Microsoft

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 Microsoft Unified Support Solution Pack.

There are **two scenarios** available to configure the assessment. Determine which scenario fits best for your organization.

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 privileged account credentials which are used on the scheduled task configured on this 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.

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.

This document was last updated on June 05, 2018. To ensure you have the latest version of this document, check here: https://go.microsoft.com/fwlink/?linkid=860104

Table of Contents

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

- Your Active Directory domain controllers must run Windows Server 2016 or later.

Common to Both Scenarios

- You will need a **log analytics workspace**
- **User account rights:**
    - A domain 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.
        - Log on as a batch job privileges on the data collection machine.

Data Collection Machine

- **Microsoft Monitoring Agent** requires computers running Windows Server 2008 SP1 or later (or Windows 7 SP1 or later – **Important**: The option of installing the Microsoft Monitoring Agent on client operating systems is strongly discouraged due to the risk of exposing privileged domain account credentials to lower trust workstations.
- 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.
- 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 4.0 or newer installed.
- The **data collection machine** 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.
- For the **Microsoft Monitoring Agent** to connect to and register with the log analytics service, it must have 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/.

OMS Gateway (required in the **OMS Gateway and data collection machine** scenario)

- The **OMS Gateway** can be a standalone or a member server. It requires Windows 10, Windows 7, Windows 8.1, Windows Server 2016.
- 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 services:** When the Windows Firewall service is disabled the installation of the OMS Gateway fails.
- **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

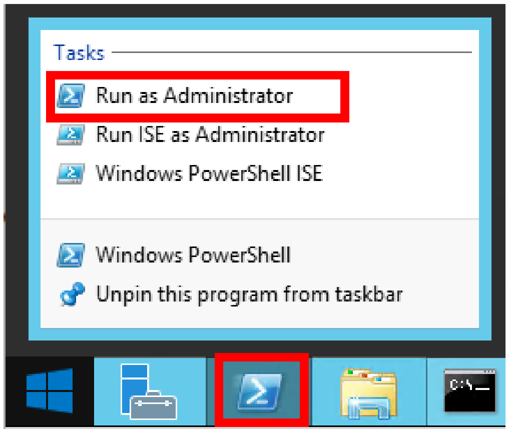
After you have finished the installation of the Microsoft Monitoring Agent/OMS Gateway, continue with the next section to set up the assessment.

Setting up the Active Directory Assessment

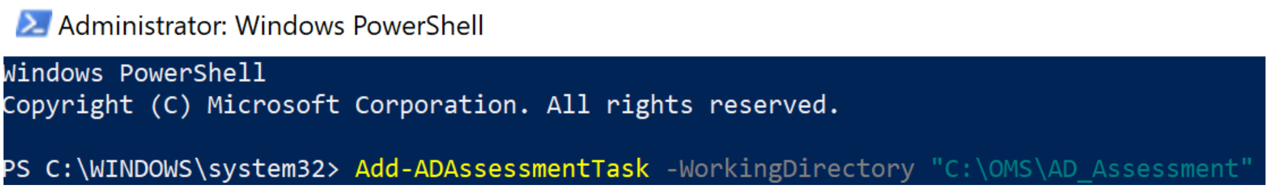
When you have finished the installation of the Microsoft Management Agent/OMS Gateway, you are ready to setup the Active Directory Assessment.

On the designated data collection machine, complete the following:

1. Open the Windows PowerShell command prompt as an Administrator



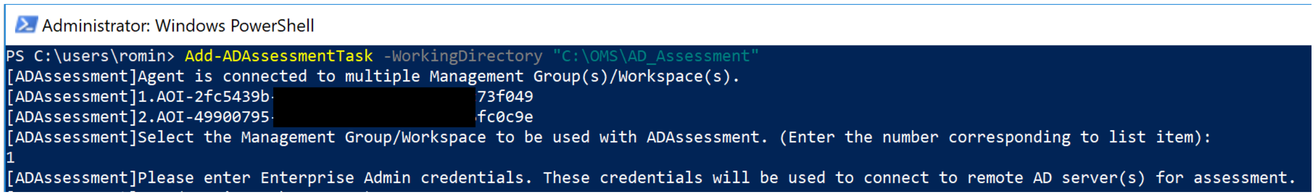
2. Run the **Add-ADAssessmentTask -WorkingDirectory <Directory>** command, where <*Directory*> is the path to an existing directory used to store the files created while collecting and analyzing the data from the environment. **Note.** If the command **Add-ADAssessmentTask** is not available, the module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



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> Add-ADAssessmentTask -WorkingDirectory "C:\OMS\AD_Assessment"
```

3. 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

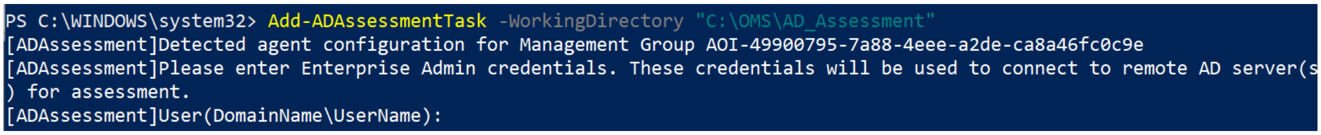
number. In this example “1”



Administrator: Windows PowerShell

```
PS C:\users\romin> Add-ADAssessmentTask -WorkingDirectory "C:\OMS\AD_Assessment"
[ADAssessment]Agent is connected to multiple Management Group(s)/Workspace(s).
[ADAssessment]1.AOI-2fc5439b-[redacted]73f049
[ADAssessment]2.AOI-49900795-[redacted]fc0c9e
[ADAssessment]Select the Management Group/Workspace to be used with ADAssessment. (Enter the number corresponding to list item):
1
[ADAssessment]Please enter Enterprise Admin credentials. These credentials will be used to connect to remote AD server(s) for assessment.
```

4. Provide the required user account credentials. These credentials are used to run the Active Directory Assessment. If you provide a wrong password it will continue to prompt for Enterprise Account and Credentials until it is correctly entered.

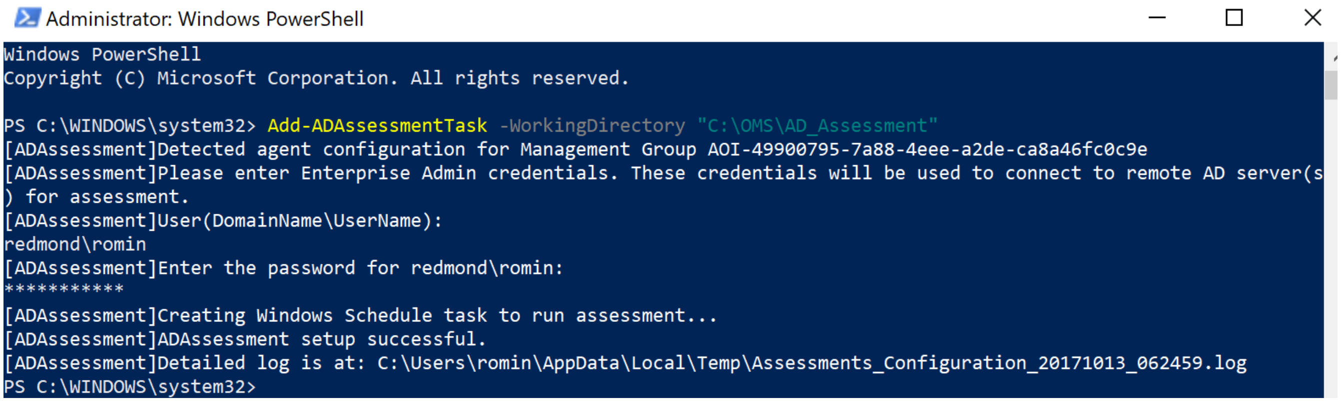


```
PS C:\WINDOWS\system32> Add-ADAssessmentTask -WorkingDirectory "C:\OMS\AD_Assessment"
[ADAssessment]Detected agent configuration for Management Group AOI-49900795-7a88-4eee-a2de-ca8a46fc0c9e
[ADAssessment]Please enter Enterprise Admin credentials. These credentials will be used to connect to remote AD server(s
) for assessment.
[ADAssessment]User(DomainName\UserName):
```

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 Assessment runs to the built-in Administrators group of that domain.
- Unrestricted network access to every domain controller in the forest.
- Log on as a batch job privileges.

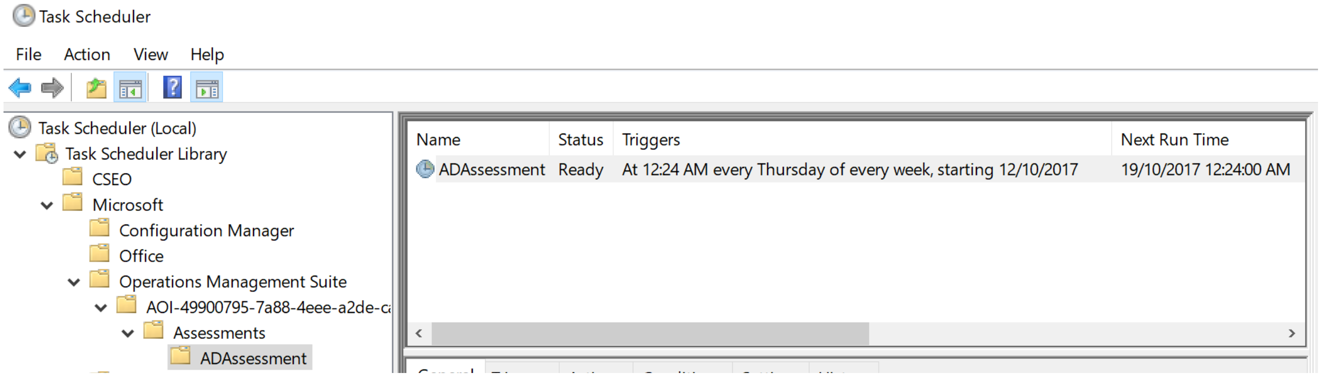
5. The script will continue with the necessary configuration. It will create a scheduled task that will trigger the data collection.



Administrator: Windows PowerShell

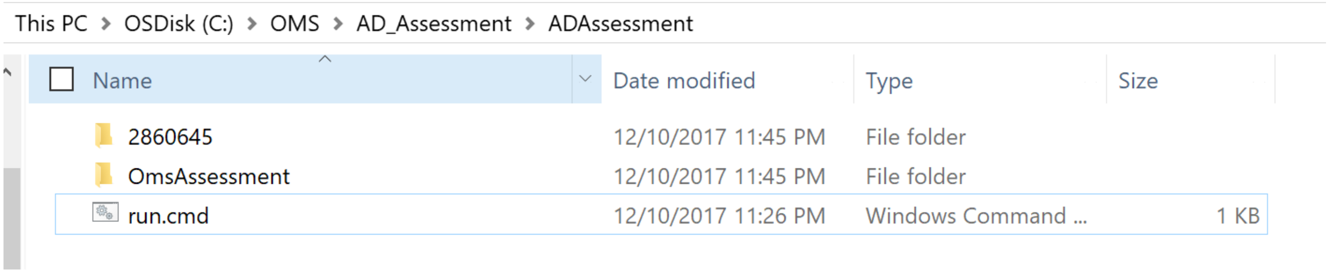
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> Add-ADAssessmentTask -WorkingDirectory "C:\OMS\AD_Assessment"
[ADAssessment]Detected agent configuration for Management Group AOI-49900795-7a88-4eee-a2de-ca8a46fc0c9e
[ADAssessment]Please enter Enterprise Admin credentials. These credentials will be used to connect to remote AD server(s
) for assessment.
[ADAssessment]User(DomainName\UserName):
redmond\romin
[ADAssessment]Enter the password for redmond\romin:
***********
[ADAssessment]Creating Windows Schedule task to run assessment...
[ADAssessment]ADAssessment setup successful.
[ADAssessment]Detailed log is at: C:\Users\romin\AppData\Local\Temp\Assessments_Configuration_20171013_062459.log
PS C:\WINDOWS\system32>
```

6. 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.



Name	Status	Triggers	Next Run Time
ADAssessment	Ready	At 12:24 AM every Thursday of every week, starting 12/10/2017	19/10/2017 12:24:00 AM

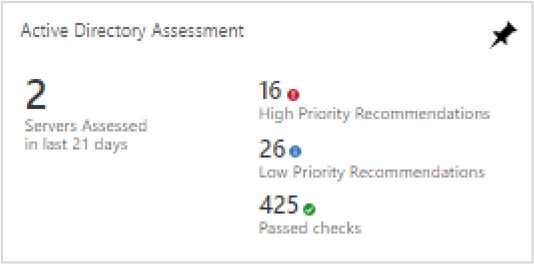
7. During collection and analysis, data is temporarily stored under the **WorkingDirectory** folder that was configured during setup, using the following structure:



Name	Date modified	Type	Size
2860645	12/10/2017 11:45 PM	File folder	
OmsAssessment	12/10/2017 11:45 PM	File folder	
run.cmd	12/10/2017 11:26 PM	Windows Command ...	1 KB

8. 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, which will then submit the data to your log analytics workspace.

9. After a few hours, your assessment results will be available on your log analytics dashboard. Click the **AD Assessment** tile to review:


Active Directory Assessment

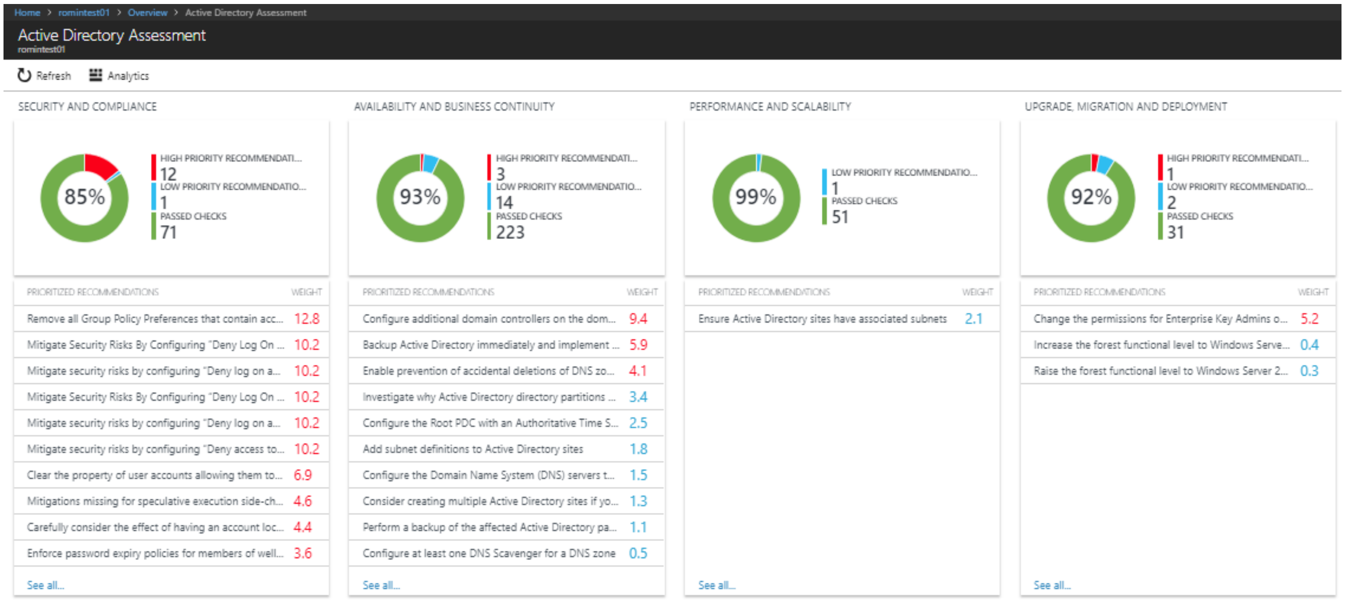
2
Servers Assessed
in last 21 days

16 ●
High Priority Recommendations

26 ●
Low Priority Recommendations

425 ●
Passed checks

10. You will then be presented with findings grouped by the focus area.



Home > romintest01 > Overview > Active Directory Assessment

Active Directory Assessment
romintest01

Refresh   Analytics

SECURITY AND COMPLIANCE

85%

HIGH PRIORITY RECOMMENDATI... 12
LOW PRIORITY RECOMMENDATIO... 1
PASSED CHECKS 71

PRIORITIZED RECOMMENDATIONS	WEIGHT
Remove all Group Policy Preferences that contain acc...	12.8
Mitigate Security Risks By Configuring "Deny Log On ...	10.2
Mitigate security risks by configuring "Deny log on a...	10.2
Mitigate Security Risks By Configuring "Deny Log On ...	10.2
Mitigate security risks by configuring "Deny log on a...	10.2
Mitigate security risks by configuring "Deny access to...	10.2
Clear the property of user accounts allowing them to...	6.9
Mitigations missing for speculative execution side-ch...	4.6
Carefully consider the effect of having an account loc...	4.4
Enforce password expiry policies for members of well...	3.6

See all...

AVAILABILITY AND BUSINESS CONTINUITY

93%

HIGH PRIORITY RECOMMENDATI... 3
LOW PRIORITY RECOMMENDATIO... 14
PASSED CHECKS 223

PRIORITIZED RECOMMENDATIONS	WEIGHT
Configure additional domain controllers on the dom...	9.4
Backup Active Directory immediately and implement ...	5.9
Enable prevention of accidental deletions of DNS zo...	4.1
Investigate why Active Directory directory partitions ...	3.4
Configure the Root PDC with an Authoritative Time S...	2.5
Add subnet definitions to Active Directory sites	1.8
Configure the Domain Name System (DNS) servers t...	1.5
Consider creating multiple Active Directory sites if yo...	1.3
Perform a backup of the affected Active Directory pa...	1.1
Configure at least one DNS Scavenger for a DNS zone	0.5

See all...

PERFORMANCE AND SCALABILITY

99%

LOW PRIORITY RECOMMENDATIO... 1
PASSED CHECKS 51

PRIORITIZED RECOMMENDATIONS	WEIGHT
Ensure Active Directory sites have associated subnets	2.1

See all...

UPGRADE, MIGRATION AND DEPLOYMENT

92%

HIGH PRIORITY RECOMMENDATI... 1
LOW PRIORITY RECOMMENDATIO... 2
PASSED CHECKS 31

PRIORITIZED RECOMMENDATIONS	WEIGHT
Change the permissions for Enterprise Key Admins o...	5.2
Increase the forest functional level to Windows Serve...	0.4
Raise the forest functional level to Windows Server 2...	0.3

See all...

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 2008 or Windows Server 2012.

2. **LDAP Collectors**

LDAP queries are used to collect data for the domain, domain controllers, nTDSSiteSettings 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.