This document explains the required steps to configure the Active Directory Security (ADS) Assessment included with your Azure Log Analytics Workspace and Microsoft Unified Support Solution Pack.

There are two scenarios available to configure the ADS solution; due to nature of the assessment identifying critical risks within your Active Directory environment, it is strongly recommended to utilize the OMS Gateway scenario.

1. OMS Gateway and data collection machine
2. Data Collection Machine only

**OMS Gateway and data collection machine**
This scenario is the most secure and recommended option to help protect and separate privileged account credentials which are used on the scheduled task configured on the data collection machine needed to run the assessment. This scenario requires two computers. One will be designated as the data collection machine, and the second machine will be the OMS Gateway. In this scenario, the data collection machine has no Internet connection and connects to the OMS Gateway to upload the data to log analytics. The OMS Gateway must have Internet access. This scenario is recommended for environments where the Internet connection is restricted from the data collection machine or where security is a concern due to this schedule task requirement. For information about the OMS Gateway, go to [https://go.microsoft.com/fwlink/?linkid=830157](https://go.microsoft.com/fwlink/?linkid=830157).

The data collection machine must be a member of the forest being assessed. It will collect data from all the domain controllers in the forest. After the data is collected, the data collection machine will analyze the information, and for increased security, will forward the data to an OMS Gateway to upload it to log analytics.

The following path shows the relationship between your Windows computers and log analytics after you have installed and configured the OMS Gateway and data collection machine.

*Data collection machine ➔ Collects data from all domain controllers in the forest ➔ Forward collected data to the OMS Gateway ➔ Submit data to the log analytics workspace*

**Data collection machine only**
This scenario can be used when the data collection machine can contact log analytics directly. It requires one computer that will be designated as the data collection machine which has to be able to access the Internet to upload data to log analytics. This scenario can be used in environments where the Internet connection is not restricted.

The data collection machine must be a member of the forest being assessed. It will collect data from all the domain controllers in the forest. After the data is collected, the data collection machine will analyze the information and then upload the data to log analytics directly, which will require HTTPS connectivity to your log analytics workspace.

The following path shows the relationship between your Windows computers and log analytics after you have installed and configured the data collection machine:

*Data collection machine ➔ Collects data from all domain controllers in the forest ➔ Submit data to the log analytics workspace.*

**Detail information on these configurations and requirements are found later in this document.**
Table of Contents

System Requirements and Configuration at Glance ................................................................. 3
  Supported Versions .............................................................................................................. 3
  Common to both scenarios ............................................................................................... 3
  OMS Gateway and Data Collection machine ................................................................. 3
  Data Collection Machine only ....................................................................................... 3
  Powershell Remoting ..................................................................................................... 4

Setting up the Active Directory Security Assessment ......................................................... 10

Appendix ........................................................................................................................... 13
  Data Collection Methods ............................................................................................... 13
System Requirements and Configuration at Glance

According to the scenario you want to use, review the following details to ensure that you meet the necessary requirements.

Supported Versions


Common to both scenarios

- You will need a log analytics workspace
- User account rights:
  - A domain account with the following rights:
    ▪ Enterprise Administrator group membership
    ▪ OR
    ▪ Administrator group membership to every domain controller in the forest.
    ▪ Membership in Local Administrators group on the Data Collection machine.
    ▪ Administrative access to all Microsoft Domain Name System (DNS) servers that the domain controllers participate with.

OMS Gateway and Data Collection machine

- **Data Collection Machine** must have Microsoft Monitoring Agent installed and configured to collect data as per [Data Collection Machine only](#) section
- **Microsoft Monitoring Agent** is required to be installed and configured on the **OMS Gateway** with the correct Workspace ID.
- The **OMS Gateway** can be a standalone or a member server. It requires Windows Server 2012 R2 or later.
- The **OMS Gateway** must be able to connect to the Internet using HTTPS to submit the collected data to your log analytics workspace. This connection can be direct, via a proxy.
- **OMS Gateway hardware**: Minimum 4 GB of RAM and 2 GHz processor.
- **OMS Gateway user account rights**: None required.

Click the link to download the “Setup Assessment” documentation to install the OMS Gateway and Microsoft Monitoring Agent.
[https://go.microsoft.com/fwlink/?linkid=860142](https://go.microsoft.com/fwlink/?linkid=860142)

Data Collection Machine only

**Important**: The option of running the on-demand assessment directly from Data Collection Machine only, and not through the OMS Gateway is strongly discouraged as it increases the risk of exposing Enterprise Administrator credentials through an internet connected machine.

The option of installing the Microsoft Monitoring Agent on a system outside the Domain Controller network or Domain Controller security zones is strongly discouraged due to the risk of exposing privileged domain account credentials to lower trust systems, which contradict Microsoft guidance and recommendations for [Securing Privileged Access](#).
• **Microsoft Monitoring Agent** requires computers running Windows Server 2008 SP1 or later (or Windows 7 SP1 or later).

• The **data collection machine** must be joined to one of the domains of the forest to be assessed.

• **Data collection machine hardware**: Minimum 8 gigabytes (GB) of RAM, 2 gigahertz (GHz) dual-core processor, minimum 10 GB of free disk space.

• The **data collection machine** is used to connect to all domain controllers in the forest and retrieve information from it. The machine is communicating over Remote Procedure Call (RPC), Server Message Block (SMB), WMI, remote registry, Lightweight Directory Access Protocol (LDAP) and Windows Remote Management (WinRM).

• Microsoft .NET Framework 4.6.2 or newer installed.

• The data collection machine must be able to submit the collected data to your workspace using HTTPS. This connection can be direct, via OMS Gateway.

• For the **Microsoft Monitoring Agent** to provide data and to connect and register with the log analytics service, it must send data and have adequate access to the internet. If you use a proxy server for communication between the agent and the log analytics service, you will need to ensure that the appropriate resources are accessible. If you use a firewall to restrict access to the Internet, you need to configure your firewall to permit access to log analytics. To ensure data can be submitted follow the steps in *Configure Proxy and Firewall Settings in Log Analytics* at [https://azure.microsoft.com/en-in/documentation/articles/log-analytics-proxy-firewall/](https://azure.microsoft.com/en-in/documentation/articles/log-analytics-proxy-firewall/).

**Powershell Remoting**

To complete the assessment with the accurate results, you will need to configure all in-scope target machines for Powershell remoting.

Powershell on the tools machine is used to scan the servers for installed security patches as well as audit policy configuration.

• Windows Update Agent must be running on all domain controllers for the security update scan.

• PowerShell version 2 or greater is required on target domain controllers and comes installed by default starting with Windows Server 2008 R2. For Windows Server 2008 SP2, PowerShell version 2 is not installed by default. It is available for download here [https://aka.ms/wmf3download](https://aka.ms/wmf3download).

**Additional requirements for Windows Server 2008-2012 R2 (or later if defaults modified) Target Machines:**

The following three items must be configured on target domain controllers to support data collection: PowerShell Remoting, WinRM service and Listener, and Inbound Allow Firewall Rules.

**Note 1:** Windows Server 2012 R2 and Windows Server 2016 have WinRM and PowerShell remoting enabled by default. The following configuration steps detailed below will only need to be implemented if the default configuration for target machines has been altered.

**Note 2:** Windows Server 2008—Windows Server 2012 have WinRM disabled by default. The following settings will need to be configured to support PowerShell Remoting:

• Execute **Enable-PSRemoting** PowerShell cmdlet on each target machine within the scope of the assessment. This one command will configure PS-Remoting, WinRM service and listener, and enable required Inbound FW rules. A detailed description of everything Enable-PSRemoting does is documented [here](https://aka.ms/wmf3download).

OR

• Configure **WinRM / PowerShell remoting** via Group Policy (Computer Configuration\Policies\Administrative...
Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service
  o In 2008 R2 it’s “Allow automatic configuration of listeners”.
  o In 2012 R2 (and later) it’s “Allow remote server management through WinRM”.
• Configure **WinRM service for automatic start** via Group Policy (Computer Configuration\Policies\Windows Settings\Security Settings\SystemServices)
  o Define **Windows Remote Management** (WS-Management) service for **Automatic startup mode**
• Configure **Inbound allow Firewall Rules**: This can be done individually in the local firewall policy of every in-scope target domain controller or via a group policy which allow communication from the tools machine.

Two steps are involved to configure a group policy to enable both WinRM listener and the required inbound allow firewall rules:

  A) Identify the IP address of the source computer where data collection will occur from.
  B) Create a new GPO linked to the domain controller organizational unit, and define an inbound rule for the tools machine

A.) **Log into the chosen data collection machine to identify its current IP address using IPConfig.exe from the command prompt.**

An example output is as follows

C:\>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . : fe80::X:X:X:X%13
  IPv4 Address . . . . . . . . . . : X.X.X.X
  Subnet Mask . . . . . . . . . . : X.X.X.X
  Default Gateway . . . . . . . . : X.X.X.X

Make a note of the IPv4 address of your machine. The final step in the configuration will use this address to ensure only the data collection machine can communicate with the Windows Update Agent on the domain controllers.
B.) Create, configure, and link a group policy object to the domain controllers OU in each domain in the forest.

1. Create a new GPO. Make sure the GPO applies to the Domain Controllers organizational unit. Give the new group policy a name based on your group policy naming convention or something that identifies its purpose similar to “AD Security Assessment”

2. Within the GPO open: (Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service). Enable “Allow remote server management through WinRM” or “Allow automatic configuration of listeners” depending on your OS.

3. Create an advanced Inbound Firewall Rule to allow all network traffic from the tools machine to the Domain Controllers. This can be applied to the same GPO that was used in step 1 above. (Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security – LDAP:/xxx\Inbound Rules)
4. To create the new rule, Right Click on “Inbound Rules” and select “New”

5. Create a custom rule and choose “Next”
6. Allow “All programs” from the tools machine and click “Next”.

7. Allow all protocols and ports, then click “Next”.
8. Specify the IP address of the tools machine and click “Next”.

8. Choose to “Allow the connection” and click Next

9. Choose to select network profile “Domain” and click “Next”

10. Choose a name for the rule (Example: ADSecurityAssessmentToolsMachine)

After you have finished the installation of the Microsoft Management Agent/OMS Gateway, and configured Powershell Remoting on the target machines, continue with the next section to set up the assessment.
Setting up the Active Directory Security Assessment

When you have finished the installation of the Microsoft Monitoring Agent/OMS Gateway, you are ready to setup the Active Directory Security Assessment.

On the designated data collection machine, complete the following:

1. Open the Windows PowerShell command prompt as an Administrator

2. Run the `Add-ADSecurityAssessmentTask` command where `<Directory>` is the path to an existing directory used to store the files created while collecting and analyzing the data from the environment.

   ```powershell
   Add-ADSecurityAssessmentTask -WorkingDirectory "C:\OMS\ADSec_Assessment"
   ```

3. Provide the required user account credentials. These credentials are used to run the Active Directory Security Assessment.

   ```powershell
   Add-ADSecurityAssessmentTask -WorkingDirectory "C:\OMS\ADSec_Assessment"
   ```

   **NOTE:** This domain account must have all the following rights:

   - An Enterprise Administrator account with admin access to every domain controller in the forest.
     - By default, the Enterprise Admins group is member of the built-in Administrators group in every domain. Ensure that this membership has not been changed. If the Enterprise Admins group is not member of the built-in Administrators group of a domain, add the account under which the Active Directory Security Assessment runs to the built-in Administrators group of that domain.
   - Unrestricted network access to every domain controller in the forest.
4. The script will continue with the necessary configuration. It will create a scheduled task that will trigger the data collection.

```
Administrator: Windows PowerShell
PS C:\users\romin> Add-ADSecurityAssessmentTask -WorkingDirectory "C:\OMS\ADSec_Assessment"
[ADSecurityAssessment]Detected agent configuration for Management Group ADI-49900795-7a88-4ee-4-a2de-ca8a46fc0c9e
[ADSecurityAssessment]Enter the credential to be used to run this assessment. Credentials will be used to connect to remote server(s) for assessment.
[ADSecurityAssessment]Entry
[ADSecurityAssessment]Enter the password for redmond\romin:
*************
[ADSecurityAssessment]Creating Windows Schedule task to run assessment...
[ADSecurityAssessment]ADSecurityAssessment setup successful.
[ADSecurityAssessment]Detailed log is at: C:\users\romin\AppData\Local\Temp\Assessments_Configuration_2017017_071514.log
PS C:\users\romin>
```

5. Data collection is triggered by the scheduled task named **ADSecurityAssessment** within an hour of running the previous script and then every 7 days. The task can be modified to run on a different date/time or even forced to run immediately.

![Task Scheduler](image)

6. During collection and analysis, data is temporarily stored under the **WorkingDirectory** folder that was configured during setup, using the following structure:

```
This PC > ODSisk (C) > OMS > ADSec_Assessment > ADSecurityAssessment
```

7. After data collection and analysis is completed on the tools machine, it will be submitted to your log analytics workspace depending on the scenario you have chosen:
   - **Directly** if the Data Collection Machine is connected to the Internet and configured to submit directly.
   - **Through to the OMS Gateway Server** if this option is configured, it will then submit the data to your log analytics workspace.
8. After a few hours, your assessment results will be available on your log analytics Dashboard. Click the **AD Security Assessment** tile to review:

![Active Directory Security Assessment](image)

9. You will then be presented with findings grouped by the focus area.
Appendix
Data Collection Methods

The Active Directory Security Assessment in the log analytics workspace and Microsoft Unified Support Solution Pack uses multiple data collection methods to collect information from your environment. This section describes the methods used to collect data from an Active Directory environment. The collectors are:

1. Registry Collectors
2. LDAP Collectors
3. .NET Framework
4. Windows PowerShell
5. FileDataCollector
6. Windows Management Instrumentation (WMI)
7. Custom C# Code

1. Registry Collectors
Registry keys and values are read from the data collection machine and all Domain Controllers. They include items such as:
   - Service information from HKLM\SYSTEM\CurrentControlSet\Services.
     This allows determination of where the AD Database and log files are located on each DC, and gets detailed information on each service relevant to the proper function of AD.
   - Operating System information from HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
     This allows one to determine Operation System information such as Windows Server 2008 or Windows Server 2012.

2. LDAP Collectors
LDAP queries are used to collect data for the Domain, DCs, Partitions, group memberships, account names and their properties, object permissions, and other components from AD itself. For a complete list of ports required by AD, see: http://support.microsoft.com/kb/179442.

3. .NET Framework

4. Windows PowerShell
Collects various information, such as:
   - ACL information on organizational unit objects in Active Directory
   - Auditing Policy Configuration
5. **FileDataCollector**

Enumerates files in a folder on a remote machine, and optionally retrieves those files. Examples include:

- Scripts in SYSVOL
- Group Policy Preference configuration files

6. **Windows Management Instrumentation (WMI)**

WMI is used to collect various information such as:

- **WIN32_Volume**
  
  WMI collects information on Volume Settings for each DC in the forest. The information is used for instance to determine the system volume and drive letter which allows the client to collect information on files located on the system drive.

- **Win32_Process**
  
  Collect information on the processes running on each DC in the forest. The information provides insight in processes that consume a large amount of threads, memory or have a large page file usage.

- **Win32_LogicalDisk**
  
  Used to collect information on the logical disks. We use the information to determine the amount of free space on the disk where the database or log files are located.

7. **Custom C# Code**

Collects information not captured using other collectors. The primary example here is the collection of effective user rights on the domain controllers.