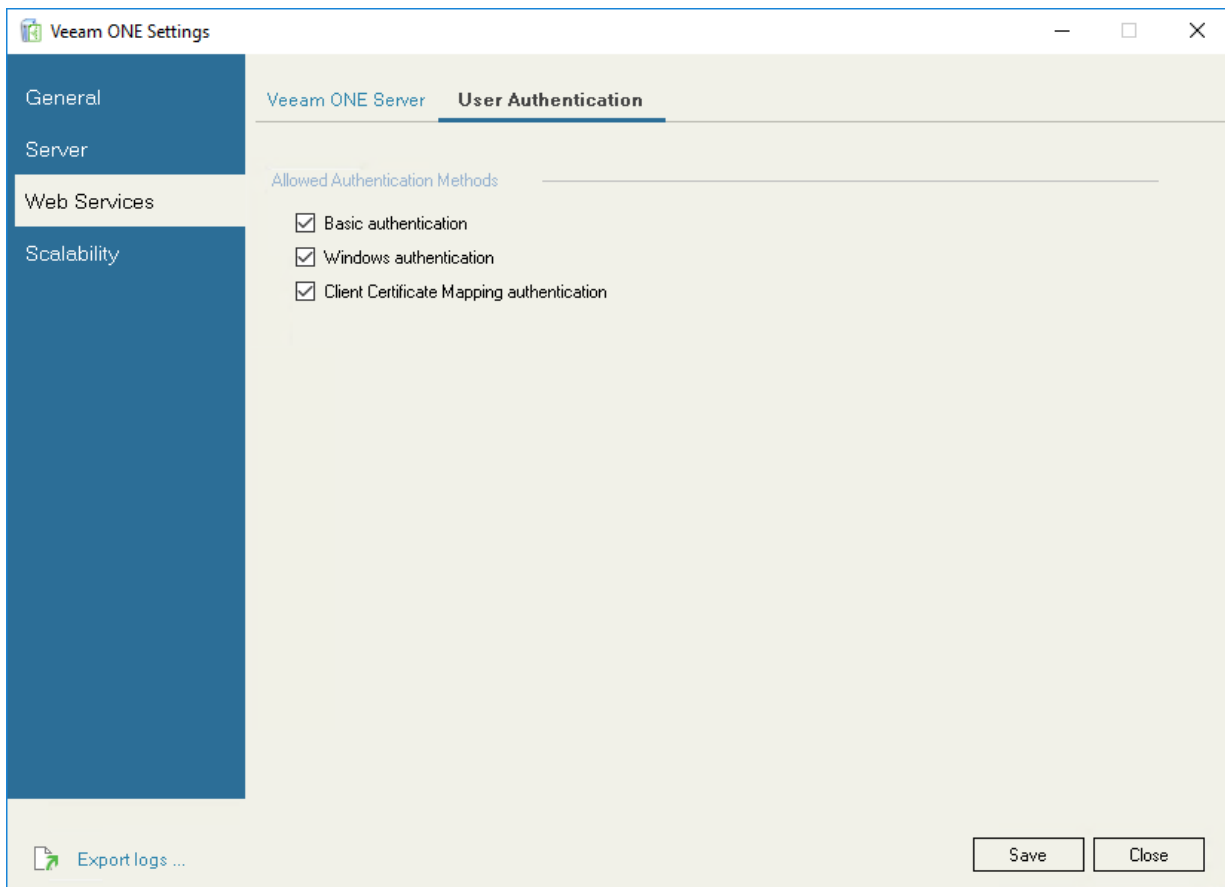
Configuring Client Certificate Mapping Authentication

To allow users to log in to Veeam ONE Web Client with multi-factor authentication (MFA) through client certificate configuration, do the following on the machine that hosts Veeam ONE Web UI component:

- Enable IIS Client Certificate Mapping authentication.

  For more information on IIS Client Certificate Mapping authentication settings, see this Microsoft article.

- If you have non-self-signed certificates in the Trusted Root Certificate Authorities store, move them to the Intermediate Certification Authorities store.

- If Veeam ONE Web UI component runs on Windows Server 2022, you must disable TLS 1.3 over TCP in the site binding settings.

Scalability

In the **Scalability** section, you can choose Veeam ONE data collection mode and metrics that Veeam ONE must collect.

This section includes the following tabs:

- Data Collection Mode

- Performance Metrics

Data Collection Mode

On the **Data Collection Mode** tab, you can choose Veeam ONE data collection mode. The data collection mode determines what metrics Veeam ONE must collect, and specifies the product configuration.

Data collection mode is specified during Veeam ONE installation. In some cases, you may need to change the data collection mode — for example, if you need to change the level of data granularity.

To change the data collection mode:

1. Select the necessary data collection option.

   For more information on data collection mode, see section Choose Data Collection Mode of the Veeam ONE Deployment Guide.

2. Click **Save**.
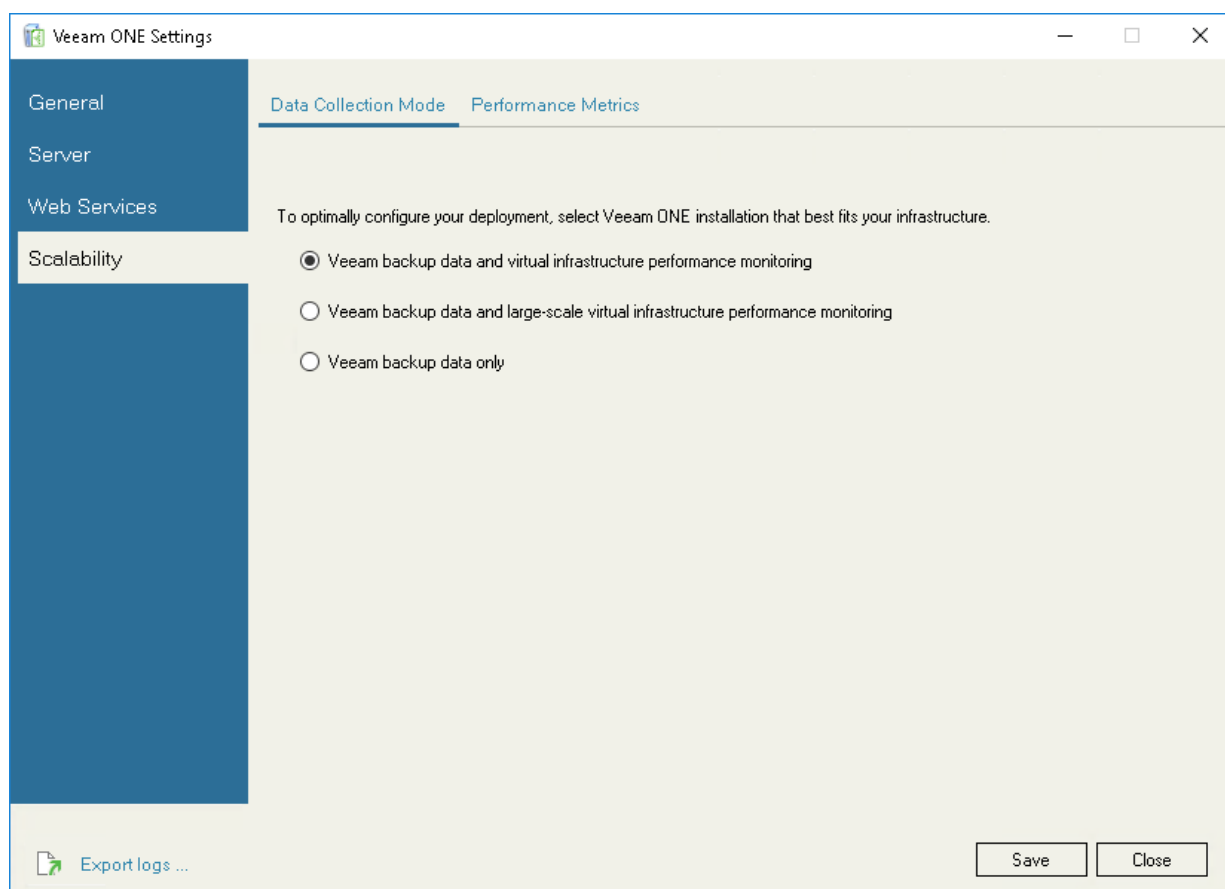
Performance Metrics

On the **Performance metrics** tab, you can explicitly define metrics that Veeam ONE must collect.

The list of metrics that Veeam ONE collects depends on the selected data collection mode. However, you can also manually add a number of performance metrics to that list.

To choose performance metrics that must be collected:

1. In the **Counters** drop-down list, select an infrastructure object to which metrics pertain.

2. In the **State** drop-down list, select the metrics state (*Enabled*, *Disabled*, *Any state*).

3. To quickly find the necessary metric, type the metric name in the search field on the right.

4. Select check boxes next to metrics that Veeam ONE must collect.

5. Click **Save**.
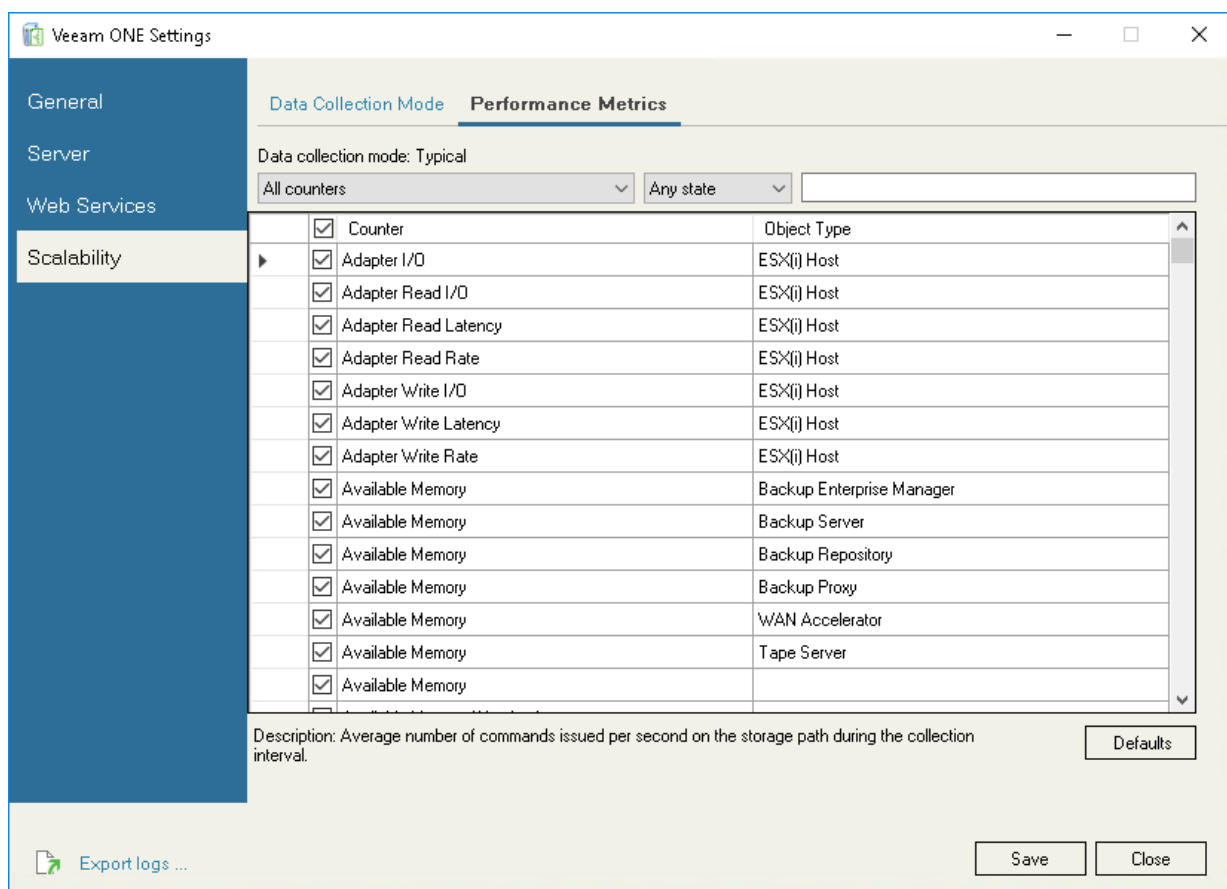
Click **Defaults** to restore Veeam ONE default settings for performance metrics, and select only those metrics that must be collected in accordance with the chosen data collection mode.

Exporting Logs

Diagnostic logs include information that can be used by the Veeam Support Team to troubleshoot issues that occur in Veeam ONE. In addition, diagnostic logs include information about the managed virtual and backup infrastructures. This type of information is used to speed up the root cause analysis when troubleshooting issues.

Veeam ONE Settings utility allows you to export diagnostic logs for the Monitoring and Reporting services:

1. At the bottom left corner of the Veeam ONE Settings utility, click **Export logs**.

2. Specify a location where the exported logs must be saved.

   The Veeam ONE Settings utility will export logs and save them to a `ZIP` archive in the specified location.
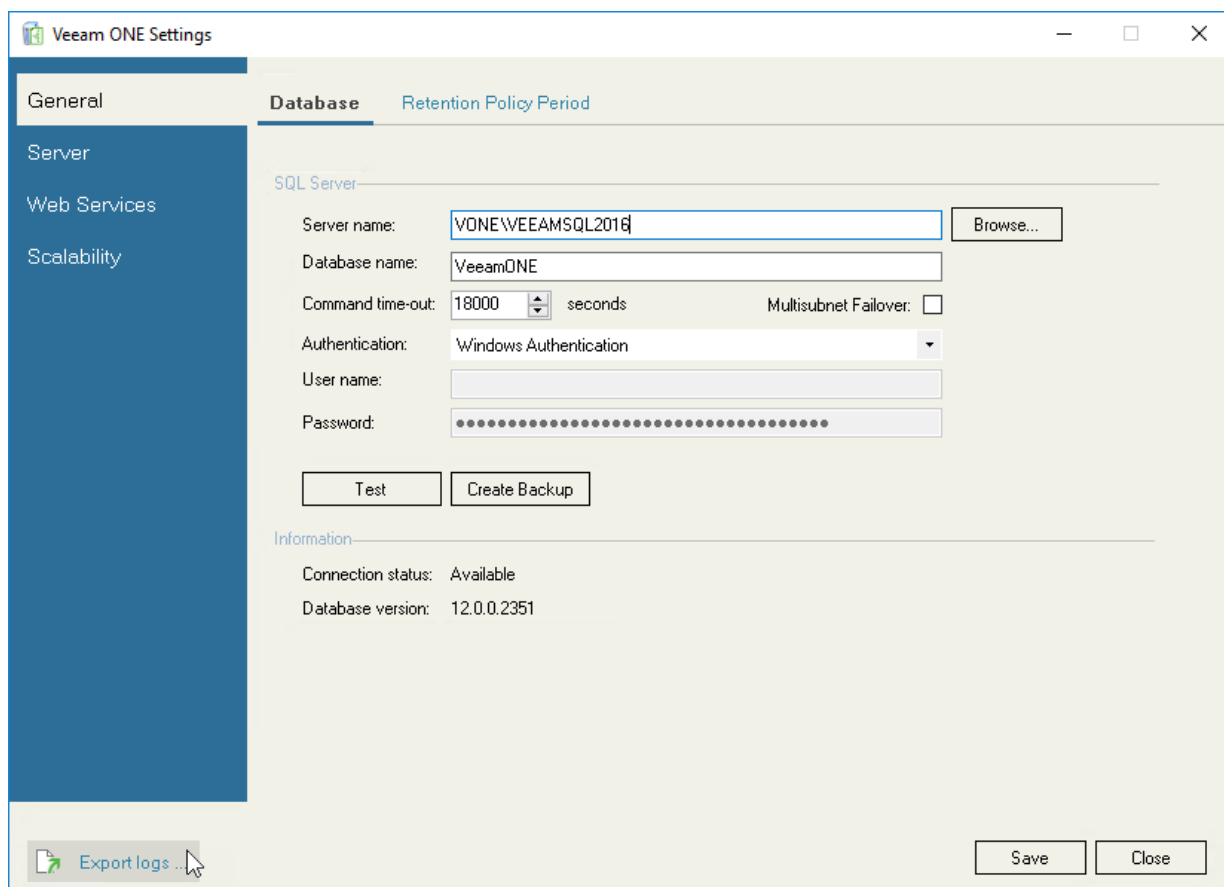
Appendix B. Grouping Expressions Syntax

You can create custom grouping expressions for categories with dynamic groups. In grouping expressions, you can use:

- Object Properties

- Operators

- Functions

- Keywords

- Constants

This section describes components that you can use in grouping expressions.

Object Properties

To create grouping expressions, you can use properties of the following types of objects:

- Host
- Storage
- Cluster
- Virtual Machine
- Computer
- Enterprise Application

Host

The following properties of host systems are supported in grouping expressions.

Property	Return Data Type	Description
CustomAttribute	Text (string)	Returns a value of a custom attribute assigned to a host. Specify the name of a custom attribute in brackets. For example, `CustomAttribute("department")` will return the value of the *'department'* attribute for a host. **Note**: - This property is available for VMware vSphere hosts only. - You cannot use methods to define the custom attribute name. However, the CustomAttribute property can be used to define values in methods.
CustomProperty	Text (string)	Returns a value of a custom property assigned to a host. Specify the name of a custom property in brackets. For example, `CustomProperty("department")` will return the value of the *'department'* property for a host. **Note**: This property is available for Microsoft Hyper-V hosts only.
Tag	Text (string)	Returns a tag assigned to a host. Specify the name of a tag category in brackets. For example, `Tag("department")` will return the tag of the *'department'* category for a host. **Note**: This property is available for VMware vSphere 5.5 or later.
Name	Text (string)	Returns a host name.

Property	Return Data Type	Description
Memory	Numeric (double precision floating-point number)	Returns an amount of host physical memory, in GB.
Location	Text (string)	Returns a location assigned to a host in Veeam Backup & Replication.
ProcessorCores	Numeric (integer)	Returns a number of processor cores for a host.
CPUFrequency	Numeric (double precision floating-point number)	Returns a CPU frequency, in MHz.
VMCount	Numeric (integer)	Returns a number of VMs registered on a host.
Datacenter	Text (string)	Returns a name of a datacenter.
HostModel	Text (string)	Returns a host model. **Note:** This property is available for VMware vSphere hosts only.
CPUSockets	Numeric (integer)	Returns a number of CPU sockets for a host.
InfrastructureLocation	Text (string)	Returns a path to a host in the virtual infrastructure.
Connection_State	Text (string)	Returns a connection state of a host.
PowerState	Text (string)	Returns a power state of a host.

Storage

The following properties of storage systems are supported in grouping expressions.

Property	Return Data Type	Description
CustomAttribute	Text (string)	Returns a value of a custom attribute assigned to a storage. Specify the name of a custom attribute in brackets. For example, `CustomAttribute("department")` will return the value of the *'department'* attribute for a storage. **Notes**: • This property is available for VMware vSphere storage systems only. • You cannot use methods to define the custom attribute name. However, the CustomAttribute property can be used to define values in methods.
Tag	Text (string)	Returns a tag assigned to a storage. Specify the name of a tag category in brackets. For example, `Tag("department")` will return the tag of the *'department'* category for a storage. **Note**: This property is available for VMware vSphere 5.5 or later.
Name	Text (string)	Returns a storage object name.
Capacity	Numeric (double precision floating-point number)	Returns storage capacity, in GB.
FileSystemType	Text (string)	Returns a type of storage file system, such as VMFS or NTFS.
FreeSpace	Numeric (double precision floating-point number)	Returns an amount of free storage space, in GB.
UsedSpace	Numeric (double precision floating-point number)	Returns an amount of used storage space, in GB.

Property	Return Data Type	Description
VMCount	Numeric (integer)	Returns a number of VMs whose files reside on a storage object.
Type	Text (string)	Returns a storage type (*Shared* or *Local*).
InfrastructureLocation	Text (string)	Returns a path to a storage object in the virtual infrastructure.
Datacenter	Text (string)	Returns a name of a datacenter.
DatastoreCluster	Text (string)	Returns a name of a cluster where storage object resides. **Note**: This property is available for VMware vSphere storage objects only.

Cluster

The following properties of clusters are supported in grouping expressions.

Property	Return Data Type	Description
CustomAttribute	Text (string)	Returns a value of a custom attribute assigned to a cluster. Specify the name of a custom attribute in brackets. For example, `CustomAttribute("department")` will return the value of the *'department'* attribute for a cluster. **Notes**: • This property is available for VMware vSphere clusters only. • You cannot use methods to define the custom attribute name. However, the CustomAttribute property can be used to define values in methods.
CustomProperty	Text (string)	Returns a value of a custom property assigned to a cluster. Specify the name of a custom property in brackets. For example, `CustomProperty("department")` will return the value of the *'department'* property for a cluster. **Note**: This property is available for Microsoft Hyper-V clusters only.

Property	Return Data Type	Description
Tag	Text (string)	Returns a tag assigned to a cluster. Specify a name of a tag category in brackets. For example, `Tag("department")` will return the tag of the *'department'* category for a cluster. **Note**: This property is available for VMware vSphere 5.5 or later.
Name	Text (string)	Returns a cluster name.
CPUFrequency	Numeric (integer)	Returns cluster CPU frequency, in MHz.
Connection_State	Text (string)	Returns a connection state of a cluster. **Note**: This property is available for Microsoft Hyper-V clusters only.
Datacenter	Text (string)	Returns a name of a datacenter.
HostCount	Numeric (integer)	Returns a number of hosts in a cluster.
Memory	Numeric (integer)	Returns a memory size of a cluster, in MB.
ProcessorCores	Numeric (integer)	Returns a sum of cores for all hosts in a cluster.
VMCount	Numeric (integer)	Returns a number of VMs whose files reside in a cluster.
InfrastructureLocation	Text (string)	Returns a path to a cluster in the virtual infrastructure.
IsDRSEnabled	Text (string)	Returns a flag that indicates if distributed resource scheduler enabled in a cluster. **Note**: This property is available for VMware vSphere clusters only.
Location	Text (string)	Returns a location assigned to a host in Veeam Backup & Replication.

Virtual Machine

The following properties of VMs are supported in grouping expressions.

Property	Return Data Type	Description
BackupJob	Text (string)	Returns a name of a backup job that protects a VM.
BackupRPO	Numeric (integer)	Returns the number of hours that passed since last backup session completed.
CheckpointCreateTime	Date and time	Returns the date and time when a checkpoint was created, in the `mm/dd/yyyy hh:mm:ss` format. **Notes:** • This property is available for Microsoft Hyper-V VMs only. • If a VM has several checkpoints, the property returns the creation date of the current checkpoint.
ComputerName	Text (string)	Returns a domain name assigned to a VM.
Connection_State	Text (string)	Returns a connection state of a VM.
CustomAttribute	Text (string)	Returns a value of a custom attribute assigned to a VM. Specify the name of a custom attribute in brackets. For example, `CustomAttribute("department")` will return the value of the *'department'* attribute for a VM. **Notes:** • This property is available for VMware vSphere VMs only. • You cannot use methods to define the custom attribute name. However, the CustomAttribute property can be used to define values in methods.
CustomProperty	Text (string)	Returns a value of a custom property assigned to a VM. Specify the name of a custom property in brackets. For example, `CustomProperty("department")` will return the value of the *'department'* property for a VM. **Note:** This property is available for Microsoft Hyper-V VMs only.
CPUFrequency	Numeric (double precision floating-point number)	Returns a frequency of a CPU in MHz. **Note:** This property is available for Microsoft Hyper-V VMs only.

Property	Return Data Type	Description
Datacenter	Text (string)	Returns a name of a datacenter where a VM resides.
Datastore	Text (string)	Returns the name of a storage system (datastore) where VM files reside. **Note:** If VM files reside on several datastores, the property returns the name of a datastore where the VM configuration file is located.
GuestOS	Text (string)	Returns a VM guest OS.
HasBackups	Text (string)	Returns a flag indicating whether a VM has backups or not (*Yes*, *No*).
HasSnapshots	Text (string)	Returns a flag indicating whether a VM has snapshots or not (*Yes*, *No*). **Note:** This property is available for VMware vSphere VMs only.
HasCheckpoints	Text (string)	Returns a flag indicating whether a VM has checkpoints or not (*Yes*, *No*). **Note:** This property is available for Microsoft Hyper-V VMs only.
Host	Text (string)	Returns a name of a host on which a VM resides.
InfrastructureLocation	Text (string)	Returns a path to a VM in the virtual infrastructure.
IpAddress	Text (string)	Returns an IP address assigned to a VM.
IsReplica	Text (string)	Returns a flag indicating whether a VM is a replica of an original VM.
IsShielded	Text (string)	Returns a flag indicating whether a VM is shielded. **Note:** This property is available for Microsoft Hyper-V VMs only.
LastBackupDate	Date and time	Returns the date and time when the latest backup session was performed for a VM in Veeam Backup & Replication, in the `mm/dd/yyyy hh:mm:ss` format. **Note:** The backup session is returned only if a restore point was created as a result of this session.

Property	Return Data Type	Description
Location	Text (string)	Returns a location assigned to a VM in Veeam Backup & Replication.
Memory	Numeric (double precision floating-point number)	Returns the amount of memory allocated to a VM.
Name	Text (string)	Returns a VM name.
Network	Text (string)	Returns the network to which a VM is connected. **Note**: If a VM is connected to several networks, the property will return a random network.
PowerState	Text (string)	Returns a VM power state. • For VMware vSphere: *Powered On*, *Powered Off*, *Suspended* • For Microsoft Hyper-V: *Powered Off*, *Running*, *Saved*
ReplicationJob	Text (string)	Returns a name of a replication job in which a VM is included in Veeam Backup & Replication. **Note**: If a VM is included in several replication jobs, the property will return a random job.
ReplicationRPO	Numeric (integer)	Returns the number of hours that passed since last replication session completed.
SnapshotAge	Numeric (integer)	Returns how many hours ago a snapshot was created. **Note**: This property is available for VMware vSphere VMs only.
SnapshotCreateTime	Date and time	Returns the date and time when a snapshot was created, in the `mm/dd/yyyy hh:mm:ss` format. **Notes**: • This property is available for VMware vSphere VMs only. • If a VM has several snapshots, the property returns the creation date of the latest snapshot.

Property	Return Data Type	Description
`Tag`	Text (string)	Returns a tag assigned to a VM. Specify the name of a tag category in brackets. For example, `Tag("department")` will return the tag of the *'department'* category for a VM. **Note**: This property is available for VMware vSphere 5.5 or later.
`vCPU`	Numeric (integer)	Returns the number of vCPUs configured for a VM.
`VirtualDiskSize`	Numeric (double precision floating-point number)	Returns the amount space occupied by all VM disks.
`VMFolder`	Text (string)	Returns a name of a folder where VM files reside. **Note**: This property is available for VMware vSphere VMs only.
`VMFolderPath`	Text (string)	Returns a user path to a VM in the virtual infrastructure. **Note**: This property is available for VMware vSphere VMs only.

Computer

The following properties of protected computers are supported in grouping expressions.

Property	Return Data Type	Description
`BackupServer`	Text (string)	Returns a name of Veeam Backup & Replication server that manages the backup agent.
`LastBackupDate`	Date and time	Returns the date and time when the latest backup session was performed for a computer in Veeam Backup & Replication, in the `mm/dd/yyyy hh:mm:ss` format.
`BackupRPO`	Numeric (integer)	Returns a number of hours that passed since last backup session completed.
`BpAgentLicenseType`	Text (string)	Returns a type of license installed on a backup agent.

Property	Return Data Type	Description
Location	Text (string)	Returns a location assigned to a computer in Veeam Backup & Replication.
BpAgentManagementType	Text (string)	Returns a management type of a backup agent (*Standalone*, *Managed by VBR*).
Name	Text (string)	Returns a name of a computer that runs a backup agent.
ProtectedComputersGroup	Text (string)	Returns a name of a protection group for a computer.
ClusterName	Text (string)	Returns a name of a failover cluster in which a computer resides.
IpAddress	Text (string)	Returns an IP address assigned to a computer that runs a backup agent.
FQDN	Text (string)	Returns an FQDN assigned to a computer that runs a backup agent.
JobName	Text (string)	Returns a name of a job that runs on a backup agent.
PolicyName	Text (string)	Returns a name of a backup policy assigned to a backup agent.

Enterprise Application

The following properties of protected enterprise applications are supported in grouping expressions.

Property	Return Data Type	Description
ApplicationPolicyName	Text (string)	Returns a name of a backup policy configured for an application.
BackupRPO	Numeric (integer)	Returns a number of hours that passed since last backup session completed.

Property	Return Data Type	Description
BackupServer	Text (string)	Returns a name of Veeam Backup & Replication server that manages the application plug-in.
FQDN	Text (string)	Returns an FQDN assigned to a server that runs a protected application.
HasDataBackupSessions	Text (string)	Returns a flag indicating whether an application has backup policies configured or not (*Yes*, *No*).
IpAddress	Text (string)	Returns an IP address assigned to a server that runs a protected application.
LastBackupDate	Date and time	Returns the date and time when the latest backup session was performed for an application in Veeam Backup & Replication, in the `mm/dd/yyyy hh:mm:ss` format.
Location	Text (string)	Returns a location assigned to an application server in Veeam Backup & Replication.
Name	Text (string)	Returns a name of a server that runs an application.
ProtectionGroup	Text (string)	Returns a name of a protection group for an applications.

Operators

To manipulate values in grouping expressions, you can use the following operators:

Operator	Return Data Type	Description	Example
+	Text (string) Numeric	Joins two string values to one string. Adds two numeric values.	For a VM included in a replication job, expression `"Replication Job: " + ReplicationJob` retuns a string similar to *Replication Job: Webserver Daily Replication*. Expression `2 + 2` returns 4. Expression `2.05 + 1` returns 3.05.
*	Numeric	Multiplies numeric values.	Expression `2 * 2` returns 4. Expression `100 * 0.5` returns 50.
/	Numeric	Divides first numeric value into the second.	Expression `2 / 2` returns 1. Expression `100 / 50` returns 2.
-	Numeric	Subtracts the second numeric value from the first.	Expression `2 - 1` returns 1. Expression `100 - 0.5` returns 99.5.
<	Boolean	Less than. Returns *True* if the value of left operand is less than the value of right operand. Otherwise, returns *False*.	For a VM, expression `Memory < 2048` returns *True* if the amount of memory configured for a VM is less than 2048 MB.
<=	Boolean	Less than or equal to. Returns *True* if the value of left operand is less than or equal to the value of right operand. Otherwise, returns *False*.	For a VM, expression `Memory <= 2048` returns *True* if the amount of memory configured for a VM is less than or equal to 2048 MB.
>	Boolean	Greater than. Returns *True* if the value of left operand is greater than the value of right operand. Otherwise, returns *False*.	For a VM, expression `Memory > 2048` returns *True* if the amount of memory configured for a VM is greater than 2048 MB.

Operator	Return Data Type	Description	Example
`>=`	Boolean	Greater than or equal to. Returns *True* if the value of left operand is greater than or equal to the value of right operand. Otherwise, returns *False*.	For a VM, expression `Memory >= 2048` returns *True* if the amount of memory configured for a VM is greater than or equal to 2048 MB.
`=`	Boolean	Equal. Returns *True* if the value of left operand is the same as the value of right operand. Otherwise, returns *False*.	For a VM, expression `Memory = 2048` returns *True* if the amount of memory configured for a VM is equal to 2048 MB. For a VM, expression `Name = "vdi001"` returns *True* if the VM name is *vdi001*.
`<>`	Boolean	Not equal. Returns *True* if the value of left operand is not the same as the value of right operand. Otherwise, returns *False*.	For a VM, expression `Memory <> 2048` returns *True* if the amount of memory configured for a VM is less or greater than 2048 MB. For a VM, expression `Tag(department) <> "support"` returns *True* if a tag of the *department* category assigned to a VM is other than *support*.
`and`	Text (string)	Joins conditions with a logical AND operator.	For a VM, expression `Memory = 2048 and Name = "vdi001"` returns *True* if the amount of memory configured for a VM is equal to 2048 MB and the VM name is *vdi001*.
`or`	Text (string)	Joins conditions with a logical OR operator.	For a VM, expression `Memory = 2048 or Name = "vdi001"` returns *True* if the amount of memory configured for a VM is equal to 2048 MB or the VM name is *vdi001*.

Functions

To manipulate values in grouping expressions, you can use the following functions:

Function	Return Data Type	Description	Example
DateAdd	Date	Returns a date value to which a time interval has been added, or from which a time interval has been subtracted. The function accepts the following arguments: 1. Date and time to which a time interval must be added, in the `YYYY-MM-DD` format. 2. Time interval that must be added to the initial date and time. The interval can be a positive or negative number. 3. Measurement unit of the time interval ("h" - hour, "d" - day, "m" - month, "y" - year).	Expression `DateAdd("2016-10-20", 7, "d")` adds 7 days to the specified date, and returns *2016-10-27*. Nested expression `SnapshotCreateTime < DateAdd (DateAdd(Today, -2, "d"))` returns *True* if the latest VM snapshot was created earlier than 2 days and 12 hour ago.
IndexOf	Numeric (integer)	Returns the position of the first occurrence of a specified value (substring) in a string. Index of the first character in a string is 0. Returns -1 if the value is not found within the string. The function accepts the following arguments: 1. String value. 2. Substring value whose index position must be found within the string value.	Expression `IndexOf("vdi001_mrk", "_")` returns *6*. Expression `IndexOf("vdi001", "_")` returns *-1*.

Function	Return Data Type	Description	Example
Left	Text (string)	Returns a substring that contains a specified number of characters from the left side of a string. The function accepts the following arguments: 1. String value. 2. Number of characters from the left side of a string to return.	Expression `Left("vdi001_mrk", 6)` returns *vdi001*. Nested expression `Left("vdi001_replica", IndexOf("vdi002_replica", "_"))` returns *vdi002*.
Length	Numeric (integer)	Returns the number of characters in a string. The function accepts a string value as an argument.	Expression `Length("123456789")` returns *9*. For a VM, expression `Length("Name")` returns the number of characters in the VM name.
Replace	Text (string)	Returns a string in which a specified substring has been replaced with another substring. The function accepts the following arguments: 1. String value. 2. Substring value that must be replaced. 3. Substring value that must replace the sought substring. **Note**: If the there are two or more equal substrings in a string, all substrings will be replaced.	Expression `Replace("vdi002 mrk", " ", "_")` changes the *vdi002 mrk* value to *vdi002_mrk*. For a VM, expression `Replace(Name, "_replica", "")` removes the *_replica* suffix from the VM name.
Right	Text (string)	Returns a substring that contains a specified number of characters from the right side of a string. The function accepts the following arguments: 1. String value. 2. Number of characters from the right side of a string to return.	Expression `Right("vdi003_mrk", 3)` returns *mrk*. Nested expression `Right("vdi003_replica", (IndexOf("vdi003_replica", "_")) + 1)` returns *replica*.

Function	Return Data Type	Description	Example
Space	Text (string)	Returns a string that consists of the specified number of spaces. The function accepts a positive integer as an argument.	Nested expression `Replace("vdi004_mrk", "_", Space(1))` changes the *vdi004_mrk* value to *vdi004 mrk*.
Substring	Text (string)	Retrieves a substring from a specified string. The substring starts at the specified character position (index) and has the specified length. Index of the first character in a string is 0. The function accepts the following arguments: 1. String value. 2. Start index position of a substring that must be retrieved. 3. Number of characters to retrieve starting with the specified index position.	Expression `Substring("vdi005_mrk", 7, 3)` returns *mrk*.
Trim	Text (string)	Returns a string with no leading or trailing spaces. The function accepts a string value as an argument.	Expression `Trim("  vdi006  ")` returns *vdi006*.
TrimLeft	Text (string)	Returns a string with no leading spaces. The function accepts a string value as an argument.	Expression `Trim("  vdi007")` returns *vdi007*.
TrimRight	Text (string)	Returns a string with no trailing spaces. The function accepts a string value as an argument.	Expression `Trim("vdi008  ")` returns *vdi008*.

Function	Return Data Type	Description	Example
ToDate	Date	Converts a string containing a valid date representation to the DateTime format. **Note**: The function is based on the DateTime.TryParse function and accepts the same input values.	Expression `ToDate("2009/03/12")` returns *2009-03-12*. Expression `ToDate("ToDate(" 2009/03/01")` returns *2009-03-01*.
ToLowerCase	Text (string)	Converts a string to lower case letters. The function accepts a string value as an argument.	Expression `ToLowerCase("LoWeRCaSe")` returns *lowercase*.
ToUpperCase	Text (string)	Converts a string to upper case letters. The function accepts a string value as an argument.	Expression `ToUpperCase("uppercase")` returns *UPPERCASE*.

Keywords

The logical operator `CASE` represents an *if-else* statement. It is used to evaluate a certain condition and execute an expression if this condition is true. If the condition is false, another expression is executed.

The `CASE` operator has the following syntax:

```
CASE
WHEN "Value" = "1" THEN "Expression 1"
ELSE "Expression 2"
END
```

Here:

- `WHEN` statement represents a condition that must be evaluated.

- `THEN` statement specifies a group to which an object must be placed if the condition is true.

- `ELSE` specifies a group to which an object must be placed if the condition is false.

You can include multiple `WHEN` statements to evaluate multiple conditions:

```
CASE
WHEN "Value" = "1" THEN "Expression 1"
WHEN "Value" = "2" THEN "Expression 2"
WHEN "Value" = "3" THEN "Expression 3"
ELSE "Expression 4"
END
```

Limitations

You cannot nest one CASE expression within another `CASE` expression. However, you can include methods to define values in a `CASE` statement.

Example

Business View includes a number of predefined categories that use `CASE` grouping expressions. You can use these predefined categories to understand how the `CASE` operator works.

For example, the *VMs with Snapshot* category uses the following grouping expression.

```
CASE
WHEN HasSnapshots = "No" THEN "No snapshots"
WHEN SnapshotCreateTime < DateAdd(Today, -30, "d") THEN "Older than 30 days"
WHEN SnapshotCreateTime < DateAdd(Today, -7, "d") THEN "Older than 7 days"
WHEN SnapshotCreateTime < DateAdd(Today, -1, "d") THEN "Older than 1 day"
ELSE "Recent snapshots"
END
```

Here:

- The first `WHEN` statement checks whether a VM has any snapshots. If a VM has no snapshots, this VM is included in the *No snapshots* group.

- The second, third and fourth `WHEN` statements check VM snapshot age. If the age more than 30 days, a VM in included in the *Older than 30 days* group. If the age more than 7 days, a VM in included in the *Older than 7 days* group. If the age more than 1 day, a VM in included in the *Older than 1 day* group.

- The `ELSE` statement includes in the *Recent snapshots* group all VMs with snapshots not older than 1 day.

Constants

To create grouping expressions, you can use the following constants.

Constant	Return Data Type	Description
vCenter	Text (string)	Returns the name of a virtualization server that manages a host, storage or VM.
Today	Date and time	Returns the current date and time in the `YYYY-MM-DDThh:mm:ss` format.