

Guide for System Center 2012 R2 Monitoring Pack for Multi-tenant Remote Access

Microsoft Corporation

Published: October 2013

Send suggestions and comments about this document to [mpgfeed@microsoft.com](mailto: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 System Center Monitoring Pack for Multi-tenant Remote Access helps you monitor the health and availability of computers configured for Multi-tenant Remote Access server role and running Windows Server 2012 R2. This guide describes how to install the System Center Monitoring Pack for Multi-tenant Remote Access in Microsoft® System Center Operations Manager 2012 R2(Operations Manager 2012 R2).

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 Multi-tenant Remote Access

This guide was written based on version 7.1.10100.0 of the Monitoring pack for Microsoft System Center 2012 R2 Multi-tenant Remote Access.

## Guide History

| **Release Date** | **Changes** |
| --- | --- |
| October 2013 | Original release of this guide |
| March 2014 | Details added on ‘Pre-requisites for Monitoring Multi-tenant RRAS in Clustering Environment’ |

## 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 Remote Access:

| **Configuration** | **Support** |
| --- | --- |
| Windows Server 2012 R2 Remote Access (Multi-tenant) | Yes |
| Windows Server 2012 Remote Access | Not supported |
| Windows Server 2008 R2 | Not supported |

## Files in this Monitoring Pack

The Monitoring Pack includes the following files:

 License Agreement

 Microsoft.Windows.RemoteAccess.MultiTenant.2012.R2.Discovery.mp

* Microsoft.Windows.RemoteAccess.MultiTenant.2012.R2.Monitoring.mp

## Monitoring Pack Purpose

The System Center Monitoring Pack for Multi-Tenant Remote Access helps you monitor the health and availability of the Multi-Tenant Remote Access Server role on computers running Windows Server 2012 R2.

This guide describes how to install the System Center Monitoring Pack for Multi-Tenant Remote Access in Microsoft® System Center Operations Manager 2012 R2 (Operations Manager 2012 R2).

The management pack provides a predefined, ready-to-run set of processing rules, alarms, monitors, and performance instrumentation that are designed to monitor the Multi-Tenant Remote Access service components. RRAS is monitored via events that are placed in the Application and System event logs by various RRAS components and subsystems and also using PowerShell cmdlets.

This guide provides information about the most common monitoring scenarios, monitor definitions, tasks, and views for Multi-tenant Remote Access. 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 Remote Access 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 Routing and Remote Access Service Management Pack

This management pack has dependencies on Windows Server 2012 R2 Discovery and Windows Server Library management packs. You need to install these management packs before installing Routing and Remote Access Service Management Pack.

## How to Import the Routing and Remote Access Service 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 2012 R2 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 try to execute the following cmdlets on the monitored servers

1. Get-RemoteAccess
2. Get-RemoteAccessRoutingDomain
3. Get-BgpPeer
4. Get-BgpStatistics
5. Get-VpnS2SInterface
6. Get-BgpRouter
7. Get-BgpRouteInformation
8. Get-RemoteAccessConnectionStatistics

The ‘Run As Account’ configured needs to have the local admin permissions on all the Remote Access Servers. It is highly recommended that you use a separate security group for the accounts configured for Operations Manager 2012 R2.

## Discovered Objects

The Multi-tenant Remote Access Management Pack discovers the object types described in the following table.

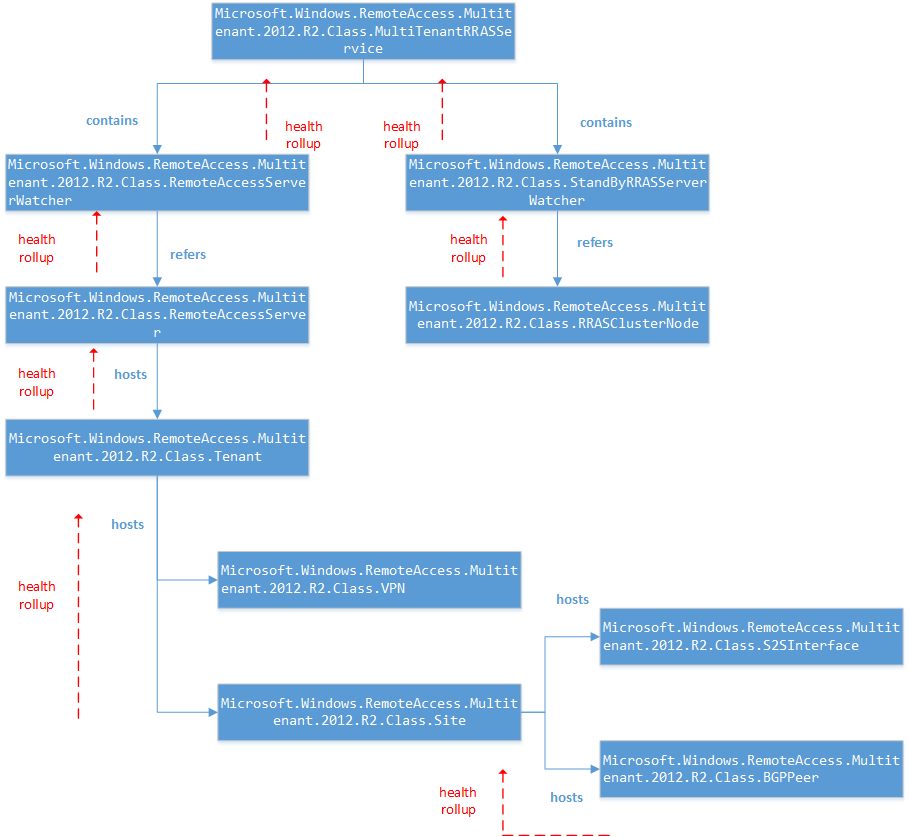
For information about discovering objects, see [Understanding Classes and Objects in System Center 2012 R2](file:///C:\Users\sankasat\Documents\Understanding%20Classes%20and%20Objects%20in%20System%20Center%202012%20R2) (<http://technet.microsoft.com/en-us/library/hh457568>) in Operations Manager 2012 R2 Help.

| **Category** | **Object Type** | **Discovered Automatically** |
| --- | --- | --- |
| Discovers Multi-Tenant RRAS Servers | * Multi-Tenant RRAS server * Multi-Tenant RRAS service * Stand-by server watcher * RRAS cluster node (for clustered environment) * RemoteAccess server watcher | Yes (every 6 hours) |
| Discovers Tenants/Routing Domains that are configured for RRAS | * Tenant | Yes (every 2 hours) |
| Discovers Sites, S2S Interfaces and BGP Peers | * Site * BGP peer * S2S interface | Yes (every 60 minutes) |
| Discovers VPN Connections group | * VPN Connections | Yes (every 60 minutes) |

All the discoveries are PowerShell based.

## How Health Rolls Up

The class hierarchy for System Center Monitoring Pack for Multi-Tenant Remote Access is shown below. The blue arrows show the hierarchy while red dotted ones show health rollup.



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

### 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 Multi-tenant RRAS Management Pack includes monitors and alarms to notify the administrator of some erroneous conditions. The following table outlines these monitors:

**RRAS Server monitors:**

|  |  |
| --- | --- |
| **Monitor** | **Description** |
| Authentication or accounting failures | The Routing and Remote Access service encountered an error while performing authentication or accounting. This monitor must be manually reset by the administrator whenever it changes to a critical state. |
| BGP routes number exceeded limit | Number of BGP routes exceeds the maximum allowed value |
| Cluster Node Monitor | The High Availability cluster set up has encountered an error |
| Core Utilization | Utilization per core goes above certain limit (90%). The limit can be over-ridden. |
| CPU Utilization | CPU utilization goes above certain limit (90%). The limit can be over-ridden. |
| Hardware device error | The connection attempt failed because the device that is connected to the port is not responding. This monitor must be manually reset by the administrator whenever it changes to a critical state. |
| IPCP negotiation failure | The Routing and Remote Access service encountered an error while assigning an IP address to dial-in client(s) during IP Control Protocol (IPCP) negotiation. This monitor must be manually reset by the administrator whenever it changes to a critical state. |
| IPsec related failures | The connection attempt failed because an IPsec-compatible certificate was not found. This monitor must be manually reset by the administrator whenever it changes to a critical state. |
| Memory Allocation Monitor | The Routing and Remote Access service could not start or is not fully functional because of a memory allocation failure. |
| Memory Utilization | Memory utilization goes above certain limit (90%). The limit can be over-ridden. |
| No more licenses monitor | A user was unable to connect to the RRAS server because the server exceeded its client license limit. This monitor must be manually reset by the administrator whenever it changes to a critical state. |
| Packet filter related failure | The Routing and Remote Access service encountered an error while configuring a packet filter. This monitor must be manually reset by the administrator whenever it changes to a critical state. |
| Radius Server Monitor | The Radius server is not responding or sending an invalid response. This monitor must be manually reset by the administrator whenever it changes to a critical state. |
| Rasman Port open failures | The Routing and Remote Access service or the Remote Access Connection Manager service encountered an error while opening a port for remote access. This monitor must be manually reset by the administrator whenever it changes to a critical state. |
| Remote Access Connection Manager unexpected termination | The Remote Access Connection Manager (RASMAN) service was unexpectedly terminated. |
| Routing and Remote Access service monitor | The Routing and Remote Access service is not running. |
| Routing and Remote Access service unexpected termination | The Routing and Remote Access service was unexpectedly terminated. |
| Tenant monitor | More than 50% of the tenants are not getting properly serviced. The % value can be over-ridden. |

``

**High Availability monitors:**

|  |  |
| --- | --- |
| **Monitor** | **Description** |
| RRAS Server Compartment Monitor | One or more tenants do not have compartment ids configured on the Stand-by server |
| RRAS Service Monitor | The Routing and Remote Access service is not running on the Stand-by server |
| RRAS Stand-by Export Failure Monitor | A failure has occurred while exporting RRAS configuration from the Active server |
| RRAS Stand-by node Import Failure Monitor | A failure has occurred while importing RRAS configuration on the Stand-by server |
| RRAS Stand-by Server Node Monitor | The clustering service on the Stand-by server node is not running |

**Tenant level monitors:**

|  |  |
| --- | --- |
| **Monitor** | **Description** |
| BGP Router Monitor | BGP connections are not running properly on more than 50% of the tenant sites |
| Compartment Monitor | The compartment id corresponding to the tenant is not available |
| S2S Interface Monitor | S2S connections are not running properly on more than 50% of the tenant sites |

**Site to site connection monitors:**

|  |  |
| --- | --- |
| **Monitor** | **Description** |
| Connection Disconnected Monitor | The S2S connection is disconnected |
| Connection Idle State Monitor | The S2S connection is idle |
| Connection State Monitor | The S2S connection is in disconnected state (PowerShell based) |
| Destination Unreachable Monitor | The S2S connection is disconnected because the destination is not reachable |
| Frequent Reconnections Monitor | This monitor gives a warning when S2S connection has reconnected more than twice in last 15 minutes. |

**BGP connection monitors:**

|  |  |
| --- | --- |
| **Monitor** | **Description** |
| BGP Peer Connectivity Status Monitor | The BGP connection is disconnected (PowerShell based) |
| BGP Peer Frequent Reconnection Monitor | The BGP connection has reconnected more than twice in last 15 minutes. |
| BGP Connection Generic Failure Monitor | The BGP connection is disconnected |
| BGP Peer Manual Start/Stop Monitor | This monitors warns that the BGP Connection has been manually stopped. |
| BGP Peer Max Prefix Limit Reached Monitor | The BGP peer has advertised more prefixes than the allowed limit. |
| BGP Peer Unreachability Monitor | The BGP Peer is unreachable |

### 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:

**Server level performance counters:**

|  |  |
| --- | --- |
| **Performance Counter** | **Description** |
| Alignment Errors | The total number of alignment errors for this server. Alignment errors occur when a byte received is different from the byte expected. |
| BGP Peer Count (Server) | The number of BGP peers configured on the server |
| BGP Route Count (Server) | The number of BGP routes on the server |
| Buffer Overrun Errors | The total number of buffer overrun errors for this server. Buffer overrun errors occur when the software cannot handle the rate at which data is received. |
| Bytes Received | The total number of bytes received for this server. |
| Bytes Received/Sec | The number of bytes received per second. |
| Bytes Transmitted | The total number of bytes transmitted for this server. |
| Bytes Transmitted/Sec | The number of bytes transmitted per second. |
| CRC Errors | The total number of cyclic redundancy check (CRC) Errors for this server. CRC errors occur when the frame received contains erroneous data. |
| Frames Received | The total number of data frames received for this server. |
| Frames Received/Sec | The number of frames received per second. |
| Frames Transmitted | The total number of data frames transmitted for this server. |
| Frames Transmitted/Sec | The number of frames transmitted per second. |
| Percent Compression In | The compression ratio for bytes being received. |
| Percent Compression Out | The compression ratio for bytes being transmitted. |
| Serial Overrun Errors | The total number of serial overrun errors for this server. Serial overrun errors occur when the hardware cannot handle the rate at which data is received. |
| Timeout Errors | The total number of timeout errors for this server. Timeout errors occur when an expected frame is not received in time. |
| Total Errors | The total number of CRC, timeout, serial overrun, alignment, and buffer overrun errors for this server. |
| Total Errors/Sec | The total number of CRC, timeout, serial overrun, alignment, and buffer overrun errors per second. |
| Total number of Active Connections | The total number of currently active remote access connections. |
| Total number of S2S Connections | The total number of currently active S2S connections |
| Total number of Tenants | The total number of tenants being serviced |
| Total number of VPN Connections | The total number of currently active VPN connections |

**Tenant level performance counters:**

|  |  |
| --- | --- |
| **Performance Counter** | **Description** |
| Bytes Received | The total number of bytes received for this tenant. |
| Bytes Received/Sec | The number of bytes received per second. |
| Bytes Transmitted | The total number of bytes transmitted for this tenant. |
| Bytes Transmitted/Sec | The number of bytes transmitted per second. |
| Tenant Peer Count | The number of BGP peers configured for the tenant |
| Tenant Route Count | The number of BGP routes for the tenant |
| Total Errors | The total number of CRC, timeout, serial overrun, alignment, and buffer overrun errors for this tenant. |
| Total number of Active Connections | The total number of currently active remote access connections for the tenant. |
| Total number of S2S Connections | The total number of currently active S2S connections for the tenant |
| Total number of VPN Connections | The total number of currently active VPN connections for the tenant |

**S2S connection performance counters:**

|  |  |
| --- | --- |
| **Performance Counter** | **Description** |
| Bytes Received | The total number of bytes received |
| Bytes Transmitted | The total number of bytes transmitted |
| Total Errors | The total number of CRC, timeout, serial overrun, alignment, and buffer overrun errors |

**BGP performance counters:**

|  |  |
| --- | --- |
| **Performance Counter** | **Description** |
| Peer Message Count | The total number of messages exchanged by the peer (apart from the Keep Alive Messages) |

### Event Monitoring Scenarios

The RRAS Management Pack includes event monitoring to let the administrator monitor the erroneous configuration or errors that occur during runtime on the RRAS server. The following table outlines these events:

|  |  |
| --- | --- |
| **Event** | **Description** |
| Rasman - PPP initialization failure | The Remote Access Connection Manager service failed to start because it encountered an error while loading RASPPP.dll. |
| Ras connection failure | The user’s connection to the RRAS server was terminated. |
| IKEv2 Configuration failure | The Routing and Remote Access service failed to start because of an invalid configuration. |
| Interface Initialization failure | The Routing and Remote Access service failed to load or create an interface. |
| Some interfaces not working | The Routing and Remote Access service encountered an error while performing an operation on the interface. |
| Demand dial connection failed | The Routing and Remote Access service failed to establish the demand-dial connection. |
| Configuration change for authentication | The Routing and Remote Access service detected a change in configuration. This may affect the connectivity of already connected user(s). |
| Out of memory error | The Routing and Remote Access service could not start or is not fully functional because of memory allocation failure. |
| Authentication/Accounting failure | The Routing and Remote Access service encountered an error while performing authentication or accounting. |
| Loading RAS supporting modules failure | The Routing and Remote Access service could not start because it failed to load and initialize one of the RAS DLLs. |
| Hardware device error | The connection attempt failed because the device that is connected to the port is not responding. |
| Control Protocol initialization failure | The Routing and Remote Access service failed to start because it encountered an error in the PPP Link Control Protocol initialization. |
| Rasman port open failure | The Routing and Remote Access service or the Remote Access Connection Manager service encountered an error while opening a port for remote access. |
| Rasman Service initialization failure | The Routing and Remote Access service could not start because of an initialization failure. |
| Multicast failure | The Routing and Remote Access service encountered a problem in multicasting. |
| Rasman service init error | The Remote Access Connection Manager service failed to start due to initialization failure. |
| RemoteAccess - PPP initialization failure | The Routing and Remote Access service failed to start because it encountered an error in the initialization of the Point-to-Point Protocol (PPP). |
| The service failed to start or terminated unexpectedly | The Routing and Remote Access service failed to start. |
| IPCP negotiation failure | The Routing and Remote Access service encountered an error assigning an IP address to dial-in clients during IP Control Protocol (IPCP) negotiation. |
| Loading 3rd Party DLL failure | The Routing and Remote Access service failed to start because it encountered an error while loading a vendor’s administration or security DLL. |
| Registry operation failure | The Routing and Remote Access service could not start because it could not access one or more required registry values. |
| IPsec related failures | The connection attempt failed because RRAS could not locate a suitable IPsec computer certificate. |
| External error | The Routing and Remote Access service encountered an error while trying to revert impersonation. |
| Multicast join failure | Internet Group Management Protocol version 2 (IGMPv2) could not join to the multicast group. |
| Configuration failure | Internet Group Management Protocol version 2 (IGMPv2) detected a configuration failure. |
| MGM operation failure | Internet Group Management Protocol version 2 (IGMPv2) encountered an error while registering with Multicast Group Manager (MGM). |
| RTM routes addition failure | Routing Information Protocol version 2 (RIPv2) failed to add routes to the Routing Table Manager (RTM). |
| Route ignored | Routing Information Protocol version 2 (RIPv2) ignored one or more routes advertised by a neighbor. |
| Socket operation failure1 | Routing Information Protocol version 2 (RIPv2) encountered an error in a socket operation. |
| Sending packets to peer failed | Routing Information Protocol version 2 (RIPv2) failed to send packets to the peer router. |
| Router manager's entry point to protocol failed2 | Routing Information Protocol version 2 (RIPv2) encountered an error in a callback function to the router manager. |
| External failure | The Routing Information Protocol version 2 (RIPv2) encountered an external error. |
| Protocol Initialization failure1 | Routing Information Protocol version 2 (RIPv2) encountered an error during initialization. |
| Discarded packet from peer1 | The Routing Information Protocol version 2 (RIPv2) discarded one or more packets from the peer router. |
| DNS proxy failure | The DNS proxy agent component of NAT encountered an error. |
| Memory allocation failure | The network address translation (NAT) protocol encountered a memory allocation failure. |
| Discarded packet from peer2 | The DHCP Relay Agent discarded one or more packets from the peer. |
| Router manager's entry point to protocol failed1 | The DHCP Relay Agent encountered an error in a callback function to the router manager. |
| Socket operation failure2 | The DHCP Relay Agent (IPBOOTP) encountered an error in socket operation. |
| Protocol initialization failure2 | The DHCP Relay Agent (IPBOOTP) encountered an error during initialization. |
| Routing protocol's entry point to MGM failed | Multicast Group Manager encountered an error during routing protocol registration while enabling a routing protocol on an interface. |
| Routing protocol registration failure | The routing protocol registration with Multicast Group Manager failed. |
| Router manager's entry point to MGM failed | Multicast Group Manager (MGM) encountered an error in a callback function to the router manager. |
| Initialization failure | The Multicast Group Manager (MGM) encountered an error during initialization. |
| Unable to process MOBIKE update | Unable to process MOBIKE update for connection |
| Disabling PPP AUTH on port | Disabling PPP AUTH on port |
| SSTP client certificate missing | The certificate that is used for Secure Socket Tunneling Protocol (SSTP) is missing. You should configure a new certificate for SSTP or use default configuration. |
| SSTP wrong certificate configuration | The certificate hash that is used for Secure Socket Tunneling Protocol (SSTP) %1 is different than the certificate bound %2 to the Web listener (HTTP.sys). Configure SSTP to use the default certificate or the certificate that is bound to SSL. You can configure Web server applications to use the same certificate that is used by SSTP. |
| SSTP cookie add failure | Secure Socket Tunneling Protocol (SSTP) service could not configure the VPN server-specific cookies. |
| No network protocols were successfully negotiated | No network protocols were successfully negotiated. |
| PPP Error on Port | PPP Error on Port |
| CallBack Failure | The remote access server’s attempt to callback user failed |
| Cannot receive initial data on port | Cannot receive initial data on port |
| License Limit Exceeded | A user was unable to connect on a port. No more connections can be made to this remote computer because the computer has exceeded its client license limit. |

# 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).