



# OMi Management Pack for Microsoft Active Directory

Software Version: 1.00

Operations Manager i for Linux and Windows® operating systems

## User Guide

Document Release Date: June 2017

Software Release Date: May 2014



**Hewlett Packard**  
Enterprise

## Legal Notices

### Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

### Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

### Copyright Notice

© 2014-2017 Hewlett Packard Enterprise Development LP

### Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft group of companies.

UNIX® is a registered trademark of The Open Group.

## Documentation Updates

To check for recent updates or to verify that you are using the most recent edition of a document, go to: <https://softwaresupport.hpe.com/>.

This site requires that you register for an HPE Passport and to sign in. To register for an HPE Passport ID, click **Register** on the HPE Software Support site or click **Create an Account** on the HPE Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HPE sales representative for details.

## Support

Visit the HPE Software Support site at: <https://softwaresupport.hpe.com/>.

Most of the support areas require that you register as an HPE Passport user and to sign in. Many also require a support contract. To register for an HPE Passport ID, click **Register** on the HPE Support site or click **Create an Account** on the HPE Passport login page.

To find more information about access levels, go to: <https://softwaresupport.hpe.com/web/softwaresupport/access-levels>.

**HPE Software Solutions Now** accesses the Solution and Integration Portal website. This site enables you to explore HPE product solutions to meet your business needs, includes a full list of integrations between HPE products, as well as a listing of ITIL processes. The URL for this website is <https://softwaresupport.hpe.com/km/KM01702731>.

# Contents

Chapter 1: OMi Management Pack for Microsoft Active Directory .....	6
Chapter 2: Getting Started .....	7
Task 1: Adding Nodes to BSM 9.2x or OMi 10.x Console .....	7
Task 2: Enabling the Enrichment Rules .....	8
Task 3: Deploying the Microsoft Active Directory Discovery Aspect .....	8
Task 4: Verifying Discovery .....	10
Task 5: Deploying the Microsoft Active Directory Management Templates or Microsoft Active Directory Aspects .....	10
Management Pack Data Collection Process .....	10
Task 5a: Identifying and Deploying Microsoft Active Directory Management Template .....	11
Task 5b: Deploying Microsoft Active Directory Aspects .....	13
Checking Topology Synchronization Settings .....	14
Chapter 3: Components .....	15
Microsoft Active Directory Management Templates .....	15
Essential Microsoft Active Directory Management Template .....	19
List of Infrastructure Aspects .....	21
Extensive Microsoft Active Directory Management Template .....	21
List of Infrastructure Aspects .....	24
Hybrid Microsoft Active Directory Management Template .....	25
List of Infrastructure Aspects .....	27
Microsoft Active Directory Aspects .....	28
List of Microsoft Active Directory Aspects .....	30
Microsoft AD Authentication .....	30
Microsoft AD Availability (Agentless) .....	32
Microsoft AD Collection Schedule .....	33
Microsoft AD DFSR Throughput .....	33
Microsoft AD DFSR Volume .....	34
Microsoft AD DFSR Logs .....	35
Microsoft AD DFSR Performance .....	35
Microsoft AD DIT .....	37

Microsoft AD Directory Services Logs .....	38
Microsoft AD DNS .....	39
Microsoft AD DNS Logs .....	39
Microsoft AD DNS Records .....	40
Microsoft AD DNS Response .....	42
Microsoft AD Directory Access .....	42
Microsoft AD Discovery .....	44
Microsoft AD FSMO Consistency .....	45
Microsoft AD FSMO Response Time .....	46
Microsoft AD FSMO Role Movement .....	47
Microsoft AD Federation Service Logs .....	47
Microsoft AD Federation Services .....	48
Microsoft AD Global Catalog .....	49
Microsoft AD Global Catalog Access .....	50
Microsoft AD Group Policy .....	50
Microsoft AD Replication .....	51
Microsoft AD Replication Auto Baseline .....	52
Microsoft AD Replication Logs .....	53
Microsoft AD Replication Statistics .....	53
Microsoft AD Response Time .....	55
Microsoft AD SYSVOL .....	57
Microsoft AD Security .....	58
Microsoft AD Security Logs .....	59
Microsoft AD Services .....	60
Microsoft AD Structure Changes .....	63
Microsoft AD Trust .....	63
Microsoft AD Event Logs .....	64
Parameters .....	65
Microsoft Active Directory Parameters .....	65
OMi MP for Microsoft Active Directory Parameters .....	65
Tuning of Parameters .....	65
Configuration Items (CIs) and Configuration Item Types (CITs) .....	66
Run-time Service Model (RTSM) Views .....	66
Enrichment Rules .....	69
Health Indicators (HIs) and Event Type Indicators (ETIs) .....	70

Topology Based Event Correlation (TBEC) Rules .....	76
Operations Orchestration (OO) Flows .....	87
Graph Templates .....	92
Tools .....	93
<b>Chapter 4: Customizing OMi MP for Microsoft Active Directory .....</b>	<b>96</b>
Creating Microsoft Active Directory Management Template .....	96
Editing Microsoft Active Directory Management Template .....	97
Editing Parameters .....	98
Editing Aspects .....	99
<b>Chapter 5: Deployment Scenarios .....</b>	<b>101</b>
Deploying OMi MP for Microsoft Active Directory to Monitor Active Directory Replication .....	101
Deploying OMi MP for Microsoft Active Directory to monitor Active Directory Servers Using ADFS .....	102
<b>Chapter 6: Troubleshooting .....</b>	<b>103</b>
Licensing count is not updated .....	103
Microsoft Active Directory CI does not appear in RTSM .....	104
Management Templates and Aspects are not deployed on the Managed Nodes .....	104
No Data for Performance Manager i (PMi) Graphs or Reports .....	105
Performance Collection Fails .....	105
Failed Binary on Managed Node .....	106
Data Logging Policies Not Logging Data .....	106
Unable to collect or log perfmon counter metrics .....	106
Tracing .....	107
<b>Appendix: Data Sources for Logging .....</b>	<b>108</b>
<b>Send documentation feedback .....</b>	<b>121</b>

# Chapter 1: OMi Management Pack for Microsoft Active Directory

The Microsoft Active Directory helps manage your corporate identities, credentials, information protection, system, and application settings. The OMi Management Pack for Microsoft Active Directory (OMi MP for Microsoft Active Directory) works with Operations Manager i (OMi) and enables you to monitor Active Directory servers and underlying infrastructure operating in your environment. It includes indicators - Health Indicators (HIs), Event Type Indicators (ETIs), and Correlation Rules that categorize and correlate the events based on the type of occurrence and reports the health status of the Active Directory servers.

The OMi MP for Microsoft Active Directory provides Management Templates, Aspects, and Policy Templates for monitoring different features such as - Active Directory database files, Directory Information Tree (DIT) disk space, replication, response time, Domain Name System (DNS), and Windows Event Log. Management Templates can be deployed by an administrator for monitoring Active Directory servers in your environment. The Subject Matter Experts (SMEs) and developers can easily customize the Active Directory Management Templates.

The OMi MP for Microsoft Active Directory works with OMi and provides the following additional functionality to support unified monitoring solution:

- Configuration Item (CI) based development and configuration
- Provides agent and agentless monitoring for Active Directory instances


## Chapter 2: Getting Started

The following section provides step-by-step instructions about monitoring Active Directory servers using OMi MP for Microsoft Active Directory.

### Task 1: Adding Nodes to BSM 9.2x or OMi 10.x Console

**Note:** If the Node already exists in RTSM, you can skip this step and proceed to Task 2.

Before you begin monitoring, you need to add the nodes to the BSM or OMi console. Follow these steps:

1. Open the Monitored Nodes pane from the Administration:  
On BSM 9.2x, click **Admin > Operations Management > Setup > Monitored Nodes**.  
On OMi 10.x, click **Administration > Setup and Maintenance > Monitored Nodes**.
2. In the Node Views pane, click **Predefined Node Filters > Monitored Nodes**, and then click , and then click **Computer > <select the OS type>**. The Create New Monitored Nodes window opens.
3. Specify the Primary DNS Name and verify the IP Address.
4. Specify the Operating System and Processor Architecture of the node from the drop-down list, and then click **OK**.

The newly created node is saved as a Configuration Item (CI) instance in Run-time Service Model (RTSM).

**Note:** The node with Operations Agent needs to be activated on OMi server and certificate must be granted.




## Task 2: Enabling the Enrichment Rules

You must enable the following enrichment rules to populate the Microsoft Active Directory CI's display label with additional information about container or the hostname:

- `SoftwareElementDisplayLabelForNewHost`
- `SoftwareElementDisplayLabelForExistingHost`
- `SoftwareElementDisplayLabelPopulator`

To enable the Enrichment rules, follow these steps:

1. Open the Enrichment manager pane:  
  
On BSM 9.2x, click **Admin > RTSM Administration > Modeling > Enrichment manager**.  
  
On OMi 10.x, click **Administration > RTSM Administration > Modeling > Enrichment manager**.
2. In the Enrichment Rules pane, select **SoftwareElementDisplayLabelForNewHost** from the list.
3. Right-click and select **Properties**. The Enrichment Rule Properties window appears.
4. Click **Next**.
5. Select **Rule is Active**.
6. Click **Finish**.
7. In the Enrichment Rules pane, click  to save the changes.
8. Select **SoftwareElementDisplayLabelForExistingHost** and repeat steps 3 to 7.
9. Select **SoftwareElementDisplayLabelPopulator** and repeat steps 3 to 7.

## Task 3: Deploying the Microsoft Active Directory Discovery Aspect

The Microsoft Active Directory Discovery Aspect enables you to discover Active Directory Domain Controller CIs in your environment. To discover the Active Directory Domain Controller CI on the added managed nodes, you must deploy the Microsoft Active Directory Discovery Aspect.




1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.

On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.

2. In the Configuration Folders pane, select **Configuration Folders > Microsoft Application Management > Microsoft Active Directory > Aspects**.

3. In the Management Templates & Aspects pane, select **Microsoft AD Discovery** and click  **Assign and Deploy Item**. The Assign and Deploy Item wizard opens.

4. In the **Configuration Item** tab, click the Windows Node CI to which you want to deploy the Discovery Aspect, and then click **Next**.

5. (Optional). In the **Required Parameters** tab, click **Next**.

**Note:** Microsoft Active Directory Discovery Aspect do not have mandatory parameters. You will get a notification stating that There are no parameters that require editing for this Assignment.

6. (Optional). In the **All Parameters** tab on BSM 9.2x or **Parameter Summary** tab on OMi 10.x, click **Next**.

7. (Optional). If you do not want to enable the assignment immediately, follow the step:

On BSM 9.2x, clear the **Enable Assigned Objects** check box.

On OMi 10.x, clear the **Enable Assignment(s)** check box.

You can then enable the assignment later using the Assignments & Tuning pane.

8. Click **Finish**.

**Note:** After the Microsoft Active Directory Discovery Aspect is deployed, a message stating the Assignment and deployment jobs created appears. To check the status of the deployment jobs, go to the following location:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Deployment Jobs**.

On OMi 10.x, click **Administration > Monitoring > Deployment Jobs**.

## Task 4: Verifying Discovery

After you deploy the Microsoft Active Directory Discovery Aspect, you must verify if the CIs are populated in the View Explorer.

To view the CIs populated in the top view, follow these steps:

1. Open the Event Perspective pane:  
  
On BSM 9.2x, click **Applications > Operations Management > Event Perspective**.  
  
On OMi 10.x, click **Workspaces > Operations Console > Event Perspective**.
2. In the Browse Views pane, select the **AD\_Logical\_View**.

## Task 5: Deploying the Microsoft Active Directory Management Templates or Microsoft Active Directory Aspects

This section provides information about data collection, deploying the management templates and aspects. For more information about deploying Microsoft Active Directory Management, go to "[Task 5a: Identifying and Deploying Microsoft Active Directory Management Template](#)". For more information about deploying Microsoft Active Directory Aspects, go to "[Task 5b: Deploying Microsoft Active Directory Aspects](#)".

## Management Pack Data Collection Process

The frequency (polling interval) at which each Aspect must be monitored is predefined with a default value in a specific frequency parameter. Frequency parameter is an expert parameter that is defined for each of the metrics regardless of whether they are for generating events or not.

Following are the four predefined frequency parameters:

Scheduler Frequency	Default value
Very High	5 mins

Scheduler Frequency	Default value
High	15 mins
Medium	1 hour
Low	24 hours

After Management Templates and Aspects are deployed, collector is triggered based on the parameter value in a specific Aspect. You can modify the default value of the parameter at following two levels:

- During deployment of the Management Template or Aspects using the Management Templates & Aspects pane
- After deployment using the Assignments & Tuning pane.

For more information about how to modify the parameter values, see [Editing Parameters](#).

## Task 5a: Identifying and Deploying Microsoft Active Directory Management Template

You **must** deploy the Microsoft Active Directory Discovery Aspect even if the CIs are already populated by any other source such as SiteScope, DDM and so on. For more information, see ["Task 3: Deploying the Microsoft Active Directory Discovery Aspect"](#).

Before deploying Microsoft Active Directory Management Templates, you must identify the Microsoft Active Directory Management Template suitable for your environment by following these recommendations:


- If you want to monitor the basic features of Microsoft Active Directory deployment such as the availability and basic performance of Microsoft Active Directory servers, you can deploy **Essential Microsoft Active Directory Management Template**.
- If you want to monitor basic feature along with advance features of Microsoft Active Directory deployment such as the in-depth monitoring and advanced performance of Microsoft Active Directory servers, you can deploy **Extensive Microsoft Active Directory Management Template**.
- If you want to use both agent and agentless monitoring, you can deploy **Hybrid Microsoft Active Directory Management Template**.

To deploy Microsoft Active Directory Management Template to the Domain Controller CIs, follow these steps:


1. Open the Management Templates & Aspects pane:


On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.

On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.

2. In the Configuration Folders pane, select **Configuration Folders > Microsoft Application Management > Microsoft Active Directory > Management Templates**.
3. In the Management Templates & Aspects pane, select the Management Template that you want to deploy, and then click  **Assign and Deploy Item**. The Assign and Deploy wizard opens.
4. In the **Configuration Item** tab, click the Active Directory Domain Controller CI to which you want to assign the Management Template. Click **Next**.
5. (Optional). In the **Required Parameters** tab, click **Next**.

**Note:** Microsoft Active Directory Management Templates do not have mandatory parameters. You will get a notification stating that There are no parameters that require editing for this Assignment.

6. (Optional). In the **All Parameters** tab on BSM 9.2x or **Parameter Summary** tab on OMi 10.x, you can change the default values of the parameters. To edit the parameters, follow these steps:
  - a. Double-click the parameter, or select the parameter from the list, and then click . The Edit Parameter window opens.
  - b. Change the default value and click **OK**.

**Note:** In the **All Parameters** tab on BSM 9.2x or **Parameter Summary** tab on OMi 10.x, you can override the default values of any parameter. You can specify a value for each parameter at the Management Template level. By default, parameters defined as expert parameters are not shown. To show expert parameters, click  **Show Expert Parameters**.

- c. Click **Next**.
7. (Optional). In the **Configure Options** tab, if you do not want to enable the assignment immediately, follow the step:

On BSM 9.2x, clear the **Enable Assigned Objects** check box.

On OMi 10.x, clear the **Enable Assignment(s)** check box.

You can then enable the assignment later using the Assignments & Tuning pane.

8. Click **Finish**.

## Task 5b: Deploying Microsoft Active Directory Aspects


You **must** deploy the Microsoft Active Directory Discovery Aspect even if the CIs are already populated by any other source such as SiteScope, DDM and so on. For more information, see "[Task 3: Deploying the Microsoft Active Directory Discovery Aspect](#)".

To deploy Microsoft Active Directory Aspects to the Domain Controller CIs, follow these steps:


1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.

On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.

2. In the Configuration Folders pane, select **Configuration Folders > Microsoft Application Management > Microsoft Active Directory > Aspects**.
3. In the Management Templates & Aspects pane, select the Aspect you want to deploy, and then click  **Assign and Deploy Item**. The Assign and Deploy wizard opens.
4. In the **Configuration Item** tab, select the Domain Controller CI to which you want to assign the Aspect and then click **Next**.
5. *(Optional)*. In the **Required Parameters** tab, click **Next**.

**Note:** Microsoft Active Directory Aspects do not have Mandatory Parameters. You will get a notification stating that There are no parameters that require editing for this Assignment.

6. *(Optional)*. In the **All Parameters** tab on BSM 9.2x or **Parameter Summary** tab on OMi 10.x, you can change the default values of the parameters. To edit the parameters, follow these steps:
  - a. Double-click the parameter, or select the parameter from the list, and then click . The Edit Parameter window opens.
  - b. Change the default value and click **OK**.
  - c. Click **Next**.
7. *(Optional)*. In the **Configure Options** tab, if you do not want to enable the assignment immediately, follow the step:

On BSM 9.2x, clear the **Enable Assigned Objects** check box.

On OMi 10.x, clear the **Enable Assignment(s)** check box.


You can then enable the assignment later using the Assignments & Tuning pane.

8. Click **Finish**.

## Checking Topology Synchronization Settings

**Note:** It is recommended to check the Topology Synchronization settings if a Node or a CI is monitored by Operations Manager.

To check the Topology Synchronization settings, follow these steps:

1. Open the Infrastructure Settings from the Administration:  
  
On BSM 9.2x, click **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.  
  
On OMi 10.x, click **Administration > Setup and Maintenance > Infrastructure Settings**.
2. In the **Infrastructure Settings** pane, select **Applications > Operations Management**.
3. In the **Operations Management - HPOM Topology Synchronization Settings**, the packages for Topology Sync contains the packages that are used for topology synchronization. Ensure that you have the package- **default;nodegroups;operations-agent;HPOprSys;HPOprAds** along with the other Topology Sync packages.
4. If the package is not available, add the toposync package by following these steps:
  - a. In the Packages for Topology Sync, click .
  - b. In Value, add **default;nodegroups;operations-agent;HPOprSys;HPOprAds** and click **Save**.

# Chapter 3: Components

The OMi MP for Microsoft Active Directory includes the following components for monitoring Microsoft Active Directory setup in an environment:

- [Microsoft Active Directory Management Templates](#)
- [Microsoft Active Directory Aspects](#)
- [Parameters](#)
- [Configuration Items \(CIs\) and Configuration Item Types \(CITs\)](#)
- [Run-time Service Model \(RTSM\) Views](#)
- [Enrichment Rules](#)
- [Health Indicators \(HIs\) and Event Type Indicators \(ETIs\)](#)
- [Topology Based Event Correlation \(TBEC\) Rules](#)
- [Graph Templates](#)
- [Operations Orchestration \(OO\)](#)
- [Tools](#)

## Microsoft Active Directory Management Templates

The Microsoft Active Directory Management Templates provide a complete monitoring solution for monitoring the availability, health, and performance of the Microsoft Active Directory servers in an environment.

By default, the OMi MP for Microsoft Active Directory consists of a set of Management Templates. You can deploy these Management Templates and monitor the Domain Controllers in your environment. The Microsoft Active Directory Management Template consists of several Aspects which enables you to monitor Active Directory setup in an environment. Based on your monitoring requirements, you can also customize the Microsoft Active Directory Management Template. In addition, you can also create Management Templates using Microsoft Active Directory Aspects.



## Overview

The OMi MP for Microsoft Active Directory comprises the following Management Templates:

- [Essential Microsoft Active Directory Management Template](#)
- [Extensive Microsoft Active Directory Management Template](#)
- [Hybrid Microsoft Active Directory Management Template](#)

### How to Access Microsoft Active Directory Management Templates

1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.

On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.

2. In Configuration Folder pane, click **Configuration Folders > Microsoft Application Management > Microsoft Active Directory > Management Templates**.

## Tasks

### How to Deploy Microsoft Active Directory Management Templates

For more information about deploying Microsoft Active Directory Management Template, [Task 5: Deploying the Microsoft Active Directory Management Templates or Microsoft Active Directory Aspects](#).

How to Automatically Assign Microsoft Active Directory Management Templates and Microsoft Active Directory Aspects


To automatically assign Microsoft Active Directory Management Templates or Microsoft Active Directory Aspects, follow these steps:

1. Open the Automatic Assignment Rules:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Automatic Assignment Rules**.

On OMi 10.x, click **Administration > Monitoring > Automatic Assignment Rules**.


Automatic Assignment Rules consists of Auto-Assignment Rules pane at the top and Parameters pane at the bottom.

2. In the Auto-Assignment Rules pane, click  and select the appropriate option. The Create Auto-Assignment Rule wizard opens.
3. In the **Select Target View** tab, select the view for which you want to create the automatic assignment rule, and then click **Next**.
4. In the **Select Item to Assign** tab, click the Management Template or Aspect that you want to automatically assign to all the CIs, and then click **Next**.

The latest version of the Management Template or Aspect that you want to assign is selected by default. Click **Next**.

5. *(Optional)*. In the **Required Parameters** tab, click **Next**.

**Note:** Microsoft Active Directory Management Templates or Aspects do not have mandatory parameters. You will get a notification stating that There are no parameters that require editing for this Assignment.

6. *(Optional)*. In the **All Parameters** tab on BSM 9.2x and **Parameter Summary** tab on OMi 10.x, you can change the default value of parameters by following these steps:
  - a. Double-click the parameter you want to edit or select the parameter from the list and click  **Edit**. The Edit Parameter window opens.
  - b. Modify the value and click **OK**.
7. Click **Next**.
8. *(Optional)*. In the **Configure Options** tab, clear the **Activate Auto- Assignment Rule** check box if you do not want to activate the assignment rule immediately. You can activate automatic assignment rules later using the Automatic Assignment Rules pane at **Administration > Monitoring > Automatic Assignment Rules**.
9. Click **Finish** to save the changes. The assignment rule is added to the list of auto-assignment rules.

An assignment may trigger an event to be sent to OMi if one of the following situations applies:

- A deployment job fails.
- An auto-assignment fails.
- An auto-assignment succeeds. This behavior can be configured in the Infrastructure Settings.

You can check if the automatic assignment rule successfully created the expected assignments as by following these steps:

1. Open the Assignments & Tuning pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Assignments & Tuning**.

On OMi 10.x, click **Administration > Monitoring > Assignments & Tuning**.


2. In the **Browse Views** tab, select the view you identified while creating your automatic assignment rule.
3. Expand the view, and select a node that corresponds to the root CI type of the assigned item. Assignments created as a result of Automatic Assignment Rules are shown in the list of assignments at the top of the right pane, and have the value Auto-Assignment in the column Assigned By.

You can consider the following options for tuning the assignment:

- Use the Auto- Assignment Rules pane to tune the parameter values for all assignments triggered by the automatic assignment rule.
- Use the Assignments pane to tune, redeploy, delete, and enable or disable individual assignments.

### How to Display an Inventory Report for Microsoft Active Directory Management Template

The Inventory Report displays the Management Templates, Aspects, and Policy Templates that are available on a server. To display an Inventory Report for Microsoft Active Directory Management Template, follow these steps:

1. Select the Management Template for which you want to create the report for.
2. Click  **Generate Inventory Report** in the Configuration Folders pane.

The report displays the Management Templates, Aspects, and Policy Templates that are available on the server.

You can display additional types of reports from the Assignments & Tuning pane.

# Essential Microsoft Active Directory Management Template

The Essential Microsoft Active Directory Management Template can be used to monitor the basic features of Active Directory servers in an environment. The Essential Microsoft Active Directory Management Template contains the most essential features for monitoring the availability and performance of Microsoft Active Directory setup.

You have a Microsoft Active Directory set up in your environment, and want to check the availability of the Active Directory servers and monitor the basic functionality of Microsoft Active Directory features - replication, DIT, response time, DNS, Windows Event Log. In such a scenario, you can deploy Essential Microsoft Active Directory on all the Active Directory Domain Controller CIs. The Essential Active Directory Management Template consists of specific Aspects to monitor these features.

**Note:** To use and deploy Infrastructure Aspects, you must install OMi Management Pack for Infrastructure software.

## How to Access the Essential Microsoft Active Directory Management Template

1. Open the Management Templates & Aspects pane:  
On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.  
On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.
2. In Configuration Folders pane, click **Configuration Folders > Microsoft Application Management > Microsoft Active Directory > Management Templates > Essential Microsoft Active Directory Management Template**.

## User Interface Reference

### Management Template - General

UI Element	Description
Name	Essential Microsoft Active Directory Management Template.

UI Element	Description
<b>Description</b>	Monitors the most essential features of Microsoft Active Directory.
<b>ID</b>	A unique identifier for the Graphic User Interface (GUI) version of the Management Template.
<b>Version ID</b>	A unique identifier for this version of the Essential Microsoft Active Directory Management Template.
<b>Version</b>	The current version of the Management Template. In this instance, the version of the Management Template is 1.0.
<b>Change log</b>	The text that describes what is new or modified in this version of the Management Template.

#### Management Template - Topology View

UI Element	Description
<b>Topology View</b>	AD_Logical_View is the Topology View for Essential Microsoft Active Directory Management Template. It contains Microsoft Active Directory related CITs that you want to manage using the Management Template.
<b>CI Type</b>	The type of the CI to which the Management Template can be assigned.

#### Management Template - Aspects

The Essential Microsoft Active Directory Management Template contains the following Microsoft Active Directory Aspects:

- [Microsoft AD Collection Schedule](#)
- [Microsoft AD DFSR Performance](#)
- [Microsoft AD Directory Access](#)
- [Microsoft AD DIT](#)
- [Microsoft AD DNS Response](#)
- [Microsoft AD Federation Services](#)
- [Microsoft AD FSMO Consistency](#)
- [Microsoft AD FSMO Response Time](#)
- [Microsoft AD Global Catalog](#)
- [Microsoft AD Replication](#)
- [Microsoft AD Replication Statistics](#)

- [Microsoft AD Response Time](#)
- [Microsoft AD Security](#)
- [Microsoft AD Services](#)
- [Microsoft AD SYSVOL](#)

## List of Infrastructure Aspects

The Essential Microsoft Active Directory Management Template contains the following Infrastructure Aspects:

### **System Fault Analysis**

The System Fault Analysis Aspect monitors the kernel log file, boot log file, and event log file for critical error conditions and instructions.

### **Resource Bottleneck Diagnosis**

The Resource Bottleneck Diagnosis Aspect identifies congestion and bottleneck conditions for system resources like the CPU, memory, network and disk. CPU bottleneck monitoring is based on global CPU utilization and load average (Run Queue Length). Memory bottleneck monitoring is based on memory utilization, free memory available, and memory swap out rate. File system monitoring is based on space utilization level for busiest file-system on the node. Network monitoring is based on Packet collision rate, packet error rate, and outbound queue length.

### **System Infrastructure Discovery**

The System Infrastructure Discovery Aspect discovers and gathers information regarding the system resources, operating system, and applications on a managed node.

## Extensive Microsoft Active Directory Management Template

The Extensive Microsoft Active Directory Management Template contains the complete set of Microsoft Active Directory Aspects and Infrastructure Aspects for monitoring availability, performance, and health of Microsoft Active Directory. The Extensive Microsoft Active Directory Management Template can be used for monitoring the advanced features of Microsoft Active Directory. It provides an in-depth monitoring of Active Directory deployment.

You have a Microsoft Active Directory set up in your environment, and want to monitor the in-depth installation and the advance features of Microsoft Active Directory functionality - replication, response time, DIT, consistency, and Role Movement. In such a scenario, you can deploy Extensive Microsoft Active Directory Management Template.

**Note:** To use and deploy Infrastructure Aspects, you must install OMi Management Pack for Infrastructure software.

### How to Access the Extensive Microsoft Active Directory Management Template

1. Open the Management Templates & Aspects pane:  
  
On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**  
  
On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**
2. In Configuration Folders pane, click **Configuration Folders > Microsoft Application Management > Microsoft Active Directory > Management Templates > Extensive Microsoft Active Directory Management Template**.

## User Interface Reference

### Management Template - General

UI Element	Description
<b>Name</b>	Extensive Microsoft Active Directory Management Template
<b>Description</b>	Provides in-depth monitoring of Microsoft Active Directory Installation.
<b>ID</b>	A unique identifier for the GUI version of the Management Template.
<b>Version ID</b>	A unique identifier for this version of the Extensive Microsoft Active Directory Management Template.
<b>Version</b>	The current version of the Management Template. In this instance, the version of the Management Template is 1.0.
<b>Change Log</b>	Text that describes what is new or modified in this version of the Extensive Microsoft Active Directory Management Template.



#### Management Template - Topology View

UI Element	Description
<b>Topology View</b>	AD_Logical_View is the Topology View for Extensive Microsoft Active Directory Management Template. It contains the CIs that you want to manage using the Management Template.
<b>CI Type</b>	The type of the CI to which the Management Template can be assigned.

#### Management Template - Aspects

The Extensive Microsoft Active Directory Management Template comprises the following Active Directory Aspects:

- [Microsoft AD Authentication](#)
- [Microsoft AD Collection Schedule](#)
- [Microsoft AD DFSR Throughput](#)
- [Microsoft AD DFSR Volumes](#)
- [Microsoft AD DFSR Logs](#)
- [Microsoft AD DFSR Performance](#)
- [Microsoft AD Directory Access](#)
- [Microsoft AD Directory Services Logs](#)
- [Microsoft AD DIT](#)
- [Microsoft AD DNS](#)
- [Microsoft AD DNS Logs](#)
- [Microsoft AD DNS Records](#)
- [Microsoft AD DNS Response](#)
- [Microsoft AD Federation Service Logs](#)
- [Microsoft AD Federation Services](#)
- [Microsoft AD FSMO Consistency](#)
- [Microsoft AD FSMO Response Time](#)
- [Microsoft AD FSMO Role Movement](#)
- [Microsoft AD Global Catalog](#)
- [Microsoft AD Global Catalog Access](#)
- [Microsoft AD Group Policy](#)

- [Microsoft AD Replication](#)
- [Microsoft AD Replication Logs](#)
- [Microsoft AD Replication Statistics](#)
- [Microsoft AD Response Time](#)
- [Microsoft AD Security](#)
- [Microsoft AD Security Logs](#)
- [Microsoft AD Services](#)
- [Microsoft AD Structure Changes](#)
- [Microsoft AD SYSVOL](#)
- [Microsoft AD Trust](#)

## List of Infrastructure Aspects

The Extensive Microsoft Active Directory Management Template contains the following Infrastructure Aspects:

### **Space Availability and Disk IOPS**

The Space Availability and Disk IOPS Aspect monitors the disk IO operations and space utilization of the system.

### **Bandwidth Utilization and Network IOPS**

The Bandwidth Utilization and Network IOPS Aspect monitors IO operations, and performance of the systems in the network. It monitors the network I/O operations and performance based on the bandwidth used, outbound queue length and average bytes transferred per second.

### **CPU Performance**

The CPU Performance Aspect monitors the overall CPU performance like the CPU utilization percentage and spike in CPU usage. Individual CPU performance monitoring is based on total CPU utilization, CPU utilization in user mode, CPU utilization in system mode and interrupt rate.

### **Memory and Swap Utilization**

The Memory and Swap Utilization Aspect monitors memory performance of the system. Memory performance monitoring is based on Memory utilization (in percentage), Swap space utilization (in percentage), Free memory available (in MBs) and Free swap space available (in MBs).

### **System Infrastructure Discovery**

The System Infrastructure Discovery Aspect discovers and gathers information regarding the system

resources, operating system, and applications on a managed node.

## Hybrid Microsoft Active Directory Management Template

The Hybrid Microsoft Active Directory Management Template comprises of Operations Agent and agentless monitors for monitoring availability and performance of Microsoft Active Directory.

### How to Access Hybrid Microsoft Active Directory Management Template

1. Open the Management Templates & Aspects pane:  
  
On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**  
  
On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**
2. In Configuration Folders pane, click **Configuration Folders > Microsoft Application Management > Microsoft Active Directory > Management Templates > Hybrid Microsoft Active Directory Management Template**.

## User Interface Reference

### Management Template - General

Provides an overview of the general attributes of the Management Template.

UI Element	Description
<b>Name</b>	Hybrid Microsoft Active Directory Management Template
<b>Description</b>	Comprises of agent and agent less monitors for monitoring availability and performance of Microsoft Active Directory
<b>ID</b>	A unique identifier for the GUI version of the Management Template.
<b>Version ID</b>	A unique identifier for this version of the Hybrid Microsoft Active Directory Management Template.
<b>Version</b>	The current version of the Management Template. In this instance, the current version is 1.0.

UI Element	Description
<b>Change Log</b>	Text that describes what is new or modified in this version of the Hybrid Microsoft Active Directory Management Template.

#### Management Template - Topology View

UI Element	Description
<b>Topology View</b>	<b>AD_Logical_View</b> is the Topology View for Hybrid Microsoft Active Directory Management Template. It contains the CIs that you want to manage using the Management Template.
<b>CI Type</b>	The type of the CI to which the Management Template can be assigned.

#### Management Template - Aspects

The Hybrid Microsoft Active Directory Management Templates comprises the following Active Directory Aspects:

- [Microsoft AD Authentication](#)
- [Microsoft AD Availability \(Agentless\)](#)
- [Microsoft AD Collection Schedule](#)
- [Microsoft AD DFSR Throughput](#)
- [Microsoft AD DFSR Performance](#)
- [Microsoft AD Directory Access](#)
- [Microsoft AD DIT](#)
- [Microsoft AD DNS](#)
- [Microsoft AD DNS Records](#)
- [Microsoft AD DNS Response](#)
- [Microsoft AD Federation Services](#)
- [Microsoft AD FSMO Consistency](#)
- [Microsoft AD FSMO Response Time](#)
- [Microsoft AD Global Catalog](#)
- [Microsoft AD Group Policy](#)
- [Microsoft AD Replication](#)
- [Microsoft AD Replication Logs](#)

- [Microsoft AD Replication Statistics](#)
- [Microsoft AD Response Time](#)
- [Microsoft AD Security](#)
- [Microsoft AD Services](#)
- [Microsoft AD SYSVOL](#)
- [Microsoft AD Trust](#)

## List of Infrastructure Aspects

The Hybrid Microsoft Active Directory Management Template contains the following Infrastructure Aspects to monitor infrastructure elements:

### **Bandwidth Utilization and Network IOPS**

The Bandwidth Utilization and Network IOPS Aspect monitors IO operations, and performance of the systems in the network. It monitors the network I/O operations and performance based on the bandwidth used, outbound queue length and average bytes transferred per second.

### **Space Availability and Disk IOPS**

The Space Availability and Disk IOPS Aspect monitors the disk IO operations and space utilization of the system.

### **Memory and Swap Utilization**

The Memory and Swap Utilization Aspect monitors memory performance of the system. Memory performance monitoring is based on Memory utilization (in percentage), Swap space utilization (in percentage), Free memory available (in MBs) and Free swap space available (in MBs).

### **CPU Performance**

The CPU Performance Aspect monitors the overall CPU performance like the CPU utilization percentage and spike in CPU usage. Individual CPU performance monitoring is based on total CPU utilization, CPU utilization in user mode, CPU utilization in system mode, and interrupt rate.

### **System Infrastructure Discovery**

The System Infrastructure Discovery Aspect discovers and gathers information regarding the system resources, operating system, and applications on a managed node.

## Microsoft Active Directory Aspects

Microsoft Active Directory Aspects are used to monitor availability, health, and performance of Microsoft Active Directory server - replication, DIT disk space, DNS, windows log event. Microsoft Active Directory Aspects include Policy Templates, instrumentation, and Parameters for monitoring Active Directory setup in an environment.

### How to Access Microsoft Active Directory Aspects

1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.

On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.

2. In the Configuration Folders pane, click **Configuration Folders > Microsoft Application Management > Microsoft Active Directory > Aspects**.

## User Interface Reference

<b>General</b>	Provides an overview of the general attributes such as, the Name, Description, Version, ID and Version ID of the Aspect.
<b>CI Type</b>	The type of CIs that the Aspect can be assigned to. This is the type of CI to which the Management Template can be assigned. The Microsoft Active Directory Aspects contain DomainController, DomainController Resource, and DomainControllerRole CITs.
<b>Instrumentation</b>	Provides a single package which contains the binaries for discovery, collection, and data logging.
<b>Aspects</b>	Provides an overview of the aspects that the Microsoft Active Directory Aspect contain.
<b>Policy Templates</b>	Provides an overview of the Policy Templates that the Microsoft Active Directory Aspect contain.

# Tasks

## How to Deploy Microsoft Active Directory Aspects




For more information about deploying Microsoft Active Directory Aspects, see "[Task 5b: Deploying Microsoft Active Directory Aspects](#)".

## How to Create Microsoft Active Directory Aspects


1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**.


On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**.

2. In Configuration Folder pane, click **Configuration Folders > Microsoft Application Management > Microsoft Active Directory > Aspects**.
3. In the Management Template & Aspects pane, click , and then click  **Create Aspect**. The Add New Aspect window opens.
4. In the **General** tab, specify a Name for the new aspect, and then click **Next**.
5. In the **CI Types** tab, select one or more CITs from **Available CI Types** pane to associate with the Aspect and click  to add them to the **Assigned CI Types** pane, and then click **Next**.

**Note:** You can use **CTRL** or **SHIFT** key to select multiple CITs.


6. In the **Instrumentation** tab, click  **Add Instrumentation** to add instrumentation categories to the Aspect. The Add Instrumentation window opens which lists the instrumentation that you want to add. Select the instrumentation and click **OK**. Click **Next**.

**Note:** You can add instrumentation based on your requirement. You can skip this step if you do not want to add instrumentation to the Aspect.



7. In the **Aspects** tab, click  **Add Existing Aspect**. The Add Existing window opens which enables you to select an existing Aspect that you want to add within an Aspect. Click an Aspect and then click **OK**. You can use **CTRL** or **SHIFT** key to select multiple Aspects. Click **Next**.

**Note:** If you are adding existing Aspects within an Aspect, ensure at least one of the CITs of the Aspect that you add must be a CIT or a parent CIT of the existing Aspect.




8. (Optional). In the **Policy Template** tab, click  **Add Policy Templates From List**. The Add New Policy Template to Aspect window opens. Select the Policy Templates that you want to add and click **OK**.

**Note:** You can use **CTRL** or **SHIFT** key to select multiple Policy Templates.

9. If suitable Policy Templates do not exist, follow these steps to add a new Policy Template:
  - a. Click , and then click  **Add New Policy Template** to create them from here. The Select New Policy Template dialog box opens.
  - b. Select the **Measurement Threshold** policy template from the **Type** drop-down list and click **OK**. The Policy Related Information dialog box opens.
  - c. In the Policy Related Information dialog box, specify a unique policy **Name** and click **OK**. A new Policy Template is added.
10. Click **Next**.
11. In the **Parameters** tab, you see a list of parameters from the Policy Templates that you added to this Aspect.

To edit parameters:

- a. Double-click the parameter or select the parameter from the list and click  **Edit**. The Edit Parameter dialog box opens.
  - b. Modify the default parameter value and click **OK**.
12. In the Add New Aspect window, click **Finish** to save the Aspect. The new Aspect appears in the Management Template & Aspects pane.

## List of Microsoft Active Directory Aspects

The OMi MP for Microsoft Active Directory consists the following Microsoft Active Directory Aspects:

### Microsoft AD Authentication

This Aspect monitors Active Directory (AD) Authentication errors.

CI Type	Policy Template	Indicator	Description	Policy Type
domaincontroller	MSAD_SecErrGrantedAccess	NA	Checks the Errors Granted Access counters for the number of access attempts that opened files successfully but were allowed no further access.	Measurement Threshold Template
	MSAD_SecErrorsLogon	LogonErrors:VeryHigh / LogonErrors:Normal, LogonErrors:High / LogonErrors:Normal	Checks the Errors Logon for the number of denied logon attempts to the server.	
domaincontroller	MSAD_AuthenticationSchedule	NA	This policy maintains the Schedule of Essential Authentication Aspect.	ConfigFile Template
domaincontroller	MSAD_SecErrAccessPermissions	AccessPermissionsErrors:VeryHigh / AccessPermissionsErrors:Normal, AccessPermissionsErrors:High / AccessPermissionsErrors:Normal	Checks the Errors Access Permissions for the number of attempts to access the server that were denied.	Measurement Threshold Template
domaincontroller	MSAD_	NA	Generates	Windows

CI Type	Policy Template	Indicator	Description	Policy Type
oller	DirComputerModif		alert messages if there is any modification to a computer in the domain.	Managem ent Interface Template
domaincontr oller	MSAD_ IQKerberosAuthentic ations	KerberosAuthenticationRate:V eryHigh KerberosAuthenticationRate:Hi gh KerberosAuthenticationRate:N ormal	Security System- Wide Statistics - Kerberos Authenticati ons	Measurem ent Threshold Template
	MSAD_ NTLMAuthentications	NTLMAuthenticationRate:Very High NTLMAuthenticationRate:High NTLMAuthenticationRate:Nor mal	Security System- Wide Statistics - NTLM Authenticati ons	

## Microsoft AD Availability (Agentless)

This aspect monitors the availability of Microsoft Active Directory Server and DNS Server using agent less monitors.

CI Type	Policy Template	Indicator	Description	Policy Type
domaincontroller Node	MSAD_DNS_Availability (:Microsoft_Active_ Directory_Server_Monitor)	NA	Monitors the availability of Microsoft Active Directory DNS Server.	SiteScope Template
domaincontroller Node	MSAD_Ping_Availability (:Microsoft_Active_ Directory_Server_Monitor)	NA	Monitors the availability of Microsoft Active Directory Server.	SiteScope Template

## Microsoft AD Collection Schedule

This Aspect contains the schedule task policies required to trigger the collection on predefined schedules.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController, DomainController Resource, DomainControllerRole	MSAD_ SCH_ ALL_ MEDIUM	NA	Contains the schedule task policy of frequency MEDIUM for collecting metrics for Microsoft Active Directory (MSAD) every hour.	Scheduled Task Template
DomainController, DomainController Resource, DomainControllerRole	MSAD_ SCH_ ALL_ VERY_ HIGH	NA	Contains the schedule task policy of frequency VERY_HIGH for collecting metrics for MSAD every 5 hours.	Scheduled Task Template
DomainController, DomainController Resource, DomainControllerRole	MSAD_ SCH_ ALL_ HIGH	NA	Contains schedule task policy of frequency HIGH for collecting metrics for Microsoft Active Directory once in 5 hours.	Scheduled Task Template
DomainController, DomainController Resource, DomainControllerRole	MSAD_ Collection Definition	NA	This Policy contains the metric definition xml which are used by Microsoft collector to collect metrics.	ConfigFile Template
DomainController, DomainController Resource, DomainControllerRole	MSAD_ SCH_ ALL_LOW	NA	Contains the schedule task policy of frequency LOW for collecting metrics for MSAD once in 24 hours.	Scheduled Task Template

## Microsoft AD DFSR Throughput

This Aspect Monitors the throughput of Microsoft Active Directory Distributed File System Replication (DFSR) service.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_DFS_	NA	Monitors the total number of	Measurement

CI Type	Policy Template	Indicator	Description	Policy Type
	Total_Bytes_recev		bytes received on the connection.	Threshold Template
DomainController	MSAD_DFS_Throughput_Schedule	NA	Contains the schedule for DFSR throughput performance statistics collection.	ConfigFile Template

## Microsoft AD DFSR Volume

This Aspect monitors the volume of DFSR activity.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_DFS_USN_Journal_Accepted	NA	Monitors Number of Update Sequence Number (USN) journal records that were processed by the DFS Replication service.	Measurement Threshold Template
	MSAD_DFS_Database_Lookups	NA	Monitors the number of database search operations performed by the DFS Replication service.	
	MSAD_DFS_USN_Journal_Percentage	NA	Monitors percent of the USN journal that has not yet been read and processed by the DFS Replication service.	
	MSAD_DFS_Database_Commits	NA	Monitors the number of database commit operations performed by the DFS Replication service.	
	MSAD_DFS_Volume_Schedule	NA	Contains schedule for collecting the monitoring DFSR replication volume statistics.	ConfigFile Template
	MSAD_DFS_USN_Journal_Read	NA	Monitors number of USN journal records that were read by the DFS Replication service.	Measurement Threshold Template

## Microsoft AD DFSR Logs

This Aspect monitors the Windows Event Logs for DFSR related logs.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_DFS_FwdAllError	NA	Forwards all log entries with severity 'Error'.	Windows Event Log Template

## Microsoft AD DFSR Performance

This Aspect monitors the performance of Microsoft Active Directory DFSR.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_DFS_Compresed_Size	NA	Monitors the compressed size (in bytes) of files received for the replicated folder.	Measurement Threshold Template
DomainController	MSAD_DFS_RDC_Number_recv	NA	Monitors the number of files that were received by the replicated folder.	Measurement Threshold Template
DomainController	MSAD_DFS_Stats_Schedule	NA	This policy monitors the performance of Active Directory DFSR.	ConfigFile Template
DomainController	MSAD_DFS_File_Installs_retired	MSAD_DFSRFileInstRetired:VeryHigh / MSAD_DFSRFileInstRetired:Normal,	Monitors the number of file installs that are being	Measurement Threshold Template

CI Type	Policy Template	Indicator	Description	Policy Type
		MSAD_ DFSFileInstRetired:High / MSAD_ DFSFileInstRetired:Normal	retried due to sharing violations or other errors encountered when installing the files.	
DomainController	MSAD_ DFS_ Conflict_ Space	NA	Monitors the total size (in bytes) of the conflict loser files and folders currently in the Conflict and Deleted folder used by the DFS Replication service.	Measurement Threshold Template
DomainController	MSAD_ DFS_Total_ Files_recv	NA	Monitors the number of files that were received for the replicated folder.	Measurement Threshold Template
DomainController	MSAD_ DFS_ Conflict_ Files	MSAD_ DFSConflictFiles:VeryHigh / MSAD_ DFSConflictFiles:Normal, MSAD_ DFSConflictFiles:High / MSAD_ DFSConflictFiles:Normal	Monitors the number of files and folders in this replicated folder that were moved to the Conflict and Deleted folder by the DFS Replication service.	Measurement Threshold Template
DomainController	MSAD_ DFS_File_ Installs_ succeeded	NA	Monitors the number of files that were successfully	Measurement Threshold Template



CI Type	Policy Template	Indicator	Description	Policy Type
			received from sending members and installed locally on the server.	
DomainController	MSAD_DFS_Bandwidth_Savings	NA	Monitors the percentage of bandwidth that was saved by the DFS Replication service for this replicated folder using a combination of remote differential compression (RDC) and other compression technologies that minimize network bandwidth.	Measurement Threshold Template

## Microsoft AD DIT

This Aspect monitors the Directory Information Tree (DIT) of Microsoft Active Directory.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_LogFilesQueueLength	DITLogFilesDiskQueueLength:VeryHigh / DITLogFilesDiskQueueLength:Normal, DITLogFilesDiskQueueLength:High / DITLogFilesDiskQueueLength:Normal	Monitors the queue length on the DIT log files disk drive.	Measurement Threshold Template

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_ DITPercentFull	DITDiskSpaceAvailability:NearCapacity / DITDiskSpaceAvailability:Normal, DITDiskSpaceAvailability:Low / DITDiskSpaceAvailability:Normal	Monitors the amount of free space on the DIT disk drive.	Measurement Threshold Template
DomainController	MSAD_ DITQueueLength	DITDiskQueueLength:VeryHigh / DITDiskQueueLength:Normal, DITDiskQueueLength:High / DITDiskQueueLength:Normal	Monitors the queue length on the DIT disk drive.	Measurement Threshold Template
DomainController	MSAD_ LogFilesPercentFull	DITLogFilesDiskSpaceAvailability:NearCapacity / DITLogFilesDiskSpaceAvailability:Normal, DITLogFilesDiskSpaceAvailability:Low / DITLogFilesDiskSpaceAvailability:Normal	Monitors the amount of free space on the DIT log files disk drive.	Measurement Threshold Template
DomainController	MSAD_ TotalDitSize	NA	Monitors the total amount of free space on the DIT disk drive in MB.	Measurement Threshold Template

## Microsoft AD Directory Services Logs

This Aspect monitors the Windows Event Log messages for directory service related logs.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_ FwdAllErrorDS	NA	Forwards all Log Entries with severity Errors in Directory Service Event Logs.	Windows Event Log Template

## Microsoft AD DNS

This Aspect monitors the consistency and performance of DNS server.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_DNS_ Obsolete_GUIDs	NA	Checks for hosts, within the forest that the domain controller resides in, that are registered under obsolete Globally Unique Identifiers (GUIDs).	Measurement Threshold Template
DomainController	MSAD_DNS_ LogDNSPagesSec	NA	Records pages per sec for use in the creation of capacity planning graphs.	Measurement Threshold Template
DomainController	MSAD_DNS_ Island_Server	NA	Checks to see if the domain controller is configured to use itself as a DNS server.	Measurement Threshold Template
DomainController	MSAD_DNS_GC_ StrandedSite	NA	Checks for the existence of a global catalog on every site within the forest that the domain controller resides in.	Measurement Threshold Template

## Microsoft AD DNS Logs

This Aspect monitors the DNS related Windows Event Logs.

CI Type	Policy Template	Indicator	Description	Policy Type
domaincontroller	MSAD_ DNSServ_ FwdAllError	NA	Forwards all Log Entries with Error of DNS Server.	Windows Event Log Template

## Microsoft AD DNS Records

This Aspect verifies various DNS records like Host Resource Records, CName Records, SRV records etc.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_DNS_DC_A_Chk	HostRecordsAvailability:NotFound / HostRecordsAvailability:Found	Ensures that DNS contains the expected host resource records for the Lightweight Directory Access Protocol (LDAP) service.	Measurement Threshold Template
DomainController	MSAD_DNS_GC_A_Chk	NA	Ensures that DNS contains the expected host resource records for the global catalog.	Measurement Threshold Template
DomainController	MSAD_DNS_Extra_LDAP_SRV_Chk	NA	Checks for extra DNS SRV resource records registered for the LDAP service.	Measurement Threshold Template

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_DNS_GC_SRV_Chk	NA	Ensures that DNS contains the expected SRV resource records for the LDAP service.	Measurement Threshold Template
DomainController	MSAD_DNS_Kerberos_SRV_Chk	KerberosSrvRecordsAvailability:NotFound / KerberosSrvRecordsAvailability:Found	Checks for expected DNS SRV resource records registered for the Kerberos service.	Measurement Threshold Template
DomainController	MSAD_DNS_LDAP_SRV_Chk	LDAPSrvRecordsAvailability:NotFound / LDAPSrvRecordsAvailability:Found	Ensures that DNS contains the expected SRV resource records for the LDAP service.	Measurement Threshold Template
DomainController	MSAD_DNS_Extra_Kerberos_SRV_Chk	NA	Checks for extra DNS SRV resource records registered for the Kerberos service.	Measurement Threshold Template
DomainController	MSAD_DNS_Extra_	NA	Checks for extra DNS SRV	Measurement Threshold Template

CI Type	Policy Template	Indicator	Description	Policy Type
	GC_SRV_Chk		resource records registered for the global catalog.	
DomainController	MSAD_DNS_DC_CNAM_E_Chk	CNameRecordsAvailability:NotFound / CNameRecordsAvailability:Found	Ensures that DNS contains the expected CName resource records for the LDAP service.	Measurement Threshold Template

## Microsoft AD DNS Response

This Aspect monitors the DNS Server response time and DNS query response time.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_DNS_Server_Response	NA	Monitors the response time given by the DNS server.	Measurement Threshold Template
DomainController	MSAD_DNS_DC_Response	DNSQueryResponse:VeryHigh / DNSQueryResponse:Normal	Monitors the response time of DNS queries made by the domain controller in milliseconds.	Measurement Threshold Template

## Microsoft AD Directory Access

This Aspect monitors the directory throughput of LDAP in Microsoft Active Directory.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_IQLDAPActiveThreads	LDAPActiveThreads:Very High / LDAPActiveThreads:Normal, LDAPActiveThreads:Very High / LDAPActiveThreads:Normal	Checks the LDAP Active Threads for the number of LDAP Active Threads of DirectoryServices object.	Measurement Threshold Template
DomainController	MSAD_GlobalCatalogSearches	DirectorySearchRate:Very High / DirectorySearchRate:Normal, DirectorySearchRate:Very High / DirectorySearchRate:Normal	Monitors the number of Directory Searches per second.	Measurement Threshold Template
DomainController	MSAD_GlobalCatalogWrites	DirectoryWriteRate:VeryHigh / DirectoryWriteRate:Normal, DirectoryWriteRate:High / DirectoryWriteRate:Normal	Checks the number of Directory Writes per second.	Measurement Threshold Template
DomainController	MSAD_IQLDAPClientSessions	LDAPClientSessions:VeryHigh / LDAPClientSessions:Normal, LDAPClientSessions:High / LDAPClientSessions:Normal	Checks the LDAP Client Sessions for the number of LDAP Client Sessions for DirectoryServices object.	Measurement Threshold Template
DomainController	MSAD_IQLDAPBindTime	NA	Checks the LDAP Bind Time for the number of LDAP Client Sessions of DirectoryServices object.	Measurement Threshold Template
DomainController	MSAD_GlobalCatalogReads	DirectoryReadRate:VeryHigh /	Monitors the number of	Measurement

CI Type	Policy Template	Indicator	Description	Policy Type
		DirectoryReadRate:Normal, DirectoryReadRate:High / DirectoryReadRate:Normal	Directory Reads per second.	Threshold Template
DomainController	MSAD_DirectoryAccessSchedule	NA	This policy maintains the Schedule of Essential Directory Access Aspect.	ConfigFile Template

## Microsoft AD Discovery

The OMi MP for Microsoft Active Directory expands the discovery and adds multiple hierarchical levels of details. At a higher level, the OMi MP for Microsoft Active Directory discovers forests and goes further to the lower levels to discover each Domain Controller (DC) with its name. The Data Sources are automatically created after the deployment of Microsoft Active Directory Discovery Aspect.

Microsoft AD Discovery Aspect discovers the Microsoft Active Directory server deployment topology and populates the corresponding CIs in the RTSM database.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController, Windows	MSAD_Discovery	NA	Discovers Microsoft Active Directory Topology.	Service Auto-Discovery Template
DomainController, Windows	MSAD_CreateDataSource	NA	Creates Microsoft Active Directory Datasource.	Scheduled Task Template

When you deploy Microsoft AD Discovery Aspect, you can see the following Microsoft Active Directory components discovered:

- Active Directory Forest
- Active Directory Domain
- Child Active Directory Domain
- Domain Controller



- Domain Controller Roles
- Windows
- Interface

## Microsoft AD FSMO Consistency

This Aspect monitors consistency of various Flexible Single Master Operations (FSMO) roles with its replication partners based on consistency state.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_FSMO_Consist_PDC	NA	Monitors consistency of the Primary Domain Controller (PDC) master with replication partners based on consistency state.	Measurement Threshold Template
DomainController	MSAD_FSMO_Consist_NAMING	NA	Monitors consistency of the Naming master with replication partners based on consistency state.	Measurement Threshold Template
DomainController	MSAD_FSMO_Consist_SCHEMA	NA	Monitors consistency of the Schema master with replication partners based on consistency state.	Measurement Threshold Template
DomainController	MSAD_SCH_FSMOConsist	NA	Schedules the FSMO Consistency check collection.	Scheduled Task Template
DomainController	MSAD_FSMO_Consist_INFRA	NA	Monitors consistency of the Infrastructure master with replication partners based on consistency state.	Measurement Threshold Template
DomainController	MSAD_FSMO_Consist_RID	NA	Monitors consistency of the Relative Identifier (RID) master with replication partners based on consistency state.	Measurement Threshold Template

## Microsoft AD FSMO Response Time

This Aspect monitors the Bind and Ping Response time of various FSMO roles.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_FSMO_INFRA_Bind	NA	Monitors the bind response time of the Infrastructure FSMO in seconds.	Measurement Threshold Template
DomainController	MSAD_FSMO_NAMING_Bind	NA	Monitors the bind response time of the Domain Naming FSMO in seconds.	Measurement Threshold Template
DomainController	MSAD_FSMO_RID_Ping	NA	Monitors the ping response time of the RID FSMO in seconds.	Measurement Threshold Template
DomainController	MSAD_SCH_FSMOLogging	NA	Logs FSMO response times.	Scheduled Task Template
DomainController	MSAD_FSMO_INFRA_Ping	NA	Monitors the ping response time of the Infrastructure FSMO in seconds.	Measurement Threshold Template
DomainController	MSAD_FSMO_PDC_Bind	NA	Monitors the bind response time of the PDC FSMO in seconds.	Measurement Threshold Template
DomainController	MSAD_FSMO_RID_Bind	NA	Monitors the bind response time of the RID FSMO in seconds.	Measurement Threshold Template
DomainController	MSAD_FSMO_PDC_Ping	NA	Monitors the ping response time of the PDC FSMO in seconds.	Measurement Threshold Template
DomainController	MSAD_FSMO_NAMING_Ping	NA	Monitors the ping response time of the Domain Naming FSMO in seconds.	Measurement Threshold Template

## Microsoft AD FSMO Role Movement

This Aspect monitors the domain controller's ownership of various FSMO Roles with respect to the state before the role movement.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_FSMO_RoleMvmt_PDC	NA	Monitors the domain controller's ownership of the PDC Emulator FSMO role.	Measurement Threshold Template
DomainController	MSAD_FSMO_RoleMvmt_INFRA	NA	Monitors the domain controller's ownership of the Infrastructure Master FSMO role.	Measurement Threshold Template
DomainController	MSAD_SCH_FSMORoleMovement	NA	Logs FSMO response times.	Scheduled Task Template
DomainController	MSAD_FSMO_RoleMvmt_SCHEMA	NA	Monitors the domain controller's ownership of the Schema Master FSMO role.	Measurement Threshold Template
DomainController	MSAD_FSMO_RoleMvmt_NAMING	NA	Monitors the domain controller's ownership of the Domain Naming FSMO role.	Measurement Threshold Template
DomainController	MSAD_FSMO_RoleMvmt_RID	NA	Monitors the domain controller's ownership of the RID Master FSMO role.	Measurement Threshold Template

## Microsoft AD Federation Service Logs

This Aspect monitors the Windows Event Logs for Active Directory Federation Services (ADFS) related logs.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_ ADFS_ FwdAllError	NA	Forwards all log entries with severity 'Error'.	Windows Event Log Template
DomainController	MSAD_ ADFS_ Security	NA	Forwards all Failure Security event log entries with category Privilege Use.	Windows Event Log Template

## Microsoft AD Federation Services

This Aspect monitors the performance of Microsoft Active Directory Federation Services.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_ ADFS_ Proxy_Requests	MSAD_ProxyRequestsRate:VeryHigh / MSAD_ProxyRequestsRate:Normal, MSAD_ProxyRequestsRate:High / MSAD_ProxyRequestsRate:Normal	Monitors the number of incoming requests sent to the federation server proxy.	Measurement Threshold Template
DomainController	MSAD_ ADFS_ Fed_Resolution_Req	MSAD_ArtifactResolutionRequestsRate:VeryHigh / MSAD_FederationMetadataRequestsRate:Normal, MSAD_ArtifactResolutionRequestsRate:High / MSAD_ArtifactResolutionRequestsRate:Normal	Monitors the number of requests to the artifact resolution endpoint per second that are sent to the federation server.	Measurement Threshold Template
DomainController	MSAD_ ADFS_ Proxy_MEX_Requests	MSAD_ProxyMEXRequestsRate:VeryHigh / MSAD_ProxyMEXRequestsRate:Normal, MSAD_ProxyMEXRequestsRate:High	Monitors the number of incoming	Measurement Threshold Template

CI Type	Policy Template	Indicator	Description	Policy Type
		/ MSAD_ProxyMEXRequestsRate:Normal	federation meta-data requests sent to the federation server.	
DomainController	MSAD_ADFS_Schedule	NA	This policy maintains the schedule for monitoring ADFS.	ConfigFile Template
DomainController	MSAD_ADFS_Token_Requests	MSAD_TokenRequestRate:VeryHigh MSAD_TokenRequestRate:High MSAD_TokenRequestRate:Normal	Monitors the number of token requests sent to the federation server.	Measurement Threshold Template

## Microsoft AD Global Catalog

This Aspect monitors Global Catalog (GC) by monitoring the status and replication consistency of GC.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController, DomainControllerRole	MSAD_GCMonitorStatus	GCConnectivity:Down / GCConnectivity:Up	Monitors the GC Query Status in Active Directory.	Measurement Threshold Template
DomainController, DomainControllerRole	MSAD_SCH_GCCheckStatus	NA	Checks the GC Query Status in Active Directory.	Scheduled Task Template

## Microsoft AD Global Catalog Access

This Aspect monitors the access parameters such as reads, writes, and searches of Microsoft Active Directory Global Catalog.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController, DomainControllerRole	MSAD_GC_Schedule	NA	This policy maintains the Schedule of Essential Authentication Aspect.	ConfigFile Template
DomainController, DomainControllerRole	MSAD_GC_GlobalCatalogWrites	NA	Monitors the number of Directory Writes/sec.	Measurement Threshold Template
DomainController, DomainControllerRole	MSAD_GC_GlobalCatalogReads	NA	Monitors the number of Directory Reads per second.	Measurement Threshold Template
DomainController, DomainControllerRole	MSAD_GC_GlobalCatalogSearches	NA	Monitors the number of Directory Searches per second.	Measurement Threshold Template

## Microsoft AD Group Policy

This Aspect monitors the group policy objects in Active Directory.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_SCH_GroupPolicy	NA	Monitors unlinked, disabled, and orphaned policies.	Scheduled Task Template
DomainController	MSAD_GPO_MessagePolicy	NA	Intercepts Group policy messages.	Windows Management Interface Template

## Microsoft AD Replication

This Aspect monitors the inter-site and intra-site replication.

CI Type	Policy Template	Indicator	Description	Policy Type
domaincontroller	MSAD_SCH_RepModifyObj	NA	Schedules modification of Replication object.	Scheduled Task Template
domaincontroller	MSAD_SCH_TimeSync	NA	Validates time synchronization with time master.	Scheduled Task Template
domaincontroller	MSAD_Rep_MonitorIntraSiteReplication	IntraSiteReplicationLatency:VeryHigh / IntraSiteReplicationLatency:Normal, IntraSiteReplicationLatency:High / IntraSiteReplicationLatency:Normal	Monitors Intra-site Replication in Active Directory.	Measurement Threshold Template
domaincontroller	MSAD_SCH_RepModifyUserObj	NA	Schedules modification of replication user object.	Scheduled Task Template
domaincontroller	MSAD_SCH_IntraSiteReplication	NA	Monitors Intra-site Replication in Active Directory for Microsoft Active Directory (MSAD).	Scheduled Task Template
domaincontroller	MSAD_Rep_TimeSync	NA	Validates time synchronization	Measurement Threshold

CI Type	Policy Template	Indicator	Description	Policy Type
			tion with time master.	Template
domaincontroller	MSAD_SCH_DelOVRRepObj	NA	Schedules deletion of replication object.	Scheduled Task Template
domaincontroller	MSAD_Rep_MonitorInterSiteReplication	InterSiteReplicationLatency:VeryHigh / InterSiteReplicationLatency:Normal, InterSiteReplicationLatency:High / InterSiteReplicationLatency:Normal	Monitors Inter-site Replication in Active Directory.	Measurement Threshold Template
domaincontroller	MSAD_SCH_InterSiteReplication	NA	Monitors Inter-site Replication in Active Directory for MSAD.	Scheduled Task Template

## Microsoft AD Replication Auto Baseline

This Aspect consists of policies which monitors replication and uses auto threshold feature to calculate and store the threshold.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_Rep_GC_Check_and_Threshold_Monitor_AT	NA	An auto-threshold policy which calculates, stores, and generate alerts during Global Catalog Replication Latency threshold breaches.	Measurement Threshold Template
DomainController	MSAD_Rep_TimeSync_Monitor_AT	NA	Validates time synchronization with time master in seconds.	Measurement Threshold Template
DomainController	MSAD_Rep_	NA	Monitors the number of inbound	Measurement



CI Type	Policy Template	Indicator	Description	Policy Type
	InboundObjects_AT		replication objects.	Threshold Template

## Microsoft AD Replication Logs

This Aspect monitors the replication related Windows Event Log messages.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_FwdAllErrorFRS	NA	Forwards all Log Entries with severity Errors in File Replication Service Logs.	Windows Event Log Template
DomainController	MSAD_ReplicationActivities	NA	Checks logs Replication Starting and Ending.	Windows Event Log Template

## Microsoft AD Replication Statistics

This Aspect monitors the replication statistics of Microsoft Active Directory. This Aspect covers both inter-site and intra-site replication.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_ADSRepInBoundBytesBetweenSites	PendingReplicationSynchronizations:VeryHigh / PendingReplicationSynchronizations:Normal, PendingReplicationSynchronizations:High / PendingReplicationSynchronizations:Normal	Checks the Inbound Bytes Between Sites counters of DirectoryServices object.	Measurement Threshold Template
DomainController	MSAD_ADSPendingSynchronizations	PendingReplicationSynchronizations:VeryHigh / PendingReplicationSynchronizations:Normal	Checks the DRA Pending	Measurement Threshold

CI Type	Policy Template	Indicator	Description	Policy Type
		ations:Normal, PendingReplicationSynchronizations:High / PendingReplicationSynchronizations:Normal	Replication Synchronizations counters for the number of synchronizations pending for DirectoryServices object.	Id Template
DomainController	MSAD_ADSReplInBoundObjectUpdatesRemaining	InboundObjectUpdatesRemaining:VeryHigh / InboundObjectUpdatesRemaining:Normal, InboundObjectUpdatesRemaining:High / InboundObjectUpdatesRemaining:Normal	Checks the DRA Inbound Object Updates Remaining in Packet for the number of objects remaining.	Measurement Threshold Template
DomainController	MSAD_Rep_InboundObjs	InboundReplicationObjectRate:VeryHigh / InboundReplicationObjectRate:Normal, InboundReplicationObjectRate:High / InboundReplicationObjectRate:Normal	Monitors the number of inbound replication objects.	Measurement Threshold Template
DomainController	MSAD_ADSReplInBoundBytesWithInSites	PendingReplicationSynchronizations:VeryHigh / PendingReplicationSynchronizations:Normal, PendingReplicationSynchronizations:High / PendingReplicationSynchronizations:Normal	Checks the DRA Inbound Bytes Not Compressed counters for the number of bytes per second	Measurement Threshold Template

CI Type	Policy Template	Indicator	Description	Policy Type
			within sites for DirectoryServices object.	
DomainController	MSAD_ReplicationSchedule	NA	Maintains the Schedule of replication Aspect.	ConfigFile Template

## Microsoft AD Response Time

This Aspect monitors the LDAP and GC query response time.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_ResponseTimeGCBind	GCLDAPBindResponseTime:VeryHigh / GCLDAPBindResponseTime:Normal, GCLDAPBindResponseTime:High / GCLDAPBindResponseTime:Normal	Monitors the bind response time of the global catalog on the domain controller in seconds.	Measurement Threshold Template
DomainController	MSAD_SCH_ResponseLogging	NA	Logs Active Directory Response times	Scheduled Task Template
DomainController	MSAD_ResponseTimeQuery	DCLDAPQueryResponseTime:VeryHigh / GCLDAPQueryResponseTime:Normal,	Monitors the response time of	Measurement Threshold Template

CI Type	Policy Template	Indicator	Description	Policy Type
		GCLDAPQueryResponseTime:High / GCLDAPQueryResponseTime:Normal	queries made to the domain controller in seconds.	
DomainController	MSAD_ResponseTimeGCQuery	ResponseTime:VeryHigh / ResponseTime:Normal, ResponseTime:High / ResponseTime:Normal	Monitors the response time of queries made to the global catalog on the domain controller in seconds.	Measurement Threshold Template
DomainController	MSAD_SCH_LDAPStatus	NA	Checks LDAP Query Status in Active Directory.	Scheduled Task Template
DomainController	MSAD_ResponseTimeBind	DCLDAPBindResponseTime:VeryHigh / DCLDAPBindResponseTime:Normal, DCLDAPBindResponseTime:High / DCLDAPBindResponseTime:Normal	Monitors the bind response time of the domain controller in seconds.	Measurement Threshold Template
DomainController	MSAD_LDAPCheckStatus	LDAPConnectivity:Down / LDAPConnectivity:Up	Monitors LDAP Query Status in Active Directory.	Measurement Threshold Template

## Microsoft AD SYSVOL

This Aspect monitors the System Volume (SYS VOL) feature of Microsoft Active Directory.

CI Type	Policy Template	Indicator	Description	Policy Type
domaincontroller	MSAD_Sysvol_AD_Sync	NA	Checks whether the Group Policy objects in Sysvol and Active Directory are in sync.	Measurement Threshold Template
domaincontroller	MSAD_SYSVOL_DiskQueueLength	SysvolDiskQueueLength:VeryHigh / SysvolDiskQueueLength:Normal, SysvolDiskQueueLength:High / SysvolDiskQueueLength:Normal	Monitors the queue length on the SYSVOL disk drive.	Measurement Threshold Template
domaincontroller	MSAD_MonitorsSYSVol	SysvolConnectivity:Down / EventTypeIndicator  SysvolConnectivity:Normal	Monitors the response time of queries made to the domain controller in seconds.	Measurement Threshold Template
domaincontroller	MSAD_SCH_SYSVOLConnectivity	NA	Checks LDAP Query Status in Active Directory.	Scheduled Task Template

CI Type	Policy Template	Indicator	Description	Policy Type
domaincontroller	MSAD_ SYSVOL_ PercentFull	SysvolDiskSpaceAvailability:NearCapacity / SysvolDiskSpaceAvailability:Normal, SysvolDiskSpaceAvailability:Low / SysvolDiskSpaceAvailability:Normal	Monitors the amount of free space on the Sysvol disk drive in terms of percentage used.	Measurement Threshold Template

## Microsoft AD Security

This Aspect monitors the security aspects of Microsoft Active Directory.

CI Type	Policy Template	Indicator	Description	Policy Type
domaincontroller	MSAD_ SecNonTransMembershipEval	NonTransitiveMembershipEvaluations:VeryHigh / NonTransitiveMembershipEvaluations:Normal, NonTransitiveMembershipEvaluations:High / NonTransitiveMembershipEvaluations:Normal	Checks the SAM Non-Transitive Membership Evaluation/sec counters for the DirectoryServices object.	Measurement Threshold Template
domaincontroller	MSAD_ SecSDPropagatorQueue	SecurityDescriptorPropagatorQueue:VeryHigh / SecurityDescriptorPropagatorQueue:Normal, SecurityDescriptorPropagatorQueue:High / SecurityDescriptorPropagatorQueue:Normal	Checks the DS Security Descriptor Propagator Run-time Queue for the number of objects remaining to be examined while processing	Measurement Threshold Template

CI Type	Policy Template	Indicator	Description	Policy Type
			the current directory service security descriptor propagator event.	
domaincontroller	MSAD_Security	NA	This policy maintains the Schedule of Essential Security Aspect.	ConfigFile Template
domaincontroller	MSAD_SecTransMembershipEvaluation	TransitiveMembershipEvaluations:VeryHigh / TransitiveMembershipEvaluations:Normal, TransitiveMembershipEvaluations:High / TransitiveMembershipEvaluations:Normal	Checks the SAM Transitive Membership Evaluations for the number of SAM transitive membership evaluations per second.	Measurement Threshold Template

## Microsoft AD Security Logs

This Aspect monitors the security events in Windows Event Log.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_SecDirectoryServiceAccess	NA	Forwards all Failure security event log entries with category Directory Service Access.	Windows Event Log Template
DomainController	MSAD_SecAdminGroupChangeMon	NA	Monitors the changes in Security Admin Group.	Windows Event Log

CI Type	Policy Template	Indicator	Description	Policy Type
				Template
DomainController	MSAD_KDCFailureGrantTicket	NA	This policy raises an alert when there is a failure to grant ticket.	Windows Event Log Template
DomainController	MSAD_PrivilegedAccount	NA	Failure to Grant Ticket	Windows Event Log Template

## Microsoft AD Services

This Aspect monitors the core Services of Microsoft Active Directory.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_HMNTFRSPageFaults	NTFRSPageFaultsRate:Very High / NTFRSPageFaultsRate:Normal, NTFRSPageFaultsRate:High / NTFRSPageFaultsRate:Normal	Checks for the number of Page Faults/sec for the NTFRS process.	Measurement Threshold Template
DomainController	MSAD_Rep_ISM_Chk	ISMServiceStatus:Down / ISMServiceStatus:Up	Checks the state of Inter site Replication Service.	Measurement Threshold Template
DomainController	MSAD_HMNTFRSPrivateBytes	NTFRSPrivateBytes:VeryHigh / NTFRSPageFaultsRate:Normal, NTFRSPrivateBytes:High / NTFRSPageFaultsRate:Normal	Checks the Private Bytes counters for NTFRS process.	Measurement Threshold Template



CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_HMLSASSProcessorTime	LSASSProcessorTime:Very High / LSASSProcessorTime:Normal, LSASSProcessorTime:High / LSASSProcessorTime:Normal	Checks the percentage of processor time the Local Security Authority Subsystem Service (LSASS) process is consuming.	Measurement Threshold Template
DomainController	MSAD_NTFRS_Chk	NTFRSServiceState:Down / NTFRSServiceState:Up	Checks the state of NTFRS Logon Service	Measurement Threshold Template
DomainController	MSAD_KDC_Chk	NetLogonServiceState:Down / NetLogonServiceState:Up	Checks the state of Kerberos key Distribution Center Service	Measurement Threshold Template
DomainController	MSAD_DFSR_Chk	DFSRServiceState:Down / DFSRServiceState:Up	Checks the state of DSFR Service.	Measurement Threshold Template
DomainController	MSAD_HMNTFRSWorkingSet	NTFRSWorkingSet:VeryHigh / NTFRSWorkingSet:Normal, NTFRSWorkingSet:High / NTFRSWorkingSet:Normal	Checks the Working Set counters of NTFRS process.	Measurement Threshold Template
DomainController	MSAD_HMNTFRSProcessorT	NTFRSProcessorTime:Very High /	Checks the	Measurement

CI Type	Policy Template	Indicator	Description	Policy Type
	ime	NTFRSProcessorTime:Normal, NTFRSProcessorTime:High / NTFRSProcessorTime:Normal	percentage of processor time the NTFRS process is consuming.	Threshold Template
DomainController	MSAD_NTDS_Chk	NetLogonServiceState:Down / NetLogonServiceState:Up	Checks the state of NTDS Logon Service.	Measurement Threshold Template
DomainController	MSAD_EssentialSvcSchedule	NA	This policy maintains the schedule of Essential Service Aspect.	ConfigFile Template
DomainController	MSAD_HMLSSASSWorkingSet	LSASSWorkingSet:VeryHigh / LSASSWorkingSet:Normal, LSASSWorkingSet:High / LSASSWorkingSet:Normal	Checks the Working Set counters of LSASS process.	Measurement Threshold Template
DomainController	MSAD_NetLogon_Chk	NetLogonServiceState:Down / NetLogonServiceState:Up	Checks the state of Net Logon Service.	Measurement Threshold Template
DomainController	MSAD_SAMSS_Chk	SamSsServiceState:Down / SamSsServiceState:Up	Checks the state of Security Accounts Manager Service	Measurement Threshold Template

CI Type	Policy Template	Indicator	Description	Policy Type
			(SAMSS) Logon Service	
DomainController	MSAD_HMLSASSPageFaults	LSASSPageFaultsRate:Very High / LSASSPageFaultsRate:Normal, LSASSPageFaultsRate:High / LSASSPageFaultsRate:Normal	Checks the Page Faults/sec for the LSASS process.	Measurement Threshold Template
DomainController	MSAD_HMLSASSPrivateBytes	LSASSPrivateBytes:VeryHigh / LSASSPageFaultsRate:Normal, LSASSPrivateBytes:High / LSASSPageFaultsRate:Normal	Checks the Private Bytes counters for LSASS process.	Measurement Threshold Template

## Microsoft AD Structure Changes

This Aspect monitors the changes to Active Directory Site, Domain, and Organizational Unit.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_DomainChanges	NA	Tracks Domain changes.	Windows Management Interface Template
DomainController	MSAD_OUChanges	NA	Tracks Organizational Unit changes.	Windows Management Interface Template

## Microsoft AD Trust

This Aspect monitors the Trust changes in Active Directory.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_Trust_Mon_Add_Del	NA	Monitors the trust changes in Active Directory (on Windows 2003 Domain Controllers only) (Additions and Deletions of Trusts)	Windows Management Interface Template

## Microsoft AD Event Logs

This Aspect monitors the Windows Event Log for general Active Directory related log messages.

CI Type	Policy Template	Indicator	Description	Policy Type
DomainController	MSAD_FwdAllInformationFRS	NA	Forwards all Log Entries with severity information in File Replication Service Logs.	Windows Event Log Template
DomainController	MSAD_DNSServ_FwdAllWarn	NA	Forwards all Log Entries with Warnings of DNS Server.	Windows Event Log Template
DomainController	MSAD_FwdAllWarnDS	NA	Forwards all Log Entries with severity Errors and warnings in Directory Service Event Logs.	Windows Event Log Template
DomainController	MSAD_FwdAllWarnFRS	NA	Forwards all Log Entries with severity warnings in File Replication Service Logs.	Windows Event Log Template
DomainController	MSAD_FwdAllInformationDS	NA	Forwards all Log Entries with severity Information in Directory Service Event Logs.	Windows Event Log Template
DomainController	MSAD_DNSServ_FwdAllInformation	NA	Forwards all Log Entries with Information.	Windows Event Log Template

## Parameters

Parameters are variables that forms an integral part of Microsoft Active Directory Management Templates, Aspects, and Policy Templates. Each parameter corresponds to a variable. Parameters contain default values that are used for monitoring the different components of Microsoft Active Directory deployment. You can also modify the values of the variables to suit your monitoring requirements.

## Microsoft Active Directory Parameters

The OMi MP for Microsoft Active Directory contains **Expert Parameters** which are used by SMEs and Administrators.

## OMi MP for Microsoft Active Directory Parameters

The OMi MP for Microsoft Active Directory consists of the following parameters:

Parameter	Description	Default Value
Frequency of High Scheduler	Frequency for the scheduler which is expected to run for high intervals (in minutes).	15
Frequency of Low Scheduler	Frequency for the scheduler which is expected to run for short intervals (in hours).	24
Frequency of Medium Scheduler	Frequency for the scheduler which is expected to run for medium intervals (in hours).	1
Frequency of VeryHigh Scheduler	Frequency for the scheduler which is expected to run for very high intervals (in minutes).	5

## Tuning of Parameters



This section provides information about editing parameters the Microsoft Active Directory Management Templates and Aspects that are deployed to the CIs.

To edit the parameters, follow these steps:

1. Open the Assignments & Tuning pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Assignments & Tuning**.

On OMi 10.x, click **Administration > Monitoring > Assignments & Tuning**.

2. In the **Browse Views** tab, select the **AD\_Logical\_View** that contains the CI for which you want to tune parameters. Alternatively, you can use **Search** tab to find a CI.
3. In the list of CI, click a CI. The Assignment Details pane lists the current parameter values.
4. You can change the default values of Parameters in the Assignment Details pane by following these steps:
  - a. Click . The Edit Parameter window opens.
  - b. Select the Parameter you want to edit and click . The Edit Parameter window opens.
  - c. Change the value and click **OK**. The new parameter values are deployed to the relevant CIs.

## Configuration Items (CIs) and Configuration Item Types (CITs)

CIs are component that needs to be managed in order to deliver an IT Service. CIs typically include IT Services, hardware, and software. CIT describes the type of a CI and its attributes. The Microsoft Active Directory CIs that are discovered in an environment are grouped together under the CITs. The OMi MP for Microsoft Active Directory consists the following CITs:

- Windows
- DomainController
- DomainControllerRole

## Run-time Service Model (RTSM) Views

A View enables you to visualize the context of an event. A typical View shows a subset of Active Directory CIs and their relationships with other neighboring CIs. Using the Views, you can visualize the topology of a Microsoft Active Directory environment. In addition, Views can be used to do the following:

- Manage the Event Perspective of Microsoft Active Directory Domain Controller CIs
- Manage the Health Perspective of Microsoft Active Directory Domain Controller CIs
- Assigning and Tuning the Management Templates, Aspects, and Policy Templates

### How to Access RTSM Views

1. Open the Modeling Studio pane:

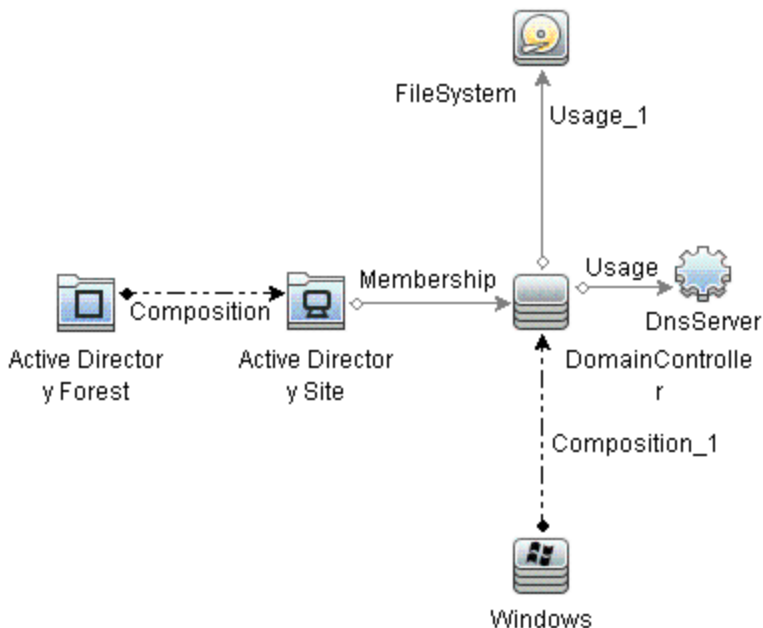
On BSM 9.2x, click **Admin > RTSM Administration > Modeling > Modeling Studio**

On OMi 10.x, click **Administration > RTSM Administration > Modeling > Modeling Studio**

2. Click **Resource Type as Views**.
3. Click **Operations Management > Active Directory** from the list.

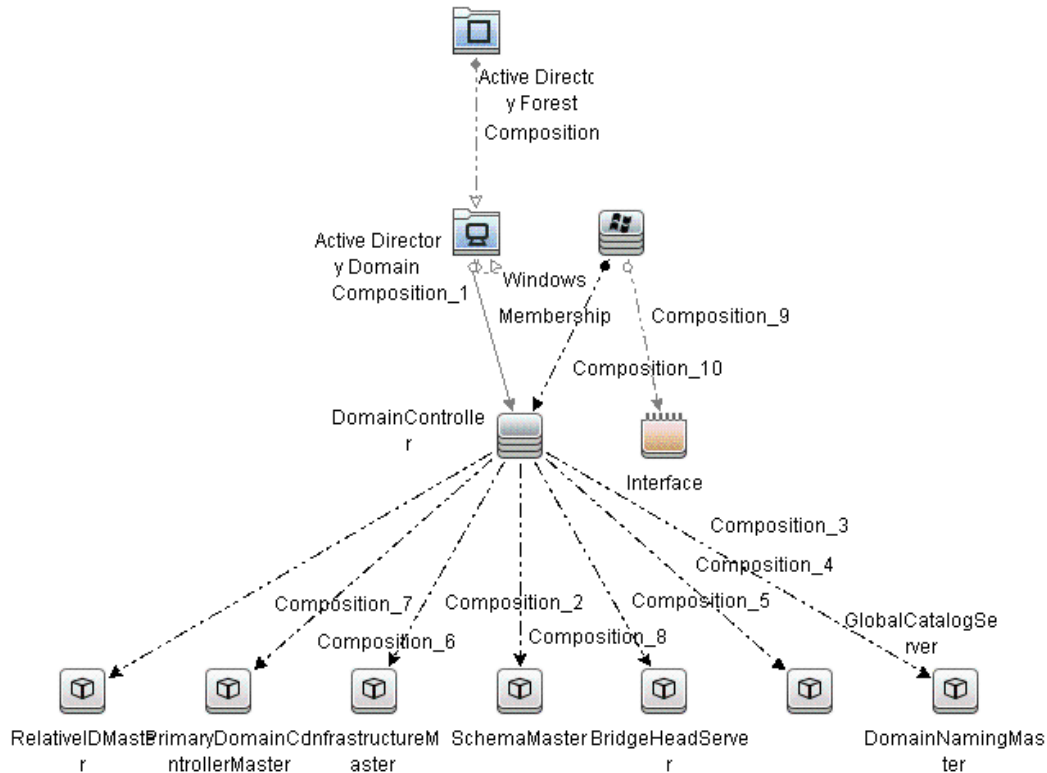
The OMi MP for Microsoft Active Directory includes the following views:

- **AD\_Physical\_View:** This view displays various components such as the Active Directory System, Active Directory Site, Domain Controller, Domain Naming Master, and Computer (Windows) CIs. The AD\_Physical\_View enables you to visualize the association of the Active Directory sites with the Domain Controllers. The following image shows the relationship among the CIs.



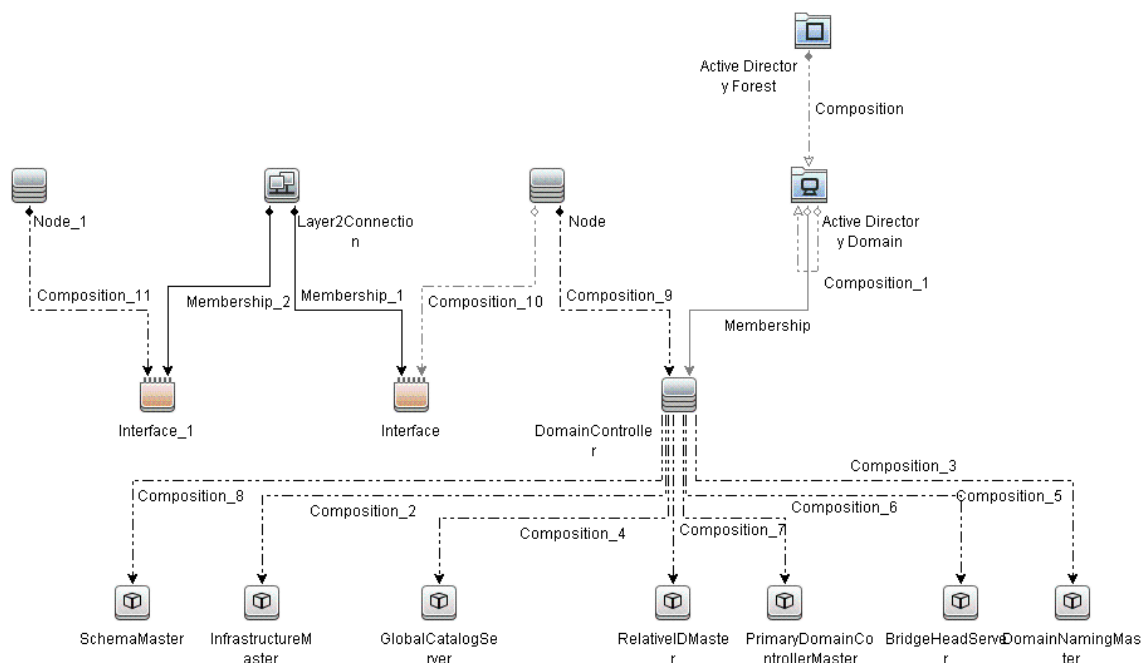
- **AD\_Logical\_view:** This view displays various components such as the Active Directory System,

Active Directory Forest, Active Directory Domain, Domain Controller, Schema Master, Domain Naming Master, Primary Domain Controller Master, Relative ID Master, Infrastructure Master, Bridge Head Server, Global Catalog Server, and Computer CITS. The AD\_Logical\_View enables you to visualize different components of Active Directory server along with the roles and its association with the Domain and the Domain Controller. The following image shows the relationship among the CITS.



- **AD\_Network\_Deployment\_View:** This view displays various components such as the Active Directory System, Active Directory Forest, Active Directory Domain, Domain Controller, Schema Master, Domain Naming Master, Primary Domain Controller Master, Relative ID Master, Infrastructure Master, Bridge Head Server, Global Catalog Server, and Node CITS. The AD\_Network\_Deployment\_View enables you to visualize the components of an associated network along with the monitored Active Directory Domain Controller CIs in your environment. The following image shows the relationship among the CITS.





## Enrichment Rules

Enrichment rules can be used for several purposes, including:

- Adding new CIs and relationships to the RTSM
- Deleting specific CI instances from the RTSM
- Updating the attribute values of specific CI instances in the RTSM

### How to Access Enrichment Rules

1. Open the Enrichment manager pane:

On BSM 9.2x, click **Admin > RTSM Administration > Modeling > Enrichment manager**

On OMi 10.x, click **Administration > RTSM Administration > Modeling > Enrichment manager**

2. Click **Operations Management > Active Directory** from the Enrichment Rules list pane.

The OMi MP for Microsoft Active Directory includes the following Enrichment Rules:

- DomainController\_Uses\_DnsServer - Binds to DNS Server on the Domain Controller
- DomainController\_Uses\_Log\_FileSystem - Binds to Log FileSystem on the Domain Controller
- DomainController\_Uses\_NTDS\_FileSystem - Binds to NTDS FileSystem on the Domain Controller
- DomainController\_Uses\_SysVol\_FileSystem - Binds to SysVol FileSystem on the Domain Controller

## Health Indicators (HIs) and Event Type Indicators (ETIs)

HIs reports the health of Active Directory servers. ETIs are categorization of Events based on the type of occurrence.

### How to Access Domain Controller Indicators

1. Open the Indicators pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Indicators**

On OMi 10.x, click **Administration > Service Health > CI Status Calculation > Health- and Event Type Indicators**

2. In the CI Types pane, click **Configuration Item > Infrastructure Element > Running Software > Directory Server > Domain Controller**.

The OMi MP for Microsoft Active Directory includes the following Domain Controller indicators to monitor Active Directory server events:

CI Type	HI/ETI	Description	Value
Domain Controller	Access Permissions Errors	Indicates the number of Access Permission Errors on the Domain Controller.	Normal, High, Very High
Domain Controller	CName Records Availability	Indicates the availability of CName Records on the DNS Server of the Domain Controller.	Found, Not Found
Domain Controller	DC LDAP Bind Response Time	Indicates the response time to bind to LDAP on Domain Controller.	Normal, High, Very

CI Type	HI/ETI	Description	Value
			High
Domain Controller	DC LDAP Query Response Time	Indicates the response time of a sample LDAP query on Domain Controller.	Normal, High, Very High
Domain Controller	DFSR Service State	Indicates the status of DFSR Service on the Domain Controller.	Up, Down
Domain Controller	DIT Disk Queue Length	Indicates the queue length of DIT disk.	Normal, High, Very High
Domain Controller	DIT Disk Space Availability	Indicates the availability of free space on DIT disk.	Normal, Low, Near Capacity
Domain Controller	DIT Log Files Disk Queue Length	Indicates the queue length of DIT Log Files disk.	Normal, High, Very High
Domain Controller	DIT Log Files Disk Space Availability	Indicates the availability of free space on DIT Log Files Disk.	Normal, Low, Near Capacity
Domain Controller	DNS Query Response	Indicates the response time of a sample DNS Query on domain controller.	Normal, High, Very high
Domain Controller	FRS Status	Indicates the status of File Replication Service.	Up, Down
Domain Controller	Host Records Availability	Indicates the availability of Host Records on the DNS Server of the Domain Controller.	Found, Not found
Domain Controller	Inbound Object Updates Remaining	Indicates the number of Inbound Object Updates remaining.	Normal, High, Very High
Domain Controller	Inter site Replication Latency	Indicates the replication latency of the Domain Controller across AD Sites.	Normal, High, Very

CI Type	HI/ETI	Description	Value
			High
Domain Controller	Intra site Replication Latency	Indicates the Replication Latency of the Domain Controller within the AD Site.	Normal, High, Very High
Domain Controller	ISM Service Status	Indicates the status of Inter-site Messaging Service.	Up, Down
Domain Controller	KDC Service Status	Indicates the status of Kerberos Distribution Center Service.	Up, Down
Domain Controller	Kerberos Authentication Rate	Indicates the rate of Kerberos Authentication on the Domain Controller.	Normal, High, Very High
Domain Controller	Kerberos Server Records Availability	Indicates the availability of Kerberos Server Records on the DNS Server.	Found, Not Found
Domain Controller	LDAP Active Threads	Indicates the number of LDAP threads which are active on the Domain Controller.	Normal, High, Very High
Domain Controller	LDAP Client Sessions	Indicates the number LDAP Client Sessions on the Domain Controller.	Normal, High, Very High
Domain Controller	LDAP Server Records Availability	Indicates the availability of LDAP Server Records on the DNS Server of the Domain Controller.	Found, Not Found
Domain Controller	Logon Errors	Indicates the number of Logon Errors on the Domain Controller.	Normal, High, Very High
Domain Controller	LSASS Page Faults Rate	Indicates rate of Page Faults for Local Security Authority Subsystem Service.	Normal, High, Very High
Domain Controller	LSASS Private Bytes	Indicates the Private Bytes used by Local Security Authority Subsystem Service on the Domain Controller.	Normal, High, Very High

CI Type	HI/ETI	Description	Value
Domain Controller	LSASS Processor Time	Indicates the Processor Time used by Local Security Authority Subsystem Service on the Domain Controller.	Normal, High, Very High
Domain Controller	LSASS Working Set	Indicates the Working Set of the Local Security Authority Subsystem Service.	Normal, High, Very High
Domain Controller	Net Logon Service State	Indicates the status of Net Logon Service on the Domain Controller.	Up, Down
Domain Controller	Non Transitive Membership Evaluations	Indicates the number of non transitive membership evaluations performed.	Normal, High, Very High
Domain Controller	Notify Queue Size	Indicates the size of notify queue.	Normal, High, Very High
Domain Controller	NTDS Service State	Indicates the status of NTDS Services on the Domain Controller.	Up, Down
Domain Controller	NTFRS Page Faults Rate	Indicates rate of Page Faults for NTFRS process.	Normal, High, Very High
Domain Controller	NTFRS Private Bytes	Indicates the Private Bytes used by the File Replication Service.	Normal, High, Very High
Domain Controller	NTFRS Processor Time	Indicates the processor time used by the File Replication Service on the Domain Controller.	Normal, High, Very High
Domain Controller	NTFRS Service State	Indicates the state of NTFRS Service on the Domain Controller.	Up, Down
Domain Controller	NTFRS Working Set	Indicates the Working Set of the File Replication Service on the Domain Controller.	Normal, High, Very High
Domain	NTLM	Indicates the rate of NTLM Authentication on the	Normal,

CI Type	HI/ETI	Description	Value
Controller	Authentication Rate	Domain Controller.	High, Very High
Domain Controller	Pending Replication Synchronizations	Indicates the number of pending Replication Synchronizations.	Normal, High, Very High
Domain Controller	SAMSS Service State	Indicates the state of Security Accounts Manager Service on the Domain Controller.	Up, Down
Domain Controller	Security Descriptor Propagator Queue	Indicates the length of Security Descriptor Propagator Queue on the Domain Controller.	Normal, High, Very High
Domain Controller	Sysvol Connectivity	Indicates the connectivity to Sysvol folder.	Up, Down
Domain Controller	Sysvol Disk Space Availability	Indicates the availability of free space on Sysvol disk.	Normal, Low, Near Capacity
Domain Controller	Transitive Membership Evaluations	Indicates the number of Transitive Membership Evaluations performed on the Domain Controller.	Normal, High, Very High
Domain Controller	Directory Read Rate	Indicates the rate of Directory Read.	Normal, High, Very High
Domain Controller	Directory Search Rate	Indicates the rate of Directory Search.	Normal, High, Very High
Domain Controller	Directory Write Rate	Indicates the rate of Directory Write.	Normal, High, Very High
Domain Controller	Inbound Replication Object Rate	Indicates the rate of Inbound Replication Objects.	Normal, High, Very High

CI Type	HI/ETI	Description	Value
Domain Controller	LDAP Connectivity	Indicates the LDAP Connectivity.	Up, Down
Domain Controller	GC Connectivity	Indicates the GC Connectivity.	Up, Down
Domain Controller	Outbound Replication Object Rate	Indicates the rate of Outbound Replication Objects.	Normal, High, Very High
Domain Controller	Synchronization Failure Rate	Indicates the rate of synchronization failures.	Normal, High, Very High
Domain Controller	Sysvol Disk Queue Length	Indicates the length of Sysvol Disk Queue.	Normal, High, Very High

To access Global Catalog Server and Domain Controller Role indicators:

1. Open the Indicators pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Indicators**.

On OMi 10.x, click **Administration > Service Health > CI Status Calculation > Health- and Event Type Indicators**.

2. In the CI Type pane, click **Configuration Item > Infrastructure Element > Application Resource > DomainController Resource > DomainConttollerRole > GlobalCatalogServer**.

The OMi MP for Microsoft Active Directory includes the following Global Catalog Server and Domain Controller Role indicators to monitor Active Directory Server events:

CI Type	HI/ETI	Description	Value
Global Catalog	GC LDAP Bind Response Time	Indicates the response time to bind to LDAP on GC.	Normal, High, Very High
Global Catalog	GC LDAP Query Response Time	Indicates the response time of a sample LDAP Query on GC.	Normal, High, Very High

CI Type	HI/ETI	Description	Value
Global Catalog	GC Replication Latency	Indicates the replication latency on GC.	Normal, High, Very High
Domain ControllerRole	Response Time	Indicates the ping response time of FSMO roles.	Normal, High, Very High

## Topology Based Event Correlation (TBEC) Rules

The OMi MP for Microsoft Active Directory includes the following rules to correlate Active Directory-related events:

For more information on how the correlation rules work, see the *Operations Manager i Concepts Guide*.

### How to Access Correlation Rules

On BSM 9.2x, click **Admin > Operations Management > Event Correlation > Topology-Based Event Correlation**

On OMi 10.x, click **Administration > Event Processing > Correlation > Topology-Based Event Correlation**

### AD::DomainController:CNameRecordsAvailability >> InterSiteReplicationLatency & IntraSiteReplicationLatency

Description: CName Records Availability on the DNS Server of the Domain Controller Impacts Inter and Intra Site Replication Latency		
Cause		
CIT: Domain Controller	ETI: CName Records Availability	Value: Not Found
Symptom 1		
CIT: Domain Controller	ETI: Inter Site Replication Latency	Value: Very High
Symptom 2		
CIT: Domain Controller	ETI: Intra Site Replication Latency	Value: Very High



#### AD::DomainController:DIT Disk Queue Length >> DomainController Performance

Description: DIT Disk Queue Length Impacts Domain Controller Performance		
Cause		
CIT: Domain Controller	ETI: DIT Disk Queue Length	Value: Very High
Symptom 1		
CIT: Domain Controller	ETI: DC LDAP Bind Response Time	Value: Very High
Symptom 2		
CIT: Domain Controller	ETI: DC LDAP Query Response Time	Value: Very High
Symptom 3		
CIT: Domain Controller	ETI: Inbound Object Updates Remaining	Value: Very High
Symptom 4		
CIT: Domain Controller	ETI: Pending Replication Synchronizations	Value: Very High

#### AD::DomainController:DIT Disk Queue Length >> GlobalCatalog Performance

Description: DIT Disk Queue Length Impacts Global Catalog Performance		
Cause		
CIT: Domain Controller	ETI: DIT Disk Queue Length	Value: Very High
Symptom 1		
CIT: Global Catalog Server	ETI: GC LDAP Bind Response Time	Value: Very High
Symptom 2		
CIT: Global Catalog Server	ETI: GC LDAP Query Response Time	Value: Very High

#### AD::DomainController:DIT Disk Space Availability >> DIT Disk Queue Length & Inbound Object Updates Remaining

Description: Available DIT Disk Space Impacts DIT Disk Queue Length and Inbound Object Updates Remaining		
Cause		
CIT: Domain Controller	ETI: DIT Disk Space Availability	Value: Near Capacity
Symptom 1		
CIT: Domain Controller	ETI: DIT Disk Queue Length	Value: Very High

**AD::DomainController:DIT Disk Space Availability >> DIT Disk Queue Length & Inbound Object Updates Remaining, continued**

**Description: Available DIT Disk Space Impacts DIT Disk Queue Length and Inbound Object Updates Remaining**

Symptom 2

CIT: Domain Controller	ETI: Inbound Object Updates Remaining	Value: Very High
------------------------	---------------------------------------	------------------

**AD::DomainController:DIT Log Files Disk Space Availability & DIT Log Files Disk Queue Length**

**Description: Available Disk Space for DIT Log Files Impact DIT Log Files Disk Queue Length**

Cause

CIT: Domain Controller	ETI: DIT Log Files Disk Space Availability	Value: Near Capacity
------------------------	--	----------------------

Symptom

CIT: Domain Controller	ETI: DIT Log Files Disk Queue Length	Value: Very High
------------------------	--------------------------------------	------------------

**AD::DomainController:FRS Status >> InterSiteReplicationLatency & IntraSiteReplicationLatency**

**Description: File Replication Service Status Impacts DC Replication Latency**

Cause

CIT: Domain Controller	ETI: FRS Status	Value: Down
------------------------	-----------------	-------------

Symptom 1

CIT: Domain Controller	ETI: Inter Site Replication Latency	Value: Very High
------------------------	-------------------------------------	------------------

Symptom 2

CIT: Domain Controller	ETI: Intra Site Replication Latency	Value: Very High
------------------------	-------------------------------------	------------------

**AD::DomainController:HostRecordsAvailability >> InterSiteReplicationLatency & IntraSiteReplicationLatency**

**Description: Host Records Availability on the DNS Server of the Domain Controller Impacts Inter and Intra Site Replication Latency**

Cause

CIT: Domain Controller	ETI: Host Records Availability	Value: Not Found
------------------------	--------------------------------	------------------

Symptom 1

**AD::DomainController:HostRecordsAvailability >> InterSiteReplicationLatency & IntraSiteReplicationLatency, continued**

<b>Description: Host Records Availability on the DNS Server of the Domain Controller Impacts Inter and Intra Site Replication Latency</b>		
CIT: Domain Controller	ETI: Inter Site Replication Latency	Value: Very High
Symptom 2		
CIT: Domain Controller	ETI: Intra Site Replication Latency	Value: Very High

**AD::DomainController:ISMServiceStatus >> InterSiteReplicationLatency & IntraSiteReplicationLatency**

<b>Description: ISM Service Status Impacts Inter and Intra Site Replication Latency on the Domain Controller</b>		
Cause		
CIT: Domain Controller	ETI: ISM Service Status	Value: Down
Symptom 1		
CIT: Domain Controller	ETI: Inter Site Replication Latency	Value: Very High
Symptom 2		
CIT: Domain Controller	ETI: Intra Site Replication Latency	Value: Very High

**AD::DomainController:KDCServiceStatus >> InterSiteReplicationLatency & IntraSiteReplicationLatency**

<b>Description: KDC Service Status Impacts Inter and Intra Site Replication Latency on the Domain Controller</b>		
Cause		
CIT: Domain Controller	ETI: KDC Service Status	Value: Down
Symptom 1		
CIT: Domain Controller	ETI: Inter Site Replication Latency	Value: Very High
Symptom 2		
CIT: Domain Controller	ETI: Intra Site Replication Latency	Value: Very High

**AD::DomainController:KerberosSrvRecordsAvailability >> InterSiteReplicationLatency & IntraSiteReplicationLatency**

<b>Description: Kerberos Server Records Availability on the DNS Server of the Domain Controller Impacts Inter and Intra Site Replication Latency</b>		
Cause		
CIT: Domain Controller	ETI: Kerberos Server Records Availability	Value: Not Found
Symptom 1		
CIT: Domain Controller	ETI: Inter Site Replication Latency	Value: Very High
Symptom 2		
CIT: Domain Controller	ETI: Intra Site Replication Latency	Value: Very High

**AD::DomainController:LDAPSrvRecordsAvailability >> InterSiteReplicationLatency & IntraSiteReplicationLatency**

<b>Description: LDAP Server Records Availability on the DNS Server of the Domain Controller Impacts Inter and Intra Site Replication Latency</b>		
Cause		
CIT: Domain Controller	ETI: LDAP Server Records Availability	Value: Not Found
Symptom 1		
CIT: Domain Controller	ETI: Inter Site Replication Latency	Value: Very High
Symptom 2		
CIT: Domain Controller	ETI: Intra Site Replication Latency	Value: Very High

**AD::DomainController:LSASS Page Faults Rate >> DomainController Performance**

<b>Description: LSASS Page Faults Rate Impacts Domain Controller Performance</b>		
Cause		
CIT: Domain Controller	ETI: LSASS Page Faults Rate	Value: Very High
Symptom 1		
CIT: Domain Controller	ETI: DC LDAP Bind Response Time	Value: Very High
Symptom 2		

**AD::DomainController:LSASS Page Faults Rate >> DomainController Performance, continued**

<b>Description: LSASS Page Faults Rate Impacts Domain Controller Performance</b>		
CIT: Domain Controller	ETI: DC LDAP Query Response Time	Value: Very High
Symptom 3		
CIT: Domain Controller	ETI: Inbound Object Updates Remaining	Value: Very High
Symptom 4		
CIT: Domain Controller	ETI: Pending Replication Synchronizations	Value: Very High

**AD::DomainController:LSASS Page Faults Rate >> GlobalCatalog Performance**

<b>Description: LSASS Page Faults Rate Impacts Global Catalog Performance</b>		
Cause		
CIT: Domain Controller	ETI: LSASS Page Faults Rate	Value: Very High
Symptom 1		
CIT: Global Catalog Server	ETI: GC LDAP Bind Response Time	Value: Very High
Symptom 2		
CIT: Global Catalog Server	ETI: GC LDAP Query Response Time	Value: Very High

**AD::DomainController:Sysvol Connectivity >> Notify Queue Size**

<b>Description: Sysvol Connectivity Impacts Notify Queue Size</b>		
Cause		
CIT: Domain Controller	ETI: Sysvol Connectivity	Value: Down
Symptom		
CIT: Domain Controller	ETI: Notify Queue Size	Value: Very High

**AD::DomainController:Sysvol Disk Space Availability >> DC Replication Latency & Inbound Replication Object Rate**

<b>Description: Available Disk Space for Sysvol Impacts Domain Controller Replication Latency and Inbound Replication Object Rate</b>		
Cause		
CIT: Domain Controller	ETI: Sysvol Disk Space Availability	Value: Near Capacity
Symptom 1		

**AD::DomainController:Sysvol Disk Space Availability >> DC Replication Latency & Inbound Replication Object Rate, continued**

<b>Description: Available Disk Space for Sysvol Impacts Domain Controller Replication Latency and Inbound Replication Object Rate</b>		
CIT: Domain Controller	ETI: Inbound Replication Object Rate	Value: Very High
Symptom 2		
CIT: Domain Controller	ETI: Inter Site Replication Latency	Value: Very High
Symptom 3		
CIT: Domain Controller	ETI: Intra Site Replication Latency	Value: Very High

**AD::DomainController: Sysvol Disk Queue Length >> Domain Controller Replication Latency & Inbound Replication Object Rate**

<b>Description: Sysvol Disk Queue Length Impacts Replication Latency</b>		
Cause		
CIT: Domain Controller	ETI: Sysvol Disk Queue Length	Value: Very High
Symptom 1		
CIT: Domain Controller	ETI: Inbound Replication Object Rate	Value: Very High
Symptom 2		
CIT: Domain Controller	ETI: Inter Site Replication Latency	Value: Very High
Symptom 3		
CIT: Domain Controller	ETI: Intra Site Replication Latency	Value: Very High

**AD::FileSystem:Disk Usage Level >> DomainController Performance**

<b>Description: DIT Disk Queue Length Impacts DC Performance</b>		
Cause		
CIT: File System	ETI: Disk Usage Level	Value: Near Capacity
Symptom 1		
CIT: Domain Controller	ETI: DIT Disk Queue Length	Value: Very High
Symptom 2		
CIT: Domain Controller	ETI: DIT Log Files Disk Queue Length	Value: Very High

#### AD::FileSystem:Disk Usage Level >> DomainController Performance, continued

Description: DIT Disk Queue Length Impacts DC Performance		
Symptom 3		
CIT: Domain Controller	ETI: Sysvol Disk Queue Length	Value: Very High
Symptom 4		
CIT: Domain Controller	ETI: Pending Replication Synchronizations	Value: Very High
Symptom 5		
CIT: Domain Controller	ETI: Inbound Object Updates Remaining	Value: Very High

#### AD::Network Interface:Interface Utilization >> Sysvol Connectivity

Description: Network Interface Utilization impacts Sysvol Connectivity		
Cause		
CIT: Network Interface	ETI: Interface Utilization	Value: High
Symptom 1		
CIT: Domain Controller	ETI: SysvolConnectivity	Value: Down

#### AD::Network Interface:Interface Communication Status >> Sysvol Connectivity

Description: Network Interface Communication Status impacts Sysvol Connectivity		
Cause		
CIT: Network Interface	ETI: Interface Communication Status	Value: Critical
Symptom 1		
CIT: Domain Controller	ETI: SysvolConnectivity	Value: Down

#### AD::Network Interface:Network IO &>> Domain Naming Master Connectivity

Description: Network IO Impacts Domain naming master connectivity		
Cause		
CIT: Network Interface	ETI: Interface Utilization	Value: High
Symptom 1		
CIT: Domain Naming Master	ETI: Response Time	Value: Very High

#### AD::Network Interface:Network IO >> DomainController Connectivity

Description: Network IO Impacts DomainController Connectivity		
Cause		

#### AD::Network Interface:Network IO >> DomainController Connectivity, continued

Description: Network IO Impacts DomainController Connectivity		
CIT: Network Interface	ETI: Interface Utilization	Value: High
Symptom 1		
CIT: Domain Controller	ETI: Inter Site Replication Latency	Value: Very High
Symptom 2		
CIT: Domain Controller	ETI: Intra Site Replication Latency	Value: Very High
Symptom 3		
CIT: Domain Controller	ETI: Notify Queue Size	Value: Very High

#### AD::Network Interface:Network IO >> DomainController Performance

Description: Network IO Impacts DomainController Performance		
Cause		
CIT: Network Interface	ETI: Interface Utilization	Value: High
Symptom 1		
CIT: Domain Controller	ETI: DC LDAP Query Response Time	Value: Very High
Symptom 2		
CIT: Domain Controller	ETI: DC LDAP Bind Response Time	Value: Very High
Symptom 3		
CIT: Domain Controller	ETI: Pending Replication Synchronizations	Value: Very High
Symptom 4		
CIT: Domain Controller	ETI: Inbound Object Updates Remaining	Value: Very High

#### AD::Network Interface:Network IO >> Global Catalog Performance

Description: Network IO Impacts Global Catalog Performance		
Cause		
CIT: Network Interface	ETI: Interface Utilization	Value: High
Symptom 1		
CIT: Global Catalog	ETI: GC LDAP Query Response Time	Value: Very High
Symptom 2		
CIT: Global Catalog	ETI: GC LDAP Bind Response Time	Value: Very High



#### AD::Network Interface:Network IO &gt;&gt; Infrastructure Master Connectivity

Description: Network IO Impacts Infrastructure master Connectivity		
Cause		
CIT: Network Interface	ETI: Interface Utilization	Value: High
Symptom 1		
CIT: Infrastructure Master	ETI: Response Time	Value: Very High

#### AD::Network Interface:Network IO >> PDC Master Connectivity

Description: Network IO Impacts PDC master Connectivity		
Cause		
CIT: Network Interface	ETI: Interface Utilization	Value: High
Symptom 1		
CIT: Primary Domain Controller Master	ETI: Response Time	Value: Very High

#### AD::Network Interface:Network IO &gt;&gt; RID Master Connectivity

Description: Network IO Impacts RID master Connectivity		
Cause		
CIT: Network Interface	ETI: Interface Utilization	Value: High
Symptom 1		
CIT: Relative ID Master	ETI: Response Time	Value: Very High

#### AD::Network Interface:Network IO >> Schema Master Connectivity

Description: Network IO Impacts Schema master Connectivity		
Cause		
CIT: Network Interface	ETI: Interface Utilization	Value: High
Symptom 1		
CIT: Schema Master	ETI: Response Time	Value: Very High

#### AD::Windows:CPU Load >> DomainController Performance

Description: CPU Load Impacts DomainController Performance		
Cause		
CIT: Windows	ETI: CPU Load	Value: Bottlenecked
Symptom 1		

#### AD::Windows:CPU Load >> DomainController Performance, continued

Description: CPU Load Impacts DomainController Performance		
CIT: Domain Controller	ETI: DC LDAP Bind Response Time	Value: Very High
Symptom 2		
CIT: Domain Controller	ETI: DC LDAP Query Response Time	Value: Very High
Symptom 3		
CIT: Domain Controller	ETI: Inbound Object Updates Remaining	Value: Very High
Symptom 4		
CIT: Domain Controller	ETI: Pending Replication Synchronizations	Value: Very High

#### AD::Windows:CPU Load >> GlobalCatalog Performance

Description: CPU Load Impacts Global Catalog Performance		
Cause		
CIT: Windows	ETI: CPU Load	Value: Bottlenecked
Symptom 1		
CIT: Global Catalog Server	ETI: GC LDAP Bind Response Time	Value: Very High
Symptom 2		
CIT: Global Catalog Server	ETI: GC LDAP Query Response Time	Value: Very High

#### AD::Windows:Logical Disk Free Space >> DomainController Performance

Description: Available Logical Disk Free Space Impacts Domain Controller Performance		
Cause		
CIT: Windows	ETI: Logical Disk Free Space	Value: Near Capacity
Symptom 1		
CIT: Domain Controller	ETI: DIT Disk Queue Length	Value: Very High
Symptom 2		
CIT: Domain Controller	ETI: DIT Log Files Disk Queue Length	Value: Very High
Symptom 3		
CIT: Domain Controller	ETI: Inbound Object Updates Remaining	Value: Very High
Symptom 4		
CIT: Domain Controller	ETI: Pending Replication	Value: Very High

#### AD::Windows:Logical Disk Free Space >> DomainController Performance, continued

##### Description: Available Logical Disk Free Space Impacts Domain Controller Performance

	Synchronizations	
--	------------------	--

#### AD::Windows:RPC Service >> DomainController Replication & Notify Queue Size

##### Description: RPC Service Status impacts Domain Controller Replication Latency and Notify Queue Size

Cause		
CIT: Windows	ETI: RPC Service	Value: Unavailable
Symptom 1		
CIT: Domain Controller	ETI: Inter Site Replication Latency	Value: Very High
Symptom 2		
CIT: Domain Controller	ETI: Intra Site Replication Latency	Value: Very High
Symptom 3		
CIT: Domain Controller	ETI: Notify Queue Size	Value: Very High

## Operations Orchestration (OO) Flows

Operations Orchestration provides OO flows that enable IT process automation and run book automation. For more information about creating the mapping and a Run Book automation rule, see *How to Create a Run Book Automation Rule* and *Run Books Configuration Page*. The following section provides information about using OO flows for OMi MP for Microsoft Active Directory.

**Note:** The OO flows shipped by OMi MP for Active Directory can only be used in deployment scenarios where the application is monitored by Smart Plug-ins managed by an Operations Manager (HPOM) server. In such a case, the OO flows included in OMi MP for Active Directory can be installed on an OO server and launched through the OMi-OO integration. For information about installing OO flows, see the section *Installing Operations Orchestration (OO) Flows* in the *OMi MP for Active Directory Installation Guide*. For more information about the OMi-OO integration, see the *OMi- Operations Orchestrations Integration Guide*.

When creating the mapping for the any of the OO flows, you can set default values for the attributes listed in the following table. You need not specify these values each time you run the flows:

Attribute	Description
omServerPort	Port number of the OM Tool WS. This is an optional attribute.
omServerUser	User name for the OM Server that will be used in the OM Tool WS.
omServerPassword	Password for the OM Server that will be used in the OM Tool WS.

The following section lists the Microsoft Active Directory OO flows:

- **Check if DomainController**

You can use this flow to check if a given node is a DomainController.

You must map this flow to the CIT **domaincontroller**.

**Note:** You can run this flow only on the nodes managed by OM.

The following table lists the user input items when executing this OO flow:

Flow input	Description
omNode	FQDN of the node. This must be a managed node for the OM Server and must be specified each time you run the OO flow.
omCmdTimeout	The timeout value to be used when running the remote command on the node. This is an optional attribute and the default value is 100000.
omServer	FQDN of the OM Server. You can map this input to the Event attribute <b>Originating Server</b> .

- **Check DIT Disk Space Availability**

You can use this flow to check the available space in the DIT Disk. This flow checks if space available in the DIT Disk is above the threshold specified in the OO Flow.

**Note:** You can run this flow only on the DomainControllers monitored by OM Smart Plug-in for Microsoft Active Directory.

You must map this flow to the CIT **domaincontroller**.

The following table lists the user input items when executing this OO flow:

Flow input	Description
omNode	FQDN of the Domain Controller. This must be a managed node for the OM Server and must be specified each time you run the OO flow.
omCmdTimeout	The timeout value to be used when running the remote command on the

Flow input	Description
	node. This is an optional variable and the default value is 100000.
threshold	The threshold value for the minimum disk space (in MB) that must be free (available) on the DIT disks. This is an optional attribute and the default value is 2048 MB (2 GB).
omServer	FQDN of the OM Server. You can map this input to the Event attribute <b>Originating Server</b> .

#### • Check DomainController Health

You can use this flow to check the health of a given Domain Controller. It flow checks the following:

- If the given node is a Domain Controller
- If the LDAP Query Response time is below the specified threshold
- If the GC Query Response time is below the specified threshold
- If the available disk space for DIT is above the specified threshold

**Note:** You can run this flow only on the Domain Controllers monitored by OM Smart Plug-in for Microsoft Active Directory.

You must map this flow to the CIT **domaincontroller**.

The following table lists the user input items when executing this OO flow:

Flow input	Description
omNode	FQDN of the Domain Controller. This must be a managed node for the OM Server and must be specified each time you run the OO flow.
omCmdTimeout	The timeout value to be used when running the remote command on the node. This is an optional variable and the default value is 100000.
diskthreshold	The threshold value for the minimum disk space in MB that should be free (available) on the DIT disks. This is an optional attribute and the default value is 2048 MB (2 GB).
ldapthreshold	The threshold value for LDAP latency/GC Query in milliseconds. This is an optional attribute and the default value is 50.
omServer	FQDN of the OM Server. You can map this input to the Event attribute <b>Originating Server</b> .

#### • Check Replication Health

You can use this flow to check the health of replication for a given Domain Controller.

This flow checks the following:

- If the given node is a Domain Controller.
- If the File Replication Service is running on the Domain Controller.
- If the SYSVOL folder on the Domain Controller is shared.
- If the File Replication Service is running on all the replication partners of the Domain Controller.
- If the replication latency for each of the replication partner is below the threshold specified in the flow.

**Note:** You can run this flow only on the Domain Controllers monitored by OM Smart Plug-in for Microsoft Active Directory.

You must map this flow to the CIT **domaincontroller**.

The following table lists the user input items when executing this OO flow:

Flow input	Description
omNode	FQDN of the Domain Controller. This must be a managed node for the OM Server and must be specified each time you run the OO flow.
omCmdTimeout	The timeout value to be used when running the remote command on the node. This is an optional variable and the default value is 100000.
replicationlatency threshold	The threshold (in milliseconds) for maximum time since last replication happened from a source. This is an optional attribute and the default value is 10.
omServer	FQDN of the OM Server. You can map this input to the Event attribute <b>Originating Server</b> .

#### • GC Query Response Time

You can use this flow to determine the time taken to perform a sample GC Query in milliseconds.

**Note:** You can run this flow only on the nodes managed by OM and are members of a Microsoft Active Directory domain.

You must map this flow to the CIT **domaincontroller**.

The following table lists the user input items when executing this OO flow:

Flow input	Description
omNode	FQDN of the node. This must be a managed node for the OM Server and must

Flow input	Description
	be specified each time you run the OO flow.
omCmdTimeout	The timeout value to be used when running the remote command on the node. This is an optional attribute and the default value is 100000.
omServer	FQDN of the OM Server. You can map this input to the Event attribute <b>Originating Server</b> .

- **Get LDAP Query Response Time**

You can use this flow to determine the time taken to perform a sample LDAP Query in milliseconds.

**Note:** You can run this flow only on the nodes managed by OM and are members of a Microsoft Active Directory domain.

You must map this flow to the CIT **domaincontroller**.

The following table lists the user input items when executing this OO flow:

Flow input	Description
omNode	FQDN of the node. This must be a managed node for the OM Server and must be specified each time you run the OO flow.
omCmdTimeout	The timeout value to be used when running the remote command on the node. This is an optional attribute and the default value is 100000.
omServer	FQDN of the OM Server. You can map this input to the Event attribute <b>Originating Server</b> .

- **Get Replication Latency**

You can use this flow to determine the time (in milliseconds) since the last successful replication occurred from a replication source.

**Note:** You can run this flow only on the nodes managed by OM.

You must map this flow to the CIT **domaincontroller**.

The following table lists the user input items when executing this OO flow:

Flow input	Description
omNode	FQDN of the Domain Controller. This must be a managed node for the OM Server and must be specified each time you run the OO flow.
omReplication	FQDN of the node, which is the source for the replication. You must specify

Flow input	Description
Source	this value each time you run the OO flow.
omCmdTimeout	The timeout value to be used when running the remote command on the node. This is an optional attribute and the default value is 100000.
omServer	FQDN of the OM Server. You can map this input to the Event attribute <b>Originating Server</b> .

## Graph Templates

The following table lists the graph templates present in the OMi MP for Microsoft Active Directory:

Graph Templates	Description	Metric Name	Table in Data Store
Active Directory DNS Query Response Time Graph	Plots average of Active Directory DNS Query Response Time	RESPTIME	ADSPI_DNSDR
Active Directory SYSVOL Disk Queue Length Graph	Plots average of Active Directory SYSVOL Disk Queue Length	SYSQVALUE	ADSPI_SYSQUEUELENGTH
Active Directory SYSVOL Disk Utilization Graph	Plots percentage of Active Directory SYSVOL Disk Utilized	SYSPERCVALUE	ADSPI_SYSVOLPTFULL
Active Directory DIT Log File Disk Queue Length Graph	Plots average of Active Directory DIT Log File Disk Queue Length	LGQLENVALUE	ADSPI_LOGQUEUELENGTH
Active Directory DIT Log File Disk Utilization Graph	Plots percentage of Active Directory Log File Disk Utilized	LGPERFULLVALUE	ADSPI_LOGPERCENTFULL



Graph Templates	Description	Metric Name	Table in Data Store
Active Directory DIT File Growth Graph	Plots growth of Active Directory DIT File	INSTANCEVALUE	ADSPI_DITDBSIZE
Active Directory DIT Disk Queue Length Graph	Plots average of Active Directory DIT Queue Length	DITQLVALUE	ADSPI_DITQUEUE LENGTH
Active Directory DIT Disk Utilization Graph	Plots percentage of Active Directory DIT Disk Utilized	DITPTVALUE	ADSPI_DITPERCENT FULL
Active Directory Bind Response Time	Plots Active Directory bind times for directory and global catalog	GCBINDTIME	ADSPI_RESPONSE TIME
Active Directory Query Response Time	Plots Active Directory query times for directory and global catalog	QUERYTIME	ADSPI_RESPONSE TIME
Active Directory Replication Time by Global Catalog	Plots average replication time for global catalog servers	LATENCYDELTA	ADSPI_GCREP
Active Directory GC Availability	Plots global catalog availability per global catalog server	GCPRESENT	ADSPI_RESPONSE TIME
Active Directory Replication Latency Graph	Plots average, minimum and maximum latency per active directory domain	LATENCYAVG	ADSPI_REPLA TENCY

**Note:** For more information about Data Store, see "[Appendix: Data Sources for Logging](#)".

## Tools

The OMi MP for Microsoft Active Directory uses different tools to view and monitor the Microsoft Active Directory environment. Tools enable operators to perform actions in the context of an event from

the Event Browser. Following are the different types of tools available:

- **Executables:** Native commands that are launched locally on a host through a deployed Operations Manager Agent.
- **Scripts:** Different kinds of scripts that are executed on a host through a deployed Operations Manager Agent.

### How to Access Tools

1. Open the Tools pane:

On BSM 9.2x, click **Admin > Operations Management > Operations Console > Tools**

On OMi 10.x, click **Administration > Operations Console > Tools**

2. In the CI Types pane, click **InfrastructureElement > RunningSoftware > DirectoryServer > DomainController**.

The OMi MP for Microsoft Active Directory consists of the following tools:

CI Type	Tool	Description
DomainController	MSAD Trust Relationships	Lists the trust relationships for a domain.
DomainController	MSAD DC Demotion Preparation	Removes objects related to tracking replication latency, prior to demoting a domain controller.
DomainController	MSAD Enable Collection Manager Trace	Enables tracing for Collection Manager components. The parameter to be passed is: \$TRACELEVEL - The trace level is a value between 0 to 4, 4 being the maximum value.
DomainController	MSAD Disable Collection Manager Trace	Disables tracing for Collection Manager components.
DomainController	MSAD Check ADS Service	Connects to the ADS service of the specific node using Active Directory Service Interfaces (ADSI).
DomainController	MSAD ADS Printer Information	Creates a list of all printers known in the Active Directory. It is possible to restrict the output on a specific Organizational Units (OU) by using the parameters '-ou < name of OU >' instead of '-all'.
DomainController	MSAD Delete Older Classes	Deletes older Active Directory Management Template data source and classes.

CI Type	Tool	Description
		<b>Note:</b> The tool has to be run only if the Active Directory Management Pack has been upgraded.
DomainController	Start File Replication Service	Starts the File Replication Service.

## Chapter 4: Customizing OMi MP for Microsoft Active Directory

The following section provides information about customization scenarios for Microsoft Active Directory.

- [Creating Microsoft Active Directory Management Template](#)
- [Editing Microsoft Active Directory Management Template](#)


### Creating Microsoft Active Directory Management Template

The following section provides information about creating Microsoft Active Directory Management Template:


1. Open the Management Templates & Aspects pane:  
  
On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**  
  
On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**
2. In the Configuration Folders pane, click **Configuration Folders > Microsoft Application Management > Microsoft Active Directory > Management Templates**.
3. If you want to create a new configuration folder, click  **Create Configuration Folder**. The Create Configuration Folder window opens.
4. Provide a name and description to the new configuration folder. For example, you can name the new configuration folder as <Test>.
5. Click **OK**. The new configuration folder is created.
6. In the Management Templates & Aspects pane, select the new configuration folder and click , and then click  **Create Management Template**. The Create Management Template window opens.
7. In the **General** tab, specify a **Name** to the new Management Template and click **Next**.

8. In the **Topology View** tab, select a topology view from the drop-down list. For example, AD\_Logical\_View. The Topology View displays all the CI types that you want to manage with this Management Template.
9. Click an item in the topology map or select the CI type from the **CI Type** drop-down list to which the Management Template can be assigned. For example, you can select DomainController.
10. Click **Next**.
11. In the **Aspects** tab, add the Aspects to the Management Template. You must add the **Microsoft AD Collection Schedule** Aspect to the new Management Template. The **Microsoft AD Collection Schedule** Aspect contains the scheduled task policy templates, which are essential for data collection.

To add an existing Aspect, follow these steps:

- a. Select the Aspect you want to add from the Available Aspects matching the CI Types pane. You can use **CTRL** or **SHIFT** key to select multiple Aspects.
  - b. Click  to move the Aspect to the Selected Aspects pane. The Aspect is added to the Management Template.
12. Click **Next**.
  13. In the **Parameters** tab, you see a list of all the parameters from the Aspects that you added to this Management Template. You can edit the default values of a parameter.

To edit parameters:

    - a. Double-click the parameter or select the parameter from the list, and then click  **Edit**. The Edit Parameter dialog box opens.
    - b. Modify the default value of the parameter and click **OK**.
  14. Click **Finish** in the Create Management Template window. The new Management Template appears in the Management Templates & Aspects pane.

## Editing Microsoft Active Directory Management Template

You can edit the Microsoft Active Directory Management Templates and modify the following components:

- Parameters
- Microsoft Active Directory Aspects


## Editing Parameters

**Use Case:** You are using Extensive Microsoft Active Directory Management Template to monitor Microsoft Active Directory set up in your environment. You are monitoring DIT disk space with low free space and want to modify the parameters corresponding to the DIT disk space to closely monitor the free space available.

To closely monitor the DIT disk space, you must modify the DIT disk space parameters - DIT Disk Percent Full. Threshold Warning.

You can edit the parameters at two levels - Before deployment and after deployment.

### Before Deployment:

1. Open the Management Templates & Aspects pane:  
  
On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**  
  
On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**
2. In the Configuration Folders pane:  
  
**Configuration Folders > Microsoft Application Management > Microsoft Active Directory > Management Templates**
3. Select **Extensive Microsoft Active Directory Management Template** from the list, and then click . The Edit Management Template window opens.
4. Click the **Parameters** tab. The Parameters list populates.
5. Select the **DIT Disk Percent Full Threshold Warning** parameter you want to modify, and then click . The Edit Parameter window opens.
6. You can change the default threshold value in the Constant Value (*Numeric*) section. Click **OK**.
7. In the Edit Management Template window, click **OK**. The version of the Microsoft Active Directory Management Template is incremented.

### After Deployment:

1. Open the Assignments & Tuning pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Assignments & Tuning**

On OMi 10.x, click **Administration > Monitoring > Assignments & Tuning**

2. In the **Browse Views** tab, select the **AD\_Logical\_View** that contains the CI for which you want to edit the value.
3. In the list of CI, click a CI. The Assignment Details pane lists the current parameter values.
4. You can change the default values in the Assignment Details pane by following these steps:
  - a. Double-click **DIT Disk Percent Full Threshold Warning** parameter. The Edit Parameter dialog box opens.
  - b. Change the value and click **OK**. The new parameter value is deployed to relevant CIs.

**Note:** The version number of the Microsoft Active Directory Management Template is incremented when any customization is made to the Microsoft Active Directory Management Template.


## Editing Aspects


**Use Case:** You are using the Essential Microsoft Active Directory Management Template to monitor critical and minimal set of Microsoft Active Directory and Server deployment. You do not want to use some Aspects which are part of the Essential Microsoft Active Directory Management Template. In this scenario, you can remove the Aspect associated with the Management Template by following these steps:

1. Open the Management Templates & Aspects pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Management Templates & Aspects**

On OMi 10.x, click **Administration > Monitoring > Management Templates & Aspects**

2. In the Configuration Folders pane, select **Configuration Folders > Microsoft Application Management > Microsoft Active Directory > Management Templates**.
3. Select the **Essential Microsoft Active Directory Management Template** and click . The Edit Management Template window opens.

4. Click the **Aspects** tab. The Aspects associated with the Essential Microsoft Active Directory Management Template appears.
5. Select the Aspect that you want to remove from the Selected Aspects pane and click  to move the Aspect to the Available Aspects pane. You can use **CTRL** or **SHIFT** key to select multiple Aspects.

**Note:** Moving the Aspect(s) from Selected Aspects pane to the Available Aspects pane removes the Aspect(s) associated with the Management Template.

6. Click **OK**. The version of the Microsoft Active Directory Management Template is incremented.



## Chapter 5: Deployment Scenarios

This section provides information about deploying OMi MP for Microsoft Active Directory for monitoring Microsoft Active Directory servers.

### Deploying OMi MP for Microsoft Active Directory to Monitor Active Directory Server Availability and Performance

To deploy OMi MP for Microsoft Active Directory to monitor the availability and performance of Microsoft Active Directory server, follow these steps:

1. Add nodes that you want to monitor to the OMi console.
2. Deploy Microsoft Active Directory Discovery Aspect on the managed nodes.
3. Deploy Essential Microsoft Active Directory Management Template.

For more information about deploying OMi MP for Microsoft Active Directory, see [Getting Started](#).

### Deploying OMi MP for Microsoft Active Directory to Monitor Active Directory Replication

To deploy OMi MP for Microsoft Active Directory to monitor Active Directory Replication, follow these steps:

1. Add nodes that you want to monitor to the OMi console.
2. Deploy Microsoft Active Directory Discovery Aspect on the managed nodes.
3. Deploy the following Aspects:
  - Microsoft AD Replication

- Microsoft AD Replication Statistics
- Microsoft AD Replication Logs

For more information about deploying OMi MP for Microsoft Active Directory, see [Getting Started](#).

## Deploying OMi MP for Microsoft Active Directory to monitor Active Directory Servers Using ADFS

To deploy OMi MP for Microsoft Active Directory to monitor Active Directory servers using ADFS, follow these steps:

1. Add nodes that you want to monitor to the OMi console.
2. Deploy Microsoft Active Directory Discovery Aspect on the managed nodes.
3. Deploy the following Aspects:
  - Microsoft AD Federation Services
  - Microsoft AD Federation Service Logs

For more information about deploying OMi MP for Microsoft Active Directory, see [Getting Started](#).

# Chapter 6: Troubleshooting

The following section provides information about troubleshooting scenarios:


## Licensing count is not updated

**Problem:** Licensing count is not updated on License Management

**Solution:** To resolve this problem, follow these steps:

1. After installing OMi MP for Microsoft Active Directory, ensure that the license is activated by following these steps:
  - a. Open the License Management pane:

On BSM 9.2x, click **Admin > Platform > Setup and Maintenance > License Management**

On OMi 10.x, click **Administration > Setup and Maintenance > License Management**
  - b. Click  and select the **license.dat** file. The license details appears in the License Management window.

License Management provides details about the name, license type, days left, expiration date, capacity, and capacity details.
2. To check for the license usage on the managed node, run the following command on the managed node:

```
<OvAgentDir>/bin/ovodetect -t
```

If the output of the preceding command is `mpinstance="1"` then Microsoft Active Directory servers are being monitored. If the output of the preceding command is `mpinstance="0"` then Microsoft Active Directory servers are not being monitored.
3. If the license is still not updated in the License Management, restart agent on the managed node by running the following command:

```
<OvAgentDir>/bin/ovc- restart opcmsga
```

## Microsoft Active Directory CI does not appear in RTSM

**Problem:** Microsoft Active Directory CI does not sync in RTSM from node.

**Solution:** To resolve this problem, follow these steps:

1. Open the Infrastructure Settings pane:

On BSM 9.2x, click **Admin > Platform > Setup and Maintenance > Infrastructure Settings**

On OMi 10.x, click **Administration > Setup and Maintenance > Infrastructure Settings**

2. In the Infrastructure Settings Manager, select **Applications > Operations Management**.
3. In the Operations Management - HPOM Topology Synchronization Settings, the packages for Topology Sync should contain the packages that are used for topology synchronization - **default;nodegroups;operationsagent;HPOprSys;HPOprAds**.
4. Ensure that the policy - **MSAD\_Discovery** is available and is deployed on the managed node for discovering Microsoft Active Directory by running the following command:

```
%ovInstalldir%\bin\ovpolicy -l
```

5. Check the Microsoft Active Directory discovery log file on the managed node:

```
<ovagentdir>/log/OvAdsDisc.log
```

## Management Templates and Aspects are not deployed on the Managed Nodes

**Problem:** Management Templates and Aspects are not deployed on the managed nodes.

**Solution:** To resolve this problem, follow these steps:

1. To check the deployment status, open the Deployment Jobs pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Deployment Jobs**

On OMi 10.x, click **Administration > Monitoring > Deployment Jobs**

2. To check the assignment status, open Assignments & Tuning pane:

On BSM 9.2x, click **Admin > Operations Management > Monitoring > Assignments & Tuning**

On OMi 10.x, click **Administration > Monitoring > Assignments & Tuning**

3. Check the following OMi log files:

```
%topaz_home%\log\EJBContainer\opr-webapp.log
```

```
%topaz_home%\log\EJBContainer\opr-configserver.log
```

## No Data for Performance Manager i (PMi) Graphs or Reports

**Problem:** The information to create graphs or reports is not available from OMi MP for Microsoft Active Directory

**Solution:** To resolve this problem, follow these steps:

1. Run the following command to check if the graph data sources are created:

```
ovcodautl -showds
```

Verify the list of data sources and ensure ADSPI data source is created.

2. If the data sources are not created, run the following command to create the data source:

```
<ovagentdir>\bin\instrumentation\adspi_ddf.bat
```

3. You can run the following command to verify if the data is being logged in the data sources:

```
ovcodautl -dumpds ADSPI
```

## Performance Collection Fails

**Problem:** Microsoft Active Directory performance collection fails

**Solution:** To solve this problem, follow these steps:

1. Check whether the collection schedule Aspect is deployed on the node.
2. On the node, go to <ovagentdir>\conf\MSAD\MSAD\_config directory and check whether the following file exists:

```
MSAD_MetricDef.xml
```

3. You can run the following command to verify if the performance collection is appearing or not:

```
msscollectionmanaer.exe -s MSAD -f MEDIUM -r ALL -o p
```

This command returns performance collection on success and lists errors on failure.

## Failed Binary on Managed Node

**Problem:** Agent fails to update the discovered services to the OM management server.

**Solution:** Run the Microsoft Active Directory discovery binary on the managed node by performing the following steps:

1. Log on to the managed node as an administrator.
2. Open the instrumentation directory from the command prompt.
3. Run the `<ovagentdir>\bin\instrumentation\ovadsdisc.exe > out.xml` command.
4. Check if `out.xml` is in the required xml format by opening it in the web browser.

## Data Logging Policies Not Logging Data

**Problem:** The data logging policy cannot log the data.

**Solution:** Check if the data source ADSPI is created. To check the data source is created, follow these steps:

1. Log on to the managed node as an administrator.
2. Run the `ovcodautl -obj > out.txt` command from the command prompt.
3. Check the `out.txt` file to ensure that the data source ADSPI is created.

## Unable to collect or log perfmon counter metrics

**Problem:** The perfmon counter metrics are not getting logged.

**Solution:** To collect perfmon counter metrics, enable the **MSAD Enable Collection Manager Trace** tool.

**Note:** After you collect the data, ensure to disable the trace using **MSAD Disable Collection Manager Trace** tool.

## Tracing

If problem occurs, turn on tracing. Tracing captures all information related to Microsoft Active Directory, including FSMO and replication conditions, status, and errors included in the Microsoft Active Directory logs.

You can trace all the Microsoft Active Directory Management Pack binaries with suffix -l 1.

Consider the following example:

The MSAD\_DNS\_DC\_A\_Chk policy has the following command:

```
ADSPI_DnsMon.exe -svc ldap -rec host -type missing -n MSAD_DNS_DC_A_Chk -L10N _en
```

To trace the binary ADSPI\_DnsMon.exe, you must change this command to:

```
ADSPI_DnsMon.exe -svc ldap -rec host -type missing -n MSAD_DNS_DC_A_Chk -L10N _en -  
l 1
```

**Note:** You can find the trace file ADSPI\_DnsMon.log in the following folder:

```
%ovagentdir%\log
```

All the Microsoft Active Directory policies with embedded scripts are traced by changing the debug variable to **DEBUG=TRUE** found in the script.

## Appendix: Data Sources for Logging

The OMi MP for Microsoft Active Directory includes the following data in the data store on the node to facilitate the data-collection procedure:

Table in Data Store	Aspects	Policy Name/Collection Name	Metrics	Metric Data Type CODA / PA
ADSPI_DITDBSIZE	Microsoft AD DIT	MSAD_TotalDitSize	INSTANCE_NAME	UTF8 / Text
			InstanceValue	UINT64 / Precision 0
ADSPI_DITPERCENT FULL	Microsoft AD DIT	MSAD_DITPercentFull	DITPTName	UTF8 / Text
			DITPTValue	REAL64/ Precision 2
ADSPI_DITQUEUE LENGTH	Microsoft AD DIT	MSAD_DITQueueLength	DITQLName	UTF8/ / Text
			DITQLValue	UINT64/ Precision 0
ADSPI_DNSDR	Microsoft AD DNS Response	MSAD_DNS_DC_Response	RespTime	REAL64/ Precision 2
ADSPI_DNSSP	Microsoft AD DNS	MSAD_DNS_LogDNSPagesSec	IsDomainCtrl	REAL64/ Precision 2
			PagesPerSec	
ADSPI_DOMAIN	Microsoft AD DIT	MSAD_TotalDitSize	DomainName	UTF8 / Text
			DomainValue	
ADSPI_FSMO	Microsoft AD FSMO Resonse	MSAD_SCH_FSMOLogging	FSMO	UTF8 / Text



Table in Data Store	Aspects	Policy Name/Collection Name	Metrics	Metric Data Type CODA / PA
	Time		SERVER	UTF8 / Text
			PINGTIME	REAL64 / Precision 2
			FSMOBINDTIME	REAL64 / Precision 2
ADSPI_FSMO_ROLE MVMT	Microsoft AD FSMO Role Movement	MSAD_SCH_FSMORoleMovement	FSMORM	UTF8 / Text
			ISROLEHOLDER	REAL64 / Precision 2
ADSPI_GCREP	Microsoft AD Replication Auto Baseline	MSAD_Rep_GC_Check_and_Threshold_Monitor_AT	GCREPName	UTF8 / Text
			LatencyDelta	REAL64 / Precision 2
ADSPI_LOGDISK SIZE	Microsoft AD DIT	MSAD_LogFilesPercentFull	DISKName	UTF8 / Text
			DISKValue	UINT64 / Precision 0
ADSPI_LOG PERCENTFULL	Microsoft AD DIT	MSAD_LogFilesPercentFull	LGPERFULLName	UTF8 / Text
			LGPERFULLValue	REAL64 / Precision 2
ADSPI_LOGQUEUE LENGTH	Microsoft AD DIT	MSAD_DITQueueLength	LGQLENName	UTF8 / Text
			LGQLENValue	UINT64 / Precision 0

Table in Data Store	Aspects	Policy Name/Collection Name	Metrics	Metric Data Type CODA / PA
ADSPI_NTDS	Microsoft AD Services	MSAD_NTDS Details	DRAInboundBTS	REAL64 / Precision 2
			DRAInboundBTS	REAL64 / Precision 2
			DRAOutboundBCSec	REAL64 / Precision 2
			DSThreadsinUse	UINT64 / Precision 0
			DRAInboundBCSec	REAL64 / Precision 2
			DRAOutboundBTS	REAL64 / Precision 2
			DRAInboundBNC WSSec	REAL64 / Precision 2
			DRAOutboundBNC WSSec	REAL64 / Precision 2
ADSPI_NTDSP	Microsoft AD Services	MSAD_NTDSPROCDETAILS	INSTANCE_NAME	UTF8/Text
			PctProcTime	REAL64 / Precision 2
			PageFaultsSecs	REAL64 / Precision 2
			WorkingSet	UINT64 / Precision 0

Table in Data Store	Aspects	Policy Name/Collection Name	Metrics	Metric Data Type CODA / PA
ADSPI_REPLA TENCY	Microsoft AD Replication	MSAD_Rep_ MonitorIntraSiteReplic ation and MSAD_ Rep_ MonitorInterSiteReplic ation	LATENCYMIN	REAL64 / Precision 2
			LATENCYMAX	
			LATENCYAVG	
			LASTREPDELTA MIN	
			LASTREPDELTA MAX	
			LASTREPDELTA AVG	
			LASTREPTIME	REAL64 / Precision 2
ADSPI_ RESPONSE TIME	Microsoft AD Response Time	MSAD_SCH_ ResponseLogging	BINDTIME	REAL64 / Precision 2
			QUERYTIME	REAL64 / Precision 2
			GCBINDTIME	REAL64 / Precision 2
			GCQUERYTIME	REAL64 / Precision 2
			GCPRESENT	UINT64 / Precision 0
			AVAILABILITY	UINT64 / Precision 0
			GCAVAILABILITY	UINT64 / Precision 0
ADSPI_SITE	Microsoft AD DIT	MSAD_TotalDitSize	SiteName	UTF8 / Text
			SiteValue	

Table in Data Store	Aspects	Policy Name/Collection Name	Metrics	Metric Data Type CODA / PA
ADSPI_ SYSVOLPT FULL	Microsoft AD SYSVOL	MSAD_SYSVOL_ PercentFull	SYSPERCName	UTF8 / Text
			SYSPERCValue	REAL64 / Precision 2
ADSPI_ TIMESYNC	Microsoft AD Replication	MSAD_Rep_ TimeSync	TIMESYNC	REAL64 / Precision 2
ADSPI_TRUST	Microsoft AD Trust	MSAD_Trust_Mon_ Add_Del	Changetype	UINT64 / Precision 0
			TrustingDomain	UTF8 / Text
			TrustedDomain	UTF8 / Text
			Trustattributes	UINT64 / Precision 0
			TrustDirection	UINT64 / Precision 0
			TrustStatus	UINT64 / Precision 0
			TrustStatusString	UTF8 / Text
			TrustType	UINT64 / Precision 0
ADSPI_DNSSR	Microsoft AD DNS Response	MSAD_DNS_Server_ Response	ResTime	REAL64 / Precision 2
ADSPI_ INBOUNDS	Microsoft AD	MSAD_Rep_ InboundObjs	InstanceName	UINT64 / Precision

Table in Data Store	Aspects	Policy Name/Collection Name	Metrics	Metric Data Type CODA / PA
	Replication Statistics			0
			Objects	REAL64 / Precision 2
ADSPI_SCHEMA MISMATCH	Microsoft AD Directory Access	MSAD_SyncSchemaMisMatch	SchemaMismatch Name	UTF8 / Text
			SchemaMismatchCnt	UTF8 /
ADSPI_OUTBOUNDS	Microsoft AD Replication Statistics	MSAD_OutboundObjs	INSTANCE_NAME	UTF8/ Text
			OUTOBJECTS	UTF64 Precision 0
ADSPI_ADFS	Microsoft AD Federation Services	MSAD_ADFS	INSTANCE_NAME	UTF8 / Text
			INSTANCE_VALUE	UTF8/ Text
ADSPI_NTDS	Microsoft AD Services	MSAD_NTDSPROCDETAILS	INSTANCE_NAME	UTF8/Text t
			PctProcTime	REAL64/ PRECISION 2
			PageFaultsSec	REAL64/ PRECISION 2
			WorkingSet	UINT64/ PRECISION 0
ADSPI_GLOBALCATALOG	Microsoft AD Global Catalog Access	MSAD_GlobalCatalogDS	INSTANCE_NAME	UTF8/ Text
			DIRECTORYWRITES	UTF8/ Text

Table in Data Store	Aspects	Policy Name/Collection Name	Metrics	Metric Data Type CODA / PA
			DIRECTORYREADS	UTF8/ Text
			DIRECTORYSEARCHES	UTF8/ Text
ADSPI_PROCESS	Microsoft AD Services	MSAD_LASSPROCDETAILS	INSTANCE_NAME	UTF8/ Text
			PAGEFAULTS	UTF8/ Text
			PRIVATEBYTES	UTF8/ Text
			PERCENTPROCTIME	UTF8/ Text
			WORKINGSET	UTF8/ Text
ADSPI_NTDS	Microsoft AD Services	MSAD_NTDS Details	INSTANCE_NAME	UTF8/ Text
			DRAINBOUNDDBTS	UTF8/ Text
			DRAOUTBOUNDBCSEC	UTF8/ Text
			DSTTHREADSINUSE	UTF8/ Text
			DRAINBOUNDBCSEC	UTF8/ Text
			DRAOUTBOUNDDBTS	UTF8/ Text
			DRAINBOUNDNBCWSEC	UTF8/ Text
			DRAOUTBOUNDNBCWSSSEC	UTF8/ Text
ADSPI_KerberosAuth	Microsoft AD	MSAD_Authentications	INSTANCE_NAME	UTF8/ Text

Table in Data Store	Aspects	Policy Name/Collection Name	Metrics	Metric Data Type CODA / PA
	Authentication	<b>Note:</b> By default, this collection is disabled. You need to enable it in the <b>MSAD_Collection Definition</b> policy to log data into it.		
			KERBAUTH	UTF8/ Text
			NTLMAUTH	UTF8/ Text
ADSPI_DirectoryAccess	Microsoft AD Directory Access	MSAD_DirectoryAccess	INSTANCE_NAME	UTF8/ Text
			LDAPACTIVTH	UTF8/ Text
			LDAPBINDTIME	UTF8/ Text
			LDAPCLIENTSES	UTF8/ Text
			DIRECTORYWRITES	UTF8/ Text
			DIRECTORYREADS	UTF8/ Text
			DIRECTORYSEARCHES	UTF8/ Text
ADSPI_RepMon	Microsoft AD Replication Statistics	MSAD_RepMon	PENDINGREPSYNC	UTF8/ Text
			PENDINGREPSYNC	UTF8/ Text
			INBOUNDBYTESCMP	UTF8/ Text
			INBOUNDBYTESNCMP	UTF8/ Text
			INBOUNDOBJUPD	UTF8/ Text
			NOTIFYQUEUE	UTF8/

Table in Data Store	Aspects	Policy Name/Collection Name	Metrics	Metric Data Type CODA / PA
				Text
ADSPI_SecMon	Microsoft AD Authentication	MSAD_AccessSecurityMon  <b>Note:</b> By default, this collection is disabled. You need to enable it in the <b>MSAD_Collection Definition</b> policy to log data into it.	SVRNAME	UTF8/Text
			ERACSPERM	UTF8/Text
			ERRGTACCESS	UTF8/Text
			ERRLOGON	UTF8/Text
ADSPI_DSSECMon	Microsoft AD Security	MSAD_DSSECURITY	INSTANCE_NAME	UTF8/Text
			OMESAMNTMEM	UTF8/Text
			SECDESC	UTF8/Text
			TWOSAMTRNMEM	UTF8/Text
ADSPI_ISMCHK	Microsoft AD Services	MSAD_Rep_ISM_Chk	SERVNAME	UTF8/Text
			SRVDISPNAME	UTF8/Text
			SERVSTATUS	UTF8/Text
			SERVSTATE	UINT32/PRECISION 0
ADSPI_KDCCHK	Microsoft AD Services	MSAD_KDC_Chk	SERVNAME	UTF8/Text
			SRVDISPNAME	UTF8/Text
			SERVSTATUS	UTF8/



Table in Data Store	Aspects	Policy Name/Collection Name	Metrics	Metric Data Type CODA / PA
				Text
			SERVSTATE	UINT32 PRECISION 0
ADSPI_NetLogon	Microsoft AD Services	MSAD_NetLogon_Chk	SERVNAME	UTF8/ Text
			SRVDISPNAME	UTF8/ Text
			SERVSTATUS	UTF8/ Text
			SERVSTATE	UINT32/ PRECISION 0
ADSPI_NTFRS	Microsoft AD Services	MSAD_NTFRS_Chk	SERVNAME	UTF8/ Text
			SRVDISPNAME	UTF8/ Text
			SERVSTATUS	UTF8/ Text
			SERVSTATE	UINT32/ Text PRECISION 0
ADSPI_SAMSS	Microsoft AD Services	MSAD_SAMSS_Chk	SERVNAME	UTF8/ Text
			SRVDISPNAME	UTF8/ Text
			SERVSTATUS	UTF8/ Text
			SERVSTATE	UINT32/ PRECISION 0

Table in Data Store	Aspects	Policy Name/Collection Name	Metrics	Metric Data Type CODA / PA
ADSPI_DSFR	Microsoft AD Services	MSAD_DSFR_Chk	SERVNAME	UTF8/ Text
			SRVDISPNAME	UTF8/ Text
			SERVSTATUS	UTF8/ Text
			SERVSTATE	UINT32 / PRECISION 0
ADSPI_NTDSCHK	Microsoft AD Services	MSAD_NTDS_Chk	SERVNAME	UTF8/ Text
			SRVDISPNAME	UTF8/ Text
			SERVSTATUS	UTF8/ Text
			SERVSTATE	UINT32/ PRECISION 0
ADSPI_DFS	Microsoft AD DFSR Throughput	MSAD_DFS_Rep_Folders	INSTANCE_NAME	UTF8/ Text
			BANDWIDTH	UTF8/ Text
			COMPRESSED	UTF8/ Text
			CONFLICT_FILE	UTF8/ Text
			CONFLICT_SPACE	UTF8/ Text
			FILE_RETIRED	UTF8/ Text
			FILE_SUCCEEDED	UTF8/ Text

Table in Data Store	Aspects	Policy Name/Collection Name	Metrics	Metric Data Type CODA / PA
			TOTAL_FILE_RECV	UTF8/ Text
			RDC	UTF8/ Text
ADSPI_DFS_Con	Microsoft AD DFSR Performance	MSAD_DFS_Rep_Connections	INSTANCE_NAME	UTF8/ Text
			BANDWIDTH	UTF8/ Text
			BYTES_RECV	UTF8/ Text
			COMPRESSED_FILES	UTF8/ Text
			TOTAL_RECV	UTF8/ Text
ADSPI_DFS_vol	Microsoft AD DFSR Volumes	MSAD_DFS_Rep_Svc_Vol	INSTANCE_NAME	UTF8/Text
			DB_COMMIT	UTF8/Text
			DB_LOOKUPS	UTF8/Text
			USN_ACCEPT	UTF8/Text
			USN_READ	UTF8/Text
			DFS_VOLS	UTF8/Text
			USN_PERCENTAGE	UTF8/Text
ADSPI_SYSQUEUELENGTH	Microsoft AD SYSVOL	MSAD_SYSVOL_DiskQueueLength	SYSQNAME	UTF8/Text
			SYSQVALUE	UINT64 / PRECISI

<b>Table in Data Store</b>	<b>Aspects</b>	<b>Policy Name/Collection Name</b>	<b>Metrics</b>	<b>Metric Data Type CODA / PA</b>
				ON 0

# Send documentation feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

**Feedback on User Guide (OMi Management Pack for Microsoft Active Directory 1.00)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to [docfeedback@hpe.com](mailto:docfeedback@hpe.com).

We appreciate your feedback!