**Microsoft System Center**

Guide for System Center Management Pack for Microsoft Windows Guarded Fabric 2016 and above

Microsoft Corporation

Published: June 2021

Send feedback or suggestions about this document to systemcenterfeedback@microsoft.com. Please include the management pack guide name with your feedback.

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.

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.

© 2016 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Bing, BizTalk, Forefront, Hyper-V, Internet Explorer, JScript, SharePoint, Silverlight, SQL Database, SQL Server, Visio, Visual Basic, Visual Studio, Win32, Windows, Windows Azure, Windows Intune, Windows PowerShell, Windows Server, and Windows Vista are trademarks of the Microsoft group of companies. All other trademarks are property of their respective owners.

Contents

[Guide for System Center Management Pack for Microsoft Windows Server Guarded Fabric 2016 and above 4](#_Toc74727284)

[Management Pack Purpose 7](#_Toc74727285)

[Monitoring Scenario 7](#_Toc74727286)

[How Health Rolls Up 8](#_Toc74727287)

[Configuring the Management Pack for Microsoft Windows Server Guarded Fabric 8](#_Toc74727288)

[Appendix: Management Pack Contents 9](#_Toc74727289)

Guide for System Center Management Pack for Microsoft Windows Server Guarded Fabric 2016 and above

Document Version

This guide is based on the version 10.0.1.2 of the Windows Server 2016 and above of the Management Pack for Microsoft Windows Server Guarded Fabric.

Revision History

|  |  |
| --- | --- |
| Release Date | Changes |
| June 2021 | The MP has been verified for Windows Server 2016 and above operating systems and branded as version agnostic. |
| October 2020 | Updated with release of Management Pack version 10.0.1.1 – fixed bugs in Guarded Host Availability, Connection and Attestation Unit monitors. |
| June 2016 | Original release of this guide |
| November 2016 | Updating names for RTM version |

Changes in version 10.0.1.2

* The MP has been verified for Windows Server 2016 and above operating systems and branded as version agnostic.

Supported Configurations

This management pack requires System Center Operations Manager 2016 or later.

**Reference links:**

SCOM 2019 :  [System requirements for System Center Operations Manager | Microsoft Docs](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fsystem-center%2Fscom%2Fsystem-requirements%3Fview%3Dsc-om-2019%23microsoft-monitoring-agent-operating-system&data=04%7C01%7Cv-temarr%40microsoft.com%7C2d65d8d0321043cb2df608d9308415e0%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637594166158763232%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=4Tl0lYS0sZqR%2FiBXI4W9j3JS3kQpBMlPJsRKErabwZQ%3D&reserved=0)

SCOM 2016 : [System requirements for System Center Operations Manager | Microsoft Docs](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fsystem-center%2Fscom%2Fsystem-requirements%3Fview%3Dsc-om-2016%23software-requirements-for-operations-manager-components&data=04%7C01%7Cv-temarr%40microsoft.com%7C2d65d8d0321043cb2df608d9308415e0%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637594166158773191%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=7fhmN7G4pT6kr8aVps%2FUL0tN%2FB6AyUZ7PIb8oZ0eTV0%3D&reserved=0)

The following table details the supported configurations for the Management Pack for Microsoft Windows Server Guarded Fabric:

|  |  |
| --- | --- |
| Configuration | Support |
| Guarded Fabric | Discovery and monitoring of Guarded Fabric roles running on Windows Server 2016 and above |
| Clustered servers | Yes |
| Agentless monitoring | Not supported/not tested |
| Virtual environment | Not supported/not tested |

Management Pack Scope

This management pack supports the discovery and monitoring of any number of machines running roles related to the Guarded Fabric scenario in the Windows Server 2016 and above operating system. It does not support testing the functional level of the Guarded Fabric itself, as that can include a variety of operating systems. Rather, this management pack configuration is for per-machine monitoring on machines running in these roles.

Mandatory Configuration

If the Host Guardian Service is running as its own domain, then the SCOM Domain must have at least a one-way trust to the domain in which the machine in the Host Guardian Service role is operating. All other best practices for configuration are found below.

Security Configuration

This Management Pack does not create any RunAs profiles due to the security and PowerShell based nature of the discovery and monitoring. Rather, the agent configured on the monitored machine, once it is discoverable, should be set with the credentials associated with the ability to run HGS Server and Guarded Host cmdlets.

Running HsLockdown

If your Host Guardian Service nodes are running the Active Directory Domain Controller role (the default configuration if you did not join them to an existing secure forest during setup), then the Health Service Lockdown tool (HsLockdown.exe) must be run for machines running the Host Guardian Service to be discoverable. To do this, navigate to where the Operations Manager Agent is installed on the monitored machine in a command prompt, then run:

*PS C:\> hslockdown /A <NameOfAccount>*

Where <NameOfAccount> is the account associated with this agent. By default, this is NT AUTHORITY\System

Enabling Local Agent by Proxy

The Host Guardian Service role in a Guarded Fabric is a clustered role, so the monitoring agent must enable local agent by proxy to be discoverable. To do this, enter the following command in the Operations Management Shell for each HGS node being managed by SCOM:

*PS C:\> Get-SCOMAgent –ComputerName <HGSComputer> | Enable-SCOMAgentProxy*

Where <HGSComputer> is the name of the computer running in the Host Guardian Service role. This can also be managed via the Operations Manager Console.

Files in this Management Pack

The Management Pack for Microsoft Windows Guarded Fabric 2016 and above includes the following files:

* **Microsoft.Windows.Server.GuardedFabric.Class.Library.mp:** Displayed as “Microsoft Windows Server Guarded Fabric Class Library,” this management pack is the library management pack that defines all of the features and components that are common to all versions of the Windows Server Guarded Fabric. This management pack contains no monitoring configuration and is a prerequisite for all other Windows Server Guarded Fabric management packs. Therefore, this management pack must be imported at the same time or prior to the version-specific management packs.
* **Microsoft.Windows.Server.GuardedFabric.2016.Discovery.mp:** Displayed as “Microsoft Windows Server Guarded Fabric 2016 Discovery,” this management pack discovers classes specific to Guarded Fabric roles in Windows Server 2016 and above. This management pack is a prerequisite for the monitoring management pack of the same version.
* **Microsoft.Windows.Server.GuardedFabric.2016.Monitoring.mp:** Displayed as “Microsoft Windows Server Guarded Fabric 2016 and above Monitoring,” this management pack defines the monitors and tasks associated with those classes discovered in the Microsoft Windows Server Guarded Fabric 2016 and above Discovery management pack.

Recommended Additional Management Packs

As the machine roles involved in the Guarded Fabric configuration can and do involve many other standalone services, it is strongly suggested that management packs for the following features are also imported for full coverage of all possible failures:

* Microsoft Active Directory Domain Services (ADDS)
* Failover Cluster
* Internet Information Services

Management Pack Purpose

This management pack provides event and script based unit monitoring for machines running roles included in the Guarded Fabric scenario, including Guarded Hosts and Host Guardian Service nodes.

In this section:

 [Monitoring Scenario](#MonitoringScenario)

 [How Health Rolls Up](#zb8b3e32eb8154a8da8b18b606568e65d)

For details on the discoveries, rules, monitors, views, and reports contained in this Management pack, see [Appendix: Management Pack Contents](#zf475f3cc57b84a049d89cda7b1f37ba8).

Monitoring Scenario

This management pack was designed with the Guarded Fabric scenario in mind. There are two roles designated within this scenario: Host Guardian Service server (HGS Server), and the Guarded Host. The Guarded Host is a Hyper-V host for Shielded Virtual Machines, and sends attestation and key distribution requests to the HGS Server. The HGS Server, either via checking the TCG log and code integrity policies for health, or AD Security Group membership, attests this host and provides keys if the Guarded Host is deemed secure. Additionally, the HGS Server can either be run as a domain controller for its own domain (along with all of its other nodes, as it is a clustered role for High-Availability purposes), or as a service within an existing domain.

Thus, this management pack is kept simple for the variety of configurations. It uses PowerShell based discovery to find instances of Guarded Hosts and HGS Servers, and implements event and PowerShell based unit monitors. These monitors cover scenarios such as:

* The HGS Server being unable to load its configuration
* The Guarded Host failing attestation
* The Guarded Host failing to unwrap a key protector

How Health Rolls Up

The following diagram shows how the health states of objects roll up in this management pack.



Configuring the Management Pack for Microsoft Windows Server Guarded Fabric

This section provides guidance on configuring and tuning this management pack.

Best Practice: Create a Management Pack for Customizations

By default, Operations Manager saves all customizations such as overrides to the Default Management Pack. As a best practice, you should instead create a separate management pack for each sealed management pack you want to customize.

When you create a management pack for the purpose of storing customized settings for a sealed management pack, it is helpful to base the name of the new management pack on the name of the management pack that it is customizing.

Creating a new management pack for storing customizations of each sealed management pack makes it easier to export the customizations from a test environment to a production environment. It also makes it easier to delete a management pack, because you must delete any dependencies before you can delete a management pack. If customizations for all management packs are saved in the Default Management Pack and you need to delete a single management pack, you must first delete the Default Management Pack, which also deletes customizations to other management packs.

Appendix: Management Pack Contents

The Management Pack for Guarded Fabric 2016 and above discovers the object types described in the following sections. Not all of the objects are automatically discovered. Use overrides to discover those objects that are not discovered automatically.

Host Guardian Service Server

This Management Pack class represents a fully initialized Host Guardian Service (HGS) Server.

Discovery Information

|  |  |  |
| --- | --- | --- |
| Interval | Enabled | When to Enable |
| 8 hours | True | Not Applicable |

Related Monitors

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Monitor | Data source | Interval | Alert | Reset Behavior | Enabled |
| Attestation Replicated Store Availability  | Triggering Events (Microsoft-Windows-HostGuardianService-Attestation/Admin): 1528Resolving Events (Microsoft-Windows-HostGuardianService-Attestation/Operational): 1518,1519,1527Represents failures to load or update attestation configuration This can often be caused by a corrupted store, or a quarantined cluster node. | Not applicable | TrueAlert priority:NormalAlert severity:Error | Automatic | True  |
| Key Distribution Service Replicated Store Availability:  | Triggering Events (Microsoft-Windows-HostGuardianService-KeyProtection/Admin):3250, 4010, 4100Resolving Event (Microsoft-Windows-HostGuardianService-KeyProtection/Operational): 2101Represents failures to load or update Key Protection configuration. This can often be caused by a corrupted store, or a quarantined cluster node. | Not applicable | TrueAlert priority: NormalAlert Severity: Error | Automatic | True |

Note

If you are using connectors, you can disable the monitor and enable its corresponding rule to enable alerts without changing health status.

Related Rules

There are no rules associated with this object.

Note

Disable the rule and enable its corresponding monitor to enable alerts, state changes, and health rollup.

Related Views

|  |  |  |
| --- | --- | --- |
| View | Description | Rules and Monitors that Populate the View |
| HGS Server State | State View of all discovered HGS Servers | Not applicable |
| HGS Server Active Alerts | Any active alerts regarding a Guarded Fabric 2016 and above Host Guardian Service Server | All alerts raised by unit monitors of this class. |

Guarded Host

This Management Pack class represents a Guarded Host running on the Windows Server 2016 and above operating system. A Guarded Host is defined as a Windows Server 2016 and above machine running the Hyper-V role and Host Guardian Hyper-V Support feature.

Discovery Information

|  |  |  |
| --- | --- | --- |
| Interval | Enabled | When to Enable |
| 8 hours | True | Not Applicable |

Related Monitors

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Monitor | Data source | Interval | Alert | Reset Behavior | Enabled |
| Attestation Availability | Triggering Events Microsoft-Windows-HostGuardianService-Client/Admin): 1019Resolving Events (Microsoft-Windows-HostGuardianService-Client/Operational): 1003Represents a failure to perform a remote attestation request due to the host being unreachable. This is often due to configuration errors in setting your Attestation URL. | Not applicable | TrueAlert priority:NormalAlert severity:Error | Automatic | True  |
| Key Protection Service Availability:  | Triggering Events (Microsoft-Windows-HostGuardianService-Client/Operational: 2014Resolving Events (Microsoft-Windows-HostGuardianService-Client/Operational): 2015This unit monitor represents a failure to unwrap a Key Protector. This is usually paired with a failure to start a Shielded VM. | Not applicable | TrueAlert priority: NormalAlert Severity: Error | Automatic | True |
| Guarded Host Connection Monitor | PowerShell Script: This script succeeds if it is able to reach the Attestation and Key Distribution URL specified when running the Get-HgsClientConfiguration cmdlet (automatically passes if running in local mode) | 1 Hour | TrueAlert Priority: NormalAlert Severity: Error | Automatic | True |
| Guarded Host Attestation Monitor | PowerShell Script: This script succeeds if the Guarded Host can pass a forced attestation request (automatically passes if running in local mode) | 8 Hours | TrueAlert Priority:NormalAlert Severity:Error | Automatic | True |

Note

If you are using connectors, you can disable the monitor and enable its corresponding rule to enable alerts without changing health status.

Related Rules

There are no rules associated with this object.

Note

Disable the rule and enable its corresponding monitor to enable alerts, state changes, and health rollup.

Related Views

|  |  |  |
| --- | --- | --- |
| View | Description | Rules and Monitors that Populate the View |
| Guarded Host State | State View of all discovered Guarded Hosts | Not applicable |
| Guarded Host Active Alerts | Any active alerts regarding a Guarded Fabric 2016 and above Guarded Host | All alerts raised by unit monitors of this class. |