White Paper

Monitoring Active Directory Using System Center Operations Manager 2007 R2

Abstract

Active Directory is a key component in many organizations IT infrastructure. This white paper discusses on basic Active Directory monitoring and some basic issues that are generated in System Center Operations Manager after an agent has been installed on the Active Directory Server. The white paper also discusses the solution to these issues thus, briefly explaining the cause for the generated alerts.

Table of Contents

Introduction

This white Paper takes into consideration, the Active Directory Environment in an IT infrastructure. Identifying and troubleshooting Active Directory Alerts can be a time consuming and lengthy process for the administrator or the helpdesk team.

SCOM has the ability to monitor many servers including Active Directory, whether in the same or different domains. This is achieved by downloading the Active Directory Management Pack and installing agents on the respective domain controllers. Once this is done, a communication channel is established between the agent and the Management Pack sitting on the SCOM Management Server. This will allow the agent to report to the Management Server any errors or issues that occur or exist in the Active Directory environment.

Situation

In this scenario we consider monitoring Active Directory. This white paper will discuss all the necessary steps that are required to monitor Active Directory Successfully.

Solution

Once Operations Manager is set up, in order to monitor Active Directory, it is required that an agent be installed on the respective Machine. Following are the steps to be taken to install an agent on the Active Directory Server in order to monitor Active Directory environment in Operations Manager:

Step 1: Installing Agent on Active Directory Server.

Unlike other machines, Agents on Active Directory cannot be pushed through the normal user account. They can only be pushed using Domain Account privileges. Therefore, agents need to be installed manually. The main reason for this is simply because, on normal servers the agents are pushed using the Local Administrator account. Now, because Active Directory does not have a Local Administrator account, agents on the Active Directory server are installed using the Domain Administrator account.

Now that the agents are installed, the Active Directory server can be found in the Operations Manager Console. However, right now no Active Directory components will be monitored as this will require Active Directory Management Pack to be imported.

Please note that at point only the current Windows Operating System will be monitored if the respective Management Pack for the Operating System has been imported.

Step 2: Management Pack for Active Directory Domain Controller

Depending on what version of Active Directory Server your organization has, you need to download and import the respective Management Pack from the Microsoft website. The link can be found at http://www.microsoft.com/downloads/details.aspx?FamilyId=008F58A6-DC67-4E59-95C6-D7C7C34A1447&displaylang=en

The Active Directory Management Pack assists in providing Proactive and Reactive Monitoring of the Active Directory Environment. The pack examines events of Active Directory components and other sub-systems placed in the Application, System and Service event logs.

The management pack will generate alerts for any configuration issues. The management pack gathers event logs and gives related knowledge articles with extra details about the user, possible causes and solutions to the causes. The pack also monitors for critical windows services that are important for Active Directory such as Net Logon, Kerberos Distribution Center, and File Replication. The pack provides real time performance and event monitoring thus allowing quick action to be taken for critical, performance or capacity alerts.

The Active Directory Management Pack monitors the Domain Controller and the external components associated with the Domain Controller. The pack includes a set of pre-defined rules, scripts and reports that are required to monitor Active Directory Domain Controllers successfully.

Step 3: Post Installation Issues

After an agent has been installed and Management Pack been imported, Active Directory alerts, warnings will start getting generated in the Operations Manager Console. Most of the alerts, warnings will be genuine related to the Organization's Active Directory Infrastructure. However there will be some generic script based warnings that need to be resolved immediately. If these warnings are not resolved they keep getting generated often and the count increases. The warning generated is **Script Based Test Failed to Complete.**

Below listed are the details of this warning:

AD Lost and Found Object Count: The script 'AD Lost and Found Object Count' Failed to create object 'McActiveDir.ActiveDirectory'. This is an unexpected Error. The error returned was 'ActiveX component can't create object' **(0x1AD)**.

AD Database and Log: The script 'AD Database and Log' failed to create Object 'McActiveDir.ActiveDirectory'. The error returned was: 'ActiveX Component can't create object' **(0x1AD).**

AD DNS Verification: An error occurred while executing 'AD DNS Verification' Invalid procedure call or argument **0x5**

AD Database and Log: The script 'AD Database and Log' failed to create Object 'McActiveDir.ActiveDirectory'. The error returned was: 'The specified Module could not be found.' **(0x8007007E).**

These script based warnings can be fixed by installing **oomads.msi** file.

Oomads.msi: oomads is the Active Directory Management Pack Helper Object. It contains some ActiveX objects to enable the scripts in the Active Directory Management Pack Object.

The Management Pack guide states that Active Directory Helper Object will be installed automatically when an agent is installed through the console. However, the main reason for these errors being generated is due to a manual agent push to the domain controllers before the Active Directory Management Pack is imported. To prevent errors from occurring before deploying Active Directory Management Pack or to recover from errors that have already been generated, you will need to install the Active Directory Helper Object File on the affected Domain Controllers. The oomads.msi file can be located on the server hosting agent in **Drive: \Program Files\System Center Operations Manager 2007\HelperObjects.**

Once the file is located in the above mentioned folder, double click on the .msi file to install oomads. After the installation is complete the Script based warnings will automatically close from the Active Alerts context in the operations console.

It should be noted that the above process is only applicable for agents that are pushed manually. For those servers that pushed using the **Discovery Wizard** the Helper Object file is automatically installed.

Therefore what this means is that we will need to install the oomads.msi on every domain controller for which an agent has been installed manually. This will be a lengthy and time consuming process if an organization has to monitor multiple Domain Controllers in the same and different domain.

The script **ADLocalDiscoveryDC.vbs** helps to solve this problem. This script automatically installs the helper object on all domain controllers provided that oomads.msi is located in **Drive: \Program Files\System Center Operations Manager 2007\HelperObjects.** Thus, we have

to ensure that the helper object is in the same directory as the one mentioned above. This means that the next time this script executes, oomads will be installed automatically on the Domain Controllers. As this script only executes on Domain Controllers, the file oomads.msi can be copied to all servers that are agent managed, which also prevents manual installation on a Domain Controller.

The way SCOM determines if a server is a domain controller or not is by running the query **"Select NumberOfProcessors From Win32_ComputerSystem Where DomainRule>3"**. If the query returns as true the computer will be marked as a domain controller.

Monitoring Active Directory in a Different Domain/Forest

The way multi forest Active Directory Environment works in SCOM is based on two workflows. These workflows are scripts that execute on the Root Management Server to discover instances of Active Directory such as forests, domains, sites, domain controllers and also identify the relationship between these instances that are spread over different forests.

The first work flow is **"Microsoft.AD.Topology.Discovery"** is defined to discover multi-forest. The second workflow **"Microsoft.AD.Remote.Topology.Discovery"** is defined to discover Connection objects. These workflows run on each Domain Controller on which an agent is installed.

It is important to note that the proxy agent should be **enabled** on the **Root Management Server** and all the **Domain Controllers** because both are required for discovery data submission.

Thus, SCOM server allows monitoring Active Directory from a different forest or domain. To discover other domains a trust relationship is required between that domain and the Root Management Server. This is possible by using certificates on the SCOM server and on the server respectively. Once the certificates are installed, agents can be pushed on the servers manually. After the agent is installed script errors will start generating in the SCOM server. These script errors are ones mentioned above.

There are two ways of building a trust between different domains. The first option is to install certificates manually on the Root Management Server and on the Active Directory Server that is in a different domain. This will build a trust relationship between the two domains and thus, enable monitoring of a server in Operation's Manager that is in a different domain.

The second option is to introduce a gateway server. Gateway servers are used enable the management of agents that are outside the Kerberos trust boundary of the Management Servers. This option suits best when there are more than five servers in a different domain that need to be monitored through Operation's Manager. Thus, by having certificates on the Gateway Server and the Root Management Server it is possible to monitor servers that are outside the trusted domain.

The advantage of this practice over the first is that, it does not require installing certificates manually on each server. Instead, by having a gateway server, a single certificate is required on this server and on the RMS to monitor multiple servers that are outside the trusted domain.

Active Directory Replication Monitoring

Active Directory Management Pack also takes into consideration the replication issues that occur in an organization's Active Directory Environment. There are certain rules and monitors defined in the Management Pack that are defined to handle Replication Monitoring.

There are 14 rules defined in the Management Pack to run the Replication Monitoring Script. These rules are defined for Windows 2000, Windows 2003 and Windows 2008 Server OS. However, it should be noted that some rules have the exact same display name. *The reason for the rules being triplicate is because they were created to differentiate replication problems from the three versions of Domain Controllers*. The rules are stated below:

AD Replication is occurring slowly (Three rules with this name)

One or More Domain Controllers May not be replicating (Three Rules with this name)

DC failed to synchronize naming context with its replication partner (Three Rules with this name)

All of the replication partners failed to replicate

AD Replication Performance Collection – Metric Replication Latency

AD Replication Performance Collection – Metric Replication Latency: Minimum

AD Replication Performance Collection – Metric Replication Latency: Maximum

AD Replication Performance Collection – Metric Replication Latency: Average

Thus, if any override value need to be disabled or configured for Replication Monitoring, the values must be set of all the above Rules.

The way replication monitoring works in SCOM is by executing an AD Replication VBscript found on all Domain Controllers. The first time the script executes, an Object in the Domain Controller in the OpsMgrLatencyMonitors Container for each Active Directory server is monitored. For every sixth execution of the script, an update is performed on the **AdminDescription** attribute in the Domain Controller's Object with the present time. In order to see these objects, you will need to run the **ADSIEdit.msc** command. In order to determine the time taken for replication by each Domain Controller, the script will run the **whenCreated** attribute and the **AdminDescription** attribute. The first attribute specifies the time the object arrived on the Domain Controller and the later specifies the time the object was updated in the Domain Controller. The time difference between these two attributes tells how long it takes to replicate an object from a given Domain Controller.

Below listed are some common alerts that are generated in SCOM related to the Active Directory Replication Monitoring.

Alert	Issue	Resolution
AD Replication Monitoring – Access Denied	This occurs on the domain controller when its fails to create the OpsMgrLatency container	The OpsMgrLatency Monitor should have permission required to create the container. If the container does not exist, it is because it does not have sufficient permissions.
KCC Cannot Computer the Replication Path	KCC detected problems on multiple domain controllers	This alert will be displayed when connectivity is lost from a site to the remote site. The site could be down due to power loss or if the domain controller has been shutdown but still exists in the perspective of Active Directory. This alert could also be generated in those environments where the site topology displays the site link but the network is configured to not display some sites.
Active Directory Replication is slower than the configured threshold. Intersite Expected Max Latency (min) default 15 Intrasite Expected Max Latency (min) default 5	This alert will occur if the connectivity is lost for long period of time.	If the alert is not current, and the repeat count is the same and not increasing and the **RepAdmin RepLsum** task comes clean, then this alert can be closed.
Active Directory Replication is slower than the configured threshold. Intersite Expected Max Latency (min) default 15 Intrasite Expected Max Latency (min) default 5	The remote replication topology was defined to be 60 minutes, not the standard of 15	The recommendation to this alert is that if your environment does not use the 15 minute latency, then the best option is to disable or override this alert.
Active Directory Replication is Occurring Slowly	Issue is the same as identified above.	This rule could be disabled or closed for those individual servers where the Active Directory Replication was not configured with the default replication time of 15 minutes.
One or More Domain Controllers may not be replicating	The AD Management Pack will report this issue across all the Domain Controllers if any one Domain Controller is down	Ensure All Domain Controllers that are monitored by Operations Manager to be up. Otherwise close alerts that are greater than 5 days if the alert represents current issue if the issue has been self-resolved.

Important Configuration Steps after Importing Management Pack

Once the Management pack is imported and installed, it is important to configure and tune the Management Pack in the right way to eliminate some generic alerts that will generate after the Pack is imported. Below described are the necessary configuration steps:

i) After the Pack is imported, make sure you can view all the Domain Controllers. This can be by done navigating to the Authoring Pane, selecting groups and then selecting the Domain Controllers. Right click on Domain Controllers and select View Group Members. This will list all the Domain Controllers.

ii) The next step is to enable the proxy agent on all domain controllers. To do so click on the administration pane then select Agent Managed under Device Management. Right Click and select properties and click on the security tab and tick the "Allow this agent to act as a proxy and discover managed objects on other computers" check box. This has to be done on all the Domain Controllers.

iii) Configure the Replication Account by navigating to the security option in the Administration Pane.

iv) It is important to validate the **OpsMgrLatencyMonitor** container. There should also be sub-folders created for each Domain Controller. If this does not happen, then this is due to insufficient permissions.

v) Now go to the monitoring pane and select the Microsoft Windows Active Directory Management Pack and view the Topology Diagram.

vi) Also, check for the Active Directory Topology Diagram in the Distributed Application which can be located in the Authoring Pane.

Conclusion

By importing Active Directory Management Pack an SCOM administrator can perform a deeper and more meaningful monitoring of Domain Controllers. To ensure that you have a healthy Active Directory Environment in SCOM it is important to have the right configuration of rules and monitors. The Management Pack will generate alerts which will display faults in the Active Directory Domain Controllers. However it should be noted that these alerts are genuine and not false positives. This white paper describes some important and necessary configuration steps and measures to eliminate false positives to accurately monitor the Active Directory Environment.

About the Author

Abdul Karim Rajiwte is System Centre Specialist presently working for Expit, Kuwait. His expertise includes System Centre Operations Manager 2007 R2.

References

Active Directory Management Pack for System Center Operations Manager 2007
http://www.microsoft.com/Downloads/details.aspx?FamilyID=008f58a6-dc67-4e59-95c6-d7c7c34a1447&displaylang=en

Expit
www.expit.com

Microsoft System Centre Operations Manager
http://www.microsoft.com/systemcenter/operationsmanager/en/us/default.aspx

Use the Agent Setup Wizard
http://technet.microsoft.com/en-us/library/cc950513.aspx