



Alerts

Avi Technical Reference (v18.1)

Copyright © 2018

Alerts

[view online](#)

Events are generated automatically within by Vantage to create a record of notable activities throughout the system. These may be Vantage errors, client traffic deviations, or many others.

Alerts may be generated when a trigger such as a system event occurs. If all conditions within the Alert Config are met, an alert is created. It may be used to actively or passively notify administrators, and may be deleted after being viewed or after an elapsed period of time.

All Alerts

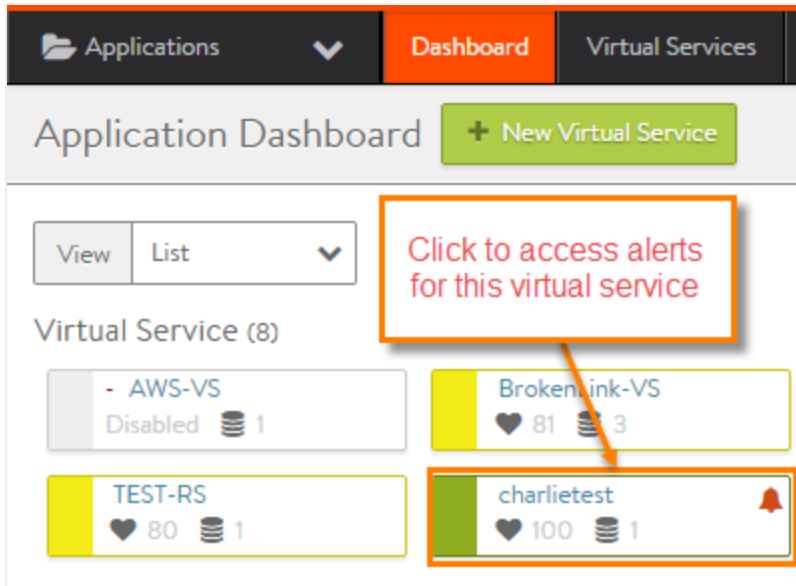
The Operations > Alerts > All Alerts page shows all Alerts across Avi Vantage.

	Timestamp	Resource Name	Level	Summary	
<input type="checkbox"/>	02/18 11:33:16 PM	test	High	Event Vs-Down occurred	+
<input type="checkbox"/>	02/18 10:33:11 PM	test	High	Event Vs-Down occurred	+
<input type="checkbox"/>	02/18 9:33:06 PM	test	High	Event Vs-Down occurred	+
<input type="checkbox"/>	02/18 8:33:01 PM	test	High	Event Vs-Down occurred	+

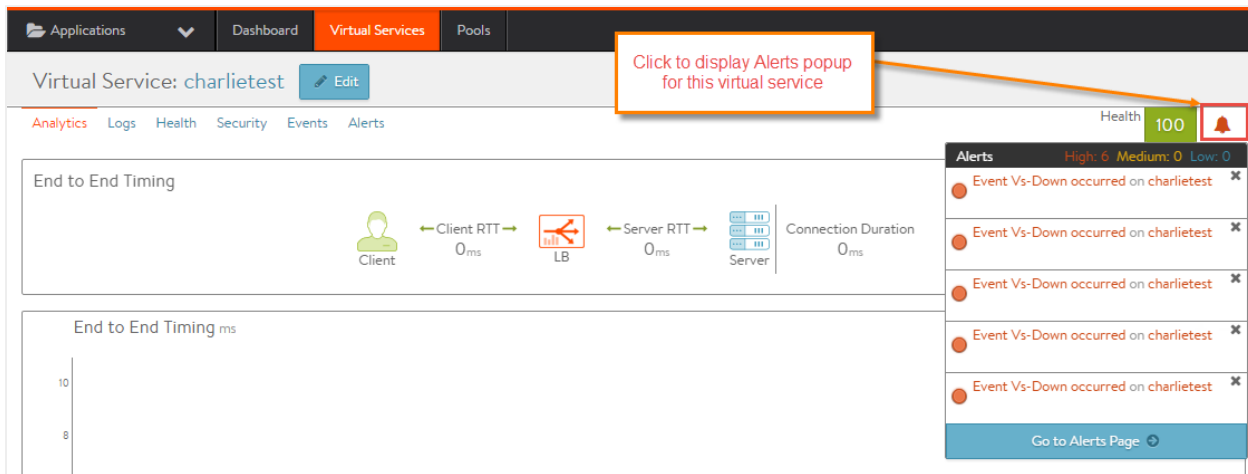
The functionality on this page is identical to that of the alerts tab found in the virtual services and pools pages; however, those pages are filtered to only show alerts related to those objects. See the Virtual Service Alerts tab for more information on navigating the Alert options.

Alerts for Specific Virtual Service

If the virtual service has alerts, an alerts icon appears on the virtual service icon on the Dashboard. Click the virtual service icon to access details for the virtual service, including its alerts:



Click Alerts to display the alerts log for the virtual service, or click the alerts icon next to the health score to display a popup list of the most recent alerts.



Alert Configuration

Alerts filter events to highlight important information. Avi Vantage includes a number of default alerts via the Alert Config page. The default alerts may not be deleted, but can be modified or disabled as needed. Alert Configs determine whether or not an alert should be generated.

Alert Config Page

The Alert Config page has the following options:

- **Search:** Search against the alert names in the table.
- **Create:** Opens the New Alert Config popup.
- **Edit:** Opens the Edit Alert Config popup.
- **Delete:** Remove the selected Alert configuration.

The table on this page contains the following information for each Alert:

Name	Alert Level	Alert Action	Type	Alert Group	Enabled
Apic-Bad-Credentials	High	System-Alert-Level-High	Real Time	Event Logs	True
Aws-Access-Failure	High	System-Alert-Level-High	Real Time	Event Logs	True
Aws-Image-Upload-Failure	High	System-Alert-Level-High	Real Time	Event Logs	True
Cc-Cluster-Vip-Config-Failure	High	System-Alert-Level-High	Real Time	Event Logs	True

- **Name:** Name of the Alert.
- **Alert Level:** Level, or severity, of the Alert (Low, Medium, or High).
- **Alert Action:** Specifies the alert action that is triggered when the Alert is generated.
- **Type:** Whether the Alert is Real Time (5-second window) or Rolling Window (5-minute window).
- **Alert Group:** Whether the Alert applies to applications (App Log), client connections (Conn Logs), or Events (Event Logs)
- **Enabled:** Whether the Alert is enabled or disabled.

Create Alert Configuration

The New and Edit Alert Config popups share the same interface.

New Alert Config:
✕

Name ?

Alert Config Status ?

Enabled

Priority

Low ▼

Alert Action ?

None ▼ *

Type ?

Rolling Window

Source

Event Metric

Alert Expiry Time ?

86400 sec

Number of Occurrences ?

1

Event Occurs ?

Select an Event ▼ *

Event Does Not Occur

Select an Event ▼

Throttle Alert

600 sec

Description ?

To create or edit an Alert notification:

- **Name:** Enter a unique name for the Alert Config.
- **Priority:** Every alert is classified with a priority level, which is used with alert actions. For example, all alerts marked as high could trigger an email notification. Alerts in the Vantage UI will indicate the level of severity. The following levels are available:
 - **External:** This alert will trigger an alert action, but will not create a local alert on Vantage.
 - **High:** Indicates a critical problem.
 - **Medium:** Indicates a less-severe problem.
 - **Low:** Indicates a minor problem.
- **Event:** If the selected event occurs, generate an alert.
- **Type:** Create an alert every time an event occurs, or only create an alert if an event occurs a specified number of times within a time window.

- Rolling Window Disabled: When the event occurs, an alert is generated.
- Rolling Window Enabled: An alert is generated if the Number of events is met or exceeded within the desired Time Window.
 - Time Window: Select a custom time frame. The default is 5 minutes.
- Alert Expiry Time: Alerts are intended to notify administrators of pressing issues that warrant attention, and many alerts are only actionable while the problem persists. Alerts are therefore automatically deleted after a period of time, with the underlying events and logs serving as the definitive long-term records. An alert may be manually dismissed using the Alerts tab for the selected item (such as a virtual service).
- Number of Occurrences: During the Rolling Window timeframe, the event must occur this many times to trigger the alert.
- Throttle Alert: Sets the duration of time within which an alert may only be created once.
- Description: Enter a custom description for the alert.
- Alert Config Status: Disable an Alert Config from generating new alerts.
- Alert Action: Points to the alert action group for the alert. The action object is configured to perform an action such as email, Syslog, etc.
- Source: Set the event or metric that will trigger the alert.
 - Event:
 - Event Occurs: If an event happens, such as login failure. This field is required when alerting on events.
 - Event Does Not Occur: If the event does not occur, trigger the event. This field is optional. When used, both this field and the Event Occurs must be true for the alert to trigger. This option is useful if expecting to see an event within a period of time defined via the Alert Threshold Duration. For instance, an Event Occurs is set to server down while Event Does Not Occur is set to server up. If the server bounces down and back up again within a 5 minute window, don't create an alert.
 - Metric:
 - Object: Inspect the metrics of an object such as virtual service, Service Engine, or pool.
 - Instance: Select the specific object of the type specified in the Object field.
 - Metric Occurs: Select a metric which is used as the trigger for the alert.
 - Comparator: The value returned by the Metric Occurs must match the greater than, less than, or equal to the Value field.
 - Value: The numeric value the metric is compared against. Some metrics will be percentage from 0 to 100, while throughput is in bits per second, such as 1000000.
 - Duration: The length of time during which the metric must be true. Generally this means an average of the metric over this period of time. Keep in mind some metrics are not collected at an aggressive rate. For instance, vCenter updates server CPU information every five minutes. Therefore duration should be longer than 600 (seconds).

Alert Actions










When an alert is generated within Vantage, it is immediately able to be viewed by an administrator. This means the administrator must sign into Vantage, navigate to the appropriate object and view the alerts to know if there is a serious issue. Alternatively, alert actions may be set up, which allow alerts to be proactively sent from Vantage to an external destination.

Alert Action Page

Select Operations > Alerts > Alert Actions to display the configured alert actions, which correspond to the three system alert levels (high, medium, and low). Alert actions can be set up to export alerts matching any of these three severity levels. The actions for these levels can be changed, but the levels themselves cannot be modified as they map to alert severity displayed throughout the Vantage web interface. This tab includes the following functions:

- Search: Search for the name of the alert action.
- Create: Opens the Create/Edit Alert Action popup.
- Edit: Opens the Create/Edit Alert Action popup.

- **Delete:** Remove the selected alert action.

<input type="checkbox"/>	Name	Syslog	Email	SNMP Trap	Control Script	External Only	
<input type="checkbox"/>	Notify Ops T...	Splunk	-None-	-None-	-None-	No	
<input type="checkbox"/>	System-Aler...	-None-	-None-	-None-	-None-	No	
<input type="checkbox"/>	System-Aler...	-None-	-None-	my_snmp	-None-	No	
<input type="checkbox"/>	System-Aler...	-None-	-None-	-None-	-None-	No	
<input type="checkbox"/>	System-Aler...	-None-	-None-	-None-	-None-	Yes	
<input type="checkbox"/>	server scale in	-None-	-None-	-None-	serverscalein	No	
<input type="checkbox"/>	server-scale...	-None-	-None-	-None-	server autos...	No	
<input type="checkbox"/>	test-anomaly	-None-	-None-	my_snmp	-None-	No	

This example shows the system default alert actions (*System-Alert-*) and some custom alert actions configured by a Vantage user. The default system alert actions may be modified, but not deleted.

The table on this tab contains the following information for each alert action:

- **Name:** The name of the alert action.
- **Syslog:** Shows whether the alert action is configured to send Syslog messages.
- **Email:** Shows whether the alert action is configured to send Email messages.
- **SNMP Trap:** Shows whether the alert action is configured to send SNMP traps.
- **Control Script:** Shows whether the alert action is configured to trigger execution of a ControlScript.
- **External Only:** Shows whether the alert action is configured to execute an external script.

Create/Edit an Alert Action

Alert actions may be stored locally on Vantage, and they may also be sent to remote systems. To direct alerts to a remote system, first configure a Notification or a ControlScript which may be referenced by the alert action.

New Alert Action:

• General Information •

Name

Only Generate External Alerts ?

AutoScale Trigger ?

Email ?

Select Email Notification
▼

Syslog ?

Select Syslog Notification
▼

SNMP Trap ?

Select SNMP Trap Notification
▼

ControlScript ?

Select ControlScript Profile
▼

Alert action options that can be configured here:

- **Name:** User friendly name for the action alert.
- **Only Generate External Alert:** By default, Vantage generates a local alert visible to admins of Vantage, in addition to any external alert systems configured. When this option is enabled, alerts mapped to this alert action will not generate a local alert within Vantage. Alerts may still be sent externally via any of the methods below.
- **AutoScale Trigger:** Use the alert to trigger AutoScaling.
- **Email:** Select an existing Email Notification.
- **Syslog:** Select an existing Syslog Notification.
- **SNMP Trap:** Select an existing SNMP Trap Notification.
- **ControlScript:** Launch a custom script. ControlScripts are Python-based scripts executed on the Avi Controller. These scripts may make configuration changes to Vantage, or send data externally to a remote system. For instance, a ControlScript could instruct an orchestrator to spin up new servers if all the servers are down within a pool or notify a security team if a virtual service is under a severe denial of service attack.