

Monitor VOS Devices and Organizations

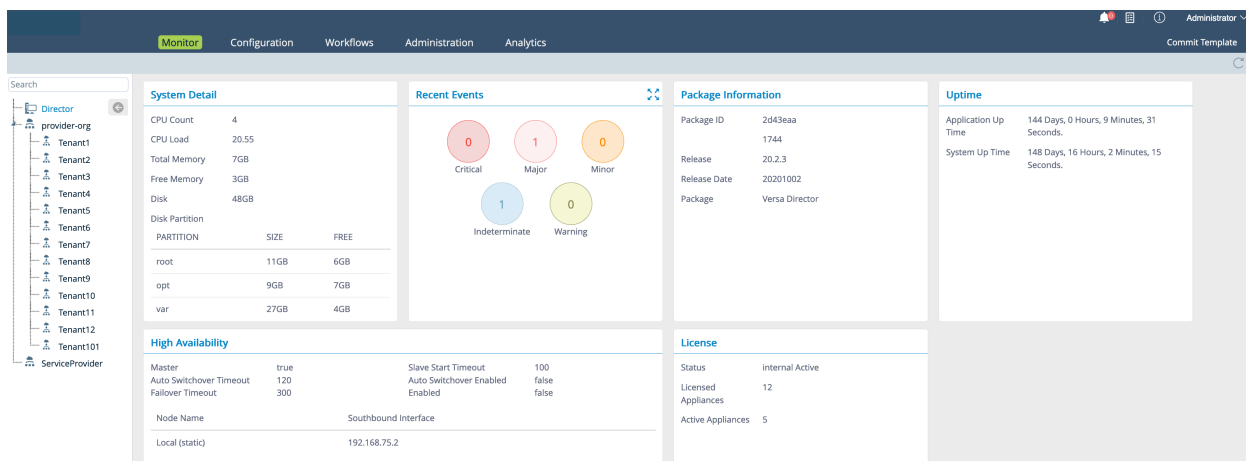
 For supported software information, click [here](#).

From a Director node, you can monitor the Director node itself, provider organizations, tenants, and Versa Operating System™ (VOS™) devices. You can view events and alarms generated by VOS devices, and you can create events and assign a status to each event. This article describes how to monitor devices and organizations.

The Director node, in conjunction with Versa Analytics, can poll VOS devices in real time to gain insight into what is happening on the devices. You can display this real-time information to gather information and to assist in troubleshooting. For information about real-time monitoring, see [Monitor VOS Devices in Real Time](#).

Monitor VOS Devices and Organizations

1. In Director view, select the Monitor tab in the top menu bar.
2. To display information about a Director node, select a Director node in the left menu bar.

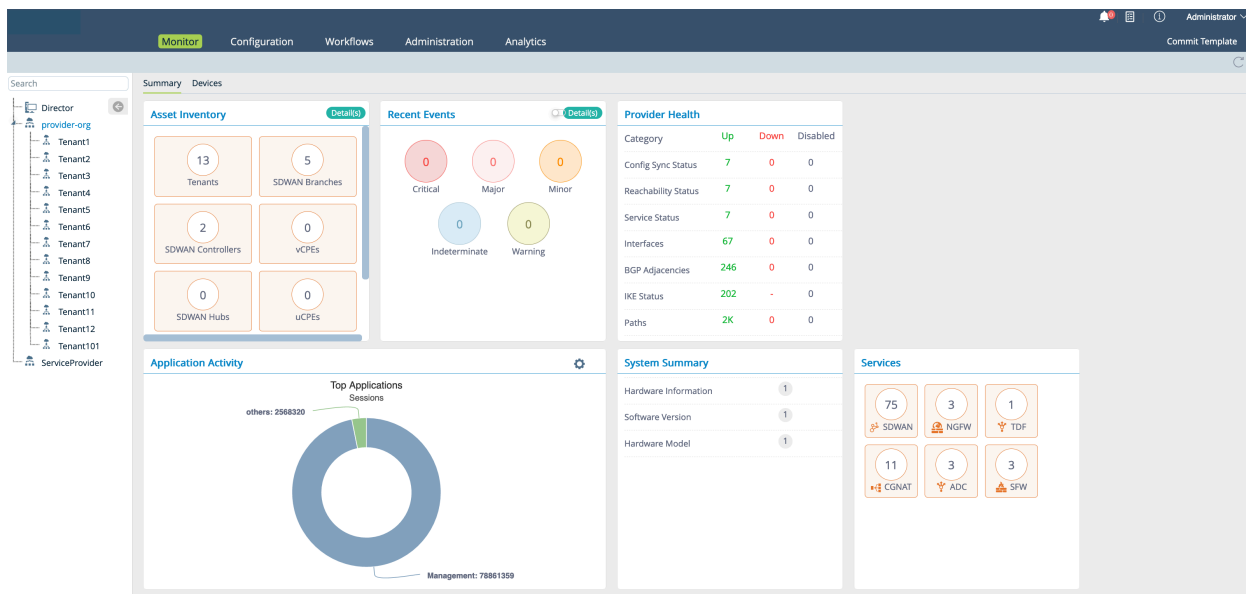


This screen contains the following panes:

- **System Detail**—Displays information about the Director node itself, including CPUs, memory, disk, and disk partitions.
- **Recent Events**—Displays information about recent events and alarms that have occurred on the Director node, by severity. Click a circle to display more information about the events and alarms of a severity type. Click the X

icon to display the events and alarms in tabular format, and click the **Back** Back button to return to the pane format.

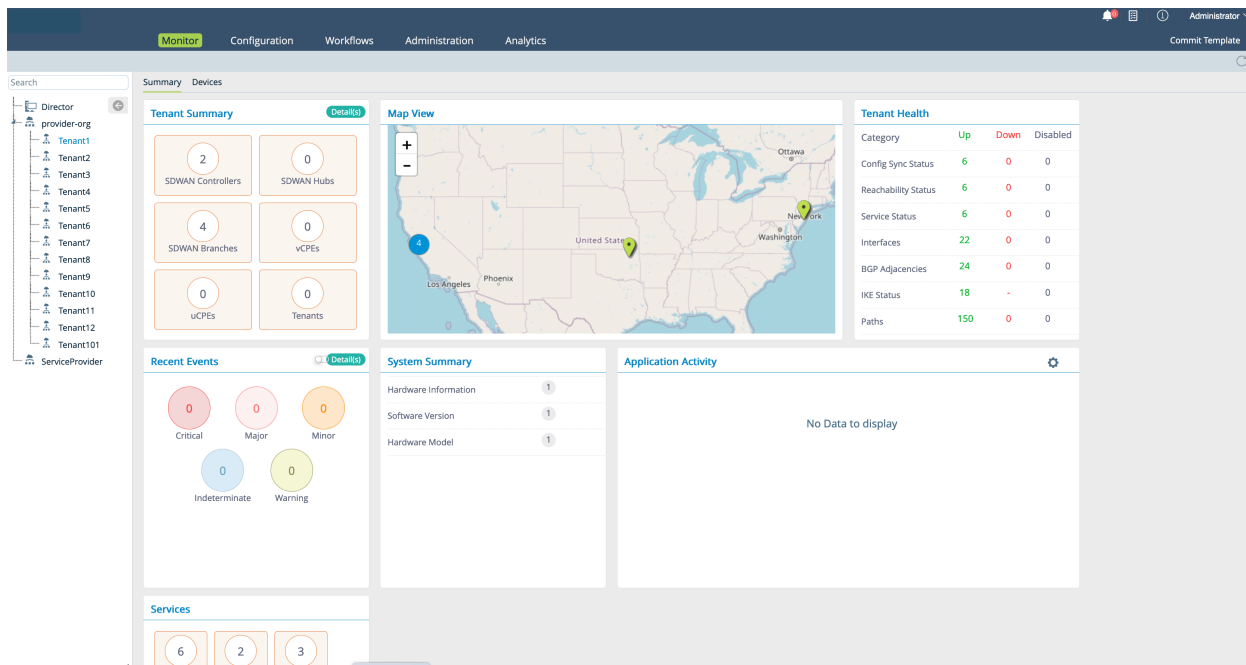
- **Package Information**—Displays information about the software package running on the Director node.
 - **Uptime**—Displays information about how long the Director node and its software have been up and running.
 - **High Availability**—Displays information about the Director node high availability (HA) configuration.
 - **License**—Displays information about the licenses that are installed on the VOS devices that the Director node is managing.
2. To display information about a provider organization, select a provider organization in the left menu bar, and then select the Summary tab in the horizontal menu bar.



This screen contains the following panes:

- **Asset Inventory**—Displays the number of tenants, SD-WAN branches, SD-WAN Controller nodes, vCPEs, SD-WAN hubs, uCPEs, Director nodes, and Analytics nodes in the organization. Click the **Detail** Details button to display more information about the assets in tabular format, and click the **Back** Back button to return to the pane format.
- **Recent Events**—Displays information about recent events and alarms that have occurred on the Director node, by severity. Click a circle to display more information about the events and alarms of a severity type. Click the **Detail** Details button to display the events and alarms in tabular format, and click the **Back** Back button to return to the pane format.
- **Provider Health**—Displays health-related statistics about the assets in the organization.
- **Application Activity**—Displays the applications that are exchanging the most data traffic. Click the Wheel icon to change the view.
- **System Summary**—Displays information about the provider organization's node itself, including CPUs, memory, disk, and disk partitions.

- **Services**—Displays number of services running in the provider organization.
3. To display information about a tenant organization, select a tenant in the left menu bar, and then select the Summary tab in the horizontal menu bar.

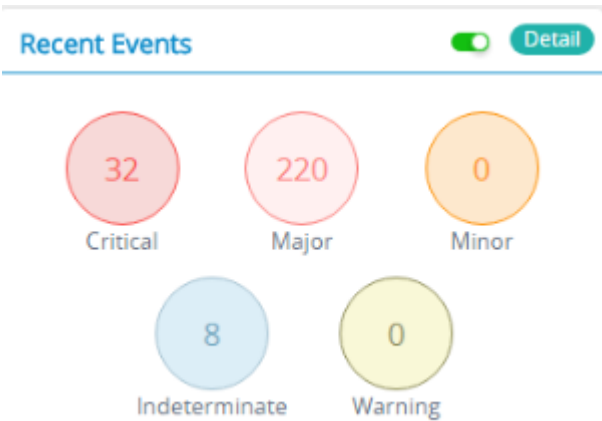


This screen contains the following panes:

- **Tenant Summary**—Displays the number of tenants, SD-WAN branches, SD-WAN Controller nodes, vCPEs, SD-WAN hubs, and uCPEs for the tenant. Click the **Detail** Details button to display more information about the assets in tabular format, and click the **Back** Back button to return to the pane format.
- **Map View**—Displays the geographical location of the tenants devices. Hover over a location to display the devices at that location.
- **Tenant Health**—Displays health-related statistics about the tenant.
- **Recent Events**—Displays information about recent events and alarms that have occurred on the tenant, by severity. Click a circle to display more information about the events and alarms of a severity type. Click the **Detail** Details button to display the events and alarms in tabular format, and click the **Back** Back button to return to the pane format.
- **System Summary**—Displays information about the tenant's node, including CPUs, memory, disk, and disk partitions.
- **Application Activity**—Displays the applications that are exchanging the most data traffic. Click the Wheel icon to change the view.
- **Services**—Displays number of services running on the device.

Display Recent Events

To display the recent events and alarms that have occurred on a Director node, in a provider organization, or for a tenant, select the Monitor tab in the top menu bar and then select the Director node, provider organization, or tenant in the left menu bar. The Recent Events pane provides a summary of all alarms by severity level—critical, major, minor, indeterminate, and warning.



Click the **Detail** Details button to display the events and alarms in tabular format:

The screenshot shows the 'Monitor' tab in the application. The table displays the following data:

Device Name	Organization Name	Alarm Type	Handling State	Severity	Status Change Time	Alarm Text
<input checked="" type="checkbox"/> Controller2	Provider	sdwan-branch-disconnect		major	Sat, Jan 27 2018, 05:26	Branch Site1Branch1 is connected
<input type="checkbox"/> Controller1	Provider	sdwan-branch-disconnect		major	Sat, Jan 27 2018, 05:26	Branch Site1Branch1 is connected
<input type="checkbox"/> Controller1	Provider	sdwan-datapath-down		major	Sat, Jan 27 2018, 05:23	Datapath from Controller1/MPLS to Site1Branc...

Click the **Back** Back button to return to the pane format.

Click the Column Filter icon to select the columns to be displayed.

Click the Alarms Filter icon to filter the alarms. In the Alarms Filter popup window, define the filters and then click Filter.

Alarms Filter

Alarm Search Criteria

Device Name

Controller1

Organization Name

ServiceProvider

Alarm Type

cpu-utilization-exceeded

Status Change Time

Severity

Major

Alarm Text

System Alarm

Cleared Alarm

Filter Type*

AND

Filter

Reset



Click a device to view its alarm history.

Related Events

Filter of severity -----Select----- X

Events (48)

Name	Event Time	Received Time	Severity
IPSEC tunnel with peer 10.2.0.105 (routing-instance Customer1-Control-VR) is...	3/10/2017, 5:01:49 AM	3/10/2017, 5:01:50 AM	major
IPSEC tunnel with peer 10.2.0.105 (routing-instance Customer1-Control-VR) is...	3/10/2017, 5:48:57 AM	3/10/2017, 5:48:58 AM	major
IPSEC tunnel with peer 10.2.0.105 (routing-instance Customer1-Control-VR) is...	3/10/2017, 12:46:23 PM	3/10/2017, 12:46:24 PM	major
IPSEC tunnel with peer 10.2.0.105 (routing-instance Customer1-Control-VR) is...	3/10/2017, 7:43:35 PM	3/10/2017, 7:43:37 PM	major
IPSEC tunnel with peer 10.2.0.105 (routing-instance Customer1-Control-VR) is...	3/10/2017, 9:00:06 PM	3/10/2017, 9:00:10 PM	major
IPSEC tunnel with peer 10.2.0.105 (routing-instance Customer1-Control-VR) is...	3/10/2017, 9:12:02 PM	3/10/2017, 9:12:04 PM	major
IPSEC tunnel with peer 10.2.0.105 (routing-instance Customer1-Control-VR) is...	3/10/2017, 10:56:23 PM	3/10/2017, 10:56:26 PM	major
IPSEC tunnel with peer 10.2.0.105 (routing-instance Customer1-Control-VR) is...	3/11/2017, 5:53:26 AM	3/11/2017, 5:53:29 AM	major
IPSEC tunnel with peer 10.2.0.105 (routing-instance Customer1-Control-VR) is...	3/11/2017, 6:39:34 AM	3/11/2017, 6:39:37 AM	major
IPSEC tunnel with peer 10.2.0.105 (routing-instance Customer1-Control-VR) is...	3/11/2017, 1:36:30 PM	3/11/2017, 1:36:33 PM	major
IPSEC tunnel with peer 10.2.0.105 (routing-instance Customer1-Control-VR) is...	3/11/2017, 2:23:19 PM	3/11/2017, 2:23:22 PM	major

Click the  Eye icon in the Handling State column of the Events screen to assign tasks. Alternatively, select the check box corresponding to a device record and click the  Handle/Assign icon on the top right menu bar to assign tasks.

Monitor

Configuration

Workflows

Administration

Analytics

Administrator

Commit Template




Search

Search

Back

1

25

Device Name	Organization Name	Alarm Type	Handling State	Severity	Status Change Time	Alarm Text
<input checked="" type="checkbox"/> Controller2	Provider	sdwan-branch-disconnect		major	Sat, Jan 27 2018, 05:26	Branch Site1Branch1 is connected
<input type="checkbox"/> Controller1	Provider	sdwan-branch-disconnect		major	Sat, Jan 27 2018, 05:26	Branch Site1Branch1 is connected
<input type="checkbox"/> Controller1	Provider	sdwan-datapath-down		major	Sat, Jan 27 2018, 05:23	Datapath from Controller1/MPLS to Site1 Branc...

The Alarm Handling screen displays. The screen displays the tasks assigned by the operator or the administrator. Enter information for the following fields.

Handling Events (1)

State	User	Assigned By	Description
observation	Operator	Administrator	Error detected

Description*

Alarm State*

--Select--

Assignee

--Select--

Submit

Field	Description
Description	Enter a description for the event.
Alarm State	Select the alarm state: <ul style="list-style-type: none"> Acknowledge Close Investigation None Observation
Assignee	Select the assignee.

Then click Submit.

Supported Software Information

Releases 20.2 and later support all content described in this article.

Additional Information

[Configure Log Collectors and Log Exporter Rules](#)

[Monitor and Manage Devices in Customer Organizations](#)

[Monitor VOS Devices in Real Time](#)