This document explains the required steps to configure the System Center Operations Manager (SCOM) Assessment included with your Azure Log Analytics Workspace and Microsoft Unified Support Solution Pack.

! **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

This document was last updated on April 18th, 2023. To ensure you have the latest version of this document, check here:

https://go.microsoft.com/fwlink/?linkid=860144

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 System Center Operations Manager environment must run on Microsoft System Operations Manager 2012 SP1 or Microsoft System Operations Manager 2012 R2, Microsoft System Operations Manager 2016, Microsoft System Operations Manager 1801, Microsoft System Operations Manager 1807, Microsoft System Operations Manager 2019

Environment Permissions

- **Assessment account rights:**
  - A domain account with the following rights:
    - Member of the local Administrators group on all servers in the environment (All Operations Manager Roles - Management Server, OpsMgr Database, Data Warehouse, Reporting, Web Console, and Gateway).
    - Operation Manager Administrator Role for the management group being assessed.
    - SysAdmin role on all Microsoft SQL servers or instances used by Operations Manager.

Data Collection Machine

- The **data collection machine** must be a member server of the Active Directory domain in which the SCOM management group that you wish to evaluate, resides.
- **Data collection machine hardware:** Minimum 16 gigabytes (GB) of RAM, 2 gigahertz (GHz) dual-core processor, and 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 one of the management servers in your management group and retrieve information from it. The machine is 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

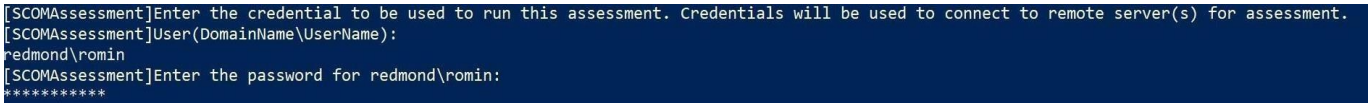
Setting up the SCOM Assessment

When you have finished the configuration of the Azure Arc enrollment/Azure VM Extension, you are ready to setup the SCOM Assessment.

1. Open the Windows PowerShell command prompt as an Administrator.

2. Run the command **Add-SCOMAssessmentTask – ServerName <YourServerName> -WorkingDirectory <Directory>** where <*YourServerName*> is the fully qualified domain name (FQDN) or the NetBIOS name of one of the management servers and <*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 directory does not exist, it must be created before you continue with the execution.

3. Provide the necessary user account credentials.



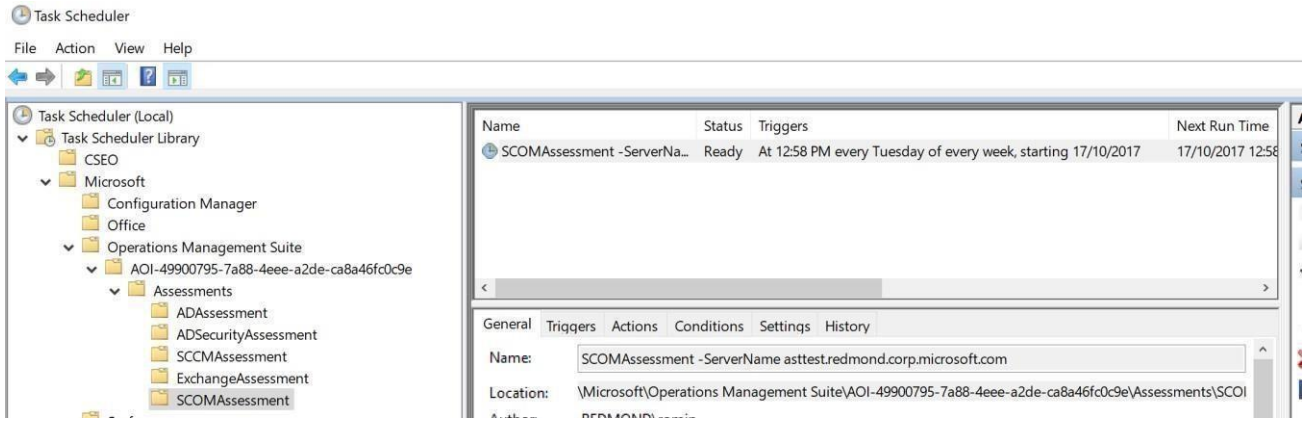
NOTE: This domain account must have all the following rights:

- Member of the local Administrators group on all servers in the environment (All Operations Manager Roles - Management Server, OpsMgr Database, Data Warehouse, Reporting, and Web Console).
- The Operation Manager Administrator Role for the management group being assessed.
- The SysAdmin role on all SQL Server instances or instances used by Operations Manager.

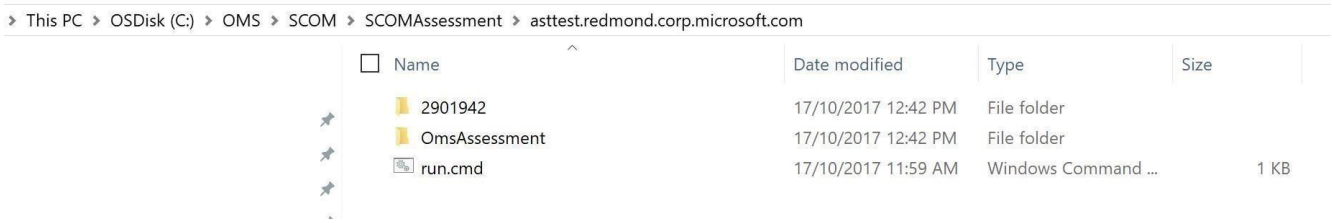
4. The script will continue with the necessary configuration. It will create a Scheduled Task that will trigger the data collection.

```
[SCOMAssessment]Enter the credential to be used to run this assessment. Credentials will be used to connect to remote server(s) for assessment.
[SCOMAssessment]User(DomainName\UserName):
redmond\romin
[SCOMAssessment]Enter the password for redmond\romin:
**********
[SCOMAssessment]Creating Windows Schedule task to run assessment...
[SCOMAssessment]SCOMAssessment setup successful.
[SCOMAssessment]Detailed log is at: C:\Users\romin\AppData\Local\Temp\Assessments_Configuration_20171017_065858.log
PS C:\users\romin>
```

Data collection is triggered by the **scheduled task** named "**SCOMAssessment -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.

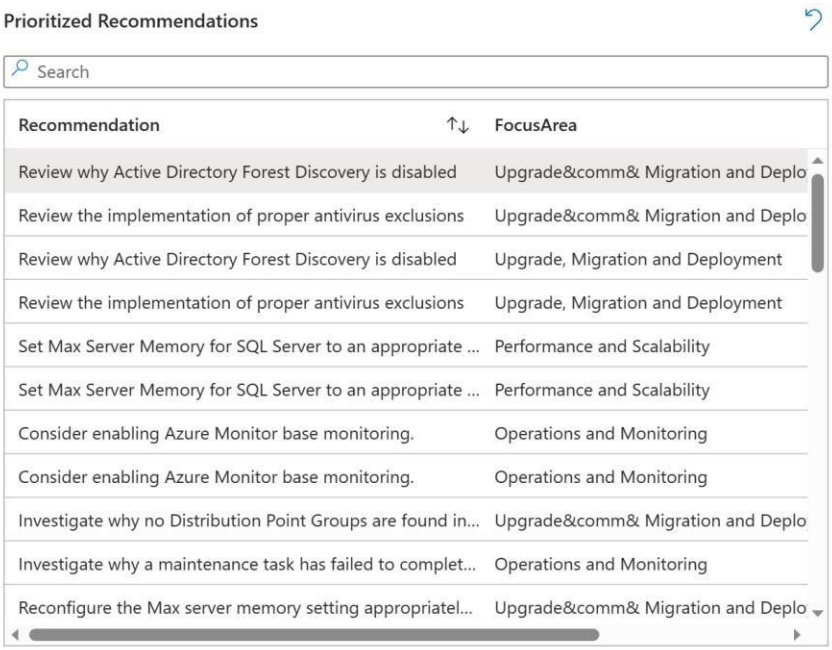


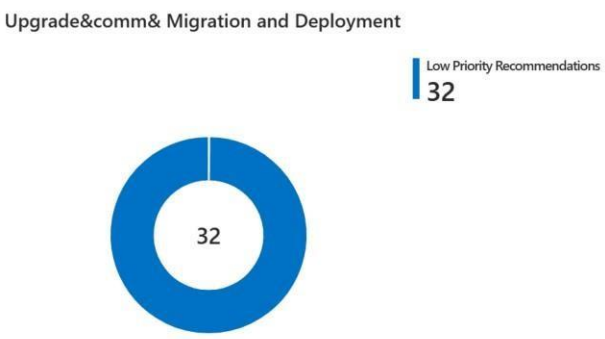
5. While the task is running, the collection data is temporarily stored under the folder you have specified during the installation using the following structure:



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

7. After a few hours, your assessment results will be available on your log analytics Workbooks. Click the **SCOM Assessment** tile to review. You will be presented the results:





Appendix

Data Collection Methods

The **SCOM 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. Event Log Collectors
3. Windows PowerShell Collectors
4. File Data Collectors
5. SQL Data Collectors
6. Windows Management Instrumentation (WMI) Collectors

1. Registry Collectors

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

- Service information from HKLM\SYSTEM\CurrentControlSet\Services. • This allows you to analyze the status of Operations Manager services.

2. Event Log Collectors

Collects the event logs from the servers. Microsoft collects the last 3 days of Information, Warnings and Errors from the Operations Manager, Application and System event logs.

3. **Windows PowerShell Collectors** Collects various information such as:

- Management Packs information
- Number of Management Servers

4. **File Data Collectors**

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

5. SQL Data Collectors

T-SQL queries are used to collect information regarding Operations Manager

6. Windows Management Instrumentation (WMI) Collectors WMI

is used to collect various information such as:

- WIN32_Volume
  Collects information on Volume Settings for each server in the environment. For example, the information is used to determine the system volume and drive letter, which allows a client to collect information on the files located on the system drive.
- Win32_Process
  Collect information on the processes running on each server in the environment. 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. Microsoft use the information to determine the amount of free space on the disk where the database or log files are located.