Description of event windows and dialog boxes

Active IQ Unified Manager

NetApp
December 23, 2021

This PDF was generated from https://docs.netapp.com/us-en/active-iq-unified-manager/events/reference_notifications_page.html on December 23, 2021. Always check docs.netapp.com for the latest.

Table of Contents

Description of event windows and dialog boxes

Events notify you about any issues in your environment. You can use the Event Management inventory page and Event details page to monitor all the events. You can use the Notification Setup Options dialog box to configure notification. You can use the Event Setup page to disable or enable events.

Notifications page

You can configure the Unified Manager server to send notifications when an event is generated or when it is assigned to a user. You can also configure the notification mechanisms. For example, notifications can be sent as emails or SNMP traps.

You must have the Application Administrator or Storage Administrator role.

Email

This area enables you to configure the following email settings for alert notification:

- **From Address**

  Specifies the email address from which the alert notification is sent. This value is also used as the from address for a report when shared. If the From Address is pre-filled with the address "ActiveIQUnifiedManager@localhost.com", you should change it to a real, working email address to make sure that all email notifications are delivered successfully.

SMTP Server

This area enables you to configure the following SMTP server settings:

- **Host Name or IP Address**

  Specifies the host name of your SMTP host server, which is used to send the alert notification to the specified recipients.

- **User Name**

  Specifies the SMTP user name. SMTP user name is required only when the SMTPAUTH is enabled in the SMTP server.

- **Password**

  Specifies the SMTP password. SMTP user name is required only when the SMTPAUTH is enabled in the SMTP server.

- **Port**

  Specifies the port that is used by the SMTP host server to send alert notification.

  The default value is 25.

- **Use START/TLS**

  Checking this box provides secure communication between the SMTP server and the management server by using the TLS/SSL protocols (also known as start_tls and StartTLS).

- **Use SSL**

  Checking this box provides secure communication between the SMTP server and the management server by using the SSL protocol.

SNMP

This area enables you to configure the following SNMP trap settings:

- **Version**

  Specifies the SNMP version you want to use depending on the type of security you require. Options include Version 1, Version 3, Version 3 with Authentication, and Version 3 with Authentication and Encryption. The default value is Version 1.

- **Trap Destination Host**

  Specifies the host name or IP address (IPv4 or IPv6) that receives the SNMP traps that are sent by the management server. To specify multiple trap destinations, separate each host with a comma.

  > All other SNMP settings, such as "Version" and "Outbound Port", must be the same for all hosts in the list.

- **Outbound Trap Port**

  Specifies the port through which the SNMP server receives the traps that are sent by the management server.

  The default value is 162.

- **Community**

  The community string to access the host.

- **Engine ID**

  Specifies the unique identifier of the SNMP agent and is automatically generated by the management server. Engine ID is available with SNMP Version 3, SNMP Version 3 with Authentication, and SNMP Version 3 with Authentication and Encryption.

- **Username**

  Specifies the SNMP user name. User name is available with SNMP Version 3, SNMP Version 3 with Authentication, and SNMP Version 3 with Authentication and Encryption.

- **Authentication Protocol**

  Specifies the protocol used to authenticate a user. Protocol options include MD5 and SHA. MD5 is the default value. Authentication protocol is available with SNMP Version 3 with Authentication and SNMP

Version 3 with Authentication and Encryption.

- **Authentication Password**

  Specifies the password used when authenticating a user. Authentication password is available with SNMP Version 3 with Authentication and SNMP Version 3 with Authentication and Encryption.

- **Privacy Protocol**

  Specifies the privacy protocol used to encrypt SNMP messages. Protocol options include AES 128 and DES. The default value is AES 128. Privacy protocol is available with SNMP Version 3 with Authentication and Encryption.

- **Privacy Password**

  Specifies the password when using privacy protocol. Privacy password is available with SNMP Version 3 with Authentication and Encryption.

Event Management inventory page

The Event Management inventory page enables you to view a list of current events and their properties. You can perform tasks such as acknowledging, resolving, and assigning events. You can also add an alert for specific events.

The information on this page is refreshed automatically every 5 minutes to ensure that the most current new events are displayed.

Filter components

Enable you to customize the information that is displayed in the events list. You can refine the list of events that are displayed using the following components:

- View menu to select from a pre-defined list of filter selections.

  This includes items such as all active (new and acknowledged) events, active performance events, events assigned to me (the logged in user), and all events generated during all maintenance windows.

- Search pane to refine the list of events by entering full or partial terms.
- Filter button that launches the Filters pane so you can select from every available field and field attribute to refine the list of events.

Command buttons

The command buttons enable you to perform the following tasks:

- **Assign To**

  Enables you to select the user to whom the event is assigned. When you assign an event to a user, the user name and the time when you assigned the event is added in the events list for the selected events.

  - Me

    Assigns the event to the currently logged in user.

- Another user

  Displays the Assign Owner dialog box, which enables you to assign or reassign the event to other users. You can also unassign events by leaving the ownership field blank.

- **Acknowledge**

  Acknowledges the selected events.

  When you acknowledge an event, your user name and the time when you acknowledged the event are added in the events list for the selected events. When you acknowledge an event, you are responsible for managing that event.

  You cannot acknowledge Information events.

- **Mark As Resolved**

  Enables you to change the event state to resolved.

  When you resolve an event, your user name and the time when you resolved the event are added in the events list for the selected events. After you have taken corrective action for the event, you must mark the event as resolved.

- **Add Alert**

  Displays the Add Alert dialog box, which enables you to add alerts for the selected events.

- **Reports**

  Enables you to export details of the current event view to a comma-separated values (.csv) file or PDF document.

- **Show/Hide Column Selector**

  Enables you to choose the columns that display on the page and select the order in which they are displayed.

Events list

Displays details of all the events ordered by triggered time.

By default the All active events view is displayed to show the New and Acknowledged events for the previous seven days that have an Impact Level of Incident or Risk.

- **Triggered Time**

  The time at which the event was generated.

- **Severity**

  The event severity: Critical (), Error (), Warning (), and Information ().

- **State**

  The event state: New, Acknowledged, Resolved, or Obsolete.

- **Impact Level**

  The event impact level: Incident, Risk, Event, or Upgrade.

- **Impact Area**

  The event impact area: Availability, Capacity, Performance, Protection, Configuration, or Security.

- **Name**

  The event name. You can select the name to display the Event details page for that event.

- **Source**

  The name of the object on which the event has occurred. You can select the name to display the health or performance details page for that object.

  When a shared QoS policy breach occurs, only the workload object that is consuming the most IOPS or MB/s is shown in this field. Additional workloads that are using this policy are displayed in the Event details page.

- **Source Type**

  The object type (for example, Storage VM, Volume, or Qtree) with which the event is associated.

- **Assigned To**

  The name of the user to whom the event is assigned.

- **Event Origin**

  Whether the event originated from the "Active IQ Portal" or directly from "Active IQ Unified Manager".

- **Annotation Name**

  The name of the annotation that is assigned to the storage object.

- **Notes**

  The number of notes that are added for an event.

- **Days Outstanding**

  The number of days since the event was initially generated.

- **Assigned Time**

  The time that has elapsed since the event was assigned to a user. If the time elapsed exceeds a week, the timestamp when the event was assigned to a user is displayed.

- **Acknowledged By**

  The name of the user who acknowledged the event. The field is blank if the event is not acknowledged.

- **Acknowledged Time**

The time that has elapsed since the event was acknowledged. If the time elapsed exceeds a week, the timestamp when the event was acknowledged is displayed.

- **Resolved By**

  The name of the user who resolved the event. The field is blank if the event is not resolved.

- **Resolved Time**

  The time that has elapsed since the event was resolved. If the time elapsed exceeds a week, the timestamp when the event was resolved is displayed.

- **Obsoleted Time**

  The time when the state of the event became Obsolete.

Event details page

From the Event details page, you can view the details of a selected event, such as the event severity, impact level, impact area, and event source. You can also view additional information about possible remediations to resolve the issue.

- **Event Name**

  The name of the event and the time the event was last seen.

  For non-performance events, while the event is in the New or Acknowledged state the last seen information is not known and is therefore hidden.

- **Event Description**

  A brief description of the event.

  In some cases a reason for the event being triggered is provided in the event description.

- **Component in Contention**

  For dynamic performance events, this section displays icons that represent the logical and physical components of the cluster. If a component is in contention, its icon is circled and highlighted red.

  See *Cluster components and why they can be in contention* for a description of the components that are displayed here.

The Event Information, System Diagnosis, and Suggested Actions sections are described in other topics.

Command buttons

The command buttons enable you to perform the following tasks:

- **Notes icon**

  Enables you to add or update a note about the event, and review all notes left by other users.

Actions menu

- **Assign to Me**

  Assigns the event to you.

- **Assign to Others**

  Opens the Assign Owner dialog box, which enables you to assign or reassign the event to other users.

  When you assign an event to a user, the user's name and the time when the event was assigned are added in the events list for the selected events.

  You can also unassign events by leaving the ownership field blank.

- **Acknowledge**

  Acknowledges the selected events so that you do not continue to receive repeat alert notifications.

  When you acknowledge an event, your user name and the time that you acknowledged the event are added in the events list (Acknowledged By) for the selected events. When you acknowledge an event, you take responsibility for managing that event.

- **Mark As Resolved**

  Enables you to change the event state to Resolved.

  When you resolve an event, your user name and the time that you resolved the event are added in the events list (Resolved By) for the selected events. After you have taken corrective action for the event, you must mark the event as resolved.

- **Add Alert**

  Displays the Add Alert dialog box, which enables you to add an alert for the selected event.

What the Event Information section displays

You use the Event Information section on the Event details page to view the details about a selected event, such as the event severity, impact level, impact area, and event source.

Fields that are not applicable to the event type are hidden. You can view the following event details:

- **Event Trigger Time**

  The time at which the event was generated.

- **State**

  The event state: New, Acknowledged, Resolved, or Obsolete.

- **Obsoleted Cause**

  The actions that caused the event to be obsoleted, for example, the issue was fixed.

- **Event Duration**

For active (new and acknowledged) events, this is the time between detection and the time when the event was last analyzed. For obsolete events, this is the time between detection and when the event was resolved.

This field is displayed for all performance events, and for other event types only after they have been resolved or obsoleted.

- **Last Seen**

  The date and time at which the event was last seen as active.

  For performance events this value may be more recent than the Event Trigger Time as this field is updated after each new collection of performance data as long as the event is active. For other types of events, when in the New or Acknowledged state, this content is not updated and the field is therefore hidden.

- **Severity**

  The event severity: Critical (), Error (), Warning (), and Information ().

- **Impact Level**

  The event impact level: Incident, Risk, Event, or Upgrade.

- **Impact Area**

  The event impact area: Availability, Capacity, Performance, Protection, Configuration, or Security.

- **Source**

  The name of the object on which the event has occurred.

  When viewing the details for a shared QoS policy event, up to three of the workload objects that are consuming the most IOPS or MBps are listed in this field.

  You can click the source name link to display the health or performance details page for that object.

- **Source Annotations**

  Displays the annotation name and value for the object to which the event is associated.

  This field is displayed only for health events on clusters, SVMs, and volumes.

- **Source Groups**

  Displays the names of all the groups of which the impacted object is a member.

  This field is displayed only for health events on clusters, SVMs, and volumes.

- **Source Type**

  The object type (for example, SVM, Volume, or Qtree) with which the event is associated.

- **On Cluster**

  The name of the cluster on which the event occurred.

You can click the cluster name link to display the health or performance details page for that cluster.

- **Affected Objects Count**

  The number of objects affected by the event.

  You can click the object link to display the inventory page populated with the objects that are currently affected by this event.

  This field is displayed only for performance events.

- **Affected Volumes**

  The number of volumes that are being affected by this event.

  This field is displayed only for performance events on nodes or aggregates.

- **Triggered Policy**

  The name of the threshold policy that issued the event.

  You can hover your cursor over the policy name to see the details of the threshold policy. For adaptive QoS policies the defined policy, block size, and allocation type (allocated space or used space) is also displayed.

  This field is displayed only for performance events.

- **Rule Id**

  For Active IQ platform events, this is the number of the rule that was triggered to generate the event.

- **Acknowledged by**

  The name of the person who acknowledged the event and the time that the event was acknowledged.

- **Resolved by**

  The name of the person who resolved the event and the time that the event was resolved.

- **Assigned to**

  The name of the person who is assigned to work on the event.

- **Alert Settings**

  The following information about alerts is displayed:

  - If there are no alerts associated with the selected event, an **Add alert** link is displayed.

    You can open the Add Alert dialog box by clicking the link.

  - If there is one alert associated with the selected event, the alert name is displayed.

    You can open the Edit Alert dialog box by clicking the link.

  - If there is more than one alert associated with the selected event, the number of alerts is displayed.

You can open the Alert Setup page by clicking the link to view more details about these alerts.

Alerts that are disabled are not displayed.

- **Last Notification Sent**

  The date and time at which the most recent alert notification was sent.

- **Send by**

  The mechanism that was used to send the alert notification: email or SNMP trap.

- **Previous Script Run**

  The name of the script that was executed when the alert was generated.

What the Suggested Actions section displays

The Suggested Actions section of the Event details page provides possible reasons for the event and suggests a few actions so that you can try to resolve the event on your own. The suggested actions are customized based on the type of event or type of threshold that has been breached.

This area is displayed only for some types of events.

In some cases there are **Help** links provided on the page that reference additional information for many suggested actions, including instructions for performing a specific action. Some of the actions may involve using Unified Manager, ONTAP System Manager, OnCommand Workflow Automation, ONTAP CLI commands, or a combination of these tools.

You should consider the actions suggested here as only a guidance in resolving this event. The action you take to resolve this event should be based on the context of your environment.

If you want to analyze the object and event in more detail, click the **Analyze Workload** button to display the Workload Analysis page.

There are certain events that Unified Manager can diagnose thoroughly and provide a single resolution. When available, those resolutions are displayed with a **Fix It** button. Click this button to have Unified Manager fix the issue causing the event.

For Active IQ platform events, this section may contain a link to a NetApp Knowledgebase article, when available, that describes the issue and possible resolutions. In sites with no external network access, a PDF of the Knowledgebase article is opened locally; the PDF is part of the rules file that you manually download to the Unified Manager instance.

What the System Diagnosis section displays

The System Diagnosis section of the Event details page provides information that can help you diagnose issues that may have been responsible for the event.

This area is displayed only for some events.

Some performance events provide charts that are relevant to the particular event that has been triggered.

Typically this includes and IOPS or MBps chart and a latency chart for the previous ten days. When arranged this way you can see which storage components are most affecting latency, or being affected by latency, when the event is active.

For dynamic performance events, the following charts are displayed:

- Workload Latency - Displays the history of latency for the top victim, bully, or shark workloads at the component in contention.
- Workload Activity - Displays details about the workload usage of the cluster component in contention.
- Resource Activity - Display historical performance statistics for the cluster component in contention.

Other charts are displayed when some cluster components are in contention.

Other events provide a brief description of the type of analysis the system is performing on the storage object. In some cases there will be one or more lines; one for each component that has been analyzed, for system-defined performance policies that analyze multiple performance counters. In this scenario, a green or red icon displays next to the diagnosis to indicate whether an issue was found, or not, in that particular diagnosis.

Event Setup page

The Event Setup page displays the list of events that are disabled, and provides information such as the associated object type and severity of the event. You can also perform tasks such as disabling or enabling events globally.

You can access this page only if you have the Application Administrator or Storage Administrator role.

Command buttons

The command buttons enable you to perform the following tasks for selected events:

- **Disable**

  Launches the Disable Events dialog box, which you can use to disable events.

- **Enable**

  Enables selected events that you had chosen to disable previously.

- **Upload Rules**

  Launches the Upload Rules dialog box, which enables sites with no external network access to manually upload the Active IQ rules file to Unified Manager. The rules are run against cluster AutoSupport messages to generate events for system configuration, cabling, best practice, and availability as defined by the Active IQ platform.

- **Subscribe to EMS Events**

  Launches the Subscribe to EMS Events dialog box, which enables you to subscribe to receive specific Event Management System (EMS) events from the clusters that you are monitoring. The EMS collects information about events that occur on the cluster. When a notification is received for a subscribed EMS event, a Unified Manager event is generated with the appropriate severity.

List view

The List view displays (in tabular format) information about events that are disabled. You can use the column filters to customize the data that is displayed.

- **Event**

  Displays the name of the event that is disabled.

- **Severity**

  Displays the severity of the event. The severity can be Critical, Error, Warning, or Information.

- **Source Type**

  Displays the source type for which the event is generated.

Disable Events dialog box

The Disable Events dialog box displays the list of event types for which you can disable events. You can disable events for an event type based on a particular severity or for a set of events.

You must have the Application Administrator or Storage Administrator role.

Event Properties area

The Event Properties area specifies the following event properties:

- **Event Severity**

  Enables you to select events based on the severity type, which can be Critical, Error, Warning, or Information.

- **Event Name Contains**

  Enables you to filter events whose name contains the specified characters.

- **Matching events**

  Displays the list of events matching the event severity type and the text string you specify.

- **Disable events**

  Displays the list of events that you have selected for disabling.

  The severity of the event is also displayed along with the event name.

Command buttons

The command buttons enable you to perform the following tasks for the selected events:

- **Save and close**

Disables the event type and closes the dialog box.

- **Cancel**

  Discards the changes and closes the dialog box.

Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system- without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.