Citrix NetScaler Management Pack Solution

Table of Contents

Introducing Citrix NetScaler Management Pack

The Citrix NetScaler Operation Manager pack provides monitors and rules to monitor the NetScaler systems deployed in your network.

The Citrix NetScaler Performance and Resource Optimization (PRO) Management Pack (MP) provides monitors and rules to monitor the health of the virtual servers configured on the managed NetScaler systems and initiate corrective actions using the PRO feature of SCVMM when the virtual servers become unhealthy.

Dependencies on Other Management Packs

The Citrix NetScaler Management Pack is dependent on the following management packs:

- System.Library
- System.Health.Library
- System.Snmp.Library
- System.Performance.Library
- Microsoft.SystemCenter.Library
- Microsoft.SystemCenter.NetworkDevice.Library
- Microsoft.SystemCenter.DataWarehouse.Library
- Microsoft.Windows.Library
- PRO pack (Note that this is applicable to the PRO pack only)
    - Microsoft.SystemCenter.VirtualMachineManager.PRO.Library
    - Microsoft.SystemCenter.VirtualMachineManager.PRO.V2.Library
    - Microsoft.SystemCenter.VirtualMachineManager.Library

Prerequisites

Before you import the management pack(s) in the SCOM Operations Console, ensure that the following prerequisites are met:

- Dependent management packs, as mentioned in the above section, are imported in to SCOM.

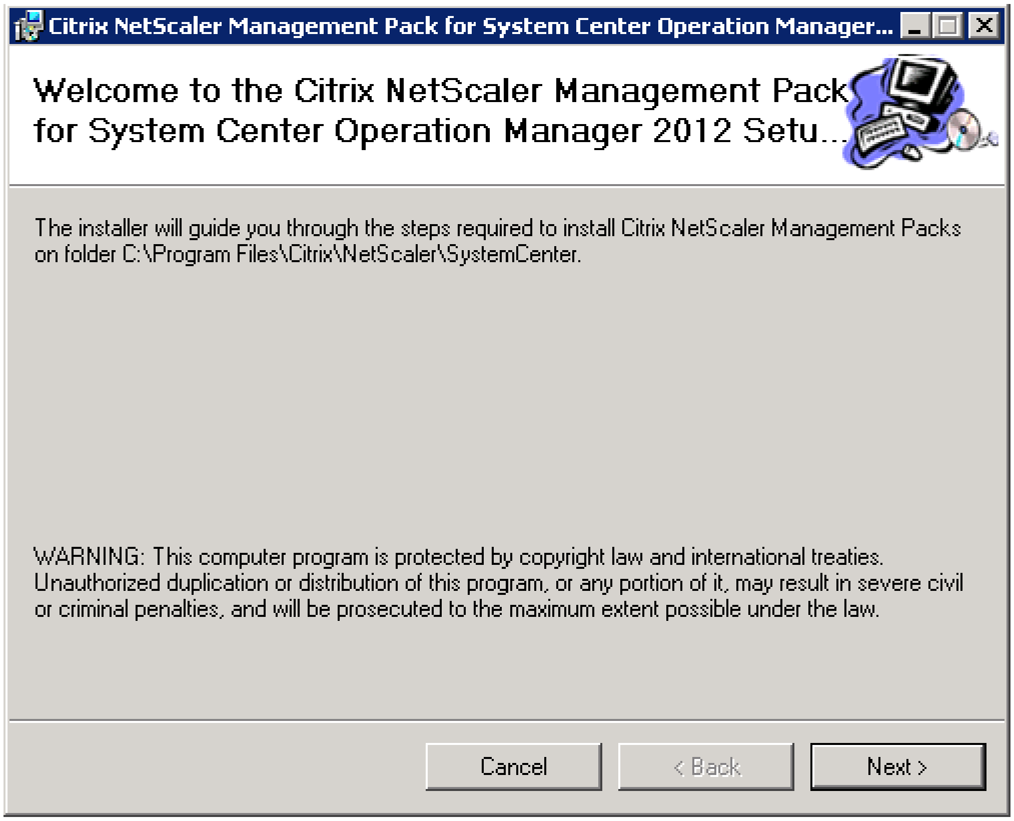
- Windows SNMP Service Feature is installed.
- Windows Server 2008/2012 (64-bit Operating System).

Installing Citrix NetScaler Management Pack

The Citrix NetScaler management pack solution is packaged as Windows installer, .msi.

To install the management pack

1. Double-click `CitrixNetScalerManagementPackSCOM2012.msi` file. The **Welcome** screen appears as shown in the figure below.



Citrix NetScaler Management Pack for System Center Operation Manager...

Welcome to the Citrix NetScaler Management Pack for System Center Operation Manager 2012 Setu...

The installer will guide you through the steps required to install Citrix NetScaler Management Packs on folder C:\Program Files\Citrix\NetScaler\SystemCenter.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

2. In the **Welcome** dialog box, click **Next.**
3. In the **License Agreement** dialog box, read the agreement, click **I Agree**, and then click **Next.**
4. In the **Confirm Installation** dialog box, click **Next** to start installation of this solution. Note that all the components are installed under `C:\Program Files\Citrix\NetScaler \SystemCenter`
5. In the **Installation Complete** dialog box, click **Close.**

Verifying the Installation

After the installation is complete, you can verify whether the management pack is successfully installed.

To verify the installation

1. Click **Start** > **Settings** > **Control Panel** > **Add or Remove Programs**.
2. In the **Add or Remove** window, check for Citrix NetScaler Management Pack for System Center Operations Manager 2012 entry.

Importing Management Packs

To import management packs

1. Open the **System Center Operations Manager** console by clicking **Start** > **Programs** > **System Center Operations Manager 2012** > **Operations Console**.
2. In the **Operations** view, click the **Administration** button.
3. Right-click the **Management Packs** node and then select **Import Management Pack**.
4. In the **Select Management Packs** window, click Add .
5. Click **Add** from disk to import the management packs from the local disk.
6. Click **No** on the message that appears.
7. Navigate to `C:\Program Files\Citrix\NetScaler\SystemCenter\mp` folder and select all the `.mp` files, and then click **Open**.
   Note: To import only the Operations Manager solution, select the `Citrix.NetScaler.mp` file. To import the PRO feature of SCVMM, import all the `.mp` files.
8. In the **Import Management Packs** screen, click **Install**.

   Note: The system may take few moments to complete the install process.
9. After the installation is completed, click **Close.**

Using the Operation Manager Solution

This section describes the features supported on the Citrix NetScaler Operations Manager solution and lists the tasks you need to perform to override performance rules.

Features supported

Citrix NetScaler Management Pack discovers SNMP-enabled NetScaler systems using the standard Discovery Wizard of SCOM 2012. It also provides fault and performance management functions.

Discovery

Citrix NetScaler Management Pack discovers SNMP-enabled NetScaler systems and places them in the Network devices node. The following state views are provided with the management pack:

- **Device state view**: This includes two views, ActiveDevices and AllDevices. The ActiveDevices view displays Standalone and Primary devices of a High Availability (HA) setup. The AllDevices view displays all NetScaler systems – Standalone, Primary, and Secondary. The Device state view is updated with the state of the device and the deployment mode of the device, which could be Standalone, Primary, or Secondary. Primary and Secondary devices are displayed as separate entries in their respective views.
  Note: In case of a failover, the device node state is refreshed during the next scheduled discovery cycle. By default, the discovery is scheduled every 6 hours.

- **License and Modes view**: This view displays the status of the license and modes of all managed devices.
  Note: Monitoring views are not supported from Citrix NetScaler Management Pack Solution version 2.0.1.2.

Fault Management

The Citrix NetScaler Management Pack collects and processes the traps generated by the managed devices. To enable the management pack to collect and process traps, ensure that the IP address of the Operation Manager is added as a trap destination in the managed NetScaler system.

To learn about the supported traps, their descriptions, and their severity levels, see Appendix – Supported Traps.

Performance Monitoring

This feature displays all the supported performance counters in their respective views. Note that, by default, the performance counters are not enabled for polling. To enable these counters, you need to override the performance rules. For more information, see section How to Override a Performance Rule.

To learn about the supported performance counters, see Appendix – Supported Performance Counters.

How to Override a Performance Rule

As mentioned in the Performance Monitoring section, by default, the performance counters are disabled for polling. However, you can enable the performance rules supported on the NetScaler SCOM pack using the override functionality of SCOM.

To enable the performance rules

Perform the following tasks to enable performance rules:

1. Create a management pack to store the override settings
2. Look for rules applicable to Citrix NetScaler MOM pack
3. Look for performance rules specific to Citrix NetScaler
4. Override the performance rule to enable/disable it from polling

Create a management pack to store the override settings

To override an attribute in Operations Manager pack, you need to create a management pack to store the overrides. You cannot use the Citrix NetScaler pack because it is a signed pack.

To create a management pack

1. Start **Operations Console (Start** > **Programs** > **System Center Operations Manager 2012** > **Operations Console).**
2. In the left pane, click the **Administration** pane.
3. In the **Administration** window, in the left pane, right-click **Management Packs** node, and then click **Create Management Pack**.
   The **Create a Management Pack** dialog box appears.
4. Under **General Properties**, in **Name**, type a name for the management pack (for example, Citrix NetScaler Overrides), and in **Version**, type a version number (for example, 0.0.0.1).
5. Click **Next**.
6. Under **Knowledge Article**, click **Create**.

   Note: The management pack you just created, Citrix NetScaler Overrides, is displayed in the management pack view.

Look for rules applicable to Citrix NetScaler MOM pack

A SCOM setup may have more than one imported management pack. You need to look for rules that are applicable to Citrix NetScaler MOM pack.

To look for rules applicable to Citrix NetScaler MOM pack

1. In **Operations Console**, click the **Authoring** pane.
2. In the **Authoring** window, in the left pane, under **Management Pack Objects**, click **Rules**.

3. In the **Rules** pane, click **Change Scope** (on the top right corner).
4. In the **Scope Management Pack objects by target**(s) dialog box, in **Look for**, type **Citrix**.
5. Select **View all targets**, and then from the **Targets** list, select **Citrix NetScaler Device**.
6. Click **OK**.

Note: In the **Rule view** pane, you can view all types of Citrix NetScaler rules, such as rules for Events, Alerts, and Performance Rules.

Look for performance rules specific to Citrix NetScaler

Citrix NetScaler Management Pack supports the following groups of Performance Rules:

- ACL Table
- App Firewall
- Compression
- Content Filter
- GSLB
- HTTP
- ICache
- ICMP
- Interface
- IP
- Resource
- Service
- SSL
- Sure Connect
- TCP
- UDP
- Virtual Server
- VLAN
- ACL6
- Simple ACL
- App Firewall Profile

To look for performance rules specific to Citrix NetScaler

In the **Rules** pane, in **Look for**, type a group name for a performance rule (for example, Virtual Server Current Services Up), and then click **Find Now**.

Note: Names of all events end with the word “Event” and names of all alerts end with the word “Alert”. You need to avoid these rules when searching for performance rules.

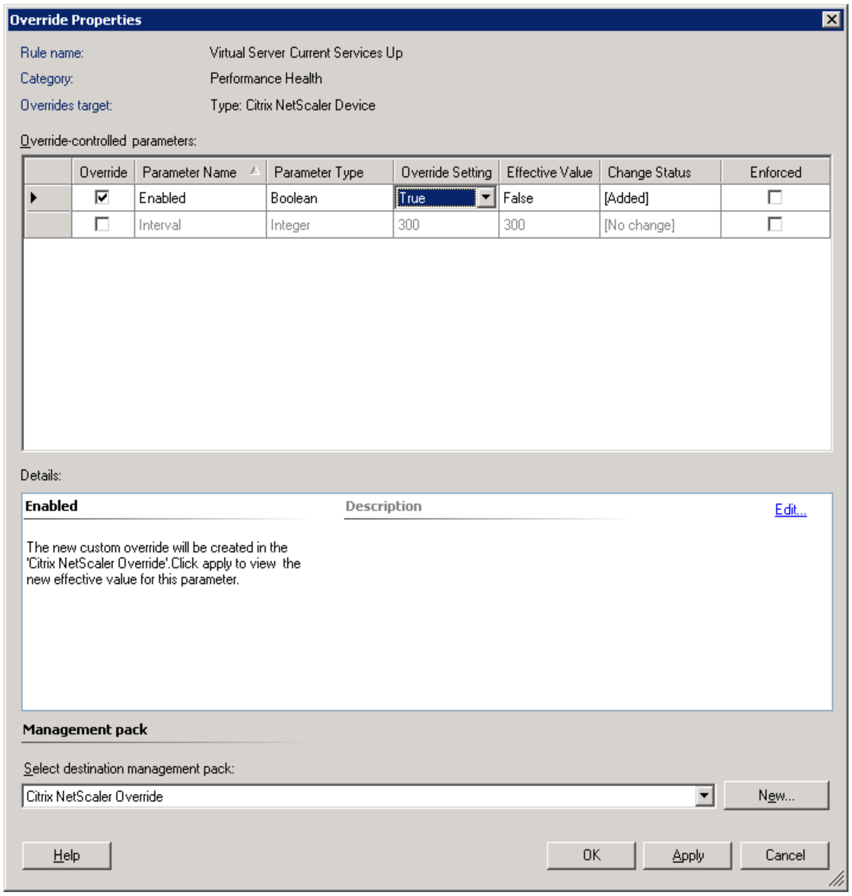
Override a performance rule to enable or disable it from polling

Citrix NetScaler Performance rules are not enabled by default. You need to enable a performance rule by setting the “Enabled” override parameter to true and/or by modifying the probe interval by setting the “Interval” override parameter.

To override a performance rule

1. In the **Rules** pane, double-click a performance rule (for example, Server Current Services Up).
2. In the **<rule name> Properties** dialog box, click the **Overrides** tab.
3. Select the **Override** button, and then select **For all objects of type: Citrix NetScaler Device**.
4. Select the destination management pack. The destination management pack should be **Citrix NetScaler Overrides**.
5. In the **Override Properties** dialog box, select the **Override** check box for the **Enabled** parameter name and under **Override Setting**, select **True**, as shown in the figure below.

   Note: Repeat the above step to modify the probe interval time.



Override Properties

Rule name: Virtual Server Current Services Up

Category: Performance Health

Overrides target: Type: Citrix NetScaler Device

Override-controlled parameters:

	Override	Parameter Name	Parameter Type	Override Setting	Effective Value	Change Status	Enforced
▶	☑	Enabled	Boolean	True	False	[Added]	□
	□	Interval	Integer	300	300	[No change]	□

Details:

Enabled

The new custom override will be created in the 'Citrix NetScaler Override'.Click apply to view the new effective value for this parameter.

Management pack

Select destination management pack: Citrix NetScaler Override

6. Click **OK**.

   Note: Repeat steps 1 through 4 for each of the performance rules you want to override.

Using the PRO Feature Solution

This section describes how to set up the security for the PRO feature, the overrides that are available, how the PRO feature works, and some troubleshooting tips.

Setting Up Security

The Citrix NetScaler Management Pack requires log on credentials of the NetScaler systems it is managing to be able to take corrective actions when the virtual servers become unhealthy.

To set up security for managing NetScaler systems

1. In the **Operations Console** click **Administration**.
2. In the **Administration** pane, under **Run As Configuration** node, right-click **Accounts**, and then select the **Create Run As Account** option.
3. In **Introduction** screen, click **Next**.
4. In **General Properties**, in **Run as Account Type**, select **Simple Authentication**.
5. In **Display name** and **Description**, type a name and description, and then click **Next.**
6. In **Credentials**, in **Account name**, type the NetScaler log on user name and in **Password***,* type the password.
7. In **Confirm Password** field, type the password again, and then click **Create**.
8. In **Distribution Security**, select **More Secure**, and then click **Create** and click **Close**. The account is displayed under **Type: Simple Authentication** view in the right pane.
9. Click **Profiles** view, and then double-click **Citrix NetScaler PRO Authentication Account**.
10. In **Introduction** screen, click **Next**.
11. In **Run As Accounts** screen, select the account you created in the previous steps, and then click **Save** and click **Close**.

    The security setup is complete.

Overrides Available for Customizations

This section describes the overrides available at discovery, monitor, and recovery configurations, and also the steps you need to perform to override the discovery, monitor, and recovery classes. Note that, all the overrides mentioned below are **mandatory** for the proper functioning of the MP.

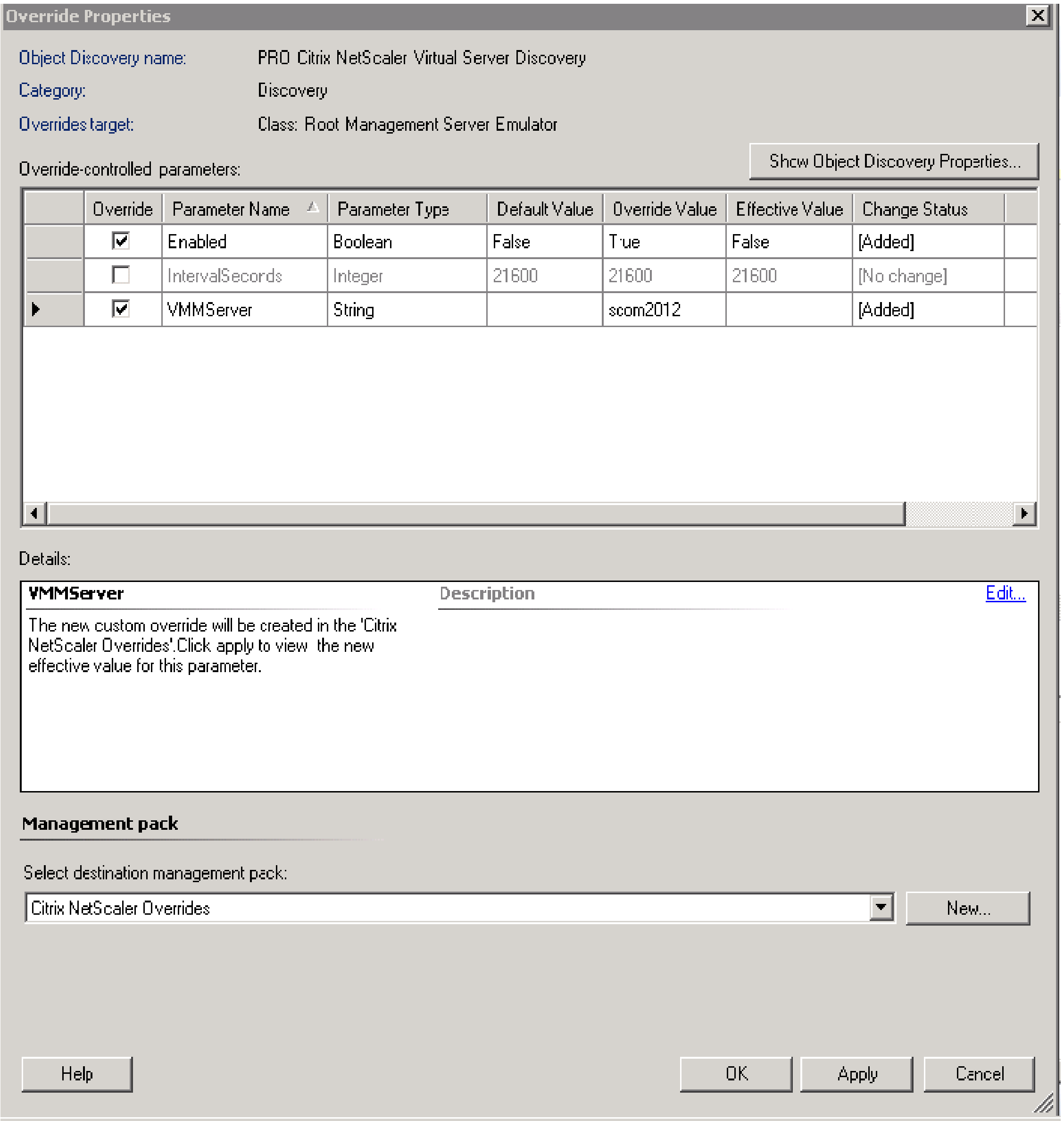
Overrides Defined at PRO Citrix NetScaler Virtual Server Discovery

Following are the overrides defined at the discovery level:

- **IntervalSeconds**: Define NetScaler device discovery interval. The default interval is 6 hours (21600 seconds).
- **VMMServer**: Specify the host name of the Virtual Machine Machine (VMM) server which would receive the PRO tip and also initiate corrective actions once a PRO tip is generated.

To override the discovery class

1. Create a management pack to store the overrides. For information on the steps to create a management pack, see Create a management pack to store the override settings.
2. In the left pane, click the **Authoring** pane.
3. In the **Authoring** window, in the left pane, under **Management Pack Objects**, click **Object Discoveries**.
4. In the **Object Discoveries** pane, click **Change Scope** (on the top right corner).
5. In the **Scope Management Pack Objects** dialog box, in **Look for**, type **Citrix**.
6. Select **View all targets**, and then from the **Targets** list, select **PRO Citrix NetScaler Virtual Server Target**.
7. Click **OK**.
8. In the **Object Discoveries** pane, under **PRO Citrix NetScaler Virtual Server Target**, double-click **PRO Citrix NetScaler Virtual Server Discovery**.
9. In the **<discovery object name> Properties** dialog box, click the **Overrides** tab.
10. Select the **Override** button, and then select **For all objects of class: Root management Server**.
11. In the **Override Properties** dialog box, select the **Override** check box for the **Enabled** parameter name and under **Override Setting**, select **True**, as shown in the figure below.



Object Discovery name: PRO Citrix NetScaler Virtual Server Discovery

Category: Discovery

Overrides target: Class: Root Management Server Emulator

Override-controlled parameters:

	Override	Parameter Name	Parameter Type	Default Value	Override Value	Effective Value	Change Status
	☑	Enabled	Boolean	False	True	False	[Added]
	☐	IntervalSeconds	Integer	21600	21600	21600	[No change]
▶	☑	VMMServer	String		scom2012		[Added]

Details:

VMMServer

The new custom override will be created in the 'Citrix NetScaler Overrides'.Click apply to view the new effective value for this parameter.

Management pack

Select destination management pack: Citrix NetScaler Overrides

12. Click **OK**.

Overrides Defined at PRO Deteriorating Virtual Server Health Monitor

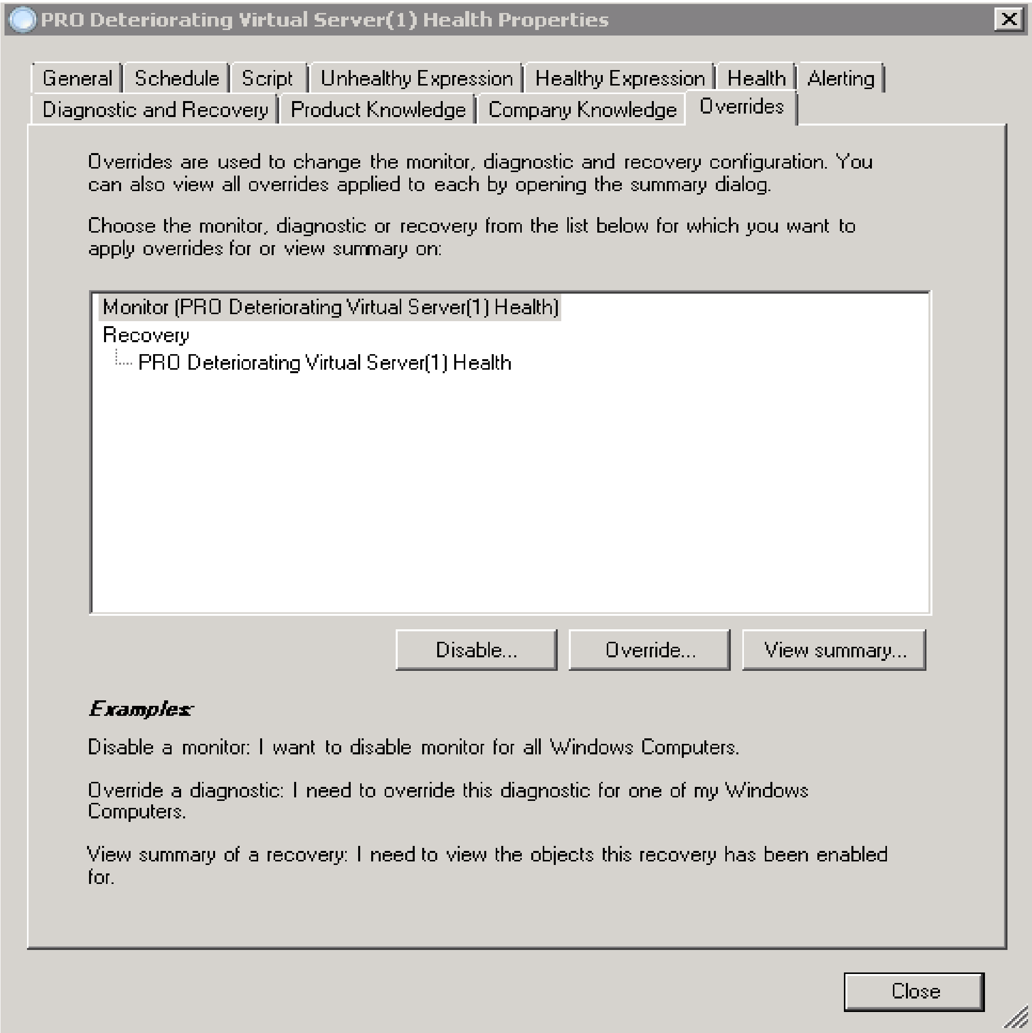
Following are the overrides defined at the monitor level:

- **NetScalerIPAddress**: Specify the IP address of the NetScaler system whose virtual server health needs to be monitored.
- **Threshold**: Define the threshold value of the virtual server health. If the polled value is less than the threshold, then a PRO tip is generated to initiate corrective action.

- **IntervalSeconds**: Define the frequency of polling the virtual server health counter.
- **Virtual Server Name**: Specify the name of the virtual server whose health needs to be monitored.

To override the monitor class

1. Create a management pack to store the overrides. For information on the steps to create a management pack, see Create a management pack to store the override settings.
2. In the left pane, click the **Authoring** pane.
3. In the **Authoring** window, in the left pane, under **Management Pack Objects**, click **Monitors**.
4. In the **Monitors** pane, click **Change Scope** (on the top right corner).
5. In the **Scope Management Pack Objects** dialog box, in **Look for**, type **Citrix**.
6. Select **View all targets**, and then from the **Target** list, select **PRO Citrix NetScaler Virtual Server Target**.
7. Click **OK**.
8. In the **Monitors** pane, expand the **PRO Citrix NetScaler Virtual Server Target** node, and then under **Peformance** subnode, double-click **PRO Deteriorating Virtual Server Health (1-5) Monitor**.
9. In the **<monitor name> Properties** dialog box, click the **Overrides** tab.
10. Select **Monitor** as shown in the figure below, click **Override** and then select **For all objects of class: PRO Citrix NetScaler Virtual Server Target**.
    Choose Monitor, Diagnostic, or Recovery from the list for which you want to apply overrides or view the summary.



PRO Deteriorating Virtual Server(1) Health Properties

Overrides are used to change the monitor, diagnostic and recovery configuration. You can also view all overrides applied to each by opening the summary dialog.

Choose the monitor, diagnostic or recovery from the list below for which you want to apply overrides for or view summary on:

Monitor (PRO Deteriorating Virtual Server(1) Health)
Recovery
PRO Deteriorating Virtual Server(1) Health

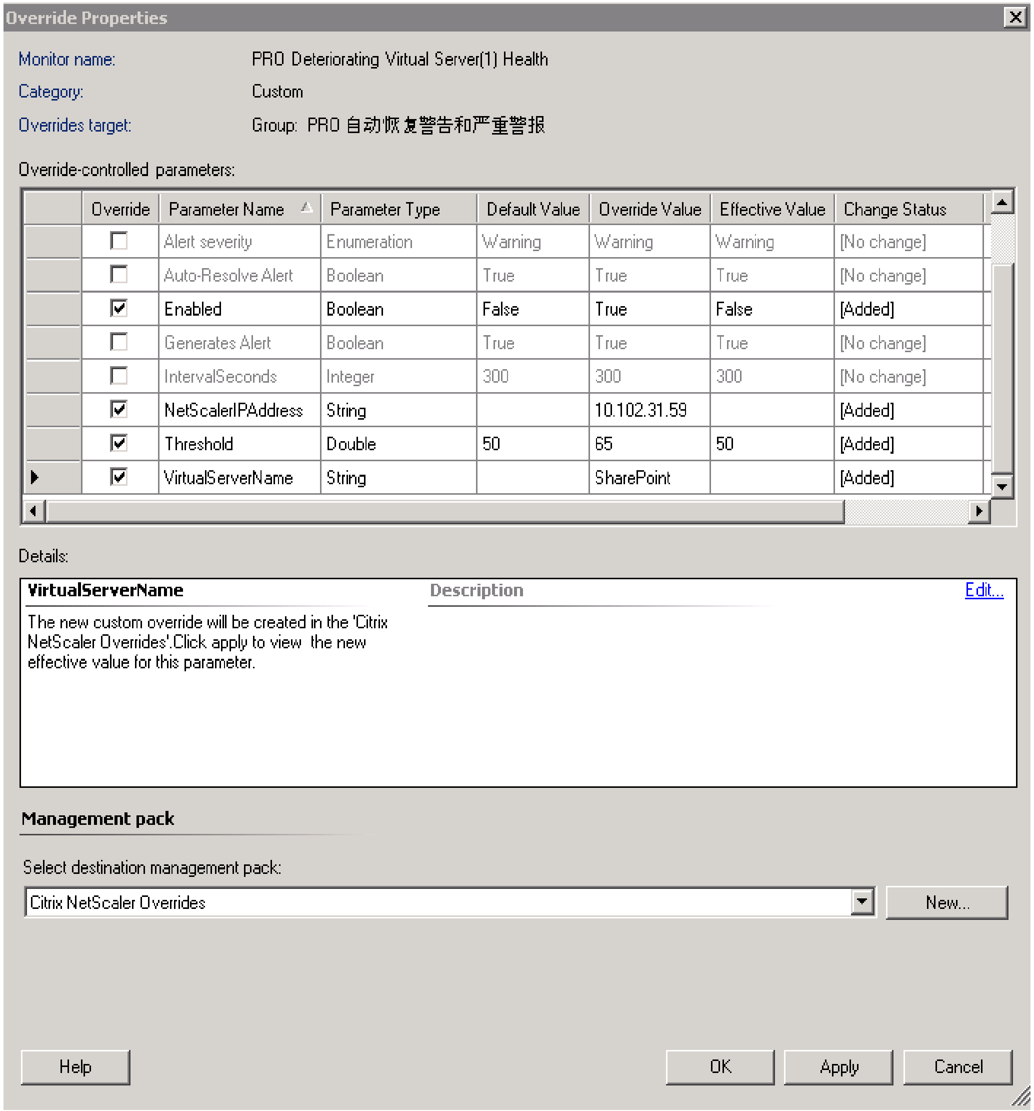
Examples:

Disable a monitor: I want to disable monitor for all Windows Computers.

Override a diagnostic: I need to override this diagnostic for one of my Windows Computers.

View summary of a recovery: I need to view the objects this recovery has been enabled for.

11. In the **Override Properties** dialog box, select the **Override** check box for the **Enabled** parameter name, and under **Override Setting**, select **True**, as shown in the figure below.



Override Properties

Monitor name: PRO Deteriorating Virtual Server(1) Health

Category: Custom

Overrides target: Group: PRO 自动恢复警告和严重警报

Override-controlled parameters:

	Override	Parameter Name	Parameter Type	Default Value	Override Value	Effective Value	Change Status
	□	Alert severity	Enumeration	Warning	Warning	Warning	[No change]
	□	Auto-Resolve Alert	Boolean	True	True	True	[No change]
	☑	Enabled	Boolean	False	True	False	[Added]
	□	Generates Alert	Boolean	True	True	True	[No change]
	□	IntervalSeconds	Integer	300	300	300	[No change]
	☑	NetScalerIPAddress	String		10.102.31.59		[Added]
	☑	Threshold	Double	50	65	50	[Added]
▶	☑	VirtualServerName	String		SharePoint		[Added]

Details:

VirtualServerName

The new custom override will be created in the 'Citrix NetScaler Overrides'.Click apply to view the new effective value for this parameter.

Management pack

Select destination management pack: Citrix NetScaler Overrides

12. Click **OK**.

Overrides Defined at VirtualServerHealth Recovery

Following are the overrides defined at the recovery level:

- **HyperVHostname**: Specify the host name of the HyperV system into which a VM needs to be provisioned as part of corrective action.
- **Protocol**: Specify the protocol of service which will be configured on the NetScaler system as part of the corrective action. This usually should be same as the protocol of the virtual vserver that is being monitored by the management pack. The default protocol is SSL.

- **Port**: Specify the port of the service to be configured on the NetScaler system. The default port is 443.

- **LibraryServer**: Specify the host name of the library server that contains the VMs that need to be deployed in the HyperV host.

To override the recovery class

1. Create a management pack to store the overrides. For information on the steps to create a management pack, see Create a management pack to store the override settings.

2. In the left pane, click the **Authoring** pane.

3. In the **Authoring** window, in the left pane, under **Management Pack Objects**, click **Monitors**.

4. In the **Monitors** pane, click **Change Scope** (on the top right corner).

5. In the **Scope Management Pack Objects** dialog box, in **Look for**, type **Citrix**.

6. Select **View all targets**, and then from the **Target** list, select **PRO Citrix NetScaler Virtual Server Target**.

7. Click **OK**.

8. In the **Monitors** pane, expand the **PRO Citrix NetScaler Virtual Server Target** node, and then under **Peformance** subnode, double-click **PRO Deteriorating Virtual Server(1-5) Health Monitor**.

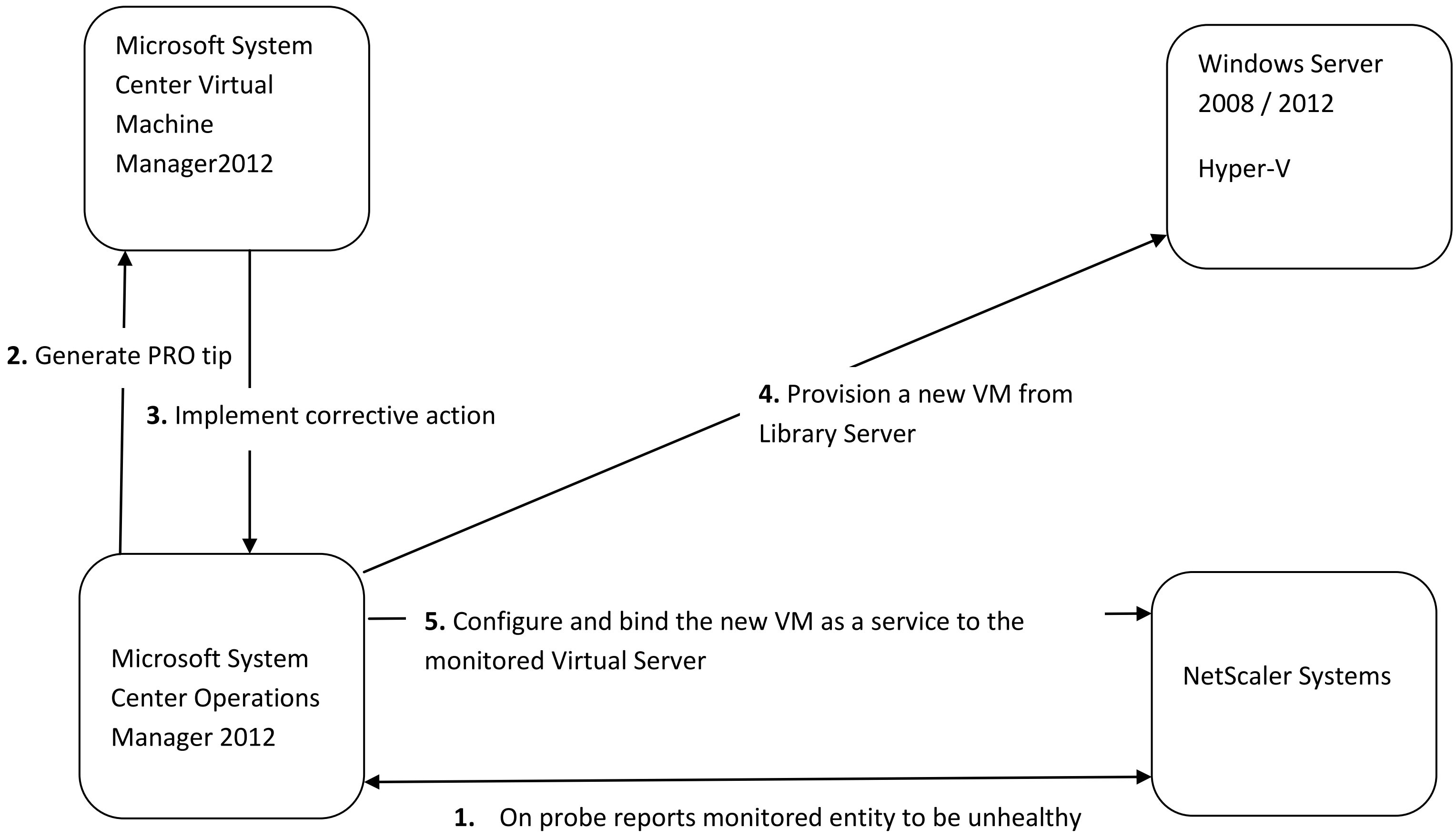
9. In the **<monitor name> Properties** dialog box, click the **Overrides** tab.

10. Select **Recovery**, click **Override** and then select **For all objects of class: PRO Citrix NetScaler Virtual Server Target**.

11. In the **Override Properties** dialog box, select the **Override** check box for the **Enabled** parameter name, and under **Override Setting**, select **True**.

12. Click **OK**.

How it Works


Microsoft System Center Virtual Machine Manager2012
Windows Server 2008 / 2012
Hyper-V
2. Generate PRO tip
3. Implement corrective action
4. Provision a new VM from Library Server
5. Configure and bind the new VM as a service to the monitored Virtual Server
Microsoft System Center Operations Manager 2012
NetScaler Systems
1. On probe reports monitored entity to be unhealthy

The following steps describe how the MP solution works:

1. At the configured poll interval, the PRO MP polls and compares the value of the virtual server's health counter with that of the threshold value. If the polled value is less than the configured threshold value, it generates a warning alert.

2. This warning alert triggers a PRO tip to be generated in the VMM PRO console.

3. On clicking the **Implement** button in the PRO window in the VMM console, corrective actions per definition in the PRO MP are initiated.

4. The first step of corrective action is to provision a VM from the defined Library Sever. This step deploys a VM available in the library Server on the HyperV host.

5. After Step 4 is complete, the MP picks the computer name of the provisioned VM and resolves it to its IP address. It is mandatory that the computer name of the new VM resolves to a proper IP address for the corrective action to be fully functional.

6. After Step 5 is complete, the next probe for the health of the monitored virtual server should become healthy with new service bound to it. For proper functioning of the MP, ensure that the overrides as mentioned in the section Override MP for Customizations are defined properly.

Troubleshooting

All the error messages are logged in the Applications node of the Windows Event Viewer. Check for error messages, if any, under *CitrixNetScalerPRO* category and resolve issues accordingly. PRO-related error message is displayed in the PRO window. Sample error messages are:

Hyper-V Host Name is empty

Resolution: Override the HyperVHostname property. Refer Overrides section above for more details.

VMM Server Name is empty

Resolution: Override the VMMServer Name property. Refer Overrides section above for more details.

Known Issue

PRO-Tip is not generated for PRO Warning & Critical Alert.

Appendix

This appendix describes the supported traps and performance counters.

Supported Traps

The following table describes the supported traps, their descriptions, and their severity levels.

Trap	Description	Severity
changeToPrimary	This trap indicates that the NetScaler is now operating in the primary mode.	Critical
changeToSecondary	This trap indicates that the NetScaler is now operating in the Secondary mode.	Critical
cpuUtilization	This trap indicates that the CPU utilization has exceeded the high threshold	Critical
entitydown	This trap is sent when the state of interface, vserver or physicalservice changed to DOWN	Critical
entityup	This trap is sent when the state of interface, vserver or physicalservice changed to UP	Information
synflood	This trap is sent when the rate at which unacknowledged SYNs are received cross a threshold value	Critical
cpuUtilizationNormal	This trap indicates that the CPU utilization has come back to normal	Information
synfloodNormal	This trap is sent when the rate at which unacknowledged SYNs are received returns to normal	Information
memoryUtilization	This trap is sent when the memory utilization of the system exceeds the threshold value	Critical
memoryUtilizationNormal	This trap is sent when the memory utilization of the system returns to normal	Information
vServerRequestRate	This trap is sent when the request rate on a vserver exceeds a threshold value	Critical

vServerRequestRateNormal	This trap is sent when the request rate on a vserver returns to normal	Information
serviceRequestRate	This trap is sent when the request rate on a service exceeds a threshold value	Critical
serviceRequestRateNormal	This trap is sent when the request rate on a service returns to normal	Information
netScalerConfigChange	This trap is sent when the configuration on the NetScaler is changed	Warning
maxClients	This trap is sent when the number of clients hits the maxClients value for a service	Critical
maxClientsNormal	This trap is sent when the number of clients falls below 70% of maxClients value for a service	Information
netScalerConfigSave	This trap is sent when the configuration on the NetScaler is saved.	Warning
serviceRxBytesRate	This trap is sent when the request byte(s) of a service exceeds a threshold value.	Critical
serviceRxBytesRateNormal	This trap is sent when the request byte(s) of a service returns to normal.	Information
vserverRxBytesRate	This trap is sent when the request byte/s of a vserver exceeds a threshold value.	Critical
vserverRxBytesRateNormal	This trap is sent when the request byte(s) of a vserver returns to normal.	Information
serviceTxBytesRate	This trap is sent when the response byte(s) of a service exceeds a threshold value.	Critical
serviceTxBytesRateNormal	This trap is sent when the response byte(s) of a service returns to normal	Information
vserverTxBytesRate	This trap is sent when the response byte(s) of a vserver exceeds a threshold value	Critical

vserverTxBytesRateNormal	This trap is sent when the response byte(s) of a vserver returns to normal	Information
serviceSynfloodRate	This trap is sent when the number of unacknowledged syns for a service exceeds a threshold value	Critical
serviceSynfloodNormal	This trap is sent when the number of unacknowledged syns for a service returns to normal	Information
vserverSynfloodRate	This trap is sent when the number of unacknowledged syns for a vserver exceeds a threshold value	Critical
vserverSynfloodNormal	This trap is sent when the number of unacknowledged syns for a vserver returns to normal	Information
svcGroupMemberRequestRate	This trap is sent when the request rate on a service group member exceeds a threshold value	Critical
svcGroupMemberRequestRateNormal	This trap is sent when the request rate on a service group member returns to normal	Information
svcGroupMemberRxBytesRate	This trap is sent when the request byte(s) of a service group exceeds a threshold value	Critical
svcGroupMemberRxBytesRateNormal	This trap is sent when the request byte(s) of a service group returns to normal	Information
svcGroupMemberTxBytesRate	This trap is sent when the response byte(s) of a service group exceeds a threshold value	Critical
svcGroupMemberTxBytesRateNormal	This trap is sent when the response byte(s) of a service group returns to normal.	Information
svcGroupMemberSynfloodRate	This trap is sent when the number of unacknowledged syns for a service group exceeds a threshold value	Critical
svcGroupMemberSynfloodNormal	This trap is sent when the number of unacknowledged syns for a service group	Information

	returns to normal	
svcGroupMemberMaxClients	This trap is sent when the number of clients hits the maxClients value for a service group member	Critical
svcGroupMemberMaxClientsNormal	This trap is sent when the number of clients falls below 70% of maxClients value for a service group member	Information
averageCpuUtilization	This trap indicates that the average CPU usage in the multi-processor NetScaler system has exceeded the highthreshold.	Critical
averageCpuUtilizationNormal	This trap indicates that the average CPU usage in the multi-processor NetScaler system has come back to normal	Information
monRespTimeoutAboveThresh	This trap is sent when the response timeout for a monitor probe exceeds the configured threshold	Critical
monRespTimeoutBelowThresh	This trap is sent when the response timeout for a monitor probe comes back to normal, less than the threshold set	Information
netScalerLoginFailure	This trap is sent when a login attempt to the NetScaler fails.	Critical
sslCertificateExpiry	This trap is sent as an advance notification when an SSL certificate is due to expire	Critical
fanSpeedLow	This trap indicates that a fan speed has gone below an alarm threshold.	Critical
fanSpeedNormal	This trap indicates that a fan speed has returned to normal	Information
voltageLow	This trap indicates that a voltage has gone low	Critical
voltageNormal	This trap indicates that a voltage has returned to normal	Information
voltageHigh	This trap indicates that a voltage has gone	Critical

	high	
temperatureHigh	This trap indicates that a temperature has gone high.	Critical
temperatureNormal	This trap indicates that a temperature has returned to normal.	Information
diskUsageHigh	This trap indicates that disk usage has gone high	Critical
diskUsageNormal	This trap indicates that disk usage has returned to normal	Information
interfaceThroughputLow	This trap indicates that interface throughput is low	Critical
interfaceThroughputNormal	This trap indicates that interface throughput has returned to normal	Information
HAVersionMismatch	This trap indicates that there is a mismatch in the OS version of the NetScalers participating in HA	Warning
HASyncFailure	This trap indicates that config synchronization has failed on secondary	Warning
HANoHeartBeats	This trap indicates that HA heartbeats are not received from the secondary	Warning
HABadSecState	This trap indicates that the secondary is in DOWN/UNKNOWN/STAY SECONDARY state	Warning
entityofs	This trap is sent when the state of entities such as vserver, physicalservice, or servicegroup changes to OUT OF SERVICE	Critical
interfaceBWUseHigh	This trap is sent when the bandwidth usage of any of the interfaces of the system exceeds the threshold value (configured in Mbits/second)	Warning
interfaceBWUseNormal	This trap is sent when the bandwidth usage of any of the interfaces of the system returns to	Information

	normal	
aggregateBWUseHigh	This trap is sent when the aggregate bandwidth usage of the system exceeds the threshold value (configured in Mbits/second)	Warning
aggregateBWUseNormal	This trap is sent when the aggregate bandwidth usage of the system returns to normal	Information
vserverRhiStateChange	This trap is sent when the vserver RHI state changes	Critical
rateLmtThresholdExceed	This trap is sent when the client exceeds the ratelimit threshold	Critical
monProbeFailed	This trap is sent when the monitor probe fails for configured number of retries in given max retries attempts	Critical
temperatureCpuHigh	This trap indicates that a CPU temperature has gone high	Warning
temperatureCpuNormal	This trap indicates that a CPU temperature has returned to normal	Information
powerSupplyFailed	This trap is sent when power supply has failed or disconnected from the system	Warning
powerSupplyNormal	This trap is sent when power supply status returned back to normal	Information
entityNameChanged	This trap is sent when vserver/service/sgroup/lbgroup/server entity is renamed.	Critical
haPropFailure	This trap indicates that config propagation has failed on secondary.	Critical
ipConflict	This trap indicates that an IP conflict exists with another device in the network.	Critical
appfwStartUrl	This trap indicates that AppFirewall Start URL violation occurred.	Critical

appfwDenyUrl	This trap indicates that AppFirewall Deny URL violation occurred.	Critical
appfwRefererHeader	This trap indicates that AppFirewall Referer Header violation occurred.	Critical
appfwCSRFTag	This trap indicates that AppFirewall CSRF Tag violation occurred.	Critical
appfwCookie	This trap indicates that AppFirewall Cookie violation occurred.	Critical
appfwFieldConsistency	This trap indicates that AppFirewall Field Consistency violation occurred.	Critical
appfwBufferOverflow	This trap indicates that AppFirewall Buffer Overflow violation occurred.	Critical
appfwFieldFormat	This trap indicates that AppFirewall Field Format violation occurred.	Critical
appfwSafeCommerce	This trap indicates that AppFirewall Safe Commerce violation occurred.	Critical
appfwSafeObject	This trap indicates that AppFirewall Safe Object violation occurred.	Critical
appfwPolicyHit	This trap indicates that AppFirewall Policy Hit occurred.	Critical
appfwXSS	This trap indicates that AppFirewall Cross-Site Scripting violation occurred.	Critical
appfwXMLXSS	This trap indicates that AppFirewall XML Cross-Site Scripting violation occurred.	Critical
appfwSQL	This trap indicates that AppFirewall SQL violation occurred.	Critical
appfwXMLSQL	This trap indicates that AppFirewall XML SQL violation occurred.	Critical
appfwXMLAttachment	This trap indicates that AppFirewall XML Attachment violation occurred.	Critical

appfwXMLDos	This trap indicates that AppFirewall XML DoS violation occurred.	Critical
appfwXMLValidation	This trap indicates that AppFirewall XML Validation violation occurred.	Critical
appfwXMLWSI	This trap indicates that AppFirewall XML WSI violation occurred.	Critical
appfwXMLSchemaCompile	This trap indicates that AppFirewall XML Schema Compile violation occurred.	Critical
appfwXMLSoapFault	This trap indicates that AppFirewall XML Soap Fault violation occurred.	Critical

Supported Performance Counters

The following table lists the supported performance counters:

Counter Group	**Counters**
ACL Table	• ACL Table Acl Hits • ACL Table Acl Priority
App Firewall	• App Firewall Start URL Violations • App Firewall Field Consistency Violations • App Firewall SQL Violations • App Firewall Requests Redirected (HTTP 302) • App Firewall Cross-site Scripting Violations • App Firewall Cookie Violations • App Firewall Requests Received • App Firewall Buffer Overflow Violations • App Firewall Requests Aborted • App Firewall Responses Handled • App Firewall Credit Card Violations • App Firewall Deny URL Violations • App Firewall Safe Object Violations • App Firewall Total Number of Violations • App Firewall field format Violations
Compression	• Compression ratio(Percentage) • Compression success ratio(Percentage)
Content Filte	Content Filters Hits

GSLB	• GSLB Custom Entries • GSLB Static Entries
HTTP	• HTTP Large/invalid chunk requests • HTTP Incomplete request headers • HTTP Incomplete HTTP headers • HTTP Incomplete response headers • HTTP Large/invalid requests • HTTP More than content length data • HTTP Server BUSY responses (500) • HTTP/1.1 pipeline requests
ICache	• ICache Hit ratio(Percentage) • ICache Recent 304 hit ratio(Percentage) • ICache Successful reval ratio(Percentage) • ICache Parameterized 304 hit ratio(Percentage) • ICache Hits being served • ICache 304 hit ratio(Percentage) • ICache Utilized memory(KB) • ICache Storable miss ratio(Percentage) • ICache Recent parameterized 304 hit ratio(Percentage) • ICache Cached objects • ICache Recent storable miss ratio(Percentage) • ICache Poll every time hit ratio(Percentage) • ICache Recent successful reval ratio(Percentage) • ICache Misses being handled • ICache Maximum memory(KB) • ICache Recent origin bandwidth saved(Percentage) • ICache Recent hit ratio(Percentage) • ICache Origin bandwidth saved(Percentage) • ICache Memory allocation failures • ICache Largest response so far(B) • ICache Byte hit ratio(Percentage) • ICache Recent byte hit ratio(Percentage)
ICMP	• ICMP packets dropped • ICMP Rate Threshold • ICMP rate threshold exceeded
Interface	• Interface Tx late collisions • Interface Tx collisions • Interface Rx Average bandwidth(bits/sec) • Interface Rx Average packet rate • Interface Tx excess collisions • Interface Tx multiple collision errors • Interface Tx Average bandwidth(bits/sec) • Interface Rx alignment errors • Interface Rx CRC errors

	• Interface Tx Carrier errors • Interface Rx Frame errors • Interface Tx Average packet rate
IP	• IP Packets with len > 1514 rcvd • IP max non-TCP clients • IP fragments received • IP Packets with bad MAC sent • IP Unknown services • IP land-attacks
Resource	• Resources CPU Usage(Percentage) • Resources Memory Usage(Percentage)
Service	• Services Genuine clients on this service • Services Maximum requests per connection • Services Javascripts sent to genuine clients • Services Active connections • Services State • Services Established connections • Services Surge count • Services Average transaction time • Services Type
SSL	• SSL Engine Status • SSL Crypto Card Status • SSL Current SSL sessions
Sure Connect	• Sure Connect Threshold conditions failed • Sure Connect URL hits • Sure Connect POST requests • Sure Connect Requests in SureConnect session • Sure Connect Requests from unsupported browsers • Sure Connect Alternate content hits • Sure Connect Delay stats reset • Sure Connect Corrupted SureConnect cookies • Sure Connect In-memory pop-up screen hits
TCP	• TCP Spare Connections • TCP All Client Connections • TCP current pending connections • TCP Server Active Connections • TCP Opening Client Connections • TCP Closing Server Connections • TCP Opening Server Connections • TCP Rejected TCP SYN cookie packets (Bad Signature) • TCP Closing Client Connections • TCP Established Client Connections • TCP Established Server Connections • TCP Current Physical servers with open cons

	• TCP All Server Connections • TCP Surge Queue • TCP Rejected TCP SYN cookie packets (Bad Seq No)
UDP	• UDP Rate Threshold • UDP unknown service errors • UDP packet rate threshold
Virtual Server	• Virtual Server Total Vserver Misses • Virtual Server Maximum requests per connection • Virtual Server Current server connections • Virtual Server Current Services UnKnown • Virtual Server Type • Virtual Server Current Services Down • Virtual Server Services Transition to Out of Svc • Virtual Server State • Virtual Server Current Services Up • Virtual Server Current client connections • Virtual Server Services Out of Svc
VLAN	• VLAN Broadcast pkts sent and received • VLAN Packets dropped
Virtual Server Service	• Virtual ServerService Persistent Hits • Virtual ServerService Weight
Virtual Server Cache Redirection Policy	Cache Redirection Policies Policy Hits
ACL6	• Acl6 Total Packets Bridged • Acl6 Total Packets Denied • Acl6 Total Packets Allowed • Acl6 Total Packets NAT • Acl6 Total Hits • Acl6 Total Misses • Acl6 per Hits • Acl6 Priority
Simple ACL	• SimpleACL Total Packets Bridged • SimpleACL Total Packets Denied • SimpleACL Total Packets Allowed • SimpleACL Total Hits • SimpleACL Tottal Misses • SimpleACL Count
App Firewall Profile	• App Firewall Requests Per Profile • App Firewall Responses Per Profile • App Firewall Aborts Per Profile • App Firewall Redirects Per Profile • App Firewall Viol Start URL Per Profile • App Firewall Viol Deny URL Per Profile

	• App Firewall Viol Referer Header Per Profile • App Firewall Viol Buffer Overflow Per Profile • App Firewall Viol CSRFtag Per Profile • App Firewall Viol Cookie Per Profile • App Firewall Viol XSS Per Profile • App Firewall Viol SQL Per Profile • App Firewall Viol Field format Per Profile • App Firewall Viol Field Consistency Per Profile • App Firewall Viol Credit Card Per Profile • App Firewall Viol Safe Object Per Profile • App Firewall Viol Wellformedness Violations Per Profile • App Firewall Viol Xdos Violations Per Profile • App Firewall Viol Msg Val Violations Per Profile • App Firewall Viol WSI Violations Per Profile • App Firewall Viol Xml Sql Violations Per Profile • App Firewall Viol Xml Xss Violations Per Profile • App Firewall Viol XmlAttachment Violations Per Profile • App Firewall Total Viol Per Profile • App Firewall Ret4xx Per Profile • App Firewall Ret5xx Per Profile • App Firewall Viol XmlSoap Fault Violations Per Profile • App Firewall Req Bytes Per Profile • App Firewall Res Bytes Per Profile • App Firewall Long Avg Resp Time Per Profile • App Firewall Short Avg Resp Time Per Profile