

Active Directory Assessment: Prerequisites and Configuration



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

There are configuration and setup tasks to be completed prior to executing the assessment setup tasks in this document. For all pre-work, follow the [Getting Started with On-Demand Assessments](#) in the Services Hub Resource Center.

Table of Contents

System Requirements and Configuration at Glance.....	2
Supported Target Operating System Versions.....	2
Environment Permissions.....	2
Data Collection Machine.....	2
PowerShell Remoting.....	2
Setting up the Active Directory Assessment	6
Configure with Managed Service Account.....	6
Configure with User Account	7
Scheduled Task Details	9
Appendix - Data Collection Methods.....	10

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.
 - If there are more than 1 million users in Active Directory, add 4GB RAM for each million user objects.
- 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.
- **PowerShell 5.1** or newer.
 - Verify that the installed version of PowerShell is at least 5.1 (type **\$PsVersionTable** in a PowerShell window) and that the PSVersion is equal to or greater than 5.1.
- The data collection machine must have the Microsoft Monitoring Agent installed and configured for one of the deployment scenarios at the beginning of this document.

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

Additional requirements for Windows Server 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: *Starting with Windows Server 2012 R2, WinRM and PowerShell remoting are 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 Windows Server 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)
 - 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 allows 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
```

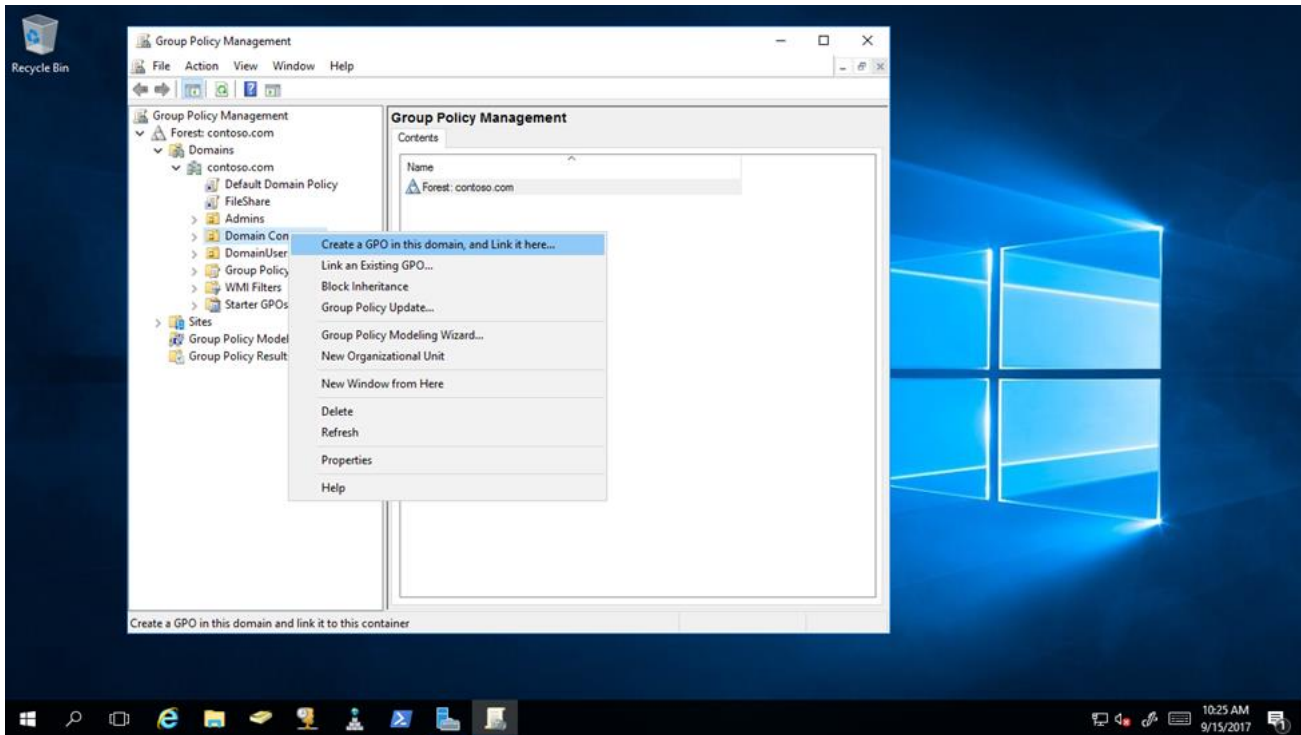
```
Subnet Mask . . . . . : X.X.X.X
```

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

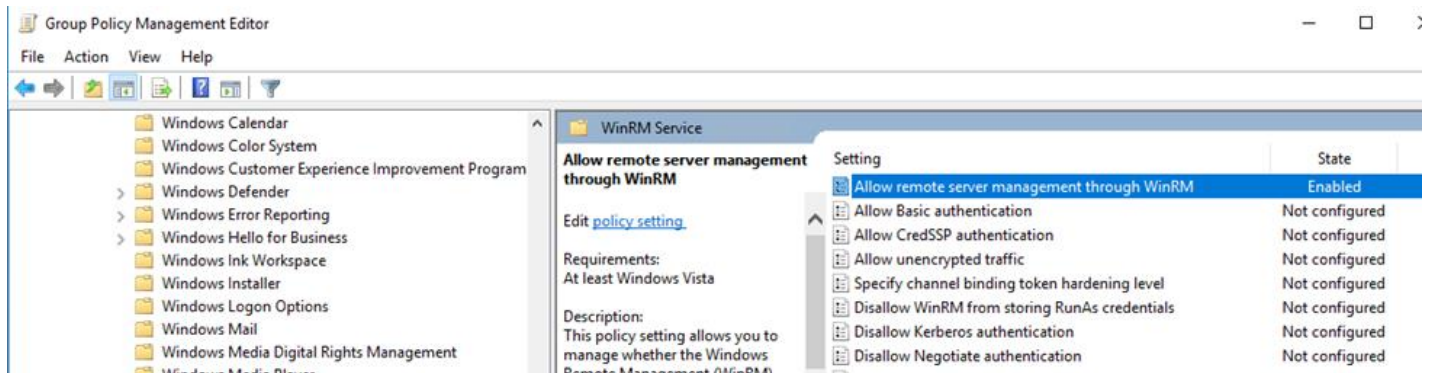
Make a note of the IPv4 address of your machine. The final step in the configuration will use this address to ensure only the data collection machine can communicate with the Windows Update Agent on the domain controllers.

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

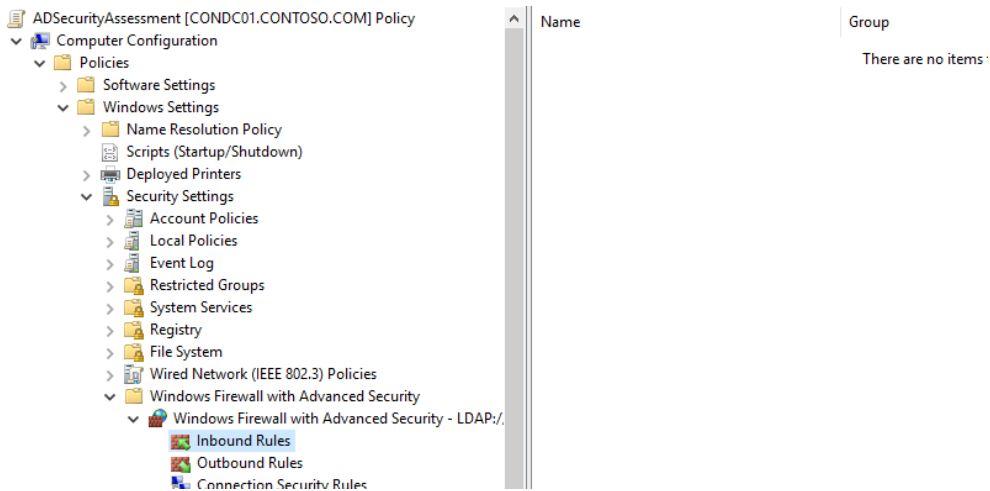
1. Create a new GPO. Make sure the GPO applies to the Domain Controllers organizational unit. Give the new group policy a name based on your group policy naming convention or something that identifies its purpose similar to “AD Security Assessment”



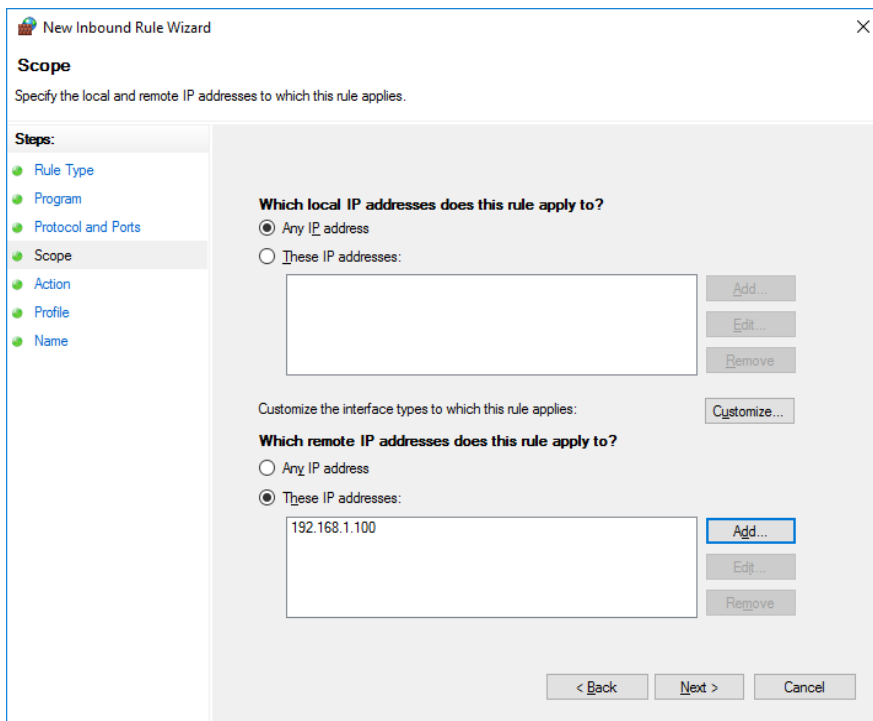
2. Within the GPO open: (Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service). Enable “**Allow remote server management through WinRM**” or “**Allow automatic configuration of listeners**” depending on your OS.



3. Create an advanced Inbound Firewall Rule to allow all network traffic between the data collection machine and the Domain Controllers. This can be 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 Assessment

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

Note: During the setup task you have the option to add an "environment" friendly name. This is the name by which the assessed environment is identified when you review your results. If you do not set it, the environment name will be the "**Forest FQDN**", i.e. contoso.com. Use the "-environment" option in the setup command when you want to use a more friendly name.

Options that are available to you during setup are:

- **EnvironmentName**
 - Add a friendly name for your environment (by default forest FQDN) which can be used in the environment filter when you review your results.
- **AssessmentID**
 - A GUID that identifies this assessed environment. If you omit it, we generate one for you.
- **ManagementGroup**
 - Include the name of the ManagementGroup to which the Microsoft Monitoring Agent has been linked.

You will not be prompted for the above options, if you do not set them default settings are used.

The minimum required input parameters for Active Directory are:

- WorkingDirectory
- Scheduledtaskusername - after which you are prompted for the password.

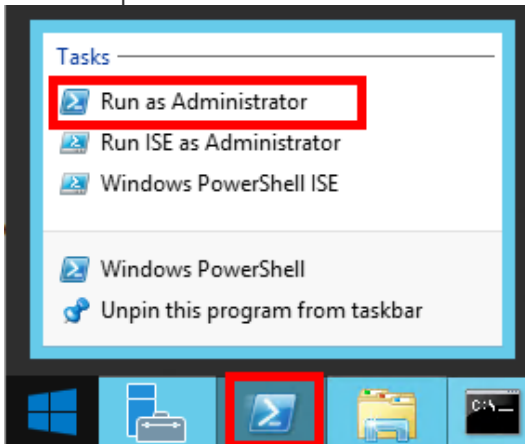
Configure with Managed Service Account

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

Select Administrator: Windows PowerShell

```
PS C:\> Add-ADAssessmentTask -WorkingDirectory c:\oms -ScheduledTaskUsername gmsa-svc$ -RunWithManagedServiceAccount $true
```

3. The Add-ADAssessmentTask 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.

Administrator: Windows PowerShell

```
PS C:\> Add-ADAssessmentTask -WorkingDirectory c:\oms -ScheduledTaskUsername gmsa-svc$ -RunWithManagedServiceAccount $true  
  
cmdlet Add-ADAssessmentTask at command pipeline position 1  
Supply values for the following parameters:  
(Type !? for Help.)  
ScheduledTaskPassword: _
```

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

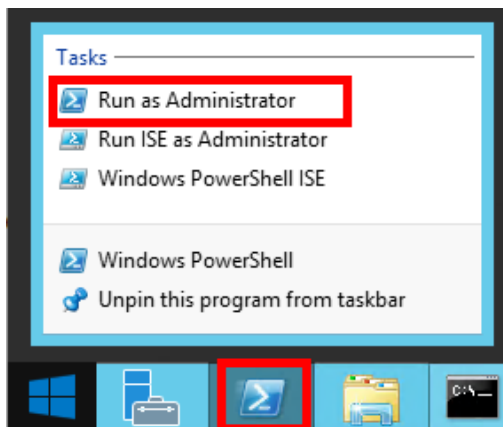
Administrator: Windows PowerShell

```
PS C:\> Add-ADAssessmentTask -WorkingDirectory c:\oms -ScheduledTaskUsername gmsa-svc$ -RunWithManagedServiceAccount $true  
  
cmdlet Add-ADAssessmentTask at command pipeline position 1  
Supply values for the following parameters:  
(Type !? for Help.)  
ScheduledTaskPassword:  
[ADAssessment]Detected agent configuration for Management Group AOI-1fd0f139-7cda  
[ADAssessment][2812]To start an ADAssessment the gmsa-svc$ user must have the 'Log on as a batch job' right. Please verify using Local Security Policy manager.  
[ADAssessment]Creating Windows Schedule task to run assessment...  
[ADAssessment]Task Creation Successful  
[ADAssessment]ADAssessment setup successful.  
[ADAssessment]Detailed log is at: C:\Users\administrator.CONTOSO\AppData\Local\Temp\Assessments_Configuration_20190417_072851.log  
[ADAssessment][2804]To receive continued assessment updates, please close this Powershell window  
PS C:\>
```

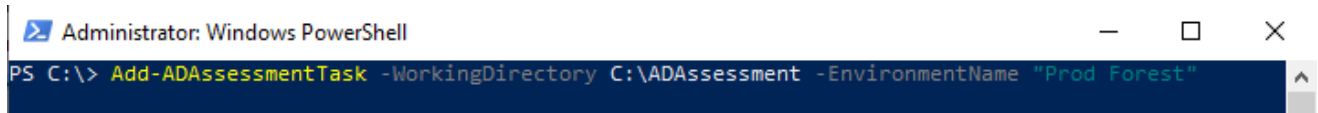
Configure with User Account

On the designated data collection machine, complete the following:

5. Open the Windows PowerShell command prompt as an Administrator

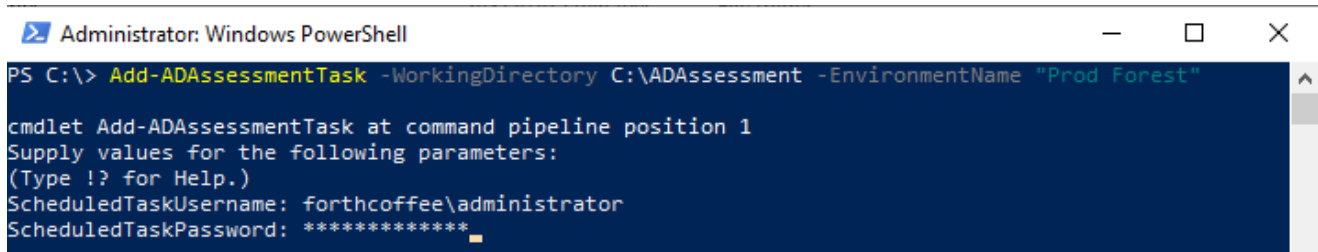


- Run the **Add-ADAssessmentTask -WorkingDirectory <Directory>** command, where *<Directory>* is the path to an existing directory used to store the files created while collecting and analyzing the data from the environment. **Note.** If the command **Add-ADAssessmentTask** is not available, the module is not yet found. It can take some time after installing the agent before it to show up.



```
Administrator: Windows PowerShell
PS C:\> Add-ADAssessmentTask -WorkingDirectory C:\ADAssessment -EnvironmentName "Prod Forest"
```

- Provide the required user account credentials. These credentials are used to run the Active Directory Assessment. If you provide a wrong password it will fail to create the scheduled task. You will see red text indicating **taskCredential**.



```
Administrator: Windows PowerShell
PS C:\> Add-ADAssessmentTask -WorkingDirectory C:\ADAssessment -EnvironmentName "Prod Forest"

cmdlet Add-ADAssessmentTask at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
ScheduledTaskUsername: forthcoffee\administrator
ScheduledTaskPassword: *****
```

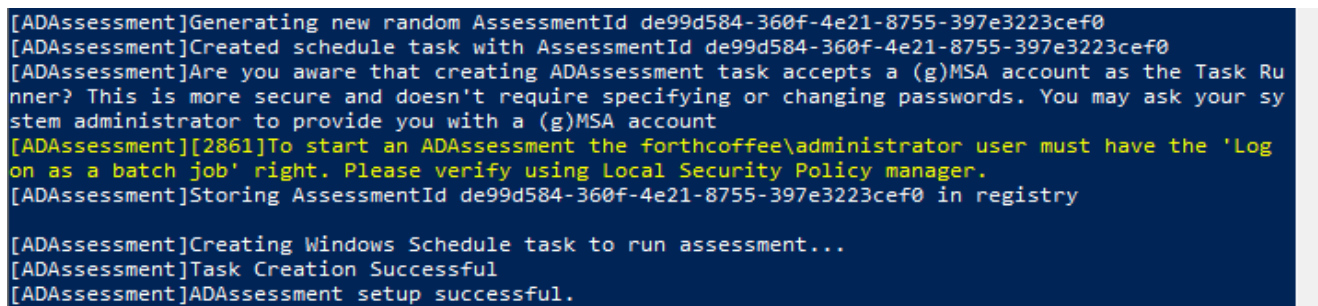
- If multiple Management Groups or Workspaces are found, for instance when the Agent also is connected to SCOM, it will prompt to select the Management Group/Workspace to be used with ADAssessment. Enter the number. In this example "1"



```
Administrator: Windows PowerShell
PS C:\> Add-ADAssessmentTask -WorkingDirectory C:\ADAssessment -EnvironmentName "Prod Forest"

cmdlet Add-ADAssessmentTask at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
ScheduledTaskUsername: forthcoffee\administrator
ScheduledTaskPassword: *****
[ADAssessment]Agent is connected to multiple Management Group(s)/Workspace(s).
[ADAssessment]1.AOI-0291a062-aaa4-47e7-81be-bf205e207996
[ADAssessment]2.AOI-22e4c571-be11-4242-8f0b-5fe40b265433
[ADAssessment]Select the Management Group/Workspace to be used with ADAssessment. (Enter the number
corresponding to list item):
1
```

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

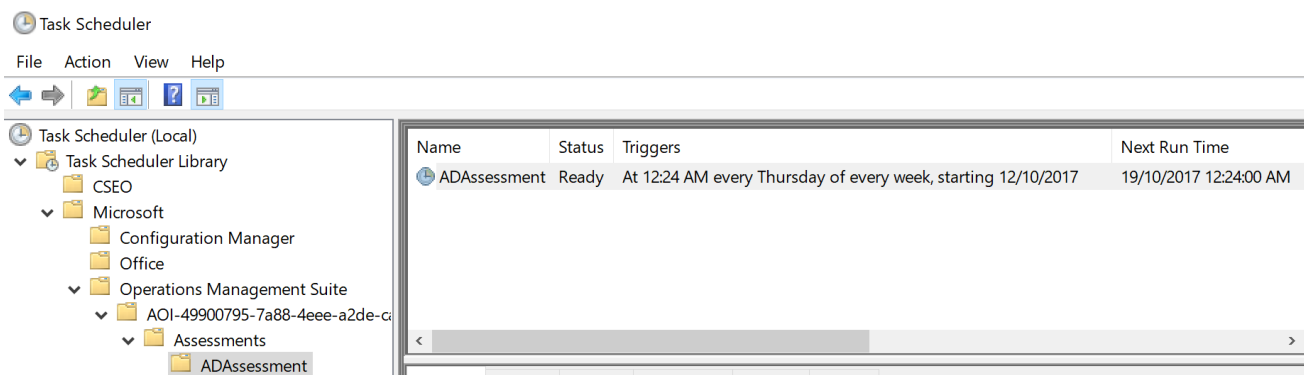


```
[ADAssessment]Generating new random AssessmentId de99d584-360f-4e21-8755-397e3223cef0
[ADAssessment]Created schedule task with AssessmentId de99d584-360f-4e21-8755-397e3223cef0
[ADAssessment]Are you aware that creating ADAssessment task accepts a (g)MSA account as the Task Runner? This is more secure and doesn't require specifying or changing passwords. You may ask your system administrator to provide you with a (g)MSA account
[ADAssessment][2861]To start an ADAssessment the forthcoffee\administrator user must have the 'Log on as a batch job' right. Please verify using Local Security Policy manager.
[ADAssessment]Storing AssessmentId de99d584-360f-4e21-8755-397e3223cef0 in registry

[ADAssessment]Creating Windows Schedule task to run assessment...
[ADAssessment]Task Creation Successful
[ADAssessment]ADAssessment setup successful.
```


Scheduled Task Details

Data collection is triggered by the **scheduled task** named **ADAssessment** 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.



For guidance and details on working with assessment results, visit [Working with Assessment Results](#) in the Services Hub Resource Center.

Appendix - Data Collection Methods

The **AD 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 your environment. No Microsoft Visual Basic (VB) scripts are used to collect data.

1. Registry Collectors
2. LDAP Collectors
3. .NET Framework
4. Event Log Collectors
5. Active Directory Service Interfaces (ADSI)
6. Windows PowerShell
7. File Data Collectors
8. Windows Management Instrumentation (WMI)
9. DCDIAGAPI
10. NTFRSAPI
11. 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 you to determine where the Active Directory database and log files are located on each domain controller and get detailed information on each service relevant to the proper function of Active Directory. Microsoft does not collect information for all services, only the ones relevant to Active Directory.

- Operating System information from HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion

This allows you to determine operation system information such as Windows Server 2016 or Windows Server 2019.

2. LDAP Collectors

LDAP queries are used to collect data for the domain, domain controllers, nTDSiteSettings objects, partitions, 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 uses the [System.DirectoryServices.ActiveDirectory](#) .NET Framework Namespace and uses the following methods:

- [GetReplicationNeighbors](#) is called to retrieve the replication status details.
- [Domain.GetAllTrustRelationships](#)— to get a collection of the trust relationships in each domain.
- [Forest.GetAllTrustRelationships](#)— collection of the trust relationships of the forest.

4. Event Log Collectors

Collects event logs from domain controllers. Microsoft collects the last 7 days of Warnings and Errors from the application, Distributed File System Replication (DFSR), DNS, File Replication Service (FRS), and System event logs. Only for the Directory Services event log, we also collect informational events to detect the amount of white space in the database if whitespace logging has been enabled.

5. ADSI

Using the domain ObjectClass, we use [ADSI](#) to get the domain password information for each domain in the forest. The domain password information consists of the domain's minimum password age, maximum password age, minimum password length, and other settings stored in the default domain policy.

6. Windows PowerShell

Used to collect WMI information for installed updates and hotfixes on domain controllers.

7. File Data Collectors

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

8. WMI

[WMI](#) is used to collect various information such as:

- WIN32_Volume

Collects information on volume settings for each domain controller in the forest. For example, the information is used to determine the system volume and drive letter, which allows the assessment 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 on 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.

9. DCDIAGAPI

Collects diagnostics information from DCs. DCDIAG analyzes the state for all DCs in the forest and reports any problems it detects.

10. NTFRSAPI

FRS can be used to replicate the SYSVOL and Netlogon folder contents. The NTFRSapi is used to dump the internal tables, thread and memory information for the NT File Replication Service (NTFRS) for DCs. It provides insight on the health of the FRS.

11. Custom C# Code

Collects information not captured using other collectors.