

Guide for Microsoft Windows Server 2016 SDN Management Pack for System Center Operations Manager

Published: September 2016

Send suggestions and comments about this document to mpgfeed@microsoft.com. Please include the monitoring pack guide name with your feedback.

We encourage you to provide feedback on the management pack by providing a review on the management pack’s page in the [Management Pack Catalog](http://go.microsoft.com/fwlink/?LinkID=82105) (http://go.microsoft.com/fwlink/?LinkID=82105).

Copyright

This document is provided "as-is". Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Some examples depicted herein are provided for illustration only and are fictitious.  No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. You may modify this document for your internal, reference purposes.

© 2011 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Windows, and Windows Server are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Abstract

Microsoft Windows Server 2016 SDN Management Pack for System Center Operations Manager helps you monitor the health and availability of computers configured for Windows Server 2016 Software Defined Networks. This guide describes how to install the System Center Monitoring Pack for Windows server 2016 SDN.

The information that is contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

Contents

[Guide for System Center Monitoring Pack for Multi-tenant Remote Access 5](#_Toc381635103)

[Guide History 5](#_Toc381635104)

[Supported Configurations 5](#_Toc381635105)

[Files in this Monitoring Pack 5](#_Toc381635106)

[Monitoring Pack Purpose 5](#_Toc381635107)

[Getting the Latest Management Pack and Documentation 6](#_Toc381635108)

[Pre-requisites for importing Routing and Remote Access Service Management Pack 6](#_Toc381635109)

[How to Import the Routing and Remote Access Service Management Pack 6](#_Toc381635110)

[Create a New Management Pack for Customizations 6](#_Toc381635111)

[Security Considerations 7](#_Toc381635112)

[Discovered Objects 7](#_Toc381635113)

[How Health Rolls Up 8](#_Toc381635114)

[Monitoring 10](#_Toc381635115)

[Pre-requisites for Monitoring Multi-tenant RRAS in Clustering Environment 10](#_Toc381635116)

[Monitors and Alarms 11](#_Toc381635117)

[Performance Monitoring Scenarios 14](#_Toc381635118)

[Event Monitoring Scenarios 17](#_Toc381635119)

[Placing Monitored Objects in Maintenance Mode 21](#_Toc381635120)

# Guide for System Center Monitoring Pack for Windows Server 2016 Software Defined Networking

This guide was written based on version 1.0.0.0 of the Monitoring pack for Microsoft Windows Server 2016 SDN.

## Guide History

| **Release Date** | **Changes** |
| --- | --- |
| October 2016 | Original release of this guide |

## Supported Configurations

This management pack requires System Center Operations Manager 2012 R2 or later.

The following table details the supported configurations for the Monitoring pack for Windows Server 2016 SDN:

| **Configuration** | **Support** |
| --- | --- |
| Windows Server 2016 Network Controller | Yes |
| Windows Server 2016 Remote Access  | Yes |

## Files in this Monitoring Pack

The Monitoring Pack includes the following files:

 License Agreement

 Microsoft.Windows.10.SDNMonitoring.Images.mp

* Microsoft.Windows.10.SDNMonitoring.mp

## Monitoring Pack Purpose

The System Center Monitoring Pack for Windows Server 2016 SDN helps you monitor the health and availability of Windows Server 2016 SDN infrastructure components and tenant resources on computers running Windows Server 2016.

This guide describes how to install the Microsoft Windows Server 2016 SDN Management Pack for System Center Operations Manager in Microsoft® System Center Operations Manager 2012 R2 (Operations Manager 2012 R2) or later. The hosts must be running Windows Server 2016.

The management pack provides a predefined, ready-to-run set of processing rules, alarms, monitors, and performance instrumentation that are designed to monitor Windows Server 2016 SDN components. Primarily SDN components are monitored by calling into REST APIs using SDN Network Controller PowerShell. Additionally, some monitors for the gateway component of SDN requires it to be either agentless or agent managed.

This guide provides information about the most common monitoring scenarios, monitor definitions, tasks, and views for Windows Server 2016 SDN components. This guide also includes instructions for deploying and operating the management pack.

## Getting the Latest Management Pack and Documentation

You can find the System Center Monitoring Pack for SDN in the [System Center Operations Manager Marketplace](http://systemcenter.pinpoint.microsoft.com/en-US/home) (<http://systemcenter.pinpoint.microsoft.com/en-US/home>).

## Pre-requisites for importing Windows Server 2016 SDN Management Pack

This management pack has dependencies on Windows Server 2016 Discovery and Windows Server Library management packs. You need to install these management packs before installing Windows Server 2016 SDN Management Pack.

The Network Controller uses an X.509 Certificate to secure the REST API and optionally (with System Center Virtual Machine Manager) Kerberos for authentication. As such, the Network Controller’s REST Endpoint Certificate (public-key only) must be installed on the SCOM machine in the localmachine’s root store. Also, the SCOM user must be added to the Network Controller Management security group.

The Network Controller nodes must be added as “Agentless” computers to SCOM before importing the SDN Monitoring Pack.

## How to Import the Windows Server 2016 SDN Management Pack

For instructions about importing a management pack, see [How to Import a Management Pack in Operations Manager 2012 R2](http://technet.microsoft.com/en-us/library/hh212691.aspx) (<http://technet.microsoft.com/en-us/library/hh212691.aspx>).

## Create a New Management Pack for Customizations

Most vendor management packs are sealed so that you cannot change any of the original settings in the management pack file. However, you can create customizations, such as overriding a default behavior or creating new monitoring objects, and then save them to a different management pack. By default, Operations Manager 2016 saves all customizations to the default management pack. As a best practice, you should instead create a separate management pack for each sealed management pack that you want to customize.

Creating a new management pack for storing overrides has the following advantages:

 It simplifies the process of exporting customizations that were created in your test and preproduction environments to your production environment. For example, instead of exporting a default management pack that contains customizations from multiple management packs, you can export just the management pack that contains customizations of a single management pack.

 You can delete the original management pack without needing to first delete the default management pack. A management pack that contains customizations is dependent on the original management pack. This dependency requires that you delete the management pack with customizations before you can delete the original management pack. If all of your customizations are saved to the default management pack, you must delete the default management pack before you can delete an original management pack.

 It is easier to track and update customizations to individual management packs.

For more information refer to [Creating a Management Pack for Overrides](http://technet.microsoft.com/en-us/library/hh212841) (<http://technet.microsoft.com/en-us/library/hh212841>).

## Security Considerations

You may need to customize your management pack. The management pack will execute the cmdlets exposed by the “RSAT-NetworkController” module to get configuration state? Examples:

1. Get-NetworkControllerVirtualNetwork -ConnectionUri $uri

The ‘Run As Account’ configured needs to be in the Network Controller Manager security group and have permissions on all the Remote Access Servers (SDN Gateway VMs). It is highly recommended that you use a separate security group for the accounts configured for Operations Manager 2016.

## Discovered Objects

The Windows Server 2016 SDN Management Pack discovers the object types described in the following table.

For information about discovering objects, see [Understanding Classes and Objects in System Center 2012 R2](file:///C%3A%5CUsers%5Csankasat%5CDocuments%5CUnderstanding%20Classes%20and%20Objects%20in%20System%20Center%202012%20R2) (<http://technet.microsoft.com/en-us/library/hh457568>) in Operations Manager 2012 R2 Help.

| **Category** | **Object Type** | **Discovered Automatically** |
| --- | --- | --- |
| Network Controller Stamp | * Network Controller Cluster (This is a singleton object, i.e. on MP will detect and manage only one cluster)
 | Yes (every 24 hours) |
| Network Controller Nodes | * Network Controller Node
 | Yes |
| Discovers Gateways | * Gateway Pool
* Gateway
 | Yes (every 4 hours) |
| Discovers Virtual Gateways | * Virtual Gateway
* Network Connection
* BGP Router
* BGP Peer
 | Yes (every 4 hours) |
| Access Control Lists | * Network Controller resource
 | Yes |
| Host Groups / Servers | * Network Controller resource which represents a physical server
 | Yes |
| Network Interfaces | * Network Controller resource which represents a VM NIC
 | Yes |
| Virtual Networks | * Network Controller resource which represents a tenant virtual network
 | Yes |
| Software Load Balancer (SLB) Muxes | * Network Controller resource which represents a Software Load Balancer Mux VM
 | Yes |

All the discoveries are PowerShell based. If the environment is Domain-Joined and using Kerberos authentication it will automatically detect the Network Controller Stamp. However, if the environment is using X.509 certificates for WinRM connectivity then the SCOM administrator must provide a certificate which can be used to connect to the Network Controller machine. This is an overridable parameter named CertificateThumbPrint under SDNMonitoringMP.SDNMonitoring.DiscoverStamp. When you are using a wildcard-based certificate for the Network Controller REST Endpoint then you also need to provide the value of the NC REST Endpoint URI in the overridable parameter named ConnectionUri under SDNMonitoringMP.SDNMonitoring.DiscoverStamp.

## How Health Rolls Up

The class hierarchy for System Center Monitoring Pack for Windows Server 2016 SDN is shown below.



Health for each individual resource group rolls up independently to the Stamp and Stamp Group.

Health Monitors are targeted to all leaf node classes of the above hierarchy. Health is rolled up along the red arrows marked above. Health is rolled up in all four categories namely

1. Configuration
2. Availability
3. Performance
4. Security

## Monitoring

### Monitoring the Network Controller Cluster

#### Pre-requisites for Monitoring the Network Controller Cluster

If the Network Controller cluster is being monitored, the SCOM admins need to do the following steps to discover the servers:

1. Admins are required to enable Agentless monitoring for all the Network Controller nodes.
2. The “Agent Proxy” must have privileges to execute cmdlets and scripts on the NC nodes.

#### Monitors and Alarms

The Windows Server 2016 SDN Management Pack includes monitors and alarms to notify the administrator of some erroneous conditions. The following table outlines these monitors:

**Network Controller monitors:**

|  |  |
| --- | --- |
| Monitor | Description |
| Port Health Monitor | The port health monitor checks the availability of ports required by Network Controller. The firewall exceptions should be in place for the ports needed by Network Controller. No program other than the Network Controller must be using these ports. |
| OS Patch Uninstall Monitor | Network Controller maintains two versions of binaries, installed version and running version. Even when you uninstall a patch, the running version of binaries is not reverted. This will cause inconsistencies between the installed version and the running version, which can lead to issues. |
| Central Log Access Monitor | This monitors the access to the central diagnostic log location from Network Controller's windows fabric cluster. It raises an alert if the central log location where the application and cluster logs of the Network Controller are uploaded, is inaccessible from one of the windows fabric cluster. |
| Rest Service Unavailable Error Monitor | A lot of inbound REST calls have resulted into "REST service unavailable" failure. This may be due to the health of the Network Controller REST services |
| Disk Usage Monitor | This monitors the usage of the logical disks on Network Controller nodes. It raises an alert if the disk consumption on one or more logical disks of Network Controller node has gone beyond threshold. |
| Memory Usage Monitor | This monitors the usage of the physical memory on Network Controller nodes. It raises an alert if the memory consumption on Network Controller node has repeatedly gone beyond threshold. |
| Time Sync Monitor | This monitors if the server time on Network Controller nodes is in sync. |
| Diagnostic Monitor | This monitors if the Network Controller nodes could connect to diagnostic locations and whether devices could connect to diagnostic location. If either Network controller node or device cannot access diagnostic locations, it could lead to logs missing (or not uploaded properly to diagnostic locations). |
| CPU Usage Monitor | This monitors the CPU consumption of Network Controller nodes. This raises an alert if one of the processes on the Network Controller node is consuming a lot of CPU cycles. |
| SB Failure Monitor | This monitors the health of southbound connections made by the Network Controller nodes. This raises an alert if a lot of south bound calls to connect to the network devices have resulted into failures. This may be due to unavailability of the southbound devices to which connections are being made, incorrect access credentials, expired certificates or networking issues in the fabric |
| Rest Internal Server Error Monitor | This indicates the health of Network Controller REST service by monitoring the number of "REST internal server error" failures reported by the server. This raises an alert if a lot of inbound REST calls have resulted into "REST internal server error". This may be due to the health of REST service as well as the underlying network. |
| Rest Forbidden Access Error Monitor | This indicates the health of Network Controller REST service by monitoring the number of "REST forbidden access error" failures reported by the server.  |
| SSL Cert Health Monitor | This monitors the health of the SSL certificate used for authentication of REST requests. This monitor may raise an alert if the SSL certificates are not properly configured, have expired or are about to expire. |
| Node Certificate Monitor | This monitors the health of node certificate used by Network Controller nodes. This monitor may raise an alert if the NC node certificates are not properly configured, have expired or are about to expire. |
| Logman Session Health Monitor | This monitors if the logman session has been enabled on Network Controller nodes. For the application diagnostic logging the logman session must be enabled on Network Controller nodes.  |
| Winfabric Service Monitor | Network controller runs as a distributed application on a windows fabric cluster. This monitors the health of the windows fabric cluster |
| Self-Signed Cert Health Monitor | This monitors the health of the self-signed certificates used for authentication of Network Controller while communicating with a device. This monitor may raise an alert if the self-signed certificates used for authentication of Network Controller while communicating with a device are not properly configured, have expired or are about to expire. |
| Node Not Reachable After OS Upgrade Monitor | This monitors the reachability of the Network controller nodes after the manifest version has been upgraded and the running version on Network Controller binaries needs to be updated. |
| Update After OS Upgrade Monitor | This monitors the update of Network Controller running binary version. Network Controller maintains two versions of binaries, installed version and running version. When a patch is installed, the installed version of binary is updated. Then the running version of binary is updated after the patch is installed on all the nodes. |
| OS Upgrade Monitor | This monitors the OS upgrade process for Network Controller cluster. A Windows Update patch for Network Controller has not been installed on some of the Network Controller nodes. Unless all the nodes have the patch, the patch will not be applied. |

``

#### Performance Monitoring Rules

**Gateway performance counters:**

|  |  |
| --- | --- |
| **Rules** | **Description** |
| SB Failure Performance Collection Rule | This collects the details about how many southbound connection attempts made by the Network Controller resulted in failures. |
| Rest Request Performance Collection Rule | This collects the details about how many REST requests were made to the Network controller. A sudden spike may be an indicator of malicious activity. |
| CPU Usage Performance Collection Rule | This collects the details about the CPU usage on the Network Controller nodes. |
| SB Success Performance Collection Rule | This collects the details about the memory consumption on the Network Controller nodes. |
| REST Response Performance Collection Rule | This collects the details about the REST responses sent by the Network Controller. |

### Monitoring the Gateways

#### Pre-requisites for Monitoring Multi-tenant RRAS in Clustering Environment

If the Multi-tenant RRAS servers being monitored are part of a cluster, the SCOM admins need to do the following steps to discover the servers:

1. Admins are required to enable Agentless monitoring for both active and passive nodes. Open Operations Manager console and go to Administration->Device Management -> Agent Managed. Select the active and passive nodes of the RRAS cluster and click properties on the task window. In the security window, enable “Agent Proxy” by checking the “Allow this agent to act as proxy and discover managed objects on other computers” check box. Click Ok.
2. Admins should over-ride Clustering MP for discovering RRAS Cluster. Open Operations Manager console and go to Authoring->Object discoveries. Search for “Windows Clustering Discovery” and right click to Overrides->Override the Object Discovery->”For all the objects of class Windows cluster Service (For Virtual Server)”. In the override properties window, override “Multiple Server Discovery” to “True” to discover all the clusters. To exclude the clusters that are not required, override “Excluded Servers” by the string which contains semicolon delimited fully qualified names of virtual servers to be excluded. Select a new management Pack and create the same. Click Apply in Override properties window.
3. Administrator must verify that the resource “Network Name” and the corresponding IP Address are configured for the given role in the cluster group. This resource is required by the Cluster Mgmt Pack to discover the cluster group and create the corresponding virtual server (the RRAS MP can discover the Multitenant RRAS Server object only on a virtual server created by cluster MP). If adding the NVGRE Gateway cluster via VMM, this resource might not be created, and hence the Multi-tenant RRAS Server discovery might not happen. To check this, open the MMC snap-in for “Failover Cluster Manager” on the RRAS Cluster node and in the left pane, expand the cluster by clicking on the name and browse to Roles. In the Roles window, click on the server role and check for its Resources in the bottom window. Check if the Client Access Point Resource is configured for this role with the (Network) Name and IP Address. This can also be verified by using the PowerShell cmdlet –

Get-ClusterResource | where {$\_.ResourceType –eq “Network Name”}

If the NetworkName and IP Address are not configured, the cluster will not be discovered by the Multitenant RRAS monitoring pack. To configure the Network Name, follow these steps –

1. In the Failover Cluster Manager UI, click on the RRAS Server Role
2. In the Action window (right pane), click on Add Resource > Client Access Point
3. Assign a Network Name and IP Address to access this Server role and click Next
4. Confirm and finish the wizard. Bring the resource online if required.

OR

Use the following PS cmdlet –

Add-ClusterResource –Name <User defined Network Name> -Group <Cluster Group / Role Name> -ResourceType “Network Name”

Bring the resource online if required.

#### Monitors and Alarms

The Windows Server 2016 SDN Management Pack includes monitors and alarms to notify the administrator of some erroneous conditions. The following table outlines these monitors:

**Virtual Network monitors:**

|  |  |
| --- | --- |
| **Monitor** | **Description** |
| Ping Test Failed | The ping test between the configured IPs failed. The source IP address should be an IP address in the virtual network, the destination IP address could be an IP address in the virtual network or external network. If the destination is external network the ping is terminated on the gateway through which the traffic is supposed to go through. |

**Gateway Pool monitors:**

|  |  |
| --- | --- |
| **Monitor** | **Description** |
| Redundancy Configuration Failed | All gateways in the gateway pool are redundant or redundancy count of the gateway pool is not met. |

**Gateway monitors:**

|  |  |
| --- | --- |
| Monitor | Description |
| Configuration Fetch Failed | The network controller is unable to fetch the configuration from the gateway. |
| Configuration Push Failed | The network controller is unable to push configuration to the gateway. |
| IP Address or Radius Configuration Failed  | The network controller is unable to configure IP addresses on the gateway. |
| Core Utilization Limit Exceeded (Requires SCOM Server) | Utilization per core goes above certain limit (90%) for the gateway. The limit can be over-ridden.  |
| CPU Utilization Limit Exceeded (Requires SCOM Server) | CPU utilization goes above certain limit (90%) for the gateway. The limit can be over-ridden. |
| External Network Interface Mac Address Mismatch | No interface with the external interface mac address was found on the gateway. |
| Stale Routing Domain Configuration | The gateway has a stale routing domain for which there is no corresponding virtual gateway in Network controller. |
| IP Configurations Update Failed | The network controller is unable to update the IP configuration on the internal interface (VSID) for the specified routing domain on the gateway. |
| SLB Rules Configuration Failed | The network controller is unable to update SLB configuration for the S2S connection on the gateway. |
| Clean up Failed | The network controller is unable to clean up the gateway. |
| Monitoring Service Start Failed | The network controller is unable to start monitoring service on the gateway. |
| Network Interface Properties Fetch Failed | The network controller is unable to communicate with the vSwitchModule and hence unable to retrieve MAC addresses of internal and external interfaces of the gateway. |
| Passive | The Gateway is in passive state. |
| Tenant Count exceeded | The number of tenants on the gateway exceeded the recommended limit. |
| Network Connection Count exceeded | The number of connection on the gateway exceeded the recommended limit. |
| Memory Utilization Limit Exceeded (Requires SCOM Server) | Memory utilization goes above certain limit (90%) for the gateway. The limit can be over-ridden. |

``

**Virtual Gateway monitors:**

|  |  |
| --- | --- |
| **Monitor** | **Description** |
| IP Address Deletion Failed  | The network controller is unable to delete IP address from unused routing domain on gateway. |
| IP Address Addition Failed | The network controller is unable to create IP address configuration on the gateway as the routing domain is not created on the gateway. |
| Stale Network Connection | There's a stale network connection for the virtual gateway. |
| Routing Domain Not Created | The network controller is unable to configure the routing domain on the gateway. |
| Virtual Network Routes Configuration Failed | The network controller is unable to configure data plane routes on gateway as the routing domain is not created. |
| Duplicate IP Address | The network controller is unable to create IP address configuration on the gateway as a duplicate IP address exists. |

**Network Connection monitors:**

|  |  |
| --- | --- |
| **Monitor** | **Description** |
| Gateway Unallocated | The network controller is unable to allocate a gateway for the connection. |
| Routing domain Not Created | The network controller is unable to configure the routing domain on the gateway. |
| Source IP Address Allocation Failed | The network controller is unable to use the configured source IP address for the connection. |
| Network Connection Configuration Failed | The network controller is unable to configure the connection on the gateway. |
| SLB Rule Configuration Failed | The network controller is unable to push slb rules for the network connection. |
| Duplicate IP Address (For L3 network connection only) | The network controller is unable to create IP address configuration on the gateway as a duplicate IP address exists. |
| Disconnected | The network connection is in disconnected state. |

**BGP Router monitors:**

|  |  |
| --- | --- |
| **Monitor** | **Description** |
| Routing domain not Created | The network controller is unable to configure the routing domain on gateway for the BGP Router. |
| BGP Router Configuration Failed | The network controller is unable to configure the BGP router on gateway. |

**BGP Peer monitors:**

|  |  |
| --- | --- |
| **Monitor** | **Description**  |
| Disconnected | The bgp peer is in disconnected state. |

#### Performance Monitoring Scenarios

The Multi-tenant RRAS Management Pack includes performance counters to let the administrator monitor the performance statistics for the RRAS server. The following table outlines these performance counters:

**Gateway performance counters:**

|  |  |
| --- | --- |
| **Performance Counter** | **Description** |
| BGP Router Count | The number of BGP routers configured on the gateway. |
| BGP Peer Count | The number of BGP peers configured on the gateway. |
| Bytes Received (Requires SCOM Server) | The total number of bytes received for the gateway. |
| Bytes Received/Sec (Requires SCOM Server) | The number of bytes received per second for the gateway. |
| Bytes Transmitted (Requires SCOM Server) | The total number of bytes transmitted for the gateway. |
| Bytes Transmitted/Sec (Requires SCOM Server) | The number of bytes transmitted per second for the gateway. |
| All Connections Count | The total number of connections configured on the gateway. |
| IPSec Connections Count | The total number of IPSec connections configured on the gateway. |
| GRE Connections Count | The total number of GRE connections configured on the gateway. |
| L3 Connections Count | The total number of L3 connections configured on the gateway. |
| Available Capacity | The available capacity on the gateway. |
| Available Capacity Percent | The available capacity percent on the gateway. |

**Network connection performance counters:**

|  |  |
| --- | --- |
| **Performance Counter** | **Description** |
| Outbound Bytes | The outbound bytes for the network connection. |
| Inbound Bytes | The inbound bytes for the network connection. |
| Rx Total Packets Dropped | The Rx total packets dropped for the network connection. |
| Tx Total Packets Dropped | The Tx total packets dropped for the network connection. |
| Rx Rate Kbps | The Rx rate kbps for the network connection. |
| Tx Rate Kbps | The Tx rate kbps for the network connection. |
| Rx Rate Limited Packets Dropped  | The Rx rate limited packets dropped for the network connection. |
| Tx Rate Limited Packets Dropped | The Tx rate limited packets dropped for the network connection. |

**BGP Peer performance counters:**

|  |  |
| --- | --- |
| **Performance Counter** | **Description** |
| Open Message Stats Sent Count | The open message stats sent count for the bgp peer. |
| Open Message Stats Received Count | The open message stats received count for the bgp peer. |
| Notification Message Stats Sent Count | The notification message stats sent count for the bgp peer. |
| Notification Message Stats Received Count | The notification message stats received count for the bgp peer. |
| Keep Alive Message Stats Sent Count | The keep alive message stats sent count for the bgp peer. |
| Keep Alive Message Stats Received Count | The keep alive message stats received count for the bgp peer. |
| Route Refresh Message Stats Sent Count | The route refresh message stats sent count for the bgp peer. |
| Route Refresh Message Stats Received Count | The route refresh message stats received count for the bgp peer. |
| Update Message Stats Sent Count | The update message stats sent count for the bgp peer. |
| Update Message Stats Received Count | The update message stats received count for the bgp peer. |
| Ipv4 Route Update Sent Count | The Ipv4 route update sent count for the bgp peer. |
| Ipv4 Route Update Received Count | The Ipv4 route update received count for the bgp peer. |
| Ipv4 Route Withdrawal Sent Count | The Ipv4 route withdrawal sent count for the bgp peer. |
| Ipv4 Route Withdrawal Received Count | The Ipv4 route withdrawal received count for the bgp peer. |
| Ipv6 Route Update Sent Count | The Ipv6 route update sent count for the bgp peer. |
| Ipv6 Route Update Received Count | The Ipv6 route update received count for the bgp peer. |
| Ipv6 Route Withdrawal Sent Count | The Ipv6 route withdrawal sent count for the bgp peer. |
| Ipv6 Route Withdrawal Received Count | The Ipv6 route withdrawal received count for the bgp peer. |

### Monitoring the Virtual Networks Group

After the SDN MP has discovered the Network Controller nodes, it will then query the Network Controller’s RESTful API (via PowerShell and Invoke-Web requests) to determine the tenant virtual networks which have been created. Each virtual network is identified by a both a Resource Id (created by the administrator) and a unique Instance Id (created by the Network Controller). In SCOM, the virtual network resources show the IP prefixes of the currently configured virtual subnets as well as the address space of the entire virtual network. Lastly, the reference to the HNV Provider (transport) logical network over which the virtual network is tunneled is specified.

#### Virtual Network Monitors and Alarms

|  |  |
| --- | --- |
| Policy Configuration Failure on VFP | Failed to configure network policies on the Virtual Filtering Platform (VFP) switch extension |
| Policy Configuration Failure | Failed to push network policies to the Hyper-V host |
| Ping Test Failed | A ping test between configured IPs (source IP in the virtual network and destination IP in the virtual or physical network) failed |

The virtual network may also reference a virtual gateway. The virtual gateway will have child elements for network connections (e.g. IPSec tunnels) as well as BGP Router properties. These virtual gateways, network connections, and BGP router resources are documented above.

### Monitoring the Network Interfaces Group

After the SDN MP has discovered the Network Controller nodes, it will then query the Network Controller’s RESTful API (via PowerShell and Invoke-Web requests) to determine the network interface resources created. Network Interfaces are created for both tenant VM NIC adapters as well as SDN fabric VM NIC adapters for the Software Load Balancer Muxes and RRAS Gateway VMs. Each network interface is represented by both a resource Id (created by the administrator) and a unique Id (created by the Network Controller).

#### Network Interface Monitors and Alarms

|  |  |
| --- | --- |
| Policy Configuration Failure on VFP | Failed to configure networking policies on the Virtual Filtering Platform (VFP) switch extension |
| Policy Configuration Failure | Failed to push NIC policies to the Hyper-V Host |
| DHCP Address Allocation Failure | DHCP Address could not be allocated for the VM NIC |
| Port Blocked | The virtual machine network interface is blocked. Could not configure NIC policies on the port |
| QoS Configuration Failure | Failed to configure QoS policies by Network Controller for the virtual server |

In order to obtain specific configuration information about a particular network interface resource, an administrator can use Network Controller PowerShell cmdlets to query the NC REST API (e.g. Get-NetworkControllerNetworkInterface -ConnectionUri <https://<FQDN of NC> -ResourceId <Resource Id>

### Monitoring the Load Balancer Muxes Group

After the SDN MP has discovered the Network Controller nodes, it will then query the Network Controller’s RESTful API (via PowerShell and Invoke-Web requests) to determine the load balancer mux resources and corresponding virtual server (VM) in which the Mux is running.

#### Load Balancer Mux Monitors and Alarms

|  |  |
| --- | --- |
| Certificate Not Trusted | The certified used by the Load Balancer mux is not trusted by the Network Controller |
| Certificate Not Authorized | An incorrect or invalid mux certificate could not be authorized or authenticated |
| Overloaded | The load balancer mux is reaching its capacity in terms of the traffic it can process |
| Route Publication Failure | The load balancer mux failed to publish routes |
| Virtual Server Unreachable | The SLB Mux VM (infrastructure VM) is unreachable from the Network Controller |

### Monitoring the Host Group

After the SDN MP has discovered the Network Controller nodes, it will then query the Network Controller’s RESTful API (via PowerShell and Invoke-Web requests) to determine the physical server (Hyper-V Host) resources. The server resources are identified by a resource Id and unique Id.

#### Host (Server) Monitors and Alarms

|  |  |
| --- | --- |
| Hyper-V Host Unreachable | Connectivity to the host failed from the Network Controller |
| PA MAC Address Pool Exhausted | The PA MAC addresses have been exhausted |
| PA IP Address Pool Exhausted | The PA IP Addresses have been exhausted |
| PA IP Address Configuration Failure | Failure to configure the PA IP Address on the host |
| Certificate Not Trusted | The Hyper-V Host X.509 certificate is not trusted by the Network Controller |
| Certificate Not Authorized | The Hyper-V Host X.509 certificate is not authorized and/or cannot be authenticated |
| Host not Connected to Network Controller | The Hyper-V Host has not yet connected to the Network Controller |
| Multiple VFP-Enabled Virtual Switches | There are multiple virtual switches where VFP extension is enabled |
| Distributed Router Configuration Failure | The Distributed Router could not be configured in the TCPIP stack of the Hyper-V Host |
| Infrastructure Port is Blocked | One or more Infrastructure virtual servers (e.g. SLB, NC, Gateway) ports are blocked |

### Monitoring the Access Control Lists

After the SDN MP has discovered the Network Controller nodes, it will then query the Network Controller’s RESTful API to determine the access control list (ACL) resources. ACLs can be referenced by either a virtual subnet or a network interface’s IP configuration. Each ACL is identified a resource Id and unique Id.

#### Access Control List Monitors and Alarms

|  |  |
| --- | --- |
| Policy Configuration Failure on VFP | Failed to configure policies on the Virtual Filtering Platform (VFP) switch extension |
| Policy Configuration Failure | Failed to push Firewall policies to the Hyper-V Host |

# Placing Monitored Objects in Maintenance Mode

When a monitored object, such as a computer or distributed application, goes offline for maintenance, Operations Manager 2012 R2 detects that no agent heartbeat is being received and, as a result, may generate numerous alerts and notifications. To prevent alerts and notifications, place the monitored object into maintenance mode. In maintenance mode, alerts, notifications, rules, monitors, automatic responses, state changes, and new alerts are suppressed at the agent.

For general instructions on placing a monitored object in maintenance mode, see [How to Put a Monitored Object into Maintenance Mode in Operations Manager 20](http://technet.microsoft.com/en-us/library/hh212870.aspx)12 R2 (http://technet.microsoft.com/en-us/library/hh212870.aspx).