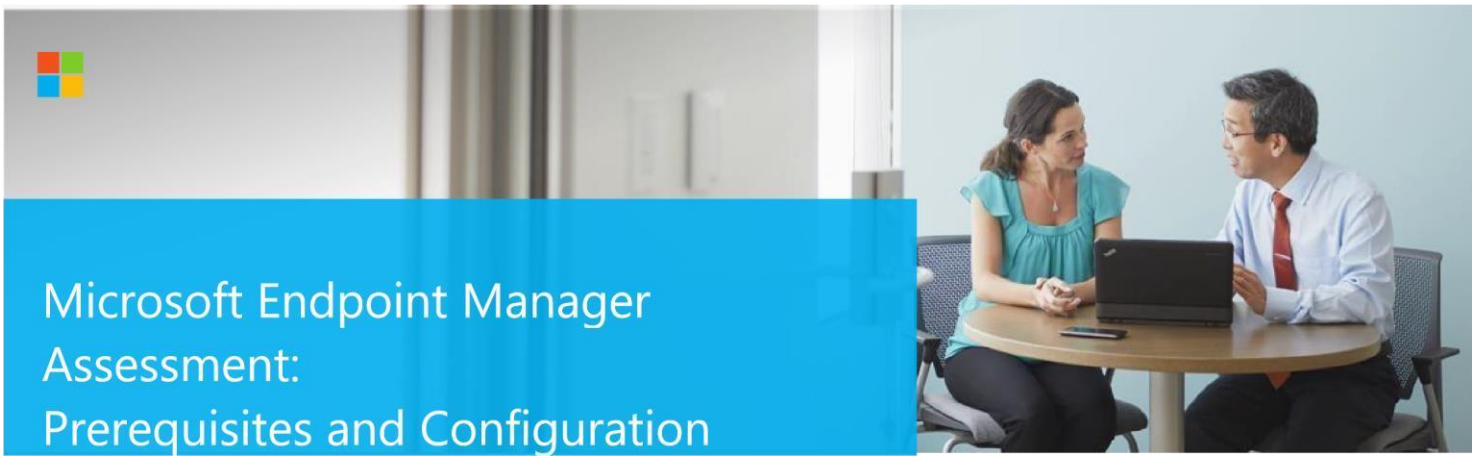


This document explains the required steps to configure the Microsoft Endpoint Manager (MEM) Assessment included with your Azure Log Analytics Workspace and entitled Microsoft On-Demand assessment.

! **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.

Table of Contents

System Requirements and Configuration at Glance....2
Supported Versions....2
Common to all Scenarios....2
Data Collection Machine....3
Setting up the MEM Assessment....3
Appendix....7
Data Collection Methods....7

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

- Supported versions of Configuration Manager with site systems running Windows Server 2012 or later.
- Configuration Manager hierarchy must be spanning across a single forest
- Management Point (MP) list must be configured on a single port to avoid MP Checks to misfire. To check this please run the below WMI:

```
(get-wmiobject -Namespace root\sms\site_<sitecode> -Query "select * from SMS_SCI_Component where ComponentName= 'SMS_MP_CONTROL_MANAGER'").Props | where-Object {$_.PropertyName -eq "IISPortsList"}
```

Common to all Scenarios

- You will need a log analytics workspace
- **User account rights:**
  - A domain account with the following rights:
    - Admin access to every server (Site System) in the Configuration Manager hierarchy. Single user account if Site Systems are in Multi-Domain Environment
    - Unrestricted network access to every server (Site System) in the Configuration Manager hierarchy
    - Administrator permissions to all SQL servers used by the Configuration Manager Sites or Software Update Points
    - Full access rights to all the Configuration Manager Site objects in all Primary Sites
    - SysAdmin permission to all SQL Instances used by Configuration Manager Sites or Software Update Points.

© 2023 Microsoft Corporation

Data Collection Machine

- The **data collection machine** must be a member server of the Active Directory domain in which the MEM Hierarchy resides that you wish to be assessed and needs to have the **MEM console installed on the data collection machine.**
- **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 your MEM Hierarchy and retrieve information from it, communicating over Remote Procedure Call (RPC), Server Message Block (SMB), WMI, remote registry, SQL Database, 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

Setting up the MEM Assessment

When you have finished the installation of the Azure Arc enrollment/Azure VM Extension, you are ready to setup the MEM 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 (outlined in steps 2 and 3 below).

On the designated data collection machine, complete the following:

1. Open the Windows PowerShell command prompt as an Administrator

© 2023 Microsoft Corporation

2. **Using a User Account:**

   Run the **Add-SCCMAssessmentTask -ServerName <YourServerName> -WorkingDirectory <DirectoryPath>** command where <YourServerName> is the FQDN or NetBIOS name of one of the Management Servers that's topmost in the hierarchy (Central or Primary Site) and <*DirectoryPath*> 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 directory does not exist, it must be created before you continue with the execution

3. **Using a 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 User Account Rights section in this document. On the designated data collection machine, complete the following in an admin powershell prompt:

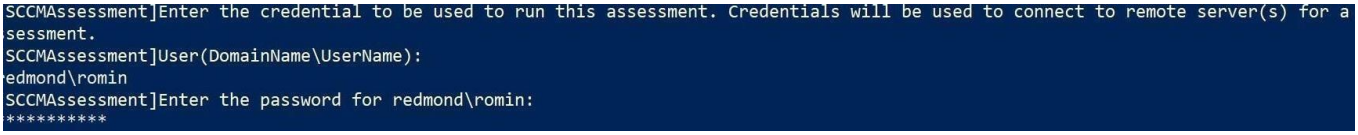
Add-SCCMAssessmentTask -ServerName <YourServerName> -WorkingDirectory <DirectoryPath>

-ScheduledTaskUsername <MSAname> -RunWithManagedServiceAccount $True

command where <YourServerName> is the FQDN or NetBIOS name of one of the Management Servers that's topmost in the hierarchy (Central or Primary Site), <*DirectoryPath*> 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.

Provide the Workspace Id for the Azure Log Analytics workspace that will be storing the data.

4. Provide the required user account credentials. These credentials are used to run the MEM Assessment.



© 2023 Microsoft Corporation

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

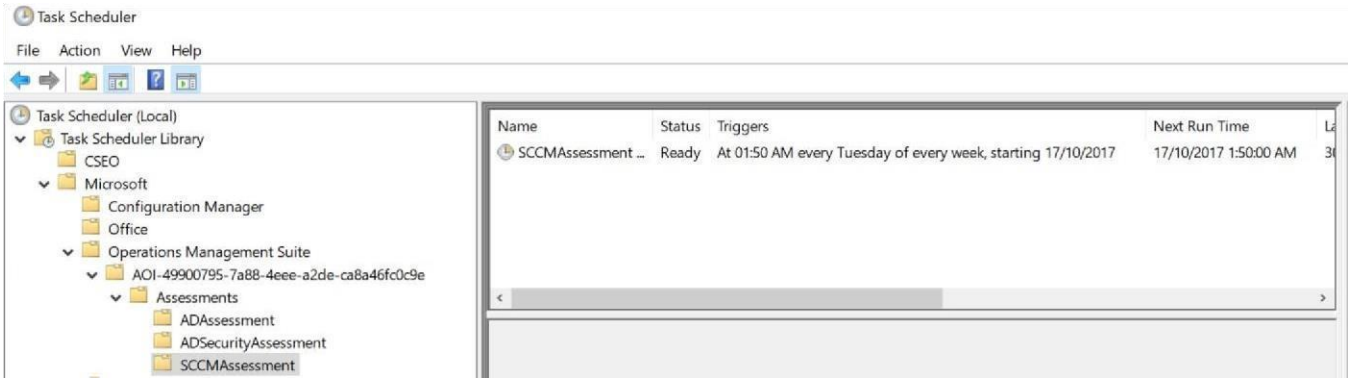
- Admin access to every server (Site System) in the Configuration Manager hierarchy. Single user account if Site Systems are in Multi-Domain Environment
- Unrestricted network access to every server (Site System) in the Configuration Manager hierarchy
- Administrator permissions to all SQL servers used by the Configuration Manager Sites or Software Update Points
- Full access rights to all the Configuration Manager Site objects in all Primary Sites
- SysAdmin permission to all SQL Instances used by Configuration Manager Sites or Software Update Points.

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

```
[SCCMAssessment]Enter the credential to be used to run this assessment. Credentials will be used to connect to remote server(s) for a
ssessment.
[SCCMAssessment]User(DomainName\UserName):
redmond\romin
[SCCMAssessment]Enter the password for redmond\romin:
**********
[SCCMAssessment]Creating Windows Schedule task to run assessment...
[SCCMAssessment]SCCMAssessment setup successful.
[SCCMAssessment]Detailed log is at: C:\Users\romin\AppData\Local\Temp\Assessments_Configuration_20171017_075011.log
PS C:\users\romin>
```

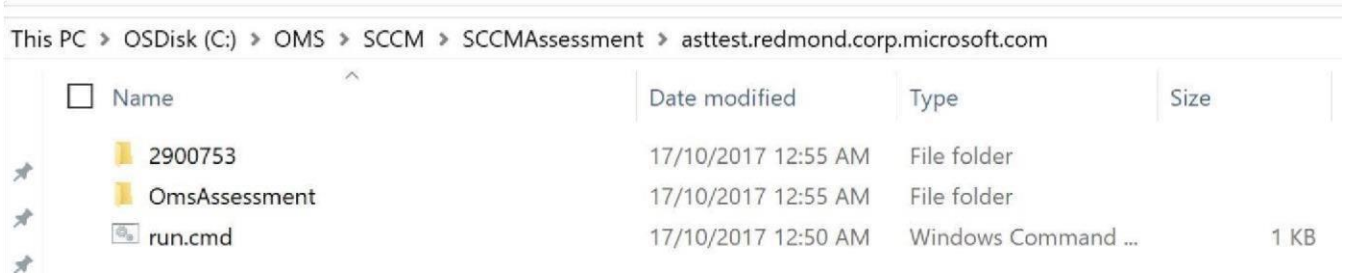
Note: *Managed Service Accounts are not officially supported by Microsoft customer service for some environmental configurations. While they work in most scenarios, it may be necessary to use a domain account when environmental configurations prevent Managed Service Account usage.*

6. Data collection is triggered by the scheduled task named “SCCMAssessment -ServerName <YourServerName>” 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.



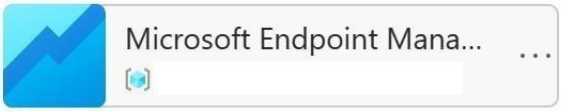
© 2023 Microsoft Corporation

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

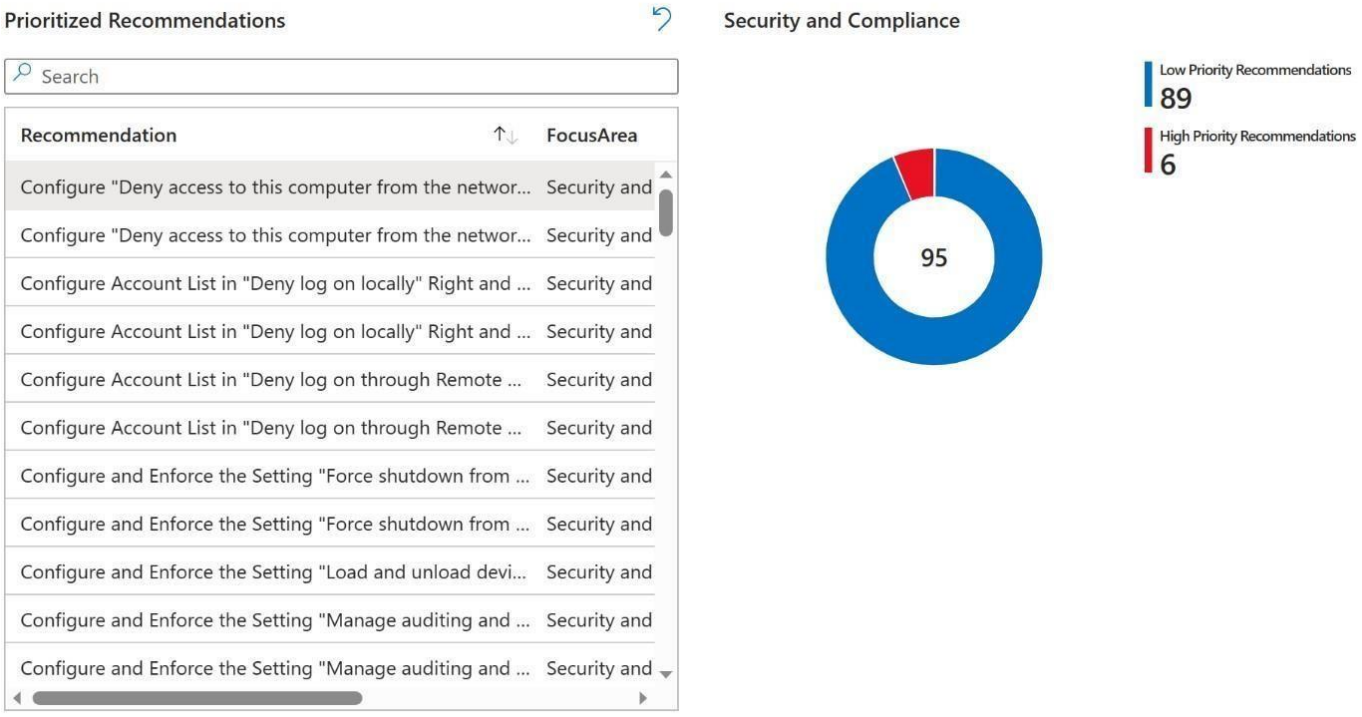


8. After data collection and analysis is completed on the tools machine, it will be submitted to your log analytics workspace, under Monitoring – **Workbooks**.

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



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



© 2023 Microsoft Corporation

Appendix

Data Collection Methods

The **MEM Assessment in the log analytics workspace** 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. Windows PowerShell
4. File Data Collectors
5. Windows Management Instrumentation (WMI)
6. SQL

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 2012 or later.

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. **Windows PowerShell**

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

4. **FileDataCollector**

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

© 2023 Microsoft Corporation

5. **Windows Management Instrumentation (WMI) Collectors** 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.

6. **SQL Data Collectors**

   SQL queries are used to collect information from Site Servers.

© 2023 Microsoft Corporation