Active Directory Security Assessment: Prerequisites and Configuration

This document explains the required steps to configure the Active Directory Security (ADS) Assessment included with your Azure Log Analytics Workspace and entitled Microsoft On-Demand assessment.

! **Important:** There are configuration and setup tasks to be completed prior to executing the assessment setup tasks in this document. For all prework, follow the Assessment Setup Guide from the Services Hub Resource Center.

Key Assessment Features
Services Hub Connector: **Creating your Connector**
Programs: **Creating your Program**

Table of Contents

This document was last updated on April 18, 2023. To ensure you have the latest version of this document, check here: https://go.microsoft.com/fwlink/?linkid=860104

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 Target Operating System Versions

- Your Active Directory domain controllers must run Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 or Windows Server 2022

Environment Permissions

- **Assessment account rights:**
  - A domain account (can be a user or a Managed Service Account) with the following rights:
    - Enterprise Administrator.
    - Administrative access to every domain controller in the forest.
    - Administrative access to all Microsoft Domain Name System (DNS) servers that the domain controllers participate with.
    - Administrative access on the data collection machine
    - Log on as a batch job privileges on the data collection machine.

Data Collection machine

- The **data collection machine** must be joined to one of the domains of the forest to be assessed.
- **Data collection machine hardware:** Minimum 16 gigabytes (GB) of RAM, 2 gigahertz (GHz dual-core processor, minimum 10 GB of free disk space.
  - Depending on the size and complexity of your environment, you will need to increase the total amount of RAM to ensure that the data collection is successful and completes in a timely manner.
- 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 Distributed Component Object Model (DCOM).

- Microsoft .NET Framework 4.8 or newer installed and running Windows Server 2012 R2 or newer.
- Antivirus and any other type of Security software need to be configured to exclude Assessment related files, file types, working directory folders and process (Omsassessment.exe) to avoid process termination, blockage and alerts. Add an exclusion to Windows Security

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. If PowerShell version 2 is not installed, it is available for download here https://aka.ms/wmf3download

Additional requirements for Windows Server 2012-2012 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.

Note1: *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 2012 has 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.

OR

- Configure **WinRM / PowerShell remoting** via Group Policy (Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service) ○ In 2012 (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) ○ 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 inscope 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 . :

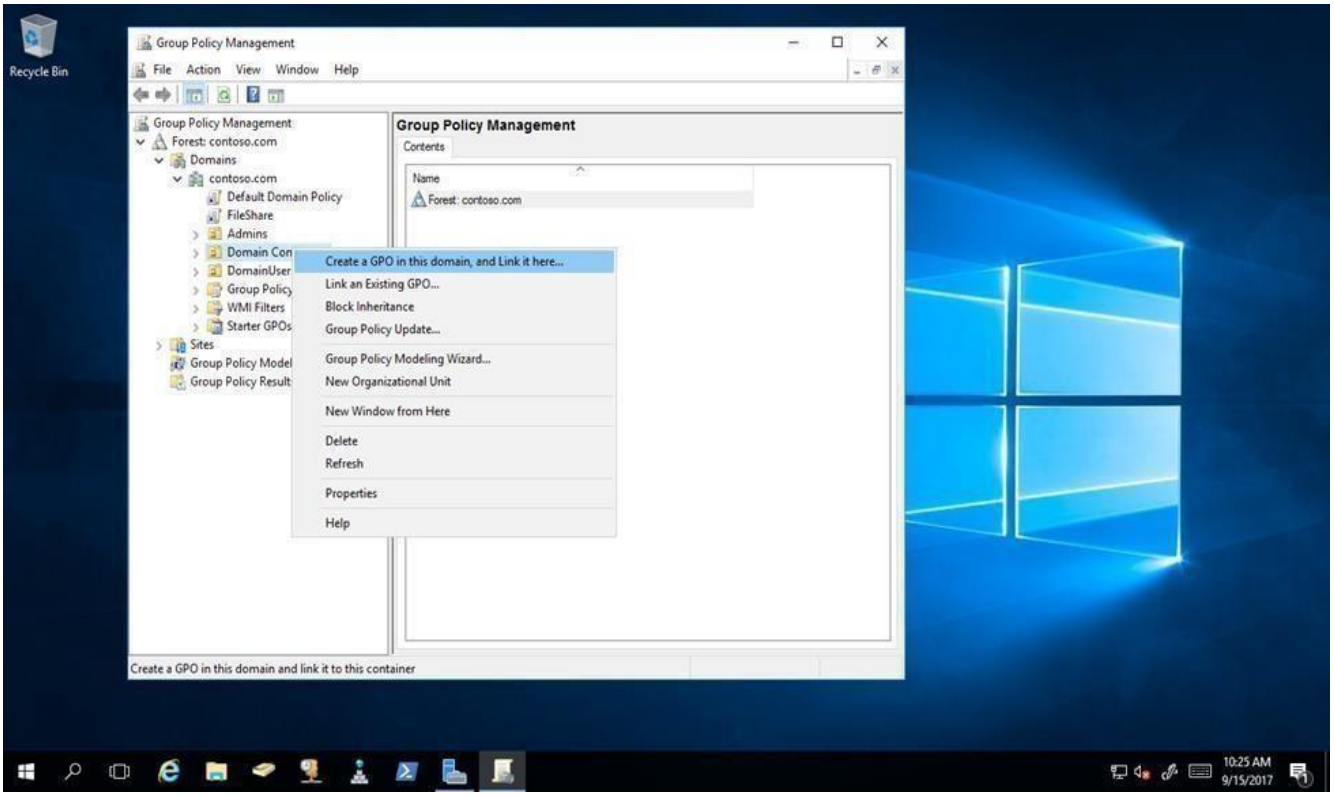
Link-local IPv6 Address . . . . . : fe80::X:X:X:X%13

IPv4 Address. . . . . : **X.X.X.X**

Subnet Mask . . . . . : X.X.X.X

Default Gateway . . . . . : X.X.X.X

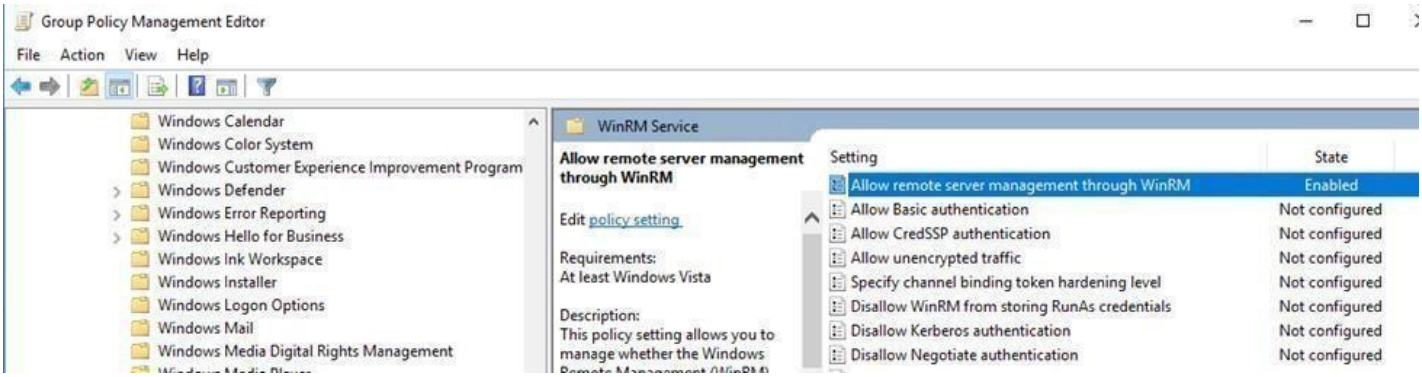
Make a note of the IPv4 address of your machine. The final step in the configuration will use this address to ensure only the data collection machine can communicate with the Windows Update Agent on the domain controllers.



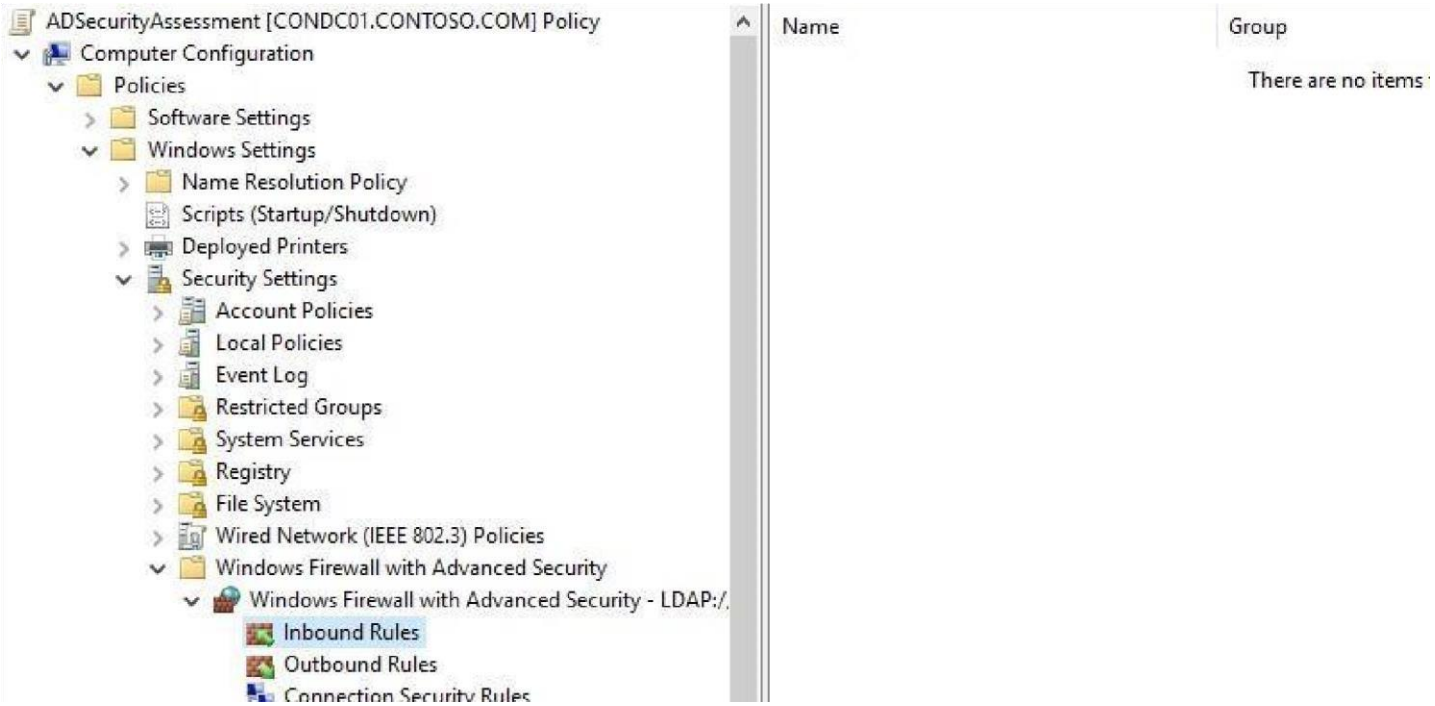
B.) Create, configure, and link a group policy object to the domain controllers OU in each domain in the forest.

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”

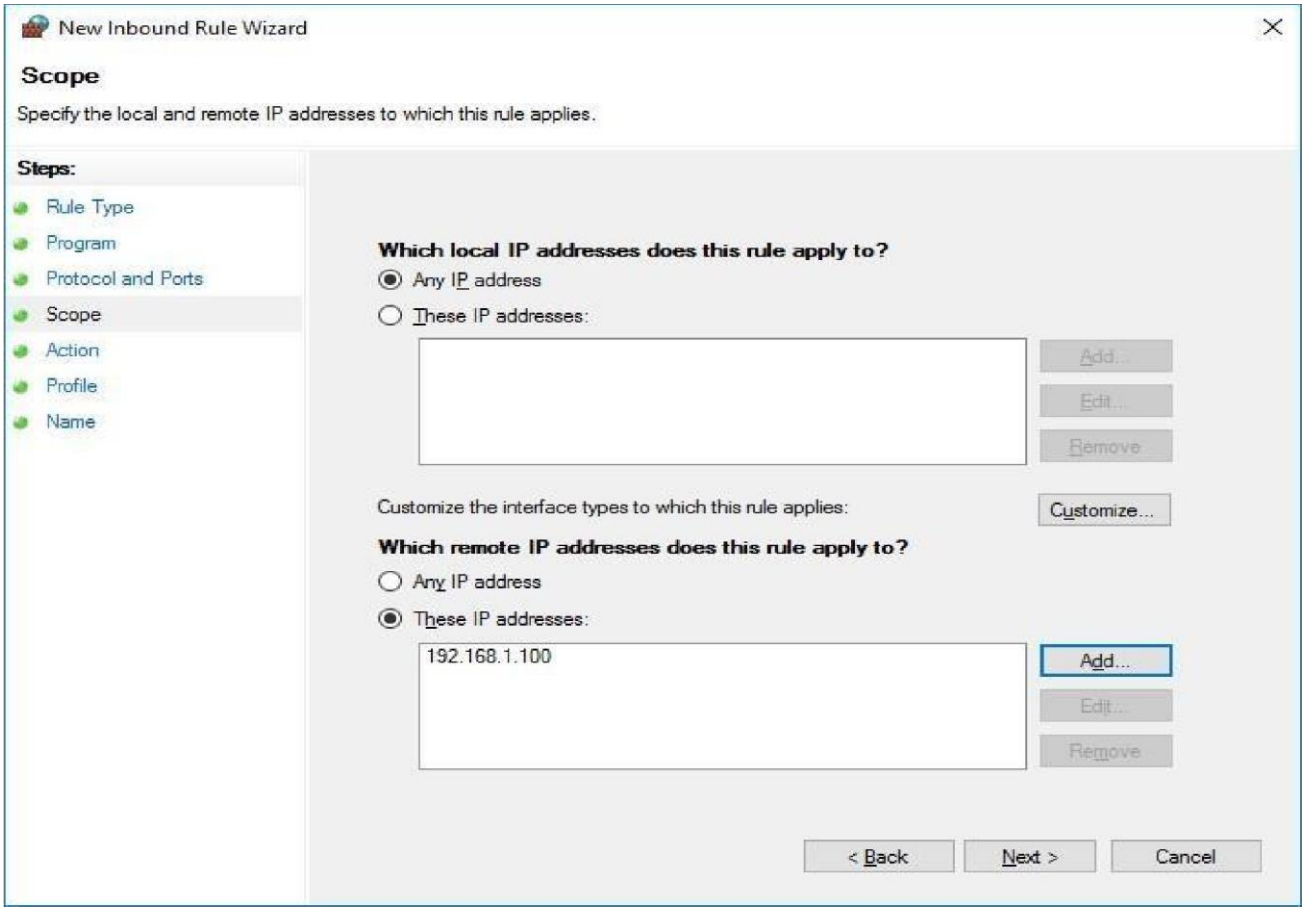
2. Within the GPO open: (Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service). Enable “**Allow remote server management through WinRM**” or “**Allow automatic configuration of listeners**” depending on your OS.



3. Create an advanced Inbound Firewall Rule to allow all network traffic between the data collection machine and the Domain Controllers. This can be the 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. On the **Rule Type** page select **Custom** rule and choose “Next”
6. On the **Program** page select “**All programs**” from the tools machine and click “Next”.
7. On the **Protocols and Ports** page, ensure **Any** protocol and **All** ports are selected, then click “Next”.
8. On the **Scope** page specify the IP address of the data collection machine under the “**Which remote IP addresses does this rule apply to?**” portion of the scope page, then select “Next”.



9. On the **Action** page, choose to “Allow the connection” and click “Next”.
10. On the **Profile** page, choose to select network profile “**Domain**” and click “Next”.
11. Choose a name for the rule (Example: ADSecurityAssessmentToolsMachine) and complete the wizard.

Setting up the Active Directory Security Assessment

When you have finished the configuration of the Azure Arc enrollment/Azure VM Extension, you are ready to setup the Active Directory Security Assessment. There are two approaches to setting up the assessment scheduled task depending on whether the scheduled task account will be a managed service account or a user account.

Configure with Managed Service Account

Managed service accounts are the preferred option for running the assessment due to their credential management and security related benefits over standard user accounts. Managed service accounts must be provisioned in Active Directory Domain Services and authorized in the environment.

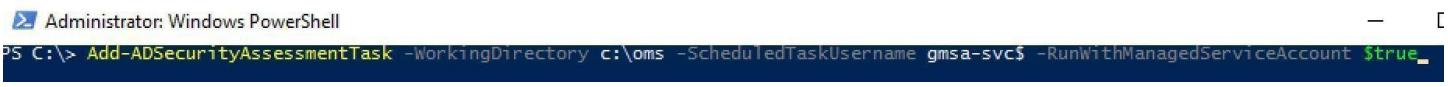
1) Follow the instructions in the provisioning KB article.
2) Authorize the account with the necessary environmental access per the Environment Permissions section in this document.

On the designated data collection machine, complete the following:

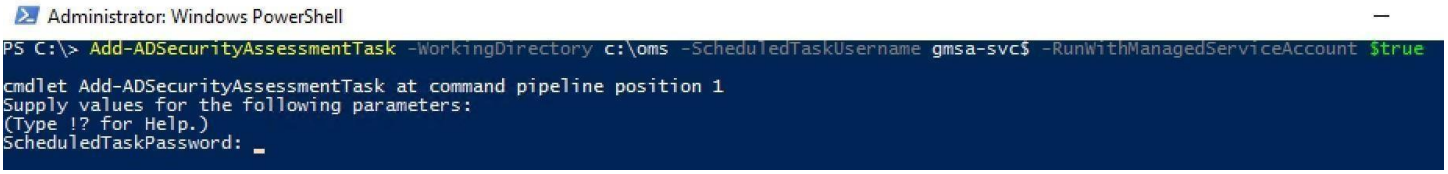
1. Open the Windows PowerShell command prompt as an Administrator

2. Run the **Add-ADSecurityAssessmentTask -WorkingDirectory <Directory> -ScheduledTaskUsername <MSAname> -RunWithManagedServiceAccount $True** 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 and <MSAname> is the SAM account name (ending with a $ sign) of the provisioned and authorized managed service account.

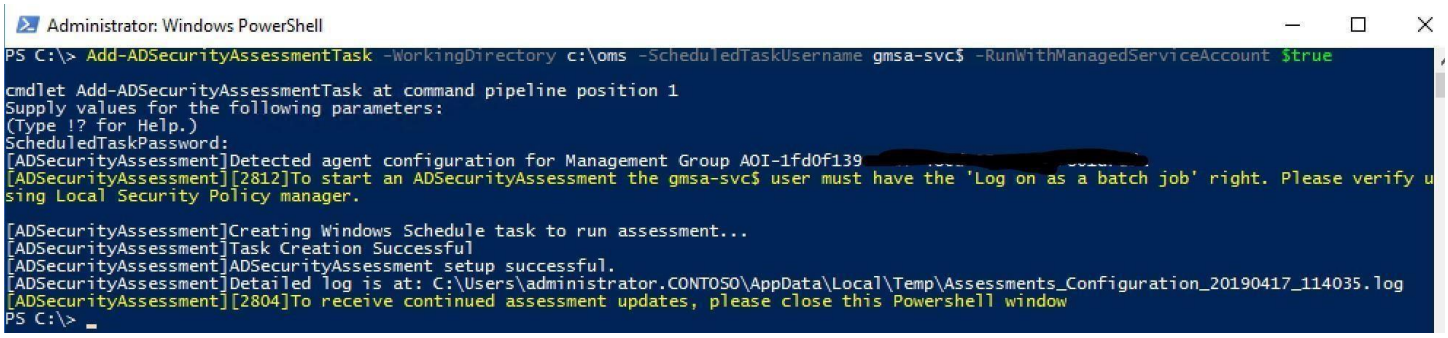
   Note. If the command **Add-ADSecurityAssessmentTask** is not available, the module is not yet found. It can take some time after installing the agent before it to show up.



3. The Add-ADSecurityAssessmentTask will prompt for the MSA password. The input accepted this prompt can be anything or nothing since managed service account credential management is handled through Active Directory or the authorized computer.



4. The script will continue with the necessary configuration. It will create a scheduled task that will trigger the data collection.



Note: *Managed Service Accounts are not officially supported by Microsoft customer service for some environmental configurations. While they work in most scenarios, it may be necessary to use a domain account when environmental configurations prevent Managed Service Account usage.*

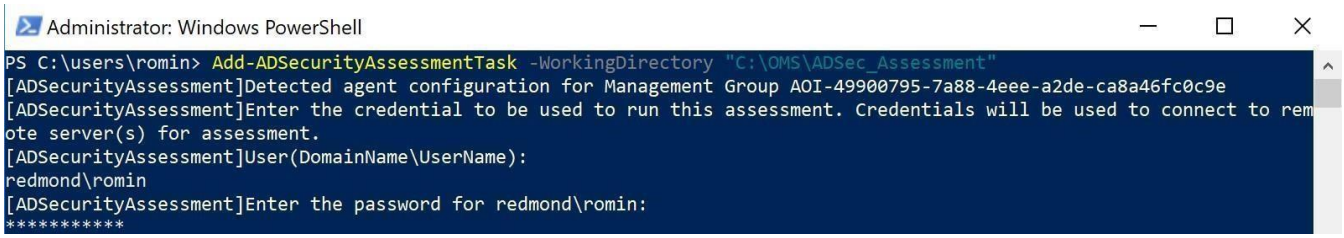
Configure with User Account

On the designated data collection machine, complete the following:

5. Open the Windows PowerShell command prompt as an Administrator

6. 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.

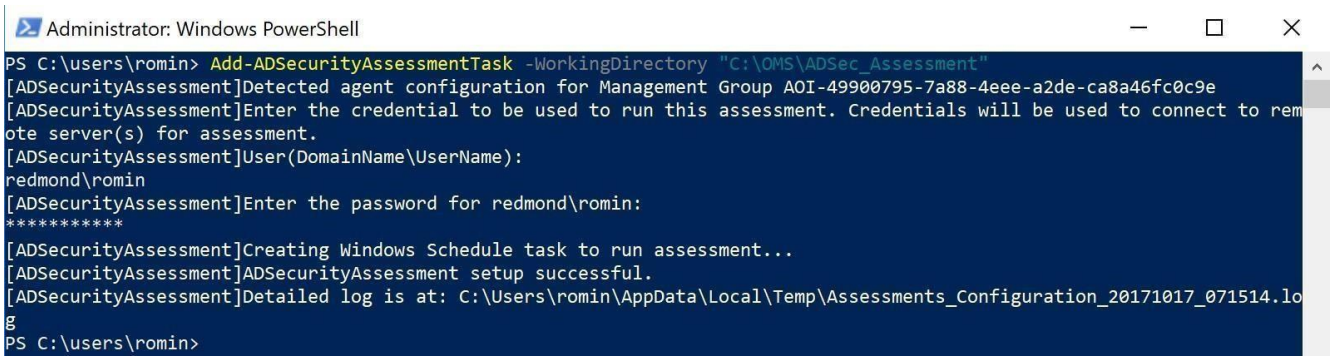
7. Provide the required user account credentials. These credentials are used to run the Active Directory Security Assessment.



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

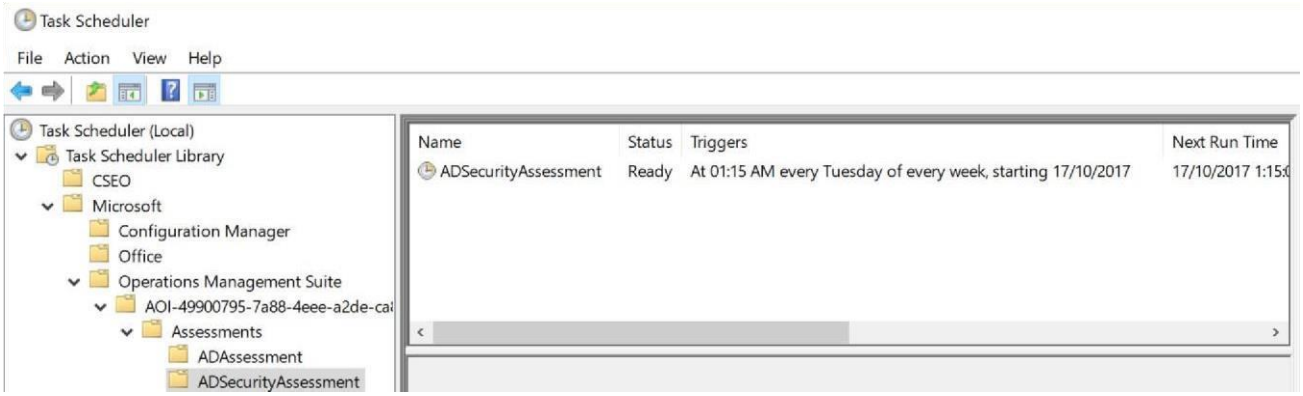
- An Enterprise Administrator account with admin access to every domain controller in the forest.
    - By default, the Enterprise Admins group is member of the built-in Administrators group in every domain. Ensure that this membership has not been changed. If the Enterprise Admins group is not member 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.

8. The script will continue with the necessary configuration. It will create a scheduled task that will trigger the data collection.



Scheduled Task Details

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.



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 2012 or Windows Server 2019.

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**

   The assessment leverages the System.DirectoryServices.ActiveDirectory .NET Framework Namespace and uses several methods to determine and collect architectural information about the directory service.

4. **Windows PowerShell**

   Collects various information, such as:

   - ACL information on organizational unit objects in Active Directory
   - Auditing Policy Configuration
   - Installed Security Updates
   - Scheduled Tasks

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.