



Exchange Server Assessment: Prerequisites and Configuration

This document explains the required steps to configure the Exchange Server Assessment included with your Microsoft Azure Log Analytics Workspace and Microsoft Unified Support Solution Pack.

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 Versions.....	2
Environment Permissions.....	2
Data Collection Machine.....	2
Setting up the Exchange Server Assessment.....	3
Appendix.....	5
Data Collection Methods.....	5

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 Exchange Servers must run Exchange Server 2010, Exchange Server 2013, Exchange Server 2016, or Exchange Server 2019.

Environment Permissions

- **User account rights:**
 - A domain account with the following rights:
 - Exchange View Only Administrator permissions to the Exchange organization
 - Administrative access to every Exchange Server in the Organization.
 - Public Folder Administrator permissions to the Exchange organization
 - NOTE:** Not required where the domain account is a Domain Administrator or an Exchange Full Administrator
 - 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** requires computers running Windows Server 2012 or later (or Windows 8.1 or later – **Important:** Windows 10 and Windows Management Framework 5 (PowerShell 5) are not currently supported).
- 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 Exchange Servers in the organization and retrieve information from them. The machine is communicating over Remote Procedure Call (RPC), Server Message Block (SMB), PowerShell, WMI, remote registry, Lightweight Directory Access Protocol (LDAP) and Distributed Component Object Model (DCOM). The data collection machine requires unrestricted access to every Exchange Server in the organization.
- Microsoft .NET Framework 4.6.2 or newer installed.
- The CLR version on the data collection machine should be using .NET 4.0 or greater. This can be verified by running `$PSVersionTable.CLRVersion` in the PowerShell prompt
- AD Module for PowerShell needs to be installed (RSAT-AD-PowerShell).
- The **data collection machine** must have the Microsoft Monitoring Agent installed and 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 or via the OMS gateway

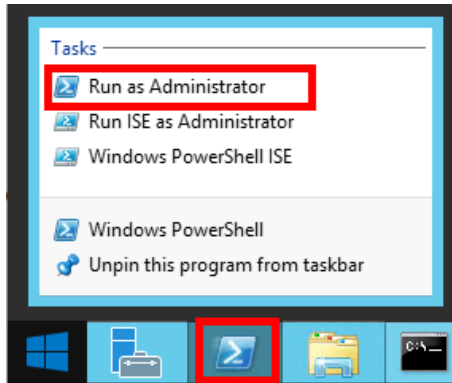
Setting up the Exchange Server Assessment

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

Follow the steps below to setup the Exchange Server Assessment.

On the designated data collection machine, complete the following:

1. Open the Windows PowerShell command prompt as an Administrator



2. Run the **Add-ExchangeAssessmentTask – 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.

```
Administrator: Windows PowerShell
PS C:\users\romin> Add-ExchangeAssessmentTask -WorkingDirectory "C:\OMS\Exchange_Assessment"
```

3. Provide the required user account credentials. These credentials are used to run the Exchange Server Assessment.

```
PS C:\users\romin> Add-ExchangeAssessmentTask -WorkingDirectory "C:\OMS\Exchange_Assessment"
[ExchangeAssessment]Detected agent configuration for Management Group AOI-49900795-7a88-4eee-a2de-ca8a46fc0c9e
[ExchangeAssessment]Enter the credential to be used to run this assessment. Credentials will be used to connect to remote server(s) for assessment.
[ExchangeAssessment]User(DomainName\UserName):
```

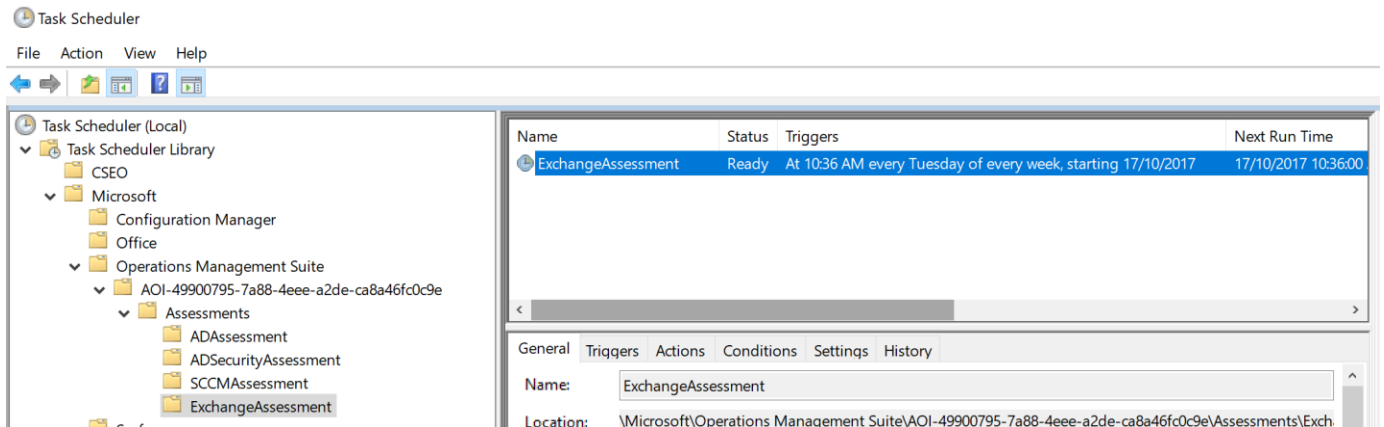
NOTE: This domain account must have all the following rights:

- A domain account with admin access to every Exchange Server in the organization.
- Unrestricted network access to every Exchange Server in the organization.

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-ExchangeAssessmentTask -WorkingDirectory "C:\OMS\Exchange_Assessment"
[ExchangeAssessment]Detected agent configuration for Management Group AOI-49900795-7a88-4eee-a2de-ca8a46fc0c9e
[ExchangeAssessment]Enter the credential to be used to run this assessment. Credentials will be used to connect to remote server(s) for assessment.
[ExchangeAssessment]User(DomainName\UserName):
redmond\romin
[ExchangeAssessment]Enter the password for redmond\romin:
*****
[ExchangeAssessment]Creating Windows Schedule task to run assessment...
[ExchangeAssessment]ExchangeAssessment setup successful.
[ExchangeAssessment]Detailed log is at: C:\Users\romin\AppData\Local\Temp\Assessments_Configuration_20171017_043648.log
```

5. Data collection is triggered by the **scheduled task** named **ExchangeAssessment** within an hour of running the previous script and then every 7 days. The task can be modified to run on a different day/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 **Exchange Server 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. EventLogCollector
5. Windows PowerShell
6. FileDataCollector
7. WMI
8. Custom C# Code
9. System Performance Data

1. Registry Collectors

Registry keys and values are read from the data collection machine and all Exchange Servers. They include items such as:

- Service information from HKLM\SYSTEM\CurrentControlSet\Services.

This allows the assessment to determine where the AD Database and log files are located on each server and get detailed information on each service relevant to the proper function of AD. We do not collect all services, only the ones relevant to AD.

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

This allows the assessment to determine Operation System information such as Windows Server 2012, Windows Server 2016 or Windows Server 2019.

2. LDAP Collectors

LDAP queries are used to collect data for the Domain, DCs, 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 Exchange Server Assessment leverages 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. EventLogCollector

Collects event logs from Exchange Server. We collect the last 7 days of Warnings and Errors from the Application and System event logs.

5. Windows PowerShell

PowerShell is used extensively in the Exchange Server Assessment to gather configuration data.

- For Exchange Server 2010 and above remote PowerShell is leveraged to gather Exchange Server specific information.

6. FileDataCollector

Enumerates files in a folder on a remote machine, and optionally retrieves those files. For example, the EdgeTransport.exe.config file for each Hub server is gathered so that the settings may be validated.

7. Windows Management Instrumentation (WMI)

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

◆ WIN32_Volume

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 Exchange Server 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 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.

8. Custom C# Code

Collects information not captured using other collectors.

9. System Performance Data

Utilizes the Performance Logs and Alerts service to create a data collector on each target server. By default the performance data will be written to the c:\perflogs directory on each server. Before the collection is started the required disk space is verified by the collector. Once the collection is completed the data collection configuration as well as the collected data are removed from each target server.