



OnCommand® Insight 7.2

Assurance User Guide for the Java UI

March 2016 | 215-10384_A0
doccomments@netapp.com

Contents

OnCommand Insight Assurance features	6
Policy management	7
Modifying default global policies to control performance	7
General policy types and their hierarchies	7
Reviewing global general policies	8
Setting and managing switch thresholds and performance alerts	9
Customizing global general policies	13
Setting violation notifications	14
Changing the severity levels for violation types	15
Creating and changing SAN path policies	16
Defining and reviewing SAN path policies	16
Editing SAN path policies	25
Disabling global path policies	26
Removing SAN path policies	26
Policies reference	26
Modify Policy wizard - first page	27
Policies view	28
SAN Path Policies view	28
Settings for FC global policies	30
Settings for Global Policies	31
Settings for iSCSI global policies	32
Violation Notification settings	33
Violation Severity settings	33
Monitoring changes in your environment	34
Types of changes you can monitor in your environment	35
Filtering the list of changes	35
Troubleshooting with topology and change history	36
Creating an HTML report of changes	37
Monitoring changes reference	37
Changes main view	37
Changes detail view	39
Datastores view	40
File Systems detail view	42
VMDKs detail view	43
Virtual Machines view	45
Allocating capacity	48
Identifying unused capacity	48
Avoiding over-commitment problems	49
Violation management	51
General violation analysis and correction	51
General violation types	52

Filtering the displayed severity levels	53
Analyzing general violations	53
Dismissing violations	61
SAN path violations analysis and correction	61
Investigating SAN path violations	61
Reviewing paths related to a violation	62
Correcting SAN path violations	62
Analyzing path outage violations	65
Analyzing a missing path redundancy violation	66
Analyzing a missing path	67
Reviewing system changes linked to a SAN path violation	68
Clearing multiple path violations quickly	68
Identifying violations associated with planned tasks	69
Setting virtualization policy and monitoring VM violations	69
Violations related to VMs	69
Analyzing VM violations: Missing virtual cluster path	70
Violations reference	71
Alerts view	71
Analyze Storage Pools dialog box	72
Port Balance Violations view	75
Reservation Violations view	76
SAN Path Violations view	77
Topology view	82
Violations Browser	82
VMDK Performance view	85
Analyzing and managing vulnerabilities	88
Viewing vulnerabilities data	88
OnCommand Insight Applications Dashboard	89
Researching vulnerabilities	90
Establishing vulnerability thresholds	91
Managing thin provisioning using vulnerabilities	91
Orphaned Volumes vulnerability	92
Spare Disks vulnerability	92
Adding hosts to application groups	93
Vulnerabilities main view and types	94
Disconnected Switch Port Zone Members vulnerability for Fibre Channel	94
Disconnected WWN Zone Members vulnerability for Fibre Channel	94
Duplicate Backend Volume Assignments vulnerability	95
High Fabric Port Usage vulnerability for Fibre Channel	95
High Volume Allocation vulnerability	95
Incomplete Application Volume Sharing vulnerability	95
Inconsistent Volume Member Disks RPM vulnerability	96
Local Replica for Undefined Volumes vulnerability	96
Low Fabric Port Usage vulnerability for Fibre Channel only	97

Orphaned Volumes vulnerability	97
Replication Capacity Mismatch vulnerability	98
Shared Volume Masking vulnerability	98
Spare Disks vulnerability	99
Unused Masked Volumes vulnerability	100
Volume and Replica Share Same Disk vulnerability	100
Volume with Members on Same Disk vulnerability	101
Volumes have LUNs with value greater than 255 vulnerability	101
Copyright information	103
Trademark information	104
How to send comments about documentation and receive update notifications	105
Index	106

OnCommand Insight Assurance features

OnCommand Insight Assurance features help you analyze and validate your SAN change processes for Fibre Channel and iSCSI data, tracking the impact of SAN changes and events even before they occur. Assurance features also enable you to define global, application, and host-based policies on parameters such as security, sharing, and minimum connections and then analyze violations against the policies.

OnCommand Insight allows you to set and change environment policies and analyze violations. When a violation occurs (often due to human error), OnCommand Insight detects it immediately, identifies the implications, and analyzes the impact and the root cause of the problem in a manner that enables rapid and effective correction.

You can use Assurance features along with virtualization management solutions, such as VMware.

These OnCommand Insight features operate with virtually all SAN devices and do not require any host agents. OnCommand Insight does not affect the SAN data paths and never changes the state anywhere in the SAN. Instead, OnCommand Insight provides detailed information and analysis tools.

Policy management

The OnCommand Insight policies are the rules used to evaluate conformance to defined preferences. There are two types of policies: specific SAN path policies and general policies.

Policies can be attached to physical system elements such as a host or storage, and also to logical elements such as virtual machines, paths, or fabrics. Policies may be based on detecting compliance with configurations, or based on transitory events like a performance spike.

All OnCommand Insight policies are pre-set with global default values that you can modify. You might also add policies to override the global policy settings in specific situations.

Modifying default global policies to control performance

Insight provides the default global policies for the elements in the environment to generate performance violation notifications when the thresholds you set are reached. These global policies cannot be removed from the system. However, you can modify or disable any of these default global performance policies using the settings options. They can be customized to treat specific elements in your environment differently from the standard global policies using the Modify Policy wizard.

About this task

These are not the SAN path global policies.

Steps

1. From the **Client Main Menu**, select **Tools > Settings**.
2. Display the current settings for these policies by selecting **Policies**, and then selecting **Global Policies**.
3. Change the value for one or more of the global performance policies:
 - Blocked Generic Devices
 - Blocked Hosts
 - High Fan-Out
 - Host Port Balance
 - Storage Pool Capacity Assurance
 - Storage Pool Capacity
 - Storage Pool Over-Commit
 - Storage Port Balance
 - Tape Port Balance
4. Click **OK** to save the changes.

Note: Any changes to these policies are reported in the Audit log.

General policy types and their hierarchies

The general policies that evaluate the elements in your environment are governed by the policy hierarchy. All of the global general policy types have default policies that govern your environment.

You can customize the default global policies and add policy exceptions on lower-level (not global level) components in the hierarchy.

Blocked Generic Devices

Alerts the administrator when unidentified hosts (generic devices) cannot contact any volumes or shares.

Blocked Hosts

Alerts the administrator when a host cannot contact any volumes or shares. This policy can only be set at the global level.

Host Port Balance

Sets the threshold for the traffic load across a device's Fibre Channel (FC) ports to be evenly distributed. You can create a policy exception for the storage level.

Storage Pool Used Capacity

Sets the percentage threshold for the used capacity of the storage pool. You can create a policy exception for storage array and then for storage pools.

Storage Pool Capacity Assurance

Defines the thin-provisioned storage pools (aggregate) where the sum of unused capacity exceeds current unused space of the storage pool. A violation is generated when a storage pool does not have enough unused capacity to accommodate remaining reserved unused space. By Default, three volumes need to maintain enough capacity to accommodate unused space. Therefore, the number in the global policy is the number of volumes required to maintain enough capacity to accommodate unused space.

Storage Pool Commit Ratio

Sets the percentage threshold for the commit ratio. You can create a policy exception for storage and then for storage pools.

Storage Pool Utilization

Sets the threshold for the hourly average of the storage pool utilization percentage.

Storage Port Balance

Sets the threshold for the traffic on storage FC ports to be evenly distributed. You can create a policy exception for storage array.

Storage Pool Fan-Out

Sets the number of masked hosts (generic devices) for storage ports. This policy can only be set at the global level.

Tape Port Balance

Sets the threshold for the traffic on a tape's FC ports to be evenly distributed. You can create a policy exception for tape.

Reviewing global general policies

To review the global general policies in your environment, use the Policies view.

Steps

1. Select **Assurance > Policies**.
Each line in the view represents a general policy type.
2. To examine specific details for a policy that has generated violations, click a policy type shown in red, expand the list, and note the description of the policy that has been violated.

Policy Type	Policy Level	Target	Description
Blocked Generic Devices (1)	Global	Global	
Blocked Hosts (1)	Global	Global	
Internal Volume Performance (1)	Global	Global	
Maximum Datastore Latency (1)	Global	Global	
Maximum Disk Utilization (1)	Global	Global	
Maximum Host Port Balance Index (1)	Global	Global	
Maximum Storage Port Balance Index (1)	Global	Global	
Maximum Tape Port Balance Index (1)	Global	Global	
Storage Pool Capacity Assurance (1)	Global	Global	
Storage Pool Commit Ratio Limit (1)	Global	Global	
Storage Pool Used Capacity Limit (1)	Global	Global	
Storage Port Fan-Out Maximum (1)	Global	Global	
Volume Performance (1)	Global	Global	

Element	Severity	Violation Type	Policy Type	Policy Level
Storage pool NTAP1:aggr... 2: Major	2: Major	Storage Pool Capacity Assurance	Storage Pool Capacity Assurance	Global
Storage pool NTAP1:aggr... 2: Major	2: Major	Storage Pool Capacity Assurance	Storage Pool Capacity Assurance	Global
Storage pool NTAP2:aggr... 2: Major	2: Major	Storage Pool Capacity Assurance	Storage Pool Capacity Assurance	Global
Storage pool NtapiSCSI1a... 2: Major	2: Major	Storage Pool Capacity Assurance	Storage Pool Capacity Assurance	Global
Storage pool NtapiSCSI1a... 2: Major	2: Major	Storage Pool Capacity Assurance	Storage Pool Capacity Assurance	Global
Storage pool NtapiSCSI2... 2: Major	2: Major	Storage Pool Capacity Assurance	Storage Pool Capacity Assurance	Global
Storage pool NtapiSCSI2a... 2: Major	2: Major	Storage Pool Capacity Assurance	Storage Pool Capacity Assurance	Global

- Click the **Violations List** icon to display the names of the elements that have violated in the selected policy type.

This example lists ten major storage pool capacity assurance violations below the Policies view.

- To modify a specific policy, right-click one or more lines in the **Violations List** or a line in the **Policies** view and select **Modify Policy**.

Setting and managing switch thresholds and performance alerts

The administrator can set thresholds that trigger performance alerts and violations.

OnCommand Insight monitors the activity on each switch port. You can change the default thresholds that constitute policies. If these policies are violated, an alert is issued.

Setting switch performance thresholds

You can set the minimum and maximum performance thresholds that constitute policies. When a threshold level is reached, an alert is issued. You can use the default thresholds or change them.

Before you begin

This option requires the Perform license. If this license is not enabled, you do not see the **Switch Thresholds** option in the tree on the left side of the Settings dialog box.

About this task

To set a threshold, enter the following parameters:

- Min:** The level above which a metric must remain to prevent an alert. If a level stays below this minimum for the time period, an alert is issued.
- Max:** The level below which a metric must remain to prevent an alert. If a level stays above this maximum for the time period, an alert is issued.
- Period (minutes):** The amount of time that a threshold can be exceeded before an alert is issued.

Steps

1. From the Insight Client menu, select **Tools > Settings**.
2. In the left tree of the **Settings**, click **Thresholds > Switch Thresholds** option.

You can set the switch performance thresholds on the Host, Switch, Storage, Generic Device, and Tape tabs.

Switch Thresholds

Set switch performance thresholds based on what the switch is connected to.

Host Switch Storage Generic Device Tape

Tx Utilization (%)	Period (minutes): 1	<input checked="" type="checkbox"/> Min: 2	<input checked="" type="checkbox"/> Max: 50
Rx Utilization (%)	Period (minutes): 1	<input checked="" type="checkbox"/> Min: 2	<input checked="" type="checkbox"/> Max: 40
Utilization (%)	Period (minutes): 1	<input checked="" type="checkbox"/> Min: 2	<input checked="" type="checkbox"/> Max: 60
CRC (%)	Period (minutes): 1	<input checked="" type="checkbox"/> Max: 60	
Other Errors (%)	Period (minutes): 60	<input type="checkbox"/> Max: 10	
Loss of Sync	Period (minutes): 60	<input type="checkbox"/> Max: 1	
Loss of Signal	Period (minutes): 60	<input type="checkbox"/> Max: 1	
Class 3 Discards	Period (minutes): 1	<input checked="" type="checkbox"/> Max: 60	
Frame Size Too Long	Period (minutes): 1	<input checked="" type="checkbox"/> Max: 60	
Frame Size Too Short	Period (minutes): 1	<input checked="" type="checkbox"/> Max: 60	
BB Credit Errors	Period (minutes): 60	<input type="checkbox"/> Max: 1	

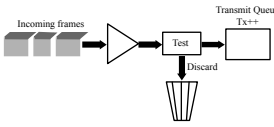
Apply

3. On any of the tabs, configure the following settings:
 - Tx Utilization %: Percentage of available bandwidth used for transmission (Tx).
 - Rx Utilization %: Percentage of available bandwidth used for reception (Rx).
 - Utilization %: Percentage of available bandwidth used for transmission (Tx) and reception (Rx).
 - Loss of Sync: Number of loss of synchronization errors. The port has to re-synchronize after each such errors, which impacts performance.
 - Loss of Signal: Number of loss of signal errors.
 - CRC: Number of CRC frame errors as percentage of the total data traffic.
 - Error %: Total number of errors (Loss of Sync, Loss of Signal, and Framing) as a percentage of the total data traffic.
 - Class 3 Discards: The count of Fibre Channel (FC) Class 3 data transport discards.

- Frame Size Too Long: The count of FC data transmission frames that are too long.
 - Frame Size Too Short: The count of FC data transmission frames that are too short.
 - BB Credit Errors: The count of FC data transmission frames in the buffer that exceed the threshold.
4. To save settings on one tab and continue with other tabs, click **Apply**.
- After you save one setting on a tab, an icon appears in the tab label indicating that the defaults were overridden.
5. Repeat all steps on the other tabs.
- You can set the switch performance thresholds based on what device is connected to the switch. Click on the tab (Host, Switch, Storage, Generic Device, or Tape) for that type of device.
6. Click **OK**.

Switch threshold types and formulas

OnCommand Insight uses these formulas to determine the switch port performance threshold data.

Threshold	Description	Formula
BB Credit Errors	Fibre Channel uses buffer-to-buffer credits to control transmission flow. The credit value is decremented when a frame is sent and replenished when a response is received. As the available credits for a given port approach zero, the error warns that the port will stop receiving transmissions when zero is reached and will not resume until the BB credits can be replenished.	
Class 3 Discards	The count of Fibre Channel Class 3 data transport discards.	
CRC Rate	CRC Rate is the measure of CRC frame errors as a percentage of the total data traffic. CRC frame errors indicate bit errors somewhere in the data path and point to poor connections, bad cables, or links that are too long.	$crcErrorRate = \frac{\Delta crcErrors}{\Delta RxFrames} 100$ 
Errors Rate	Total number of errors (Loss of Sync, Loss of Signal, and Framing)	$errorRate(\%) = \frac{\Delta error}{\Delta error + \Delta RxFrames + \Delta TxFrames} 100$
Frame Size Too Long	The count of Fibre Channel data transmission frames that are too long.	
Frame Size Too Short	The count of Fibre Channel data transmission frames that are too short.	
Loss of Signal	If a Loss of Signal error occurs, there is no electrical connection and a physical problem exists.	$lossOfSignal / sec(\%) = \frac{\Delta lossOfSignal}{\Delta sec} 100$

Threshold	Description	Formula
Loss of Sync	If a Loss of Sync error occurs, the hardware cannot make sense of the traffic or lock onto it. All of the equipment might not be using the same data rate or the optics or physical connections might be of poor quality. The port must re-sync after each such error, which impacts system performance.	$lossOfSync / sec(\%) = \frac{\Delta lossOfSync}{\Delta sec} 100$
Received Utilization	Percentage of available bandwidth used for Rx.	$RxUtilization(\%) = \frac{\Delta RxBits}{\Delta Seconds \cdot ActualSpeedBits} 100$
Transmit Utilization	Percentage of available bandwidth used for Tx.	$TxUtilization(\%) = \frac{\Delta TxBits}{\Delta Seconds \cdot ActualSpeedBits} 100$
Utilization	Percentage of available bandwidth used for Tx and Rx.	$Utilization(\%) = \frac{\max(\Delta RxBits, \Delta TxBits)}{\Delta Seconds \cdot ActualSpeedBits} 100$

Reviewing and confirming alerts

After you identify the cause of an alert or determine that you no longer need to be reminded about that alert, you need to clear alerts from the Switch Port Performance Alerts main view and Alerts detail view.

About this task

An alert is triggered when the performance metrics for any port exceed the threshold for the time specified.

Steps

1. In the OnCommand Insight **Open** menu, select **Assurance > Switch Port Performance Alerts**.
2. Expand the alert categories and select an alert that you want to examine in more detail.
3. Click the **Alerts** icon to see all of the switches and ports associated with the selected alert.
4. Select one or more of the switches in the Alerts view.
5. Click the **Performance Chart** icon to see a graphic display of the alerts.
6. You might also want to display the Changes and Switch Port Performance information for selected alerts.
7. To confirm and delete an alert from the display, right-click the line in the Alerts view.

If you do not confirm an alert, it appears every time you display the Switch Port Performance Alerts view.

Changing or disabling switch thresholds

You can change switch thresholds at any time. The threshold set at a particular time appears when an alert condition occurs. You can also disable thresholds.

Steps

1. From the OnCommand Insight **Open** menu, select **Assurance > Switch Port Performance Alerts**.
2. In the **Switch Port Performance Alerts** view, right-click on a threshold and select **Configure**.
The Switch Thresholds settings dialog box opens.
3. Change the values as needed.
4. To disable any thresholds for which you no longer want to receive alerts, clear the **Max** and **Min** check boxes.
5. Click **Apply** to save the changes on one tab and move to another tab.
6. Click **OK** to save all of the threshold changes.

Customizing global general policies

You might want to modify global general policies, not the global SAN path policies, for special characteristics in one area of your environment.

About this task

Using the Modify Policy wizard, you can customize the global general policies, create exceptions to these policies, and remove exceptions to the global policies for the selected items. You can also disable the evaluation of the parent global policy at the selected level.

Steps

1. From the OnCommand Insight **Open** menu, select **Assurance** and any of these views:
 - Violations Browser
 - Storage Pool Utilization Violations
 - Port Balance Violations
 - Policies

Or you might open any of these **Inventory** views:

- Hosts
 - Datastores
 - Storage Arrays
 - Tapes
2. Select one or more items in the selected view to examine and possibly modify the global general policy to customize it for one area of your environment.
 3. Right-click and select **Modify Policy**.

4. If more than one policy type applies to the selected items, these policy types are listed on the first page of the Modify Policy wizard. Select the policy type you want to examine and possibly change. Click **Next**. Otherwise, the second page is displayed.

At any point, you can return to previous pages in the wizard to review or make additional changes.

5. Select the type of policy modification you want.

If you selected more than one item in the view, you might be modifying different settings of the same policy, and the wizard shows that condition by listing the **Current policy** as “Mixed”.

6. Select a policy.

7. Click **Next** to save the selected modification type.

8. The third page of the wizard enables you to enter settings for the policies. Make the setting selections and click **Next**.

9. The fourth and final wizard page lists the previous policy and the changes you made so that you can review and confirm those changes.

If there were multiple policy types listed on the first page and you want to make changes to a different policy type, select **Modify another policy on the same selections** on the confirmation page.

10. Click **Finish** to save your changes

All changes to the policies are recorded in the Audit log.

Setting violation notifications

You can use the OnCommand Insight SNMP, Syslog, and email settings to notify administrators when violations are generated from the general or path policies.

Steps

1. From OnCommand Insight **Client Main Menu**, select **Tools > Settings**.
2. In the settings tree, click **Violation Notification**.
3. You can optionally use the link for the SNMP and Syslog servers to check or change the current SNMP trap and Syslog configurations and then return to this dialog box.
4. Below the link, select the message management methods you want to use: SNMP traps and the Syslog.
5. Select the threshold of the violation severity for these notifications.

Any violation with a severity below the selected level will not generate a notification.

Configure Violation Notification

Configure the notifications that will occur when violations are detected

☐ Notify by SNMP traps every violation detected with severity at or above: 4: Warning ▼

☐ Notify by Syslog message every violation detected with severity at or above: 4: Warning ▼

☒ Send email to the addresses below for any violation with severity at or above: 2: Major ▼

email Address

bobsmith@company.com

Add

Edit

Remove

i SNMP, Syslog, and email settings can be configured in the [OnCommand Insight Portal](#)

6. To notify specific individuals when violations reach a specific severity, click **Add** to enter their email addresses and select the severity level.
7. Click **OK**.

Changing the severity levels for violation types

You can change the severity levels assigned to violation types to match conditions in your environment. The severity settings also control the notifications for violations generated from the general policies. For example, if you want to be notified as soon as there is activity approaching a threshold, you set that severity to Warning, but if one of the general violations is a serious problem in your environment, you might set the notification level to Major or even Critical.

Steps

1. On the **Client Main Menu**, select **Tools > Settings**.
2. In the **Settings** window, expand the Policies tree.
3. Select **Violation Severity**.
4. Select the new severity level for any of the violation types.

The violation types are grouped into categories such as array performance and blocked devices violations. You can set a violation severity level for every violation type.

5. Click **OK**.

If a new severity setting raises the notification level, notifications will be generated. You should also check the SNMP trap and Syslog message levels to verify that severity levels that generate notifications are not conflicting with these settings.

Creating and changing SAN path policies

After designing the global storage policy and identifying any exceptions to it for your network, you are ready to enter the SAN path policies and make changes as needed.

About this task

To create and refine the SAN path policies for your network, follow these general steps:

Steps

1. To define the ideal storage environment, enter the global storage policy information into OnCommand Insight.
2. Enter any additional global policy information required for Volume Type and Volume Capacity exceptions.
3. Review vulnerabilities and violations to observe your SAN path policies in your environment.
4. Define any additional policies needed to handle exceptions to your global policy.

Note: Limit the number of policies to reduce the work required to investigate violations in the future.
5. Enter any required host or path policies.
6. Review vulnerabilities and violations to observe your policies in your environment.
7. Change or delete policies as needed.

Defining and reviewing SAN path policies

OnCommand Insight monitors your SAN paths based on service policies.

Service policies contain thresholds that allow OnCommand Insight to monitor your network and notify you of vulnerabilities and violations:

For each path, one and only one policy is enforced at any point in time. By verifying the path against this policy, OnCommand Insight does the following:

- Authorizes the access between the path's host and its data on a volume.
- Enforces the required level of redundancy for the path.
- Ensures that a minimum number of host ports have access to the storage volume or tape device.
- Ensures that a minimum number of storage ports have access to the host.
- Monitors the number of switch hops, making sure it does not exceed the maximum allowed by the policy.

Global path policies

OnCommand Insight supports global policies for Fibre Channel and iSCSI to authorize paths in the absence of a more restrictive host or specific path policy. The global path policies reduce overall maintenance and eliminate the need to configure policies for each path.

Specific host and path policies

You might specify an individual policy for a special host environment or an individual path that has an ongoing relationship to a specific volume.

- Host policies apply to specific host servers. OnCommand Insight uses a host policy to authorize new paths to the corresponding host automatically. Host policies also have these special characteristics:
 - If a global policy exists for the specific volume type or volume capacity, the global policy takes precedence.
 - Host policies are typically used as exceptions to the global policies when there are unique host requirements such as a laboratory environment.
- Path policies allow you to establish detailed path-specific policies, as needed. Global and host policies can reduce the need for individual path policies.
 - **Best practice:** Reserve path policies for use as exceptions that cannot be handled by these higher-level policies.
 - Path policies should be rare and only used for specific exceptions to your global policy.

Creating global SAN path policies

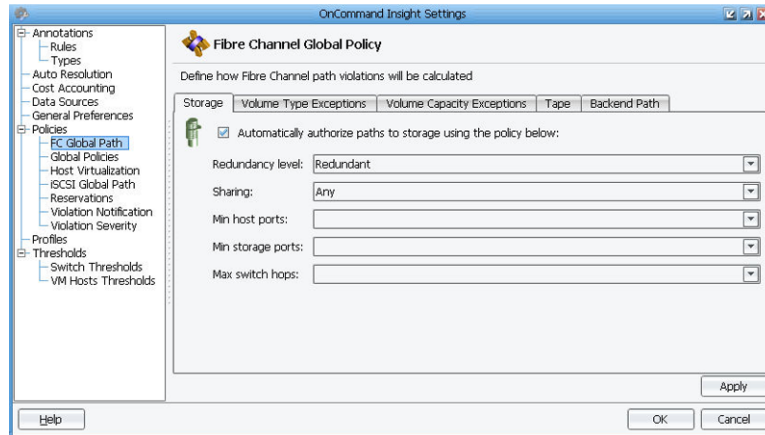
To establish global SAN path policies easily, create global policies for the Fibre Channel and iSCSI environments. This feature is available with the Assure license.

Steps

1. On the main menu, select **Tools > Settings**.
2. In **Settings**, expand the Policies tree.
3. Select **FC Global Path** for Fibre Channel global policies or **iSCSI Global Path**.
4. Click the tab to define a specific type of global policy.

In this example, the types of Fibre Channel global policies are accessed using these tabs:

- Storage
- Volume Type Exceptions
- Volume Capacity Exceptions
- Tape
- Backend Path



Defining the global Fibre Channel storage policy

The global storage Fibre Channel policy authorizes new paths to all storage volumes. This policy describes the ideal storage environment for your network. Any other policies you create are exceptions to this global policy.

Steps

1. On the main menu, select **Tools > Settings**.
2. In the **Settings** window, expand the Policies tree and select **FC Global Path**.
3. Be certain that the **Storage** tab is selected and the **Automatically authorize paths to storage using the policy below** check box is selected to activate the completed policy automatically.
4. Select the **Redundancy level** as one of the following:
 - **No SPF** - requires the host to reach the storage device through at least two different paths, where both can be on a single fabric.
 - **Redundant** - requires the host to reach the storage device through at least two different fabrics.
5. Select the type of **Sharing** as one of the following:
 - **Any** - any host can share the storage volume, so OnCommand Insight does not monitor volume sharing.
 - **No Sharing** - only one host can access a particular volume at any given moment. If two hosts access the same SAN volume and this access is not coordinated, it is likely to cause data corruption and loss.
 - **Application** - hosts that share at least one application with the hosts covered by this global policy can share the same volume, but other hosts cannot.
6. Select the minimum number of **host ports** that should be active (that is, ports that have access to the storage volume or tape device) for the path.
7. Select the minimum number of **storage ports** that can be set for each path.
8. Select the maximum number of **switch hops** on the shortest path between the host of the path and its storage data.
9. Click **OK**.

Only one global storage policy can be created for your network.

Defining global volume type exceptions for Fibre Channel

The Fibre Channel global volume type exceptions policy authorizes new paths to a particular type of volume such as BV, Meta LUN, or SFS. This is particularly useful when specific volumes require a low-end policy and when new paths provide access to backup copies.

Steps

1. On the main menu, select **Tools > Settings**.
2. In the **Settings** window, expand the Policies tree and select **FC Global Path**.
3. Click the **Volume Type Exceptions** tab.
4. Select the **Automatically authorize paths to storage with volumes of type** check box to activate the completed policy automatically.
5. In the scrolling selection box, check each of the volume **Types** to which this policy applies.
6. Select the **Redundancy level** as one of the following:
 - **None** - no redundancy is required on the path.
 - **No SPF** - no single point of failure.
 - **Redundant** - requires the host to reach the storage device through at least two different fabrics.
7. Select the type of **Sharing** as one of the following:
 - **Any** - any host can share the storage volume.
 - **No Sharing** - all access to the volume must originate from the path's host device.
 - **Application** - hosts that share at least one application with this host can share the same volume, but other hosts cannot.
8. Select the minimum number of **host ports** that should be active for the path.
9. Select the minimum number of **storage ports** that can be set for each path.
10. Select the maximum number of **switch hops** on the shortest path between the host of the path and its storage data.
11. Click **OK**.

Defining global volume capacity exception policies for Fibre Channel

The Fibre Channel global volume capacity exception policy authorizes new paths that access volumes smaller than a specified capacity. This policy typically targets management volumes used by vendors' management tools such as EMC Solutions Enabler. The volumes tend to be small and allow you to establish a low-end policy for them.

Steps

1. On the main menu, select **Tools > Settings**.
2. In the **Settings** window, expand the Policies tree and select **FC Global Path**.
3. Click the **Volume Capacity Exceptions** tab.
4. Select the **Automatically authorize paths to storage with volumes smaller than** check box to activate the completed policy automatically.

5. Enter the volume **Capacity** in megabytes.
6. Select the **Redundancy level** as one of the following:
 - **None** - no redundancy is required on the path.
 - **No SPF** - no single point of failure.
 - **Redundant** - requires the host to reach the storage device through at least two different fabrics.
7. Select the type of **Sharing** as one of the following:
 - **Any** - any host can share the storage volume.
 - **No Sharing** - all access to the volume must originate from the path's host device.
 - **Application** - hosts that share at least one application with this host can share the same volume, but other hosts cannot.
8. Select the minimum number of **host ports** that should be active for each path.
9. Select the minimum number of **storage ports** that can be set for each path.
10. Select the maximum number of **switch hops** on the shortest path between the host of each path and its storage data.
11. Click **OK**.

Defining global tape policies for Fibre Channel

The Fibre Channel global tape policy authorizes new paths to tape devices.

Steps

1. On the main menu, select **Tools > Settings**.
2. In the **Settings** window, expand the Policies tree and select **FC Global Path**.
3. Click the **Tape** tab.
4. Select the **Automatically authorize paths to tape with the policy below** check box to activate the completed policy automatically.
5. Select the **Redundancy level** as one of the following:
 - **None** - no redundancy is required on the path.
 - **No SPF** - no single point of failure.
 - **Redundant** - requires the host to reach the storage device through at least two different fabrics.
6. Select the minimum number of **host ports** that should be active for the path.
7. Select the minimum number of **storage ports** that can be set for the path.
8. Select the maximum number of **switch hops** on the shortest path between the host of the path and its storage data.
9. Click **OK**.

Defining global backend path policies for Fibre Channel

Set the global backend path policy to generate a path outage violation when the connectivity between storage units goes down.

Steps

1. On the main menu, select **Tools > Settings**.
2. In the **Settings** window, expand the Policies tree and select **FC Global Path**.
3. Click the **Backend Path** tab.
4. Select the **Automatically authorize paths to backend storage using the policy below** check box to activate the completed policy automatically.
5. Select the **Redundancy level** as one of the following:
 - **None** - no redundancy is required on the path.
 - **No SPF** - no single point of failure.
 - **Redundant** - requires the virtualizer port to reach the storage device through at least two different fabrics.
6. Select the minimum number of **virtualizer ports** that should be active for the path.
7. Select the minimum number of **backend storage ports** that can be set for each path.
8. Select the maximum number of **switch hops** on the shortest path between the virtualizer port of the path and its storage data.
9. Click **OK**.

Defining the global storage policy for iSCSI

The iSCSI global storage policy authorizes new paths to all storage volumes. This policy describes the ideal storage design for your environment. Only one global storage policy can be set for your environment. Any other policies you create are exceptions to this global policy.

Steps

1. On the main menu, select **Tools > Settings**.
2. In the **Settings** window, expand the Policies tree and select **iSCSI Global Path**.
3. Be certain that the **Storage** tab is selected and the **Automatically authorize paths to storage using the policy below** check box is selected to activate the completed policy automatically.
4. Select the **Require security** option as **Yes** or **No**.
5. Select the type of **Sharing** as one of the following:
 - **Any** - any host can share the storage volume.
 - **No Sharing** - all access to the volume must originate from the path's host device.
 - **Application** - hosts that share at least one application with this host can share the same volume, but other hosts cannot.
6. Select the minimum number of **sessions** required. The default is two.
7. Select the minimum number of **connections** required. The default is two.

8. Click **OK**.

Defining global volume type exceptions policies for iSCSI

The iSCSI global volume type exceptions policy authorizes new paths to selected volume types. This is particularly useful for volumes that require a low-end policy.

Steps

1. On the main menu, select **Tools > Settings**.
2. In the **Settings** window, expand the Policies tree and select **iSCSI Global Path**.
3. Click the **Volume Type Exceptions** tab.
4. Select the **Automatically authorize paths to storage with volumes of type** check box to activate the completed policy automatically.
5. Select all of the applicable volume **Types** from the scrollable list.
6. Select the **Require security** option as **Yes** or **No**.
7. Select the type of **Sharing** as one of the following:
 - **Any** - any host can share the storage volume.
 - **No Sharing** - all access to the volume must originate from the path's host device.
 - **Application** - hosts that share at least one application with this host can share the same volume, but other hosts cannot.
8. Select the minimum number of **sessions** required.
9. Select the minimum number of **connections** required.
10. Click **OK**.

Defining global volume capacity exceptions policies for iSCSI

The iSCSI global volume capacity exceptions policy authorizes new paths that access volumes that are smaller than a specified capacity.

Steps

1. On the main menu, select **Tools > Settings**.
2. In the **Settings** window, expand the Policies tree and select **iSCSI Global Path**.
3. Click the **Volume Capacity Exceptions** tab.
4. Select the **Automatically authorize paths to storage with volumes smaller than** check box to activate the completed policy automatically.
5. Enter the **Capacity** in megabytes.
6. Select the **Require security** option as **Yes** or **No**.
7. Select the type of **Sharing** as one of the following:
 - **Any** - any host can share the storage volume.
 - **No Sharing** - all access to the volume must originate from the path's host device.

- **Application** - hosts that share at least one application with this host can share the same volume, but other hosts cannot.
8. Select the minimum number of sessions required.
 9. Select the minimum number of connections required.
 10. Click **OK**.

Creating specific path policies

You can specify a policy for the host of a particular path or a specific path. A path policy overrides any other policy settings that might apply for a path. In the absence of a specific path policy, OnCommand Insight authorizes the path using a global or host policy.

About this task

You can set a policy for paths one at a time, or you can group paths to use the same policy settings. Then you can authorize them in a single step.

Steps

1. To display a list of all of your network paths, click the OnCommand Insight **Open** menu and select **Inventory > Paths**.
2. Select the path that needs a policy.

Note: You can select a range of paths using the <Shift> key or multiple non-contiguous paths using the <Ctrl> key.
3. Right click and select **Set Path Policy**.

Note: A path policy is used infrequently because it defines a host that has an on-going relationship to a volume.
4. Make the necessary selections for the type of policy you selected.

Set Fibre Channel Path Policy

Configure the options for this Fibre Channel path policy

Redundancy level: No SPF

Sharing: Any

Min host ports: 2

Min storage ports: 2

Max switch hops: 2

OK Cancel

5. Click **OK**.

Result

The system authorizes the selected path using the policy settings specified.

Creating host policies

You can specify a policy for the host. In the absence of a path policy, OnCommand Insight authorizes a path using a global or host policy.

Steps

1. To display a list of all of your network paths, click the **Open** menu and select **Inventory > Paths**.
2. To create a host policy, you only need to highlight one path for the host. OnCommand Insight automatically applies the policy to any other paths that share the same host server.
3. Right click and select **Set Host Policy**.

Note: A host policy defines a special environment that does not comply with the global policy such as a laboratory.

4. Make the necessary selections for the type of policy you selected.
5. Click **OK**.

The system authorizes new paths to the corresponding host.

Reviewing SAN path policies

To review the SAN path policies in your environment, use the SAN Path Policies view. In this view, you can highlight a row to display information about the policy and all of the SAN changes that relate to the policy including the physical actions and configuration changes and the implications of those changes. If a row is displayed in red, that policy has been violated and requires research into the cause.

Steps

1. Click the **Open** menu and select **Assurance > SAN Path Policies**.

Beside the table title is the total number of policies in the list and the number of groups of policies. Each row in the table represents a single policy for a specific path or for all paths for a specific host. If a row is red, OnCommand Insight has detected a SAN path policy-related violation.

2. To examine the specific details for a policy, select the policy in the **SAN Path Policies** view and click one of the icons at the bottom of the window.

These icons open the detail views below the SAN Path Policies view with this information:

- Properties
- Fibre Channel ports
- iSCSI sessions
- Network portals
- Zone members
- Masking
- Disks
- Volumes
- Backend Volumes
- SAN Path Violations

- Changes
- Replications

You can open multiple detail views at the same time. This example shows a policy selected in the SAN Path Policies view with the Volumes and SAN Path Violations detail views for that policy.

The screenshot displays three panels in the OnCommand Insight interface:

- SAN Path Policies (85) Group: 33**: A table listing various policies. The selected policy is 'exchange_nrl (8)'.
- Volumes (8)**: A table showing storage volumes associated with the selected policy. The selected volume is 'XP 1024-11... 00:00'.
- SAN Path Violations (8)**: A table showing violations for the selected volume. The selected violation is 'Path Missing Redundancy each...'.

Technology	Policy Type	Host	Storage	Volume	Owner	Since	Redundancy	Sharing	Min Host Port	Min Storage	Max Hops	Require Security
FC	Path	1	NtapSantest1		admin		Redundant	Any	Any	Any	Any	Any
FC	Path	1	Roddick		admin		Redundant	Any	2	Any	1	Any
FC	Path	1	Satin		admin		Redundant	Any	2	Any	1	Any
FC	Path	1	Sampras		admin		Redundant	Any	2	Any	1	Any
FC	Path	3	NtapSantest2		admin		Redundant	Any	Any	Any	Any	Any
FC	Path	8	exchange_nrl		admin		Redundant	Any	Any	Any	Any	Any
FC	Path	exchange_nrl	XP 1024-11...	00:00	admin	8/15/1...	Redundant	Any	Any	Any	Any	Any
FC	Path	exchange_nrl	XP 1024-11...	00:01	admin	8/15/1...	Redundant	Any	Any	Any	Any	Any
FC	Path	exchange_nrl	XP 1024-11...	00:02	admin	8/15/1...	Redundant	Any	Any	Any	Any	Any
FC	Path	exchange_nrl	XP 1024-11...	00:03	admin	8/15/1...	Redundant	Any	Any	Any	Any	Any
FC	Path	exchange_nrl	XP 1024-11...	00:04	admin	8/15/1...	Redundant	Any	Any	Any	Any	Any
FC	Path	exchange_nrl	XP 1024-11...	00:05	admin	8/15/1...	Redundant	Any	Any	Any	Any	Any
FC	Path	exchange_nrl	XP 1024-11...	00:06	admin	8/15/1...	Redundant	Any	Any	Any	Any	Any
FC	Path	exchange_nrl	XP 1024-11...	00:07	admin	8/15/1...	Redundant	Any	Any	Any	Any	Any

Volume	Label	Storage	Storage Pool	Label	Internal Volume	Qtree	Virtualizer	Virtual Storage B
00:00	XP 1024-1112005	SP-0						
00:01	XP 1024-1112005	SP-1						
00:02	XP 1024-1112005	SP-0						
00:03	XP 1024-1112005	SP-1						
00:04	XP 1024-1112005	SP-0						
00:05	XP 1024-1112005	SP-1						
00:06	XP 1024-1112005	SP-0						
00:07	XP 1024-1112005	SP-1						

Policy Type	Violation Type	Host	Volume	Storage Pool	Volume	Capacity (GB)	Active
Path	Missing Redundancy each...	XP 102...	SP-0		00:00	8.00	
Path	Missing Redundancy each...	XP 102...	SP-0		00:02	8.00	
Path	Missing Redundancy each...	XP 102...	SP-0		00:04	8.00	
Path	Missing Redundancy each...	XP 102...	SP-0		00:06	8.00	
Path	Missing Redundancy each...	XP 102...	SP-1		00:01	8.00	
Path	Missing Redundancy each...	XP 102...	SP-1		00:03	8.00	
Path	Missing Redundancy each...	XP 102...	SP-1		00:05	8.00	
Path	Missing Redundancy each...	XP 102...	SP-1		00:07	8.00	

Editing SAN path policies

After creating and reviewing SAN path policies, you might need to edit them.

Before you begin

Enter one global storage SAN path policy for your environment and any exception policies you need. Inspect the SAN Path Violations view to see how well the policies work in your environment.

Steps

1. To locate a policy associated with a violation, click the OnCommand Insight **Open** menu and select **Assurance > SAN Path Policies**.

If the SAN Path Policies tab is already displayed, you can use it to display the SAN Path Policies view.

2. In the **SAN Path Policies** view, select the policy row(s) for the policy definition you need to edit.

Note: To edit a host policy, you only need to select one row for the host.

If you selected a grouped row and the nested policies differ, or you selected multiple rows for which the policies differ, OnCommand Insight reports the corresponding policy setting as mixed.

3. Right-click the highlighted policy and select **Edit Policy**.

OnCommand Insight displays the current policy settings.

4. Make the necessary changes to the displayed list of policy selections.

5. Click **OK**.

The new policy settings apply immediately.

Disabling global path policies

To make a global path policy inactive, but keep it available in your environment, remove the automatic authorization from the policy description.

Before you begin

To examine the path policies used in your environment, click the **SAN Path Policies** tab and identify which global path policy to disable.

Steps

1. On the main menu, select **Tools > Settings**.
2. In the **Settings** window, expand the Policies tree and select **FC Global Policy** or **iSCSI Global Policy**.
3. Select the tab for the global policy type (for example, Volume Capacity Exceptions).

Note: Remember that the global storage policy controls the majority of your network paths and generally should not be disabled except in special circumstances.
4. Clear the **Automatically authorize...** check box in the policy definition window.
5. Click **OK**.

Any paths that were authorized using the disabled policy are re-evaluated, using the next level of policy in effect for those paths.

If no policy is specified for a given path, it is classified as an Unauthorized Path in the SAN Path Violations view.

Removing SAN path policies

If you no longer need a SAN path policy for one or more storage elements or you want to reduce the number of path policies, you can remove unnecessary path policies easily. However, you cannot delete the global path policies.

Steps

1. To display the policies in your environment, click the OnCommand Insight **Open** menu and select **Assurance > SAN Path Policies**.
2. Select one or more policies on specific storage elements that you want to delete.
3. Right-click and select **Remove Policy**.
4. Examine the description of the policy displayed, and click **Yes** to complete the operation.

If you selected more than one policy, OnCommand Insight displays a separate confirmation for each policy. Click **Yes to All** if you do not want to review the individual confirmations.

Policies reference

Setting policies for your environment defines the best practices you follow and establishes the environment thresholds used to alert administrators of potential problems.

OnCommand Insight supplies some global policies as a starting point for defining your environment. You can modify and add policies at the global, host, and path levels.

Modify Policy wizard - first page

You use the Modify Policy wizard to change the policies governing specific items you select in different OnCommand Insight views.

Navigation

To display the Modify Policy wizard, use any of these methods:

- Click the OnCommand Insight Open menu, and then select **Inventory** and the **Datastores**, **Hosts**, **Storage Arrays**, or **Tapes** views.
Select one or more items in the list. Right-click and select the **Modify Policy** option.
- Click the OnCommand Insight Open menu and select **Assurance** and the **Policies**, **Storage Pool Utilization Violations**, or **Port Balance Violations** view, or the Violations Browser.
Select one or more items in the list. Right-click and select the **Modify Policy** option.

Description

If there is more than one policy type represented by the selection in the view, the first page of the wizard lists all of the types so that you can select the policy type you want to change. If there is only one policy type, the second page opens for you to select the change option.

On the confirmation (final) page, you can select **Modify another policy on the same selections** to return to the first page of the wizard and select a different policy type than you did before.

Modify Policy wizard - select option page

The second page of the wizard lists the current policy in effect for the selected item. You use this page to select the type of policy modification you want to perform. This page opens first if there is only one policy type associated with the selected item in the view.

Navigation

Select the policy type you want to examine and possibly change. Click **Next**. The second page of the wizard displays the current policy for the selected item in the view and lists the possible changes you can make to the policy. Select one of the options and click **Next**.

Note: If you selected more than one item in the view, you might be modifying different policies, and the wizard shows that condition by listing the **Current policy** as "Mixed."

Modify Policy wizard - settings page

The third page of the Modify Policy wizard allows you to select the specific settings you want to change for the selected policy. For example, you might select a new threshold for a violation type.

If the setting choices on this page do not give you the options you expected, return to the previous page or pages to make new selections.

Click **Next** to go to the confirmation page of the wizard.

Modify Policy wizard - confirmation page

This page shows the current policy and the proposed changes for you to confirm before saving them. All policy changes are recorded in the Audit log.

On the final confirmation page, you might select **Modify another policy on the same selections** to return to the first page of the wizard and select a different policy type than you did the first time.

Policies view

The Policies view lists the global policies controlling the general violations. You can group the policies and customize the table to focus on items of interest. You might want to select a policy type, shown in red, and click the Violations List icon to display all of the elements affected by a policy violation. You can also modify a selected policy from this view.

Navigation

From the Open menu, select **Assurance > Policies**.

Column descriptions

blank

Applicable with any presentation order other than No Grouping. This column lists the organized data according to the selected grouping format:

- Policy Type
- Target
- Owner

The number in parentheses indicates the number of (grouped) policies reported in each row.

Policy Type

Type of general violation controlled by the policy such as Maximum Datastore Latency or Storage Pool Capacity Assurance.

Policy Level

Type of general policy as a Global or Host.



(Are there violations?)

Icon that indicates a general policy violation.

Target

Type of general policy as a Global or Host.

Description

Explanation of a violation.

Since

The date when the violation first occurred.

Owner

Name of the user who defined and is responsible for the policy.

SAN Path Policies view

The SAN Path Policies view lists paths with their controlling policies. Any paths that violate their policies are displayed in red. You can group the policies and customize the table to focus on items of interest.

Navigation

- From the Insight Open menu, select **Assurance > SAN Path Policies**.
- At the bottom of a view, click the **SAN Path Policies** icon.

Column descriptions

The Insight licenses control the columns that are displayed in the view.

blank

Applicable with any presentation order other than No Grouping. This column lists the organized data according to the selected grouping format:

- Storage
- Host
- Storage then Host
- Host then Storage
- End Points
- Since (by date)

The number in parentheses indicates the number of (grouped) policies reported in each row.

Technology

The SAN (FC and iSCSI) protocols that the policy supports.

Policy Type

Type of policy as a Global, Path, or Host.



(Violation)

Icon that marks the line that describes the location of the violation. A number in this column is the total violations for the selected grouping such as Storage or Host grouping.

Host

Name of the host associated with the policy.

Storage

Name of the storage device associated with the policy (applicable only for path-specific policies).

Volume

Name of the storage volume where the data resides (applicable only for path-specific policies that use disk storage).



(Registered)

Icon indicating that the host referenced by the policy is registered to the current user. To view only those policies for your registered hosts, filter by this icon.

Owner

Name of the user who defined and is responsible for the policy.

Since

Date and time the violation was first detected.

Redundancy

Required redundancy level, as defined when the policy was created.

Sharing

Level of volume sharing permitted by the host, as defined when the path was authorized.

Capacity (GB)

Usable capacity, in gigabytes.

Min Host Port Count

Minimum number of host ports that should be active for the paths (that is, the number of host ports that should have access to the storage volume or tape device). This field is "Any" if no redundancy is required (Redundancy field is None).

Min Storage Port Count

Minimum number of storage ports that can be set per path.

Max Hops

Maximum number of switch hops specified by the policy, between the host and its storage. This field is "Any" if the policy does not specify a maximum number of hops.

Require Security

Inbound and outbound connections between the initiator and target require CHAP security or not.

Min Sessions

Minimum number of sessions required.

Min Connections

Minimum number of connections required.

Settings for FC global policies

The Fibre Channel global path policies have these settings and tabs.

Navigation

Select **Policy > FC Global Policy**.

Settings and tabs

To establish the global Storage policies, be certain to check the "automatically authorize" option to implement the changes and then select the appropriate settings for your environment. Click these additional tabs to set special criteria for your FC global policies:

- Volume Type Exceptions
- Volume Capacity Exceptions
- Tape
- Storage
- Backend Path

Settings	Options and Definitions
Redundancy level	<ul style="list-style-type: none"> • None - No redundancy is required on the path • No SPF - If you select this No Single Point of Failure option, the policy requires at least two paths between the host and its storage device, and OnCommand Insight verifies that each path travels through unique devices. In other words, all SAN devices traversed by a given path must be redundant. If two paths use the same switch, the switch is a possible point of failure for both paths and would be marked as a violation. • Redundant - The policy requires the host to reach the storage device through at least two different fabrics.

Settings	Options and Definitions
Sharing	<p>Level of volume sharing permitted by the host, as follows:</p> <ul style="list-style-type: none"> • Any - Any host can share the storage volume with the host assigned to this policy. • No Sharing - All access to the volume must originate from the host device on the path. If another host accesses the same volume, the host assigned to this policy will be in violation of its policy. • Application - Hosts that share at least one application with this host can share the same volume, but other hosts cannot. If a host accesses the same volume but does not share at least one application, the host assigned to this policy is in violation of its policy. <p>You can ignore the application-sharing setting for the policy on an application-by-application basis.</p>
Min virtualizer ports	Minimum number of virtualizer ports that should be active for the path.
Min backend storage ports	Minimum number of backend storage ports that can be set per path.
Min host port count	Minimum number of host ports that should be active (that is, have access to the storage volume or tape device) for the path.
Min storage port count	Minimum number of storage ports that can be set per path.
Maximum switch hops	Maximum number of switch hops on the shortest path between the host and its storage data on the path.

Settings for Global Policies

You can change the threshold values for the global general policies that determine what the policies monitor, and manage the functioning of your environment with respect to array performance and thin provisioning.

Navigation

From OnCommand Insight Client Main Menu, select **Tools > Settings**. In the settings tree, click **Global Policies**.

Description

The threshold values can be changed for these global policies to meet the requirements of your environment. The types of policies are grouped to indicate what the policies monitor and manage, such as array performance and blocked devices. The High Fan-Out and Virtual Machine Performance policies have only one threshold value to set.

Blocked Devices

- Detect blocked generic devices
- Detect blocked hosts

High Fan-Out

- Maximum fan-out

Switch Performance

- Maximum host port balance index
- Maximum storage port balance index
- Maximum tape port balance index

Thin Provisioning

- Maximum storage pool commit ratio
- Maximum storage pool used capacity
- Storage pool capacity assurance threshold

Settings for iSCSI global policies

When you are defining iSCSI global path policies, use these settings.

Navigation

From the Client Main Menu, select **Policy > iSCSI Global Policy**.

Settings and tabs

To establish the global Storage policies, be certain to check the "automatically authorize" option to implement the changes and then select the appropriate settings for your environment. Click these additional tabs to set special criteria for your iSCSI global policies:

- Storage
- Volume Type Exceptions
- Volume Capacity Exceptions

Settings	Options and Definitions
Require Security (iSCSI)	Yes or No
Sharing	<p>Level of volume sharing permitted by the host is defined by one of these options:</p> <ul style="list-style-type: none"> • Any - any host can share the storage volume with the host assigned to this policy. • No Sharing - All access to the volume must originate from the host device for the path. If another host accesses the same volume, the host assigned to this policy is in violation of its policy. • Application - Hosts that share at least one application with this host can share the same volume, but other hosts cannot. If a host accesses the same volume but does not share at least one application, the host assigned to this policy is in violation of its policy. <p>You can ignore the application-sharing setting for the policy on an application-by-application basis.</p>
Min Sessions	Minimum number of sessions required.
Min Connections	Minimum number of connections required.

Violation Notification settings

You can configure the general violations to send notifications to selected users.

Navigation

From OnCommand Insight Client Main Menu, select **Tools > Settings**. In the settings tree, click **Violation Notification**.

Description

You can select SNMP traps and Syslog messages for the notifications.

You might need to add SNMP or Syslog configurations to support the general violation messages.

If you want email notifications sent to specific individuals, add their email addresses to the table and select a violation severity that will trigger the emails to be sent.

Note: These features can also be configured from the Main Menu using the **SNMP/Syslog** and **Mail** options.

Violation Severity settings

When you are defining the policies for your system, you might also want to select the severity level for one or more general policy types.

Navigation

From OnCommand Insight Client Main Menu, select **Tools > OnCommand Insight Settings**. In the settings tree, click **Violation Severity**.

Description

If there is more than one similar violation type, the violation types are grouped into categories in the settings dialog box. The numbered severity level can be changed for any of these general policy violation types:

Note: Remember that these severity levels are tied to the notifications sent to users.

- Blocked Devices
 - Blocked Generic Devices
 - Blocked Hosts
- High Fan-Out
- Switch Performance
 - Host Port Balance
 - Storage Port Balance
 - Tape Port Balance
- Thin Provisioning
 - Storage Pool Capacity
 - Storage Pool Capacity Assurance
 - Storage Pool Over-Commit

Monitoring changes in your environment

View a list of physical and logical changes to devices in your environment. Insight reports on changes such as equipment additions and removals, zoning and masking changes, cabling reconfigurations, and outages. If you want to eliminate violations due to maintenance or other planned activities, you can clear the **Show transient violations** setting.

About this task

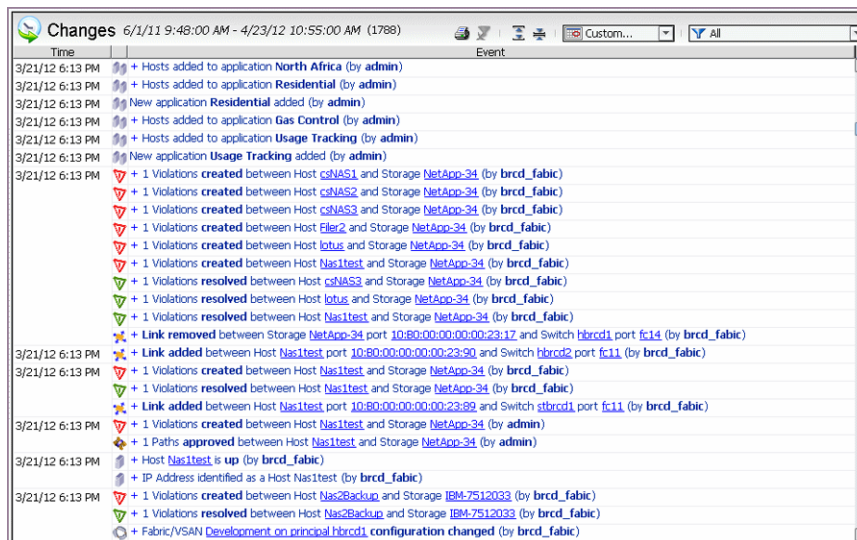
You might see violations in the Changes list, indicated with a red icon.

You can perform the following tasks related to the changes:

- View environment history with the Topology and Changes views. You might want to do this to view the state of your environment at a specific time and troubleshooting a problem.
- Limit the list of changes to a particular time range.
- Filter the list of changes.
- Use the **Show transient violations** setting to adjust the number of violations displayed
- Create an HTML report of changes.

Steps

1. From the **Open** menu, select **Assurance > Changes**.



You might want to adjust the date range or grouping for this view to show only the information that is important to you. This example shows all of the changes for a customized date range. You might select the Devices grouping for this week or today.

2. Expand entries with a plus sign to display more details about the change.
3. To identify problems that might be related to changes, locate a red violation icon in front of a described change.

Check to be certain the violation has not been resolved. You can find this information by matching the violation description with a "resolved" description below in the list.

4. If the violation has not been resolved, click the links in the violation message to display additional information.

Types of changes you can monitor in your environment

You can view physical and logical modifications to devices in your environment, including equipment additions and removals, zoning and masking changes, cabling reconfigurations, and system outages.

Insight shows the following types of changes:

System element	Change type
Device	Additions and attribute, configuration, and resolution changes
Port	Connected or disconnected state
Zone	Zone state, zone routing, and zone member
Fabric/VSAN	Switch joined or left fabric changes and fabric configuration changes
Path	State
Violations	State of the violations with their location identification
Application	Applications, hosts, iSCSI path policies, and iSCSI host policies
Volume	Volume maps and masking
Backend LUN	Backend LUNs
Host	State, policies, and authorizations
Virtualization	VM states, data store, violation, and policy changes
Qtree	Qtree status, security style, and oplocks
Switch	State
Links	Added and removed between system elements such as hosts, ports, switches, and storage
IP Address	Identification of the IP address of a host specified in a change description
Storage	State of the storage array including shares, storage pools, qtrees, and volume masking

Filtering the list of changes

You can concentrate on a particular type of change. You can filter the list of changes by path-related changes, device-related changes, or device-related start-up and shut-down events. You can also filter by data in any column in the Changes view.

Steps

1. From the OnCommand Insight **Open** menu, click the Changes icon.
This opens the Changes main view. Or, display an inventory main view and click the Changes icon to display the Changes detail view.
2. To the right of the Changes filter drop-down option, click the arrow and choose from one of the following:

Option	Description
All	All changes
Paths, Policies, and Violations	This filter includes the following types of changes: path up/down, violation up/down, and policy added/removed/changed.
Devices	Events related only to devices.
Device up/down	Events related to devices starting up or shutting down.
Host Virtualization	This filter includes the following types of changes related to a virtual server: VM up/down, VM property changed, VM moved to different host, datastore added/removed/changed, virtual disk added to/removed from VM, ESX excluded from/included in policy, VM violation up/down, ESX property changed, VM LUN policy changed. It also includes the following host-related change types: device up/down, device created, device property changed, device configuration changed, host added to application, and host removed from application.

3. To filter by column data, click on the column header, enter filter criteria, and press Enter.

Troubleshooting with topology and change history

To simplify troubleshooting and correction, you can use the Topology and Changes views to examine the state of your environment on a previous date and step through each action thereafter.

Steps

1. From the OnCommand Insight **Open** menu, select any of these Inventory views: Hosts, Virtual Machines, Datastores, Paths, Zones, and Generic Devices.
2. In the selected Inventory view, select an item of interest and click the **Topology** icon to show the **Topology** view.
3. Click the **Changes** icon below the Topology view.
4. In the **Changes** detail view, expand all of the entries to show all details and note when any change was made. Step your way through the list of changes, watching the topology change.

Example

In this example, the Virtual Machine view indicates in the State column that there are VMs that are not running. For the selected VM, the topology shows the VM with a violation and displays information about changes that might have caused the problem in the Changes detail view.

The screenshot displays the OnCommand Insight interface. At the top, the 'Virtual Machines' view shows a table with columns: Name, DNS Name, IP, Host Names, Host IPs, V-Cluster, VM Capacity (GB), VM Provisioned Capacity, VM Used Capacity (GB), OS, VM Memory (MB), Processors, State, and Datastore. Several VMs are listed, including 'QA-VM-6' and 'vm-18', with their respective states and datastores.

Below the table, the 'Topology' view is shown, displaying a diagram of the VM's connectivity. The diagram includes a legend with icons for Connectivity, Modified / Rapped, Path, Path Violation, and Zoned. The topology shows a path from the VM to a host (QA-ESX2), then to a storage (NFS), and finally to a network (NTAP-Perform).

At the bottom, the 'Changes' view is displayed, showing a list of events. The events include 'Hosts added to application Glass Collection Centers (by admin)' and 'Host QA-ESX2 added to application Glass Collection Centers'. The changes are filtered by 'Custom...' and 'Devices'.

Creating an HTML report of changes

You can generate a Web-based report of changes. If you filtered the list of changes by time or content, the report includes only the changes that show currently. Use your browser options to display or print the report.

Steps

1. From the OnCommand Insight **Open** menu, click the Changes icon.

This opens the Changes main view. Or, display an inventory main view and click the Changes icon to display the Changes detail view.

2. From the Changes view, click the printer icon.

Monitoring changes reference

When you monitor changes, you use the Changes views.

Changes main view

Use this view to see physical and logical modifications to devices in your environment, including equipment additions and removals, zoning and masking changes, cabling reconfigurations, and system outages. Using the Changes main view and the Topology view, you can select a time frame and view the topology and the changes for a previous time. This helps you view the state of your environment at different times.

From this view, you can see changes to both SAN and NAS configurations.

Navigation

You can view changes in any of the following ways:

- From the Open menu, select **Assurance > Changes**.
- From the navigation pane, select **Assurance > Changes**.
- With the Changes detail view open, click on a device or path in the Topology view. A list of changes that relate to the currently selected device or path appears.
- With the Changes detail view open, from the Hosts, Paths, or Storage Arrays main view, select a host, path, or storage array. A list of changes that relate to the currently selected device or path appears.

You can view changes in a main view, which shows all the changes to your entire environment. You can also select a host or storage array and view changes to the selected device in a detail view.

Time	Event
3/21/12 6:13 PM	+ Hosts added to application North Africa (by admin)
3/21/12 6:13 PM	+ Hosts added to application Residential (by admin)
3/21/12 6:13 PM	New application Residential added (by admin)
3/21/12 6:13 PM	+ Hosts added to application Gas Control (by admin)
3/21/12 6:13 PM	+ Hosts added to application Usage Tracking (by admin)
3/21/12 6:13 PM	New application Usage Tracking added (by admin)
3/21/12 6:13 PM	+ 1 Violations created between Host csNAS1 and Storage NetApp-34 (by brcd_fabric)
3/21/12 6:13 PM	+ 1 Violations created between Host csNAS2 and Storage NetApp-34 (by brcd_fabric)
3/21/12 6:13 PM	+ 1 Violations created between Host csNAS3 and Storage NetApp-34 (by brcd_fabric)
3/21/12 6:13 PM	+ 1 Violations created between Host Eller2 and Storage NetApp-34 (by brcd_fabric)
3/21/12 6:13 PM	+ 1 Violations created between Host lotus and Storage NetApp-34 (by brcd_fabric)
3/21/12 6:13 PM	+ 1 Violations created between Host Nas1test and Storage NetApp-34 (by brcd_fabric)
3/21/12 6:13 PM	+ 1 Violations resolved between Host csNAS3 and Storage NetApp-34 (by brcd_fabric)
3/21/12 6:13 PM	+ 1 Violations resolved between Host lotus and Storage NetApp-34 (by brcd_fabric)
3/21/12 6:13 PM	+ 1 Violations resolved between Host Nas1test and Storage NetApp-34 (by brcd_fabric)
3/21/12 6:13 PM	+ Link removed between Storage NetApp-34 port 10:80:00:00:00:23:17 and Switch hbrcd1 port f14 (by brcd_fabric)
3/21/12 6:13 PM	+ Link added between Host Nas1test port 10:80:00:00:00:23:90 and Switch hbrcd2 port f11 (by brcd_fabric)
3/21/12 6:13 PM	+ 1 Violations created between Host Nas1test and Storage NetApp-34 (by brcd_fabric)
3/21/12 6:13 PM	+ 1 Violations resolved between Host Nas1test and Storage NetApp-34 (by brcd_fabric)
3/21/12 6:13 PM	+ Link added between Host Nas1test port 10:80:00:00:00:23:89 and Switch hbrcd1 port f11 (by brcd_fabric)
3/21/12 6:13 PM	+ 1 Violations created between Host Nas1test and Storage NetApp-34 (by admin)
3/21/12 6:13 PM	+ 1 Paths approved between Host Nas1test and Storage NetApp-34 (by admin)
3/21/12 6:13 PM	+ Host Nas1test is up (by brcd_fabric)
3/21/12 6:13 PM	+ IP Address identified as a Host Nas1test (by brcd_fabric)
3/21/12 6:13 PM	+ 1 Violations created between Host Nas2Backup and Storage IBM-7512033 (by brcd_fabric)
3/21/12 6:13 PM	+ 1 Violations resolved between Host Nas2Backup and Storage IBM-7512033 (by brcd_fabric)
3/21/12 6:13 PM	+ Fabric/VSAN Development on principal hbrcd1 configuration changed (by brcd_fabric)

Field descriptions

The number following the table title identifies the total number of changes in the list. Each row in the table represents a specific change and includes the information below.

You might see violations in the Changes list. Violation tracking is a feature provided through the Assure license.

To see details for a single device, path, or violation, click on the change in the Changes main view. At the bottom of the Insight Client window, in the icon bar, click the Properties icon.

To see details for changes that affect multiple objects, expand the change row in the main view.

Time

Date and time at which a data source reported this event. This timestamp allows Insight to recreate and display the state of your environment at any point in time.

icon

Indicates the type of event, for example, equipment additions and removals, zoning and masking changes, cabling reconfigurations, and system outages.

Event

The change action that occurred at the time indicated.




Changes that resulted from a single action are stamped with the same time and are grouped in the display. Click the + sign to display more detailed change information for events that are nested.

The information included here reports not only the change itself, but also the impact of the change on the access path.

Options

The Changes main view includes the following options:

- **HTML report:** Click the Printer icon to generate an HTML report of changes. If you have filtered the list, the HTML report includes only the changes currently listed.
- In the **Tools > Settings > General Preferences** option, clear the **Show transient violations** option to remove the violations generated by maintenance or other planned activities from the Changes main view. Check that option to include all of those violations.

- Clear filter: Click the Clear Filter icon to clear all filters set on any columns. 
- Expand rows: Click the Expand icon to expand all rows that have a + to the left. 
- Collapse rows: Click the Collapse icon to collapse all child rows under parent entries. 
- Time period: Click this to change the time frame for the list of changes. You can also enter a custom time period.
- Filter: Click the Filter drop-down list to see all changes or only a subset of the changes. You can filter the Changes list by one of the following filters:
 - All: Shows all changes.
 - Paths, Policies, and Violations: Shows only the events that are related to paths and policies and the associated violations.
 - Devices: Shows only the events that are related to device configuration.
 - Device up/down: Shows only the events that are related to devices shutting down or starting up.
 - Host Virtualization: Shows only the events related to virtual machines.

With the Topology view open, in the main Changes main view, click on any change to view the topology as of the date and time when that change occurred. Then, step your way through the Changes list, watching the topology change. For example, as devices are added, you can select them and review the detail views to ensure that they were added correctly.


From the Changes main view, right-click to show a menu. The Insight licenses control the types of information displayed in the view.

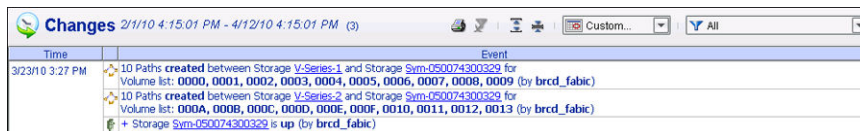
Changes detail view

Use this view to identify physical and logical modifications to a selected device in your environment, including equipment additions and removals, zoning and masking changes, cabling reconfigurations, and system outages. The Changes detail view displays a list of changes related to a selected path, switch, host, storage array, or tape device.

Navigation

You can access this detail view in one of the following ways:

- From the Insight Client menu, select **View > Detail Views > Changes**.
- At the bottom of Insight Client views, click the Changes detail view icon. 



Time	Event
3/23/10 3:27 PM	10 Paths created between Storage V-Series-1 and Storage Sym-050074300329 for Volume list: 0000, 0001, 0002, 0003, 0004, 0005, 0006, 0007, 0008, 0009 (by brcd_fabric)
	10 Paths created between Storages V-Series-2 and Storage Sym-050074300329 for Volume list: 000A, 000B, 000C, 000D, 000E, 000F, 0010, 0011, 0012, 0013 (by brcd_fabric)
	+ Storage Sym-050074300329 is up (by brcd_fabric)

Column descriptions

Insight displays the following information for each change that relates to the selected item or displays a set of changes that occurred at a specified date and time.

You can also view changes in a main view, which shows all the changes to your entire environment.

The Insight licenses control the types of information displayed in the view. For example, you might see violations in the Changes list. Violations detection is a feature provided by the Assure license.

Time

The date and time at which a data source reported this event or events. This timestamp allows Insight to recreate and display the state of your environment at any point in time.

The most current change appears at the top and the changes are in descending order by time stamp.

icon

Icon indicating the type of event.

Event

The change action that occurred at the time indicated.

Changes that resulted from a single action are stamped with the same time and are grouped in the display. Click the + sign to display more detailed change information for events that are nested.

The information included here reports not only the change itself, but also the impact of the change on the access path.

To display properties for the device in a row, click the link in the row.

Options

Open changes in a web browser

Generates an HTML report of changes that you can view in a web browser. If you have filtered the list, the report includes only the changes currently listed. To distribute or print the report, use the standard browser options.

Time Period

Changes the time frame for the list of changes. You can also enter a custom time period.

Filter

Filters the list of changes. You can filter to show only those changes related to devices being up or down or changes related to all devices. If you have other licenses installed, additional options appear.

Datastores view

You use this view to compare the capacity and performance characteristics of the ESX, storage and fabric. You can also determine which data store to choose for the next virtual machine allocation.

Navigation

You can access this view in one of the following ways.

- From the Insight Open menu, select **Inventory > Datastores**.
- From the navigation pane on the left, select **Inventory > Datastores**.
- From the OnCommand Insight Open menu, select **Inventory > Hosts**. Click the **Datastores** icon.
- From the OnCommand Insight Open menu, select **Assurance > Changes**. Click the **Datastores** icon.

Column descriptions

blank

When you group the data using the Grouping drop-down list, this column shows the grouped values. For example, if you grouped this data by storage, this column displays the storage names. The number in parentheses indicates the number of data stores in each grouped row.

Name

The name of the data store.

Virtual Center IP

The IP address of the Virtual Center host for the data store.

VM Count

The number of virtual machines whose files are contained in this data store.

Hypervisor Count

The number of ESX hosts (hypervisors) that use this data store for their virtual machines.

FC Ports

The number of FC ports on the hypervisor hosts in the physical storage paths that this data store logically represents.

Unused Capacity (GB)

The usable capacity that might be available for storing additional data on the storage pool, in gigabytes.

Capacity (GB)

Usable capacity or configured size of the data store, in gigabytes.

Provisioned Capacity (GB)

The amount of total capacity that has been set aside for potential use, based on the virtual machines using this data store. Includes space set aside for virtual machine files of all types.

Used Capacity (GB)

The used capacity of the data store, in gigabytes.

VMDKs Capacity (GB)

The VMDKs usable capacity, in gigabytes.

Over-committed Capacity

The amount of capacity that has been overcommitted from the storage pool. When thin provisioning is in use, the total size of volumes and internal volumes that are created from a storage pool can exceed the total size of the capacity committed to volumes and internal volumes versus the total capacity of the storage pool. If there is no overcommitment on the storage pool, the value is 0.

Commit Ratio

The ratio (%) of the sum of the capacity of all virtual disks allocated on a data store to the capacity of the data store. If thin provisioning is in place, the ratio can be greater than 100%.

Storage

Name of volume or internal volume.

Resource Name

The volumes or internal volumes in the path.

Resource Capacity (GB)

The total capacity, in gigabytes, of the volumes or internal volumes in the paths for this data store.

Resource Used Capacity (GB)

The total used capacity, in gigabytes, of the volumes or internal volumes, in the paths for this data store.

Resource Technology

The SAN (FC and iSCSI) or NAS (NFS and CIFS) protocols that the device supports.

Deduplication Savings

The known amount of storage savings through deduplication, a process that detects blocks with identical content and replaces subsequent identical blocks with a reference to a single copy of the block.

Storage Pools

Storage pools associated with the data store.

Options

Open in Web UI

Available only with the Perform license. Displays a corresponding web UI page for the selected resource.

Analyze

Available only with the Perform license. Allows you to investigate the performance of the selected data store. For example, you can determine contention issues, availability issues, and array performance. The Data Store Summary tab provides information that might be needed for troubleshooting.

Analyze Storage Pools

Available only with the Assure license. Allows you to select a specific storage pool and assess its status related to the thin-provisioning policies. You can use this dialog box, instead of the Violations Browser, to see the current thin provisioning violations and how close the storage pool is to reaching the policy limits.

Edit Annotations

Allows you to assign a predefined or custom category to this device so that you can later group the devices by the annotation. For example, you might want to group all devices in a specific data center or tier.

File Systems detail view

Use this view to identify the file systems in your environment. File systems make use of an underlying data storage device that offers access to an array of fixed-size blocks, for example, a local hard drive, SAN LUN, or SAN volume.

Navigation

If you have the Insight Plan license, you can access this detail view from one of the following views:

- Paths (if the link between the LUN or NAS share is discovered)
- Changes
- Hosts
- Topology (if the link between the LUN or NAS share is discovered)

Click the **File Systems** detail view icon. 

Column descriptions

The File Systems detail view displays the following, depending on what you select in the main view or Topology view.

blank

When you group the data using the Grouping drop-down list, the Grouping column shows the grouped values. For example, if you grouped the data by fabric, the Grouping column displays the fabric names. The number in parentheses indicates the number of switches in each grouped row.

Name

Displays the name of the file system.

Capacity (GB)

Displays the usable capacity of the file system, in gigabytes.

Used Capacity (GB)

The sum of all internal volumes' consumed capacity, including reserved capacity, Snapshot used capacity, Snapshot reserved capacity, and storage efficiency technology overhead. If no internal volumes are present, Capacity Used is the sum of all volumes consumed capacity, including reserved capacity, Snapshot used capacity, Snapshot reserved capacity, and storage efficiency technology overhead.

Utilization

Displays the percentage of storage space used on the file system.

Location Type

Displays the type of file system location, for example, SAN, NAS, or local.

Type

Displays the type of file system, for example, NTFS or FAT32.

Last Agent Report Time

This is the last time the data source reported to Insight.

VMDKs detail view

Use this view to monitor virtual machine disk (VMDK) performance characteristics such as IOPS, throughput, latency CPU, and memory utilization. You can also look for busy VMDKs by data store or storage.

Navigation

This detail view is available after clicking a device in one of the following views:

- Changes main view
- Hosts main view
- Paths main view
- Storage Arrays view
- Virtual Machines view

You can access this detail view in any of the following ways:

- From the Insight menu, select **View > Detail Views > Virtual Machines Disks**.
- At the bottom of the Insight view, click the VMDKs detail view icon.

Column descriptions

A row exists for each virtual disk. This differs from the VM Paths detail view, which shows one row for each volume.

The Insight licenses control the types of information displayed in the view.

blank

When you group the data using the Grouping drop-down list, this column shows the grouped values. For example, if you grouped this data by virtual machine, this column displays the virtual machine names. The number in parentheses indicates the number of virtual machines in each grouped row.

Name

The name of the virtual machine disk (VMDK file name).

Virtual Machine

The name of the virtual machine. May be blank when the row represents a SAN volume or NAS share that is being accessed from a virtual host (ESX) but does not contain virtual machine data.

Datastore

Name of the data store residing on a volume.

Capacity

Storage capacity allocated to the virtual machine disk (provided by the SDK). If you are using raw device mappings (RDMs), this is blank because the virtual machine has no knowledge of RDMs.

Used Capacity (GB)

Capacity that is allocated to virtual machines (provided by the SDK). For RDM, this is blank.

RDM

Raw device mapping. A VMware feature that exposes SCSI targets (or LUNs) directly to a virtual machine. RDMs are an alternative to using VMFS. RDMs are special files in a VMFS volume that act as a proxy for a raw device.

Host Names

Name of the host owning the virtual machine.

Storage

Storage associated with the ESX host. This column may be blank if Insight is unable to identify the storage containing the virtual machine.

Resource Name

Volume or internal volume name.

Resource Technology

Indication of whether the disk uses NFS, iSCSI, or FC technology.

Resource Capacity (GB)

Size of the virtual disk, in gigabytes. Note that each row represents a single virtual disk, as opposed to a row in the VM Paths detail view that represents an aggregate of all the virtual disks and meta data of a virtual machine stored on a single data store.

Resource Used Capacity (GB)

Used capacity of the virtual disk, in gigabytes.

Deduplication Savings

The known amount of storage savings through deduplication, a process that detects blocks with identical content and replaces subsequent identical blocks with a reference to a single copy of the block.

Right-click options

From this view, right-click on a row to show a pop-up menu containing the following options.

Analyze

Available only with the Perform license. Allows you to investigate the performance of the selected data store. For example, you can determine contention issues, availability issues, and array performance.

Virtual Machines view

You use this view to see all the virtual machines available to the host (ESX server) that Insight has detected, their allocated capacity, and all the data stores accessible by the host.

Navigation

You can access this view in any of the following ways:

- From the Insight Open menu, select **Inventory > Virtual Machines**.
- From the navigation pane on the left, select **Inventory > Virtual Machines**.
- From the Insight Open menu, select **Assurance > Changes**. Click the **Virtual Machines** icon.

Column descriptions

Each row represents a relationship between a virtual machine and a volume on the SAN or a NAS share. Each row represents a virtual machine that is available to the virtualization host (ESX server) and one of the following:

- A data store containing a portion of the virtual machine
- A SAN device to which it is mapped

The number following the table heading (in parentheses) indicates the total number of virtual machines in the list.

If other modules are installed, additional columns might appear.

Name

The name of the virtual machine.

DNS Name

The host domain name.

IP

The IP address for the virtual machine.

Host Names

Name of the ESX host owning with the virtual machine.

Host IPs

ESX host IP address.

V-Cluster

Name of a cluster of virtualization hosts that share access to the same SAN volumes or NAS share. For a standalone host, this is blank.

VM Capacity (GB)

The capacity allocated to the virtual machine on the data store. This is the sum of all virtual disks stored on the data store that are used by the virtual machine. Represents the amount of usable space for the guest operating system and applications.

VM Provisioned Capacity (GB)

The amount of capacity that a virtual machine can use from its data stores, in aggregate. This includes the basic VM capacity from its virtual disks (VMDK), but also other items, such as memory swap files, Snapshot files, configuration files, and log files.

VM Used Capacity (GB)

The amount of capacity currently used by the virtual machine from its data stores, in aggregate. This includes used disk capacity across all types of files, such as virtual disks, swap files, Snapshot files, configuration files, and log files.

OS

The guest operating system running on the ESX server.

VM Memory (GB)

Memory available for the virtual machine.

Processors

The number of processors for the virtual machine.

State

The power state of the virtual machine. For RDM, this is blank.

Datastore

The data stores accessible by the host.

Storage

Storage system associated with the ESX host, for example, virtualizer or NetApp storage.

Resource Name

The name of the volume or internal volume.

Resource Technology

The SAN (FC and iSCSI) or NAS (NFS and CIFS) protocols that the device supports.

Resource Capacity (GB)

Total capacity of the storage resource identified in the Storage Resource column.

Resource Used Capacity (GB)

Used capacity of the storage resource identified in the Storage Resource column.

Deduplication Savings

The known amount of storage savings through deduplication, a process that detects blocks with identical content and replaces subsequent identical blocks with a reference to a single copy of the block.

RDM

Raw device mapping. A VMware feature that exposes SCSI targets (or LUNs) directly to a virtual machine. RDMs are an alternative to using VMFS. RDMs are special files in a VMFS volume that act as proxies for a raw device.

Power State

Indication of the state of the storage resource as Suspended, On, or Off.

V-Policy

A green check mark indicates that the host is included in the VM Host policy. If the host is excluded, a red "X" appears.

FC Port Count

The number of licensed ports on the device.

Application

Name of applications associated with the resource.

Application Priority

The priority (high, medium, or low) assigned to the application.

Tenant, Line of Business, Business Unit, Project

Columns listing the business entity components associated with the applications.

Right-click options

From this view, right-click on a row to show a pop-up menu containing the following options. If other Insight components are installed, additional options appear.

Analyze

If the OnCommand Insight Perform license is enabled, shows the Analyze dialog box and views where you can view disk contention, view performance, and analyze congestion for the selected virtual machine.

Analyze Storage Pools

Available only with the Assure license. Allows you to select a specific storage pool and assess its status relative to the thin-provisioning policies. You can use this dialog box, instead of the Violations Browser, to see the current thin provisioning violations and how close the storage pool is to reaching the policy limits.

Set Applications

Assigns the selected host to one or more applications that you select.

Set Business Entities

Assigns the select host or hosts to a business entity (tenant, line of business, business unit, and project).

Automatically Add Applications

Automatically adds hosts to applications based on a host naming pattern.

Set/Clear Annotation

Enables you to edit or assign a predefined or custom category to this resource so that you can later group the resources by the annotation. For example, you might want to group all resources in a specific data center or tier. The Clear option removes the annotation from the resource.

Allocating capacity

You can use OnCommand Insight options and reports to allocate capacity efficiently in your environment in a pro-active manner rather than in reaction to problems.

OnCommand Insight provides these tools to assist you with capacity allocation:

- Analyze Storage Pools option identifies unused capacity and shows potential over-commitment problems.
- Storage Capacity Trend report estimates the length of time before the preset threshold will be reached.

To keep track of capacity trends while away from the office, you can schedule reports to be sent to your email address and display them on a tablet device.

Identifying unused capacity

If you want to identify unused capacity in your storage pools, you can assess the status of all of the storage pools relative to the thin provisioning policies using the Analyze Storage Pools option. It shows how close the storage pools are to reaching the thin-provisioning policy limits as well as the current thin-provisioning violations.

Before you begin

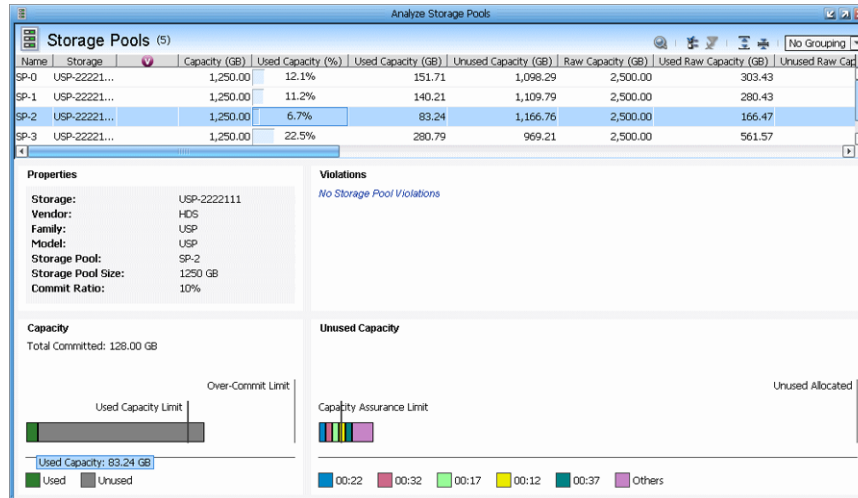
The Global Policies contain default thin-provisioning policies that you should check and change if they do not meet your needs.

Steps

1. Open a view and select a storage pool or multiple storage pools.
2. Right-click and select the **Analyze Storage Pools** option.
3. Select a storage pool of interest and review the information below. You can position the mouse pointer over the Capacity graph to display the value in pop-up text.

Example

In this example, the total committed capacity is 128 GB, but in the pop-up text, only 83.28 GB have been used. The graph shows that the used capacity has not come close to the over-commit limit. Therefore, this storage pool would be a good candidate to receive more traffic.



Result

This proactive approach allows you to make more efficient use of your resources and assists you in planning upgrades and other changes before problems occur.

Avoiding over-commitment problems

You can pro-actively review the used capacity of your storage pools to avoid over-commitment problems.

Before you begin

The Global Policies contain default thin provisioning policies that you should check and change if they do not meet your needs.

Steps

1. Open a view that includes storage pools and select an item of interest.
2. Open the **Storage Pools** detail view for the selected item.

Example

In this example, the storage pools for the selected data store are listed, and the storage pool with a high Used Capacity is selected for analysis. You could also select an item in the main view.

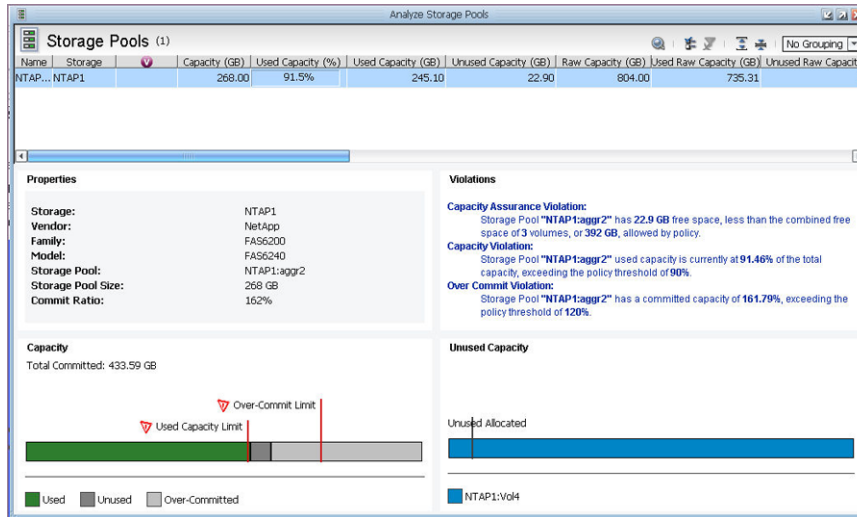
Datastores (11) Groups: 5										
	Name	Virtual Center ID	VM Count	Hypervisor Count	FC Ports	Unused Capacity (GB)	Capacity (GB)	Provisioned Capacity (GB)	Used Capacity (GB)	VM
NTAP1 (5)	1.1.1.1, 1.1.1.1...					2,441.733	7,324.828	4,882.812	4,883.095	
	DS-NtapiESK-1	1.1.1.1	8	1	0	488.47	1,465.06	976.56	976.59	
	DS-NtapiESK-2	1.1.1.2	10	1	0	488.25	1,464.86	976.56	976.61	
	DS-NtapiESK-3	1.1.1.3	18	1	0	488.35	1,464.91	976.56	976.56	
	DS-NtapiESK-4	1.1.1.4	12	1	0	488.17	1,464.93	976.56	976.76	
	DS-NtapiESK-5	1.1.1.5	5	1	0	488.49	1,465.07	976.56	976.57	
NTAP-Perform (2)	1.1.1.10, 1.1.1.1...					39.062	195.312	390.625	156.25	
	NTAP2 (2)	1.1.1.6, 1.1.1.7				976.679	2,929.926	1,953.125	1,953.247	
Virtualizer (1)	ds-30	1.1.1.7				19.531	97.656	195.312	78.125	
Sym-Perf (1)	ds-31	1.1.1.8				19.531	97.656	195.312	78.125	

Storage Pools (3)										
Name	Storage	Capacity (GB)	Used Capacity (%)	Used Capacity (GB)	Unused Capacity (GB)	Raw Capacity (GB)	Used Raw Capacity (GB)	Unused Raw Capacity (GB)	Type	Auto Tiering
NTAP... NTAP1		8,694.74	47.8%	4,153.32	4,541.42	11,564.00	5,523.92	6,040.084	Aggregate	
NTAP... NTAP1		2,821.05	38.5%	1,084.96	1,736.09	3,752.00	1,443.00	2,309.002	Aggregate	
NTAP... NTAP1		268.00	91.5%	245.10	22.90	804.00	735.31	68.692	Aggregate	

3. Select a storage pool, right-click, and select the **Analyze Storage Pools** option.

Example

In this example, the Used Capacity Limit graph shows that the Used Capacity Limit has been reached and three violations have been generated. The violations are described on the right.



Violation management

The Insight violations indicate that elements are not conforming to the policies governing them. Changes in data related to environment elements cause Insight to re-evaluate policies.

There are two types of violations:

SAN path violations

Indicate problems related to global paths or the path for a specific host or application. You can see a list of these violations in the SAN Path Violations view.

General violations

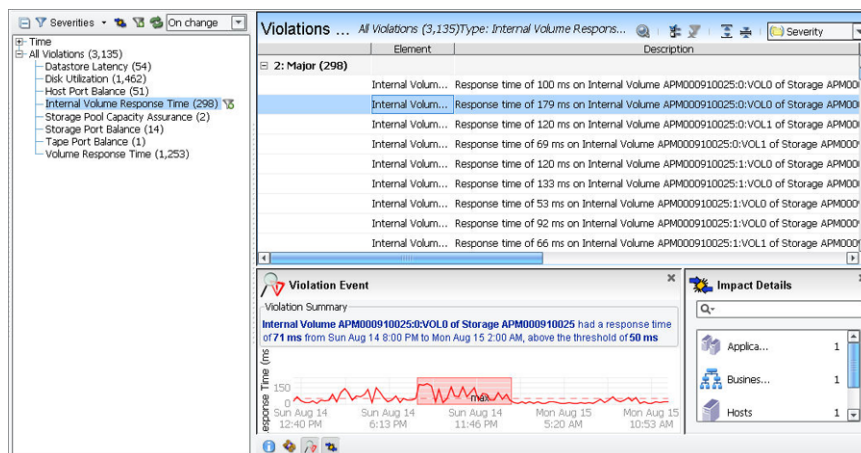
Indicate problems with other environment elements such as performance and port balancing. You can see a list of all of these violations in the [Violations Browser](#) and selected violations in these views:

- Port Balance Violations view
- Storage Pool Utilization Violations view

General violation analysis and correction

In the Java UI, you can use the Violations Browser to view all of the OnCommand Insight environment violations and identify areas that require attention based on violation count and severity. You can filter the violation severities that are shown on the tree (on the left) to focus on higher-priority problems.

The Violations Browser is the starting point for your general violations research.



You can perform the following tasks in the Violations Browser:

- Review all general violations.
- Sort violations to focus on specific criteria.
- Change the severity of violations.
- Set the browser refresh rate.
- Review system changes that might have caused a selected violation.

- Analyze selected violations.
- Identify the root cause, impact, and policy details of a violation.
- Toggle off the Impact display to improve browser display speed.
- Dismiss violations (available only on some violation types).
- Modify a policy that created a violation.

General violation types

General violations are detected and reported based on the general policies. OnCommand Insight provides default settings for all policies. You can modify the settings reported on in the policies. These general violation types are displayed in the Violations Browser, and these types are also the values used in the *violationType* field for SNMP traps.

The violation type names, below, are listed without spaces to show the precise values in the *violationType* field of the SNMP trap.

BlockedGeneric

Occurs when a generic device (sometimes called an unidentified host) cannot reach any volumes or shares.

BlockedHost

Occurs when a host cannot reach any volumes or shares.

DatastoreLatency

Occurs when the hourly average or the maximum of the data store latency is above the policy threshold value.

StoragePoolUtilization

Occurs when the hourly average of the storage pool utilization percentage is above the policy threshold.

HighFanOut

Occurs when number of masked hosts/generic devices for a storage port is above the policy threshold.

HostPortBalance

Occurs when the traffic load across the Fibre Channel (FC) ports of a device is not evenly distributed. A violation is generated when the balance index for a host is above the threshold specified in the policy relevant for that host. The higher the balance index is, the more unevenly distributed the traffic is across the ports.

InternalVolumeIops

Occurs when IOPS for an internal volume is above the policy threshold.

InternalVolumeResponseTime

Occurs when the hourly average or the maximum of the internal volume response time is above the policy threshold.

StoragePoolUsedCapacity

Occurs when the percentage of the used (not free) capacity of the storage pool is above the policy threshold.

StoragePoolCapacityAssurance

Occurs when the free capacity of the storage pool cannot satisfy the free space of X consumers. Consumers are volumes or internal volumes. OnCommand Insight sums up the unused capacity for all combinations of top consumers and determines whether the storage pool can satisfy the requirements.

StoragePoolOverCommit

Occurs when the commit ratio exceeds the specified percentage in the policy. OnCommand Insight monitors the space requirements of volumes used in each storage pool and compares them to the storage pool physical sizes.

StoragePortBalance

Occurs when the traffic on the FC ports for storage is not evenly distributed, to the point where the balance index also exceeds the policy threshold.

TapePortBalance

Occurs when the traffic on FC ports for a tape is not evenly distributed, to the point where the balance index also exceeds the policy threshold.

VolumeIops

Occurs when IOPS for a volume is above the policy threshold.

VolumeResponseTime

Occurs when the hourly average or the maximum of the volume response time is above the policy threshold.

Filtering the displayed severity levels

You can filter the severity levels of the violations displayed in the Violations Browser.

Steps

1. From the Insight **Open** menu, select **Assurance > Violations Browser**.
2. At the top of the browser tree, click **Severities** to display the list of violation severities that are currently shown in the Violations Browser.
3. Select one or more of these severity levels to remove or add they to the display:
 - Critical
 - Major
 - Average
 - Warning
 - Minor

Analyzing general violations

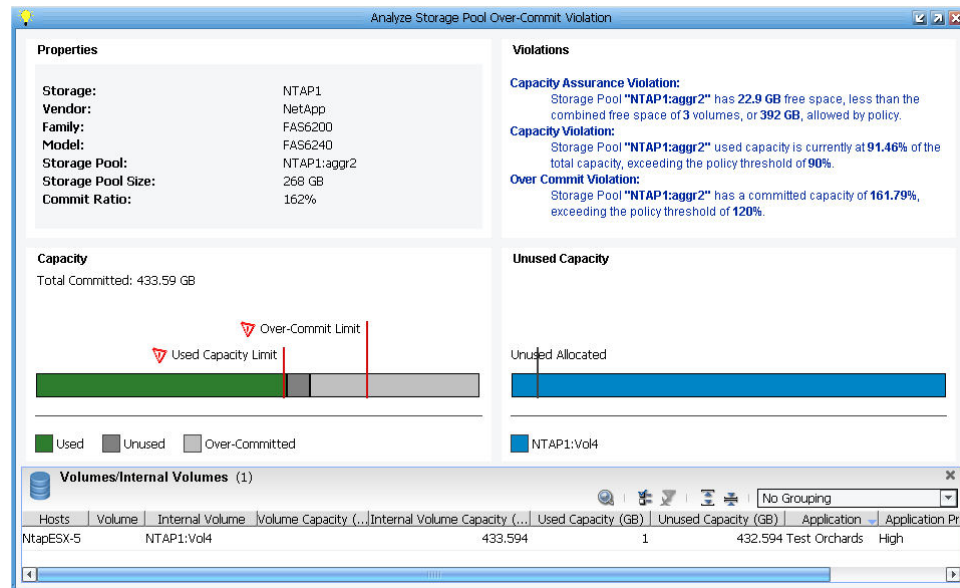
You can select individual violations in the Violations Browser and display more information about them. Each general violation type provides unique detailed information for your analysis.

Steps

1. From the Insight **Open** menu, select **Assurance > Violations Browser**.
2. Expand the browser tree branches and use filters to narrow the list of violations to the specific types of violations that you want to examine.
3. In the **Violations List**, select a specific violation.
4. Click the **Violation Event** icon and examine the overview of the problem that this view provides.
5. For more detailed analysis, right-click the violation, and select the **Analyze** option.

Depending on the type of violation, you have different analysis options.

As shown in this example, you can right-click a Storage Pool Over-commit violation and select the Analyze Violation option to display more information. Check the Volumes and Internal Volumes information at the bottom of the view.



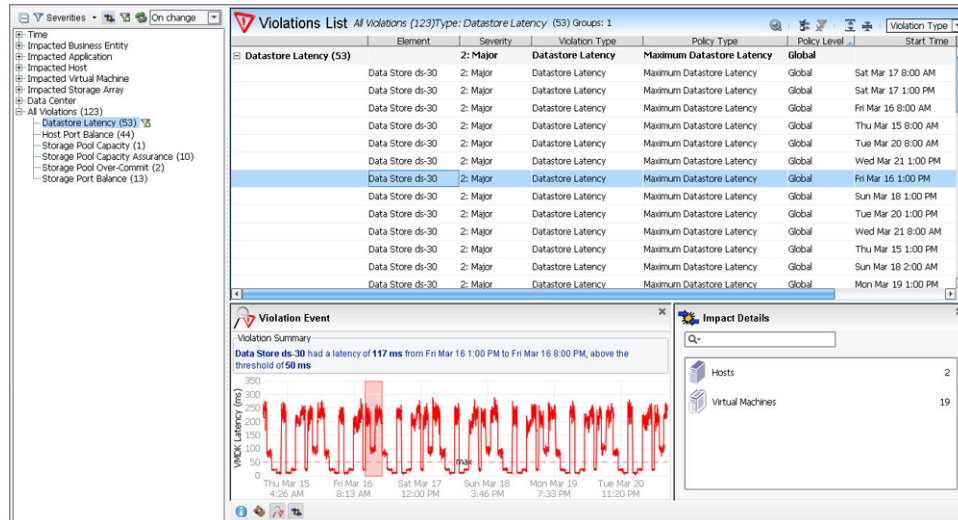
6. After investigating a violation, correct the condition causing the violation in your environment or adjust the policy that generates the violation.

Analyzing data store latency violations

If busy application traffic is causing latency problems, you can check the data store latency violations in the Violations Browser or begin with the Datastore Performance view and locate VMDK latency. From both starting points, you can right-click and select the Analyze option. On the Data Store Summary tab, you can select individual volumes and explore details for that volume or look at the environment including that volume to pinpoint the source of the problem.

Steps

1. From the OnCommand Insight **Open** menu, select **Assurance > Violations Browser**.
2. In the browser tree list of **All Violations**, select **Datastore Latency**.

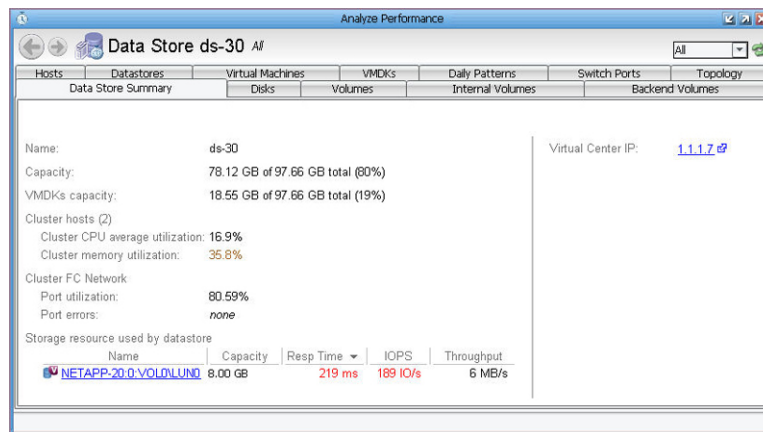


3. In the **Violation Event** chart, check to see if the latency is a problem over time or simply a brief event.

In this example, latency is consistently more than double the 50 ms threshold.

4. Select a location of interest in the **Violation Event** chart, right-click, and select **Analyze**. The Data Store Summary tab lists important information for this research.

In this example, the Cluster memory utilization and Response Time for a Storage resource (shown in red) need to be examined.



5. To see the detailed information for the storage resource involved the latency problem, click the linked **Name** in the table.
6. To check the virtual machine performance, click the **VMDKs** tab.

In this example, the problematic latency times are shown in red in the Latency and Top Latency columns :

VMKD Performance (19)

Host Name	Resource Name	Resource Capacity (GB)	IOPS 0	IOPS 1	IOPS 2	IOPS 3	Throughput 0	Throughput 1	Throughput 2	Throughput 3	Latency 0	Latency 1	Latency 2	Latency 3
esx2	NETAPP-20.0.VOLUME1	8.00	69 80	12 10	80 83	188 10	2.00	1.00	3.00	1.00	75 ms	33 ms	109 ms	218 ms
esx2	NETAPP-20.0.VOLUME1	8.00	69 80	12 10	81 80	188 10	2.00	1.00	3.00	1.00	91 ms	18 ms	109 ms	210 ms
esx1	NETAPP-20.0.VOLUME1	8.00	68 80	12 10	79 80	184 10	2.00	1.00	4.00	1.00	91 ms	19 ms	111 ms	206 ms
esx2	NETAPP-20.0.VOLUME1	8.00	67 80	11 10	78 80	186 10	2.00	1.00	3.00	1.00	89 ms	26 ms	116 ms	221 ms
esx2	NETAPP-20.0.VOLUME1	8.00	71 80	12 10	83 80	187 10	2.00	1.00	3.00	1.00	93 ms	23 ms	116 ms	244 ms
esx1	NETAPP-20.0.VOLUME1	8.00	66 80	11 10	77 80	177 10	2.00	1.00	3.00	1.00	92 ms	23 ms	116 ms	206 ms
esx2	NETAPP-20.0.VOLUME1	8.00	67 80	11 10	78 80	175 10	2.00	1.00	3.00	1.00	95 ms	22 ms	117 ms	205 ms
esx1	NETAPP-20.0.VOLUME1	8.00	67 80	11 10	78 80	176 10	2.00	1.00	3.00	1.00	93 ms	24 ms	117 ms	204 ms
esx1	NETAPP-20.0.VOLUME1	8.00	71 80	12 10	83 80	176 10	2.00	1.00	4.00	1.00	100 ms	23 ms	123 ms	225 ms
esx1	NETAPP-20.0.VOLUME1	8.00	70 80	12 10	82 80	189 10	2.00	1.00	3.00	1.00	105 ms	21 ms	126 ms	195 ms
esx1	NETAPP-20.0.VOLUME1	8.00	66 80	11 10	78 80	184 10	2.00	1.00	3.00	1.00	103 ms	19 ms	127 ms	204 ms
esx1	NETAPP-20.0.VOLUME1	8.00	70 80	12 10	82 80	184 10	2.00	1.00	3.00	1.00	105 ms	24 ms	127 ms	204 ms
esx1	NETAPP-20.0.VOLUME1	8.00	73 80	12 10	86 80	184 10	2.00	1.00	4.00	1.00	116 ms	22 ms	136 ms	205 ms
esx1	NETAPP-20.0.VOLUME1	8.00	68 80	11 10	79 80	183 10	2.00	1.00	3.00	1.00	116 ms	22 ms	139 ms	204 ms
esx1	NETAPP-20.0.VOLUME1	8.00	70 80	12 10	83 80	188 10	2.00	1.00	3.00	1.00	113 ms	26 ms	139 ms	244 ms
esx1	NETAPP-20.0.VOLUME1	8.00	67 80	11 10	78 80	189 10	2.00	1.00	3.00	1.00	120 ms	19 ms	139 ms	209 ms
esx1	NETAPP-20.0.VOLUME1	8.00	73 80	12 10	85 80	188 10	2.00	1.00	4.00	1.00	118 ms	24 ms	143 ms	240 ms

No selectors in VMDK Performance

7. You might want to select one or more items, right-click, and select **Analyze** to pinpoint the source of the problem.

Analyzing host port balance violations

To identify the cause of high traffic volume on a port, you can analyze the violation details and work through the information to identify the source of the out-of-balance condition.

About this task

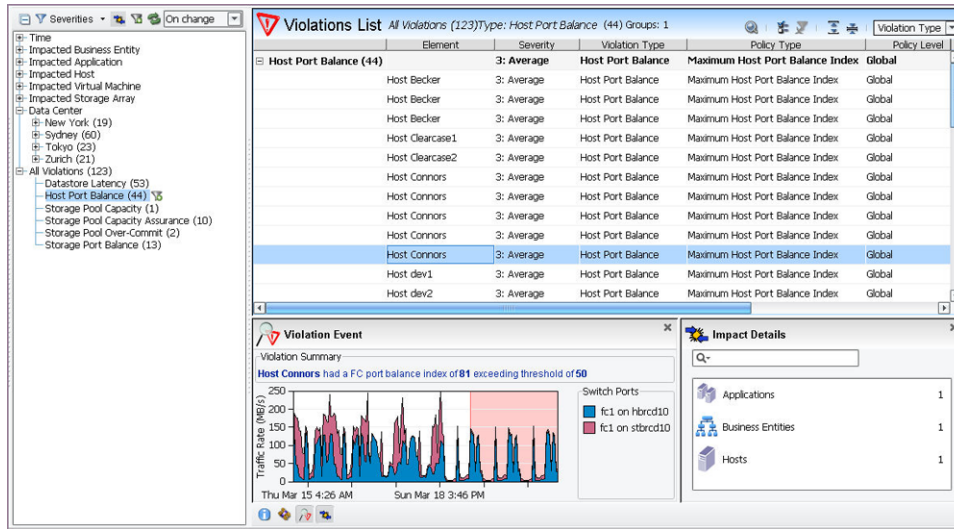
The host port balance violations are also listed in the Port Balance Violations view along with the storage port balance and tape port balance violations.

Steps

1. From the **Open** menu, select **Assurance > Violations Browser**.
2. In the browser tree, expand the **All Violations** branch of the tree and select **Host Port Balance**.
3. In the Violations List, expand the list and select a host port balance violation you want to examine in more detail.
4. If they are not already selected, click the **Violation Event** and **Impact Details** icons to display additional information about the selected violation.

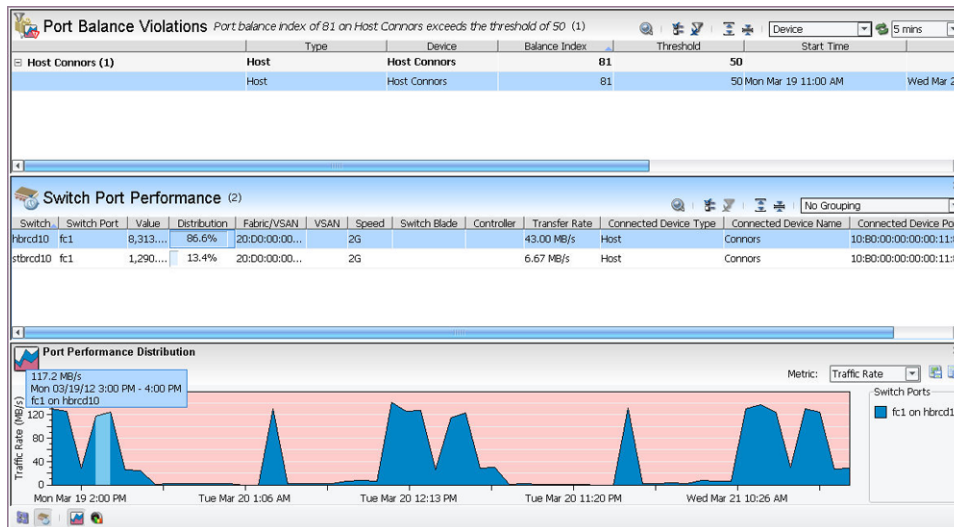
Example

In this example, the Violation Summary shows a higher traffic volume (81) than the maximum threshold set in the policy (50). The Violation Event chart also highlights, in a shaded pink area, when the violation occurred. The problem affects one host, as shown in the Impact Details view.



- Right-click the violation in the Violation List and select the **Analyze Violation** option.
- In the **Port Balance Violations** view, select an item of interest.
- Click the **Switch Port Performance** and **Port Performance Distribution** icons to display additional data relating to the violation.
- Position the mouse pointer over items in the Port Performance Distribution chart to display the time stamp and port identification, as shown in this example:

Example



- After determining the source of the problem, correct the condition causing the violation in your environment or adjust the policy that generates the violation message.

Analyzing storage port balance violations

To address storage port balance violations, you can use the analysis tools to pinpoint the cause of the out-of-balance condition.

About this task

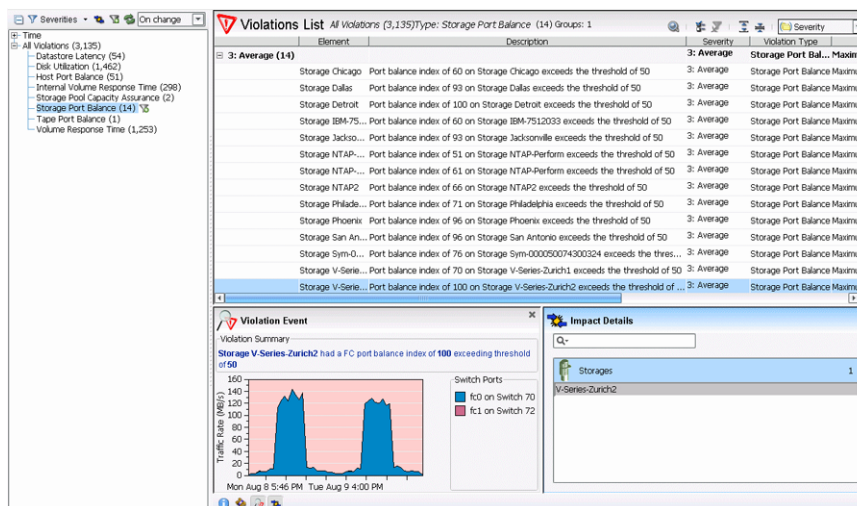
The storage port balance violations are also listed in the Port Balance Violations view along with the host port balance and tape port balance violations.

Steps

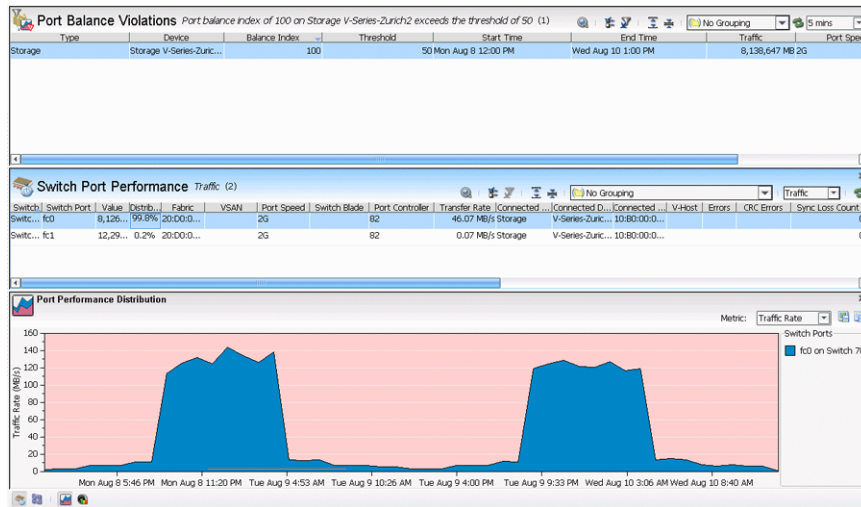
1. From the **Open** menu, select **Assurance > Violations Browser**.
2. Expand the **All Violations** branch on the tree, and select **Storage Port Balance**.
3. In the Violations List, expand the list and select a violation you want to examine in more detail.

Example

In this example, two switch ports are shown in the event chart.



4. Right-click the violation in the list and select the **Analyze Violation** option.
5. In the **Switch Port Performance** view, select the switch of interest and the **Port Performance Distribution** chart shows when the traffic rate was unusually high on the selected switch, as in this example.



6. After determining the source of the problem, correct the condition causing the violation in your environment or adjust the policy that generates the violation.

Analyzing storage pool capacity violations

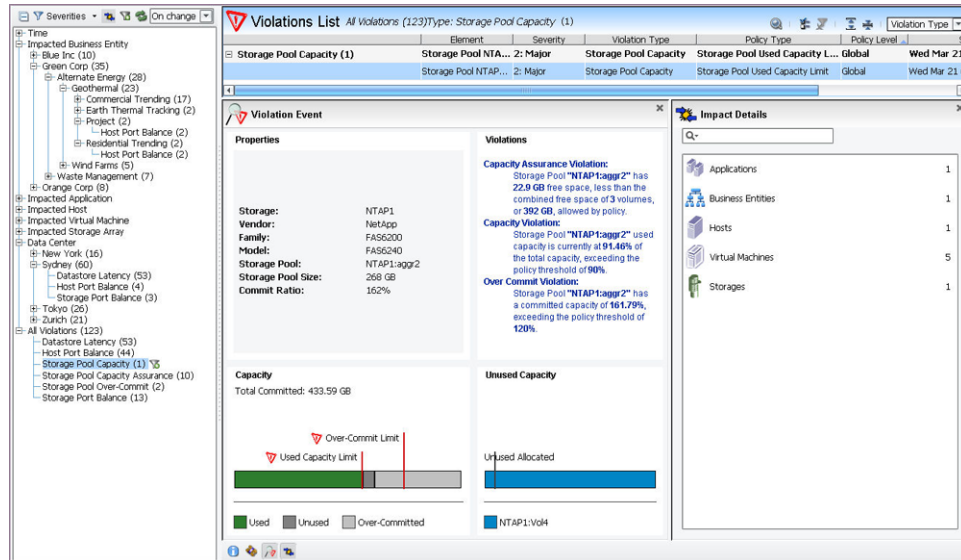
You can gather thin-provisioning allocation information about a storage pool by checking the violation and the Violation Event details to pinpoint the source of a problem.

Steps

1. From the Insight **Open** menu, select **Assurance > Violations Browser**.
2. Expand the **All Violations** branch on the tree, and select **Storage Pool Capacity**.
3. In the **Violations List**, expand the list and select a violation you want to examine in more detail.
4. Examine the information in the **Violation Event** area to identify any changes required in the storage pool or to the policy controlling this violation.

Example

You can check the Used Capacity and Unused Allocated bar graphs and the Violations descriptions to be certain that the storage pool has sufficient disk space even if the specified number of volumes becomes full.



Analyzing storage pool utilization violations

When you analyze a storage pool utilization violation, you can see when the problem occurred, what system elements were impacted, and what generated abnormally high utilization.

Steps

1. From **Open** menu, select **Assurance > Storage Pool Utilization Violations**.
2. Select violations of interest and click the detail view icons to display information about the selected violations.
3. To examine more information for a violation, right-click and select the **Analyze** option.
4. In the **Storage Pool Summary** tab, note any error messages or data listed in red and check these fields for indications of potential problems:
 - Used capacity
 - Top utilization
 - Top response time
 - Top IOPS
5. In the **Resources provisioned from storage pool** table, check this information:
 - Number of resources listed in the table in parentheses after the table title
 - Provisioned capacity percentage
6. Click the link for any resource in the table that has a high **Used Capacity** and examine the details for that resource.
7. Correct the condition causing the violation in your environment or adjust the policy to prevent the violation message from being generated.

Dismissing violations

Violations caused by transitory events, such as spikes in performance, can be dismissed using this procedure. However, other violations cannot be dismissed and must be addressed by either fixing the issue or modifying the policy.

Steps

1. Select **Assurance > Violations Browser**.
2. Expand the list of violations and group the violations as needed.
3. Select one or more violations in the **Violations List**.
4. Right-click and select **Dismiss Violations**.
5. In the confirmation dialog box, click **Yes** to complete the operation.

Result

Dismissing a violation removes it from the Violations Browser display and cannot be reversed .

SAN path violations analysis and correction

You can view a list of all open SAN path violations and filter the list to see the violations related to a specific host or application priority. Path violations that have been corrected do not appear in the list of violations; however, you can view them using the Changes main view.

When you identify a SAN path violation, you can use the Topology and Changes view to isolate the cause of the violation.

Investigating SAN path violations

You can view a list of all open SAN path violations. You can filter the list to see SAN path violations related to a specific host or application priority. Path violations that have been corrected do not appear in the list of violations; however, you can view them using the Changes main view.

About this task



For Unauthorized Sharing violations, any additional hosts having access to the target volume (and that violate the policy) are also displayed.

Steps

1. From the OnCommand Insight **Open** menu, select **Assurance > SAN Path Violations**.

All open SAN path violations appear.

Policy Type	Violation Type	Host	V-Host	V-Cluster	Storage	Storage Alias	Storage Pool	Volume	Capacity (GB)	Active SP	LUFS	Event	DataSource
Path Outage (40)	Path Outage								435.01				
Missing Redundancy (207)	Global Bac...	Missing Red...		Cluster 2					2,172.03	0			
Missing Virtual Cluster Paths (1)	Host Virt...	Missing Vert...	esx2	Cluster 1	Virtual...				8.00				Data... brocd_fabric
Single Point of Failure (3)	Path	Single Point ...							24.00				Data... brocd_fabric
	Path	Single Point o...	csN...		NetApp...		vol	NETAP...	8.00				Data... brocd_fabric
	Path	Single Point o...	csN...		NetApp...		vol	NETAP...	8.00				Data... brocd_fabric
	Path	Single Point o...	Nat...		IBM-75...		SP-1	0126	8.00				Data... brocd_fabric
Switch Hop Count (1)	Path	Switch Hop ...	filer2		NetApp...		vol	NETAP...	8.00				Data... brocd_fabric
	Path	Switch Hop C...	filer2		NetApp...		vol	NETAP...	8.00				Data... brocd_fabric
Missing Virtual Cluster NAS Share (54)	Host Virt...	Missing Vert...		Frozen ...									Appli... User - ad...
Session Count (16)	Global St...	Session Count							128.00				Polic... User - ad...
Connection Count (24)	Global St...	Connection ...							192.00				Polic... User - ad...
Unauthorized Sharing (16)	Host	Unauthoriz...							128.00				Polic... User - ad...
Missing Security (16)	Host, Path	Missing Secu...			NetApp...				128.00				Polic... User - ad...

2. To filter the list by planned or not planned violations, in the far right drop-down box, select one of the following:
 - Planned : Displays violations that correlate to a planned task that is in Implementation mode. Once a task is placed into Implementation mode, OnCommand Insight correlates that task to any outstanding violations.
 - Not planned: Displays violations that are based on existing paths and their policies.
 - All: Displays both planned and unplanned violations.
3. To see only those violations related to hosts that are registered to your logged-in user ID, click the Registered  column.
4. To sort the path violations by priority impact, click the App Priority (application priority) column.

Reviewing paths related to a violation

You can review the paths related to a violation in a graphical topology map. Paths appear in red on the map if a violation exists. For path outage violations (which have no connectivity), a line runs between the path endpoints.

Steps

1. From the Launch menu, select **Assurance > SAN Path Violations**.
2. In the **SAN Path Violations** view, select a violation.

The detail views display data related to the currently selected row in the main view.

3. Click the Topology icon at the bottom of the Insight view.

The Topology view appears in the center.



4. From the Topology view, select any device in the view and open a detail view for that device to review information that might explain the problem.

Correcting SAN path violations

After investigating violations, you have two general methods for correcting the violations: changing the SAN configuration or working with the policies.

About this task

- If the violation represents a problem in the SAN (actual or planned), change the SAN configuration to resolve the violation. OnCommand Insight clears the violation automatically after the change is made to the SAN.
- If the policy definition is missing or incorrect, either add, edit, or delete the policy, as necessary to clear the violation. To correct the path policies, you perform one or more of these operations:
 - Edit an existing path policy that is incorrect.
 - Delete an unnecessary path policy.

- Authorize a path that exists physically, but does not yet have a policy.
- Add a policy for a path that does not yet exist by specifying a host or global policy.

SAN path violation types and suggested solutions

OnCommand Insight detects several types of SAN path violations. Each violation type might require a different solution to resolve.

This table defines the path violations. Review these violations and any potential risks and suggested solutions.

Violation	Description
Connection Count (iSCSI)	<p>The number of connections used for the path is less than the minimum required by the policy.</p> <ul style="list-style-type: none"> • Solution: Increase the number of connections used for the path, or if the path does not need as many connections, change the policy.
FC Switch Hop Count	<p>A path exists (or is planned) between a server and a specific volume, but there are too many switch hops in the path.</p> <ul style="list-style-type: none"> • Risk: Path performance is compromised. • Solution: If the path can operate with more switch hops, edit the policy to reflect this.
Inconsistent LUNs	<p>A volume that is mapped to ESX hosts is using different LUNs. When analyzing this violation, determine the following:</p> <ul style="list-style-type: none"> • Locate all of the LUNs that are mapped to the volume in question, then find the common LUN. • For each host not using the common LUN, verify that the common LUN is not mapped to another volume. If the common LUN is not mapped to another volume, then the volume should be mapped to the most common LUN.
Missing Active Host Ports (Fibre Channel)	<p>A path exists (or is planned) between a server and a specific volume, but too few host ports have access to the volume.</p> <ul style="list-style-type: none"> • Risk: Path performance is compromised. • Solution: If the path can operate with fewer host ports, edit the policy to adjust or remove the requirement for host port redundancy.
Missing Active Storage Ports (Fibre Channel)	<p>A path exists (or is planned) between a server and a specific host, but the host is mapped to too few storage ports.</p> <ul style="list-style-type: none"> • Risk: Path performance is compromised. • Solution: If the path can operate with fewer storage ports, edit the policy to adjust or remove the requirement for storage port redundancy.


Violation	Description
Missing Redundancy (Fibre Channel)	<p>A path exists (or is planned) between a server and a specific volume, but the required dual-fabric redundancy does not exist. The policy specifies that the host must reach the storage device through at least two different fabrics.</p> <ul style="list-style-type: none"> • Risk: Because the redundancy level is not met, a single failure could cause downtime. • Solution: If the path does not require redundancy, edit the policy to remove the redundancy requirement.
Missing Security (iSCSI)	A required inbound or outbound CHAP is missing for this path.
Missing Virtual Cluster	<p>A host in a cluster does not access a NAS share that is being accessed by other hosts in that cluster. When analyzing this violation, determine the following:</p> <ul style="list-style-type: none"> • Which hosts in the cluster access the NAS share and which hosts do not. • If the hosts in the cluster should be accessing this NAS share at all. • Is the host not accessing the NAS share? Unlike SAN volume access, OnCommand Insight cannot help find the reason why a host does not access a NAS share.
Path Outage (Fibre Channel and iSCSI)	<p>Path is down.</p> <ul style="list-style-type: none"> • Risk: The path is inactive and the server cannot access its data volume, which results in downtime. • Solution: If this is a path that you removed, from the Policy or right-click menu, choose Dismiss Path Outage to delete the corresponding policy.
Session Count (iSCSI)	<p>The number of sessions used for the path is less than the minimum required by the policy.</p> <ul style="list-style-type: none"> • Solution: Increase the number of sessions needed for this path or if the path does not need as many sessions, change the policy.
Single Point of Failure (Fibre Channel)	<p>A path exists (or is planned) between a server and a specific volume, but the required no-SPF redundancy does not exist. The policy specifies that all SAN devices on this path must be redundant.</p> <ul style="list-style-type: none"> • Risk: Path availability is compromised. Any device that's included in the path could present a single point of failure. • Solution: If the path does not require protection against a single point of failure, edit the policy to remove the no-SPF restriction.

Violation	Description
Unauthorized Path (Fibre Channel and iSCSI)	<p>A path exists (or is planned) between a server and a specific volume, but the path is not authorized (that is, no policy is defined for it).</p> <ul style="list-style-type: none"> • Risk: This could be the result of a SAN change that inadvertently led to the creation of an invalid path, or it might represent a potential security problem. • Solution: If the path was created unintentionally, remove its enabling configuration parameters.
Unauthorized Sharing (Fibre Channel and iSCSI)	<p>The volume accessed by more than one host results in a sharing policy violation.</p> <ul style="list-style-type: none"> • Risk: Data access violation, security breach, compliance and regulation issues, or a simple mistake that may turn into application downtime and data corruption. • Solution: If the volume should not be shared to the extent that it is currently specified in the policy, change the SAN configuration to fix this problem. This violation is ignored if a group of hosts shares the same application scope as defined in the global host or path policy or that belong to the same virtual cluster.
Virtual Volume Missing Backend Support	<p>A virtual volume does not have a backend storage volume (a path outage between a virtual volume and the backend storage).</p>

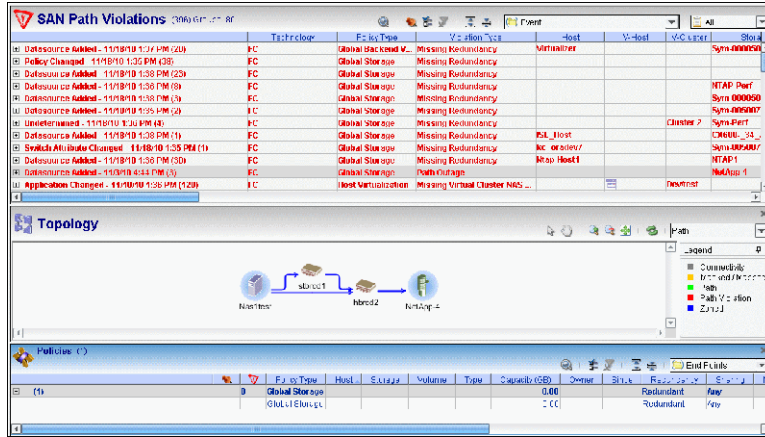
Analyzing path outage violations

You can analyze the reasons for a path outage violation by using the SAN Path Violations view, the Topology view, and the Analyze dialog box.

Steps

1. From the OnCommand Insight Open menu, select **Assurance > SAN Path Violations**.
2. In the **SAN Path Violations** view, group by event.
3. Sort by violation type so that all the Path Outage violations appear sorted within the event group.
4. Select a path violation to research.
 - a. In the bottom icon bar, click the topology icon. 
 - b. In the **Topology** view, identify paths in red.

The Topology view might show a path in red, indicating a path violation.




5. Right-click a violation and select **Analyze**.

OnCommand Insight analyzes the situation and then displays the Analyze dialog box with tabs summarizing the conditions that generated the violation.

Analyzing a missing path redundancy violation

Because OnCommand Insight audits and logs all changes, when a change occurs that affects a path service, OnCommand Insight automatically displays a violation alert. You can investigate the reasons why a missing path redundancy violation was issued.

Steps

1. From the OnCommand Insight Open menu, select **Assurance > SAN Path Violations**.
2. Sort by violation type so that all the Missing Redundancy violations appear sorted within the event group.
3. Select a violation to research.
4. Look at the topology by doing the following:
 - a. In the bottom icon bar, click the Topology icon. 
 - b. In the **Topology** view, look at the paths to determine whether a redundancy exists or is needed.

The Topology view might show that path in blue, indicating that the path is zoned, but maybe it is not masked or mapped. You might find that all applications are running; however, a failure on a good path could affect the applications.

Technology	Policy Type	Violation Type	Host	V-Host	V-Cluster	Storage	Storage Pool	Vol
FC	Path	Missing Redundancy	Agassi			Sym-00.. SP-1		00:0
FC	Path	Missing Redundancy	Becker			Sym-00.. SP-1		00:0
FC	Path	Missing Redundancy	Connors			Sym-00.. SP-1		00:0
FC	Path	Missing Redundancy	exchange_...			XP 1024.. SP-0		00:0
FC	Path	Missing Redundancy	exchange_...			XP 1024.. SP-0		00:0
FC	Path	Missing Redundancy	exchange_...			XP 1024.. SP-0		00:0
FC	Path	Missing Redundancy	exchange_...			XP 1024.. SP-1		00:0
FC	Path	Missing Redundancy	exchange_...			XP 1024.. SP-1		00:0

5. Right-click the violation and select **Analyze**.

Use the tabs to see the exact time and date of any system changes that triggered the violation. This dialog box also shows potential causes. You might see that a port was added to a zone and that there are not enough host and storage ports that are masked and mapped and share the same zone.

You might also find that all applications are running; however, a failure on a good path could affect the applications. You might conclude that path redundancy is needed and respond proactively.

Analyzing a missing path

If you do not see a path that you expect to see, use the Analyze Missing Path option to research the problem.

Steps

1. From the OnCommand Insight **Open** menu, click the **Paths** option.
Search for the path in the list of active paths.
2. If the expected path is not listed, select **Tools > Analyze Missing Path**.
3. Click the source host, the target storage device, and volume for the missing path.

4. Click **OK**.

OnCommand Insight analyzes the configuration and opens the Analyze SAN Path Violation window with the analysis summary and details.

Reviewing system changes linked to a SAN path violation

You can select a violation and look at any system changes related to it in the Violations Changes detail view. However, if you think multiple violations resulted from one event, you might want to use the Group by Event process instead.

Steps

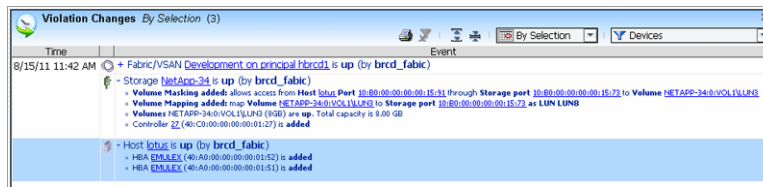
1. From the Insight **Open** menu, select **Assurance > SAN Path Violations**.

2. In the **SAN Path Violations** view, select a violation.

The detail views display data related to the currently selected row in this view.

3. Do one of the following:

- From the Insight Client, select **View > Detail views** and check the detail view or views that you want to display.
- At the bottom of the view, click the **Changes** icon.



4. From the Violations Changes detail view, select the time period.

5. Review the system changes related to the selected violation.

Clearing multiple path violations quickly

You can clear many path violations at the same time if you group them by event.


About this task

Often, a system event can cause many violations. Rather than investigating individual path violations, you can identify the system event that triggered multiple violations by grouping the violation by event. For example, if you group violations by event, you can easily see that a simple policy change (event) caused eight violations. That means if you correct that policy issue (the event), you clear all eight violations at the same time.


Grouping by event to analyze violations is particularly useful when many violations are generated from:

- Addition or removal of a data source
- Storage configuration change, for example, mapping, masking, or volume change
- Device state change
- Zoning change


Steps

1. From the OnCommand Insight **Open** menu, select **Assurance > SAN Path Violations**.
2. In the Grouping box, select **By Event**.
This is the single most important option you can set in this view.
3. Optionally, filter the list using the Planned column to display only planned or not planned violations.
4. To see only those violations related to hosts that are registered to your logged-in user ID, click the Registered  column.
5. To sort the violations by priority impact, click the Application Priority column.

Identifying violations associated with planned tasks

When a violation correlates to a planned task that is in Implementation mode, OnCommand Insight displays the Planned icon  for that violation, and identifies the planned tasks in the Tasks field. It may be useful to locate the offending tasks.

Steps

1. From the OnCommand Insight **Open** menu, select **Assurance > SAN Path Violations**.
2. In the **SAN Path Violations** view, sort the data by the Planned column.
3. Select a row with the Planned icon  in the Planned column.
4. Do one of the following:
 - Right-click and select **Go to Tasks**.
 - From the Actions menu, select **Go to Tasks**.
5. In the Plans view, review the description of the violation and the offending tasks in the Task List.
6. For each task, review the actions and errors.

Setting virtualization policy and monitoring VM violations

You can set policies that help you monitor virtualization configurations. After you set these policies, OnCommand Insight monitors your environment and issues alerts if a violation occurs on these policies. This requires the Assure license.

Violations related to VMs

After you set policies that help you monitor virtualization configurations using Settings, OnCommand Insight monitors your environment and issues alerts if a violation occurs on these policies.

The settings in the Host Virtualization Policy option in Settings can generate the following violations:

Violation	Condition	Issued for
Active path conflict	A volume in an active/passive storage array is accessed through multiple storage processors. This situation can lead to "path thrashing."	All paths to the volume being accessed.
Inconsistent LUNs	A volume is presented (mapped) to different hosts in a group using different LUNs.	All paths to the volume that are mapped using different LUNs.
Datastore Latency	When the virtual machine latency of the datastores in your environment exceeds the threshold set in the global general policies.	<p>You can set the notification policy for the violation to be generated when the latency first exceeds the threshold (peak) or when the average of an hour of samples exceeds the threshold.</p> <p>Note: This violation appears in the Violations browser while the others appear in the SAN Path Violations view.</p>
Missing virtual cluster NAS share	A host in a cluster does not access a NAS share that is being accessed by other hosts in that cluster.	
Missing virtual cluster paths	A host in a virtual cluster cannot access some volumes while another host in the group can.	For each host and for all volumes that other hosts in the group can access. Issued for each missing path.

Analyzing VM violations: Missing virtual cluster path

If OnCommand Insight issues a "Missing virtual cluster path" violation, you can research the cause. This violation means that a host in a virtual cluster cannot access volumes that another host in the cluster can.

About this task

A path does not exist for the host within the cluster, and so no path exists from the virtual machine to the volume. All hosts need access to the same storage to ensure that in the event of path outage, the virtual machine can fail over to another host in the cluster.

To analyze this violation, ask these questions:

- Which hosts in the cluster have access to the volume? Which hosts do not?
- Should the hosts in the cluster access this volume? If not, then access to the volume should be prevented from all the hosts in the cluster.
- Why does a host not have access? This is similar to analyzing a "Path Outage" violation:
 - Connectivity: Are the host and storage active and connected to the same fabric?
 - Zoning: Do the host and storage share zones? Do any of the shared zones contain connected or active ports of the host and storage?

- Volume masking and mapping: Does the storage map and mask the volume to the host use connected ports that are members of the same zone?

To prevent this violation from occurring, you should provide sufficient connectivity and configure matching zoning, mapping, and masking. This grants the host access to the volume.

Steps

1. From the Open menu, select **Assurance > SAN Path Violations**.
2. Group the data by violation type.
3. Look at the Volume column to see if the host is using different active storage to get to the selected volume.
If this is the case, you must know which VMs are affected by this violation so that you can attempt to prevent a performance degradation.
4. Look in the V-Host column.
An icon with a green triangle in the column indicates that a VM is present.
5. From the **SAN Path Violations** view, select a row showing the “Missing Virtual Cluster Paths” violation.
6. In the status bar on the bottom, click the Virtual Storage icon to show the **Virtual Storage** detail view.
This view displays all the active VM paths to the SAN volume (except the VM paths to a NAS share). If there is a path conflict, there are at least two VMs shown in the Impacted Hosts column that are accessing the same volume. Throughput immediately suffers as a result.
Note: To see violations related to VM paths to a NAS share, select the “Missing Virtual Cluster NAS Share” violation in the SAN Path Violations view.
7. From the **SAN Path Violations** view, you might also want to right-click the row and select **Analyze** to use the summary information and further isolate the issue.

Violations reference

The following views are used when viewing and analyzing violations.

Alerts view

Use the Alerts view to review alerts that indicate a performance threshold has been exceeded. The Alerts view shows the switch and port on which the alert condition occurred.

Navigation

From the OnCommand Insight Open menu, select **Assurance > Switch Port Performance Alerts**. Select an alert (in red) and click the **Alerts** icon.

Column descriptions

You can sort the data in the columns by the following:

- Switch
- [next sort]

Switch

Switch on which the alert occurred.

Port

Port on which the alert occurred.

Connected to

Name of the host, storage, or switch device to which the switch port is connected.

Start time

Date and time when the port activity first crossed the threshold. If the list is grouped, this field represents the range of dates and times for all child rows.

End Time

Date and time when the port activity returned to below the threshold. If the list is grouped, this field represents the range of dates and times for all child rows.

Value

Average actual (out-of-range) value for the period reported. If the list is grouped, this field represents the range of values for all child rows.

Minimum/maximum

Minimum or maximum threshold value at the time of the alert.

Analyze Storage Pools dialog box

The Analyze Storage Pools dialog box allows you to select a specific storage pool and assess its status relative to the thin-provisioning policies. You can use this dialog box instead of the Violations Browser to see the current thin-provisioning violations and how close the storage pool is to reaching the policy limits. This information is useful when planning changes to the environment.

Navigation

From the OnCommand Insight Open menu, select one of these views:

- **Inventory > Hosts**
- **Inventory > Virtual Machines**
- **Inventory > Storage Arrays**
- **Inventory > Datastores**
- **Inventory > Paths**
- Disks detail view
- Paths detail view
- Storage Pools detail view
- **Assurance > SAN Path Violations**
- **Performance > Application Performance**
- **Performance > Host Performance**
- **Performance > Storage Performance**

Right-click a storage pool in the view and select the **Analyze Storage Pools** option.

Column descriptions

The Analyze Storage Pools dialog box provides the following information about the selected storage pool:

blank

Column that organizes the data according to the selected grouping format. Applicable with any presentation order other than No Grouping.

Name

Name of device.

Storage

Name of the storage array.

icon (Is virtual?)

A "V" icon in this column indicates that the device is a virtualized volume.

Capacity (GB)

Size of the volume that is accessible to host applications, in gigabytes.

Used Capacity (%)

The percentage of capacity consumed in the storage pool in gigabytes.

Used Capacity (GB)

The amount of capacity holding actual data in the storage pool. Includes usage based on all file types.

Unused Capacity (GB)

The usable capacity that might be available for storing additional data on the storage pool in gigabytes.

Raw Capacity (GB)

The physical disk capacity of the storage pool, in gigabytes. Raw capacity is derived by the device manufacturer. This differs from usable capacity when technologies such as RAID-5 are used, where some of the raw capacity is used for protection purposes.

Used Raw Capacity (GB)

The amount of raw capacity in use on the storage pool, in gigabytes.

Unused Raw Capacity (GB)

The raw capacity that might be available for storing additional data on the storage pool, in gigabytes.

Type

The type of storage pool, for example, Aggregate for NetApp storage systems, RAID Group, Thin Provisioning for a thin provisioned storage pool, or Backend Group for array virtualization.

Auto Tiering

A checkmark indicates that the selected storage pool is using the automatic storage tiering technology (for example, FAST VP).

Vendor Tier

Indicates the tier as taken from the vendor's data. This is different from the tier assigned in Settings. The vendor tier usually matches the type of the disks in the storage pool, for example, SATA, FC, or EFD disk types. Vendor tier is the building block in an automated tiering policy. The vendor tier appears in the Auto Tiering Policy Constraints column in the Volumes detail view.

Uses Flash Pools

A checkmark indicates that the selected storage pool is using SSD disks as cache (for example, Flash Pool technology). In this case, the SSD disks are used for cache and do not contribute to the usable size of the storage pool.

Status

Information about whether the storage pool is online, offline, or other status.

Over-committed Capacity (GB)

The amount of capacity, in gigabytes, that has been overcommitted from the storage pool. When thin provisioning is in use, the total size of volumes that are created from a storage pool can exceed the total capacity of the storage pool. This value displays the difference between the total size of the capacity committed to volumes versus the total capacity of the storage pool. If there is no overcommitment on the storage pool, the value is 0. In an environment with internal volumes that support thin provisioning, if the committed capacity of the volumes exceeds the capacity of the internal volume, the overcommitted size will be the size of the volumes.

Commit Ratio

The ratio of the total space on the storage pool to the capacity that is allocated from it. This value can be greater than 100% when thin provisioning is in use (the pool is overcommitted).

Snapshot Reserve (GB)

The amount of usable capacity, in gigabytes, of the storage pool that is reserved for Snapshot copy data.

Snapshot Used (GB)

The amount of usable capacity, in gigabytes, of the storage pool that has been used for Snapshot copy data.

Snapshot Used (%)

The percent of usable capacity of the storage pool out of the Snapshot reserved capacity that has been used for Snapshot copies.

Redundancy

Level of mirroring defined for the device based on the storage technology, for example, RAID-DP, underlying the device. This is taken from the device itself. For an explanation of values, see the device documentation.

Disk Types

The type of physical disks (for example, Fibre Channel or ATA) on which the storage pool is based. Taken from the device itself. If there are disks with multiple disk types, speed, or size, the information appears in a comma-separated list. If a storage pool is on a virtual LUN, "vLUN" appears as the disk type, the LUN size appears as the disk size, and Disk Speed is blank.

Disk Size (GB)

Comma-separated list of the sizes of the physical disks on which the storage pool is based.

Disk Speed (RPM)

Speed of the disk as used by the volume, in revolutions per minute (RPM).

annotations

User-defined terminology associated with each volume.

Analysis panel

The Analysis panel (the lower half of the dialog box) provides this information:

- Basic properties of the storage pool including vendor, storage pool size, and commit ratio.
- Any storage pool violations.
- A capacity bar gauge indicating percent used, with vertical lines indicating the used capacity limit and over-commit limits.

- An unused capacity bar gauge displaying unused capacity broken down by volumes or internal volumes.
- Vertical lines indicating the capacity assurance limit (if less than the number of volumes) and the unused allocated capacity.

Port Balance Violations view

This view shows the balance violations for the storage ports, host ports, and tape ports together in a single view. This view helps the user to identify when devices with traffic on fibre channel ports are not balanced. The ports are not balanced when the traffic is not distributed evenly among the ports for a particular duration. In an unbalanced situation, one or more ports could be servicing much more traffic than other ports on the device.

Navigation

From the OnCommand Insight Open menu, select **Assurance > Port Balance Violations**. Select one violation of interest and right-click. Select **Analyze**.

Column descriptions

blank

Applicable with any presentation order other than No Grouping. Column that organizes the data according to the selected grouping format.

Type

The type of port balance violation for the row including Host, Storage, and Tape.

Device

Name of the device with the violation.

Balance Index

Index measurement from 0 to 100 indicating how balanced the traffic is among device ports. The lower the value, the more balanced the traffic is (0 is perfectly balanced, 100 is completely out of balance). For example, a device is out of balance if it has two ports and all of the traffic goes over one of the ports and none of the traffic goes over the other.

Threshold

The balance index threshold is set in the port balance policy applied to the device. When the balance index of the device is calculated to be above the threshold, a violation is created.

Start Time

The time when the port balance issue was detected for this violation.

End Time

The time when the port balance issue of the violation was resolved. Blank values indicate the violation is on-going.

Traffic

The amount of traffic that passed over all of the device ports during the time of the violation.

Port Speed

The speeds of the fibre channel ports on the device.

Port Count

The number of fibre channel ports on the device.

Options

The following options are available from the right-click menu:

Analyze

Available only with the Perform license. Allows you to investigate the performance of the selected resources affected by the violation. For example, you can determine contention issues, availability issues, and array performance. The Host Summary tab provides information that might be needed for troubleshooting.

Modify Policy

Changes the policies governing specific items you select in different OnCommand Insight views.

Dismiss Violations

Violations caused by transitory events, such as spikes in performance, can be dismissed using this option. However, other violations cannot be dismissed and must be addressed either by fixing the issue or by modifying the policy.

Reservation Violations view

From the Reservation Violations view, the storage administrator investigates the different reservation-related violations, identifies the problems, and makes corrections using the Planning features.

Navigation

From the OnCommand Insight Open menu, select **Assurance > Reservation Violations**.

Column descriptions

blank

Applicable with any presentation order other than No Grouping. Column that organizes the data according to the selected grouping format.

Violation

Indicates the type of violation on the reservation. It can be Error, Warning, or Info.

Type

Identifies the resource problem generating the violation of the reservation.

Details

Additional information about the resource problem.

Request

Name of the resource reservation entered on the ticket.

Request Ticket

Code identifying the request in the system.

Device Type

The system element that has caused the request violation.

Device

Description of the system element that has caused the request violation.

Since

When the violation was identified.

annotations

User-defined terminology associated with the reservation violations including Violation Severity and Note.


SAN Path Violations view

Use this view to display all open path violations. Violations that have been corrected do not appear in this view. For Unauthorized Sharing violations, any additional hosts that access the target volume and violate the policy are also displayed.

Navigation

- From the Open menu, select **Assurance > SAN Path Violations**.
- At the bottom of a view, click the **SAN Path Violations** icon.


You can limit the list as follows:

- By filtering the Registered  column, you can view only those violations related to host systems that are registered to your user ID.
- By filtering on the Application Priority field, you can sort the violations by priority impact.

Column descriptions

There is one row for each violation.

blank

Column that organizes the data according to the selected grouping format (applications, storage, and so forth). The number in parentheses indicates the number of violations reported in each (grouped) row. Applicable with any presentation order () other than No Grouping.

Technology

Indicates whether the violation relates to an FC or iSCSI path.

Policy Type

Type of policy currently enforced for the path for the Paths main table. Any given path can have several policies that apply for it, but only one policy will be in effect at a time. As necessary, open the Hosts Inventory for the path's host server, then look at the Policies detail pane for a list of all policies that currently apply for that host (but may not be enforced).

Violation Type



Type of SAN path violation.


Host

Name of the host from which the violating path originates.

V-Host

Icon indicating that the host is a virtual machine host. The icon with the green arrow indicates that a given host is currently running. The following information or icons could appear:

- Blank: Indicates a standard host.
- : Indicates that this is a virtualization host (ESX server), but it is not running.
- : Indicates that this is a virtualization host (ESX server) and it is running. At least one of the virtual machines accessing this volume from this host is running.

- : Indicates that this is a virtualization host (ESX server), but the volume is not mounted.

V-Cluster

Group of virtualization hosts sharing access to the same SAN volumes. A V-Cluster is either a VMware high availability cluster or a manually-defined group of hosts.

Storage

Name of the storage device where the data for this path resides.

Storage Alias

The user-defined name for storage.

Storage Pool

Name of the storage pool on which the volume resides.

icon (Array Virtualization Type)

Indicates virtualization type for a volume. A "V" icon indicates that the device is a *virtualized volume*, and a "B" icon indicates that the device is a *backend volume*.

Volume

Name of the volume where the data for this path resides (applicable with disk storage only).

Capacity (GB)

Size of the volume, in gigabytes.

Active SP

The name of the storage processor used by the active path from the host to the volume. There can be only one active path for a given pair of (host, volume) and thus one storage processor.

LUNs

LUNs associated with the violation. Internal volumes are carved from storage pools and exposed to hosts as shares or LUNs.

Initial Event

The first system event associated with this violation.

Data Source

Data source providing device data associated with the violation.

Since

Date and time when this violation was first detected.



(Registered)

Icon indicating that the host associated with the violation is registered to the current user. Each user can register with any number of hosts, then filter on this field to view only the hosts of interest.

Application

Name of the applications to which the reported host is dedicated. Applicable if the violating path's host is assigned to run specific applications.


Application Priority

Priority for each application, listed in the same order as the applications are listed in the App field. Applicable if the host is assigned to run specific applications.

Tenant, Line of Business, Business Unit, Project

Columns listing the business entity components associated with the applications.

Planned

Icon  indicating that Insight has correlated one or more planned tasks with the violation. If you see this icon, look in the Tasks field for a list of correlated planned tasks.

Host FC Port Count

Number of host ports that can access the storage volume or tape device (blank if none), followed by the number required by the policy, in parentheses. If there is no number in parentheses, no host redundancy is specified in the policy. This field is blank for Path Outage violations.

Storage FC Port Count

Number of storage ports that can access the host, followed by the number required by the policy, in parentheses. If there is no number in parentheses, no storage redundancy is specified in the policy. This field is blank for Path Outage violations.

Hops

Actual Switch Hop Count (Fibre Channel) between the host and the storage (blank if unknown, as for a Path Outage violation). This first number is followed by the number required by the policy, in parentheses. If there is no number in parentheses, no switch-hop maximum is specified in the policy.

Sharing

Level of volume sharing permitted by the host, as specified by the policy (Any, No Sharing, or Application).

CHAP Required

Indicates whether CHAP security is in use on the path. Values are "None," "Inbound," "Outbound," and "Both In & Out."

Session Count

Number of iSCSI sessions that are used by this violation path.

Connection Count

N Number of iSCSI connections that are used by this violation path.

Host Fabrics

Comma-separated list of fabrics to which the host is connected (fabric name if available; otherwise the fabric WWN). By filtering this field, you can view only those hosts that are connected to particular fabrics.

Tasks

Shows as a blank column between Host Fabrics and Tasks. Displays a comma-separated list of planned tasks that relate to the violation. This list applies only with the Planned icon.

RDM

A VMware feature that exposes SCSI targets (or LUNs) directly to a virtual machine. RDMs are an alternative to using VMFS. RDMs are special files in a VMFS volume that act as a proxy for a raw device.

Datastore

The name of data store residing on a volume.

V-Policy

A check mark in this column indicates that a Host Virtualization policy has been applied. The column also displays the check mark when a host is excluded from the VM Host policy. Otherwise, the column is blank.

annotations

Annotations associated with each path that has a violation.

Options

To see details for a particular storage array, click on it in the main view. At the bottom of the Client window in the icon bar, click the Properties icon. 

This view includes the following options:

Show Registered only

Displays only those violations related to host systems that are registered to your logged-in user ID.

Customize

Lets you add or remove columns from the view.

Reset Filters

Displays data with the default filters.

Expand (Collapse) All Groups

Expands (or collapses) all groups in the table.

Group by box

Groups the data by the selection in the drop-down box.

Planned or Not Planned filter

Filters the data to show only planned or not planned violations.

- **Planned:** Displays violations that correlate to a planned task that's in Implementation mode. Once a task is put into Implementation mode, Insight automatically correlates that task to any outstanding violations.
- **Not Planned:** Displays violations that are based on existing paths and their policies.
- **All:** Displays all violations.

From the main view, right-click to show a pop-up menu containing the following options. If other Insight licenses are installed, additional options appear.

Set Path Policy

Allows you to create and modify a policy for a specific path.

Set Host Policy

Allows you to create and modify a policy for the host of a particular path.

Remove Path Policy

Deletes a policy for a specific path.

Remove Host Policy

Deletes a policy for the host of a particular path..

Host Virtualization Policy

Displays the Settings dialog box, where you can configure and activate a policy that governs host virtualization.

Dismiss Path Outage

Allows you to remove path outage violations for paths where the outage is expected or acceptable.

Analyze Violation

Opens the Analyze Violation dialog box that displays multiple tabs that you can use to investigate the selected violation, view root-cause analysis information, see the tests that were conducted leading to the violation analysis, and see the topology map graphically showing how the violation impacted your resources. Applies to Fibre Channel only. Only some violation types support this.

Go to Tasks

If the violation was created as a result of the execution of a plan, the plan icon appears in the Planned column in the Violations view. If the violation is planned, the Go to Tasks option displays the Plans view, and highlights the item on the task list that resulted in generating this violation.

Set Application

After you define applications with their business entities, this option associates the applications with the hosts on which they run.

Manage Applications

Define the applications for your system and then associate them with specific hosts and business entities.

Manage Business Entities

Add more business entities without associating them with applications immediately.

Analyze

Available only with the Perform license. Allows you to investigate the performance of the selected resources affected by the violation. For example, you can determine contention issues, availability issues, and array performance.

Analyze Storage Pools

Available only with the Assure license. Allows you to select a specific storage pool and assess its status related to the thin-provisioning policies. You can use this dialog box, instead of the Violations Browser, to see the current thin provisioning violations and how close the storage pool is to reaching the policy limits.

Edit Annotations

Allows you to edit annotations for the selected violation. You can change the note text and severity or remove the annotation.

Set Annotation

Allows you to assign an annotation value to the selected violations. For example, you might want to set notes or indicate the severity of the violation. You can later sort the violations by the annotation, for example, by severity.

Clear Annotation

Removes the assigned annotation.

Violation Changes view

Use the Violation Changes view to changes to the system that are associated with a violation selected in the SAN Path Violations main view. Using the Changes view and the Topology view, you can select a time frame and view the topology and the changes for a previous time. This helps you view the state of your environment at different times.

Navigation

From the Open menu, select **Assurance > SAN Path Violations** and click the **Changes** icon.

Column descriptions

To see details for changes that affect multiple objects, expand the change row in the main view.

Time

Date and time at which a data source reported this event or events. This timestamp allows Insight to recreate and display the state of your environment at any point in time.

icon

Indicates the type of event, for example, equipment additions and removals, zoning and masking changes, cabling reconfigurations, and system outages.

Event

The change action that occurred at the time indicated.

Changes that resulted from a single action are stamped with the same time and are grouped in the display. Click the + sign to display more detailed change information for events that are nested.

The information included here reports not only the change itself, but also the impact of the change on the access path.

Topology view

Use this view to visualize your SAN or NAS environment, the devices, and their connections. Every device in your environment is shown as an icon that represents the device type, while physical connections appear as lines connecting the devices. Each time you select a different device or path in a main view, the Topology representation changes as well.

Access

You can display a Topology map from the majority of the main views; however, you cannot access the Topology Map from the Switches, Storage Arrays, or Tapes main views. From a main view, select a device or path and click the Topology icon in the bottom of the Client view.

Operations

From the Topology view, you can perform the following operations:

- Position the mouse pointer over a device or path to see its detail.
- Click any device icon to view port information.
- Use the Topology toolbar to adjust settings.
- Select different view representations on the Topology Map.
- Change the link style to rounded or square.
- Add a watermark to the map.
- Add connected devices.
- Export the Topology layout as an image.

Violations Browser

You use the Violations Browser to monitor the current violation state of your monitoring environment and focus on violations based on various criteria, such as time, violation type, and impacted devices.

Navigation

From the Insight Open menu, select **Assurance > Violations Browser**.

Browser tree

Use the browser tree to the left of the Violations List to identify areas that require attention based on the violation count. Expand branches of the tree to see the groupings of violations. You might filter the items in the tree to focus on a particular host or VM of interest.

Click an item in the tree to see the details in the Violations List.

The severity levels, shown in the browser, can be changed to focus on high priority issues.

Violations Browser tree

You use the browser tree to the left of the Violations List to identify areas that require attention based on the violation count.

Navigation

From the Open menu, select **Assurance > Violations Browser**.

Browser features

You might want to filter the items in this list to show only the violations of current interest.

You can control the refresh rate of the browser with the **Refresh Now** icon or by selecting a setting from the **Refresh** pull-down menu:

- On Change
- 5 mins
- Manual

To improve browser speed, you can toggle off the Impact display. Click the **Don't show violation impacts in browser** icon so that only the Time and All Violations branches are shown in the tree.

All of the branches of the tree contain the following information:

- **Time**
Groups violations by type for different time periods including Today, Yesterday, Last Week, and Last Month.
- **Impacted < >**
Lists the affected business entities, applications, hosts, virtual machines, storage array, and tape for the violation types.
- **Data Center**
Lists the data centers, assigned using the annotations, with their associated violation totals and types.
- **All Violations**
Displays the total number of violations identified. Lists each type of violation identified with the totals of each.

Click an item in the tree to see the details in the Violations List. Your last selection in the browser tree is used as the first arrangement of the tree when you open the Violations Browser the next time.

After examining the expanded list of categories, you might want to combine the branches again with the **Collapse All** button at the top of the browser tree.

These **Severities** can be filtered in or out of Violations List display:

- Critical
- Warning

Violations List

The Violations List displays the violations to global general policies so that you can analyze the cause of the violation.

Navigation

The Violations List is integrated into the Violations Browser and is also a detail view available from the Policies view. You can group violations in the list by severity, violation type, element, or start time. When you select a violation, you can display detailed information for that violation.

Column descriptions

blank

Column that organizes the data according to the selected grouping format. Applicable with any presentation order other than No Grouping.

Element

Item in the system that the violation was detected on or associated with, such as disks, storage pools, storage arrays, or switch ports.

Description

Information about the problem detected.

Severity

Indication of how critical the violation is to the user's data center environment. The default severity for each violation type is configurable by the user in Settings, and the severity of individual violations can be changed manually using the Set Severity menu action.

Violation Type

Category of the problem.

Policy Type

Category of the policy generated violation.

Policy Level

Indicates the position in the policy hierarchy of the policy that generated the violation.

Start Time

The beginning of the time range of when the policy was violated.

End Time

The end of the time range of when the policy was violated. Some types of violations, such as performance alerts, are time range dependent, and remain present until they are dismissed. Other violation types reflect the current state of the environment and only have start times .

Options

Depending on the violation type, you might have additional information available from these right-click menu options:

Dismiss Violations

Violations caused by transitory events, such as spikes in performance, can be dismissed using this option. However, other violations cannot be dismissed and must be addressed by either fixing the issue or modifying the policy.

Modify Policy

Allows you to modify or remove a policy that caused a violation.

Analyze Violation

For violations displayed in the Violations Browser, you can display a summary of violation event details and list the volumes and internal volumes affected by the violation. Applies to Fibre Channel only. Only some violation types support this.

Analyze

Available only with the Perform license. Allows you to investigate the performance of the selected resources affected by the violation. For example, you can determine contention issues, availability issues, and array performance.

Violation Event view

You use this chart within the Violations Browser.

Navigation

From the OnCommand Insight Open menu, select **Assurance > Violations Browser**. Highlight a violation in the list. Click the **Violation Event** icon.

Description

The chart provides details of the event that caused the violation. Different types of violations provide different details to describe the violation event.

For example, a Storage Pool Utilization violation shows the percentage of utilization in relation to the threshold and the date and time when the event began. The dotted “Threshold” line across the chart represents the limit set in the policy covering this violation. Move the mouse pointer across the jagged lines in the chart to display the date, time, and percentage each point represents.

Impact Details view

Within the Violations Browser, you can identify the specific applications, hosts, virtual machines, and storage affected by the violations using the Impacted Details view.

Navigation

From the Open menu, select **Assurance > Violations Browser**. Select a violation. Click the **Impacted Details** icon.

Description

Click one of the element types in the list to display the names of the specific elements impacted by the selected violation.

VMDK Performance view

Use this view to determine which disks are the top consumers of IOPS. From this list, you can choose the top consumers and use the VM Performance Distribution Chart to compare their IOPS.

Navigation

- From the Insight Open menu, select **Performance > Virtual Machine Performance**. Click the VMDK Performance view icon.

Column descriptions

blank

Column that organizes the data according to the selected grouping format (by, for example, device name, connected device name). Applicable with any presentation order

other than No Grouping. The number in parentheses indicates the number of ports reported in each (grouped) row.

Name

Name of the virtual machine disk.

Virtual Machine

Name of virtual machine.

Datastore

The name of data store residing on this virtual machine disk.

Capacity (GB)

Total storage array capacity that is accessible to host applications, in gigabytes.

Used Capacity (GB)

The amount of capacity holding actual data in the virtual machine disk. Includes usage based on all file types.

RDM

A VMware feature that exposes SCSI targets (or LUNs) directly to a virtual machine. RDMs are an alternative to using VMFS. RDMs are special files in a VMFS volume that act as a proxy for a raw device.

Host Names

Hosts associated with the virtual machine disk.

Storage

Storage arrays used by this virtual machine disk.

Resource Name

The volumes or internal volumes in the path.

Resource Technology

The SAN (FC and iSCSI) or NAS (NFS and CIFS) protocols that the device supports.

Resource Capacity (GB)

The total capacity, in gigabytes of the volumes or internal volumes, in the paths of this virtual machine storage pool.

Resource Used Capacity (GB)

The total used capacity, in gigabytes of the volumes or internal volumes, in this virtual machine paths.

Deduplication Savings

The known amount of storage savings through deduplication, a process that detects blocks with identical content and replaces subsequent identical blocks with a reference to a single copy of the block.

IOPS (R&W)

The number of Read or Write I/O service requests passing through the I/O channel or portion of that channel per unit of time (measured in I/O per sec).

IOPS

The portion or ratio of I/O service requests by the selected host or application passing through the I/O channel per unit of time (measured in I/O per sec).

Top IOPS

The maximum sum of IOPS reported by the measured devices.

Throughput (R&W)

The rate at which data is read or written to the measured devices in a fixed amount of time. The value is measured in megabytes per second. The actual calculation of throughput depends on the device vendor.

Throughput

Rate that data is being transmitted in a fixed amount of time in response to I/O service requests (measured in MB per sec).

Top Throughput

The maximum sum of throughputs reported by the measured devices.

Latency (R&W)

The rate at which data is read or written to the virtual machines in a fixed amount of time. The value is measured in megabytes per second.

Latency

The average response time from the virtual machines carved from a data store.

Top Latency

The highest response time from the virtual machines carved from a data store.

Options

The following options are available from the right-click menu:

Analyze

Available only with the Perform license. Allows you to investigate the performance of the selected virtual machines. For example, you can determine contention issues, availability issues, and performance.

Analyzing and managing vulnerabilities

OnCommand Insight reports possible problems in your network configuration and usage that are contrary to best practices.

About this task

To generate vulnerabilities, OnCommand Insight monitors your network and identifies potential problems based on the policies you established, best practices, and the current network configuration and operation. You can set the thresholds for vulnerabilities.

Each vulnerability might not represent an actual problem on your network; however, you should review the list to be certain there are no concerns.

You have several tools to review these notifications:

- **Vulnerabilities main view** lists each type of vulnerability that OnCommand Insight monitors and tells how many occurrences there are of each type.
- **Vulnerabilities details view** provides information about a selected vulnerability in the main view.
- **Applications dashboard** shows potential problems associated with the applications running on your network.

Viewing vulnerabilities data

Use the Vulnerabilities summary list to see each type of vulnerability that OnCommand Insight monitors and how many occurrences there are of each type. The details for a selected vulnerability can be displayed in a separate window.

Steps

1. To display the vulnerabilities on your network, click the OnCommand Insight **Open** menu and select **Assurance > Vulnerabilities**. Each row in the list represents a single vulnerability.

If there are any occurrences of a vulnerability in your SAN, the row for that vulnerability displays in red to indicate a potential problem.
2. Click on a vulnerability type that is shown in red.
3. To display the network details for the selected vulnerability type, click the Vulnerabilities Details icon at the bottom of the window. You might need to expand the details tree to display more information for specific items.
 - Total number of vulnerability types represented in the view is shown next to the "Vulnerabilities" title.
 - Number of occurrences of each vulnerability type in the network is displayed on the right side.

Name	Description
Disconnected Switch Port Zone Members	Ports defined in a port-zoning configuration and have no device connected to them
Disconnected WWN Zone Members	WWNs defined in a WWN zoning configuration and are not connected to the fabric
Duplicate Backend Volume Assignments	Backend volume is assigned to more than one device
High Fabric Port Usage	Fabrics in which the number of connected ports is higher than 90%
High Volume Allocation	Storage devices in which percentage of masked volumes exceeds 90%
Incomplete Application Volume Sharing	Volumes that are not shared by all hosts in application
Inconsistent Volume Member Disks RPM	Inconsistent Volume Member Disks RPM
Local Replica for Undefined Volumes	Local replica for undefined volumes
Low Fabric Port Usage	Fabrics in which the number of connected ports is lower than 70%
Orphaned Volumes	Volumes that have not been accessed in the last 30 days

Fabric/VSAN	Used Ports	Total Ports	Switches
20:00:00:00:00:00:10	4	64	1
20:00:00:00:00:00:11	4	64	1
20:00:00:00:00:00:16	6	64	1
20:00:00:00:00:00:17	5	64	1
20:00:00:00:00:00:20 (Datacenter_Fabric_Gamma)	3	16	1
20:00:00:00:00:00:21 (Datacenter_Fabric_Alpha)	4	16	1
20:00:00:00:00:00:22 (Datacenter_Fabric_Beta)	3	16	1
20:00:00:00:00:00:37	3	16	1
20:00:00:00:00:00:38	2	16	1
20:00:00:00:00:00:39	1	2	1

The information displayed in the details window changes depending on the vulnerability type selected in the Vulnerabilities view. You might want to filter or group the information in the details window.

OnCommand Insight Applications Dashboard

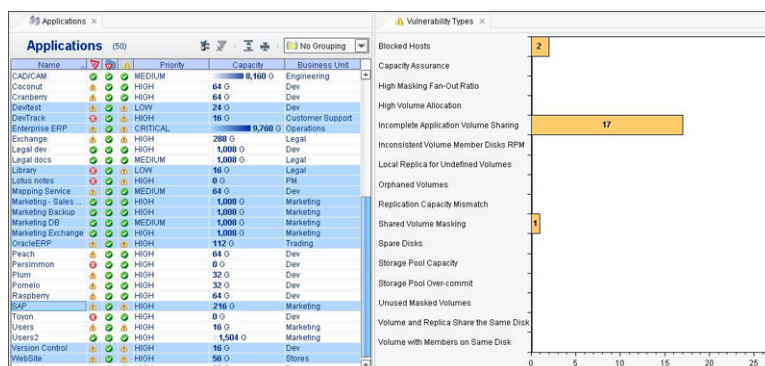
The Applications Dashboard provides the latest update and overall status of application storage service. At a glance, you can view the list of applications and see graphs that show service problems and change activity.

Using the dashboard, you can:

- Sort by capacity usage to see how much storage space is available for an application.
- Evaluate the cost-effectiveness of storage space allocation.
- See how well applications are functioning in your SAN at any given moment in time.

Predefined and user-defined schemes determine which indications and charts are displayed. Based on that capsule data, you can then investigate violations and vulnerabilities related to each application in greater detail by drilling down into OnCommand Insight.

The Applications Dashboard table can be grouped by business unit or priority. Focusing on a group of applications, you are able to correlate between applications. In this example, the selected applications on the left have a vulnerability due to incomplete application volume sharing (shown in the chart on the right). This could be intentional and, therefore, is not a problem.



Researching vulnerabilities

OnCommand Insight provides tools to research vulnerabilities and decide if any changes to your network are needed.

Before you begin


To display the vulnerabilities on your network, click the OnCommand Insight Open menu and select **Assurance > Vulnerabilities**.

To research the vulnerabilities in your network, follow these steps:

Steps

1. In the Vulnerabilities main view, select one vulnerability to research.

Note: Remember vulnerabilities are only potential problems.

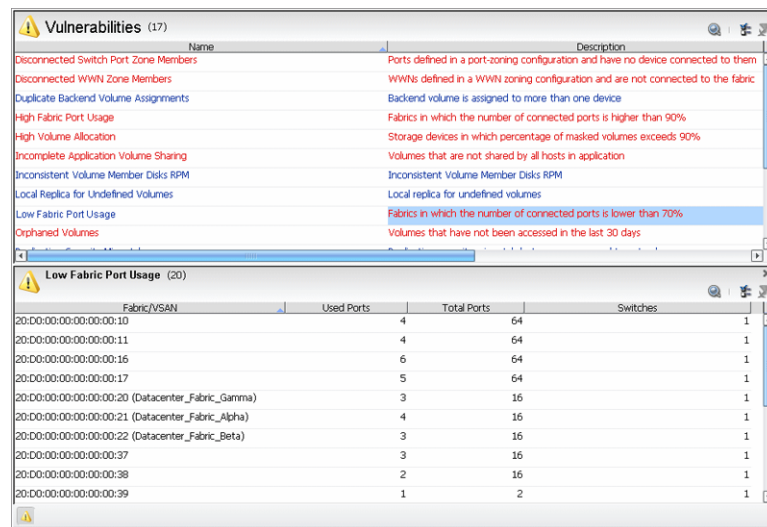
2. Click the  Vulnerabilities details icon below the window to display information about each selected vulnerability.

Each vulnerability type displays different detailed information depending on the type.

3. Focus on the details of each vulnerability type.

In this example, you select the Inconsistent Volume Member Disks RPM to determine which hard drives might be slowing the processing because they have slower speeds that other drives.

4. Examine the detailed information for the drives by grouping the drive information using the pull-down menu on the right and expanding the trees.



The screenshot shows the 'Vulnerabilities (17)' window. The 'Low Fabric Port Usage' vulnerability is selected, showing a detailed view with 20 items. The table below represents the data shown in the detailed view.

Fabric/VSAN	Used Ports	Total Ports	Switches
20:00:00:00:00:00:10	4	64	1
20:00:00:00:00:00:11	4	64	1
20:00:00:00:00:00:16	6	64	1
20:00:00:00:00:00:17	5	64	1
20:00:00:00:00:00:20 (Datacenter_Fabric_Gamma)	3	16	1
20:00:00:00:00:00:21 (Datacenter_Fabric_Alpha)	4	16	1
20:00:00:00:00:00:22 (Datacenter_Fabric_Beta)	3	16	1
20:00:00:00:00:00:37	3	16	1
20:00:00:00:00:00:38	2	16	1
20:00:00:00:00:00:39	1	2	1

After you finish

To see how applications might have vulnerabilities, select the OnCommand Insight Open menu and select **Assurance > Applications Dashboard**.

Establishing vulnerability thresholds

OnCommand Insight allows you to set multiple thresholds to define when a condition needs to be reported as a vulnerability.

Steps

1. Choose the **Configure Vulnerabilities** option from the Action or the right-click menu in the **Vulnerabilities** view.
2. In the dialog box that opens, enter the threshold values for these settings.

Vulnerability	Cause
High volume allocation: Percentage of masked volumes	The percentage of masked volumes on a storage array exceeds the stated percent.
Low fabric port usage: Percentage of connected hosts	The number of connected ports in a fabric is lower than the stated percent.
High fabric port usage: Percentage of connected hosts	The number of connected ports in a fabric is higher than the stated percent.
Spare Disks: Number of spare disks per disk type	The number of spare disks for any disk type is less than the stated number.
Orphaned volume identification: Days since last accessed	The number of days since last accessed used to identify orphaned volumes in your environment.
RAID RPMs not equal: Allowed percentage of faster disks	For the "Inconsistent Volume Member Disks RPM" vulnerability only, the percentage of disks that are allowed to be faster than other disks before the vulnerability warning is triggered.

Managing thin provisioning using vulnerabilities

Thin provisioning optimizes the efficiency with which space is utilized in storage area networks, based on the minimum space required at any specified time. Thin provisioning allows space to be easily allocated to servers on a just-enough and just-in-time basis, and thus substantially improves poor utilization rates. A single shared storage pool can be accessed by multiple volumes.

Enabling thin provisioning introduces challenges because you need to:

- Ensure that there is enough capacity (and define what is enough capacity) to support the thin provisioning.
- Mitigate the impact of a server on any other servers.

To maximize efficiency, thin provisioning allows you to "over-provision" or reserve more storage for applications than you actually have, knowing that applications rarely use all of the storage that is reserved for them at any given time. To safeguard against running out of space under such circumstances, OnCommand Insight provides the vulnerabilities described in the next sections.

Orphaned Volumes vulnerability

To identify orphaned volumes, OnCommand Insight checks the last accessed time for volumes on devices for which acquisition is set up to collect data.

If a volume has not been accessed in at least the interval of days you set as the threshold, the Orphaned Volumes (by last access time) vulnerability is triggered. The Description column in the Vulnerabilities view displays the message: "Volumes that have not been accessed in the last <number of configured days> days."

Viewing the Client

The Orphaned Volumes detail view shows the following columns for the data provided:

Column	Description
<i>blank</i>	Applicable with any presentation order other than No Grouping.
Storage	Name of the storage device.
Vendor	Vendor of the storage device.
Family	Family of the storage device.
Model	Model of the storage device.
Volume	Name of the volume (for SAN volumes; LUN for NetApp).
Volume Type	Volume type.
Capacity (GB)	Total capacity of the volume.
Last Known Access Time	Last time this volume was accessed.

Grouping:

All data can be grouped by:

- Storage (the summary row for each storage device shows the sum of the capacities of all orphaned volumes).
- Storage Vendor
- Storage Model
- Volume Type and then Storage

Spare Disks vulnerability

Storage arrays require that spare disks be of the same type (speed, capacity and protocol) as the standard disks. For each disk type discovered in the storage array, OnCommand Insight verifies that there are a minimum number of spare disks of the same type.

If there are an insufficient number, the **Spare Disks** vulnerability is triggered. The description column in the main Vulnerabilities view contains the text "Storage arrays with an insufficient number of spare disks."

Viewing the client

The Spare Disks detail view shows the following columns for the data provided:

Column	Description
Storage	Name of the storage device.

Column	Description
Vendor	Vendor of the storage device.
Family	Family of the storage device.
Model	Model of the storage device.
Disk Type	Vendor-specific type of volume (for example, SFS, B.V.).
Disk Size	Size of the volume that is accessible to host applications, in gigabytes.
Disk Speed	Disk speed, in revolutions per minute (rpm)
Actual Spares	Number of spare disks found.

The rows of the view represent the spares for every storage array in the storage environment. Arrays whose disk types do not satisfy the "Number of Spare Disks per Type" threshold only show the disk type entries for those disk types for which there are not sufficient spares.

Note: For Solid State Disk types, OnCommand Insight does not show a speed.

Grouping


All data can be grouped by:

- Disk Type
- Disk Type and then Disk Size
- Storage Name
- Storage Model
- Storage Vendor

Adding hosts to application groups

Based on the information supplied in the Shared Volume Masking vulnerability, you might add a host to an application group.

Steps

1. Select the red **Shared Volume Masking** line in the Vulnerabilities main view.
2. Click the  Vulnerabilities Details icon at the bottom of the window.
3. Right-click on one or more hosts in the Vulnerabilities Details view and select one of these options:

Option	Description
Add accessing Hosts to Application	manually adds selected hosts to an application group.
Automatically add accessing Hosts to Application	adds the selected hosts automatically to an application group, extracting the application name using a regular expression.

Vulnerabilities main view and types

OnCommand Insight gathers potential network vulnerability information based on best practices for the vulnerability types listed in the main view.

Navigation

To display the Vulnerabilities main view, open the OnCommand Insight Open menu and select **Assurance > Vulnerabilities**.

Vulnerability descriptions

The vulnerability types provide information that is generally important, but might not represent a danger. For example, you might want to know that a host is not zoned because it is orphaned and might need to be retired. Select a vulnerability to display the details below.

Disconnected Switch Port Zone Members vulnerability for Fibre Channel

This type of vulnerability identifies ports that are defined in a switch-port based zoning configuration, but have no device connected to them.

Column	Description
<i>blank</i>	Column that organizes the data according to the selected grouping format (fabric then switch, for example). Applicable with any presentation order other than No Grouping. The number in parentheses indicates the number of items reported in the (grouped) row.
Fabric/VSAN	Fabric where the port is defined.
Zone	Zone where the port is defined.
Switch	Name of the switch for the unconnected port.
Member	Number to identify the unconnected port on the referenced switch.

Disconnected WWN Zone Members vulnerability for Fibre Channel

This type of vulnerability identifies unconnected ports that are defined in a WWN-based zoning configuration.

Column	Description
Fabric/VSAN	Fabric where the port is defined.
Zone	Zone where the port is defined.
Member	WWN to identify the unconnected port on the referenced device.
Status	Status of the vulnerability (e.g., port not connected).
Device Name	Name of the switch for the unconnected port.

Duplicate Backend Volume Assignments vulnerability

This vulnerability indicates that the backend volume has been assigned to more than one device.

Column	Description
<i>blank</i>	Applicable with any presentation order other than No Grouping. Column that organizes the data according to the selected grouping format (for example, storage).
Storage	Name of the storage array.
Backend Volume	Name of backend volume.
Devices	Device names to which the same backend volume has been assigned.

High Fabric Port Usage vulnerability for Fibre Channel

This type of vulnerability identifies fabrics in which the number of connected ports is higher than the percent configured using the Vulnerabilities Thresholds dialog box.

Column	Description
<i>blank</i>	Applicable with any presentation order other than No Grouping.
Fabric/VSAN	Fabric/VSAN that is nearing capacity on port usage.
Used Ports	Number of ports in use currently.
Total Ports	Number of ports available for use.
Switches	Number of switches on this fabric.

High Volume Allocation vulnerability

This type of vulnerability identifies storage arrays where the percentage of masked volumes exceeds the percent configured via the Vulnerabilities Thresholds dialog box (defaults to 90%).

Column	Description
Storage	Name of the storage array.
Total Volumes	Number of volumes currently defined on this array.
Allocated Volumes	Number of masked volumes on the array.

Incomplete Application Volume Sharing vulnerability

This type of vulnerability identifies volumes that are not shared by all the hosts assigned to a particular application. This lack of complete sharing can be intentional or not, so this vulnerability does not necessarily represent a problem.

Column	Description
<i>blank</i>	Applicable with any presentation order other than No Grouping (column that organizes the data according to the selected grouping format such as storage or application).

Application	Name of the application to which the host servers are assigned.
Storage	Name of the storage array being accessed (contains the volume, displayed next).
Volume	Name of a volume that is not shared by all hosts sharing the application.
Capacity (GB)	Size of the volume in GB.
Volume Type	Vendor-specific type of volume (for example, Meta).
Hosts with Paths	List of host names that are masked to access the referenced volume, but that cannot actually access that volume (due to problems such as an invalid zoning configuration, cabling errors, bad mapping, or connection to the wrong fabric).
Hosts without Paths	List of host names that do not have a valid path to the volume.

Inconsistent Volume Member Disks RPM vulnerability

This type of vulnerability identifies volumes that have volume members spanning disks with unequal RPM (for example, when three of four disks are operating at 7,200 RPM and one is running at 10,000 RPM). Because all the disks are not using the same RPM, the operations are bound by the slowest disk, introducing latency to the configuration.

You can set the "RAID RPMs not equal" threshold for this vulnerability as a percentage of the disks that are allowed to be faster than other disks before the vulnerability warning is triggered. This threshold is particularly useful if you are replacing older, slower disks with newer, faster disks and do not want to be warned about this inconsistency unless it is more pervasive.

Column	Description
<i>blank</i>	Column that organizes the data according to the selected grouping format (for example, storage). Applicable with any presentation order other than No Grouping. The number in parentheses indicates the number of items reported in the (grouped) row.
Storage	Name of the storage array on which the volume exists
Volume	Name to identify the volume
Volume Member	The names of volume member that has unequal RPM
Hosts	The hosts accessing this specific volume
Disks	Disks that the volume member spans

Local Replica for Undefined Volumes vulnerability

The disaster-recovery configuration is flawed due to an undefined volume.

Column	Description
<i>blank</i>	The blank column is used for grouping. In this case there is only one grouping (Storage). Thus it would contain the storage name in the summary row when grouping is enabled.
Storage	Name of the storage array being replicated.
Source Volume	The volume that is being copied.

Column	Description
Target Volume	The volume receiving the copy.
Missing	When checking the disaster-recovery configuration, the system detects a synchronization entry for two volumes, but finds that one of the volumes is missing. The value of the missing volume is shown here.

Low Fabric Port Usage vulnerability for Fibre Channel only

This type of vulnerability identifies fabrics where the number of connected ports is lower than the percent configured using the Vulnerabilities Thresholds dialog box (defaults to 70%).

Column	Description
Fabric/VSAN	Fabric/VSAN that is low on port usage.
Used Ports	Number of ports in use currently.
Total Ports	Number of ports available for use.
Switches	Number of switches on this fabric.

Orphaned Volumes vulnerability

To identify orphaned volumes, OnCommand Insight checks the last accessed time for volumes on devices for which acquisition is set up to collect data.

If a volume has not been accessed in at least the interval of days you set as the threshold, the Orphaned Volumes (by last access time) vulnerability is triggered. The Description column in the Vulnerabilities view displays the message: "Volumes that have not been accessed in the last <number of configured days> days."

Viewing the Client

The Orphaned Volumes detail view shows the following columns for the data provided:

Column	Description
<i>blank</i>	Applicable with any presentation order other than No Grouping.
Storage	Name of the storage device.
Vendor	Vendor of the storage device.
Family	Family of the storage device.
Model	Model of the storage device.
Volume	Name of the volume (for SAN volumes; LUN for NetApp).
Volume Type	Volume type.
Capacity (GB)	Total capacity of the volume.
Last Known Access Time	Last time this volume was accessed.

Grouping:

All data can be grouped by:

- Storage (the summary row for each storage device shows the sum of the capacities of all orphaned volumes).

- Storage Vendor
- Storage Model
- Volume Type and then Storage

Replication Capacity Mismatch vulnerability

This vulnerability signals a replication capacity mismatch between source and target volumes.

Column	Description
blank	Applicable with any presentation order other than No Grouping. Column that organizes the data according to the selected grouping format (for example, storage).
Source Storage	Name of the source storage array.
Source Volume	Name of source volume for use in replication.
Source Capacity (GB)	The size of the volume used as the source in replication.
Target Storage	Name of target storage array.
Target Volume	Name of target volume in storage array to receive the replicated data.
Target Capacity (GB)	The size of the volume that is supposed to receive the replicated data. It must be equal to or larger than the Source Capacity.

Shared Volume Masking vulnerability

This type of vulnerability identifies volumes that are masked to more than one host that do not share any applications.

This vulnerability is not reported for hosts (including both Accessing Hosts and Masked Only) that access the same volume and share at least one application.

Column	Description
<i>blank</i>	Applies to any presentation order other than No Grouping. The column organizes the data according to the selected grouping format (for example, storage). The number in parentheses indicates the number of items reported in the (grouped) row.
Storage	Specifies the name of the storage array.
Volume	Specifies the name used to identify the volume.
Capacity	Specifies the size of the volume, in gigabytes.
Type	Specifies the volume type (for example, Meta).
Accessing Hosts	Specifies the names used to identify one or more hosts to which the volume is masked (comma-separated if there is more than one host). The host information is based on the volume-masking configuration.

Column	Description
Masked Only	Specifies the names used to identify one or more hosts that are enabled to access the volume through the masking mechanism, but that cannot physically access the volume (comma-separated if there is more than one host).

Spare Disks vulnerability

Storage arrays require that spare disks be of the same type (speed, capacity and protocol) as the standard disks. For each disk type discovered in the storage array, OnCommand Insight verifies that there are a minimum number of spare disks of the same type.

If there are an insufficient number, the **Spare Disks** vulnerability is triggered. The description column in the main Vulnerabilities view contains the text "Storage arrays with an insufficient number of spare disks."

Viewing the client

The Spare Disks detail view shows the following columns for the data provided:

Column	Description
Storage	Name of the storage device.
Vendor	Vendor of the storage device.
Family	Family of the storage device.
Model	Model of the storage device.
Disk Type	Vendor-specific type of volume (for example, SFS, B.V.).
Disk Size	Size of the volume that is accessible to host applications, in gigabytes.
Disk Speed	Disk speed, in revolutions per minute (rpm)
Actual Spares	Number of spare disks found.

The rows of the view represent the spares for every storage array in the storage environment. Arrays whose disk types do not satisfy the "Number of Spare Disks per Type" threshold only show the disk type entries for those disk types for which there are not sufficient spares.

Note: For Solid State Disk types, OnCommand Insight does not show a speed.

Grouping

All data can be grouped by:

- Disk Type
- Disk Type and then Disk Size
- Storage Name
- Storage Model
- Storage Vendor

Unused Masked Volumes vulnerability

This type of vulnerability identifies masked disk volumes that cannot be reached from any host.

Column	Description
<i>blank</i>	Column that organizes the data according to the selected grouping format for example, storage then host). The number in parentheses indicates the number of items reported in the (grouped) row. Applicable with any presentation order other than No Grouping.
Storage	Name of the storage array for the masked volume.
Volume	Name of the masked volume that is not reachable.
Capacity (GB)	Size of the volume, in gigabytes.
Type	Vendor-specific type of volume (for example, BCV).
Storage Port	Storage port to which the volume is masked.
Host WWN	WWN to identify the host to which the volume is masked.
Host	Name of the host to which the volume is masked.
Policy	Policy icon - Displays if the masked volume participates in an authorized path (this is, if a path that complies with its policy exists from any host to this volume).
Unused Since	Date and time that the volume was last accessible from any host.
Detailed Status	Information about whether there is any problem with the masking. For example, you might see a message indicating that the host and storage devices do not share zones or that there is a disconnected host port.

Volume and Replica Share Same Disk vulnerability

This type of vulnerability identifies volumes and replicas (Business Continuity Volume--BCV) that share the same disk, an event which causes performance problems (potential contention and degradation of service).

If the volumes and replicas share the same disk, this also prevents full backup, since information that is shared by both the BCV and the volume on the same disk could be lost if the disk is corrupted or fails. That is, if the BCV is used for backup and the disk goes down, you lose both the volume *and* the backup.

Column	Description
<i>blank</i>	Applicable with any presentation order () other than No Grouping. Column that organizes the data according to the selected grouping format (for example, storage). The number in parentheses indicates the number of items reported in the (grouped) row.
Storage	Storage name of the source volume.
Source Volume	The volume on the disk.

Target Volume	The replica (BCV) that is on the same disk as the volume.
Hosts	Host(s) of the source volume.
Disks	The disk(s) in contention.

Volume with Members on Same Disk vulnerability

This type of vulnerability identifies volume members that belong to the same metavolume and are sharing the same disk. The idea is to distribute I/O--if Volume Members are on the same disk, you have a potential bottleneck.

The SAN administrator must ensure that the conflict is resolved by placing volume members on different disks.

Column	Description
<i>blank</i>	Applicable with any presentation order other than No Grouping. Column that organizes the data according to the selected grouping format (for example, storage).
Disk	The number in parentheses indicates the number of items reported in the (grouped) row.
Volume	Name of the disk being shared.
Volume Members	Name to identify the volume that contains the volume members sharing the same disk.
Hosts	The names of volume members that are sharing the same disk.

Volumes have LUNs with value greater than 255 vulnerability

This type of vulnerability identifies volumes exposed as SCSI targets (LUNs) that are greater than 255, and their relation to hosts and operating systems.

Column	Description
<i>blank</i>	Column that organizes the data according to the selected grouping format (for example, storage then host). The number in parentheses indicates the number of items reported in the (grouped) row. Applicable with any presentation order other than No Grouping.
Storage	Name of the storage array for the masked volume.
Volume	Name of the masked volume that is not reachable.
Capacity (GB)	Size of the volume, in gigabytes.
Raw Capacity (GB)	Actual raw disk capacity used by the volume. For example, a RAID-5 volume uses extra capacity to prevent failure in case of a single disk failure.
Storage Port	Storage port to which the volume is masked.

Column	Description
LUN	Logical Unit Number used by the host to access this volume.
Status	Status of whether volume has been mapped (allocated) to a storage port or not.
Host	Name of the host to which the volume is masked.
Host Initiator	WWN or node name for the host port to which the storage volume is masked.
Storage Target	Date and time that the volume was last accessible from any host.
Protocol Controller	Protocol converter through which the volume is mapped to the storage port (applicable only for some types of storage arrays, such as EMC CLARiiON).
Host OS	Operating system running on the host.

Copyright information

Copyright © 1994–2016 NetApp, Inc. All rights reserved. Printed in the U.S.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

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

Trademark information

NetApp, the NetApp logo, Go Further, Faster, AltaVault, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCenter, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, and WAFL and other names are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web at <http://www.netapp.com/us/legal/netapptmlist.aspx>.

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email to doccomments@netapp.com. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

Index

A

- alerts
 - disabling performance thresholds [13](#)
 - list of [71](#)
 - reviewing and confirming [12](#)
- analyzing
 - data store latency [54](#)
 - host port balance [56](#)
 - missing cluster path [70](#)
 - missing path redundancy [66](#)
 - path outages [65](#)
 - storage pool capacity [59](#)
 - storage pool utilization [60](#)
 - storage port balance [58](#)
- applications
 - causing latency problems [54](#)

B

- balance
 - host port [56](#)
 - storage port [58](#)
 - violations for all port types [75](#)
- best practices
 - path policy uses [17](#)

C

- capacity
 - avoiding over commitment [49](#)
 - identifying unused [48](#)
 - storage pool violation [59](#)
 - trend report [48](#)
- changes
 - details [39](#)
 - list of [37](#)
 - monitoring [34](#)
 - showing possible problems [36](#)
- clusters
 - missing virtual path violation [70](#)
- comments
 - how to send feedback about documentation [105](#)
- configuration
 - violation notification [14](#)
 - violation severity levels [15](#)

D

- data store
 - latency policy [7](#)
- data stores
 - list of [40](#)
- disks
 - virtual machine [43](#)
- documentation
 - how to receive automatic notification of changes to [105](#)

how to send feedback about [105](#)

F

- feedback
 - how to send comments about documentation [105](#)
- Fibre Channel
 - backend path policies [21](#)
 - global policies [30](#)
 - global SAN path policies [17](#)
 - global storage policy [18](#)
 - global tape policies [20](#)
 - global volume capacity policies [19](#)
 - global volume type policies [19](#)
- file systems
 - list of [42](#)

G

- global policies
 - customizing general [13](#)
 - hierarchies for customization [7](#)
 - modifying default [7](#)
 - SAN path [17](#)
 - settings for general [31](#)

H

- hosts
 - policies [17, 24](#)

I

- information
 - how to send feedback about improving documentation [105](#)
- iSCSI
 - global SAN path policies [17](#)
 - global storage policy [21](#)
 - global volume capacity policy [22](#)
 - global volume type policy [22](#)
 - setting global policies [32](#)

L

- latency
 - analyzing problems [54](#)

M

- modifying
 - policies [8](#)
- monitoring
 - changes [34](#)

P

paths

- correcting violations [62](#)
- missing [67](#)
- missing redundancy [66](#)
- missing virtual cluster violation [70](#)
- policies [17](#), [23](#)
- violations [65](#), [77](#)

performance

- alerts [71](#)
- analyzing general violations [53](#)
- customizing general policies [13](#)
- disabling thresholds [13](#)
- policies, modification [27](#)
- setting global policies [7](#)
- switch thresholds [9](#)
- VM disks [85](#)

planning

- storage pool allocation [72](#)

policies

- and violations [6](#)
- backend path [21](#)
- creating SAN path [16](#)
- customizing global general [13](#)
- disabling global path [26](#)
- editing SAN path [25](#)
- general [8](#)
- global [18](#), [21](#)
- global general [28](#), [84](#)
- global general, settings for [31](#)
- global hierarchy [7](#)
- global tape for Fibre Channel [20](#)
- global volume capacity for Fibre Channel [19](#)
- global volume capacity for iSCSI [22](#)
- global volume type for iSCSI [22](#)
- host [24](#)
- iSCSI [32](#)
- modifying [27](#)
- path [23](#)
- removing SAN path [26](#)
- reviewing [24](#)
- SAN path [16](#), [28](#)
- setting global performance [7](#)
- specific host and path [17](#)
- types [7](#)
- volume type [19](#)

ports

- all balance violations [75](#)
- balance violations [56](#), [58](#)

R

reports

- storage capacity trends [48](#)

S

setting

- switch performance thresholds [9](#)

settings

- global general policies [31](#)

Violation Severity [33](#)

SNMP traps

- general violation types in [52](#)

storage pools

- allocating [72](#)
- avoiding over commitment [49](#)
- identifying unused capacity [48](#)
- utilization violations [60](#)

suggestions

- how to send feedback about documentation [105](#)

switch thresholds

- types and formulas [11](#)

switches

- changing thresholds [13](#)
- setting performance thresholds [9](#)

T

tapes

- global policies [20](#)

tasks

- path violations related to [69](#)

thin provisioning

- policies [7](#)
- policy severity settings [33](#)
- setting global policies [7](#)
- storage pool violations [59](#)
- storage pools status [72](#)

thresholds

- global performance [7](#)
- performance [13](#)
- switch performance [9](#)
- vulnerabilities [91](#)

topology

- analyzing path violations [62](#)
- showing problem paths [36](#)
- view operations [82](#)

troubleshooting

- using Topology and Changes [36](#)

Twitter

- how to receive automatic notification of documentation changes [105](#)

U

utilization

- storage pools [60](#)

V

violations

- analyzing general [53](#)
- browser [82](#)
- capacity over commitment [49](#)
- changes [34](#)
- clearing multiple path [68](#)
- correcting path [62](#)
- critical [83](#)
- data store latency [54](#)
- dismissing [61](#)
- filter display by severity [53](#)
- general [51](#)

- general types [52](#)
- global general [84](#)
- host port balance [56](#)
- list of global general [84](#)
- missing path [67](#)
- missing path redundancy [66](#)
- missing virtual cluster path [70](#)
- notification configuration [14](#)
- notifications [7](#)
- path outages [65](#)
- path problems related to tasks [69](#)
- path types [63](#)
- policies [8](#)
- refresh [83](#)
- SAN path [61](#), [77](#)
- severity [83](#)
- severity level [15](#)
- severity level settings [33](#)
- storage pool capacity [59](#)
- storage pool utilization [60](#)
- storage port balance [58](#)

- system changes [68](#)
- thin provisioning [72](#)
- viewing types [51](#)
- warning [83](#)
- virtual machines
 - disk performance [85](#)
 - disks [43](#)
 - list of [45](#)
- virtualization policies
 - introduction to setting [69](#)
- VM violations
 - introduction to monitoring [69](#)
- VMDK [43](#)
 - See also* virtual machine disks
- volumes
 - setting performance policies [7](#)
- vulnerabilities
 - analyzing [88](#)
 - setting thresholds [91](#)
 - unused masked volumes [100](#)
 - volumes have LUNs greater than 255 [101](#)