# Table of Contents

## Use the app
- Log in and get started ................................................................. 1
- User roles ..................................................................................... 2
- Dashboards overview ................................................................. 3
- Navigation and operation ............................................................. 7

## Dashboard Reference
- Home ............................................................................................ 10
- Knowledge Objects ....................................................................... 14
- Proactive Monitoring ................................................................. 15
- Virtual Machine Detail ............................................................... 22
- Host System Detail ....................................................................... 26
- Cluster Detail ................................................................................ 29
- Datastore Detail ........................................................................... 32
- Performance of Hosts and VMs .................................................. 36
- Capacity Planning Hosts .............................................................. 38
- Capacity Planning Clusters .......................................................... 40
- Capacity Planning for Clusters - CPU Headroom ...................... 42
- Capacity Planning for Clusters - Memory Headroom ................. 44
- Capacity Forecasting ................................................................. 45
- Virtual Machine Snapshots .......................................................... 47
- ESXi Log Browser ....................................................................... 49
- vCenter Log Browser .................................................................. 50
- ESXi Hosts Task Overview ......................................................... 52
- Task and Event Details ............................................................... 52
- Security Overview ........................................................................ 53
- Useful Saved Searches ............................................................... 54
- Threshold Configuration .............................................................. 55
- Collection Configuration ............................................................ 56
- App Install Health ........................................................................ 57
- App Data Volume ......................................................................... 58
- Hydra Framework Status ............................................................ 59
- Hydra Scheduler Status ............................................................... 62

## Reference
- Common use cases ....................................................................... 64
- Reports .......................................................................................... 66
Use the app

Log in and get started

You now have the Splunk App for VMware installed in your environment and it is configured to collect performance data from your vCenter servers. You can also (optionally) collect syslog data from your ESX/i hosts and from your vCenter Servers and forward the data to the app.

Use the app to proactively monitor and troubleshoot your environment.

Requirements

- You have a Splunk Enterprise username and password. Use this to log in to the Splunk App for VMware. Contact your system administrator for more information.
- The Splunk App for VMware is set up to run on a search head and you have network access to it.

Log in to Splunk Web

To log into Splunk Web and access the Splunk App for VMware:

1. Check that Splunk Enterprise is running in your environment.
2. Open a browser and log into Splunk Web on your search head. Access Splunk Web at http://<hostname>:port where hostname is the host system and port is the port you specified during the installation (the default port is 8000).
3. Log in using the default login, username=admin and password=changeme.
4. When using a Splunk Enterprise license, launching Splunk Web for the first time takes you to the login screen. Follow the message that asks you to authenticate with the default credentials.
5. When you sign in with your default password, you are asked to create a new password. You can either skip this step or create a new password (optional). You do not need to authenticate to use Splunk Enterprise with a free license. In this case, when you start Splunk Web you are directed to the Home page or to the default App for your account.
6. Select App > VMware to navigate to the Splunk App for VMware.
7. In the Splunk App for VMware, select Home. The Home dashboard provides an overview of the health of your virtualized environment.
User roles

Role-Based Access Control

The Splunk App for VMware provides role-based access control. Two roles are defined to provide operators and administrators of the Splunk App for VMware with the specific access each needs.

The default role settings are specified in

```
$SPLUNKHOME/etc/apps/splunk_TA_vmware/default/authorize.conf
```

The following two roles are defined:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>splunk_vmware_user</td>
<td>Select the user role to assign a permission level for operators of the app who manage virtual environments. As a user you are interested in looking at the data in the dashboards.</td>
</tr>
<tr>
<td>splunk_vmware_admin</td>
<td>Select the admin role to assign a permission level for administrators of the app who are responsible for installing the app and configuring it to collect data from your virtual environment.</td>
</tr>
</tbody>
</table>

The following table lists the dashboards that each role can access in the Splunk App for VMware:

<table>
<thead>
<tr>
<th>Dashboard</th>
<th>User role</th>
<th>Admin role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Search</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Knowledge objects (reports and dashboards)</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Proactive Monitoring and Entity views</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Performance and capacity planning views</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Troubleshooting and security</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Threshold Configuration</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Collection configuration</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

Both the admin role and the user role have permissions to search the following indexes by, default, when no index is specified in the search:
Dashboards overview

This topic introduces you to all of the dashboards in the Splunk App for VMware.

More detailed descriptions of each of the dashboards are available in the Dashboard Reference.

### Dashboard description

<table>
<thead>
<tr>
<th>Menu name: Dashboard name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Home                     | On the Home page you can find details about virtual machines and hosts that are in a critical state in your environment.  
This is the first place to look to see if there's any trouble in your environment. Get high level information about your datastores and check on recent VMware alarms. See Home. |
| Knowledge Objects: Reports | Extend the current app functionality or create custom dashboards by editing the properties of a report or adding a report to a dashboard. See Knowledge Objects. |
| Knowledge Objects: Dashboards | Edit dashboards to extend the current app functionality and customize them to meet your own needs.  
This a list of of all of the dashboards that the Splunk App for VMware uses. See Knowledge Objects. |
<table>
<thead>
<tr>
<th>Menu name: Dashboard name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proactive Monitoring</td>
<td>Use the proactive monitoring view to get an overall view of the topology of your VMware environment. Drill down and view specific areas of your environment or pin entities for later comparison. See Proactive Monitoring.</td>
</tr>
<tr>
<td>Proactive Monitoring: Entity view: Virtual Machine Detail</td>
<td>Get more detailed information about a specific virtual machine in your environment such as the configuration and status of the virtual machine, changes to the virtual machine configuration, migration history, and so on. See Virtual Machine Detail.</td>
</tr>
<tr>
<td>Proactive Monitoring: Entity view: Host System Detail</td>
<td>Get more detailed information about a specific host system such as the host configuration and status, recent tasks and events, and more information specific to the selected host. See Host System Detail.</td>
</tr>
<tr>
<td>Proactive Monitoring: Entity view: Cluster Detail</td>
<td>Get more detailed information about a cluster. See Cluster Detail.</td>
</tr>
<tr>
<td>Proactive Monitoring: Entity view: Datastore Detail</td>
<td>Get more detailed information about your data stores, such as the type of storage, the capacity of the storage, the free space available, and so on. See Datastore Detail.</td>
</tr>
<tr>
<td>Performance and Capacity planning: Performance of Hosts and VMs</td>
<td>Chart the performance of selected host systems or selected virtual machines for specific performance metrics over the selected time period. Visually compare the performance of hosts and virtual machines in your environment. See Performance of Hosts and VMs.</td>
</tr>
<tr>
<td>Performance and Capacity planning: Capacity Planning Hosts</td>
<td>See how the hosts in your environment use memory and cpu</td>
</tr>
<tr>
<td>Menu name: Dashboard name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Performance and Capacity planning: Capacity Planning Clusters</td>
<td>See how a cluster uses memory and CPU resources. See Capacity Planning Clusters.</td>
</tr>
<tr>
<td>Performance and Capacity planning: Capacity Forecasting</td>
<td>Predict the usage of the resources (CPU, memory, and disk) in your virtual environment over time. See Capacity Forecasting.</td>
</tr>
<tr>
<td>Troubleshooting and Security: Hydra Scheduler Status</td>
<td>Use the Hydra Scheduler Status page to identify issues related to jobs handled your scheduler.</td>
</tr>
<tr>
<td>Troubleshooting and Security: Hydra Framework Status</td>
<td>Use the Hydra Framework Status page to identify issues related to jobs</td>
</tr>
<tr>
<td>Menu name: Dashboard name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Troubleshooting and Security: ESX/i Log Browser</td>
<td>Get quick access to ESX/i log data (collected via syslog) by filtering the results using the Log Browser. See ESXi Log Browser.</td>
</tr>
<tr>
<td>Troubleshooting and Security: vCenter Log Browser</td>
<td>Get quick access to vCenter log data (collected via syslog) by filtering the results using the Log Browser. See vCenter Log Browser.</td>
</tr>
<tr>
<td>Troubleshooting and Security: ESX/i Host Task Overview</td>
<td>Get quick access to the tasks performed on hosts and virtual machines in your environment. See ESXi Hosts Task Overview.</td>
</tr>
<tr>
<td>Troubleshooting and Security: Task and Event Detail</td>
<td>Monitor tasks and events in your environment over a selected time period. Get insight into user and system actions. See Task and Event Details.</td>
</tr>
<tr>
<td>Troubleshooting and Security: Useful Saved Searches</td>
<td>Use the reports to extend the functionality of dashboards or to create new custom dashboards. See Useful Saved Searches.</td>
</tr>
<tr>
<td>Settings: Threshold Configuration</td>
<td>See a list of metrics collected by the Splunk App for VMware that have default threshold values set. Configure values for thresholds for existing metrics. Add or remove performance metrics collected by the Splunk App for VMware. See Threshold Configuration.</td>
</tr>
<tr>
<td>Settings: App Install Health</td>
<td>Check that the Splunk App for VMware is set up correctly and that it collects data from your environment. See App Install Health.</td>
</tr>
<tr>
<td>Settings: App Data Volume</td>
<td>Get information about the data that is indexed. Check the status of the</td>
</tr>
<tr>
<td>Menu name: Dashboard name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>Splunk App for VMware licenses that you have installed. See App Data Volume.</td>
</tr>
</tbody>
</table>

**Note:** Collection Configuration page will not be visible from `splunk_for_vmware` app. A user can see this page from `Splunk_TA_vmware` app.

## Navigation and operation

### Navigating the topology map

The topology map is used to represent your VMware vSphere environment. You can access it on the Proactive Monitoring dashboard.

You can navigate your topology map in two dimensions. This provides an alternate view to the data displayed.

- To pan within the view, click and drag the map.
- To zoom in or out, click + or - on the legend.

You can get additional information about your environment:

- Hover on a node to display the tooltip for that node.
- Click on a node to display or hide the child entities of that node.
- Parent nodes have node status indicators (a doughnut chart wrapped around the node).
  - A node that is red is in a critical state for the metric selected.
  - A node with a ring around it provides a visual view of the state of the environment under that node.

See [Proactive Monitoring](#) for more information.

### Making selections

You can filter the data displayed on many of the dashboards using drop-down list, autocomplete textboxes, or a menu tree.

**Drop-down lists**

Select an item from the list to filter your search selection. In many of the dashboards search selection filtering is done using a combination of drop-down
lists and one other search method.

**Autocomplete textbox**

Use the autocomplete search feature to search your VMware vSphere hierarchy of entities. Navigating very large environment is fast and easy. You can perform two different types of search:

- Entity level search.
- Full path search.

You can search using the name or a partial name of an asset. As you type, the textbox automatically generates a drop-down list of predicted searches based on your search criteria. Predictive search allows you to search on a single entity at a time. Search predictions are based on all of the search characters entered in the text box.

If your search term does not display any results, then the specific asset is not in your environment. Try generalizing your search.

**Examples**

- Search for a host, for example esxi-01:
  - Select the host button to predetermine the search type.
  - Enter any part of the asset name, such as "01", to get a list of all possible matches. The full hierarchy for the entity is displayed in the drop-down list and the hosts that match the search criteria are displayed and highlighted in a list to the right of the hierarchy.

- Search for a virtual machine, for example vmw-65-01:
  - Select the VM button to predetermine the search type.
  - Enter the search criteria, such as "vmw", and a drop-down list is populated with all possible matches. The full hierarchy for the entity is displayed in the drop-down list and the virtual machines are displayed and highlighted in a list to the right of the hierarchy.

- Enter an invalid option and the the text box turns red to indicate an invalid entry.
- Use the up arrow on your keyboard to move up a selection in the list.
- Use the down arrow on your keyboard to move down the selection in the list.
**Menu tree**

Use the menu tree to search across multiple entities at a time. It supports the multi-select feature.

**Color usage**

The level of criticality in your environment is highlighted in the app using a basic color set. The following colors are used as indicators:

- Red indicates a critical state.
- Orange indicates a warning state.
- Green indicates normal operation for your environment.
- Grey indicates that the data is unavailable or that the entity is not powered on.
Dashboard Reference

Home

The Home page displays details about virtual machines and hosts that are in a critical state in your environment. This is the first place to look to see if there’s any trouble in your environment.

To check that you are receiving data, you can look at the Proactive Monitoring view and see that the topology tree is built from your environment, or you can look at the App Install Health page.

All of the panels in this dashboard (except for Recent Alarms) are driven by performance metrics.

Understanding the gauges

The first two panels in this dashboard report on this set of key metrics that enable you to monitor the health of the virtual machines and hosts in your environment.

As the value changes over time, the gauge marker changes position within this range. Gauges provide a dynamic visualization of saved searches.

Each of the gauges in the Virtual Machine Health panel and Host System Health panel are graphical representations of the entities (hosts and virtual machines) that are in critical states in your environment for the specified metrics. The gauges measure how your entire environment performs for the critical level. Each gauge displays a percentage (of the total number) of virtual machines and hosts that are in a critical state, over the time period specified, for the specific metric. This value is a numerical representation of the display on the gauge and is based on the same search used to drive the gauge. It displays the current result for that search and the display changes as the results of the search change. The numerical value is mapped against a range of colors. As the value changes over time, the gauge marker changes position within this range.

A gauge can be in one of the following states:

- Red - when virtual machines or hosts are in a critical state for the metric.
- Orange - when virtual machines or hosts are in a warning state for the metric.
• Green - when virtual machines or hosts are in a normal state for the metric.

In addition to specifying a percent value, each gauge can also display:

• 0% - A gauge that displays 0% indicates that none of the virtual machines or hosts in your environment are in a critical state for that metric.
• " no data" - A gauge displays this message when performance data is not collected from your environment and is not coming into Splunk.

Looking at the gauges you can identify if there are problems with hosts or virtual machines that need immediate attention in your environment.

A performance metric for a virtual machine or for host system can be in one of three states: normal, warning, or critical and are driven by the thresholds set for them. You can modify the thresholds for the metrics on the Threshold Configuration page of the app.

For example, in this dashboard a gauge that shows a value of 0% for High CPU Usage indicates that none of the virtual machines in your environment are in a critical state for that metric. This means that of all the performance data that is collected for all of the virtual machines, none of the virtual machines in your environment have a performance metric that meets the critical threshold level set for it. Each of the metrics measured have default thresholds defined for them in the app. You can see the default values or configure other values using the Threshold Configuration dashboard in the app. For information on how to configure critical and warning thresholds for the metrics, see "Add, edit, and delete threshold settings" in the Splunk App for VMware Configuration Guide.

Virtual Machine Health

The gauges displayed in this panel are a measure of how your virtual machines perform for the critical level.
The following key metrics, used to show the health of the virtual machines, drive the gauges in the Virtual Machine Health panel:

- **High CPU usage** - The threshold for the metric `average_cpu_usage_percent` drives this gauge. This is the virtual machines's average cpu usages as a percent value.
- **High memory usage** - The threshold for the metric `average_mem_usage_percent` drives this gauge. This is the average of the amount of memory the virtual machine uses, as a percent value.
- **High CPU Sum Ready time** - The threshold for the metric `summation_cpu_ready_millisecond` drives this gauge. This metric is measured in milliseconds and it is a measure of how long a virtual machine has been waiting for processing time from the host. The virtual machine is ready, but it can't do anything as the host has not allocated any resources to it. Sometimes a virtual machine that has too many resources allocated to it does not get scheduled to run by the host and is left waiting.

- **Total VMs**: This is a count of the total number of virtual machines in your environment. Click on the number for Total VMs to see more details about each of the virtual machines in your environment, such as the host system that it is on and the associated vCenter.
- **Total VM Migrations**: This is the total number of virtual machines that migrated. Click on the number for Total VM Migrations get more details about the virtual machines that migrated in the last four hours. To see the virtual machines that migrated the most, you can re-order this list by "TotalMigrations".

**Host System health**

The gauges displayed in this panel measure how your host systems perform for the critical level.

The following key metrics, used to show the health of the host systems, drive the gauges in the Host System Health panel:

- **High Memory Ballooning** - The threshold for the metric `average_mem_vmmemctl_kiloBytes` drives this gauge. This is the sum of all values from VMware's ballooning driver for all powered-on virtual machines. The host memory must be large enough to support the active memory of all virtual machines on the host. This number should be 0. Balloon drivers activate when memory is scarce. It's best not to have any ballooning activity.
• High Memory swapping - The threshold for the metric average_mem_llSwapUsed_kiloBytes drives this gauge. This is the amount of memory from all virtual machine that has been swapped by the host. This is a host swapping memory and is always a sign of the host being in a stressed state. Whenever this threshold is triggered, the host has no memory, and cannot reclaim it from the ballooning driver. This number should be 0.

• High CPU usage: The threshold for the metric average_cpu_usage_percent drives this gauge. This is the host systems average cpu usages as a percent value.

• Total Hosts: This is a count of the total number of hosts in your environment. Click on the value displayed for Total Hosts to see more details about each individual host.

Datastore information

Look at this panel to get information about all of the datastores in your environment. The data is measured in Mega bytes. (It is not a percentage value.) The indicator shows the amount of free space and the amount of storage committed.

You can quickly see if a datastore is close to capacity and in a critical state. Datastores can be in critical, warning, or normal operational states. If the app cannot gather sufficient information about a datastore then the datastore is represented in gray, indicating that the data for the datastore is unavailable or that the entity is not powered on.

Recent VMware alarms

In this panel you can see events that occurred in your environment that triggered alarms. Alarms can be triggered for a number of reasons such as memory usage reaching a critical level for a virtual machine or cpu usage for a host reaching a critical level.

For example, click on an alarm for "virtual machine memory usage" to see the event that triggered it. The Virtual Machine detail page is displayed. You can now see details about the event that triggered the alarm:

Max CPU usage during the selected time range peaked at a critical level with value of 112%. This VM may be undercommitted on CPU or the host is stressed.
The source type `vmware:events` drives the data that is displayed in this panel.

**Knowledge Objects**

This topic describes the reports and dashboards provided as knowledge objects in the app.

**Reports**

On this dashboard you have access to all of the reports used in the Splunk App for VMware. Reports are created from saved searches. You can use the default reports or you can customize the reports to suit your environment. Click on a report title to see the report. The time range for each of the reports is set by default to -8h.

You can:

- Open the report in the Search window and edit the search that powers it. From here, you can clone the report and save it as a Dashboard Panel, an Alert, or an Event Type
- Edit the description and the permissions for a report.
- Schedule a report.

For a description of each of the reports, see "Reports" in the reference section of this manual.

**Dashboards**

On this dashboard you have access to all of the dashboards used in the Splunk App for VMware. You can customize the dashboards to suit your environment.

You can:

- Modify the content of any of these dashboards by editing the source XML.
- Change the title and descriptions of dashboards.
- Clone a dashboard and use the basic functionality to power another dashboard.

For a description of each of the dashboards, See "Dashboards overview" in this manual.
Proactive Monitoring

Use the Proactive Monitoring dashboard to quickly troubleshoot your environment and get to the details to identify problems in your infrastructure. You can see how different entities in your environment perform for different performance metrics. Use this data to directly manage any performance concerns that you have in your IT environment (at scale) and to prevent bottlenecks and outages in other areas of the enterprise.

The main focus of the Proactive Monitoring dashboard is the topology tree, built from topology information from vCenter. The topology tree provides insight to the overall state of your virtual environment. The tree is sorted based on the count of critical entities in your environment, with the most critical entities shown on the left hand side of the tree.

You can:

- Change how you view the topology tree. You can display the topology from the host system or the virtual machine perspective.
- Change the performance metric type displayed. The tree is redrawn to display your environment for the new metric.
- Navigate around your environment expanding and reducing the view of your environment.
- Drill down to the entity level to get a more detailed view of that entity.
- Compare how entities perform for different metrics.

The data displayed in the topology map is performance data based on the metrics data that the app collects and uses to monitor the performance of your environment. Note that in the Splunk App for VMware, the performance metric name (for example, average_cpu_usage) and the value used to measure it (percent) are connected as shown by the display name for the metric (average_cpu_usage_percent).

The Topology Tree

The Topology tree is a top down representation of the hierarchy of the entities in your VMware environment (from the selection point). The environment displayed by the topology tree depends upon how you navigate to the Proactive Monitoring dashboard. The entire tree is sorted based on the count of critical entities, so the left hand side will always have the most critical stuff.
Drill down from the **Home** dashboard. In this case the tree displayed is predetermined by the source of the data. For example, if you click **High CPU Usage** in the Hosts panel and drill down to the Proactive Monitoring dashboard from the Home dashboard, the tree is generated and populates with information from the host level for the metric used to determine High CPU Usage (average_cpu_usage_percent).

Navigate using the App menu. You can navigate to the Proactive Monitoring view using the App menu. In this case the tree is generated when you use the drop-down lists to filter your selection for displaying the topology map of your environment.

Each node in the tree represents an entity in your environment. Environments, virtual centers, clusters, and hosts stack horizontally in the tree. Virtual machines are displayed in a vertical stacks underneath their parent host node, to the right side of the anchor point. Each of the entities are sorted by criticality (red, yellow, green).
The severity levels displayed by each node (and node indicator) are driven by the thresholds set for the metrics selected. You can change a metric for the displayed entities or change the entity and the tree updates and repopulates with the latest information (within seconds).

You can select how you want to view your environment. You can view the topology map down to the hosts system level or get a complete view down to the virtual machine level. The ability to pan across the topology map or zoom in to specific entities enables you to get the visibility you need to actively monitor your environment.

The color coding of the nodes on the topology tree provides a bottom up indication of the status of your environment. Nodes are colored red, yellow, or green indicating the level of criticality in the entity or in the child entities. This color coding gives you a quick status of the node. You can get more details when you hover over a node to display the associated tooltip.

You can compare the entities for selected metrics when you pin them on the pinboard. You can drill down on nodes in the topology tree to more detailed views of specific entities to find the root cause of problems in your environment.

Use the drop-down lists on the dashboard to filter your selection for displaying the topology map of your environment.

To create a topology map using the drop-down lists:

- Select an Entity type. This can be virtual machine or host system.
- Select a Performance Type. This is the type of performance data (such as cpu, mem, disk, and so on) upon which to base the performance measurement of your environment.
- Select a Metric. Each performance data type has a set of metrics associated with it. Metrics have thresholds set for them in the Splunk App for VMware. The level of criticality in the system is determined by the average of the metric for a particular entity in relation to the metric's threshold settings.
- Select a time range over which you want to run the search.
- Click Search to create the topology map.

The topology tree populates only if you have set values in the drop-down lists on the dashboard. These values power the searches that generates the topology map.

Note that the topology tree does not function in real time.
**Nodes**

A node represents a single entity in your VMware vSphere hierarchy. It contains references to its parents and children, threshold status, name, identifiers, and so on. Nodes are used to show the overall state of the entity it represents (cluster, host, virtual machine) and are color coded to provide a quick view of the state of your environment. The nodes display green, yellow, or red depending on the state of the environment. Nodes at the virtual machine level are organized by criticality. Virtual machines that are in the most critical state appear higher in the hierarchy, while those in a healthier state appear lower on the hierarchy.

Nodes have a status associated with them. All leaf nodes show a single color, which is the status for that node, while parent nodes display a color indicating the highest level of criticality for the nodes in the environment below it. Parent nodes also display node status indicators. You can:

- Hover on a node to display the tooltip for the node.
- Click on a node to expand it and display the child nodes.
- Pin a node to the dashboard so that you can compare the details of that node with other nodes.

**Node status indicator**

The node status indicator is a doughnut indicator that encompasses a node. Only nodes that have children (parent nodes) display this indicator. It provided a quick view into the status of your environment. The absence of an indicator indicates that the node does not have children and does not expand further.

The node status indicator can be divided into three segments to show the state of the selected performance metric for the entities in the environment. A metric for an entity can be in one of four states - normal, warning, critical, or unknown/offline. Each segment of the three segment chart around the node indicates the portion of children nodes in each of the three status states (red, yellow, green). The color of the node itself (the color in the center) indicates the status of the largest group of entities in your environment.
**Tooltips**

A tooltip is displayed when you hover on a node in the topology map. Tooltips are displayed for specific entities (virtual machines, hosts, clusters) in your environment. They display data for that entity, the complete environment, and/or a branch of the hierarchy.

Using the tooltip you can:

- See the state of the metric (in this example, `summation_cpu_ready_millisecond`) measured for the selected entity over time.
- Pin the entity. This enables you to compare it (on the pinboard) to other entities in your environment.
- Drill down to get detailed information on the entity.

For example, if you hover over a virtual machine, the tooltip displays the following information:

- The name of the virtual machine.
- The time range over which the data is mapped.
- The metric used to measure the performance of the particular virtual machine.
- A distribution stream chart that maps performance data distribution over time for a selected metric.
  - The white line on the tooltip represents the performance of the virtual machine or the average of all nodes in the branch mapped for the specific metric selected, over the specific time range.
  - The light grey line is the global median.
  - The light grey zone displays results within 1 standard deviation of the global median.
  - The dark grey zone displays results within 2 standard deviations of the global median.

**Note:** Host information is displayed in the tooltip when host is selected.
Pinning an entity

Having the ability to compare data for different entities in your environment is very powerful. In the Splunk App for VMware you can organize and compare various parts of your environment for different performance metrics and different entities.

The pinboard in the Proactive Monitoring dashboard is used to store pinned entities in your environment. A pinned entity is one that you selected in the topology tree to save to the pinboard so that you can compare it with other entities. Pinned entities stay on the dashboard even when you change the entity and metric used to monitor the behavior of your environment. You can drill down on the entities within a pinned entity.

The pinboard is a collection of detailed views. When a parent node is pinned, detail information for it and the child entities is displayed in the detail pinned panel. When a leaf node is pinned, a detail pinned panel is displayed showing information only for that entity.

Note that the data displayed for pinned entities is not affected by changing the time range on the page. Pinned entities are not preserved upon reloading a page. Once a page reloads you must pin entities once again. You can delete the entity or minimize it. All other actions on the page have no effect on it.

To pin an entity:

1. Hover over a node to display the tooltip for that node.
2. Click the pin in the tooltip.
3. The entity is pinned on the pinboard.
4. The detail pinned panel is displayed for the particular entity.

Virtual Center detail pinned panel

When you pin a virtual center to the pinboard, detailed information about the virtual center is displayed in the detail pinned panel. This information includes the following:

- A title bar showing the name of the virtual center and a link to navigate to details page (arrow).
- The total number of hosts managed by the virtual center.
- The total number of virtual machines on the hosts.
- The number of clusters.
• For each host, a sparkline chart is displayed that shows the event count trend for cpu performance for the hosts. Now you can easily compare systems and see patterns in your data that may have been invisible before. For example, if you monitor cpu performance (based on percentage usage) of the host systems in your environment, when you pin a virtual center (or cluster) to the pinboard, a sparkline chart is displayed that shows the event count trend for cpu performance for the hosts over the specified time period for the selected metric.

**Cluster detail pinned panel**

When you pin a cluster to the pinboard, the following information is displayed in the detail pinned panel for the cluster:

• A title bar that shows the name of the cluster and a link to navigate to details page (arrow).
• AvgEffCpu_MHz. The total available CPU resources of all hosts within a cluster (in MHz).
• AvgEffMem. The total amount of memory of all hosts in the cluster that can be used for virtual machine memory.
• A list of all of the hosts in the cluster. The following is displayed for each host:
  ♦ An indicator showing the current status of the host. The list of hosts is sorted by criticality, with the most critical shown at the top of the list.
  ♦ The name of the host.
  ♦ A sparkline chart that shows the event count trend for the host for the specific performance metric.

**Host detail pinned panel**

When you pin a host system to the pinboard, detailed information about the host is displayed in the detail pinned panel. This information includes, but is not limited to, the following:

• A title bar showing the host name and a link to navigate to details page (arrow).
• The overall status of the host (green, yellow, red).
• The manufacturer and model number of the host.
• System specifications such as the number of NICs, processors, and sockets.
• Memory and cpu usage of the host.
• Information about the cores.
• A chart showing the last 24 hours of processing load on the host system for the selected metric.

**Virtual Machine detail pinned panel**

When you pin a virtual machine to the pinboard, the following information is displayed in the tooltip for the virtual machine:

• A title bar. The tooltip title bar displays the virtual machine name and a link to navigate to the virtual machine details page (arrow).
• Power State. This shows if the virtual machine is powered on.
• numCPU. The number of vCPUs allocated to the virtual machine.
• guestFullName. The full name of the guest operating system installed and running in the virtual machine.
• toolsStatus. The status of VMTools, if it is installed.
• numCoresPerSocket. The number of cores per virtual socket.
• memorySizeMB. The amount of memory (in MB) allocated to the virtual machine.
• cpuReservation. The guaranteed cpu (in MHz) allocated to the virtual machine.
• memoryReservation. The guaranteed memory allocated to the virtual machine to ensure stable performance.
• memSharesLevel. The memory allocation level for the virtual machine.
• memSharesShares.
• cpuSharesLevel. The cpu allocation level for the virtual machine.
• cpuSharesShares.
• Performance chart. A graph showing the load on the virtual machine for the last 24 hour period. This is overlaid on a chart of the average load for all virtual machines on this host.

**Virtual Machine Detail**

On this dashboard you can see the details for a specific virtual machine. Using this dashboard you can:

• Track virtual machines in your environment as they migrate across hosts.
• Identify the root cause of issues.
• Check how the virtual machine performs for key performance metrics.
• Get insight into the granular virtualization layer data, which helps solve problems quickly.
Virtual Machine Configuration and Status

This panel provides basic configuration information about the state of your virtual machine. It displays:

- The name of the virtual machine.
- The operating system installed on it.
- The state of the virtual machine, whether it is powered on or off.
- A status for VMTools, if VMTools is installed on it.
- The resource details of the virtual machine. Having sufficient resources is important to prevent a bottleneck in your system. The resources include the number of vCPUs (cores) assigned to the virtual machine, the memory allocation as well as the reservations and shares for each of these resources.
- The cluster and the host to which it belongs. Drill down on the cluster or the host information to get to the detail dashboards for the selected entity.
- High level details about the datastore connected to the virtual machine and how much space the virtual machine is taking up on the datastore.

Drill down on the Datastore details

Click the datastore name to drill down to the specific details for that datastore, shown on the Datastore Detail dashboard.

Click [Click to Show] to see the file types and file sizes for this virtual machine. You get visibility into the types of files that take up space on the datastore. This
view enables you to plan your storage requirements. For example, if log files are taking up a lot of space, you can create a report that tells you the amount of space that log files are taking up on the datastore.

**Configuration Changes**

Look at this panel to see all of the configuration changes for the virtual machine.

You can investigate the root cause of problems. For example, If a virtual machine goes down you can check if a scheduled task or an unscheduled task was the cause of the outage. You can also check resource allocations, such as how CPU or memory resources changed for the virtual machine.

**Migrations**

Look at this panel to see all of the migrations for the specific virtual machine.

If the virtual machine migrated from one host to others over a period of time, the list of hosts is displayed. You can use the chart in the last panel to split migrations across hosts to get more detailed information.

**Chart of performance data for a virtual machine**

In this panel you can look at the virtual machine at a very detailed level. You can:

- Control the charting of performance data for a specific virtual machine.
- Show the performance of the virtual machine as it migrated across hosts.
- See when the virtual machine was last on a host.

The chart shows the performance of the virtual machine for a metric of a specific performance data type, optionally split by host, mapped against the critical and warning threshold for the metric selected. The chart is driven by performance metrics for the virtual machine.

Use the drop-down lists to filter your selection for charting the data. Select from the following:

- The performance type. This is the type of performance data you want to measure for the virtual machine.
- Instance data. If instance level data is turned on, this drop-down list is populated with values representing instances. If instance level data is not being collected from your environment, then the menu defaults to
aggregated (aggregated data for all of the instances).
• The performance metric to measure.
• The statistical operation on the data (average, min, max),

You can correlate the data with migration information for the virtual machine. Use the "split by" drop-down list to correlate the data by the physical host of the virtual machine (this is the physical host for a specific data point) You can see a history of where the virtual machine has been over a period of time (the hosts it resided on). You can also see when the virtual machine was last on a host.

**To filter the data and split by host:**

1. Select a performance type, such as cpu, from the drop-down list.
2. Select a value for instance data from the options available, if you have instance level data turned on, or select aggregated.
3. Select a metric for the performance type, such as average_cpu_usage_percent.
4. Select none or host. Selecting host charts the data and splits it by host. If the virtual machine migrated, all of the hosts on which it resided are displayed in the chart. Splitting by host shows a history of what host it was on and when. Keep the value at none if you do not want to split the results
5. Select how you want to view the data on the chart.

A chart is displayed showing the critical and warning threshold levels set for the selected metric. The performance of the virtual machine in relation to this metric is charted. If the virtual machine migrated from one host to others, then the results are split across the hosts. Check for spikes on the chart and investigate why they are happening.
Host System Detail

On this dashboard you can see the details for a specific host system over the time range selected. You can:

- Get a quick view of the state of your host system.
- Identify the root cause of issues on the host.
- Check how the host performs for key performance metrics.

You can drill down to this dashboard from another dashboard to see host detail information, or from the app menu, select Proactive Monitoring > Host System Detail, and search for the specific host using the search bar.

Host Configuration and Status

On this panel get basic configuration information about the state of the specific host. You can see:

- The status of the host.
- The available and total processing power (in MHZ) for the host.
- The available and total memory (in MB) for the host.
- The name of the host. This is the same name that is displayed in the search bar on the dashboard.
- The cluster to which it belongs, if it is configured as part of a cluster.
- Specific manufacturer and model number for the host.
- The hyperthreading status, active or none.
- The resource details of the host. Having sufficient resources is important. The resources include the number of NICs, the number of CPU cores assigned to the host, processor information, and socket information, in addition to the memory and processing allocations.
Connected Datastores

This panel shows a list of datastores connected to the host. Click the datastore name to drill down to the specific details for that datastore, shown on the Datastore Detail dashboard. You get visibility into the file types residing on that datastore. Using this information you can plan your storage requirements for the host.

Virtual Machine Information

This panel displays high level information about the virtual machines that reside on this host. You can see:

- The total number of virtual machines on the host.
- The total number of virtual machines powered on and off.
- The number of virtual machines that migrated off this host.
- The number of virtual machines that migrated on to this host.

Select the value associated with each of the fields to see specific details for that field. For example, click 23 for Total VMs to display a table with details for all the virtual machines on the host.

Recent Tasks and Events

You can view recent tasks associated with the host and event that have occurred on the host. This panel lists all completed tasks on the host. The task list includes tasks performed on the virtual machines on the host. You can see alarms that activate when there was a change status for a resource, for example, "Alarm 'Virtual machine memory usage' on apps-vc200 changed from Yellow to Green".

Use this information to investigate the root cause of problems on your host. For example, if a host goes down, you can see if a particular task caused it. You can also check if the host is resourced correctly.

Recent ESXi Log Entries

On this panel get a quick look at log files generated by VMware ESXi hosts. ESXi host logs are written to the file system and provide information about system operational events. You can examine the log files in detail drilling down to system events that can identify particular issues in your environment.
Chart of performance data for a host

On this panel you can look at the host system at a very detailed level and control the charting of performance data for a specific host based upon the selections you make from the drop-down lists.

The chart shows the performance of the host for a specific performance data type, mapped against the critical and warning threshold selected for the metric. The chart is driven by performance metrics for the host.

Use the drop-down lists to filter your selection for charting the data. Select from the following:

- The performance type. This is the type of performance data you want to measure.
- Instance data. When instance level data collection is turned on, performance data is collected as specific instances of performance counters. If instance level data is turned on, this drop-down list is populated with an identifier or a number of identifiers derived from configuration information. For example, the name of a disk, virtual Ethernet adapter, or CPU core. If instance level data is not from your environment, then the drop-down list defaults to aggregated (aggregated data for all of the instances).
- The performance metric to measure.
- The statistical operation on the data (average, min, max). This determines the chart results.

The chart displays the critical and warning threshold levels set for the selected metric. The performance of the host in relation to this metric is charted. Check for spikes on the chart and investigate why they are happening.

Cluster Detail

On this dashboard you can see the details for a specific cluster over the time range selected.

You can:

- Get a quick view of the state of the hosts in the cluster.
- Identify the root cause of issues in the cluster.
- Check how the cluster performs for key performance metrics.
Cluster Configuration and Status

On this panel get basic configuration information about the state of the cluster. You can see:

- The status of the cluster.
- The available and total processing power (in MHZ) for the cluster.
- The available and total memory (in MB) for the cluster.
- The total number of cores assigned to the cluster and the processing power of each (in MHZ).
Connected Datastores

Look at a list of datastores connected to the host systems in the cluster. Click the datastore name to drill down to the specific details for that datastore, shown on the Datastore Detail dashboard. You get visibility into the file types residing on that datastore. Using this information you can plan your storage requirements for the cluster.

Host System Members Information

Look at high level information about the host systems in the cluster. You can see:

- The total number of host.
- A roll up status of hosts that are in the normal, warning, and critical states for the thresholds defined.

To get more details for each hosts system, click on the value associated with the field. For example, click 23 for Total Hosts to display a table with details for all the host systems in the cluster.

Recent Tasks and Events

Look at recent tasks and events that have occurred on the cluster. This panel lists all completed tasks on the cluster. The task list includes tasks performed on the host systems, for example, you can see alarms that activate when there is a change status for a resource on a host system.

Use this information to investigate the root cause of problems in your cluster. You can isolate problems down to the task that caused it.

Recent ESX/i Log Errors

Look at the log files generated by VMware ESXi hosts in the cluster. ESXi host logs are written to the file system and provide information about system operational events. You can examine the log files in detail drilling down to system events that can identify particular issues in your environment.

Chart of performance data for a cluster

Look at this chart to see the performance of the cluster for a specific performance data type.
Filter your result by selecting a performance metric and then by selecting the statistical operation on the data.

**Datastore Detail**

On the Datastore Detail dashboard you can access information about the storage layer in your environment. Using this dashboard you can:

- Monitor the most important performance metrics such as latency and IOPS for the connected datastore, at the filer and at the volume level.
- Correlate virtual machine performance with storage performance (specifically NetApp storage).
- Reduce the time it takes to identify a problem if storage performance degradation affects all of the hosts or some of the virtual machines on a particular datastore.

**Display datastore details**

Look at the details for a specific datastore either by using the drop-down lists to select a specific datastore, or drill down from another dashboard in the app to automatically populate the dashboard.

Use the drop-down lists to select:

1. a virtual center.
2. a datastore.
3. a time range.

The panels in the dashboard populate with data about the datastore you selected.
Look at the configuration and status of the datastore

On this panel you can get information about the state of the datastore, such as:

- If the datastore is accessible.
- The volume type, for example, an NFS volume.
- The available space and total space, in GB, on the datastore.
- The space provisioned, in GB, for a virtual machine, and the percent overprovisioned.
- The path to the datastore and the associated URL.
- The number of virtual machines on the datastore.

The following search is used to populate the panel:

```
sourcetype="ontap:volume" (source=volume-get-iter OR source=volume-list-info-iter-start) | eval name=coalesce(name, "volume-id-attributes.name") | stats values(name) as volname by host | lookup dnslookup clienthost AS host OUTPUT clientip AS ip | mvexpand volname | table * | join type=inner ip, volname [search sourcetype=vmware:inv:datastore changeSet.info.nas.type="NFS" earliest=-24h latest=now | rename changeSet.info.nas.name as name, changeSet.info.nas.remotePath as path, changeSet.info.nas.remoteHost as filer, host as vcenter | dedup path, filer | rex field=path ".+/(?<volname>[^/]+)" | lookup dnslookup clienthost AS filer OUTPUT clientip AS ip | table name, moid, path, filer, ip, volname, vcenter] | rename name as "Datastore name", path as "Path", volname as Volume, filer as "Filer (VMware data)", host as Filer, ip as IP, vcenter as VCenter | search moid=$name.moid$
```
Get the Datastore Filer Latency rate

look here to quickly see whether storage latency is a contributing factor to reduced performance in your environment. Spikes in latency rates indicate that you need to investigate more.

Filer latency rates are measured by monitoring performance metrics that track average reads and writes to the filer. Measuring latency is important to prevent performance problems in the application layer.

The following search is used to populate the panel:

```
| `tstats` avg(read_latency_average), avg(write_latency_average),
  avg(other_latency_average) from netapp_perf_volume groupby _time
  span=2m, host | search [search `SystemHostname($filer[0].Filer$)`] | timechart avg(read_latency_average), avg(write_latency_average),
  avg(other_latency_average) by host | rename avg(read_latency_average)
  AS read_latency, avg(write_latency_average) AS write_latency,
  avg(other_latency_average) AS other_latency | eval
  read_latency=read_latency/1000 | eval write_latency=write_latency/1000
  | eval other_latency=other_latency/1000
```

Get the Datastore Filer IOPS rate

Look at this panel to monitor filer IOPS if you are concerned about latency in your environment. You can get poor virtual machine performance if your virtual machines do not have enough I/O per second (IOPS), or network throughput.

The following search is used to populate the panel:

```
| `tstats` avg(read_ops_rate), avg(write_ops_rate),
avg(other_ops_rate), avg(total_ops_rate) from netapp_perf_system
  groupby _time span=5m, host | search [search
  `SystemHostname($filer[0].Filer$)`] | timechart limit=5
avg(read_ops_rate), avg(write_ops_rate), avg(other_ops_rate),
avg(total_ops_rate) by host
```

Get the Datastore Volume Latency rate

On this panel you can measure volume latency rates by monitoring performance metrics that track average reads and writes to the volume on the disk.

The following search is used to populate the panel:
Get the Datastore Volume IOPS rate

In this panel you can monitor volume IOPS if you are concerned about latency in your environment. You can get poor virtual machine performance if your virtual machines do not have enough I/O per second (IOPS).

The following search is used to populate the panel:

```
sourcetype=ontap:perf source=VolumePerfHandler host=$volume[0].Filer$ objname=$volume[0].Volume$ | timechart limit=5 first(total_ops_rate) as total_ops_rate first(write_ops_rate) as write_ops_rate first(read_ops_rate) as read_ops_rate first(other_ops_rate) as other_ops_rate by objname
```

Correlate VMware data with NetApp ONTAP storage data

Issues in the storage layer can impact the performance of virtual machines in your environment. You can correlate issues in your VMware infrastructure with NetApp storage issues using the Datastore Detail dashboard. This correlation feature enables you to better troubleshoot problems in your infrastructure and identify where the problems exist between the VMware hosts and your NetApp ONTAP filers.

For example, if virtual machines on an NFS datastore named "ISO" in the Splunk App for VMware cause a problem in your environment, you can drill down to the filer and the specific volume in the Splunk App for NetApp Data ONTAP and look at the performance information for the datastore known in your VMware environment as "ISO".

**Correlation Requirements**

To correlate VMware data with NetApp ONTAP data, you must have the following apps installed in your environment:

- The Splunk App for VMware.
- The Splunk App for NetApp Data ONTAP.
The correlation feature enables you to drill down from a dashboard in the Splunk App for VMware to the Splunk App for NetApp Data ONTAP and get specific filer and volume performance information.

For more information about installation and configuration of the apps, see their respective Installation and Configuration Guides, the "Splunk App for VMware Installation Guide" and the "Deploy and Use the Splunk App for NetApp Data ONTAP" manual.

**Required sourcetypes**

The following sourcetypes must be present for this dashboard to populate:

- The `ontap:volume` and `ontap:perf` sourcetypes must be present to get information about the volumes in the NetApp ONTAP environment.
- The `vmware:inv:datastore` sourcetype must be present to get information about the NFS volumes in the VMware environment.

**Display Filer volume level details**

Drill down from the filer to the datastore level to see details for a specific filer volume.

**To display volume level details:**

1. In the **Datastore Filer Latency rate** panel, click a filer name.
2. The Filer View dashboard of the Splunk App for NetApp Data ONTAP is displayed.
3. Look at the specific storage controllers that have an impact on the performance of your environment.

For information on this dashboard, see "Filer View" in the *Deploy and Use the Splunk App for NetApp Data ONTAP* manual.

**Performance of Hosts and VMs**

Use this dashboard to visually compare the performance statistics, for hosts and virtual machines, in your VMware vSphere® environment, based on a selected performance metric.
You can compare the performance statistics of:

- A host on one VMware vCenter Server with another host on the same vCenter Server.
- Multiple hosts in a vCenter Server with hosts on another vCenter Server.
- One or more virtual machines with other virtual machines.

Panel description

On each of the panels on this dashboard, use the toggle buttons, the search box, and the drop-down lists to set your search criteria. The name of the selected host or virtual machine is displayed in the panel, and a chart shows the performance statistics for that host or virtual machine.

You can chart up to a maximum of 50 hosts or virtual machines and compare the performance statistics for each. To change the default limit, edit the value set for limitSelectionCount in the SOLNSelector module in the host_vm_perf view:

```
name="limitSelectionCount">50
```

To clear the chart, click on each of the listed entity names in the panel to remove them.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host / vm toggle</td>
<td>Use this toggle to select either host or vm.</td>
</tr>
</tbody>
</table>
Click host to chart the search results at the host level in your environment.
Click vm to chart the search results at the virtual machine level in your environment.

**Search box**
- When host is selected, in the search box, enter the name of the host, for example, apps-esx-21. As you type your search, a filtered list of possible matches is displayed. This helps you to search an entity (virtual machine or host system) through virtual center, host, or cluster. To select all the entity matches shown in the results list, use the wildcard character "/" after the "/".
- When you select vm, enter the name of a virtual machine, for example apps-21vm. A filtered list of predicted virtual machines is displayed as you enter your search. Select a virtual machine from the list. You can chart the performance of any number of virtual machines by making more selections.

**Drop-down lists**
- Select a performance metric category from the list provided, for example, cpu.
- Select a performance metric, for example, average_cpu_usage_percent.
- Select a time range for the search.

**Capacity Planning Hosts**

Use the Capacity Planning (Hosts) dashboard to monitor and plan the allocation of resources to hosts in your environment. This dashboard shows the performance of hosts, over time, based on the memory or cpu resources used. These resources are critical components of your virtual infrastructure.

Looking at this dashboard you can see the performance of hosts for the specific metric selected. Using the data provided you can provision your hosts and virtual machines with the correct amount of physical memory and cpu resources.

The Splunk App for VMware uses VMware’s key performance counters to determine the memory and cpu resource demands of the hosts.
Host Performance

You can generate a report to monitor the performance of hosts based on cpu or memory usage. In the Capacity Planning (Hosts) dashboard create a search using the drop-down lists on the dashboard.

To show host performance:

1. Select a time range for the search, for example Last 24 hours.
2. In the **Show Hosts with** drop-down list, select a key performance metric, max cpu usage or max memory usage, on which to base the search. For example, max cpu usage.
3. Define a usage percent for a resource, for example 70%.
4. Specify whether you want the search to include results that are higher or lower that the percent specified (in the next step). In this example select "or higher".
5. Define a percentage of time over which the resource is used, for example 5%.

A results table shows host performance for all hosts for which max_cpu_usage was 70% or higher more than 5% of the time.

Chart host performance

Click on a host in the results table to chart the individual host performance. The average and maximum usage for the performance category (mem or cpu) for the host is displayed in relation to the threshold you defined.

**Metrics used to populate the dashboard**

<table>
<thead>
<tr>
<th>Name</th>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
</table>

39
<table>
<thead>
<tr>
<th>Name</th>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>max cpu usage</td>
<td>p_average_cpu_usage_percent</td>
<td>This is the virtual machine's average memory usage as a percent value.</td>
</tr>
<tr>
<td>max memory usage</td>
<td>p_average_mem_usage_percent</td>
<td>This is the virtual machine's average memory usage as a percent value.</td>
</tr>
</tbody>
</table>

**Searches that populate the dashboard**

The following searches are used to populate the Capacity Planning (Hosts) dashboard:

- d_capacity_planning_hosts_list_usage_cpu
- d_capacity_planning_hosts_list_usage_mem

**Capacity Planning Clusters**

Use the Capacity Planning (Clusters) dashboard to monitor and plan the allocation of resources for virtual machines in your cluster. Using this dashboard you can see memory and cpu utilization for specific clusters, and you can identify those clusters that are nearing maximum capacity for the specific resource. CPU utilization is expressed as a percentage of time (0 to 100%) that the CPU executes at the threshold you define.

You can also view a list of clusters excluded due to lack of hosts or services. These are clusters that do not support cluster services and that contain less than two hosts.

**Cluster Performance**

Filter your search results using the drop-down lists in this panel. The data displayed in the table is populated with the results of the search. Using the results in the table you can monitor the activity of certain clusters or better provision resource (cpu or memory) for them.

**To show cluster performance:**

1. Select a time range for the search, for example Last 24 hours.
2. In the **Show clusters with** drop down, select a key performance metric, max cpu usage or max memory usage, on which to base the search. For
example, max cpu usage.
3. Define a usage percent for a resource, for example 80%.
4. Specify whether you want the search to include results that are higher or lower that the percent specified (in the next step). In this example select "or higher".
5. Define a percentage of time over which the resource is used, for example 5%.

A table displays the clusters where cpu usage met or rose above 80% more than 5% of the time.

**Chart cluster performance**

Click on a cluster in the results table to display a chart showing the performance of the cluster in relation to the threshold you set for that metric.

**Metrics used to populate the dashboard**

<table>
<thead>
<tr>
<th>Name</th>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>max cpu usage</td>
<td>p_average_clusterServices_effectivecpu_megaHertz</td>
<td>The total available CPU resources of all hosts within a cluster.</td>
</tr>
<tr>
<td>max memory usage</td>
<td>p_average_clusterServices_effectivemem_megaBytesv</td>
<td>The total amount of machine memory of all hosts in the cluster that is available for use for virtual machine memory.</td>
</tr>
</tbody>
</table>
Searches that populate the dashboard

The following searches are used to populate the Capacity Planning (Clusters) dashboard:

- d_capacity_planning_cluster_cpu.
- d_capacity_planning_cluster_mem.

Capacity Planning for Clusters - CPU Headroom

Use this dashboard to get an estimate for the number of virtual machines that you can add to the cluster based on current cpu consumption (of the ESXi hosts) and total cpu capacity allocated to virtual machines in the cluster. This dashboard reports only on powered on virtual machines in the cluster.

The Capacity Planning for Clusters - CPU Headroom dashboard displays:

- Capacity statistics for a cluster.
- A list of powered on virtual machines showing their cpu usage in the cluster.
- A chart showing current cpu usage, safe cpu usage, and total cpu capacity for the cluster.

You can view a list of clusters excluded due to lack of hosts or services. These are clusters that do not support cluster services and that contain less than two hosts.

To display details for a specific cluster, select a time range and the cluster name from the Cluster drop-down list. Details for the cluster are displayed in the panels.
Capacity statistic

In the Capacity statistics panel you can see:

- The number of hosts in the cluster
- The number of powered on virtual machines
- Average CPU usage in (MHz) per virtual machine.
- Total CPU usage MHz available in cluster
- Estimated number of virtual machines that can be added to the cluster

Powered on virtual machines in the cluster

A table displays the powered on virtual machines in the cluster and the average and maximum cpu usage (in MHZ) for each virtual machine.

Currently used (MHz) and Total Capacity

A chart displays the total capacity of the cluster, the current cpu usage of the cluster, and safe usage over the time period specified.

Metrics used

The following metrics are used to calculate cpu utilization:

- cpu usage for the cluster is calculated based on
  \( p_{\text{average\_cluster\_Services\_effective\_cpu\_megahertz}} \).
- Average cpu usage (MHz) is calculated based on
  \( p_{\text{average\_cpu\_usagemhz\_megahertz}} \).
- Maximum cpu usage (MHz) is calculated based on
  \( p_{\text{maximum\_cpu\_usagemhz\_megahertz}} \).
- Minimum cpu usage (MHz) is calculated based on
  \( p_{\text{minimum\_cpu\_usagemhz\_megahertz}} \).

Searches that populate the dashboard

The following searches populate the panels in the dashboards:

- \( d_{\text{capacity\_planning\_cluster\_cpu}} \)
- \( d_{\text{capacity\_planning\_clusters\_cpu\_chart}} \)
- \( d_{\text{cluster\_detail\_AvgCpuPerVM\_mhz}} \)
- \( d_{\text{cluster\_detail\_AvgCpuUsg\_pct}} \)
- \( d_{\text{cluster\_detail\_TotUsg\_mhz}} \)
Capacity Planning for Clusters - Memory Headroom

Use this dashboard to get an estimate for the number of virtual machines that you can add to the cluster based on current memory consumption and overhead memory allocated to the virtual machines in the cluster. This dashboard reports only on powered on virtual machines in the cluster.

Using the data on this dashboard you can make better resource provisions to minimize and resolve bottlenecks, increases availability of systems and improve overall performance of the systems.

The Capacity Planning for Clusters - Memory Headroom dashboard displays:

- Capacity statistics for the cluster.
- A list of powered on virtual machines showing their memory usage in the cluster.
- A chart showing current memory usage (in GB) for the cluster, and total memory capacity for the cluster.

Dashboard Panels

To display details for a specific cluster, select a time range and the cluster name from the Cluster drop-down list. The details for the cluster are displayed in the panels.

Capacity statistic

Look on the Capacity statistics panel for information about:

- The number of hosts in the cluster.
• The number of powered on virtual machines.
• Average consumed memory (in GB) per virtual machine.
• Average overhead memory usage (in GB) per virtual machine.
• Total memory available in the cluster (in GB).
• Estimated number of virtual machines that you can add to the cluster.

Powered on virtual machines memory usage in the cluster

Look on this panel to see the memory usage for each powered on virtual machines in the cluster. Virtual machine memory overhead is the amount of machine memory allocated to a virtual machine beyond its reserved amount. This table shows the average and maximum overhead usage (in GB) for each virtual machine.

- AvgOverheadUsg_GB is the metric used to measure the memory used by VMWare to actually power the virtual machine.
- MaxOverheadUsg_GB is the metric used to measure the maximum memory used by VMWare to actually power the virtual machine, over the summarization period.
- AvgConsumedUsg_GB is the metric used to measure the average memory consumed by the virtual machine in the cluster.
- MaxConsumedUsg_GB is the metric used to measure the maximum amount of memory consumed by a virtual machine over the summarization period.

Currently used (GB) and Total Capacity

A chart displays the total capacity of the cluster, the current cpu usage of the cluster, and safe usage over the time period specified.

Capacity Forecasting

Use capacity forecasting to predict resource usage for different entities in your environment. Predicted results are based on historical values. Using these predictions you can optimize your environment for peak performance and be prepared, in advance, to handle unexpected usage periods.

Using the Capacity Forecasting dashboard, you can:

- Predict cpu usage over a specified time.
- Predict memory usage over time.
• Predict disk usage over time.

Use the drop-down lists to filter your selection for charting predicted resource usage. You can:

• Select a time range for the search using the Time Selector.
• Select a specific virtual center in your environment.
• Select all host systems managed by the virtual center or select a specific host system.
• Select all virtual machines or select a specific virtual machine.
• Set a prediction time. A value of "0" indicates current time. A value of "1" indicates that you want to predict resource usage for 1 "time unit" from now.
• Select a time unit, for example, minutes, days, weeks, or months into the future.
• Select a forecasting algorithm. The prediction algorithms are:
  ♦ LLP-Seasonal local level - This is a univariate model with seasonality. The periodicity of the time series is automatically computed. It requires the minimum number of data points to be twice the period.
  ♦ LL-Local level - This is a univariate model with no trends and no seasonality. It requires a minimum of 2 data points.
  ♦ LLT-Local level trend - This is a univariate model with trend but no seasonality. It requires a minimum of 3 data points.

For more information on the forecasting algorithms used, see "Predict" in the Splunk Enterprise Search Reference manual.
Capacity Forecasting Panel Description

The Capacity Forecasting dashboard charts predicted usage of a resource (cpu, memory, disk). In each of the charts on this dashboard, the lower and upper confidence interval parameters default to lower95 and upper95. This specifies a confidence interval where 95% of the predictions are expected to fall. The vmw:perf:* source type must be present for the panels to populate.

<table>
<thead>
<tr>
<th>Panel</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Usage Prediction over Time (%)</td>
<td>The chart displays predicted cpu usage for a host system, or all of the host systems in a virtual center over the time range specified. CPU usage prediction is calculated as a percent value using the p_average_cpu_usage_percent metric.</td>
</tr>
<tr>
<td>Mem Usage Prediction over Time (%)</td>
<td>The chart displays predicted memory usage for a host system, or all of the host systems in a virtual center over the time range specified. Memory usage prediction is calculated as a percent value using the p_average_mem_usage_percent metric.</td>
</tr>
<tr>
<td>Disk Usage Prediction over Time (KBs/sec)</td>
<td>The chart displays predicted disk usage for a virtual machine or all the virtual machines in a virtual center over the time range specified. Disk Usage Prediction is calculated in KB/sec using the p_average_disk_usage_kiloBytesPerSecond metric.</td>
</tr>
</tbody>
</table>

Virtual Machine Snapshots

Use the Virtual Machine Snapshots dashboard to get information about snapshotting activities for virtual machines in your environment. Act on the data by consolidating, migrating, or deleting the snapshots.

On the Virtual Machine Snapshots dashboard, you can:
• See the number of snapshots per virtual machine.
• See the space used by the snapshots.
• Track the usage of resources that snapshots consume.
• Look at individual details about snapshot files such as file creation dates, file sizes, and so on.

The information displayed in each of the panels in the dashboard is determined by the selection you make in the drop-down lists.

Snapshots present on VM

On this panel the resources consumed by snapshots on the datastore are tracked. Look at the information in this view to see whether snapshot behavior has an impact on your overall environment. You can decide whether you want to make changes to the snapshot activity in your environment.

Use the drop-down lists to select a virtual center and a time range over which you want to examine snapshot activity.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Center</td>
<td>The name of the virtual center.</td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>The name of the virtual machine.</td>
</tr>
<tr>
<td>Datastore</td>
<td>The name of the datastore. Click on the datastore to drill down and see the snapshot details on it.</td>
</tr>
<tr>
<td>SnapshotFiles</td>
<td>The names of the files in the snapshot.</td>
</tr>
<tr>
<td>TotalFiles</td>
<td>The total number of snapshot files.</td>
</tr>
<tr>
<td>SnapshotSpace</td>
<td>The space used by vmsn (VMware snapshot) files. A vmsn file is used to store the exact state of the virtual machine when the snapshot was taken.</td>
</tr>
</tbody>
</table>
A snapshot contains vmsn files along with other files. TotalSpace is the space used by vmsn files in addition to the space used by the following files:

- vmsd files that store the metadata or structure of the snapshot tree.
- vmdk files. Virtual Machine Disk files. These are descriptor files.
- delta.vmdk file. This file contains the changes made on this snapshot in relation with the parents.

**Snapshot Statistics for Datastore**

In this panel, use the drop-down lists to select a virtual center, a datastore, and a time range over which you want to examine snapshot activity.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snapshot space used on disk</td>
<td>The chart displays the snapshot space (in bytes) used on the disk over the time range selected.</td>
</tr>
<tr>
<td>Number of Snapshots on datastore</td>
<td>The chart displays a count of the number of snapshots on the data store over the selected time range.</td>
</tr>
</tbody>
</table>

**ESXi Log Browser**

The ESXi Log Browser is a quick and easy way to look at ESX/i logs collected from the host systems. Configure the forwarding of syslog data to Splunk App for VMware. Browse the following log data:

- vCenter server vpxa agent logs (vpxa.log). These logs contain communication information with vCenter Server and the Host Management hostd agent.
- Syslog management service logs.
- hostd management service logs (hostd.log). The logs include virtual machine and host Task and Events information, information related to communication between the vSphere Client and the vpxa agent, and they store information about SDK connections.

Use the drop-down lists on the dashboard to filter your search results.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time range</td>
<td>The time range over which events are reported.</td>
</tr>
<tr>
<td>ESX/i</td>
<td>A list of ESX/i hosts from which you are collecting syslog data. The default value is All.</td>
</tr>
<tr>
<td>Common Terms</td>
<td>Common terms that exist in ESX/i logs. This is a static list of options. HTTP and event are examples of common terms. The default value is Any.</td>
</tr>
<tr>
<td>Field/Value</td>
<td>Common field values extracted at index time from events. This is a static list of options. The default value is Any.</td>
</tr>
<tr>
<td>Error/Fault</td>
<td>Common errors of faults that appear in syslog data, classified into a single grouping. The default value is Any.</td>
</tr>
<tr>
<td>Managed Objects</td>
<td>A list of all objects managed by the vCenter Server. The default value is All.</td>
</tr>
<tr>
<td>API Related</td>
<td>A list of all API related search terms that can appear in syslog data. The default value is All.</td>
</tr>
<tr>
<td>Component</td>
<td>A list of all services running on the the vCenter server. The default value is All.</td>
</tr>
<tr>
<td>Sublogger</td>
<td>A list of the log listener services installed. The default value is All.</td>
</tr>
<tr>
<td>Look for</td>
<td>Enter the term that you want to specifically search for in the logs.</td>
</tr>
<tr>
<td>Level</td>
<td>A logging level. This can be DEBUG, INFO, WARN, ERROR, or FATAL.</td>
</tr>
</tbody>
</table>

### vCenter Log Browser

The vCenter Log Browser is a quick and easy way to look at vCenter server logs.

You can browse the following log data:

- Main vCenter diagnostic logs (vpxd).
- Storage management service logs (sms logs).
- vCenter web services logs (vws/tomcat/stat/cim-diag).
For this dashboard to work correctly, you must have vclog data set up to forward to the Splunk App for VMware. See Collect optional log data section of the Splunk Add-on for VMWare manual for detailed instructions.

Use the drop-down lists on the dashboard to filter your search results. The drop-down lists are explain in the table below.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time range</td>
<td>The time range over which events are reported.</td>
</tr>
<tr>
<td>vCenter</td>
<td>A list of vCenter servers from which you are collecting syslog data.</td>
</tr>
<tr>
<td></td>
<td>The default value is All.</td>
</tr>
<tr>
<td>Look for</td>
<td>Enter the term that you want to specifically search for in the logs.</td>
</tr>
<tr>
<td>Level</td>
<td>A logging level. This can be DEBUG, INFO, WARN, ERROR, or FATAL. The default is ERROR.</td>
</tr>
</tbody>
</table>

The following source types must be present for the data to populate the panels:

<table>
<thead>
<tr>
<th>Panel</th>
<th>Source type</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpxd</td>
<td>vmware:vclog:vpxd</td>
</tr>
<tr>
<td>sms</td>
<td>vmware:vclog:sms</td>
</tr>
<tr>
<td>vws/tomcat/stat/cim-diag</td>
<td>vmware:vclog:vws or vmware:vclog:stats or</td>
</tr>
<tr>
<td></td>
<td>vmware:vclog:cim-diag or</td>
</tr>
<tr>
<td></td>
<td>vmware:vclog:vim-tomcat-shared or</td>
</tr>
<tr>
<td></td>
<td>vmware:vclog:tomcat</td>
</tr>
</tbody>
</table>
ESXi Hosts Task Overview

Look at this dashboard to get insights into the state of your virtual environment.

You can:

- Get a quick view of the state of your host system, getting visibility into the tasks performed on the hosts and the related virtual machines.
- Identify the root cause of issues on the host. Look down the list of tasks to see if there are any anomalies in your environment.

Use the search bar and menu tree on the dashboard to select the hosts or virtual machines you want to display. The search bar allows you to make a single selection. The menu tree supports multiple selection of hosts and virtual machines.

You can filter the data displayed based on:

- **User.** Search for a specific message relating to a user.
- **State.** This is the error state.
- **Description.** Enter a value in this field to create a results table listing the details for the hosts that have messages that match your search criteria. The search looks in the error messages returned in the syslog data for the word you entered.

The source type `vmware:tasks` must be present for this dashboard to work correctly.

Task and Event Details

Use the Task and Event details dashboard to quickly and easily look at tasks and events that have occurred on the various entities in your environment.

You can filter results based on:

- Specific tasks.
- Users.
- A specific message.
• Entities in your environment, such as vCenter servers, hosts, virtual machines, and so on.

The source types `vmware:events` or `vmware:tasks` must be present for this dashboard to work correctly.

Use the drop-down lists on the dashboard to filter your search results. The drop-down lists are explained in the table below.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time range</td>
<td>The time range over which events are reported.</td>
</tr>
<tr>
<td>Event Classification</td>
<td>This is a list of all events that you can review. The default value is All.</td>
</tr>
<tr>
<td>Virtual Center</td>
<td>Enter the name of a vCenter server.</td>
</tr>
<tr>
<td>Datacenter</td>
<td>Enter the name of a data center.</td>
</tr>
<tr>
<td>Cluster</td>
<td>Enter the name of a cluster.</td>
</tr>
<tr>
<td>Host</td>
<td>Enter the name of a host.</td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>Enter the name of a Virtual Machine.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the name of a user.</td>
</tr>
<tr>
<td>Task</td>
<td>Enter a specific task.</td>
</tr>
<tr>
<td>Message</td>
<td>Enter a specific message relevant to a task or event.</td>
</tr>
</tbody>
</table>

**Security Overview**

Use this dashboard to investigate into security relevant events and to check for potential security breaches. Get visibility into user activity using access controls and look at the history of user related tasks and events.

Using this dashboard you can look at the following security information about your environment:

• Added, removed, or changed roles for users.
• Repeated login attempts.
• Attempted actions outside permissions.
• Potentially harmful logins.

The source type `vmware:events` must be present for this dashboard to populate.
Useful Saved Searches

Use these searches to help troubleshoot problems with network connectivity.

You can:

- Edit the search and save it as a report, a dashboard panel, an alert, or an event type.
- Edit the description and the permissions for the search.
- Schedule the search.
- Add the search to a dashboard.

Useful saved search description

<table>
<thead>
<tr>
<th>Name</th>
<th>Search</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vProb errors in logs</td>
<td>sourcetype=&quot;vmware:<em>log</em>*&quot; error &quot;vProb**&quot;</td>
<td>Detects network problems with storage devices.</td>
</tr>
<tr>
<td>vmfs volume locked</td>
<td>sourcetype=&quot;vmware:<em>log</em>*&quot; vmfs volume locked</td>
<td>Detects if a volume is locked by another host.</td>
</tr>
<tr>
<td>vCenter starts</td>
<td><code>VcLogSourcetypes</code> &quot;Starting * VirtualCenter&quot;</td>
<td>Detects if there are problems starting the vCenter server.</td>
</tr>
<tr>
<td>All paths are dead</td>
<td>sourcetype=&quot;vmware:<em>log</em>*&quot; &quot;APD&quot;</td>
<td>Detects if a storage device was removed from an ESX/i host in an uncontrolled manner.</td>
</tr>
<tr>
<td>SCSI reservation error-i/o failed</td>
<td>sourcetype=&quot;vmware:<em>log</em>*&quot; &quot;SCSI reservation error - i/o&quot;</td>
<td>Detects the virtual</td>
</tr>
</tbody>
</table>
Threshold Configuration

The Threshold Configuration dashboard is an administration dashboard with restricted access to users of the Splunk App for VMware who have administration privileges. If you do not have these privileges, then you cannot access this dashboard.

Use the Threshold Configuration dashboard to configure threshold settings for performance metrics that have default threshold set for them in the Splunk App for VMware. All metrics listed on this page can be found in VMware’s PerformanceManager or VMware VirtualMachineQuickStats unless it is a Splunk defined metric.
By default, the Splunk App for VMware collects the complete set of VMware performance metrics. You can see the complete set of metrics in the Splunk App for VMware on the Proactive Monitoring dashboard and on the Performance of Hosts and VMs Dashboard.

Using the Threshold Configuration dashboard you can:

- Add and delete metrics.
- Editing warning and critical threshold values for metrics.
- Enable or disable metric collection.

For more information, see "Add, edit, and delete threshold settings" and the "Performance metrics reference table" in the Splunk App for VMware Configuration Guide.

Collection Configuration

Use the Collection Configuration dashboard to configure data collection settings for the Splunk App for VMware.

This is an administration dashboard with restricted access to users of the Splunk App for VMware who have administration privileges. If you do not have these privileges, then you cannot access this dashboard.
Using this dashboard you can:

- Add data collection nodes and VMware vCenter Servers to the scheduler configuration.
- Start the Distributed Collection Scheduler to collect data from your VMware vSphere environment.
- Configure the collection of data from specific hosts systems.

For information on how to set up a data collection node, see "Deploy OVA to create a Data Collection Node" in the Splunk App for VMware Installation Guide.

**App Install Health**

Look at the App Install Health dashboard to see that the Splunk App for VMware is installed and configured correctly to collect data from your VMware vSphere environment.

Using this dashboard you can:

- Validate the integrity of your data by examining the status of your environment.
- Check the components you installed into your environment.
- See how your environment is configured to collect data.
- Check that you are collecting the correct data types.
App Data Volume

The App Data Volume dashboard provides information about the quantity and types of data you collect in the Splunk App for VMware. You can get a quick view of the total volume of data created by the app.

Use this dashboard to see:

- The total data volume over the last 24 hours.
- The breakdown of data by data type and unique sourcetypes for each of the data source collected.
- The installed Splunk App for VMware licenses.
- Daily data volume remaining.

Note:

- The **Installed VMware App Licenses** panel populates only when the app is installed on the search head that acts as a license master.
- For this dashboard to populate and report accurate license usage information, install the app on a search head that acts as a license master, or make the _internal index of the license master accessible to distributed search.

Dashboard description

<table>
<thead>
<tr>
<th>Panel</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall Data Volume, over the last 24 hours</td>
<td>The total volume of data indexed in the last 24 hours.</td>
</tr>
<tr>
<td>Detailed Data Volume, over the last 24 hours</td>
<td>Shows the volume of indexed data broken down by data type. The sourcetype _internal must be present for this panel to populate.</td>
</tr>
<tr>
<td>Installed VMware App Licenses</td>
<td>Displays details for the installed Splunk App for VMware licenses.</td>
</tr>
<tr>
<td>Daily Data Volume Remaining</td>
<td></td>
</tr>
</tbody>
</table>
### Panel Description

#### Hydra Framework Status

Use the Hydra Framework Status page to identify issues related to jobs handled by **SA-Hydra**. Page can be viewed by following the below link for your Splunk platform deployment.


Enable data population for this page.

1. **Navigate to** Splunk_TA_vmware/local/input.conf
2. **Set the** log_level **to** DEBUG **for all enabled worker stanzas.**
3. **Save your changes and restart your Splunk platform deployment.**

<table>
<thead>
<tr>
<th>Dashboard name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Expirations by DCN</td>
<td>Number of jobs assigned and expired on each DCN versus time. DCN (Worker) logs are required to populate this panel.</td>
</tr>
<tr>
<td>Jobs Handled by DCN</td>
<td>Number of jobs successfully completed by each DCN versus time. DCN (Worker) logs are required to populate this panel.</td>
</tr>
<tr>
<td>Job Scheduling Duration Range (DEBUG level logs only)</td>
<td>Average, Max and Min time taken for Scheduler to assign jobs to DCNs at every iteration versus time. It will populate when DEBUG level is enabled on your scheduler. Scheduler logs are required to populate this panel.</td>
</tr>
<tr>
<td>Collection Task Duration Range (Log Scale)</td>
<td>Minimum, Median and Maximum execution time to perform all the task. DCN (Worker) logs are required to populate this panel.</td>
</tr>
<tr>
<td>Median Task Performance Over Targets</td>
<td>Target (vCenter) and task wise median job execution time reported by Worker on DCN. DCN (Worker) logs are required to populate this panel.</td>
</tr>
<tr>
<td>Task Expiration Count Over DCN</td>
<td>Task wise no. of jobs assigned and expired on each DCN. DCN (Worker) logs are required to populate this panel.</td>
</tr>
<tr>
<td>Dashboard name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>panel.</td>
<td></td>
</tr>
<tr>
<td>Task Failure Count Over Target</td>
<td>Task wise no. of jobs assigned and failed on each DCN. DCN (Worker) logs are required to populate this panel.</td>
</tr>
<tr>
<td>Last 100 Worker Errors - excluding expiration</td>
<td>Last 100 errors occurred in worker processes in all DCNs excluding errors which occurred due to job expiration. DCN (Worker) logs are required to populate this panel.</td>
</tr>
<tr>
<td>Last 100 Scheduler Errors</td>
<td>Last 100 errors occurred in Scheduler process. Scheduler logs are required to populate this panel.</td>
</tr>
</tbody>
</table>
Hydra Scheduler Status

Use the Hydra Scheduler Status page to identify issues related to jobs handled your scheduler. Page can be viewed by following the below link for your Splunk platform deployment.

Enable data population for this page.

1. Navigate to Splunk_TA_vmware/local/input.conf
2. Set the log_level to DEBUG for all enabled worker stanzas.
3. Save your changes and restart your Splunk platform deployment.

<table>
<thead>
<tr>
<th>Dashboard name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Assignment by DCN</td>
<td>Number of jobs assigned to each DCN versus time. It will populate when DEBUG level is enabled on scheduler. Scheduler logs are required to populate this panel.</td>
</tr>
<tr>
<td>Max Unclaimed Queue Length by DCN</td>
<td>Number of unclaimed jobs reported by each DCN to Scheduler versus time. It will populate when DEBUG level is enabled on scheduler. Scheduler logs are required to populate this panel.</td>
</tr>
<tr>
<td>Dead Nodes</td>
<td>List of dead nodes (DCNs) and their count at every 5 minute interval. Scheduler logs are required to populate this panel.</td>
</tr>
</tbody>
</table>
Reference

Common use cases

Use the Splunk App for VMware to get a greater understanding of what is happening at the operational level in your VMware vSphere environment. Some use cases for the app are described in this topic.

<table>
<thead>
<tr>
<th>Use case</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory monitoring</td>
<td>The Splunk App for VMware collects inventory data that enables you to better monitor the components in your VMware vSphere environment. These inventory objects include hosts, virtual machines, data stores, and networks.</td>
</tr>
<tr>
<td>Performance monitoring</td>
<td>All of the dashboards in the Splunk App for VMware display a real-time operational state of the entities in your vSphere environment based on thresholds that are predefined in the Splunk App for VMware. In addition to reporting on VMware performance, you can:   - Look at host details and compare hosts in your environment.   - Monitor real-time dashboards that visualize performance events across the virtual topology map.   - Drill down to problem sources and access granular performance metrics using accelerated Splunk Enterprise searches.   - Proactively detect performance issues and prevent them from impacting your end users.</td>
</tr>
<tr>
<td>Correlation</td>
<td>The Splunk App for VMware gathers granular performance and event data from your virtualization layer. Correlate that data with data from other entities (such as datastores) to resolve issues in your environment.</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>Use the dashboards in the Splunk App for VMware to determine the root cause of performance problems in your environment.</td>
</tr>
<tr>
<td>Use case</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Navigable</strong></td>
<td>• Navigate the topology map in the Proactive Monitoring view and drill down to discover the source of problems in your environment.</td>
</tr>
<tr>
<td><strong>Capacity planning and reporting</strong></td>
<td>• Track migrating virtual machines in your environment (as they migrate from one physical host to the next).</td>
</tr>
<tr>
<td><strong>Scaling</strong></td>
<td>The Proactive Monitoring view builds an interactive topology map of your environment. It is designed to scale to the largest of virtual environments and provides quick access to the data.</td>
</tr>
<tr>
<td><strong>Proactive (operational) monitoring</strong></td>
<td>Use the searches and reports to track changes in your environment.</td>
</tr>
<tr>
<td></td>
<td>• Use the interactive visual maps of your virtual environment and alert on abnormalities to proactively manage issues.</td>
</tr>
<tr>
<td></td>
<td>• Look at the real-time operational state (Home view) based on predefined thresholds and drill down into an interactive topology map to isolate problems.</td>
</tr>
<tr>
<td><strong>Security reporting</strong></td>
<td>Look at a visual display of security relevant events and check for potential security breaches.</td>
</tr>
<tr>
<td></td>
<td>• Get visibility into user activity using access controls and an audit of tasks and events on your virtual environment.</td>
</tr>
</tbody>
</table>
Use case | Description
--- | ---
infrastructure. | Audit changes to your environment, manage users and roles, and get insight to the scope and impact of changes that can negatively affect availability, performance, security and capacity.

| Change tracking | Keep track of your virtual infrastructure, the state of the assets, and trend the performance impact of migrating virtual machines (from host to host).
| Monitor events to get a definitive record of what happened in your environment.
| Explore the topology map of your virtual environments. Highlight problems and make comparisons based on performance metrics.

**Reports**

This topic describes the reports provided as knowledge objects in the Splunk App for VMware.

**Memory reports**

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory Ballooning by VC</td>
<td>This report displays a time chart, split by hosts, showing memory ballooning for all the hosts over the selected time range. It also displays this data for each host as a table. You can see the amount of physical memory reclaimed by the host through VMware's ballooning driver. Frequent ballooning indicates a host in stress.</td>
</tr>
<tr>
<td>Memory Swapped by VC</td>
<td>This report displays a time chart, split by hosts (vcenters), showing the amount of memory from a virtual machine that was swapped by the host. This indicates that a host is stressed and needs more memory.</td>
</tr>
<tr>
<td>Memory Usage by VC</td>
<td>This report displays the percentage amount of memory used by the virtual machines in your environment.</td>
</tr>
<tr>
<td>Report Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Memory Utilization by Cluster</td>
<td>This search shows memory usage for all clusters over time.</td>
</tr>
<tr>
<td>Average Memory Provisioning</td>
<td>This search shows the average memory provisioning for all hosts.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Host System Reports</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Report Name</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Top Hosts with Ballooning</td>
<td>A report that shows the top 10 Hosts with Memory Ballooning for all the hosts. The report uses the p_average_mem_vmmemctl_kiloBytes metric. It calculates the sum of all memory balloon driver (vmmemctl) values for all powered-on virtual machines.</td>
</tr>
<tr>
<td>Host System- Count by Status</td>
<td>A report that displays host system status as chart and a table. You can visually see the high level status of your hosts. The report is based on the sourcetype vmware:inv:hostsystem.</td>
</tr>
<tr>
<td>Host System- Count by Free CPU</td>
<td>A report that displays a count of host systems with free cpu. You can visually see the high level status and drill down for individual details for each host system. The reports is based on the source type vmware:inv:hostsystem.</td>
</tr>
<tr>
<td>Host System- Count by Available Memory</td>
<td>A report that displays a count of host systems by available memory. You can visually see the high level status and drill down for individual details for each host system. The reports is based on the source type vmware:inv:hostsystem.</td>
</tr>
<tr>
<td>Host System- Count by Total Processing</td>
<td>The report displays a count of the host systems by total cpu usage for the hosts. This is the total actively used cpu (in MHz). The reports is based on the source type</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Report Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Host System- Count by Total Memory</td>
<td>The report displays a count of the host systems by total memory usage for the hosts (in MB). The report is based on the source type vmware:inv:hostsystem.</td>
</tr>
<tr>
<td>Host System- Count by Manufacturer</td>
<td>The report displays a count of the host systems by hardware vendor. The report is based on the source type vmware:inv:hostsystem.</td>
</tr>
<tr>
<td>Host System- Count by Model</td>
<td>The report displays a count of the host systems by hardware model. The report is based on the source type vmware:inv:hostsystem.</td>
</tr>
<tr>
<td>Host System- Count by Number of NICs</td>
<td>The report displays a count of the host systems by network interface controllers (NICs). The report is based on the source type vmware:inv:hostsystem.</td>
</tr>
<tr>
<td>Host System- Count by Hyperthreading</td>
<td>The report displays a count of the host systems that use hyper threading. You can see if Hyperthreading is enabled or inactive. The report is based on the source type vmware:inv:hostsystem.</td>
</tr>
<tr>
<td>Host System- Count by CPU Cores</td>
<td>The report displays a count of the host systems by cpu cores. The report is based on the source type vmware:inv:hostsystem.</td>
</tr>
<tr>
<td>Host System- Count by Processor Type</td>
<td>The report displays a count of the host systems by the type of processor they use. The report is based on the source type vmware:inv:hostsystem.</td>
</tr>
<tr>
<td>Host System- Count by ProcessorSockets</td>
<td>This report displays a count of the number of cpu sockets on the hosts. This number is calculated using the number of physical CPU packages (numCpuPkgs) on the host. The report is based on the source type</td>
</tr>
<tr>
<td>Report Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Host System- Count by Cores per Socket</td>
<td>The report displays a count of host systems by cpu cores per socket. The report is based on the source type vmware:inv:hostsystem.</td>
</tr>
<tr>
<td>Host System- Count by Logical Processors</td>
<td>The report displays a count of host systems by logical cores that run on them. Hyperthreading is used to share the workload between them. The report is based on the source type vmware:inv:hostsystem.</td>
</tr>
</tbody>
</table>

**Virtual Machine Reports**

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snapshots older than 14 days</td>
<td>This search shows all snapshots taken that are older than 14 days. You can see the details for each snapshot such as the file name, the host, when it was created, the size of the snapshot, and so on.</td>
</tr>
<tr>
<td>Top 5 Migrated VMs</td>
<td>This chart shows the top five virtual machines that migrated across all hosts.</td>
</tr>
<tr>
<td>Top OSs</td>
<td>This chart shows the top 10 operating systems installed on the virtual machines across all of the hosts in your environment.</td>
</tr>
<tr>
<td>OS Installed on VMs</td>
<td>This chart shows the various operating systems and the associated operating system versions (if available) that are running on the virtual machines.</td>
</tr>
<tr>
<td>Virtual Machine- Count by Tools Status</td>
<td>This chart shows the status of VMware Tools running in your environment, for all of the the virtual machines in your environment. The status can be &quot;VM tools not installed&quot;, &quot;VM tools old&quot;, and &quot;VM tools installed&quot;, &quot;VM tools ok&quot;, &quot;VM tools not running&quot;, and &quot;Not available&quot;.</td>
</tr>
<tr>
<td>Virtual Machine- Count by cores</td>
<td>This is a count by virtual machine of the number of virtual CPUs (vCPU) in a virtual</td>
</tr>
<tr>
<td>Report Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Machine vCPUs in the VMware environment</td>
<td>vCPUs in the VMware environment appear to the operating system as single core CPUs.</td>
</tr>
<tr>
<td>Virtual Machine - Count by Memory Usage Severity</td>
<td>This chart displays a total count for all virtual machines of memory usage severity. The severity levels are critical, normal, and warning. You can drill down on the severity levels to see the details of the machines and the threshold set for that severity level for that metric (average_mem_usage_percent).</td>
</tr>
<tr>
<td>Virtual Machine - Count by Disk Usage Severity</td>
<td>This chart displays a count of virtual machines for their disk usage severity. The search is based on the average_disk_usage_kiloBytesPerSecond metric and it's looking for a threshold severity &quot;unchecked&quot;. Drill down from the chart to see details for each virtual machine.</td>
</tr>
<tr>
<td>VMs With Old or No Tools</td>
<td>This search result shows all of the virtual machines in your environment that that have an old version of VMware Tools installed and those that do not have VMware Tools installed.</td>
</tr>
<tr>
<td>Total VM Migrations</td>
<td>This chart displays the total number of virtual machines that migrated across all of the hosts in your environment. Drill down on the Total Migrations count to get a list of all migrated virtual machines.</td>
</tr>
<tr>
<td>Powered Off VMs</td>
<td>This search produces a list of all virtual machines that were powered off. The sourcetype=&quot;vmware:inv:vm&quot; is used in the report.</td>
</tr>
<tr>
<td>Max Disk Latency per VM</td>
<td>This is the maximum disk latency per virtual machine for all of the hosts in your environment. The latency severity is broken down into critical, normal, and warning. Drill down on the severity level to get more details. The metric</td>
</tr>
<tr>
<td>Report Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>latest_disk_maxTotalLatency_millisecond</td>
<td>is used to determine severity.</td>
</tr>
</tbody>
</table>

### Security reports

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vmware Security changes</td>
<td>A report that shows changes to user roles on the host systems in your environment. The source type <code>vmware:events</code> must be present.</td>
</tr>
</tbody>
</table>

### User activity reports

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Per-Panel Filtering - Activity By User Over Time</td>
<td>A report that displays user activity over the time range specified.</td>
</tr>
<tr>
<td>Per-Panel Filtering - Recent Activity</td>
<td>A report that displays recent user activity.</td>
</tr>
<tr>
<td>Per-Panel Filtering - Top Users</td>
<td>A report that shows the most frequent users.</td>
</tr>
</tbody>
</table>

### Reports on critical status

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical CPU Ready</td>
<td>A report that displays all of the virtual machines that reached the critical threshold set for cpu ready for all of the virtual centers. CPU ready reports on the amount of time (in milliseconds) that a virtual machine waited for cpu cycles. The report uses the <code>p_summation_cpu_ready_millisecond</code> metric.</td>
</tr>
<tr>
<td>Critical CPU Usage</td>
<td>A report that displays all of the virtual machines with critical CPU usage for all of the virtual centers in your environment. The report uses the <code>p_average_cpu_usage_percent</code> metric.</td>
</tr>
<tr>
<td>Critical Disk Usage</td>
<td>A report that displays all of the virtual machines with critical disk usage for all of the hosts in your environment. The report uses the <code>p_average_disk_usage_kiloBytesPerSecond</code> metric.</td>
</tr>
<tr>
<td>Critical Mem Usage</td>
<td></td>
</tr>
</tbody>
</table>

71
A report that displays all of the virtual machines with critical memory usage for all the virtual centers in your environment. The report uses the `p_average_mem_usage_percent` metric.

### CPU reports

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average VM CPU Ready</td>
<td>The virtual machine CPU Ready state for all of the hosts. It uses the <code>p_summation_cpu_ready_millisecond</code> metric.</td>
</tr>
<tr>
<td>CPU Ready by VC</td>
<td>This report displays a timechart for CPU Ready for all of the hosts. It uses the <code>p_summation_cpu_ready_millisecond</code> metric.</td>
</tr>
<tr>
<td>CPU Usage by Cluster</td>
<td>This report displays the CPU usage by cluster for all of the virtual centers in your environment. It uses the <code>p_average_cpu_usage_percent</code> metric.</td>
</tr>
<tr>
<td>CPU Usage by VC</td>
<td>This report displays the CPU usage by each virtual center for the selected time. It uses the <code>p_average_cpu_usage_percent</code> metric.</td>
</tr>
<tr>
<td>Average CPU Utilization</td>
<td>This report displays the average CPU usage as a percent and a count for the state of the critical, warning, and normal threshold severity levels. It uses the <code>p_average_cpu_usage_percent</code> metric.</td>
</tr>
</tbody>
</table>

### Storage/network error Reports

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All paths are dead</td>
<td>The All Paths Down (APD) state occurs when a storage device is removed from an ESX/i host in an uncontrolled manner (administrative error or device failure). This condition can affect task execution on a host as the host processes can wait for a device to return and there is no certainty that it will return. The search uses the sourcetype <code>vmware:*log:*</code>.</td>
</tr>
<tr>
<td>SCSI reservation error - i/o failed</td>
<td>This search shows virtual machines that experience I/O failures due to too many</td>
</tr>
<tr>
<td>Report Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Lost connectivity        | VMware vSphere logs an alert that contains 'Configuration Issue' when it loses connectivity to a device. The search uses the sourcetype vmware:*log:*.
| Duplicate IPs            | An error messages indicates that a duplicate IP address exists. Search VMware ESX/i logs for the string "duplicate IP". The sourcetype vmware:esx:*:* is used in the search. |
| Datastore Free Space state | This chart shows the severity level associated with the free space capacity on the data store. The source type vmware:inv:datastore is used. The metric RemainingCapacity_GB is used. Drill down on the threshold severity to see more details such as the capacity of the data store, the amount of free space, the name of the data store, the threshold critical level, and more. |

**Alarm reports**

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarms</td>
<td>This search shows alarms from all of the virtual centers in your environment. Click on the alarm to drill down to more details. The sourcetype vmware:events is used in the search.</td>
</tr>
</tbody>
</table>