

Veeam ONE

Version 10a

Working with Alarms

July, 2020

© 2020 Veeam Software.

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

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

NOTE:

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

Contents

CONTACTING VEEAM SOFTWARE	5
ABOUT THIS DOCUMENT	6
ABOUT ALARMS	7
How Alarms Work.....	8
Alarm Rules.....	9
Alarm Severity.....	11
Alarm Assignment Options	12
Alarm Notification Options	13
Alarm Remediation Actions	14
Advanced Alarm Options	15
Alarm Reports	16
CONFIGURING ALARMS.....	17
Creating Alarms.....	18
Step 1. Select Alarm Object Type.....	19
Step 2. Specify General Alarm Settings.....	21
Step 3. Specify Alarm Rules.....	22
Step 4. Specify Alarm Assignment Scope.....	31
Step 5. Specify Alarm Notification Options	34
Step 6. Specify Alarm Remediation Actions	36
Step 7. Configure Alarm Suppression Settings	37
Step 8. Specify Alarm Details	39
Step 9. Save Alarm Settings	40
Modifying Alarms.....	41
Adding Alarm Rule from Task or Event	43
Adding Alarm Rules from Performance Counters	44
Changing Alarm Assignment Scope	45
Modifying Alarm Assignment Scope	46
Excluding Single Objects from Alarm Assignment Scope	48
Excluding Multiple Objects from Alarm Assignment Scope	49
Excluding Objects from Multiple Alarms.....	51
Viewing Alarm Exclusions.....	53
Copying Alarms	54
Disabling and Enabling Alarms	55
Deleting Alarms	56
Exporting and Importing Alarms.....	57
Suppressing Alarms.....	59

Maintenance Mode	60
Alarm-Specific Suppression Settings	63
Suppressing Guest Disk Space Alarms.....	64
Modeling Alarm Number	65
Configuring Alarm Notifications	67
Configuring Email Notifications	68
Configuring SNMP Traps.....	84
WORKING WITH TRIGGERED ALARMS.....	90
Viewing Triggered Alarms	91
Resolving Alarms	93
Resolving Individual Alarms	94
Resolving Multiple Alarms.....	95
Notifications on Resolved Alarms	96
Acknowledging Alarms.....	97
Acknowledging Individual Alarms.....	98
Acknowledging Multiple Alarms.....	99
Notifications on Acknowledged Alarms	100
Approving Alarm Remediation Actions	101
Approving Actions for Individual Alarms.....	102
Approving Actions for Multiple Alarms.....	103
Viewing Alarm History.....	104
Exporting Triggered Alarms	105
WORKING WITH INTERNAL ALARMS.....	106
Viewing Internal Alarms	107
Configuring Internal Alarms	108
APPENDIX A. ALARMS	109
Veeam Backup & Replication Alarms	110
VMware vSphere Alarms	119
Microsoft Hyper-V Alarms	156
Internal Alarms	176
APPENDIX B. ALARM RULES.....	182
Alarm Rules for VMware vSphere	183
Alarm Rules for Microsoft Hyper-V.....	191
Alarm Rules for Veeam Backup & Replication	196
Rules for Internal Alarms.....	201
APPENDIX C. REMEDIATION ACTIONS	202

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 at www.veeam.com/support.html 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 offices location, visit www.veeam.com/contacts.html.

Online Support

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

- Full documentation set: www.veeam.com/documentation-guides-datasheets.html
- Community forum at forums.veeam.com

About This Document

This document describes how to work with Veeam ONE alarms for Veeam Backup & Replication, VMware vSphere, and Microsoft Hyper-V infrastructures. It provides instructions on configuring alarms, enabling alarm notifications and working with triggered alarms in Veeam ONE Monitor.

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 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:

- VMware vSphere and vCloud Director alarms
- Microsoft Hyper-V alarms
- Veeam Backup & Replication 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.

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 Monitor 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 Monitor 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 Monitor 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 Monitor 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

For rules based on resource usage counters, Veeam ONE allows to select an 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.

Aggregation Type	Condition	
	Above	Below
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](#).

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 Veeam ONE 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 Veeam ONE 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 details on installing and configuring Veeam ONE agents, see section [Managing Veeam ONE Agents](#) of the Veeam ONE Monitor User Guide.

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 Reporter 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 Reporter Guide](#).

Configuring Alarms

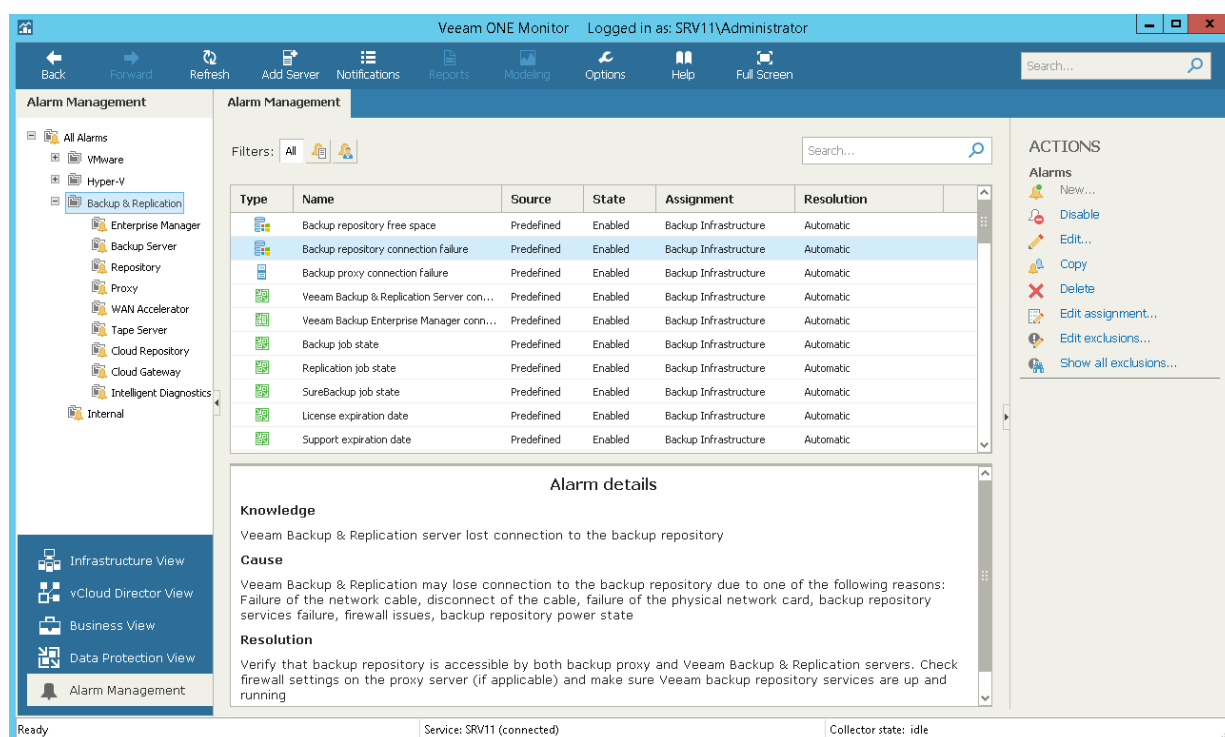
Veeam ONE comes with a set of predefined alarms that cover most common monitoring scenarios. You can customize predefined alarms or create new alarms to meet specific monitoring conditions.

To access the list of alarms:

1. Open Veeam ONE Monitor.

For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

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, vCloud Director components, Veeam Backup & Replication 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 Monitor.

For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

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 Monitor.

For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

2. Choose the necessary view — Infrastructure view, vCloud Director View, Business View or Data Protection 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, choose **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 Monitor.

For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

2. Select the necessary view — Infrastructure view, vCloud Director View, Business View or Data Protection 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](#).

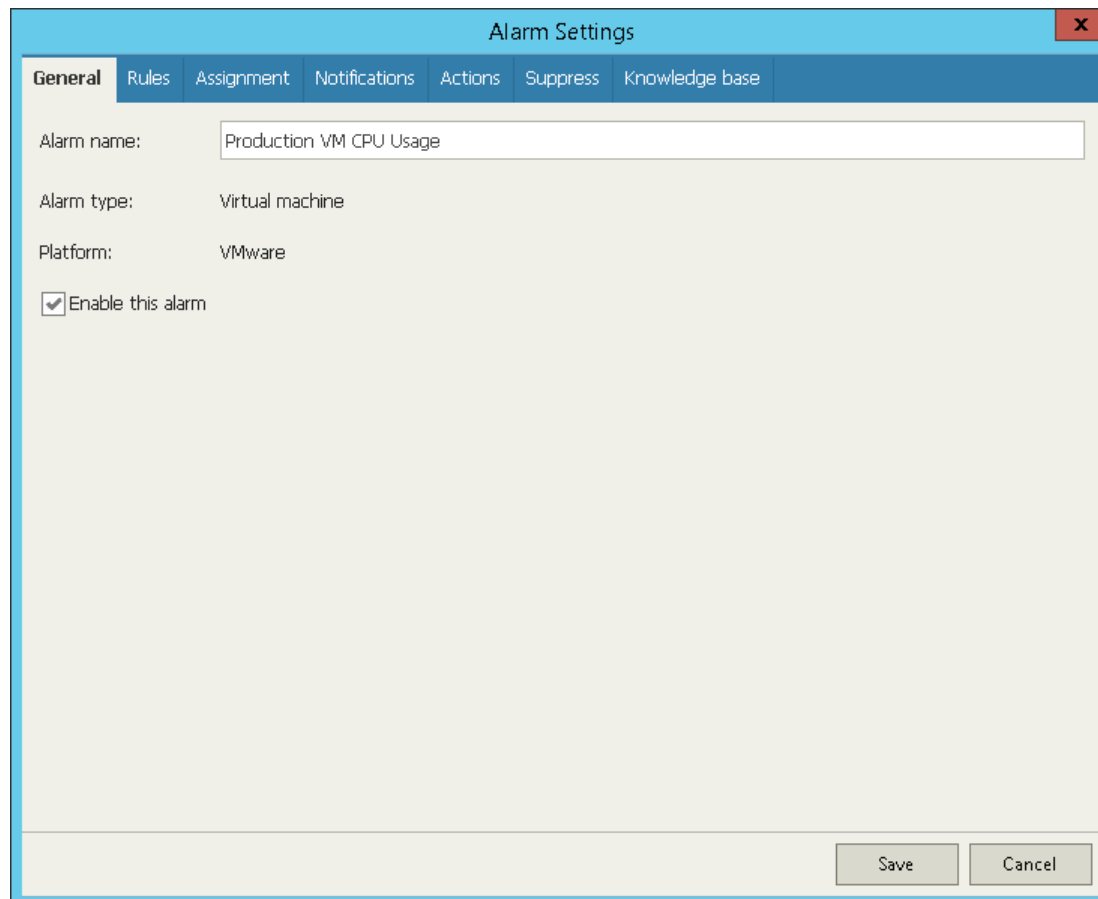
1. Open Veeam ONE Monitor.
For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.
2. Choose the necessary view — Infrastructure view, vCloud Director View, Business View or Data Protection View.
3. In the object tree, select an object for which you want to create 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.



The screenshot shows the 'Alarm Settings' window with the 'General' tab selected. The window has a title bar with a close button (X). Below the title bar is a tabbed interface with tabs for 'General', 'Rules', 'Assignment', 'Notifications', 'Actions', 'Suppress', and 'Knowledge base'. The 'General' tab is active, showing the following fields:

- Alarm name:** A text box containing 'Production VM CPU Usage'.
- Alarm type:** A dropdown menu set to 'Virtual machine'.
- Platform:** A dropdown menu set to 'VMware'.
- Enable this alarm:** A checked checkbox.

At the bottom right of the window are two buttons: 'Save' and 'Cancel'.

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 **Rule for specific conditions or state**.
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 unselect this check box, the rule settings will be saved, but the rule will be disregarded.

7. Click **Finish**.

Alarm Settings

General Rules Assignment Notifications Actions Suppress Knowledge base

Add New Rule

Define Rule
Specify the resource usage thresholds for this alarm

Choose Rule Type

Define Rule

Counter: CPU Usage (%)

When counter stays: Above

For the following time period: 15 min

Warning: 70 %

Error: 80 %

Aggregation: Avg

☒ Enable this rule

Previous Next Finish Cancel

Save Cancel

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](#).
 - 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 unselect this check box, the rule settings will be saved, but the rule will be disregarded.

4. Click **Finish**.

The screenshot shows the 'Add New Rule' dialog box within the 'Alarm Settings' application. The dialog has a title bar with a close button. Below the title bar is a tabbed interface with 'General', 'Rules', 'Assignment', 'Notifications', 'Actions', 'Suppress', and 'Knowledge base'. The 'Rules' tab is active. Inside the 'Rules' tab, there is a 'Define Rule' section. This section has a sidebar on the left with 'Choose Rule Type' and 'Define Rule' options. The 'Define Rule' section contains the following fields and controls:

- Event name:** A text box containing 'VeeamBpSbSessionErrorEvent'.
- Event text:** A text box containing '*'.
- Severity:** A dropdown menu with 'Error' selected.
- Ignore after:** A text box with '1' and up/down arrows.
- Trigger after:** A text box with '0' and up/down arrows.
- Enable this rule:** A checked checkbox.

At the bottom of the dialog, there are buttons for 'Previous', 'Next', 'Finish', 'Cancel', 'Save', and 'Cancel'.

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**.

The screenshot shows the 'Alarm Settings' window with the 'Rules' tab selected. A modal dialog titled 'Add New Rule' is open, showing the 'Define Rule' step. The dialog has a sidebar with 'Choose Rule Type' and 'Define Rule' options. The 'Define Rule' section contains the following fields:

- Alarm name:** A dropdown menu showing 'High memory usage'.
- Delay time:** A numeric input field with '5' and a unit dropdown menu showing 'min'.
- Enable this rule:** A checked checkbox.

At the bottom of the dialog are buttons for 'Previous', 'Next', 'Finish', and 'Cancel'. At the bottom of the main window are buttons for 'Save' and 'Cancel'.

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 Monitor, 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 Monitor Guide.
- Names of drives must be specified with the backward slash, for example, C:\; Z:\.

5. Click **Finish**.

The screenshot shows the 'Alarm Settings' dialog box with the 'Rules' tab selected. Inside, the 'Add New Rule' window is open, displaying the 'Define Rule' configuration. The rule is named 'Disk/ESXi: Datastore Command Aborts (N...)'. The configuration includes: 'Counter' set to 'Disk/ESXi: Datastore Command Aborts (N...)', 'When counter stays' set to 'Above', 'For the following time period' set to '15 min', 'Warning' threshold set to '3', 'Error' threshold set to '5', 'Aggregation' set to 'Avg', and 'Exclude instances' set to an empty field. The 'Enable this rule' checkbox is checked. At the bottom of the 'Add New Rule' window are buttons for 'Previous', 'Next', 'Finish', and 'Cancel'. At the bottom of the main 'Alarm Settings' window are 'Save' and 'Cancel' buttons.

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:
 - **AND** – if rules are linked with this operator, the alarm is triggered when conditions for all linked rules are met.
 - **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.

The screenshot shows the 'Alarm Settings' window with the 'Rules' tab selected. The window contains two rules linked together with an 'AND' operator. The first rule is 'VM snapshot age' with a value of 72 hours and a severity of Warning. The second rule is 'VM snapshots count' with warning and error thresholds of 3 and 5 respectively. The rules are linked with an 'AND' operator. The window includes tabs for General, Rules, Assignment, Notifications, Actions, Suppress, and Knowledge base. On the right, there are buttons for Add..., Move up, Move down, Link..., Unlink, and Remove. At the bottom are Save and Cancel buttons.

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.

The screenshot shows the 'Alarm Settings' dialog box with the 'Rules' tab selected. The dialog has a title bar with a close button (X) and a tab bar with 'General', 'Rules', 'Assignment', 'Notifications', 'Actions', 'Suppress', and 'Knowledge base'. The 'Rules' tab contains a list of rules, each with a checkbox on the left. The first rule is selected and expanded, showing its configuration: 'Rule type: VM snapshot age', 'VM snapshot age: 72 hour', 'Severity: Warning', and a status of 'Enabled'. Below this is an 'AND' operator. The second rule is also expanded, showing 'Rule type: VM snapshots count', 'Warning, snapshots number: 3', 'Error, snapshots number: 5', and a status of 'Enabled'. To the right of the rules list are buttons: 'Add...', 'Move up', 'Move down', 'Link...', 'Unlink', and 'Remove'. The 'Unlink' button is highlighted with a mouse cursor. At the bottom right are 'Save' and 'Cancel' buttons.

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**.

The screenshot shows the 'Alarm Settings' dialog box with the 'Rules' tab selected. The dialog has a blue header bar with a close button (X) in the top right corner. Below the header is a tabbed interface with tabs for 'General', 'Rules', 'Assignment', 'Notifications', 'Actions', 'Suppress', and 'Knowledge base'. The 'Rules' tab is active, displaying a list of rules. The first rule is 'VM snapshot age' with a severity of 'Warning'. The second rule is 'VM snapshots count' with a severity of 'Warning' and a snapshots number of 3. The 'Remove' button is highlighted with a mouse cursor. The 'Save' and 'Cancel' buttons are at the bottom right.

Rule type	VM snapshot age	VM snapshot age	Severity	Warning, snapshots number	Error, snapshots number
<input type="checkbox"/>	VM snapshot age	72	Warning		
<input checked="" type="checkbox"/>	VM snapshots count	3	Warning	3	5

Buttons: Add..., Move up, Move down, Link..., Unlink, Remove, Save, Cancel

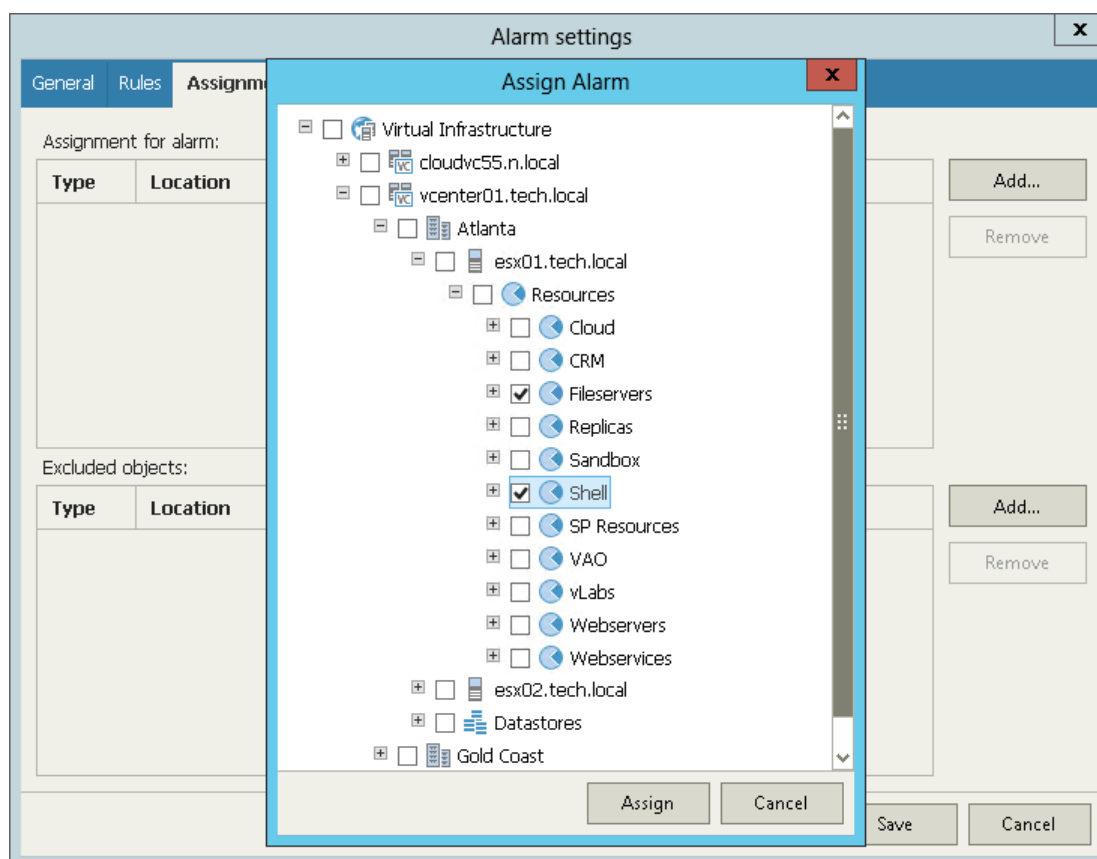
Step 4. Specify Alarm Assignment Scope

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:

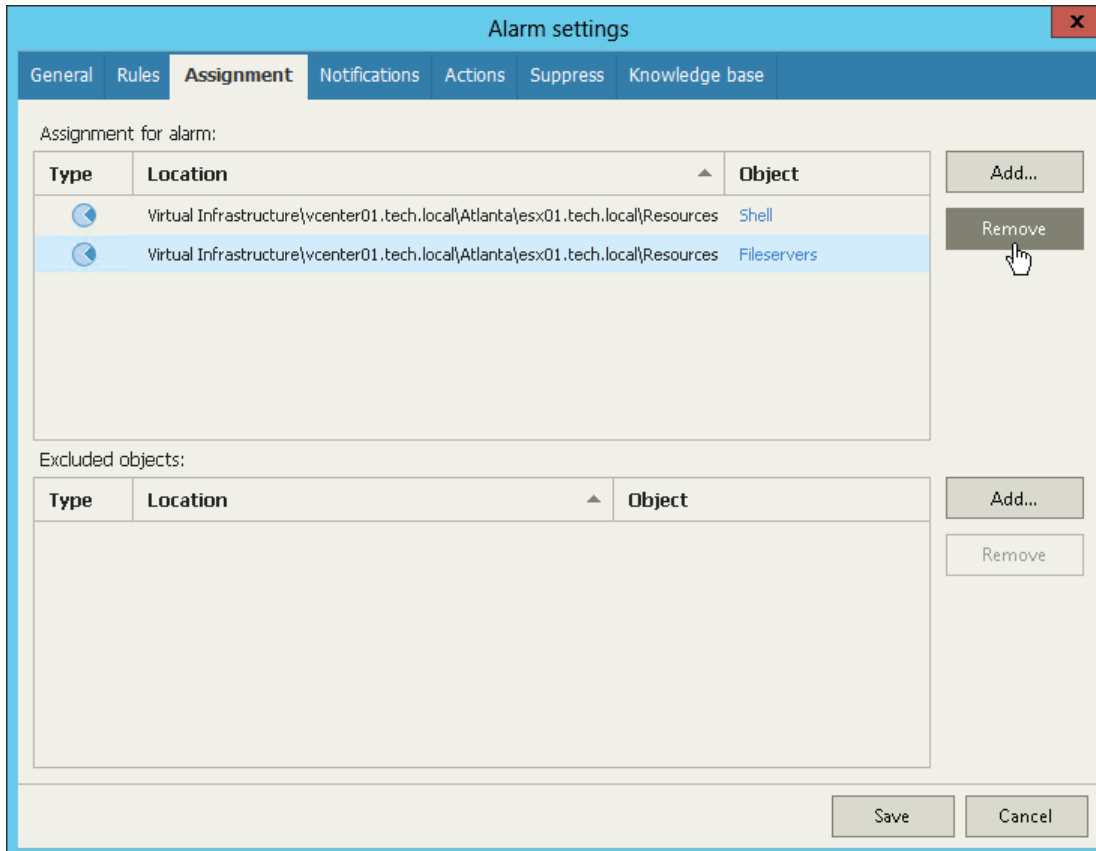
1. On the **Assignment** tab, in the **Assignment for alarm** section, click **Add** and select the necessary node – Infrastructure tree, Business View, vCloud Director View, or Data Protection View.
2. In the **Assign Alarm** window, select check boxes next to objects to which you want to assign the 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**.

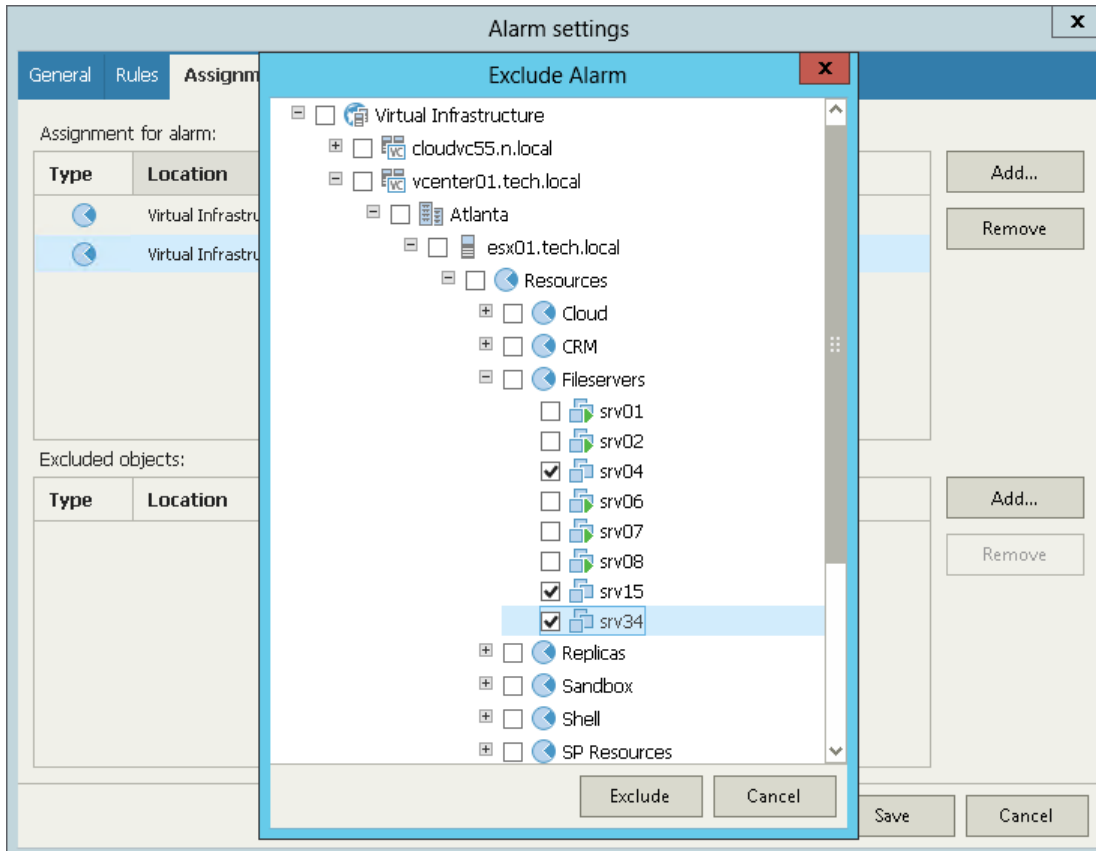


Excluding Objects from Alarm Assignment Scope

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 – Infrastructure tree, Business View, vCloud Director View, or Data Protection 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 Monitor Configuration Wizard or in Veeam ONE Monitor 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:

- **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](#).
- **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 Veeam ONE Business View group settings. For details, see [Configuring Multiple-Condition Categorization](#).
- **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](#).
- **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](#).
- **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 – time; %5 – alarm status; %6 – previous alarm status.

2. In the **Condition** field, specify when the action must be performed:

- **Errors and warnings** — select this option if the action must be performed every time when the alarm status changes to *Error* or *Warning*.
- **Errors only** — select this option if the action must be performed every time when the alarm status changes to *Error*.

- **Resolved** – select this option if the action must be performed every time when the alarm status changes to *Resolved*.
- **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.

Alarm Settings [X]

General Rules Assignment **Notifications** Actions Suppress Knowledge base

Notifications are sent when alarms with the corresponding severity are triggered. Use the list below to define notification options.

Action	Value	Condition
Send email to a default group		Any state
Send email notification	administrator@veeam.com	Errors and warnings
Send email to Business View...		Any state

Buttons: Add, Remove

Dropdown menu options (for the third row):

- Send email to a default group
- Send email to Business View group owner
- Send email notification
- Send SNMP trap
- Run script

Buttons: Save, Cancel

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.

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.

The screenshot shows the 'Alarm Settings' window with the 'Actions' tab selected. The window has a title bar with a close button (X) and a tab bar with 'General', 'Rules', 'Assignment', 'Notifications', 'Actions' (selected), 'Suppress', and 'Knowledge base'. Below the tab bar, a message states: 'Actions are performed when alarms with the corresponding severity are triggered. Click Add to define actions.' There are two action configuration blocks. The first block has 'Action' set to 'Run script', 'Execution type' set to 'By Approval', 'Severity' set to 'Warning', and 'Path to script' set to 'C:\\Scripts\\warning.bat'. The second block has 'Action' set to 'Run script', 'Execution type' set to 'Automatic', 'Severity' set to 'Error', and 'Path to script' set to 'C:\\Scripts\\error.bat'. To the right of these blocks are 'Add' and 'Remove' buttons. At the bottom of the window are 'Save' and 'Cancel' buttons.

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 with the corresponding severity and will 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.

Alarm Settings

General

Rules

Assignment

Notifications

Actions

Suppress

Knowledge base

Suppress when certain task is performed:

☒ Veeam Backup activity

☐ Snapshot creation

☐ Snapshot deletion

Suppress alarm based on schedule:

Day

Start time

End time

Comment

Add

Sunday

10:30 AM

12:00 AM

maintenance

State	Day	Start time	End time	Comment	
<input checked="" type="checkbox"/>	Sunday	10:30 AM	12:00 AM	maintenance	Edit Delete
<input checked="" type="checkbox"/>	Friday	12:30 PM	5:00 PM	performance tests	Edit Delete

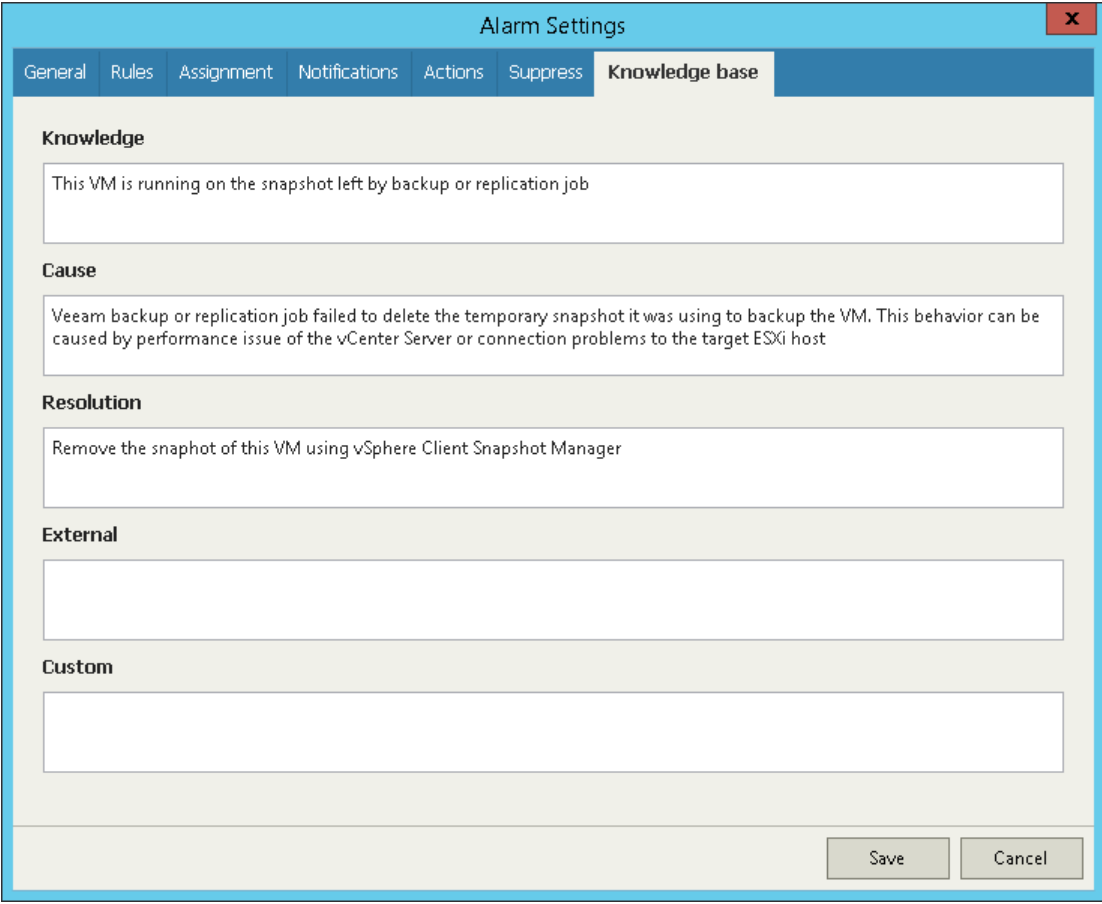
Save

Cancel

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 Monitor, 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.



The screenshot shows the 'Alarm Settings' window with the 'Knowledge base' tab selected. The window has a blue header bar with the title 'Alarm Settings' and a close button. Below the header is a tab bar with 'General', 'Rules', 'Assignment', 'Notifications', 'Actions', 'Suppress', and 'Knowledge base'. The 'Knowledge base' tab is active, showing five text input fields: 'Knowledge', 'Cause', 'Resolution', 'External', and 'Custom'. The 'Knowledge' field contains the text 'This VM is running on the snapshot left by backup or replication job'. The 'Cause' field contains the text 'Veeam backup or replication job failed to delete the temporary snapshot it was using to backup the VM. This behavior can be caused by performance issue of the vCenter Server or connection problems to the target ESXi host'. The 'Resolution' field contains the text 'Remove the snapshot of this VM using vSphere Client Snapshot Manager'. The 'External' and 'Custom' fields are empty. At the bottom right of the window are 'Save' and 'Cancel' buttons.

Tab	Field	Content
Knowledge base	Knowledge	This VM is running on the snapshot left by backup or replication job
	Cause	Veeam backup or replication job failed to delete the temporary snapshot it was using to backup the VM. This behavior can be caused by performance issue of the vCenter Server or connection problems to the target ESXi host
	Resolution	Remove the snapshot of this VM using vSphere Client Snapshot Manager
	External	
	Custom	

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 Monitor.
For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.
2. At the bottom of the inventory pane, click **Alarm Management**.
3. Select an alarm from the list and do either of the following:
 - Double click the alarm.
 - Right-click the alarm and choose **Edit** from the shortcut menu.
 - 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 Infrastructure View, Business View, vCloud Director View, or Data Protection View.

1. Open Veeam ONE Monitor.
For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.
2. At the bottom of the inventory pane, click the necessary view — Infrastructure View, Business View, vCloud Director View, or Data Protection 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:
 - Right-click the alarm and select **Edit alarm** from the shortcut menu.
 - 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 Monitor.
For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

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:
 - Right-click the selected alarms and click **Edit** in the shortcut menu.
 - 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 event '*Create virtual machine*' and notifies you whenever a new VM is created.

To create a new rule from a task or event:

1. Open Veeam ONE Monitor.

For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

2. At the bottom of the inventory pane, click the necessary view — Infrastructure View, Business View, vCloud Director View, or Data Protection 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 Monitor.
For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.
2. At the bottom of the inventory pane, click the necessary view — Infrastructure View, Business View, vCloud Director View, or Data Protection 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. VCloud Director alarms apply to the root vCloud 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.

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 Monitor.

For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

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:
 - Right-click the alarm and select **Edit assignment** from the shortcut menu.
 - 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:
 - **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.
 - **Business View** — choose this option if you want to assign the alarm to custom categorization groups that you have configured in Veeam ONE 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.
 - **vCloud Director View** — choose 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.
 - **Data Protection 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, vCloud Director and Veeam ONE 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 Veeam ONE Business View groups: the alarm type must match the Business View category type. You cannot assign an alarm of the Host type to a Veeam ONE 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 Monitor.

For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

2. At the bottom of the inventory pane, click the necessary view — Infrastructure View, Business View, vCloud Director View, or Data Protection View.
3. In the information pane, open the **Alarms** tab.
4. Select the necessary alarm in the list and do either of the following:
 - Right-click the alarm and select **Exclude** from the shortcut menu.
 - In the **Actions** pane on the right, click **Exclude**.

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 Monitor.

For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

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:
 - Right-click the alarm and select **Edit exclusions** from the shortcut menu.
 - In the **Actions** pane on the right, click **Edit exclusions**.
4. In the **Edit exclusions** window, click **Add** and choose objects that you want to exclude from the assignment scope:

- **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.

- **Business View** — choose this option if you want to assign the alarm to custom categorization groups that you have configured in Veeam ONE 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.

- **vCloud Director View** — choose 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.

- **Data Protection 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, vCloud Director and Veeam ONE 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 Infrastructure View, Business View, vCloud Director View, or Data Protection View.

1. Open Veeam ONE Monitor.

For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

2. At the bottom of the inventory pane, click the necessary view — Infrastructure View, Business View, vCloud Director View, or Data Protection 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.

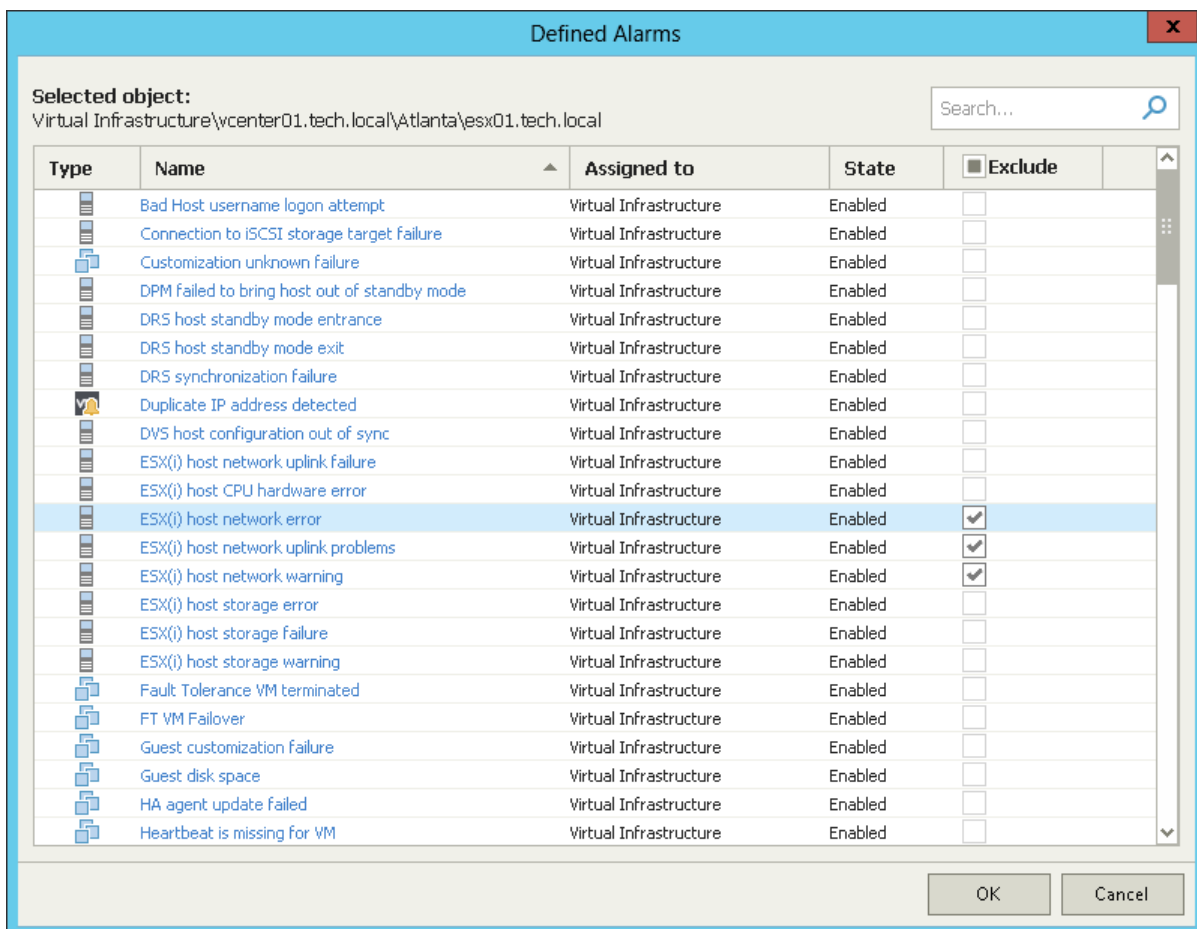
Excluding Objects from Multiple Alarms

You can exclude a single infrastructure object from the scope of multiple alarms:

1. Open Veeam ONE Monitor.
For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.
2. At the bottom of the inventory pane, click the necessary view – Infrastructure View, Business View, vCloud Director View, or Data Protection 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:
 - Right-click the alarm and select **Defined alarms** in the shortcut menu.
 - In the **Actions** pane on the right, click **Defined alarms**.

Alternatively, you can right-click the object in the inventory pane and select **Alarms > Exclude** from the shortcut menu.

6. In the **Defined 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 Monitor.




For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

2. At the bottom of the inventory pane, click the necessary view — Infrastructure View, Business View, vCloud Director View, or Data Protection View.
3. In the inventory pane, right-click the necessary object in the inventory pane and select **Alarms > Exclude** from the shortcut menu.
4. In the **Defined 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 Monitor.
For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.
- 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.

All exclusions			
Type	Location	Object	Alarm Name
	Virtual Infrastructure\vcenter01.tech.l...	esx02.tech.local	ESX(i) host network uplink problems
	Virtual Infrastructure\vcenter01.tech.l...	esx02.tech.local	ESX(i) host network error
	Virtual Infrastructure\vcenter01.tech.l...	esx02.tech.local	ESX(i) host network warning

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, vCloud Director objects, Veeam ONE Business View groups, or Veeam Backup & Replication infrastructure components.

To copy an alarm:

1. Open Veeam ONE Monitor.

For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

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:

- Right-click the selection and click **Copy** from the shortcut menu.
- 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 Monitor.
For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.
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:
 - Right-click the selection and select **Disable** from the shortcut menu.
 - 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 Monitor.
For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.
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:
 - Right-click the selection and select **Enable** from the shortcut menu.
 - 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 Monitor.
For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.
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:
 - Right-click the selection and choose **Delete** from the shortcut menu.
 - 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 10a supports import of alarm settings that were exported from Veeam ONE 8.0 and 9.0.

Exporting Alarms

To export alarms to an XML file:

1. Open Veeam ONE Monitor.
For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.
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:

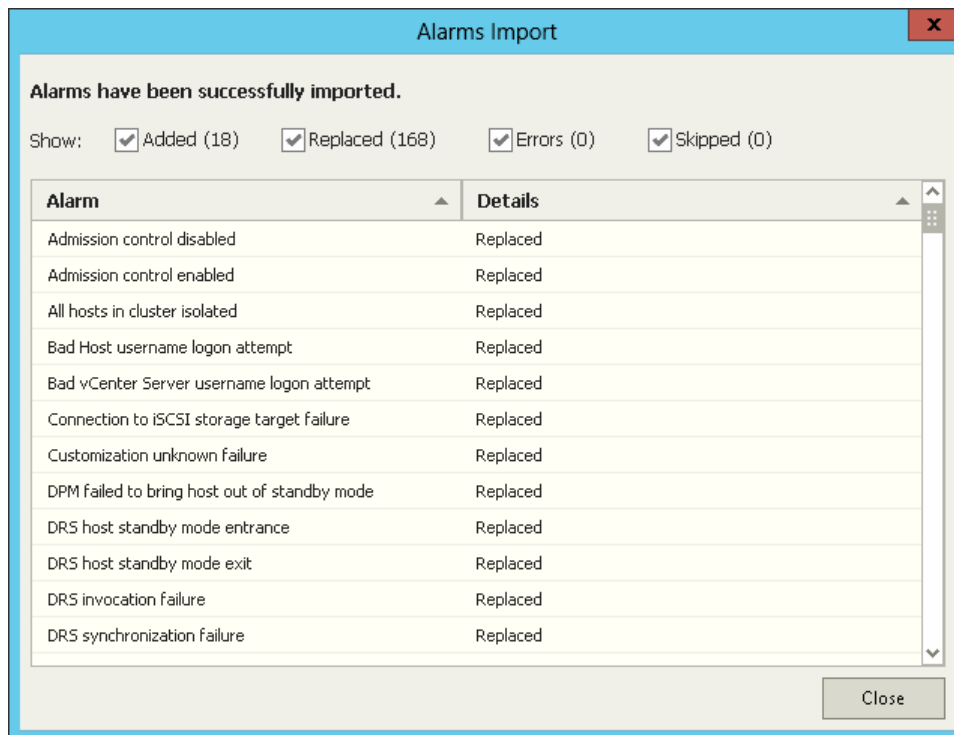
1. Open Veeam ONE Monitor.
For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.
2. At the bottom of the inventory pane, click **Alarm Management**.
3. In the alarm management tree, right-click any object and choose **Import Alarms** from the shortcut menu.
4. In the **Alarms Import** window:
 - Specify a path to an XML file with alarm settings.
 - Select the **Import assignment** check box if you want to import a list of alarms together with their assignment settings.
 - 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.

- When the import is finished, the **Alarm 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 **Import Alarms** 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 Monitor.

For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

2. At the bottom of the inventory pane, click the necessary view — Infrastructure View, Business View, vCloud Director View, or Data Protection 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:

- 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.
- 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 Monitor.

For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

2. At the bottom of the inventory pane, click the necessary view — Infrastructure View, Business View, vCloud Director View, or Data Protection 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**.

Schedule Maintenance Mode

Add maintenance schedule date or edit existing

☐ Type: Monthly, Day: 10, Start time: 6:00 AM, End time: 10:30 AM, ☒ Enabled, ☒ Apply to child objects. Comment (optional): Planned monthly maintenance for production servers.

☐ Type: Once, Date: 09/30/2016, Start time: 10:00 PM, End time: 12:00 PM, ☒ Enabled, ☒ Apply to child objects. Comment (optional): Updates and patches.

Buttons: Add, Delete, OK, Cancel.

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 Monitor.
For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.
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](#).

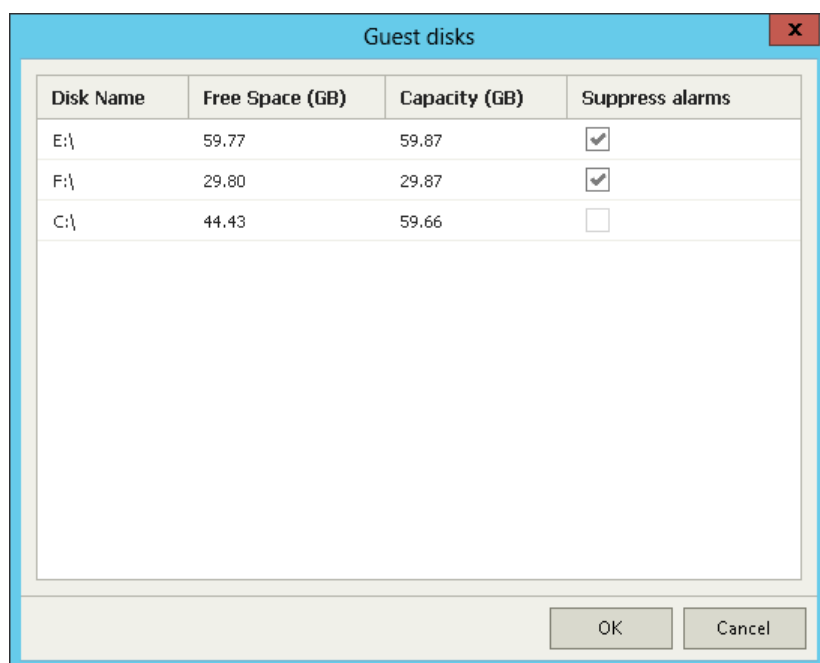
Suppressing Guest Disk Space Alarms

You can suppress *Guest disk space* alarms for specific VM guest OS disks:

1. Open Veeam ONE Monitor.

For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

2. At the bottom of the inventory pane, click the necessary view – Infrastructure View, Business View or vCloud Director 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

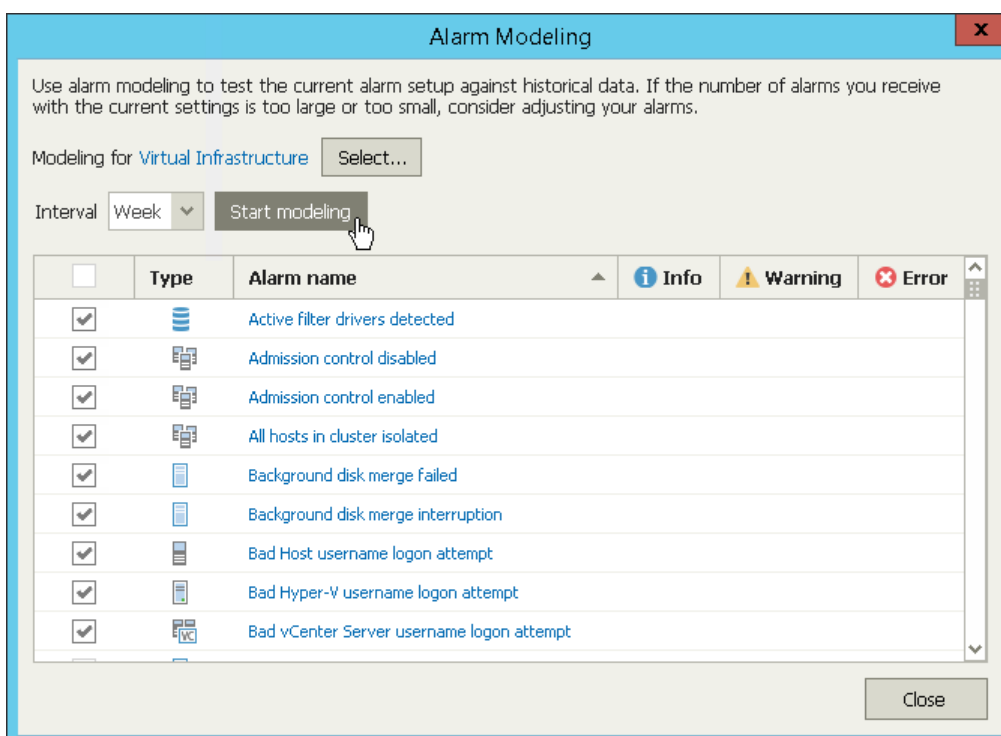
Alarm modeling allows you to forecast the number and type of alarms that will be sent for a specific infrastructure object within a specified time interval. To model the alarm number, Veeam ONE applies the current alarm settings to historical data collected for the selected infrastructure object, and 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 Monitor.
For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.
2. On the toolbar, click **Modeling**.
3. In the **Alarm Modeling** window, click **Select** and choose the necessary type of infrastructure objects – Infrastructure View, vCloud Director, Business View or Data Protection 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. In the **Use data for the past** list, specify 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 Monitor.
For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.
2. At the bottom of the inventory pane, click the necessary view – Infrastructure View, vCloud Director, Business View or Data Protection View.
3. In the inventory pane, right-click an infrastructure object and select **Alarms > Modeling** from the shortcut menu.
4. In the **Use data for the past** list, specify 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 Monitor.
For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.
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. In the **Alarm Modeling** window, click **Select** and choose the necessary type of infrastructure objects – Infrastructure View, vCloud Director, Business View or Data Protection 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. In the **Use data for the past** list, specify 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 Monitor.

For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

2. On the toolbar, click **Options** and select **Server Settings**.

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

3. In the **SMTP server** field, specify DNS name or IP address of the SMTP server that must be used for sending email notifications.

4. In the **Port** field, change the SMTP communication port if required.

The default port number is 25.

5. 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.

6. For an SMTP server with SSL support, select **Enable SSL security** to enable SSL data encryption.

7. If your SMTP server requires authentication, select the **Use authentication** check box and specify authentication credentials in the **Login** and **Password** fields.

The screenshot shows the 'Server Settings' dialog box with the 'SMTP Settings' tab selected. The dialog has a title bar with a close button (X). Below the title bar is a tabbed interface with the following tabs: 'SMTP Settings' (active), 'Notification Policy', 'SNMP', 'Credentials', 'Monitored Datastores', 'Monitored VMs', 'Business View', and 'Other'. The 'SMTP server settings:' section contains the following fields and controls:

- SMTP server:** Text field containing 'mail.veeam.com'.
- Port:** Text field containing '25'.
- From:** Text field containing 'one@veeam.com'.
- ☒ **User secure connection**
- ☒ **Use authentication**
- Login:** Text field containing 'administrator@veeam.com'.
- Password:** Password field with masked characters '.....'.
- Send test email...** button.

The 'Email format:' section contains the following controls:

- Text: 'Send email notifications in this format:'
- ☒ **HTML**
- ☐ **Plain Text** (KB Articles will not be included)

At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

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.

The screenshot shows the 'Server Settings' window with the 'SMTP Settings' tab selected. The 'SMTP server settings' section contains the following fields: 'SMTP server' (mail.veeam.com), 'Port' (25), 'From' (one@veeam.com), 'Login' (administrator), and 'Password' (masked with dots). There are two checked checkboxes: 'Use secure connection' and 'Use authentication'. A 'Test email settings' dialog box is overlaid on top, prompting the user to 'Enter email address to send test message to:' with the input field containing 'john.smith@veeam.com'. The dialog has 'OK' and 'Cancel' buttons. Below the SMTP settings is the 'Email format' section with two radio buttons: 'HTML' (selected) and 'Plain Text (KB Articles will not be included)'. At the bottom of the 'Server Settings' window are 'OK' and 'Cancel' buttons.

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:

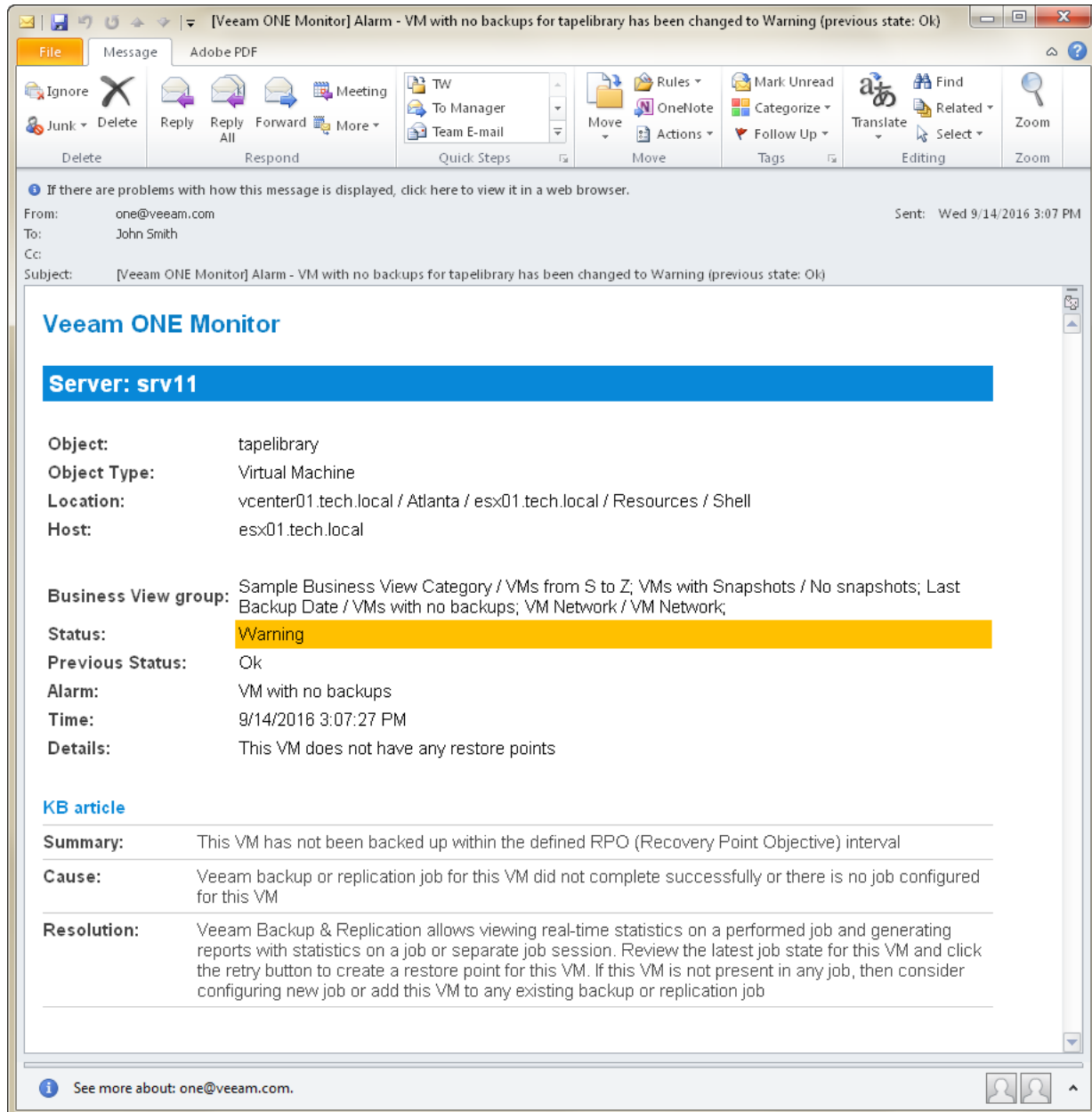
- [Mission Critical](#)
- [Other](#)

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.



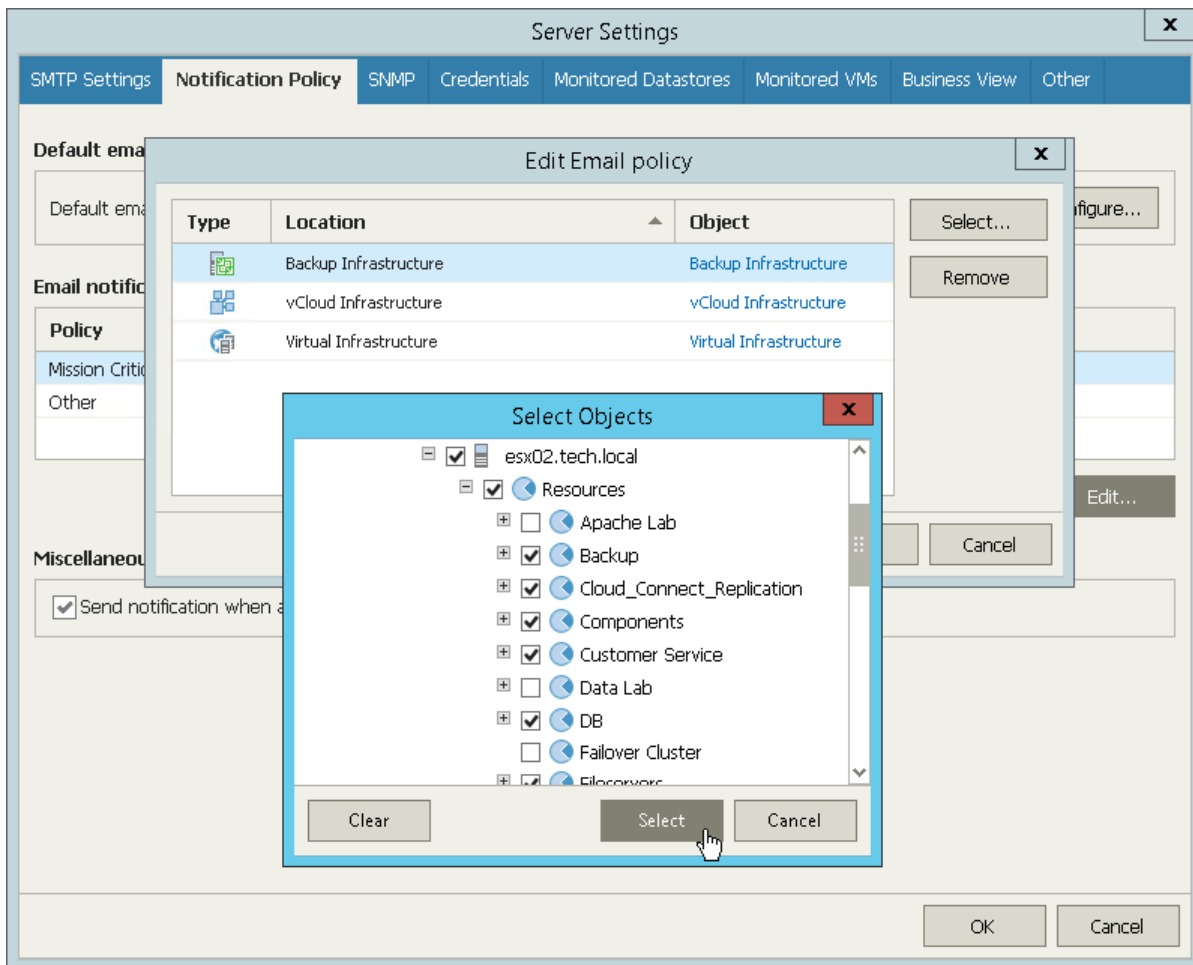
To apply the **Mission Critical** notification policy to an infrastructure object:

1. Open Veeam ONE Monitor.
For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.
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 following options:
 - **Infrastructure Tree** – browse the virtual infrastructure hierarchy and select check boxes next to objects or infrastructure segments to which the policy settings must apply.

- **Business View** – browse the Veeam ONE Business View hierarchy and select check boxes next to groups or infrastructure objects to which the policy settings must apply.
- **Data Protection View** – browse the Veeam Backup & Replication infrastructure and select check boxes next to infrastructure components to which the policy settings must apply.
- **vCloud Director View** – browse the vCloud Director infrastructure and select check boxes next to infrastructure components to which the policy settings must apply.

6. In the **Select Objects** window, click **Select**.

7. In the **Edit Email Policy** window, Click **OK**.

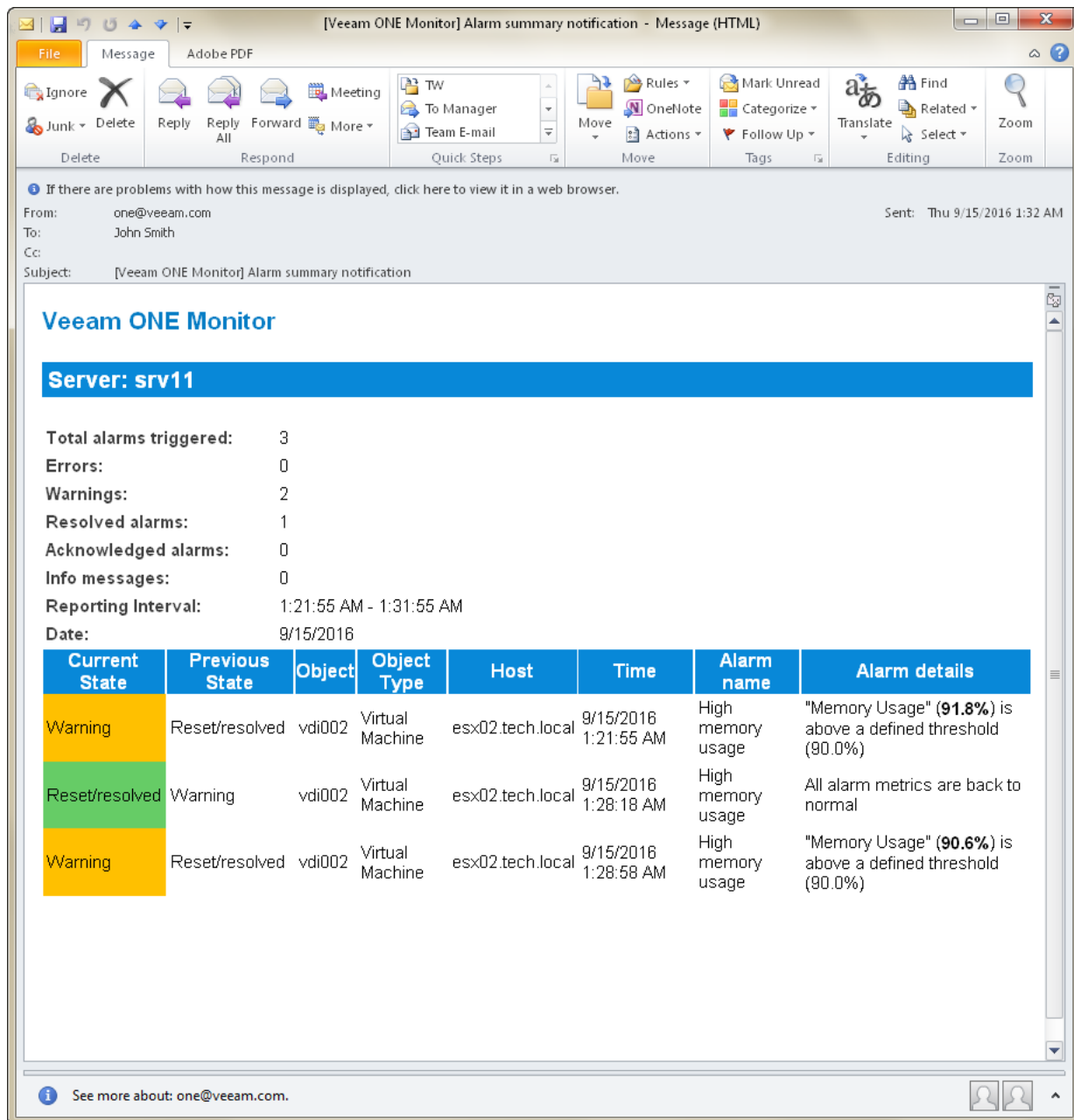


Enabling Summary Notifications

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 Monitor.
For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.
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 – Virtual Infrastructure, vCloud Infrastructure or Backup Infrastructure) 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 Monitor.

For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

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**.

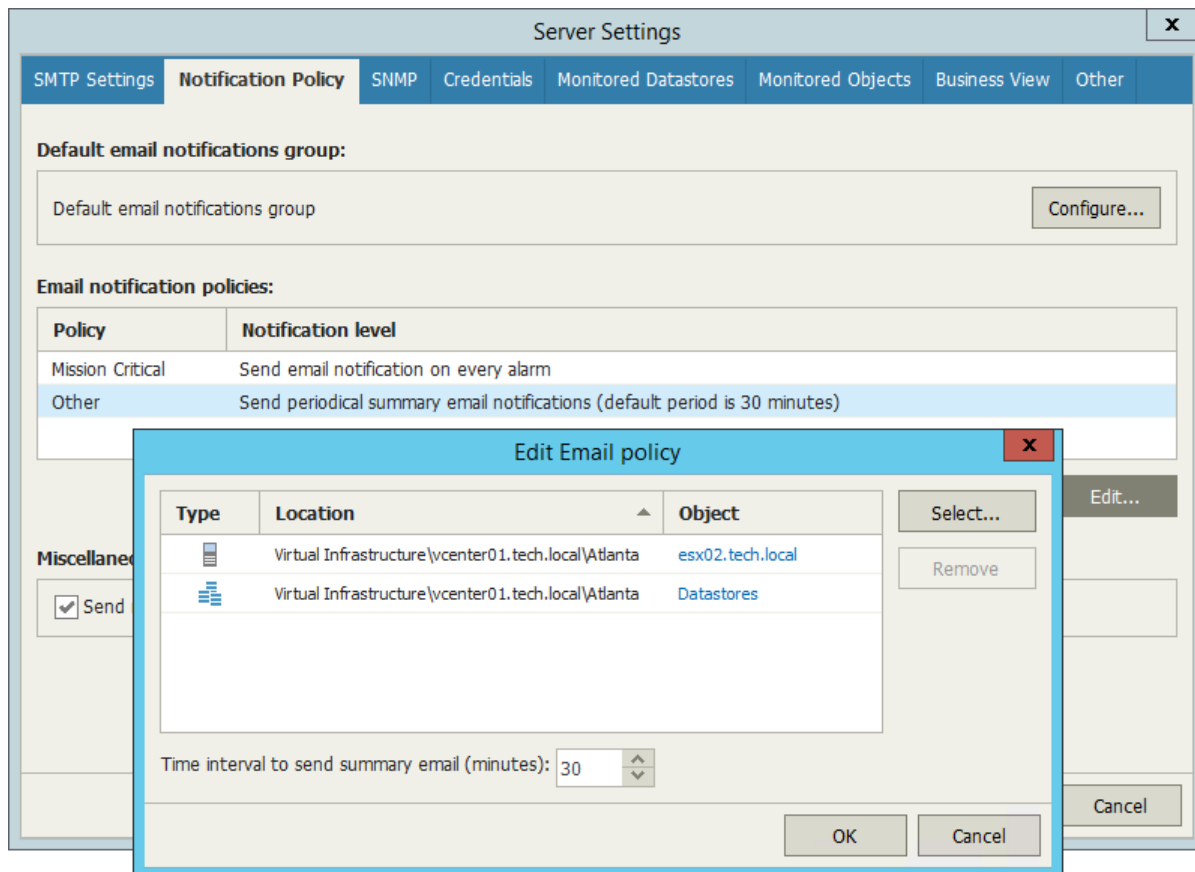
5. In the **Edit Email Policy** window, click **Select** and choose one of the following options:

- **Infrastructure Tree** — browse the virtual infrastructure hierarchy and select check boxes next to objects or infrastructure segments to which the policy settings must apply.
- **Business View** — browse the Veeam ONE Business View hierarchy and select check boxes next to groups or infrastructure objects to which the policy settings must apply.
- **Data Protection View** — browse the Veeam Backup & Replication infrastructure and select check boxes next to infrastructure components to which the policy settings must apply.
- **vCloud Director View** — browse the vCloud Director infrastructure and select check boxes next to infrastructure components to which the policy settings must apply.

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 Monitor.
For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.
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
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.

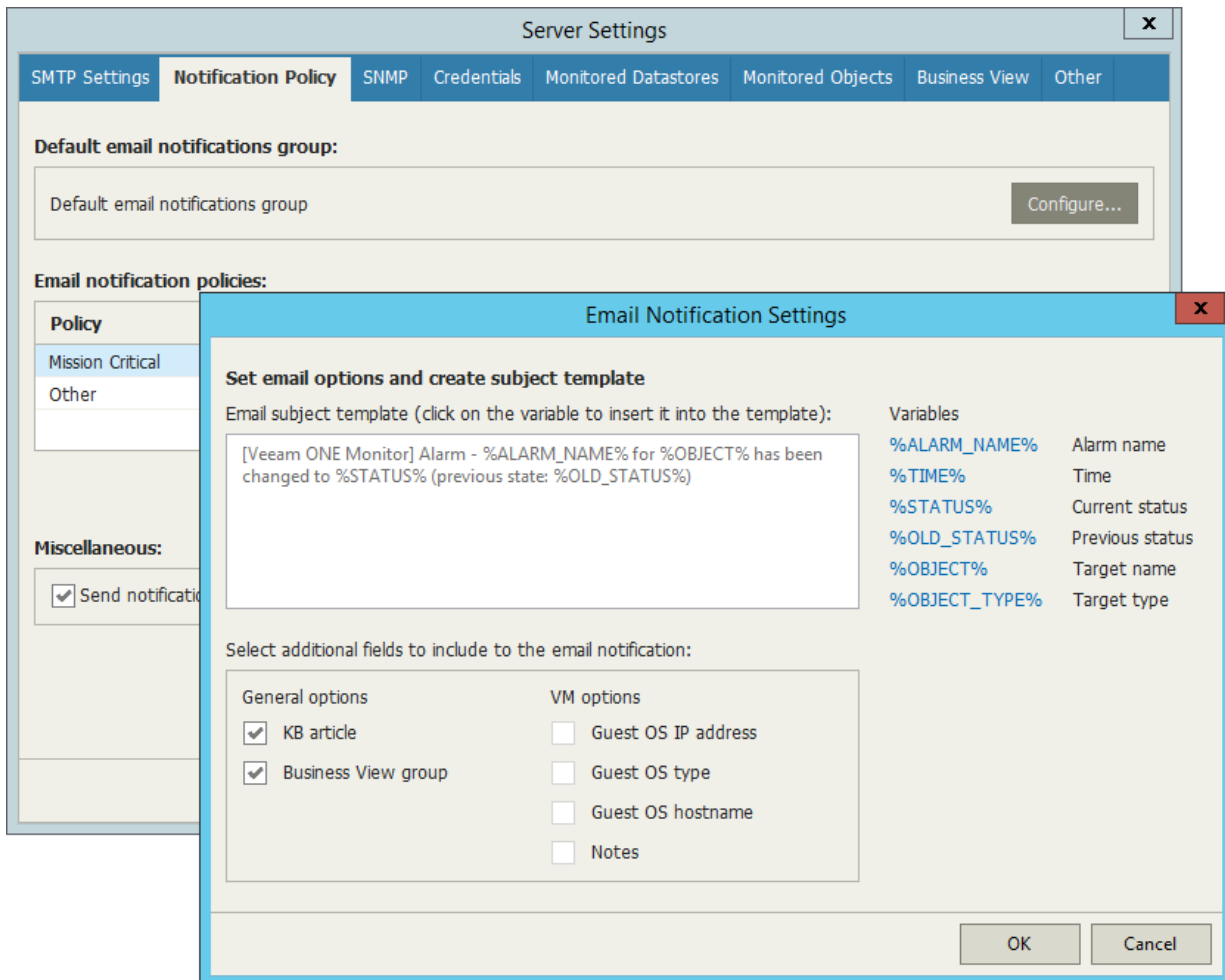
- **KB article** – select this check box if an email notification must include a knowledge base article.
- **Business View group** – select this check box if an email notification must include a category assigned to the object in Veeam ONE Business View.

VM options apply to email notifications for VM alarms.

- **Guest OS IP address** – select this check box if an email notification must include IP and MAC addresses of the affected VM.

- **Guest OS type** – select this check box if an email notification must include information about the guest OS of the affected VM.
- **Guest OS hostname** – select this check box if an email notification must include a DNS name of the affected VM.
- **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 Monitor.
For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.
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.

The screenshot shows the 'Server Settings' dialog box with the 'SMTP Settings' tab selected. The 'SMTP server settings' section contains fields for 'SMTP server' (mail.veeam.com), 'Port' (25), 'From' (one@veeam.com), 'Login' (administrator@veeam.com), and 'Password' (masked with dots). There are checkboxes for 'User secure connection' and 'Use authentication', both of which are checked. A 'Send test email...' button is located below the password field. The 'Email format' section has a label 'Send email notifications in this format:' and two radio buttons: 'HTML' (selected) and 'Plain Text (KB Articles will not be included)'. A mouse cursor is pointing at the 'HTML' radio button. At the bottom right, there are 'OK' and 'Cancel' buttons.

Server Settings

SMTP Settings | Notification Policy | SNMP | Credentials | Monitored Datastores | [TBD]Monitored VMs | Business View | Other

SMTP server settings:

SMTP server: mail.veeam.com Port: 25

From: one@veeam.com

☒ User secure connection

☒ Use authentication

Login: administrator@veeam.com

Password:

Send test email...

Email format:

Send email notifications in this format:

☒ HTML ☐ Plain Text (KB Articles will not be included)

OK Cancel

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 Monitor.

For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

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**.

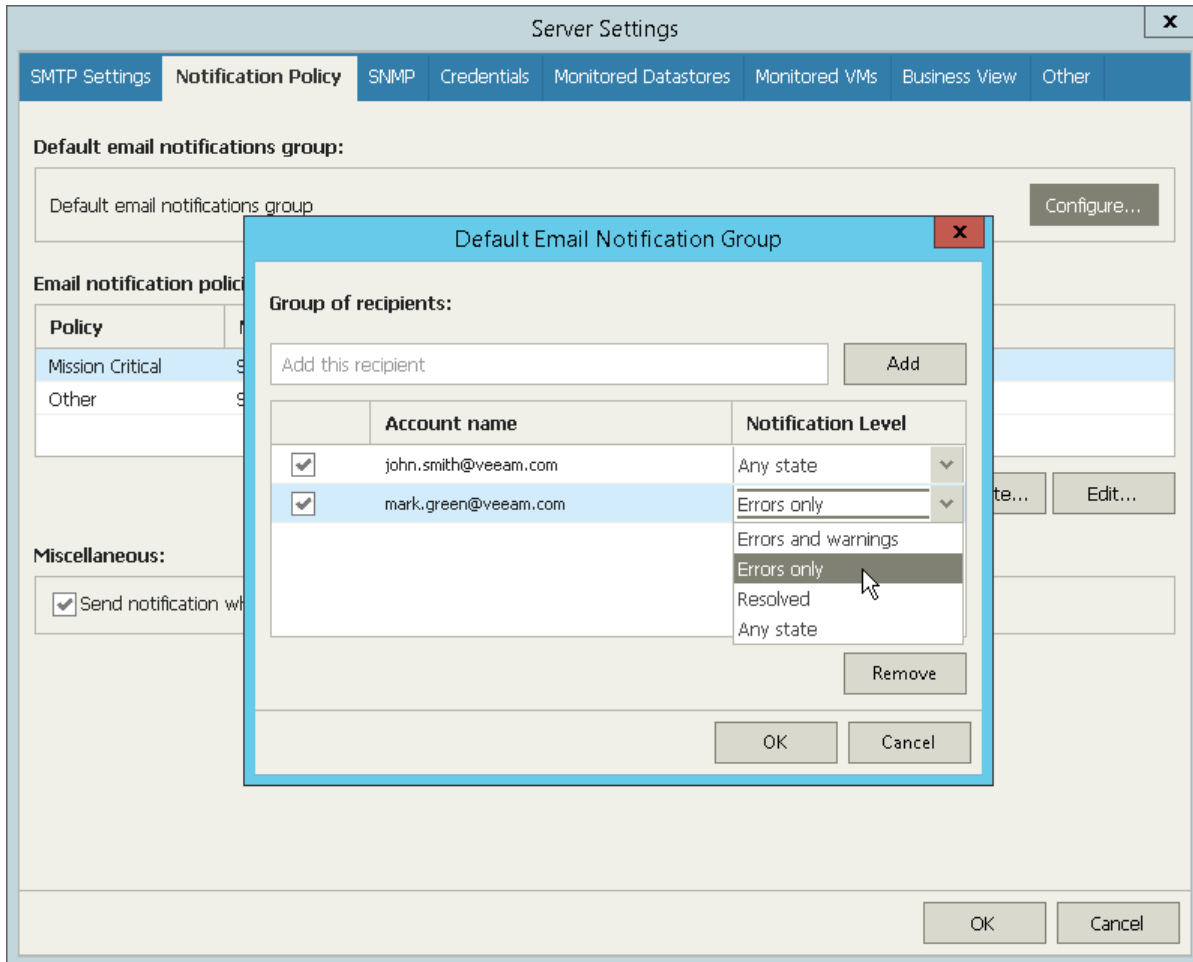
5. In the **Default Email Notification Group** window, specify email addresses of notification recipients.

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*.

- 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.

- In the **Default Email Notification Group** window, clear the check box next to recipient email address.
- Click **OK**.

To permanently remove a recipient from the default email notification group:

- In the **Default Email Notification Group** window, select an email address you want to delete and click **Remove**.
- 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:

- Open Veeam ONE Monitor.
For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.
- 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 **Actions** tab.

5. On the **Actions** 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**.

The screenshot shows the 'Alarm Settings' window with the 'Notifications' tab selected. The window has a title bar with a close button (X) and a tabbed interface with 'General', 'Rules', 'Assignment', 'Notifications' (active), 'Actions', 'Suppress', and 'Knowledge base'. Below the tabs, a text box states: 'Notifications are sent when alarms with the corresponding severity are triggered. Use the list below to define notification options.'

Action	Value	Condition
Send email to a default group		Any state
Send email notification	administrator@veeam.com	Errors and warnings
Send email notification		Any state

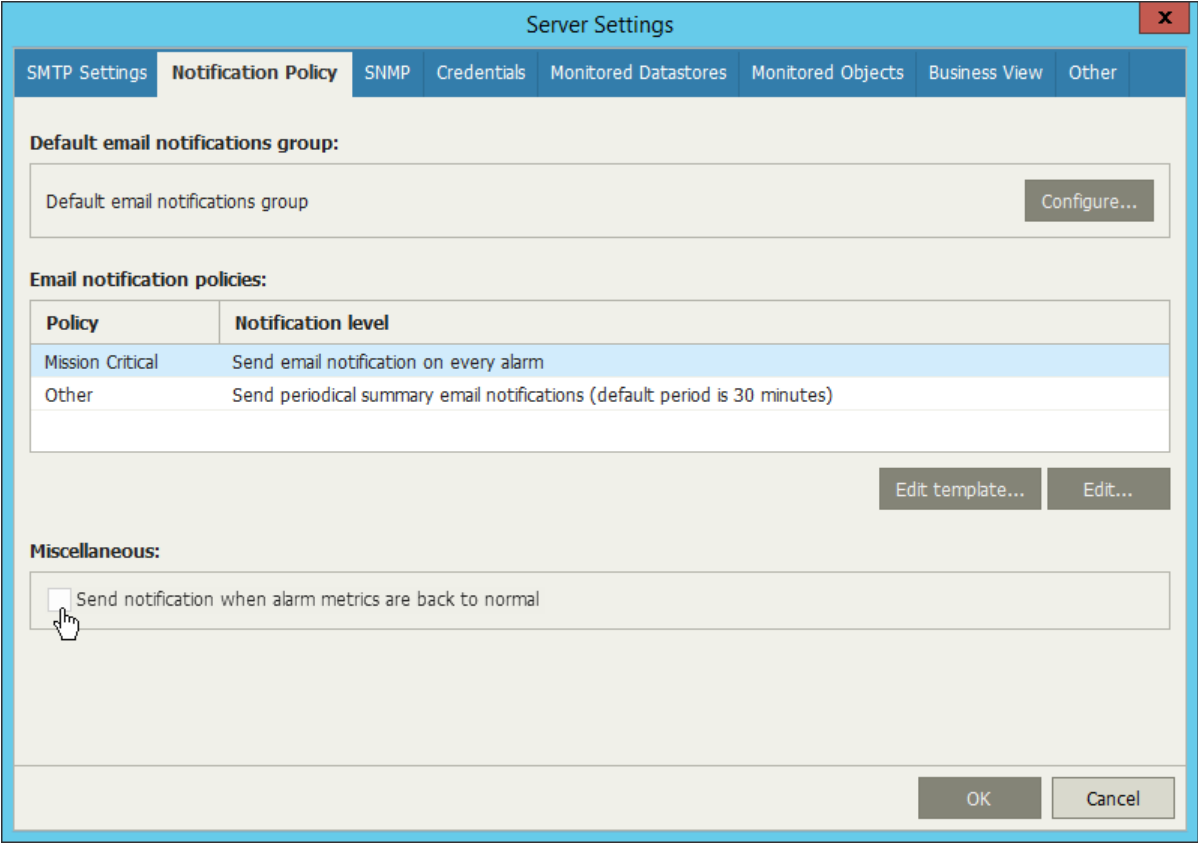
On the right side of the table, there are 'Add' and 'Remove' buttons. The 'Condition' dropdown for the third row is open, showing options: 'Any state', 'Errors and warnings', 'Errors only', 'Resolved', and 'Any state' (highlighted). At the bottom of the window are 'Save' and 'Cancel' buttons.

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 Monitor.
For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.
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**.



The screenshot shows the 'Server Settings' window with the 'Notification Policy' tab selected. The window has a blue title bar and a tabbed interface. The 'Notification Policy' tab is active, showing settings for email notifications. The 'Default email notifications group' section has a text field and a 'Configure...' button. The 'Email notification policies' section contains a table with two rows: 'Mission Critical' and 'Other'. The 'Miscellaneous' section at the bottom has a checkbox labeled 'Send notification when alarm metrics are back to normal', which is currently unchecked. The 'OK' and 'Cancel' buttons are at the bottom right.

Policy	Notification level
Mission Critical	Send email notification on every alarm
Other	Send periodical summary email notifications (default period is 30 minutes)

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.

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. For example, to learn how to configure an SNMP receiver in Windows Server, see [SNMP Traps in Windows Server](#). 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 Monitor.

For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

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:

- 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**.

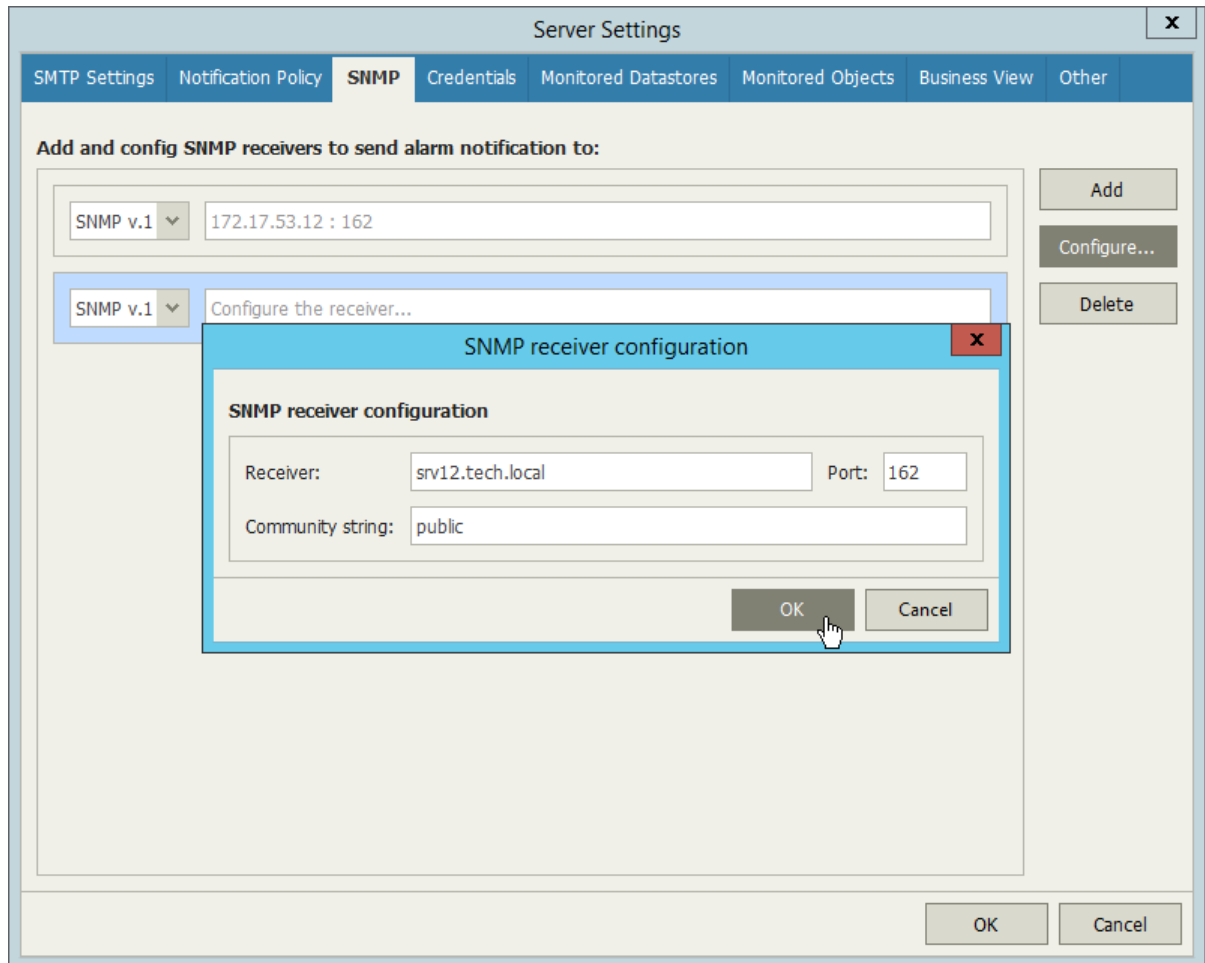
- ii. In the **Receiver** field, specify FQDN or IP address of the SNMP receiver.

- 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 Monitor.
For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.
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 necessary 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 **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**.

Alarm Settings

General Rules Assignment **Notifications** Actions Suppress Knowledge base

Notifications are sent when alarms with the corresponding severity are triggered. Use the list below to define notification options.

Action	Value	Condition
Send email to a default group		Any state
Send SNMP trap		Errors and warnings

Errors and warnings
Errors only
Resolved
Any state

Add Remove

Save Cancel

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 Monitor.
For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.
2. At the bottom of the inventory pane, click the necessary view – Infrastructure View, Business View, vCloud Director View, or Data Protection 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.

The screenshot displays the Veeam ONE Monitor interface. The top navigation bar includes buttons for Back, Forward, Refresh, Add Server, Notifications, Reports, Modeling, Options, Help, and Full Screen. The main content area is divided into three panes. The left pane shows the Infrastructure View with a tree structure of objects. The middle pane shows the Alarms tab for the selected object, displaying a table of alarms with columns for Status, Time, Source, Type, Name, Repeat Count, and Remediation. The right pane shows the ACTIONS section with various alarm management options. Below the table, there is an 'Alarm details' section with Description, Knowledge, Cause, and Resolution information.

Status	Time	Source	Type	Name	Repeat Count	Remediation
Warning	6:35:45 PM	srv-49	VM	VM total disk latency	129	
Warning	6:35:20 PM	esx01-das2	Datastore	Datastore write later	126	
Warning	6:32:55 PM	VBR04	VM	VM total disk latency	88	
Warning	6:32:55 PM	tapelibrary	VM	VM total disk latency	57	
Warning	6:32:32 PM	esx01-das3	Datastore	Datastore write later	107	
Warning	6:30:09 PM	esx01-das3	Datastore	Datastore read later	145	
Warning	6:23:44 PM	esx01-ds-hpvsa	Datastore	Datastore write later	62	
Warning	6:23:44 PM	esx01-ds-hpvsa	Datastore	Datastore read later	23	

Alarm details

Description
"Datastore Highest Latency" (74.0 Milliseconds) is above a defined threshold (50.0 Milliseconds)

Knowledge
Highest latency value across all disks used by the VM

Cause
Response times for read and write operations for this VM in the last collection interval has exceeded the configured threshold

Resolution
View VM latency for historical information. If your Guest OS workload is disk-intensive, consider relocating this VM to another datastore

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 a corresponding 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.

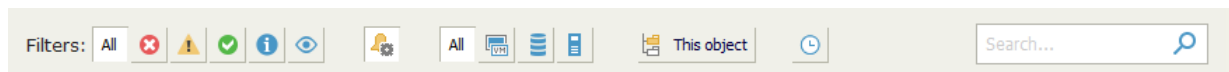
For more information on remediation actions, see [Alarm Remediation Actions](#).

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 display or hide alarms with a specific severity, click the **Status** icons – *Show all alarms*, *Show objects with errors*, *Show objects with warnings*, *Show resolved alarms*, *Show information messages*, and *Show acknowledged messages*.
- To display alarms with configured remediation actions, click the **Show remediable** 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.
- To find alarms by alarm name, use the search field.

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 Monitor.

For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

2. At the bottom of the inventory pane, click the necessary view — Infrastructure View, Business View, vCloud Director View, or Data Protection 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:
 - Right-click the selection and choose **Resolve** from the shortcut menu.
 - In the **Actions** pane, click **Resolve**.

Press and hold the [CTRL] 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 Monitor.

For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

2. At the bottom of the inventory pane, click the necessary view — Infrastructure View, Business View, vCloud Director View, or Data Protection 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:
 - Right-click anywhere in the list of alarms and choose **Resolve all alarms** from the shortcut menu.
 - In the **Actions** pane, click **Resolve all alarms**.
7. 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](#).

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.



Fri 12/28/2018 6:47 PM

Veeam@Notification.com

[Veeam ONE Monitor] Alarm resolve notification

To  Mark Green

Veeam ONE Monitor



Server: srv11

Total alarms resolved:2

Resolve action:Manual

Resolve time:12/28/2018 6:47:07 PM

Resolve reason:Resolved

	Previous State	Object	Object Type	Host	Alarm name
	Warning	esx01-das3	Datastore	esx01.tech.local	Datastore read latency
	Error	srv08	Virtual Machine	esx01.tech.local	VM total disk latency

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 Monitor.

For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

2. At the bottom of the inventory pane, click the necessary view — Infrastructure View, Business View, vCloud Director View, or Data Protection 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:
 - Right-click the selection and choose **Acknowledge**.
 - 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 Monitor.

For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

2. At the bottom of the inventory pane, click the necessary view — Infrastructure View, Business View, vCloud Director View, or Data Protection 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:
 - Right-click anywhere in the list of alarms and choose **Acknowledge all alarms** from the shortcut menu.
 - In the **Actions** pane, click **Acknowledge all alarms**.
7. In the **Acknowledge Alarm** 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.



Fri 12/28/2018 6:46 PM

Veeam@Notification.com

[Veeam ONE Monitor] Alarm acknowledgement notification

To  Mark Green

Veeam ONE Monitor

Server: srv11

Total alarms acknowledged: 6

Acknowledge action: Manual

Acknowledgetime: 12/28/2018 6:46:18 PM

Acknowledges reason: Ok

	Previous State	Object	Object Type	Host	Alarm name
Warning		srv49	Virtual Machine	esx01.tech.local	VM total disk latency
Warning		esx01-das3	Datastore	esx01.tech.local	Datastore write latency
Warning		esx01-das2	Datastore	esx01.tech.local	Datastore write latency
Warning		esx01-das1	Datastore	esx01.tech.local	Datastore write latency
Warning		tapelibrary	Virtual Machine	esx01.tech.local	VM total disk latency
Warning		srv21	Virtual Machine	esx01.tech.local	VM total disk latency

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 Monitor.

Approving Actions for Individual Alarms

To approve actions for individual alarms:

1. Open Veeam ONE Monitor.

For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

2. At the bottom of the inventory pane, click the necessary view — Infrastructure View, Business View, vCloud Director View, or Data Protection 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 remediable** icon.
6. In the list of alarms, select one or more alarms and do either of the following:
 - Right-click the selection and choose **Approve Action** from the shortcut menu.
 - In the **Actions** pane, click **Approve Action**.

Press and hold the [CTRL] or [SHIFT] key to select multiple alarms.

7. In the **Approve Remediation 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**.

Approving Actions for Multiple Alarms

To approve actions for all displayed alarms at once:

1. Open Veeam ONE Monitor.

For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

2. At the bottom of the inventory pane, click the necessary view — Infrastructure View, Business View, vCloud Director View, or Data Protection 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:
 - Right-click anywhere in the list of alarms and choose **Approve all actions** from the shortcut menu.
 - In the **Actions** pane, click **Approve all actions**.
7. In the **Approve Remediation 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 Monitor.

For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

2. At the bottom of the inventory pane, click the necessary view – Infrastructure View, Business View, vCloud Director View, or Data Protection View.
3. In the information pane, open the **Alarms** tab.
4. Select the necessary alarm and do either of the following:
 - Click the **Repeat Count** link in the list of alarms.
 - Double-click the alarm in the list.
 - Right-click the alarm and select **Show history** from the shortcut menu.
 - In the **Actions** pane, click **Show history**.

Alarm history

Alarm name: VM total disk latency
Alarm type: Virtual machine
Node: db01

Status	Time	Rule	Comment
Warning	12/28/2018 6:46:59 PM	"Datastore Highest Latency" (58.0 Milliseconds) is a...	
Resolved	12/28/2018 6:46:47 PM	Resolved by user Administrator	Resolved
Warning	12/28/2018 6:02:44 PM	"Datastore Highest Latency" (52.0 Milliseconds) is a...	
Resolved	12/28/2018 6:01:13 PM	All alarm metrics are back to normal	
Warning	12/28/2018 5:04:19 PM	"Datastore Highest Latency" (51.0 Milliseconds) is a...	
Resolved	12/28/2018 4:57:12 PM	All alarm metrics are back to normal	
Warning	12/28/2018 3:47:53 PM	"Datastore Highest Latency" (51.0 Milliseconds) is a...	
Resolved	12/28/2018 3:40:18 PM	All alarm metrics are back to normal	
Warning	12/28/2018 3:38:27 PM	"Datastore Highest Latency" (53.0 Milliseconds) is a...	
Resolved	12/28/2018 3:36:10 PM	All alarm metrics are back to normal	

Page 1 of 3

Close

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

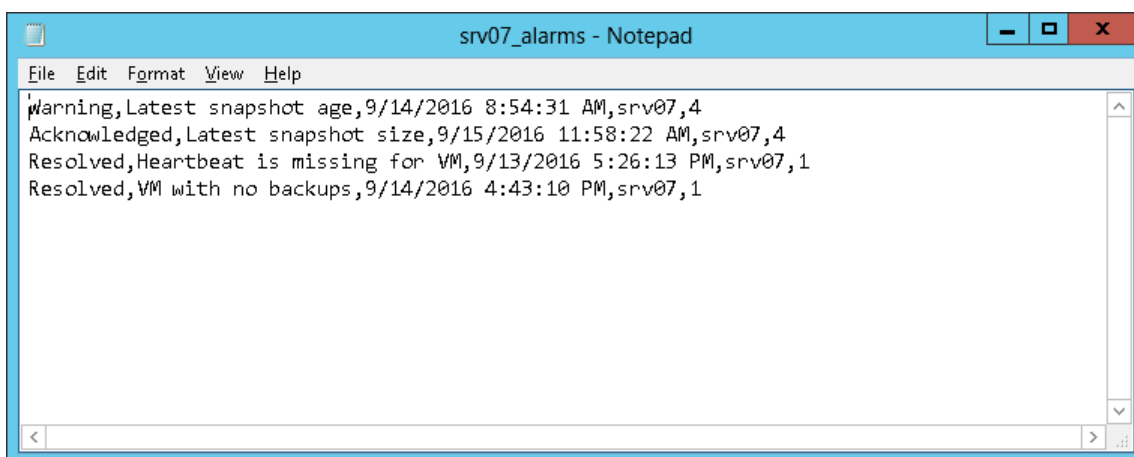
To export one or more triggered alarms to a CSV file:

1. Open Veeam ONE Monitor.

For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

2. At the bottom of the inventory pane, click the necessary view – Infrastructure View, Business View, vCloud Director View, or Data Protection 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 history**.
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](#).

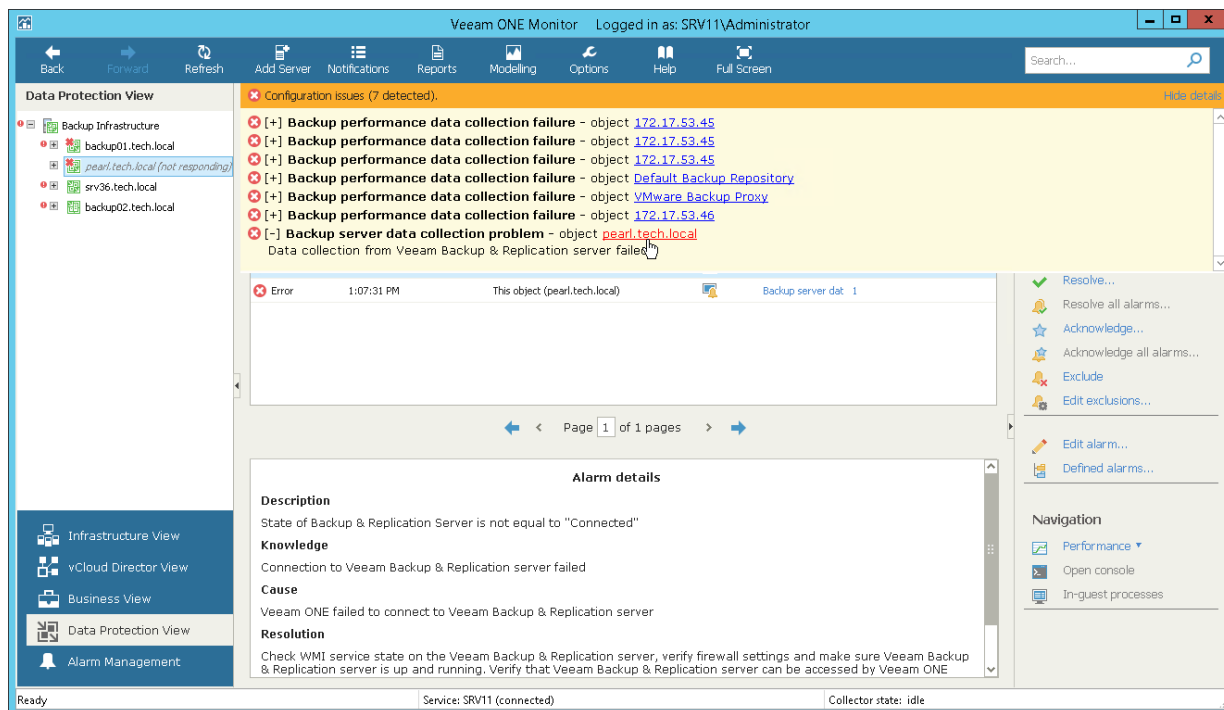
Viewing Internal Alarms

To view Veeam ONE internal alarms:

1. Open Veeam ONE Monitor.

For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

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:

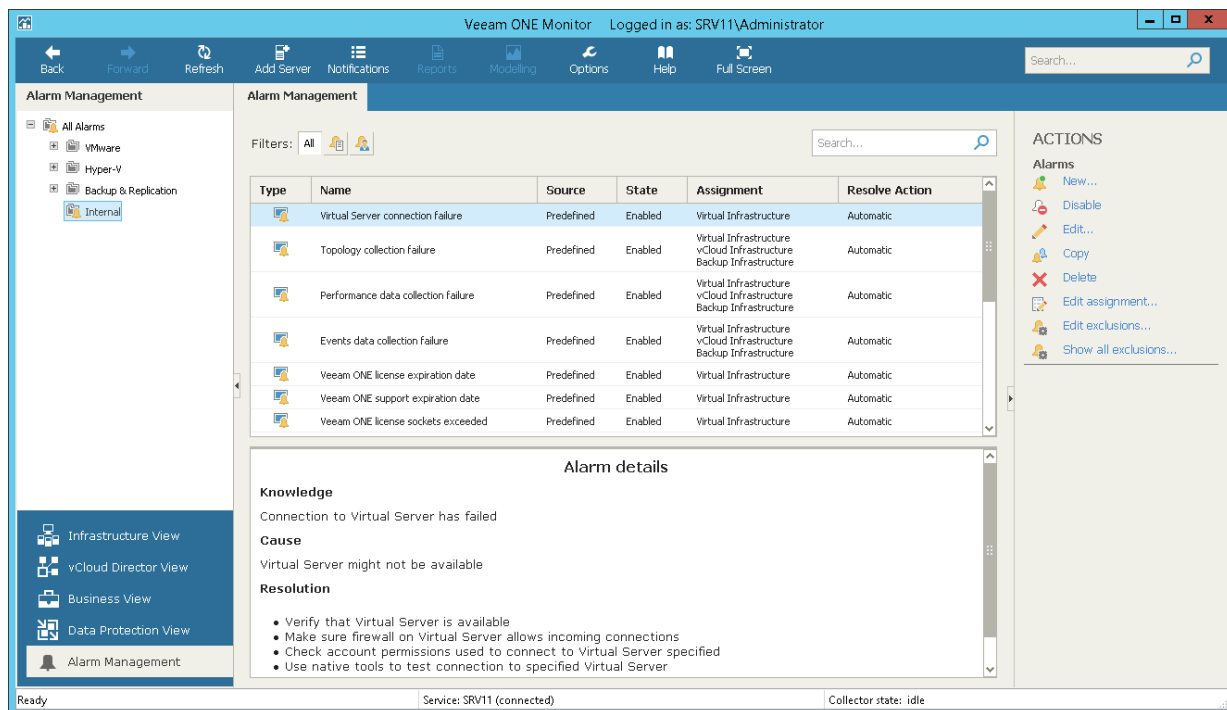
1. Open Veeam ONE Monitor.

For details, see section [Accessing Veeam ONE Monitor](#) of the Veeam ONE Monitor User Guide.

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:
 - Double click the alarm.
 - Right-click the alarm and choose **Edit** from the shortcut menu.
 - In the **ACTIONS** pane, click **Edit**.

5. Change the necessary alarm settings.

For details on working with alarm settings, see [Creating Alarms](#).



Appendix A. 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](#)
- [Backup Server](#)
- [Repository](#)
- [Proxy](#)
- [WAN Accelerator](#)
- [Tape Server](#)
- [Cloud Repository](#)
- [Cloud Gateway](#)
- [Intelligent Diagnostics](#)

Enterprise Manager

Veeam Backup Enterprise Manager connection failure	State does not equal <i>Connected</i> .	Error	Automatic	Veeam ONE failed to connect to Veeam Backup Enterprise Manager.

Veeam Backup & Replication Server

Agent backup job state	State of an agent backup job equals <i>Warning</i> .	Warning	Automatic	One or more computers failed to back up successfully.
	State of an agent backup job equals <i>Failed</i> .	Error		
Agent backup policy session state	State of a backup policy session equals <i>Warning</i> .	Warning	Automatic	One or more computers failed to back up successfully.
	State of a backup policy session equals <i>Failed</i> .	Error		

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 <i>Warning</i> .	Warning	Automatic	One or more objects could not be successfully copied from the backup repository.
	State of an backup copy job equals <i>Failed</i> .	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.
Backup job disabled	Job is disabled for more than 12 hours.	Warning	Automatic	Job is in a disabled state for more than allowed time period.

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 <i>Warning</i> .	Warning	Automatic	One or more VMs failed to back up successfully.
	State of a backup job equals <i>Failed</i> .	Error		
	State of a Nutanix backup job equals <i>Warning</i> .	Warning		
	State of a Nutanix backup job equals <i>Failed</i> .	Error		
Cloud backup policy session state	Status of a cloud backup policy session equals <i>Warning</i> .	Warning	Automatic	Policy finished with warning or error.
	Status of a cloud backup policy session equals <i>Error</i> .	Error		
NAS Backup job state	State of a file-level backup job equals <i>Warning</i> .	Warning	Automatic	One or more file sources failed to back up successfully.
	State of a file-level backup job equals <i>Failed</i> .	Error		
File copy job state	State of a file copy job equals <i>Warning</i> .	Warning	Manual	One or more files failed to be transferred to the destination folder.
	State of a file copy job equals <i>Failed</i> .	Error		

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		
Max allowed job duration	Job duration is more than 480 minutes.	Error	Manual	Job has exceeded its allowed execution time.
	Job duration is more than 120 minutes.	Warning		
Veeam AHV proxy connection failure	Nutanix AHV cluster connection failure.	Error	Automatic	Veeam Backup & Replication server lost connection to proxy appliance on a Nutanix AHV cluster.
Quick Migration job state	Based on event VeeamBpQMMigrationSessionWarningEvent.	Warning	Automatic	One or more VMs failed to migrate to another host.
	Based on event VeeamBpQMMigrationSessionErrorEvent.	Error		
Replication job state	State of a replication job equals <i>Warning</i> .	Warning	Automatic	One or more VMs failed to replicate successfully.
	State of a replication job equals <i>Failed</i> .	Error		

Restore activity	Based on event 290 Veeam MP.	Information	Automatic	Restore session started.
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 <i>Warning</i> .	Warning	Automatic	One or more VMs could not be successfully verified.
	State of a SureBackup job equals <i>Failed</i> .	Error		
Suspicious increment backup size	One of 3 last backup job increment sizes is above 150% of configured threshold.	Warning	Automatic	Newly created restore point size is significantly different from the previously created ones.
	One of 3 last backup job increment sizes is above 200% of configured threshold.	Error		
	One of 3 last agent backup job increment sizes is above 150% of configured threshold.	Warning		
	One of 3 last agent backup job increment sizes is above 200% of configured threshold.	Error		
	One of 3 last agent backup policy increment sizes is above 150% of configured threshold.	Warning		
	One of 3 last agent backup policy increment sizes is above 200% of configured threshold.	Error		
Tape job state	Status of the file to tape backup job equals <i>Warning</i> .	Warning	Manual	One or more VMs or files failed to be transferred
	Status of the file to tape backup job equals <i>Failed</i> .	Error		

	Status of the backup to tape job equals <i>Warning</i> .	Warning		to the tape device.
	Status of the backup to tape job equals <i>Failed</i> .	Error		
Veeam Backup & Replication Server connection failure	State does not equal <i>Connected</i> .	Error	Automatic	Connection to Veeam Backup & Replication server failed.
Veeam Broker Service state	Based on event VeeamBackupServerBrokerServiceDownEvent.	Warning	Automatic	Veeam Broker Service that interacts with virtual infrastructure to collect and cache its topology is not started and not working properly.
	Based on event VeeamBackupServerBrokerServiceDownEvent.	Resolve		
	Based on event VeeamBackupServerBrokerServiceDownEvent.	Resolve		

Repository

Backup repository connection failure	State equals <i>Not accessible</i> for more than 5 minutes.	Error	Automatic	Veeam Backup & Replication server lost connection to the backup repository.
	State equals <i>Partially accessible</i> 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.

Proxy

Backup proxy connection failure	State does not equal <i>Accessible</i> for more than 5 minutes.	Error	Automatic	Veeam Backup & Replication server lost connection to the 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.

WAN Accelerator

WAN accelerator connection state	State does not equal <i>Accessible</i> 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

Tape server connection state	State does not equal <i>Accessible</i> 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

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

Cloud gateway connection state	State does not equal <i>Accessible</i> 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.

Intelligent Diagnostics

List of intelligent diagnostics alarms depends on the set of installed signatures. For details, see [Veeam Intelligent Diagnostics](#).

VMware vSphere Alarms

This section describes predefined alarms for VMware vSphere infrastructure components:

- [vCenter Server](#)
- [Cluster](#)
- [Host](#)
- [Virtual Machine](#)
- [Datastore](#)
- [Any VMware Object](#)
- [vCloud Director vApp](#)
- [vCloud Director Organization](#)
- [vCloud Director Org VDC](#)
- [vCloud Director Provider VDC](#)

vCenter Server

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.
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.
vCenter Server license expired	Based on event ServerLicenseExpiredEvent.	Error	Manual	This event records an expired vCenter Server license.

Cluster

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.
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.	Warning	Manual	One of the hosts in an HA cluster has been isolated.
	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.			

Host

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	<p>This event records that Distributed Power Management tried to bring a host out of standby mode, but failed.</p> <p>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.</p>
	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.
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.	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).
	Based on event esx.problem.net.lacp.uplink.fail.speed.			
	Based on event esx.problem.net.lacp.uplink.inactive.			
ESXi host CPU hardware error	Based on event esx.problem.cpu.amd.mce.dram.disabled.	Error	Manual	ESXi host has experienced a CPU hardware error.
	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.			
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.disconnecte d.			
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.no ne.			
ESXi host storage error	Based on event esx.problem.scsi.device.state.permanent loss.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		
Host available memory	Average memory usage is for 15 minutes is above 80%.	Warning	Automatic	This host is low on available memory.
	Average memory usage is for 15 minutes is above 90%.	Error		
Host connection failure	Host state equals <i>Disconnected</i> 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 <i>Not responding</i> 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		
Host disk SCSI aborts	Average datastore command aborts for 15 minutes is above 2.	Warning	Automatic	This host disk (vmhba) has logged one or more 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	<p>This event records that the host failed to exit standby mode.</p> <p>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.</p>
	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.
	Hardware sensor equals <i>Warning</i> .	Warning	Automatic	One of the hosts' hardware sensors has changed its status.

Host hardware status	Hardware sensor equals <i>Alert</i> .	Error		
	Hardware sensor equals <i>Unknown</i> .	Warning		
Host IP inconsistent	Based on event HostIpInconsistentEvent.	Warning	Manual	This event records that the IP address resolution returned different addresses on the host.
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 connection state	Based on event esx.problem.net.vmnics.linkstate.down.	Error	Automatic	Physical NIC linkstate is down.
	Based on event esx.clear.net.vmnics.linkstate.up.	Resolve		
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.
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		
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.
Network rollback detected	Based on event NetworkRollbackEvent.	Error	Manual	<p>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:</p> <ul style="list-style-type: none"> • 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.
	Based on event vprob.storage.connectivity.lost.	Error	Automatic	The event indicates a loss in connectivity to the specified

Storage connection failure	Based on event esx.problem.storage.connectivity.lost.			storage device. The path indicated is the last path that went down.
	Based on event esx.clear.storage.connectivity.restored.	Resolve		
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	Based on event HostConnectionLostEvent.	Error	Automatic	vCenter Server has lost connection to this host.

lost connection to host	Based on event HostCnxFailed.			
	Based on event HostConnectedEvent.	Resolve		
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

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.
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 customization sequence in the guest failed. Cannot complete customization of VM.
Guest disk space	Guest disk free space space is below 10%.	Warning	Automatic	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.

Heartbeat is missing for VM	Heartbeat not detected for 15 minutes.	Error	Automatic	<p>The heartbeat is the communication to the VMware tools heartbeat running inside the VM.</p> <p>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.</p>
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

	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.

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, would trigger 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.

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	Automatic	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	Automatic	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.

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 might have been 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		

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		

	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

	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.

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 API 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		

VM power status	State not equals <i>Running</i> 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		

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 <i>Unknown</i> .	Warning	Automatic	There is a problem with VMware Tools in this Virtual Machine.
	VMware VM tools state changes equals <i>Out-of-date</i> .	Warning		
	VMware VM tools state changes equals <i>Not installed</i> .	Error		
	VMware VM tools state changes equals <i>Not running</i> .	Error		

Datastore

Datastore free space	Free space is below 10%.	Warning	Automatic	Datastore is low on available free space.
	Free space is below 5%.	Error		
Datastore is inaccessible	State not equals <i>Accessible</i> 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		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
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.
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	vCloud Director object task status equals <i>Warning</i> .	Warning	Automatic	vApp health status has changed
	vCloud Director object task status equals <i>Alert</i> .	Error		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
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 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 runtime lease timeout is 7 days.	Error		
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	

Alarm Name	Rule Event	Severity	Resolve Action	Description
	Network pool usage is above 95%.	Error		Network pool usage has exceeded the configured threshold for this alarm
Org VDC CPU usage	Average CPU usage for 15 minutes is above 80%.	Warning	Automatic	This organization VDC has exceeded the threshold for CPU Usage
	Average CPU usage for 15 minutes is above 90%.	Error		
Org VDC health status	vCloud Director object task status equals <i>Warning</i> .	Warning	Automatic	Org VDC health status has changed
	vCloud Director object task status equals <i>Alert</i> .	Error		
Org VDC memory usage	Average memory usage for 15 minutes is above 80%.	Warning	Automatic	This organization VDC has exceeded the threshold for Memory Usage
	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	This org VDC has exceeded the threshold for Storage Usage
	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	This provider VDC has exceeded the threshold for CPU Usage
	Average CPU usage for 15 minutes is above 90%.	Error		

Alarm Name	Rule Event	Severity	Resolve Action	Description
Provider VDC health status	vCloud Director object task status equals <i>Warning</i> .	Warning	Automatic	Provider VDC health status has changed
	vCloud Director object task status equals <i>Alert</i> .	Error		
Provider VDC memory usage	Average memory usage for 15 minutes is above 80%.	Warning	Automatic	This provider VDC has exceeded the threshold for Memory Usage
	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	This provider VDC has exceeded the threshold for Storage usage
	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](#)
- [Virtual Machine](#)
- [Cluster](#)
- [Cluster Shared Volume](#)
- [Local Storage](#)
- [Any Hyper-V Object](#)

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.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
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.
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 <i>Connected</i> for 5 minutes or more.	Error	Automatic	This alarm monitors Hyper-V host connection state.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
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		
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		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
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		
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.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
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.
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.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
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.
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 might be in inconsistent state.
Failed to power on VM	Based on event 12010 Microsoft-Windows-Hyper-V-Worker.	Error	Manual	Failed to power on VM.
	Based on event 12030 Microsoft-Windows-Hyper-V-Worker.			

Alarm Name	Event/Condition	Severity	Resolve Action	Description
	Based on event 12040 Microsoft-Windows-Hyper-V-Worker.			
	Based on event 12050 Microsoft-Windows-Hyper-V-Worker.			
Failed to restore VM	Based on event 12080 Microsoft-Windows-Hyper-V-Worker.	Error	Manual	Failed to restore a VM.
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

Alarm Name	Event/Condition	Severity	Resolve Action	Description
	Based on event 12560 Microsoft-Windows-Hyper-V-Worker.			assigned dynamic MAC addresses.
	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 exceeded the configured threshold.
	Hyper-V VM checkpoint size is above 20% of the VM size.	Error		
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.			

Alarm Name	Event/Condition	Severity	Resolve Action	Description
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 assigned dynamic MAC addresses.
	Based on event 12562 Microsoft-Windows-Hyper-V-Worker.			
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.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
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.
VM power status	State not equals <i>Running</i> 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.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
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.
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.
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

Alarm Name	Event/Condition	Severity	Resolve Action	Description
	Based on event VeeamHvClusterReserveStateErrorEvent.	Error		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 corresponding alarm will be fired.
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.
Cluster service cannot be started	Based on event 1090 Microsoft-Windows-FailoverClustering.	Error	Manual	The Cluster service cannot be started. An attempt to read configuration data from the Windows registry failed.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Cluster service failed to start	Based on event 1105 Microsoft-Windows-FailoverClustering.	Error	Manual	The Cluster service failed to start because it was unable to register interface(s) 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.
Cluster service shut down	Based on event 1177 Microsoft-Windows-FailoverClustering.	Error	Manual	The Cluster service is shutting down because quorum was lost.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
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).
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.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
Failed to migrate virtual machine	Based on event 22506 Microsoft-Windows-Hyper-V-High-Availability.	Error	Manual	Live migration for this VM did not succeed.
	Based on event 22505 Microsoft-Windows-Hyper-V-High-Availability.			
	Based on event 21100 Microsoft-Windows-Hyper-V-High-Availability.			
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.
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.

Alarm Name	Event/Condition	Severity	Resolve Action	Description
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		
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		

Alarm Name	Event/Condition	Severity	Resolve Action	Description
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		
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.			
	Based on event 12240 Microsoft-Windows-Hyper-V-VMMS.			
	Based on event 12240 Microsoft-Windows-Hyper-V-Worker.			

Alarm Name	Event/Condition	Severity	Resolve Action	Description
	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.

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 server data collection problem	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	
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	
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	
Topology collection failure	Based on event VeeamInfCollectionFailedEvent.	Error	Veeam ONE failed to collect

	Based on event VeeamInfCollectionFailedResolvedEvent.	Resolve	infrastructure topology.
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	
vCloud Director blocking tasks update failure	Based on event VeeamVcdBlockingTaskUpdateFailedEvent.	Error	Veeam ONE failed to update vCloud Director blocking tasks list.
	Based on event VeeamVcdBlockingTaskUpdateFailedResolvedEvent.	Resolve	
vCloud Director connection failure	Based on event VeeamNoVcdHostConnectionEvent.	Error	Veeam ONE failed to collect performance and configuration data from vCloud Director.
	Based on event VeeamNoVcdHostConnectionResolvedEvent.	Resolve	
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	
vCloud Director stranded items update failure	Based on event VeeamVcdStrandedItemUpdateFailedEvent.	Error	Veeam ONE failed to update vCloud Director stranded items list.
	Based on event VeeamVcdStrandedItemUpdateFailedResolvedEvent.	Resolve	
Veeam B&R license exceeded	Based on event VeeamBpExceedErrorEvent.	Error	Veeam Backup & Replication license limit has been exceeded.
	Based on event VeeamBpExceedWarningEvent.	Warning	
	Based on event VeeamLicenseGraceOverEvent.	Error	
	Based on event VeeamBpExceedResolvedEvent.	Resolve	
	Based on event VeeamLicenseChangedEvent.	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	
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 sockets exceeded	Based on event VeeamSocketExceedEvent.	Error	The number of licensed servers

	Based on event VeeamSocketExceedResolvedEvent.	Resolve	has been exceeded.
	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, etc. 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 VMs exceeded	Based on event VeeamVMsExceedErrorEvent.	Error	Your license limit has been exceeded. You need to purchase additional VMs licensing before all VMs exceeding the licensed amount will no longer be monitored.
	Based on event VeeamVMsExceedWarningEvent.	Warning	
	Based on event VeeamVMsExceedResolvedEvent.	Resolve	
	Based on event VeeamMonitorServicesStartedEvent.	Resolve	
Veeam ONE Reporter collection job	Job state equals <i>Failed</i> .	Error	Veeam ONE Reporter session task failed.
	Job state equals <i>Warning</i> .	Warning	
Veeam ONE Reporter service state	Veeam ONE Reporter service is not running.	Error	Veeam ONE Reporter 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	
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	

Appendix B. Alarm Rules

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](#)
- [Cluster](#)
- [Host](#)
- [Resource Pool](#)
- [Virtual Machine](#)
- [Datastore](#)
- [Any Object](#)
- [vCloud Director vApp](#)
- [vCloud Director Organization](#)
- [vCloud Director Org VDC](#)
- [vCloud Director Provider VDC](#)

vCenter Server

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

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

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.
Hardware sensor state changes	An alarm is triggered if the sensor state reports to be equal or not equal to a specific state value (<i>Normal, Warning, Alert, Unknown</i>).
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

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

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 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 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	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 resource usage is out of allowed range	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	An alarm is triggered if VM process state is equal or not equal to a specific state value (<i>Terminated, Running</i>).
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	An alarm is triggered if service state is equal or not equal to a specific state value (<i>Running, Paused, Stopped</i>).
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

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 alarm is triggered if the provisioned disk space exceeds 500 GB or 400% compared to the datastore capacity.
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

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

Event-based rule	An alarm is triggered if some vApp-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 value (for example, if the storage usage exceeds 80%).
System health status change	An alarm is triggered if the object health state changes.
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

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

Event-based rule	An alarm is triggered if some event is generated on the organization VDC.
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

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](#)
- [Virtual Machine](#)
- [Cluster](#)
- [CSV](#)
- [Local Storage](#)
- [Any Object](#)

Host

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 (<i>Running, Paused, Stopped</i>).
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 (<i>Running, Paused, Stopped</i>).

Virtual Machine

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.
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	An alarm is triggered if the number of services running on a VM is greater than the specified threshold.
Process resource usage is out of allowed range	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	An alarm is triggered if VM process state is equal or not equal to a specific state value (<i>Terminated</i> , <i>Running</i>).
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	An alarm is triggered if service state is equal or not equal to a specific state value (<i>Running, Paused, Stopped</i>).
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

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)

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

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

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 (<i>Terminated</i> , <i>Running</i>).

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](#)
- [Backup Server](#)
- [Repository](#)
- [Proxy](#)
- [WAN Accelerator](#)
- [Tape Server](#)
- [Cloud Repository](#)
- [Cloud Gateway](#)

Enterprise Manager

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

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.
Job/Policy status	An alarm is triggered if the job or policy status is equal or not equal to the specified value.
Nutanix AHV cluster connection failure	An alarm is triggered if the backup server fails to connect the Nutanix AHV cluster.
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 backup or replication job exceeds a threshold duration value (specified in minutes).
Power or connection state changes	An alarm is triggered if the state of Veeam Backup server is equal or not equal to the specified value (for example, if connection to the backup server is lost).

Repository

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.
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).

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

Event-based rule	An alarm is triggered if some Veeam Backup & Replication event is generated for the backup proxy.
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 backup proxy is equal or not equal to the specified value (for example, if connection to the proxy server is lost).

WAN Accelerator

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.

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

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

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.

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

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).

Rules for Internal Alarms

Veeam ONE offers the following types of rules for internal alarms:

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%).
Veeam ONE Reporter collection job state	An alarm is triggered if Veeam ONE Reporter collection job state is equal or not equal to a specific state value (<i>Failed</i> , <i>Warning</i> , <i>Success</i>).

Appendix C. Remediation Actions

This section lists alarms with predefined remediation actions.

Backup job disabled	Veeam Backup & Replication	Enable job	Default action for warning severity	Veeam ONE runs the script that enables the disabled job.
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.

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	<p>Veeam ONE runs the script that adds the VM to an existing backup job.</p> <p>For this action you must specify a backup server and a job to which the VM must be added.</p> <p>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.</p>
		Add VM to backup job and run	Extra action	<p>Veeam ONE runs the script that adds the VM to an existing backup job and starts that job.</p> <p>For this action you must specify a backup server and a job to which the VM must be added.</p> <p>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.</p>
		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 <i>Success</i> status.
		Start Quick backup	Extra action	<p>Veeam ONE runs the script that starts a quick backup job for the VM.</p> <p>For this action you must specify backup server.</p> <p>For details on quick backup, see Quick Backup.</p>

		Start VeeamZIP	Extra action	<p>Veeam ONE runs the script that creates an independent full backup file.</p> <p>For this action you must specify a backup server and a backup repository.</p> <p>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.</p> <p>For details on VeeamZIP, see VeeamZIP.</p>
VM with no replica	VMware vSphere	Add VM to replication job	Default action for warning severity	<p>Veeam ONE runs the script that adds the VM to an existing replication job.</p> <p>For this action you must specify a backup server and a job to which the VM must be added.</p> <p>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.</p>
		Add VM to replication job and run	Extra action	<p>Veeam ONE runs the script that adds the VM to an existing replication job and starts that job.</p> <p>For this action you must specify a backup server and a job to which the VM must be added.</p> <p>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.</p>
		Run parent replication job	Extra action	<p>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 <i>Success</i> status.</p>

		Start Quick backup	Extra action	<p>Veeam ONE runs the script that starts a quick backup job for the VM.</p> <p>For this action you must specify backup server.</p> <p>For details on quick backup, see Quick Backup.</p>
		Start VeeamZIP	Extra action	<p>Veeam ONE runs the script that creates an independent full backup file.</p> <p>For this action you must specify a backup server and a backup repository.</p> <p>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.</p> <p>For details on VeeamZIP, see VeeamZIP.</p>
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.

VM with no backup	Microsoft Hyper-V	Add VM to backup job	Default action for warning severity	<p>Veeam ONE runs the script that adds the VM to an existing backup job.</p> <p>For this action you must specify a backup server and a job to which the VM must be added.</p> <p>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.</p>
		Add VM to backup job and run	Extra action	<p>Veeam ONE runs the script that adds the VM to an existing backup job and starts that job.</p> <p>For this action you must specify a backup server and a job to which the VM must be added.</p> <p>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.</p>
		Run parent backup job	Extra action	<p>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 <i>Success</i> status.</p>
		Start Quick backup	Extra action	<p>Veeam ONE runs the script that starts a quick backup job for the VM.</p> <p>For this action you must specify backup server.</p> <p>For details on quick backup, see Quick Backup.</p>

		Run VeeamZIP	Extra action	<p>Veeam ONE runs the script that creates an independent full backup file.</p> <p>For this action you must specify a backup server and a job to which the VM must be added.</p> <p>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.</p> <p>For details on VeeamZIP, see VeeamZIP.</p>
VM with no replica	Microsoft Hyper-V	Add VM to replication job	Default action for warning severity	<p>Veeam ONE runs the script that adds the VM to an existing replication job.</p> <p>For this action you must specify a backup server and a job to which the VM must be added.</p> <p>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.</p>
		Add VM to replication job and run	Extra action	<p>Veeam ONE runs the script that adds the VM to an existing replication job and starts that job.</p> <p>For this action you must specify a backup server and a job to which the VM must be added.</p> <p>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.</p>
		Run parent replication job	Extra action	<p>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 <i>Success</i> status.</p>

		Start Quick backup	Extra action	<p>Veeam ONE runs the script that starts a quick backup job for the VM.</p> <p>For this action you must specify backup server.</p> <p>For details on quick backup, see Quick Backup.</p>
		Run VeeamZIP	Extra action	<p>Veeam ONE runs the script that creates an independent full backup file.</p> <p>For this action you must specify a backup server and a job to which the VM must be added.</p> <p>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.</p> <p>For details on VeeamZIP, see VeeamZIP.</p>