

Guide for System Center Management Pack for Active Directory, Domain Services

Microsoft Corporation

Published: April 2022

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 Active Directory, Domain Services (ADDS) 4](#_Toc100223259)

[Recommended Additional Management Packs 8](#_Toc100223260)

[Management Pack Purpose 9](#_Toc100223261)

[Monitoring Scenarios 10](#_Toc100223262)

[MP Health Roll Up 10](#_Toc100223263)

[Monitoring Scenarios 11](#_Toc100223264)

[Replication 12](#_Toc100223265)

[Essential Services 15](#_Toc100223266)

[Trust Monitoring 16](#_Toc100223267)

[Directory Service Availability 16](#_Toc100223268)

[Active Directory Database Monitoring 17](#_Toc100223269)

[Time Skew Monitoring 18](#_Toc100223270)

[Active Directory Web Service Monitoring 19](#_Toc100223271)

[Domain Controller Performance 19](#_Toc100223272)

[Domain Member Perspective 19](#_Toc100223273)

[Configuring the Management Pack for Active Directory, Domain Services (ADDS) 20](#_Toc100223274)

[Links 26](#_Toc100223275)

Guide for System Center Management Pack for Active Directory, Domain Services (ADDS)

This guide was written based on version 10.0.2.4 of the Management Pack for ADDS.

Revision History

|  |  |
| --- | --- |
| Release Date | Changes |
| December 2015 | Original release of this guide |
| December 2016 | Updated with changes to the final release |
| October 2018 | Updated to include version 10.0.2.2 information |
| December 2018 | Updated the language packs to fix an import error due to a missing element in the library MP |
| July 2020 | Added clarification in the guide regarding topology discovery for two-way transitive trusts |
| April 2022 | * False positive alerts issue has been fixed for LSASS Process Monitor and Rule
* The MP has verified for Windows Server 2016/2019/2022 operating systems and branded as version agnostic (2016 and above)
 |

Changes in Version 10.0.2.4

Fixed the following bugs:

* False positive alerts issue has been fixed for LSASS Process Monitor and Rule

Changes in Version 10.0.2.2

Fixed the following bugs:

* Updated the RODC Group to include OS version
* Updated NTService monitors to allow for overriding when the service is not set to automatic start
* Fixed AD Topology discovery when the SCOM server and action account are in a child domain

Changes in Version 10.0.2.1

Fixed the following bugs:

* Replaced Corrupted Language Packs with correct Language Packs

Changes in Version 10.0.2.0

Fixed the following bugs:

* Replaced the use of Get(“rootDomainNamingContext”) with Get(“defaultNamingContext”) in a number of scripts
* Fixed Override contexts that were breaking the override view in the Operations Manager Console
* Removed Unused References

Changes in Version 10.0.1.0

Added MPs to support down level OS versions. Now supports Windows 2012, 2012R2, and 2016.

Changes in Version 10.0.0.0

Version 10.0.0.0 of the Management Pack for ADDS is an initial release of a new Management Pack for Active Directory® (AD). It is based on the Active Directory Management Pack (AD MP) and includes many changes from the AD MP.

* Removed Event Alert rules, all Error and Warning events from AD related event logs are now only collected in the Events collections.
* Informational events can be collected as well by turning on the Information Events rules.
* Replication Monitoring replaced with the following monitors:
	+ AD Replication Queue Monitor
	+ AD Show Replication Check
	+ Replication Partner Count Monitor
	+ Replication Consistency Monitor
* Removed Reliance on OOMADS.dll for Domain Controller monitoring removed oomads dependency from all MPs.
* Removed dependency on down-level DC discovery MPs
* Created well defined aggregate roll-ups for health monitors
* New server health monitors
	+ Strict replication
	+ DNS service
	+ Group Policy
	+ Network adapters
	+ Strict replication
* New domain member monitors
	+ Reliable time server
	+ Secure channel
	+ DC health
	+ Group policy
* Removed deprecated rules, alerts, and tools
* Added additional information to alerts and monitors and updated knowledge base information
* Added performance collection rules for DNS perf counters

Supported Configurations

This Management Pack requires System Center Operations Manager 2012 or later. A dedicated Operations Manager management group is not required. The configurations in the following table are supported:

| **Configuration** | **Supported?** |
| --- | --- |
| Windows Server 2016 | Yes |
| Windows Server 2012 R2  | Yes |
| Windows Server 2012 | Yes |
| Windows Server 2008 R2 | No |
| Windows Server 2008 | No |
| Windows Server 2003 R2 | No |
| Windows Server 2003 | No |
| Windows Server 2000 | No |
| Virtual environment | Yes |
| Clustered servers | No |
| Writeable domain controllers | Yes |
| Read-only domain controller (RODC) | Yes |
| Domain member computers and servers | Yes |
| Agentless monitoring | No |
| Stand-alone or workgroup member computers | No |
| x64  | Yes |
| x86 | Yes |

Important

Migration from the Active Directory® Management Pack (AD MP) to Active Directory, Domain Services (ADDS) Management Pack is not supported, but a side-by-side installation of these two products is supported.

**For SCOM Support for Microsoft Windows Server 2016 and above, refer below links:**

<https://docs.microsoft.com/en-us/system-center/scom/system-requirements?view=sc-om-2016#microsoft-monitoring-agent-operating-system>

<https://docs.microsoft.com/en-us/system-center/scom/system-requirements?view=sc-om-2019#microsoft-monitoring-agent-operating-system>

<https://docs.microsoft.com/en-us/system-center/scom/system-requirements?view=sc-om-2022#microsoft-monitoring-agent-operating-system>

Note

The step-by-step procedures in this guide are based on the System Center Operations Manager 2016 or later user interface. The actual steps may vary if you are using a newer version.

Management Pack Scope

The AD DS Management Pack runs on Domain Controllers in your domain as well as Domain Members. It monitors the health of Domain Controllers as well as the health of the domain.

Prerequisites

The following requirements must be met to run this Management Pack:

* The AD DS Remote Server Administrations Tools must be installed on your Domain Controllers (DC). They are installed by default when a DC is promoted.
* System Center Operations Manager 2012 or newer
* Domain Controllers running Windows Server 2012 or newer

Mandatory Configuration

The following configurations are recommended on first installation of the ADDS Management Pack.

* [Best Practice: Create a Management Pack for Customizations](#CreateManagementPackForCustom)
* [Enable the Agent Proxy setting on all domain controllers.](http://technet.microsoft.com/en-us/library/ee662300.aspx)
* [Configure the domain member(s) to use for Domain Member Monitoring.](#DomainMemberConfig)

See Configuration tasks section for help with the above configurations

Files in this Management Pack

The Management Pack for ADDS includes the following files:

* Microsoft.Windows.Server.AD.Class.Library.mp
* Microsoft.Windows.Server.AD.DomainMemberMonitoring.mp
* Microsoft.Windows.Server.AD.2012.Discovery.mp
* Microsoft.Windows.Server.AD.2012.Monitoring.mp
* Microsoft.Windows.Server.AD.2012R2.Discovery.mp
* Microsoft.Windows.Server.AD.2012R2.Monitoring.mp
* Microsoft.Windows.Server.AD.2016.Discovery.mp
* Microsoft.Windows.Server.AD.2016.Monitoring.mp

Recommended Additional Management Packs

Although no further Management Packs are required for the Active Directory Management Pack to perform, the following Management Packs might be of interest because they complement the Active Directory® monitoring services:

 Windows Server DNS Management Pack

 File Replication Service and Distributed File System Replication Management Packs

 Windows Server Group Policy Management Packs

Management Pack Purpose

The Active Directory® Management Pack provides both proactive and reactive monitoring of your Active Directory deployment. It also monitors the overall health of the Active Directory system and alerts you to critical performance issues.

The monitoring provided by this Management Pack includes monitoring of the domain controllers and monitoring of health from the perspective of clients utilizing Active Directory resources. To monitor the domain controllers, the Active Directory Management Pack provides a predefined, ready-to-run set of processing rules, monitoring scripts, and reports that are designed specifically to monitor the performance and availability of the Active Directory domain controllers.

The client in your environment might experience connectivity and service issues even though the domain controller appears to be operating correctly. The Active Directory Domain Member Management Pack, included in the Active Directory Management Pack, helps to identify these issues. This Management Pack monitors the services provided by the domain controller. It provides information in addition to that collected directly on the domain controller about whether they are available by running synthetic transactions against the directory service, such as Lightweight Directory Access Protocol (LDAP) binds and LDAP pings.

In addition to health monitoring capabilities, this Management Pack provides a complete Active Directory monitoring solution by monitoring the health of vital processes that your Active Directory deployment depends upon, including the following:

 Replication

 Lightweight Directory Access Protocol (LDAP)

 Domain Controller Locator

 Trusts

 Net Logon service

 File Replication Service (FRS)

 Inter-site Messaging service

 Windows Time service

 Active Directory Web Services (ADWS)

 Active Directory Management Gateway Service

 Key Distribution Center (KDC)

 Monitoring service availability

 Collecting key performance data

With this Management Pack, information technology (IT) administrators can automate one-to-many management of users and computers, simplifying administrative tasks and reduce IT costs. Administrators can efficiently implement security settings, enforce IT policies, and minimize service outages.

In this section:

 [Monitoring Scenarios](#z5a9ff008734b4183946f840ae0464ab0)

 [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 Scenarios

The Active Directory Management Pack (ADMP) is designed to provide valuable monitoring information about the health of your directory service. The following nine scenarios describe the most common ADMP monitoring scenarios.

All the configuration options described in this document are optional and not required for a typical operating environment. Administrators can choose to set some options to more accurately monitor specific areas of their environment.

The following monitoring scenarios are discussed in this section of the guide:

* [Multi-Forest Monitoring](#za18381ac79714291ac3876b91625b089)
* [Replication](#z9ab66720d7b54e41b9018b579c9a157a)
* [Essential Services](#zc8576b3cb3f5471eb9d9223f543564f3)
* [Trust Monitoring](#zaa75788ed379465b8cad6e32b34eb354)
* [Directory Service Availability](#z9df695f6b0144e55b85de601c9664765)
* [Active Directory Database Monitoring](#z6750e1d7b4024b629ad8c2173fc7503c)
* [Time Skew Monitoring](#z9d66203863dd42d0bd7fb2db887788b7)
* [Active Directory Web Service Monitoring](#z6d4160e4f36f4a3599981d47d0504d13)
* [Domain Controller Performance](#z833cf5bf711b4279be3f81c09ec93f67)
* [Domain Member Perspective](#DomainMemberPerspective)

MP Health Roll Up

The Active Directory, Domain Services Management Pack views the Active Directory system as a layered structure, where each layer depends on the lower layer to be healthy. The top of this structure is the entire Active Directory environment, and the lowest level is all of the domain controllers. When enough of one layer changes state, the layer above it changes state to match. This action is called rolling up health.

The following diagram shows how the health states of components roll up in this Management Pack.



This model captures the idea that if only a few domain controllers are in an error state, it is unlikely that the entire site or forest they belong to is down. However, if most of the domain controllers in a site are in an error state, it is likely that the site is in trouble, while the forest that contains the site might still be healthy.

Health for each of the layers rolls up to next-highest layer when 60 percent of the objects in the lower layer change state. For rolling up health, an unknown state is an error state, while Maintenance mode is ignored. Active Directory domains are treated slightly differently than sites. Health from domain controllers rolls up to the domain, but domains do not roll up to the forest layer.

Monitoring Scenarios

### Multi-Forest Monitoring

The ADMP supports the monitoring of forests in addition to the forest where Operations Manager and the Management Pack are installed. You can deploy agents to remote forests. The Management Pack will gather health and performance data for the remote forest per the view of the domain controller where the agent is installed.

Monitoring of domain controllers in remote forests is nearly identical to the monitoring done of domain controllers in the local forest.

Important

All multiple forest monitoring scenarios, events, alerts, and performance data collections are fully supported in this release. Topology views automatically discover all forests that have two-way transitive trusts with the local forest; transitive trusts cannot use Selective Authentication. However, cross-forest monitoring of a forest that is not fully trusted is not supported.

Multi-forest discovery consists of two workflows:

1. Microsoft.AD.Topology.Discovery

2. Microsoft.AD.Remote.Topology.Discovery

Microsoft.AD.Topology.Discovery is the major workflow for multi-forest discovery, and it is defined in Microsoft.Windows.Server.AD.Library.mp.

This workflow runs on the Root Management Server (RMS) and discovers Active Directory instances such as forests, domains, sites, sitelinks, and domain controller computers in addition to relationships between those instances that are spread over different forests with two-way transitive trust.

Note

Because the RMS submits discovery data, it is required to enable the proxy at the RMS.

The other workflow, Microsoft.AD.Remote.Topology.Discovery, is defined in each version of discovery Management Pack (that is, Microsoft.Windows.Server.AD.[version].Discovery.MP) and runs on each of the domain controllers with Operations Manager agents deployed.

The major task of the Microsoft.AD.Remote.Topology.Discovery workflow is to discover connection objects. Also in this workflow, the proxy must be enabled (as described in [Enable the AgentProxySetting on All Domain Controllers](http://technet.microsoft.com/en-us/library/ee662300.aspx)) at each of the agents to complete discovery data submission.

The two workflows are configured to run once a day.

Replication

Replication of data is a key aspect of any Active Directory installation. Replication Monitoring ensures that replication is occurring correctly in your environment. The following three specific aspects of replication are monitored:

 Replication Partner Count. This aspect ensures that every domain controller has an acceptable number of partners with which to replicate. If a domain controller has either too many or too few partners, the health of the domain controller will be degraded.

 Replication Latency Monitoring. This aspect ensures that changes made to the Active Directory installation are being replicated throughout the environment in a timely manner. This is done by periodically checking replication health and delay. This aspect fails if a DC has not replicated within the configured timeframe or fails to replicate with a partner.

 Replication Queue Monitor. This aspect functions as a performance monitor as well as a replication health monitor. The replication queue, which is the number of replication requests that are pending on any one DC, is tracked and when the queue gets to large a warning or error is thrown. The replication queue can help you identify replication spikes or DC’s that are not able to keep up with the domain load.

Replication is the mechanism by which domain controllers in a domain exchange changes to the directory. This mechanism is essential to the operation of the Active Directory deployment in a forest. The topic of replication is both deep and wide, and a full view of every aspect of replication is beyond the scope of what the Active Directory Management Pack (ADMP) attempts to monitor. For this Management Pack, you should strive to monitor the critical aspects of replication to give information technology (IT) administrators an overall assessment of replication for their environment.

The following three specific aspects of replication are monitored:

 Replication Partner Count – This aspect validates that each domain controller does not have too many or too few replication partners.

 Replication Latency – This aspect validates that updates to the directory are propagated to other domain controllers within a reasonable timeframe.

 Replication Queue Monitor – This aspect validates that a DC is keeping up with the replication load and is not acting as a bottle neck.

These three aspects of replication are monitored to provide an overall view of the replication mechanism of the Active Directory environment. Sometimes, it will be appropriate to utilize a tool that is more specialized in monitoring replication. For example, if the Replication Provider verification fails, the guidance might be to use the Replprov tool to gather more detailed information about the failure.

Replication Partner Count

With replication, as one of the cornerstones of the Active Directory environment, it is essential that the domain controllers in the forest are all able to replicate with each other, and that there are not excessive connections being created between domain controllers. Excessive connections can degrade the performance of the forest, while a lack of connectivity can create replication site islands. A replication site island occurs when a single domain controller or group of domain controllers in a site do not have any connections to domain controllers in another site. The domain controllers in a replication site island are unable to propagate their own changes to the other domain controllers in the domain and forest.

The replication partner count specifically validates the following three cases are true:

 A domain controller always has at least one outbound connection. Because replication connections are always seen as inbound connections, there is no need to record outbound connections. This means that the replication partner count mechanism will validate that a minimum number of connections exist by checking all the other domain controllers in the domain to see if the domain controller in question has a connection.

Note

A domain containing a single domain controller is considered a lone domain controller, and the replication partner count check will be ignored.

 A domain controller has at least one connection to another site. When sites are created, they must have a way to replicate changes to domain controllers from other sites. By default, when a site is created beyond the initial Default-Site-First-Name site, the Enterprise Administrator needs to create a site link to connect these two sites. A site always needs to have at least one inter-site connection to another site.

Note

If the domain or forest contains only a single site, the replication site island check will be ignored.

 A domain controller does not have more than a specified number of connections. When a domain controller has too many connections, the performance of the directory can become degraded. The replication partner count validation mechanism checks that a domain controller does not have too many connections. The specific threshold is a parameter to the script, so that it can be overridden and customized for any environment.

Replication Latency

The purpose of replication latency monitoring is to ensure that changes are being properly replicated across the forest. An Active Directory deployment comprises domain controllers, all of which (excluding read-only domain controllers (RODCs)) can modify the collective directory. When a change is recorded, it will be replicated to neighboring domain controllers within a given time interval.

Replication latency monitoring in this Management Pack is done checking the replication status of a domain controller. It checks to verify that the domain controller replicates within the maximum allowed time of 60min for each partition. As well as verifying that the domain controller does not have any replication errors with its replication partners.

How and when replication occurs between domain controllers is heavily dependent on the site location of the domain controller. Replication can be divided into two categories:

 Replication between domain controllers that are within the same site (known as intra-site replication)

 Replication between domain controllers that are in different sites (known as inter-site replication)

When a change is made on a domain controller, the replication partners of that domain controller need to receive a copy of that change. Because domain controllers belonging to the same site are considered to be well connected, changes are proactively pulled by other domain controllers from the same site almost as soon as the changes are made. For domain controllers belonging to a separate site, the assumption is made that these domain controllers are not as well connected, so you should request changes only on a scheduled interval. This way, changes from the previous x minutes will be patched together and transferred at the same time.

Replication Queue Monitor

The Replication Queue Monitor verifies that a given domain controller is keeping up with the changes being applied in the domain. This check is a critical part of replication because it gives the IT worker a clear view of replication load on a DC and a domain. It is critical in tuning performance of the domain and hardware decisions.

Essential Services

The Active Directory system comprises several services, some that provide services directly and some that support the Active Directory system itself. For this reason, the Management Pack continually checks to ensure that these essential services are working correctly. Note that some services might or might not be monitored, depending on the version of Windows Server being used and the configuration of your environment. The services that this Management Pack monitors include the following:

 Distributed File System Replication (DFSR)

 Windows Time Service (W32time)

 Inter-site Messaging (ISM)

 Key Distribution Center (KDC)

 NT Directory Services (NTDS)

 Net Logon (NetLogon)

 Active Directory Web Service (ADWS)

The DFSR service provides a file replication service. The Management Pack examines your environment to determine if the required service is not running.

The Windows Time Service (W32time) is responsible for keeping the various domain controllers on your network in time synchronization with each other. This Management Pack verifies that W32time is running on all domain controllers that are monitored.

Inter-site Messaging is required on Windows 2000 Server domain controllers and Windows Server 2003 domain controllers that are not operating at the Windows Server 2003 forest functional level. Inter-site Messaging will be monitored where applicable.

The KDC is a key service for facilitating Kerberos in Active Directory deployments. The Management Pack will verify that the KDC service is running on all domain controllers being monitored.

On a domain controller that runs Windows Server 2008 or later, Active Directory Domain Services (AD DS) hosts the Active Directory processes. This service must be running for the Active Directory system to function.

The Net Logon (NetLogon) service is responsible for handling several fundamental Active Directory authentication and location services. The ADMP verifies that the NetLogon service is running on all domain controllers being monitored.

The Active Directory Web Service (ADWS) provides services that are required by the Active Directory Administrative Center and the Active Directory module for Windows PowerShell.

SYSVOL Availability

On every domain controller, the SYSVOL share must be accessible. The Management Pack tests the availability of the domain controller by attempting to map a network drive using the path \127.0.0.1\SYSVOL, which represents the SYSVOL directory on the domain controller. If the script that is associated with SYSVOL availability is not able to map a network drive, it generates an event indicating the error that is returned from the attempt. If the script can map a network drive to the domain controller, it will not generate an event, and it will subsequently remove the mapped drive.

Configuration

There are no recommended configuration settings for this scenario.

Trust Monitoring

Trusts between forests and domains are fundamental to the operation of the Active Directory deployment. This Management Pack monitors these trusts to ensure that services and resources in your environment will be available where appropriate.

TrustMon, which is included on Windows Server 2003 domain controllers and newer, is the Windows Management Instrumentation (WMI) trust monitoring provider. The Active Directory Monitor Trusts script uses TrustMon to enumerate the trusts on the local domain controller, and it generates alerts if any problems are found.

The Active Directory Monitor Trusts script configures the TrustMon WMI provider to return all trusts, and then it queries for all instances of the Microsoft\_DomainTrustStatus object in the \root\MicrosoftActiveDirectory WMI namespace.

For each object that is returned; if the TrustType property of the object is not Down-level or Up-level (the other options are Kerberos Realm and DCE, which cannot be monitored effectively by TrustMon), the trust is ignored.

If the TrustType of the object indicates that it can be monitored, the TrustStatus property of the object is checked. If TrustStatus is not 0, the trust is in an error state and the trust and its TrustStatusString (a textual description of the current state of the trust) are formatted and relayed as the trust status.

After all the Microsoft\_DomainTrustStatus objects have been processed, the local domain is obtained from the \root\MicrosoftActiveDirectory:Microsoft\_LocalDomainInfo object.

Directory Service Availability

For Active Directory, Domain Services Management Pack services include the following:

* Domain is available\*
* Able to ping and query the PDC\*
* A domain controller responds to IP pings
* A domain controller responds to LDAP queries within a threshold
* Able to query using LDAP all FSMO role holders
* A domain controller that is a global catalog role holder is available\*
* Group policy updates are succeeding\*
* A reliable time server is available in the domain\*
* A domain controller is advertising, DCLocator

\* Indicates monitors from the Domain Member Perspective MP

Active Directory Database Monitoring

Active Directory Database Monitoring verifies that the underlying files used to host the directory (sometimes referred to as the DIT) are in a consistent state, and that there is available room for the database files to grow. This includes both the database files and the log files on each domain controller that is monitored by the ADMP.

The Active Directory Database and Log File workflow monitors database and log file size and available free space on the associated disk volumes.

The Active Directory Database and Log File script first stores the returned values for drive free space and database size as performance data. The script then on subsequent runs again stores the returned values for drive free space and database log size as performance data. If both calls succeed, the script attempts to determine if a significant decrease has occurred in the amount of free space on either drive, and, if possible, it identifies the cause of the free space reduction.

To make this determination, the script records the following data:

 Active Directory Database (DIT) Size

 Log Size

 Free DB Space

 Free Log Space

 SYSVOL Size

 Last Run Time

Database and Log File Growth

When a domain controller is not in its first replication cycle, the Active Directory Database and Log File script performs a test to determine whether excessive growth in either the database or the log files is occurring.

Note

Immediately after Active Directory deployment and a computer becomes a domain controller, an initial, complete replication cycle must occur before the domain controller begins advertising its services on the network. During this initial replication cycle, the database and log file sizes are expected to grow significantly. This growth is not reported by the script as an error. However, for a new domain controller, the script still reports any low-disk-space conditions.

To determine whether the domain controller is in its initial replication cycle, an attempt is made to read the replUpToDateVector attribute on the LDAP://RootDSE object of the local computer. If the attribute exists, the domain controller has already completed its first replication cycle.

A comparison of the current and previous values for database and log file size is used to determine whether the database or log has grown more than 20 percent since the last time that the script ran. If excessive growth has occurred, an event is generated that indicates the amount of growth and the time difference (in minutes) between the current and previous measurements.

Note

The 20-percent value is fixed, and it cannot be configured by the user.

Required Disk Space

If the database and log files reside on separate logical drives, the script verifies that the logical drive holding the database file has the greater of 500,000 kilobytes (KB) or 20 percent of the current database size available. The script also verifies that the logical drive holding the log file has the greater of 200,000 KB or 5 percent of the current database size available.

If the database and log files reside on the same logical drive, the script verifies that the greater of 700,000 KB or 25 percent of the current size of the database is available on the drive.

First, the script determines whether the database and log files reside on the same logical drive. The script makes this determination by comparing the first two characters of the file path for both the database and the log files. (If one path uses a Universal Naming Convention [UNC] path name and the other path uses a drive\directory path name, the check fails.)

If both files reside on the same drive, the amount of free space that is required on the database drive is added to the amount of free space on the log drive.

The required amount of free space is then checked against the available free space. If the required free space is greater than the available free space, an event is generated. The event contains the current free space on the drive and the calculated, required free space on the drive.

Time Skew Monitoring

The authentication that the Active Directory application uses is built on the Kerberos authentication protocol, which assumes that all computers that participate in authentication are kept within five minutes of one another. Because all computers will have some amount of time skew between them, the ADMP continually verifies that all computers are within an acceptable time skew.

The Management Pack will generate a warning or an error depending on the amount of time skew. If the time skew is above the warning threshold, the time skew monitor for the domain controller is in a warning state. If the time skew is above the error threshold, the time skew monitor for this domain controller is in an error state.

For every domain controller that uses the Management Pack, it will compare its time to the time on the PDC. By default, an error is thrown when the time skew is greater than 120 seconds. Even though the domain can function with 5 minutes of skew it is best to keep the skew down below 2 minutes.

Note

The time source that the Management Pack uses is the PDC. Therefore, this monitor will not throw an error if the whole domain is skewed from real time. It will only error when individual DCs are skewed from each other. This was done to simplify the Management Pack and more closely represent the health of the domain. I.e. the domain does not need to be synced with an external time source for it to function.

Active Directory Web Service Monitoring

Active Directory Web Services (ADWS) is a new service beginning in Windows Server 2008 R2. The Active Directory Management Gateway Service is an equivalent service that can be added to Windows Server 2008 and Windows Server 2003. These services provide support for commands in the Active Directory module for Windows PowerShell commands, as well as the Active Directory Administrative Center. If ADWS or the Active Directory Management Gateway Service is not functioning properly on their respective operating systems, Windows PowerShell commands and the Active Directory Administrative Center will not function properly. The ADDS MP monitors the ADWS to ensure it is running and available.

| **Monitor** | **Description** |
| --- | --- |
| Active Directory Web Services Service Health | Verifies that Active Directory Web Services and the service port on servers that run Windows Server 2016 are functioning, and reports any service failures or port blockages. |

Domain Controller Performance

It is critical to an Active Directory environment that services and responses are not only available but that they can be located and queried within an acceptable amount of time. The specific areas of domain controller performance include the following:

* The LSASS process is using an acceptable amount of CPU resources.
* Binding can occur with a domain controller within an acceptable amount of time.
* FSMO roles bind times occur within an acceptable amount of time.

Including the above monitors several performance counters are collected and stored in the Operations Manager Data Warehouse. There are several performance reports available in the Monitoring tab that allow the IT worker to view the performance counters.

Domain Member Perspective

The Domain Member Monitoring Management Pack deploys a set of rules and monitors to a computer that represents an Active Directory member server or client. These rules and monitors provide monitoring data, such as connectivity, latency and availability, from the perspective of the member.

Your monitoring needs dictate where you decide to place the Active Directory client and how many clients you choose. When you make your decision, consider the following factors:

 Servers that have applications that depend on Active Directory Domain Services (AD DS), such as computers running Microsoft Exchange Server, are good candidates for client monitoring.

 The Active Directory client-monitoring measurements include network time. Therefore, measurements differ, depending on where your client computer is located. Use information about network speeds to place Active Directory Domain Member Monitoring on computers in strategic locations. For example, if you have a branch office that is connected to a domain controller with a T1 connection, you would probably use Domain Member Monitoring on one of the branch office computers to monitor the experience for the users who relate to the T1 connection.

 Domain Member Monitoring generates overhead and should not be used for every Active Directory client in an installation. Instead, turn it on for selected computers that give you a representative picture of the environment. For example, you might perform Domain Member Monitoring from one server in a branch office, or you might pick one server per Exchange Server deployment.

Configuring the Management Pack for Active Directory, Domain Services (ADDS)

Add sections for additional configuration tasks, and let customers know whether a task is required or optional.

This section provides guidance on configuring and tuning this Management Pack.

* [Best Practice: Create a Management Pack for Customizations](#z2)
* [Security Configuration](#z3)
* [Tuning Performance Threshold Rules](#z4)
* [Turn on Domain Member Perspective Monitoring](#DomainMemberConfig)

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 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.

Security Configuration

|  |  |  |
| --- | --- | --- |
| Run As Profile Name | Associated Rules and Monitors | Notes |
| Local System | All Rules and monitors run as Local System |  |

Tuning Performance Threshold Rules

The following table lists performance threshold rules that have default thresholds that might require additional tuning to suit your environment. Evaluate these rules to determine whether the default thresholds are appropriate for your environment. If a default threshold is not appropriate for your environment, you should obtain a baseline for the relevant performance counters, and then adjust the thresholds by applying an override to them.

|  |  |
| --- | --- |
| Rule Name | Default Threshold |
| AD Database File Disk Free Space Monitor | Warning: 20%, Error 10% |
| AD Log File Disk Free Space Monitor | Warning: 20%, Error 10% |
| AD Show Replication Check | Replication Delay Allowed: 65 (min) |
| Time Skew Monitor | Error Threshold: 120 (sec) |
| AD Replication Queue Monitor | Warning: 20, Error 50 |
| LSASS Process Monitor | Total CPU %: 80 |
| LDAP Bind Time Monitor | Warning: 5, Error 10 (sec) |
| Domain Naming Master LDAP Bind Performance Monitor | Warning: 5, Error 10 (sec) |
| Infrastructure Master LDAP Bind Performance Monitor | Warning: 5, Error 10 (sec) |
| PDC LDAP Bind Performance Monitor | Warning: 5, Error 10 (sec) |
| RID Master LDAP Bind Performance Monitor | Warning: 5, Error 10 (sec) |
| Schema Master LDAP Bind Performance Monitor | Warning: 5, Error 10 (sec) |
| Domain Naming Master Ping Performance Time Monitor | Warning: 5, Error 10 (sec) |
| Infrastructure Master LDAP Ping Performance Monitor | Warning: 5, Error 10 (sec) |
| PDC LDAP Ping Performance Monitor | Warning: 5, Error 10 (sec) |
| RID Master LDAP Ping Performance Monitor | Warning: 5, Error 10 (sec) |
| Schema Master LDAP Ping Performance Monitor | Warning: 5, Error 10 (sec) |
| Global Catalog Performance Monitor\* | Warning: 5, Error 10 (sec) |
| PDC Bind Performance Monitor\* | Warning: 5, Error 10 (sec) |
| PDC Ping Performance Monitor\* | Warning: 5, Error 10 (sec) |

\* Indicates monitors from the Domain Member Perspective MP

Turn on Domain Member Perspective Monitoring

After you import the Active Directory Domain Member Management Pack, Domain Member Monitoring is performed on computers that you add to the AD Domain Member Monitoring Discovery rule.

It is possible to enable AD Domain Member Monitoring Discovery on individual computer objects but it is recommended that you manage the computers via an Operations Manager group.

Caution

Do not enable Domain Member Monitoring on all your member servers or desktop client computers running Windows. If you have too many clients running transactions only for the sake of monitoring, you can degrade the performance of your Active Directory deployment. It is recommended to use 1-2 member servers based upon your network infrastructure and your monitoring needs.

To add a computer to the AD Domain Member Monitoring Discovery rule

|  |
| --- |
| 1. Create a group used to contain the member servers you wish to use as domain member monitors. see [Creating and Managing Groups](https://technet.microsoft.com/en-us/library/hh212842%28v%3Dsc.12%29.aspx) (https://technet.microsoft.com/en-us/library/hh212842(v=sc.12).aspx).
2. In the Operations Console, click Authoring.
3. Expand Management Pack Objects, and then click Object Discoveries.
4. In the Object Discoveries pane, right-click AD Domain Member Monitoring Discovery, click Overrides, click Override the Object Discovery, and then click For a group.
5. Note
	1. If you do not see the rule, check that your scope is set to include Active Directory Domain Member Perspective by clicking the Scope in the Operations Console toolbar.
6. In the Select Object dialog box, find the group of computers that you have created for the purpose of client monitoring, select it and then click OK.
7. In the Override Properties dialog box, ensure that the Override box that corresponds to Enabled in the Parameter Name column is selected, and then change Override Value to True.
8. If the Select Destination Management Pack drop down list is blank, select the Management Pack that you want to use to save this customization. If you have not yet created a Management Pack for your overrides, you can click New to create one now. Click OK.
 |

**Configuring Agent Computers to Run in Low-Privilege Scenarios**

Monitoring functionality on an agent computer is provided by both the Health Service (HealthService.exe) and the Action Account. On Windows Server, the Action Account must be a member of the local administrators group. You can use a low-privileged account for the agent’s Action Account under certain circumstances. However, configuring the Action Account with the necessary rights and privileges to run the Active Directory Management Pack features requires significant configuration on the Domain Controllers.

On Windows Server, the Action Account must have the following minimum privileges applied via group policy:

* Member of the **Local Users Group**
* Member of the **Local Performance Monitor Users** group
* Manage auditing and security log privilege (**SeSecurityPrivilege**)
* Generate security audits privilege (**SeAuditPrivilege**)
* Allow log on locally logon right (**SeInteractiveLogonRight**)

The following security changes can be made via Group Policy or done manually on each Domain Controller you wish to monitor.

* Read Access to registry keys (See the Access Types Required by the Active Directory Management Pack chart)
* Read Access to ntds.dit file (See the Access Types Required by the Active Directory Management Pack chart)
* Full access to %ProgramFiles%\Microsoft Monitoring Agent\Agent

Access Types Required by the Active Directory Management Pack

|  |  |  |
| --- | --- | --- |
| **Resource** | **Access Type** | **Instructions** |
| Registry keys | Read | Add the Action Account to the registry properties of **HKLM\System\CurrentControlSet\Service\** **NTDS\Parameters**, and provide Read access. This enables the Action Account to find the location of NTDS.dit and the Active Directory log files.You must add the Action Account to the registry properties on each domain controller. |
| Directories containing NTDS.dit and Active Directory log files | Read | The Action Account must have Read access to the file path location of NTDS.dit and the Active Directory log files.The directory location of NTDS.dit is:**HKLM\System\CurrentControlSet\Service\** **NTDS\Parameters\DSA Database File** The directory location of the Active Directory log files is: **HKLM\System\CurrentControlSet\Service\** **NTDS\Parameters\Database Log Files Path** You must provide access to the file path location on each domain controller. |

Also the Action Account must be added to the built in security group **Event Log Readers** in the domain of the domain controllers being monitored.

**Note:**

To monitor trusts the Action Account must be a member of either the Domain Admins group or the Administrators group in the domain in which trusts are monitored. If the Action Account is not a member of either of these groups you will continue to receive a failure message until you disable the following rule:

Disable rule: **Microsoft Windows Active Directory\Active Directory Monitor Trusts\Script-AD Monitor Trusts.**

Links

The following links connect you to information about common tasks that are associated with System Center Management Packs:

System Center Operations Manager

* [Management Pack Life Cycle](https://go.microsoft.com/fwlink/?linkid=2024509)
* [How to import, export, and remove an Operations Manager management pack](https://go.microsoft.com/fwlink/?linkid=2024512)
* [How to create a management pack for overrides](https://go.microsoft.com/fwlink/?linkid=2024520)
* [How to override a rule or monitor](https://go.microsoft.com/fwlink/?linkid=2024439)
* [How to enable or disable a rule or monitor](https://go.microsoft.com/fwlink/?linkid=2024524)
* [How to create a Run As account and associate with a Run As profile](https://go.microsoft.com/fwlink/?linkid=2024431)

Important

All information and content on non-Microsoft sites is provided by the owner or the users of the website. Microsoft makes no warranties, express, implied, or statutory, as to the information at this website.