SCOM Lab Guide

Version 20.10

Ahmed Abdelwahed
ahmed@abdelwahed.me
www.abdelwahed.me
LinkedIn
GitHub

Contents

Introduction to System Center Operations Manager (SCOM) 3
Service Life Cycle and Its Relation with SCOM 5
Step-by-Step Guide for Installing System Center Operations Manager (SCOM) 7
Post Installation Tasks and Configurations 20
Installing SCOM Agent 32
Implementing Active Directory integration 38
SCOM Administration Roles 43
Managing SCOM Agent Settings 44
Importing and Managing Management Packs in SCOM 46
Sealed and Unsealed Management Packs in SCOM 51
Installing SCOM Agent on Linux 56
Alerts and Monitoring in SCOM 63
Using "My Workspace" in SCOM 66
Computer Task Options in SCOM 68
Configuring SSL for SQL Server Reporting Services (SSRS) on SCOM 70
Generating a CPU Utilization Report in SCOM 72
Configuring Exchange SMTP Settings for SCOM 76
Configuring Notifications in SCOM 79
Enabling Email Report Delivery in SQL Server Reporting Services (SSRS) 85
Customizing Reports 88
Complete Lab for Audit Collection Services (ACS) 89
SCOM Maintenance Mode 96
SCOM Updates 99
SCOM Upgrade 101

Introduction to System Center Operations Manager (SCOM)

System Center Operations Manager (SCOM) is a cross-platform data center management system for operating systems and hypervisors. It uses a single interface that shows state, health, and performance information of computer systems. SCOM helps organizations ensure predictable performance and availability of critical applications, providing a comprehensive monitoring solution for IT environments.

Key Features and Benefits of SCOM:

1. **Proactive Monitoring**:
    - SCOM monitors the health, performance, and availability of systems and applications, providing alerts before issues impact end users.
2. **Comprehensive Coverage:**
    - It supports monitoring for a wide range of services and applications, including Windows and Linux operating systems, SQL Server, Exchange, Active Directory, and many third-party applications.
3. **Centralized Management:**
    - SCOM provides a single pane of glass for monitoring across the data center, reducing the complexity of managing multiple tools.
4. **Customizable Dashboards and Reports:**
    - It offers customizable dashboards and reporting capabilities, enabling administrators to gain insights into the performance and health of their environments.
5. **Intelligent Alerts and Notifications:**
    - SCOM reduces noise with intelligent alerting and provides detailed information to help quickly identify and resolve issues.
6. **Extensibility:**
    - With management packs, SCOM can be extended to monitor additional applications and services, including those developed in-house.

Core Components of SCOM:

1. **Management Server**:
    - The central component that manages the overall SCOM infrastructure, processing data from agents and communicating with the database.
2. **Operations Console:**
    - The user interface for SCOM administrators and operators to view and manage monitoring data, alerts, and reports.
3. **Operations Database:**
    - Stores all the configuration data and monitoring data collected from the managed devices.
4. **Data Warehouse:**
    - A separate database designed for long-term storage and reporting of historical monitoring data.
5. **Agents:**
    - Installed on each monitored system, agents collect data and send it to the management server.

6. **Management Packs:**
    - Predefined sets of monitoring settings and rules specific to applications or services, providing the necessary logic to monitor them effectively.

Use Cases of SCOM:

1. **Data Center Monitoring**:
    - Monitoring the health and performance of servers, storage, and network devices to ensure optimal data center operations.
2. **Application Monitoring:**
    - Tracking the availability and performance of critical applications such as Exchange, SQL Server, and custom enterprise applications.
3. **Compliance and Reporting:**
    - Generating compliance reports and ensuring that systems are adhering to organizational and regulatory standards.
4. **Hybrid Cloud Monitoring:**
    - Extending monitoring capabilities to cloud environments, including Azure and AWS, to maintain visibility across hybrid infrastructures.

Getting Started with SCOM:

1. **Installation and Configuration**:
    - Install the management server, configure the operations database, data warehouse, and install agents on target systems.
2. **Deploy Management Packs:**
    - Import and configure management packs for the applications and services you need to monitor.
3. **Create and Customize Dashboards:**
    - Use the Operations Console to create dashboards that provide insights into the performance and health of your environment.
4. **Set Up Alerts and Notifications:**
    - Configure alerting rules and notifications to ensure the right personnel are informed about potential issues promptly.
5. **Analyze and Report:**
    - Use SCOM's reporting capabilities to analyze historical data and generate reports for management and compliance purposes.

Service Life Cycle and Its Relation with SCOM

The Service Life Cycle is a critical concept in IT service management, representing the stages through which a service goes from inception to retirement. SCOM plays a significant role in supporting various stages of the Service Life Cycle by providing monitoring, management, and reporting capabilities.

Stages of the Service Life Cycle:

1. **Service Strategy**:
   - **Objective**: Define the market and the service offerings.
   - **SCOM Relation**: Though SCOM is not directly involved in the strategic planning of services, it provides critical historical data and performance reports that can inform decision-making during the strategy phase.
2. **Service Design:**
   - **Objective**: Design the service to meet business objectives and customer needs.
   - **SCOM Relation**: SCOM can be used to test and monitor prototype designs, ensuring they meet the required performance and availability standards before moving into production.
3. **Service Transition:**
   - **Objective**: Ensure that new or modified services are effectively transitioned into production.
   - **SCOM Relation**: During this phase, SCOM helps by monitoring the deployment of services, ensuring that any issues during the transition are quickly identified and resolved. This includes tracking changes and validating that new services meet the designed specifications.
4. **Service Operation:**
   - **Objective**: Ensure the effective and efficient delivery and support of services.
   - **SCOM Relation**: This is the primary phase where SCOM is extensively used. It monitors the health, performance, and availability of services, providing real-time alerts, dashboards, and reports. SCOM ensures that services are running optimally and helps in incident management by detecting and notifying of issues.
5. **Continual Service Improvement (CSI):**
   - **Objective**: Continuously improve the quality and effectiveness of services.
   - **SCOM Relation**: SCOM contributes to CSI by providing detailed performance and availability reports, trend analysis, and historical data. This information is vital for identifying areas for improvement and measuring the impact of improvement initiatives.

How SCOM Supports Each Phase:

Service Strategy:

- **Data Collection and Reporting**:
  - Historical performance data helps in understanding service demand and performance trends.
  - Reports generated by SCOM can influence strategic decisions regarding capacity planning and resource allocation.

Service Design:

- **Prototype Monitoring:**
  - SCOM can monitor prototype environments, ensuring that design specifications meet performance and availability standards.
  - Provides feedback on potential design flaws or bottlenecks.

Service Transition:

- **Change Management:**
  - Monitors changes in the environment to ensure they are implemented smoothly.
  - Tracks configuration changes and validates that new services integrate seamlessly with existing ones.
- **Deployment Validation:**
  - Ensures that services deployed to production meet the required performance and availability metrics.

Service Operation:

- **Real-Time Monitoring:**
  - Monitors the health, performance, and availability of services in real-time.
  - Provides alerts and notifications for any issues, enabling quick resolution.
- **Incident Management:**
  - Helps in identifying the root cause of issues, reducing downtime and improving service reliability.
- **Operational Dashboards:**
  - Provides customizable dashboards for different stakeholders, showing the status and performance of services.

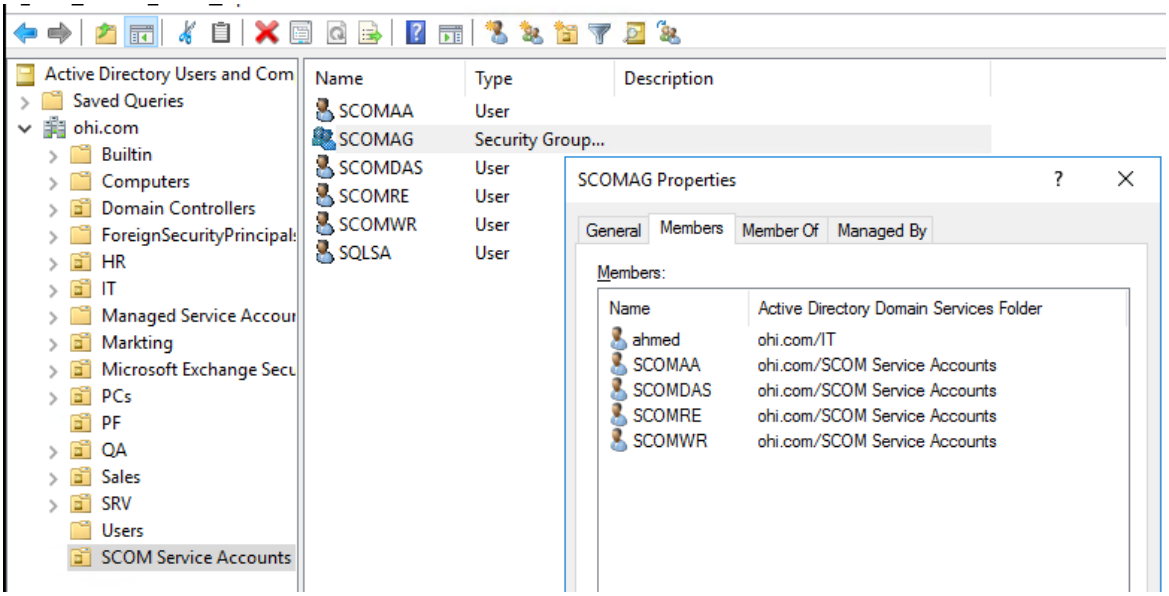
Continual Service Improvement:

- **Performance Analysis:**
  - Analyzes performance trends over time to identify areas for improvement.
  - Helps in benchmarking and setting performance targets.
- **Service Reviews:**
  - Uses data from SCOM to review service performance and identify improvement opportunities.
- **Impact Measurement:**
  - Measures the impact of improvement initiatives on service performance and availability.

Step-by-Step Guide for Installing System Center Operations Manager (SCOM)

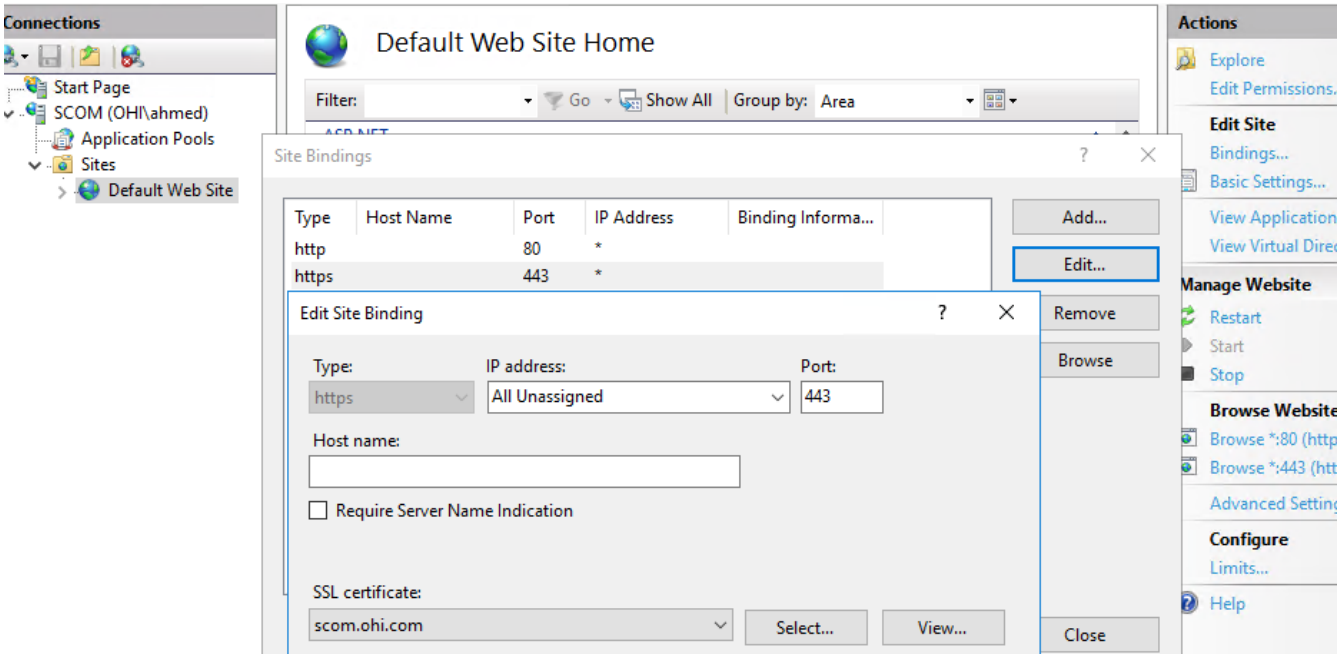
Pre-Installation Steps

1. **Set Up Service Accounts in Active Directory**
    - Create the following service accounts in Active Directory and set their passwords to never expire:
        - SCOM Action Account
        - SCOM Datawarehouse Reader Account
        - SCOM Datawarehouse Write Account
        - SCOM SQL Service Account
        - SCOM Admin Account
    - Ensure these accounts have appropriate permissions and are securely managed.



2. **Create OMAdmin Group and Configure Group Policy**
    - Create a security group named OMAdmin.
    - Add the OMAdmin group to the local administrators group on all computers using Group Policy.
        - Open Group Policy Management Console (GPMC).
        - Create or edit a Group Policy Object (GPO).
        - Navigate to Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Restricted Groups.
        - Add the OMAdmin group to the local administrators group.

3. **Apply for an Active Directory Certificate for SCOM**
    - Request and install a certificate for SCOM from your Active Directory Certificate Services (AD CS) to ensure secure communication.

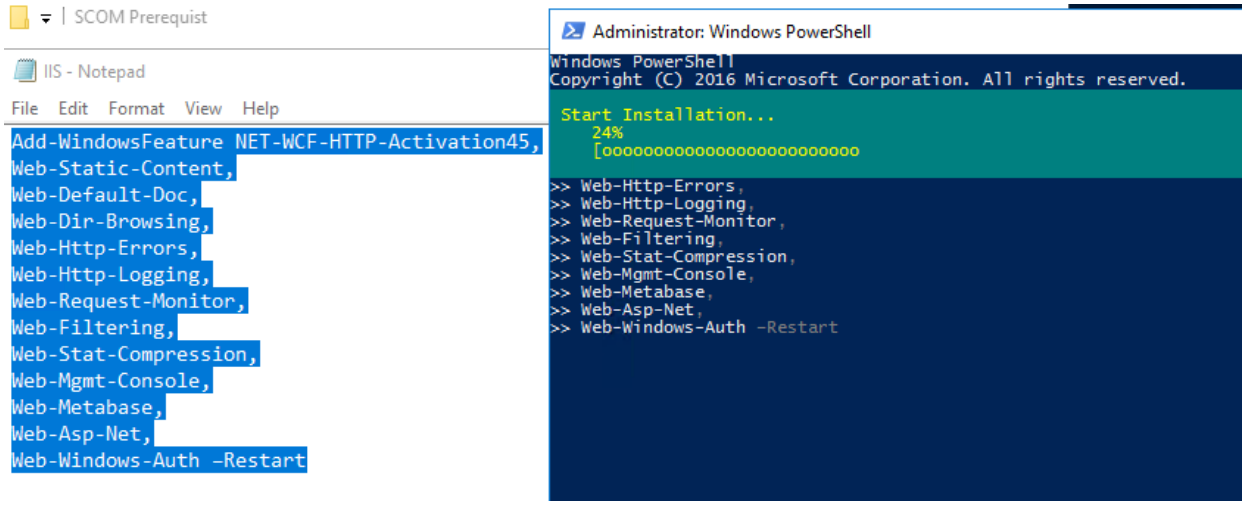


If you are unable to link AD CS to request a computer certificate for SCOM, you should initially add the AD CS server certificate to SCOM's trusted root CA.

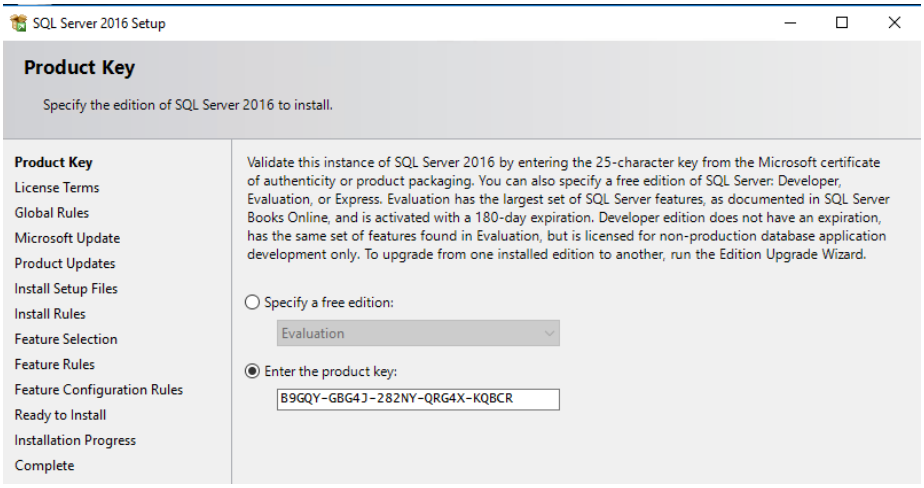
4. **Download and Install Report Viewer**
    - Download Report Viewer from Microsoft.
    - Install Report Viewer on the management server.
5. **Install Microsoft System CLR Types for SQL Server 2014**
    - Download and install the Microsoft System CLR Types for SQL Server 2014 from the Microsoft Download Center.
6. **Complete IIS Requirements**
    - Install Internet Information Services (IIS) on the management server and SQL server.
    - For Windows Server 2016, use the following PowerShell command to install IIS and required features:

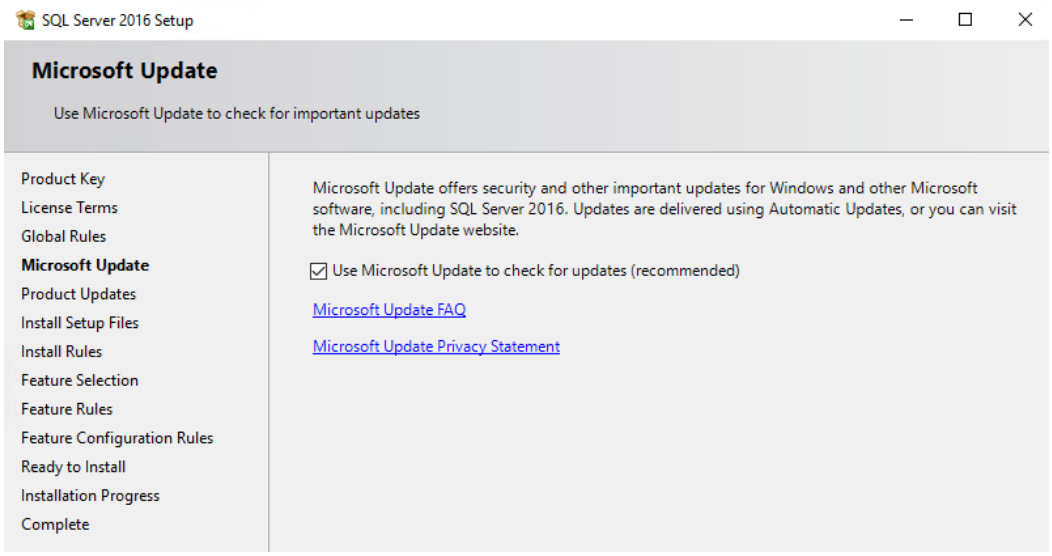
```
Install-WindowsFeature -name Web-Server,Web-Common-Http,Web-Default-Doc,Web-Dir-Browsing,Web-Http-Errors,Web-Static-Content,Web-Http-Redirect,Web-Asp-Net,Web-Net-Ext,Web-ISAPI-Ext,Web-ISAPI-Filter,Web-Http-Logging,Web-Request-Monitor,Web-Stat-Compression,Web-Dyn-Compression,Web-Security,Web-Windows-Auth,Web-Filtering,Web-Mgmt-Console,NET-Framework-Features,NET-Framework-45-Features,NET-Framework-Core,NET-HTTP-Activation,NET-WCF-HTTP-Activation45 -source f:\sources\sxs
```

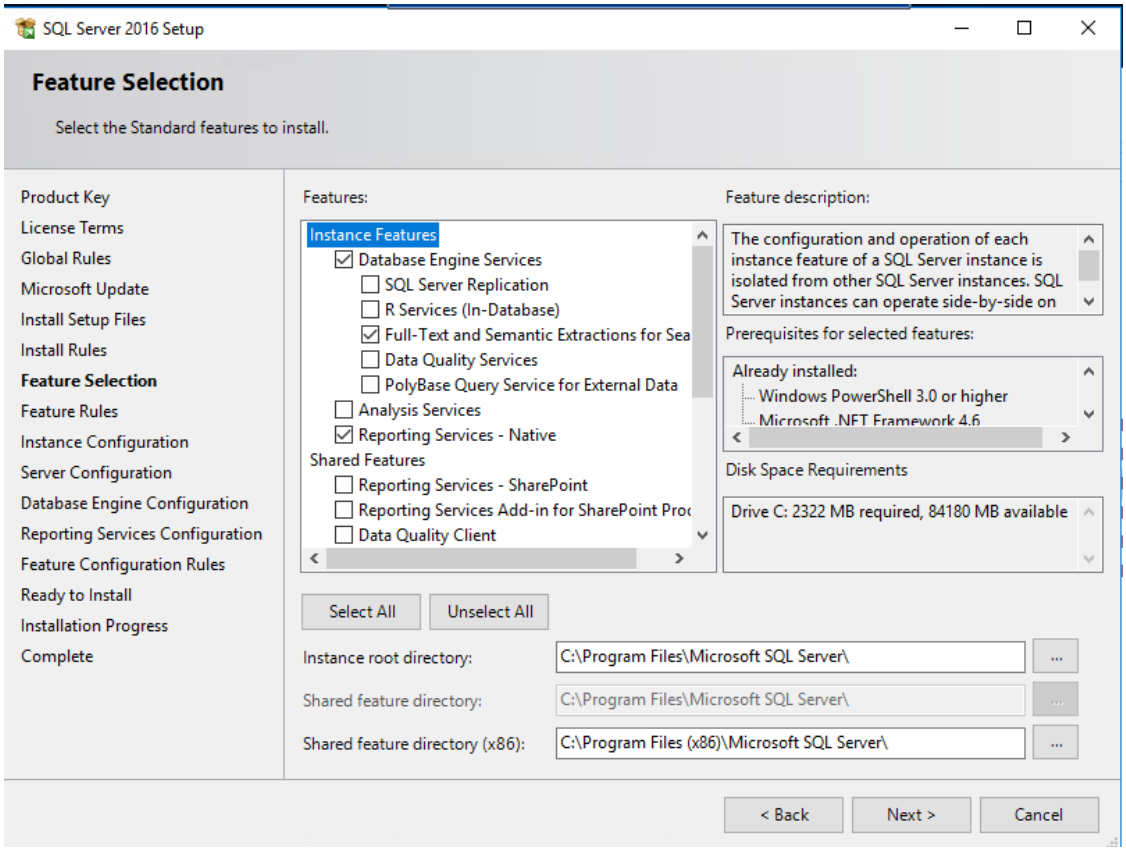
- Restart the server after completing the IIS setup.

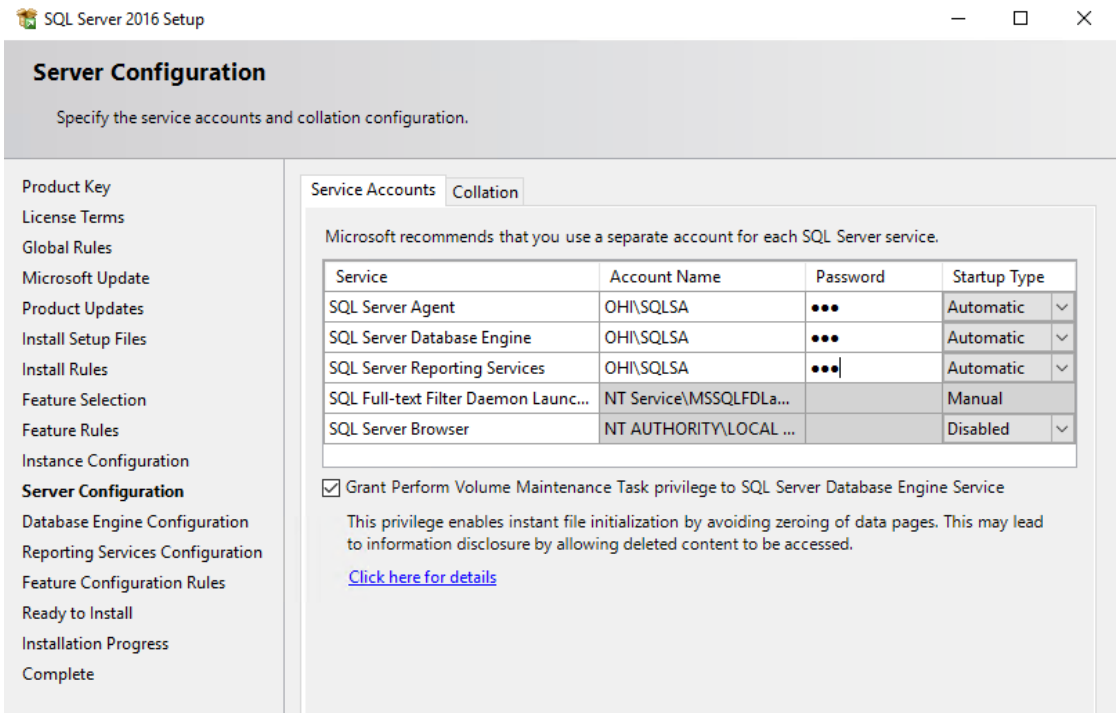


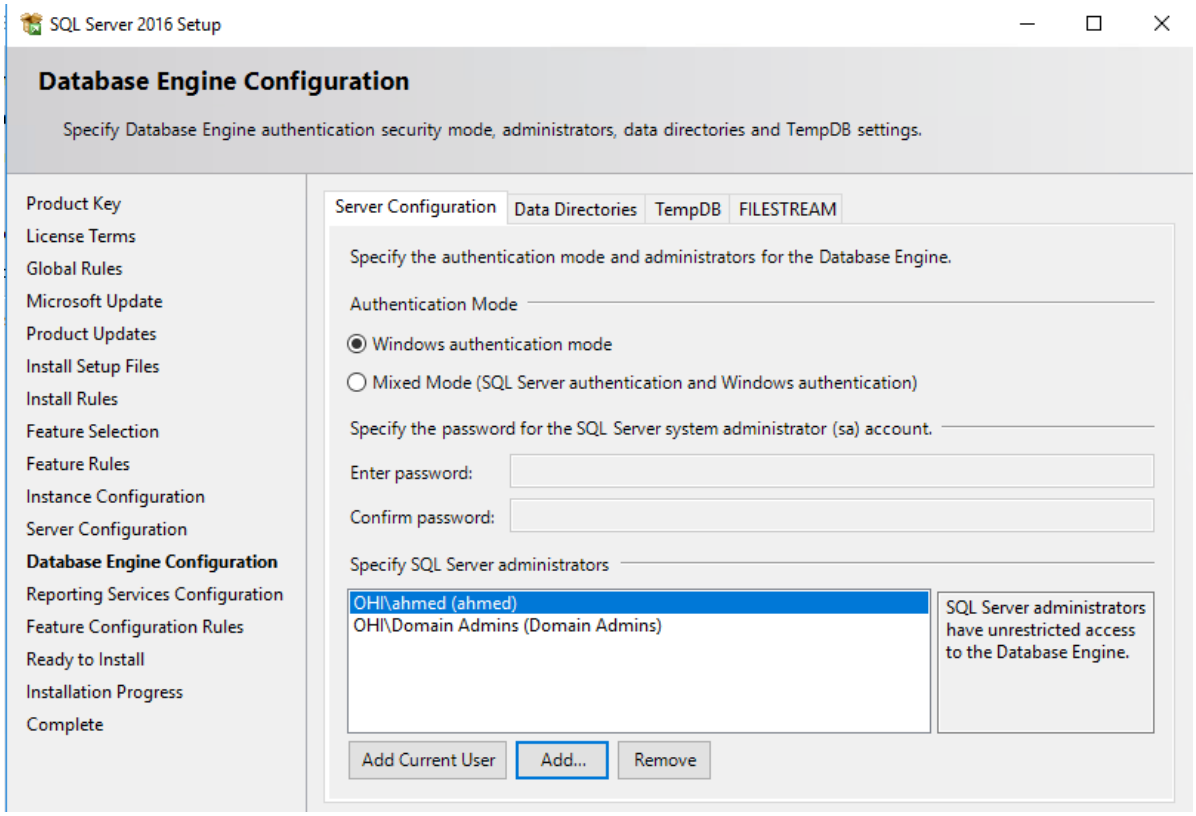
7. **Activate HTTPS**
   - Ensure HTTPS is enabled and configured correctly for secure communication.
8. **Configure Firewall Settings**
   - Allow inbound traffic on SQL TCP port 1433 for SQL Server:
     - Open Windows Firewall with Advanced Security.
     - Create a new inbound rule for TCP port 1433 and allow edge traversal.
   - Allow inbound SCOM traffic on the following ports:
     - TCP ports 5723, 1271, 135 for Windows.
     - TCP ports 1270, 22 for Linux.
9. **Prepare SQL Server 2016 Standard Edition**
   - Install SQL Server 2016 Standard Edition on your SQL server.
   - Configure SQL Server for SCOM by setting up the necessary databases and permissions.

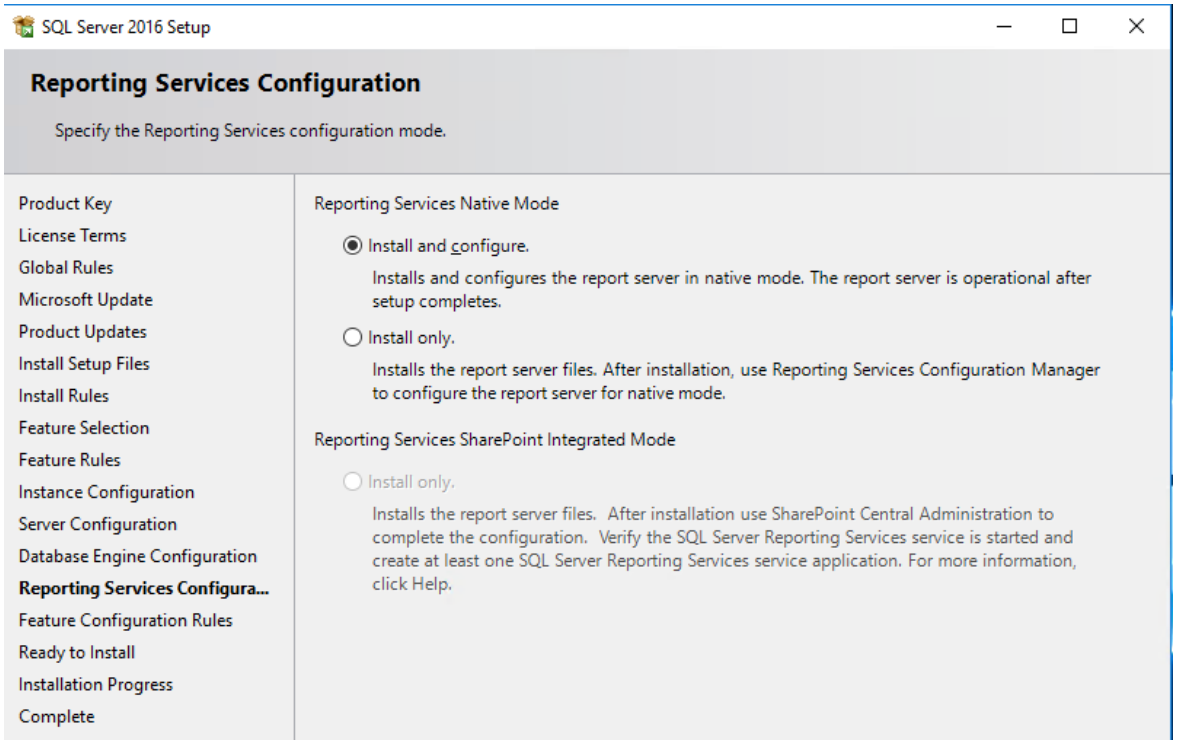


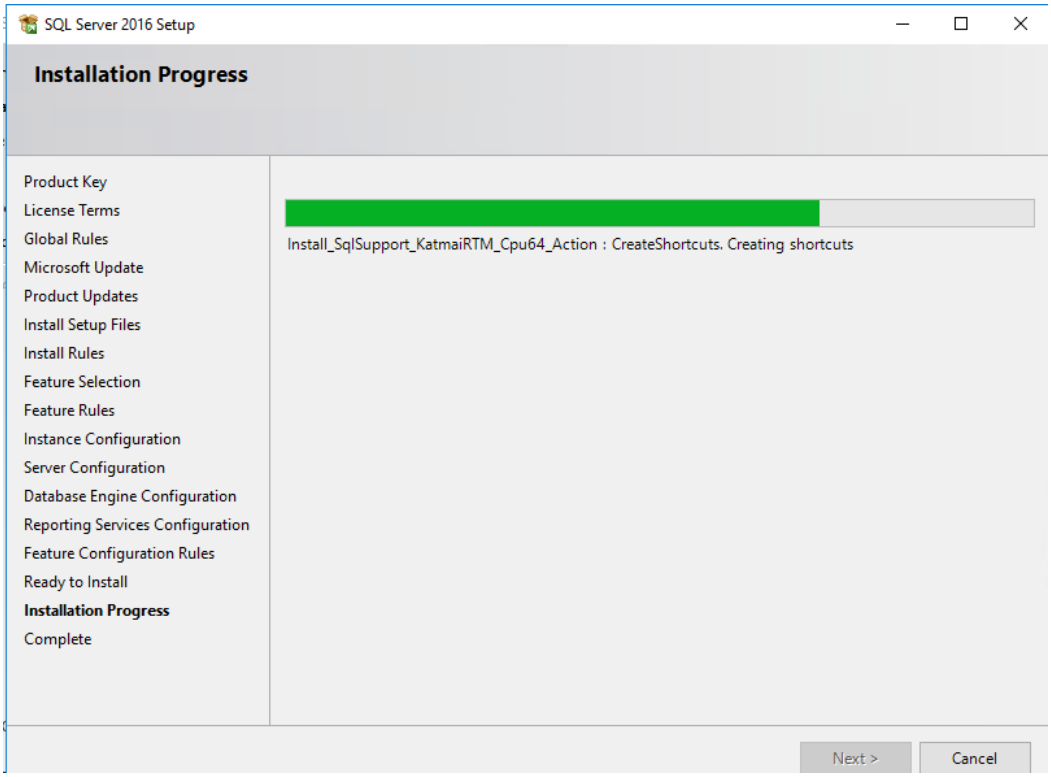

SQL Server 2016 Setup
Microsoft Update
Use Microsoft Update to check for important updates
Product Key
License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Microsoft Update offers security and other important updates for Windows and other Microsoft software, including SQL Server 2016. Updates are delivered using Automatic Updates, or you can visit the Microsoft Update website.
Use Microsoft Update to check for updates (recommended)
Microsoft Update FAQ
Microsoft Update Privacy Statement

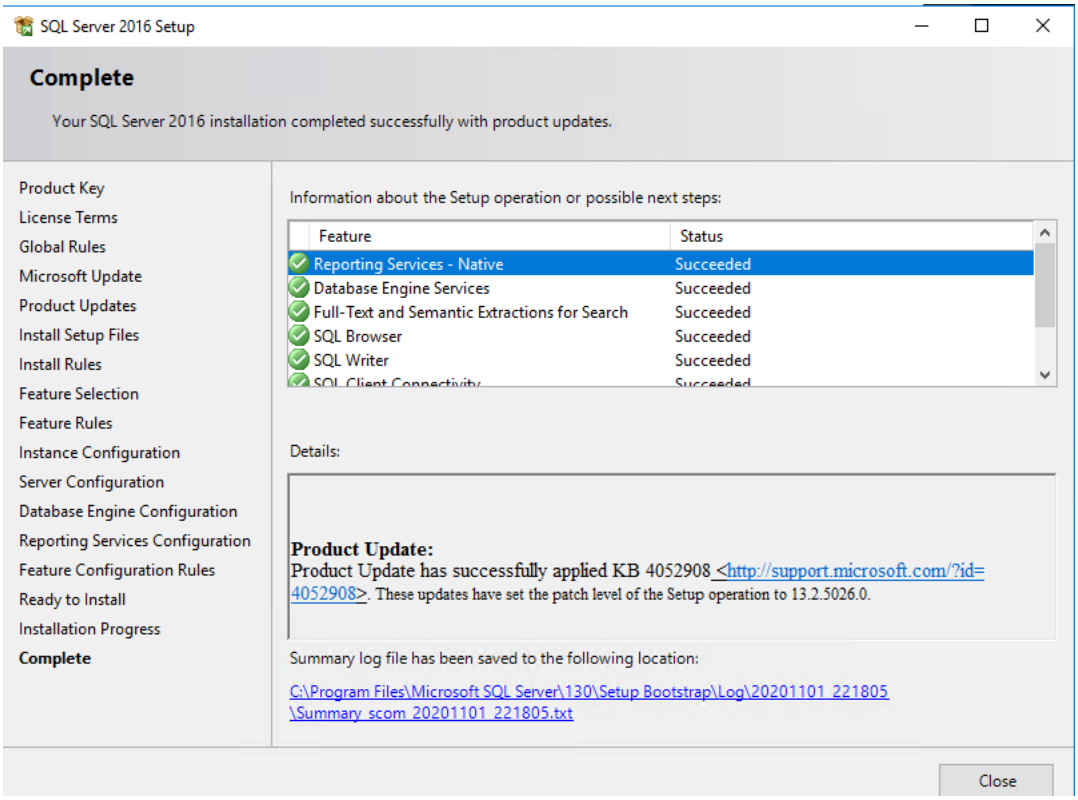

SQL Server 2016 Setup
Feature Selection
Select the Standard features to install.
Product Key
License Terms
Global Rules
Microsoft Update
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Reporting Services Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Features:
Instance Features
Database Engine Services
SQL Server Replication
R Services (In-Database)
Full-Text and Semantic Extractions for Sea
Data Quality Services
PolyBase Query Service for External Data
Analysis Services
Reporting Services - Native
Shared Features
Reporting Services - SharePoint
Reporting Services Add-in for SharePoint Proc
Data Quality Client
Feature description:
The configuration and operation of each instance feature of a SQL Server instance is isolated from other SQL Server instances. SQL Server instances can operate side-by-side on
Prerequisites for selected features:
Already installed:
Windows PowerShell 3.0 or higher
Microsoft .NET Framework 4.6
Disk Space Requirements
Drive C: 2322 MB required, 84180 MB available
Select All
Unselect All
Instance root directory:
C:\Program Files\Microsoft SQL Server\
Shared feature directory:
C:\Program Files\Microsoft SQL Server\
Shared feature directory (x86):
C:\Program Files (x86)\Microsoft SQL Server\
< Back
Next >
Cancel


SQL Server 2016 Setup
Server Configuration
Specify the service accounts and collation configuration.
Product Key
License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Reporting Services Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Service Accounts
Collation
Microsoft recommends that you use a separate account for each SQL Server service.
Service
Account Name
Password
Startup Type
SQL Server Agent
OHI\SQLSA
Automatic
SQL Server Database Engine
OHI\SQLSA
Automatic
SQL Server Reporting Services
OHI\SQLSA
Automatic
SQL Full-text Filter Daemon Launc...
NT Service\MSSQLFDLa...
Manual
SQL Server Browser
NT AUTHORITY\LOCAL ...
Disabled
Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service
This privilege enables instant file initialization by avoiding zeroing of data pages. This may lead to information disclosure by allowing deleted content to be accessed.
Click here for details


SQL Server 2016 Setup
Database Engine Configuration
Specify Database Engine authentication security mode, administrators, data directories and TempDB settings.
Product Key
License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Reporting Services Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Server Configuration
Data Directories
TempDB
FILESTREAM
Specify the authentication mode and administrators for the Database Engine.
Authentication Mode
Windows authentication mode
Mixed Mode (SQL Server authentication and Windows authentication)
Specify the password for the SQL Server system administrator (sa) account.
Enter password:
Confirm password:
Specify SQL Server administrators
OHI\ahmed (ahmed)
OHI\Domain Admins (Domain Admins)
SQL Server administrators have unrestricted access to the Database Engine.
Add Current User
Add...
Remove


SQL Server 2016 Setup
Reporting Services Configuration
Specify the Reporting Services configuration mode.
Product Key
License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Reporting Services Configura...
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Reporting Services Native Mode
Install and configure.
Installs and configures the report server in native mode. The report server is operational after setup completes.
Install only.
Installs the report server files. After installation, use Reporting Services Configuration Manager to configure the report server for native mode.
Reporting Services SharePoint Integrated Mode
Install only.
Installs the report server files. After installation use SharePoint Central Administration to complete the configuration. Verify the SQL Server Reporting Services service is started and create at least one SQL Server Reporting Services service application. For more information, click Help.

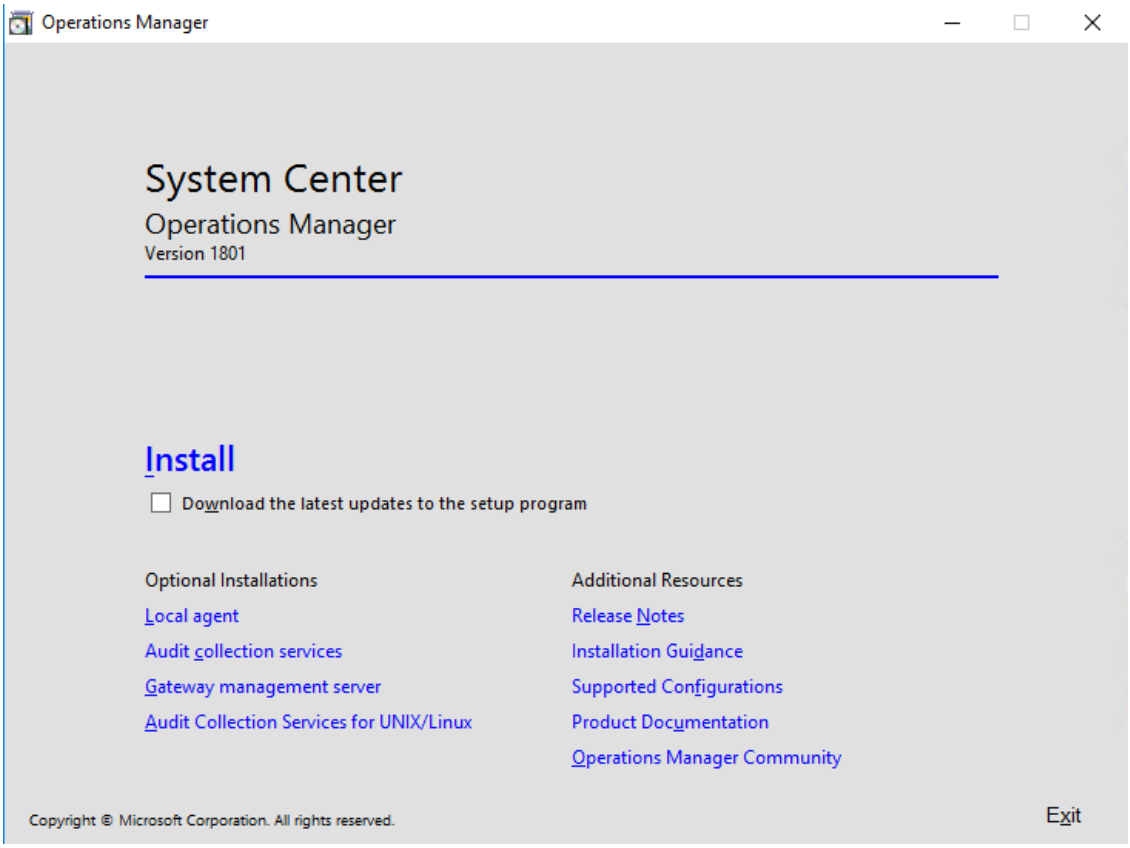

SQL Server 2016 Setup
Installation Progress
Product Key
License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Reporting Services Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Install_SqlSupport_KatmaiRTM_Cpu64_Action : CreateShortcuts. Creating shortcuts
Next >
Cancel

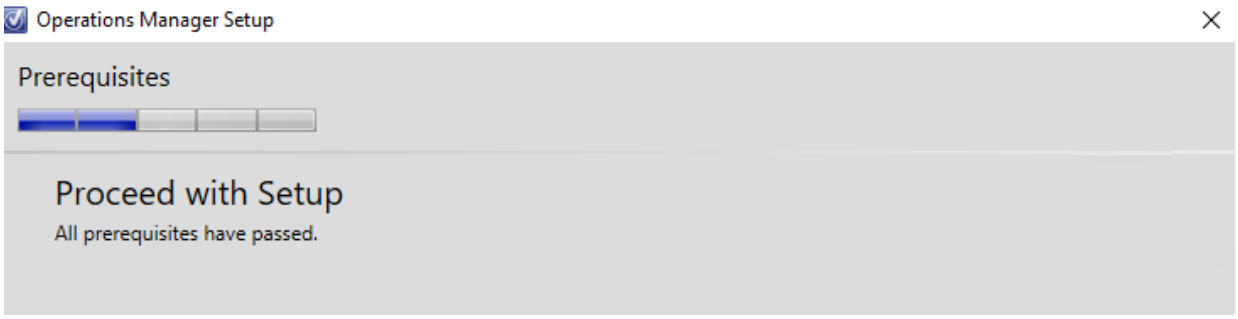


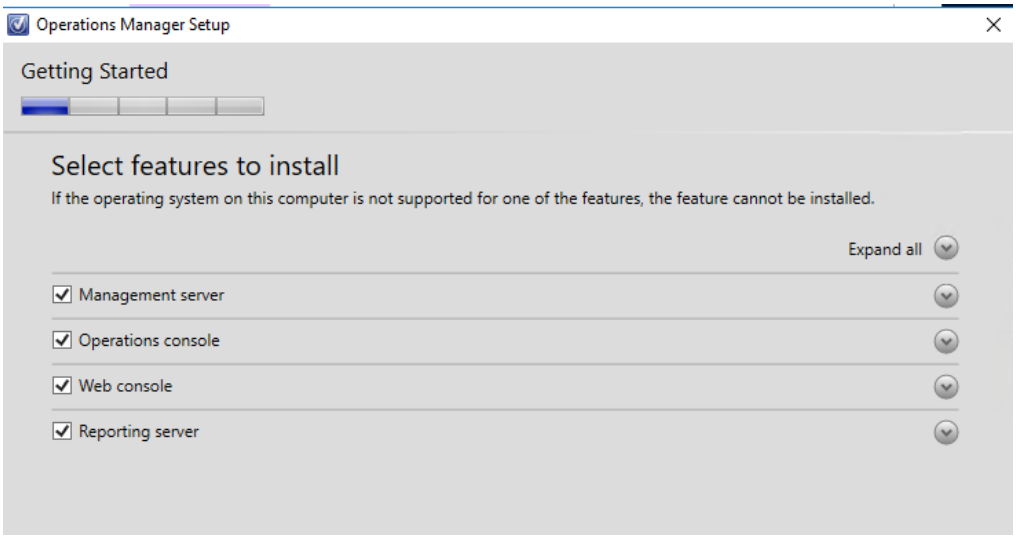
Installation Steps

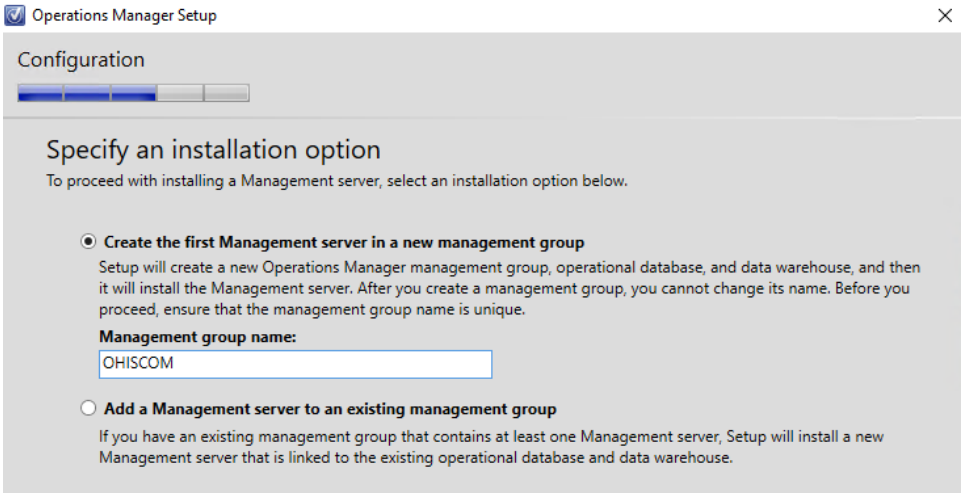
1. **Install SCOM Prerequisites**
    - On the management server, install the necessary prerequisites including:
        - .NET Framework.
        - IIS components.
        - SQL Server CLR Types.
        - Report Viewer.
2. **Install SCOM Management Server**
    - Run the SCOM setup wizard and follow these steps:
        - Select "Install" to start the installation process.
        - Select "Management Server" as the feature to install.
        - Accept the license terms.
        - On the "Configure the operational database" page, specify the SQL Server instance and database name.
        - On the "Configure the data warehouse database" page, specify the SQL Server instance and database name for the data warehouse.

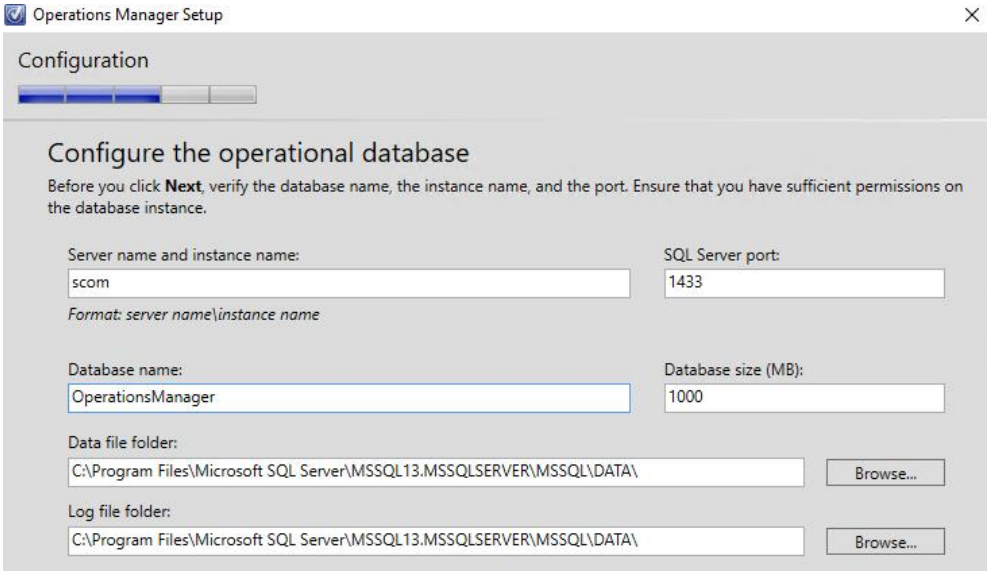
- On the "Specify a management group" page, provide a name for your management group.
- On the "Specify an action account" page, enter the credentials for the SCOM Action Account.
- On the "Specify a Data Warehouse write account" page, enter the credentials for the SCOM Datawarehouse Write Account.
- On the "Specify a Data Warehouse read account" page, enter the credentials for the SCOM Datawarehouse Reader Account.
- Complete the installation and verify that the Management Server is installed successfully.

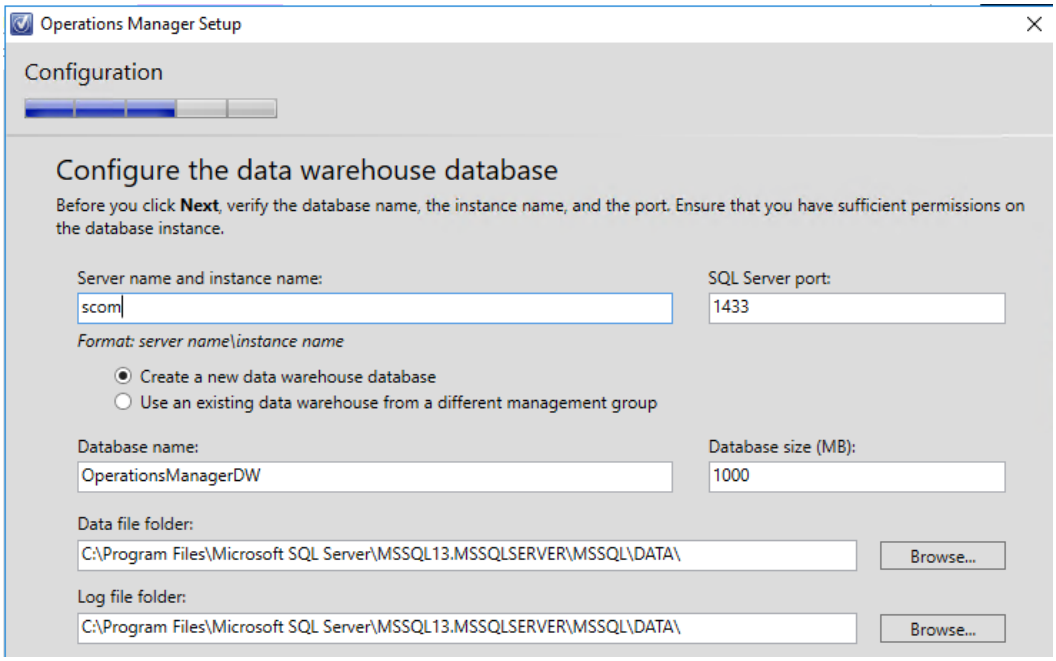




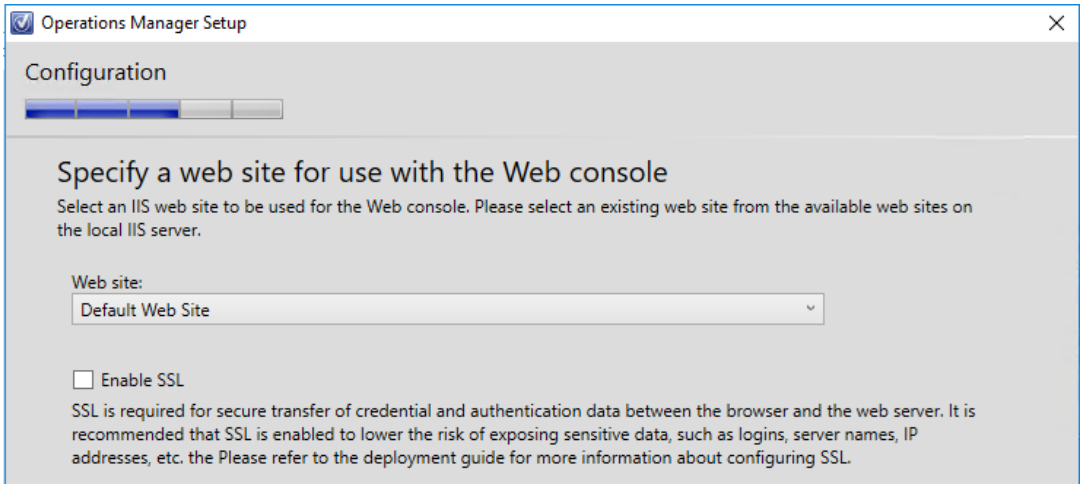

Operations Manager Setup
Getting Started
Select features to install
If the operating system on this computer is not supported for one of the features, the feature cannot be installed.
Expand all
Management server
Operations console
Web console
Reporting server


Operations Manager Setup
Configuration
Specify an installation option
To proceed with installing a Management server, select an installation option below.
Create the first Management server in a new management group
Setup will create a new Operations Manager management group, operational database, and data warehouse, and then it will install the Management server. After you create a management group, you cannot change its name. Before you proceed, ensure that the management group name is unique.
Management group name:
OHISCOM
Add a Management server to an existing management group
If you have an existing management group that contains at least one Management server, Setup will install a new Management server that is linked to the existing operational database and data warehouse.

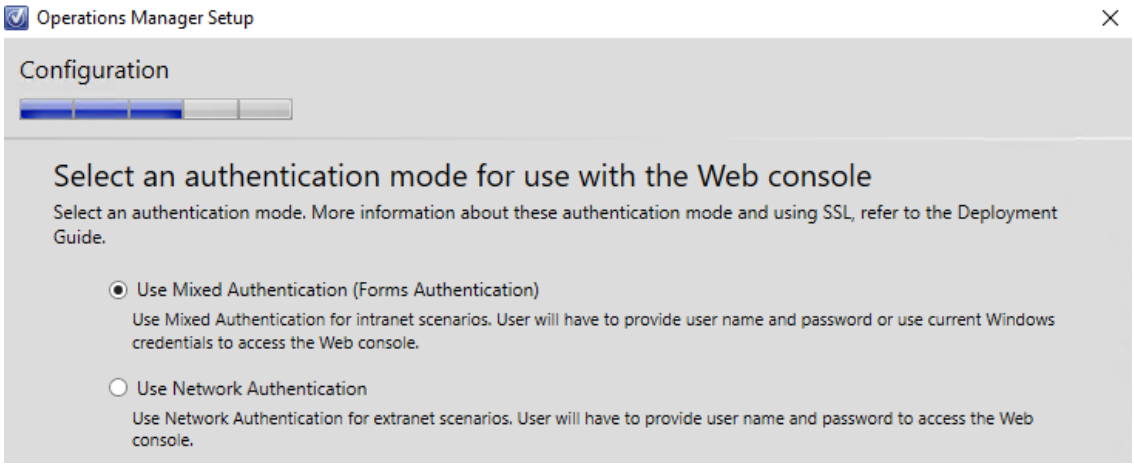

Operations Manager Setup
Configuration
Configure the operational database
Before you click Next, verify the database name, the instance name, and the port. Ensure that you have sufficient permissions on the database instance.
Server name and instance name:
scom
SQL Server port:
1433
Format: server name\instance name
Database name:
OperationsManager
Database size (MB):
1000
Data file folder:
C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\DATA\
Browse...
Log file folder:
C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\DATA\
Browse...

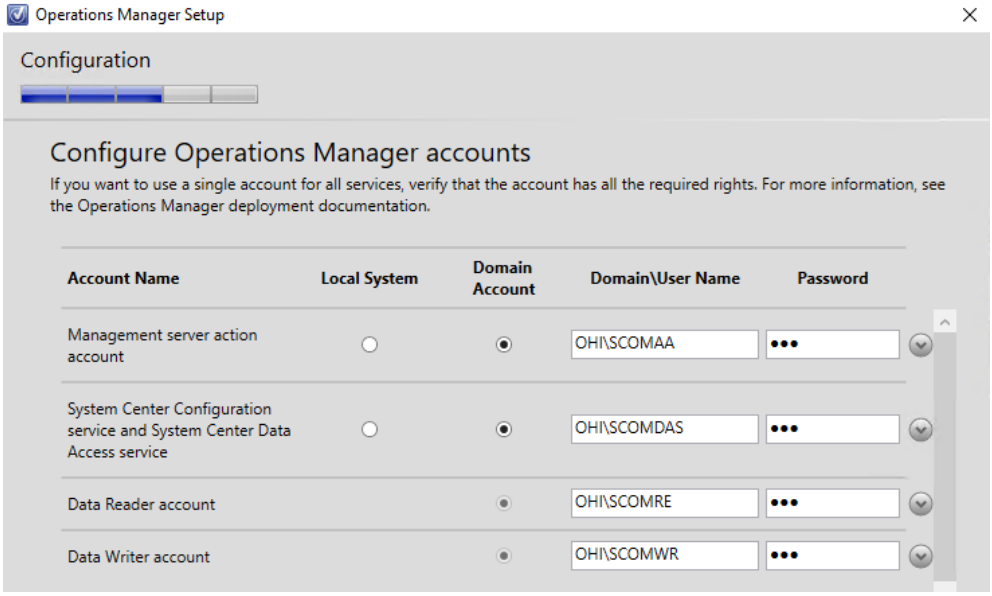


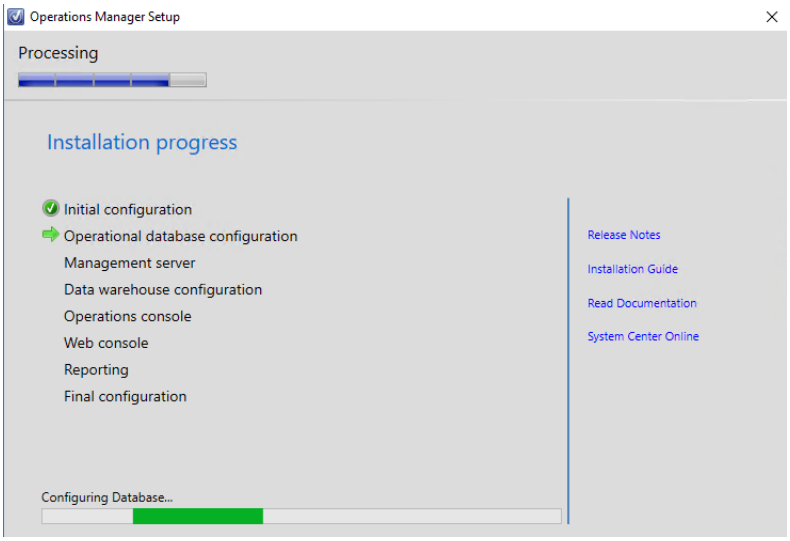


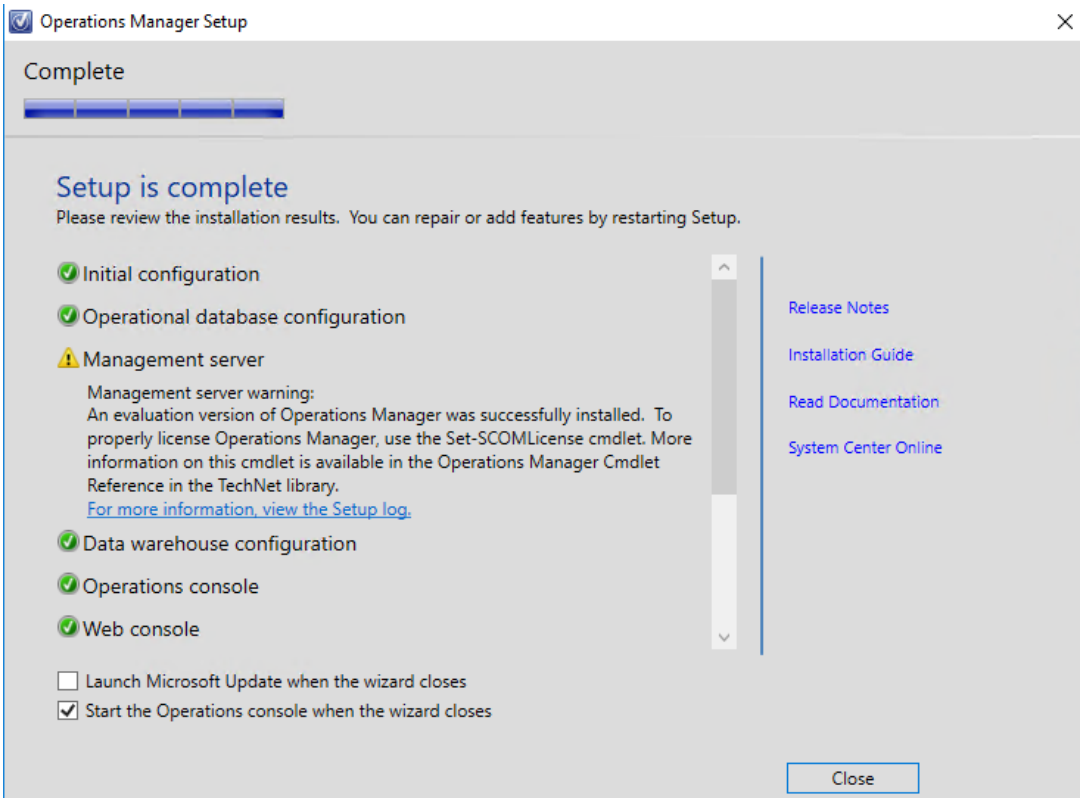


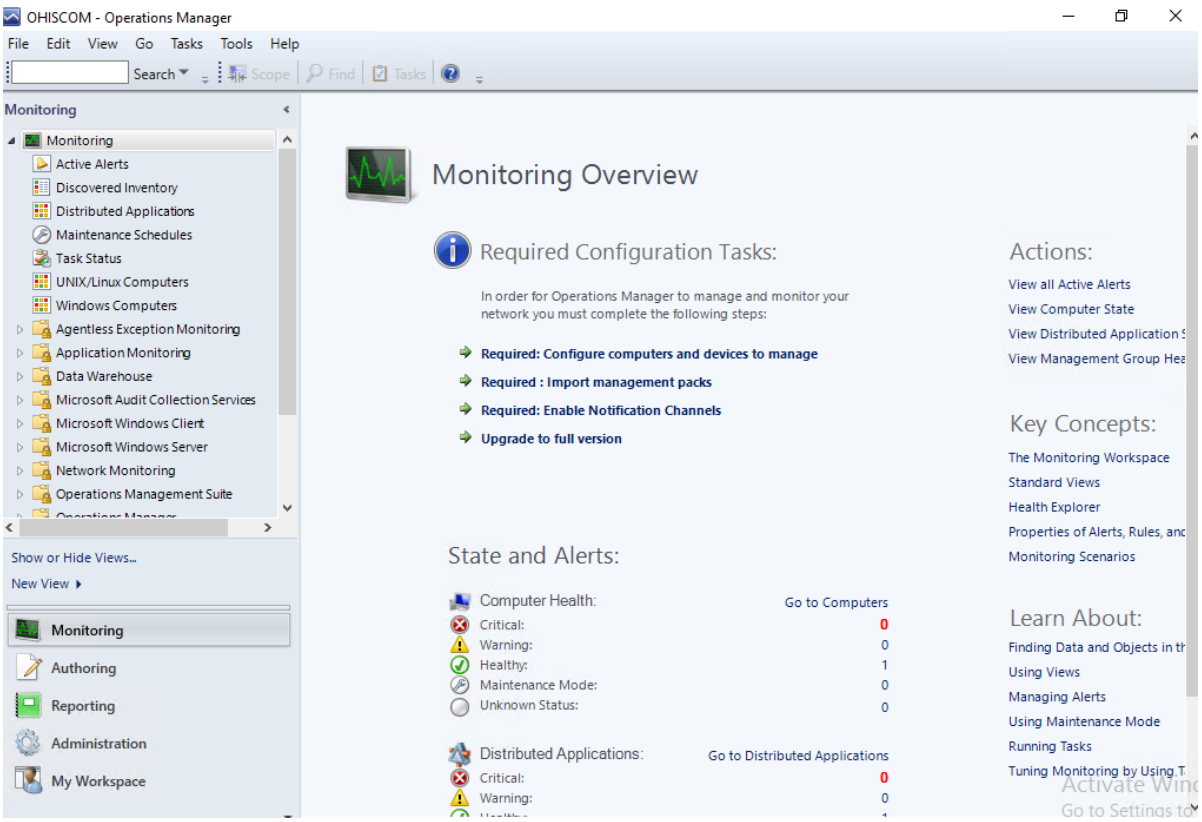
Please remember to include SCOMAG as a member of the local administrators' group.


Operations Manager Setup
Configuration
Select an authentication mode for use with the Web console
Select an authentication mode. More information about these authentication mode and using SSL, refer to the Deployment Guide.
Use Mixed Authentication (Forms Authentication)
Use Mixed Authentication for intranet scenarios. User will have to provide user name and password or use current Windows credentials to access the Web console.
Use Network Authentication
Use Network Authentication for extranet scenarios. User will have to provide user name and password to access the Web console.

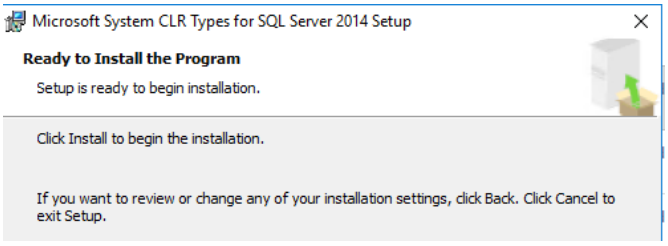

Operations Manager Setup
Configuration
Configure Operations Manager accounts
If you want to use a single account for all services, verify that the account has all the required rights. For more information, see the Operations Manager deployment documentation.
Account Name
Local System
Domain Account
Domain\User Name
Password
Management server action account
OHI\SCOMAA
System Center Configuration service and System Center Data Access service
OHI\SCOMDAS
Data Reader account
OHI\SCOMRE
Data Writer account
OHI\SCOMWR

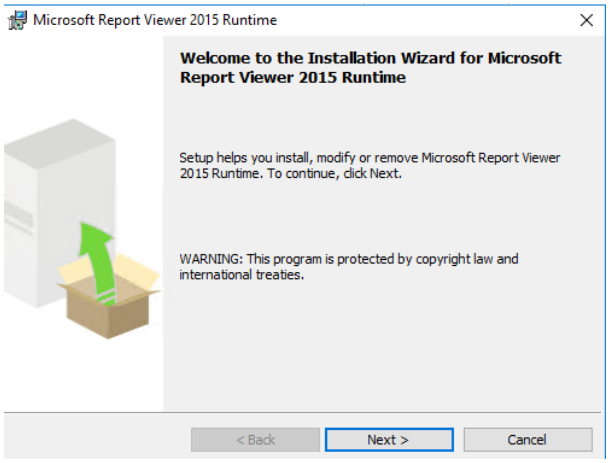

Operations Manager Setup
Processing
Installation progress
Initial configuration
Operational database configuration
Management server
Data warehouse configuration
Operations console
Web console
Reporting
Final configuration
Release Notes
Installation Guide
Read Documentation
System Center Online
Configuring Database...


Operations Manager Setup
Complete
Setup is complete
Please review the installation results. You can repair or add features by restarting Setup.
Initial configuration
Operational database configuration
Management server
Management server warning:
An evaluation version of Operations Manager was successfully installed. To properly license Operations Manager, use the Set-SCOMLicense cmdlet. More information on this cmdlet is available in the Operations Manager Cmdlet Reference in the TechNet library.
For more information, view the Setup log.
Data warehouse configuration
Operations console
Web console
Release Notes
Installation Guide
Read Documentation
System Center Online
Launch Microsoft Update when the wizard closes
Start the Operations console when the wizard closes
Close


OHISCOM - Operations Manager
File Edit View Go Tasks Tools Help
Search Scope Find Tasks
Monitoring
Active Alerts
Discovered Inventory
Distributed Applications
Maintenance Schedules
Task Status
UNIX/Linux Computers
Windows Computers
Agentless Exception Monitoring
Application Monitoring
Data Warehouse
Microsoft Audit Collection Services
Microsoft Windows Client
Microsoft Windows Server
Network Monitoring
Operations Management Suite
Show or Hide Views...
New View
Monitoring
Authoring
Reporting
Administration
My Workspace
Monitoring Overview
Required Configuration Tasks:
In order for Operations Manager to manage and monitor your network you must complete the following steps:
Required: Configure computers and devices to manage
Required : Import management packs
Required: Enable Notification Channels
Upgrade to full version
State and Alerts:
Computer Health:
Go to Computers
Critical: 0
Warning: 0
Healthy: 1
Maintenance Mode: 0
Unknown Status: 0
Distributed Applications:
Go to Distributed Applications
Critical: 0
Warning: 0
Actions:
View all Active Alerts
View Computer State
Key Concepts:
The Monitoring Workspace
Standard Views
Health Explorer
Monitoring Scenarios
Learn About:
Using Views
Managing Alerts
Using Maintenance Mode
Running Tasks

3. **Install SCOM Reporting Server**
    - Run the SCOM setup wizard and select "Reporting Server" as the feature to install.
    - Follow the prompts to configure the SQL Server Reporting Services instance.
    - Specify the Data Warehouse Reader Account for running queries against the reporting data warehouse.
    - Complete the installation and verify that the Reporting Server is installed successfully.



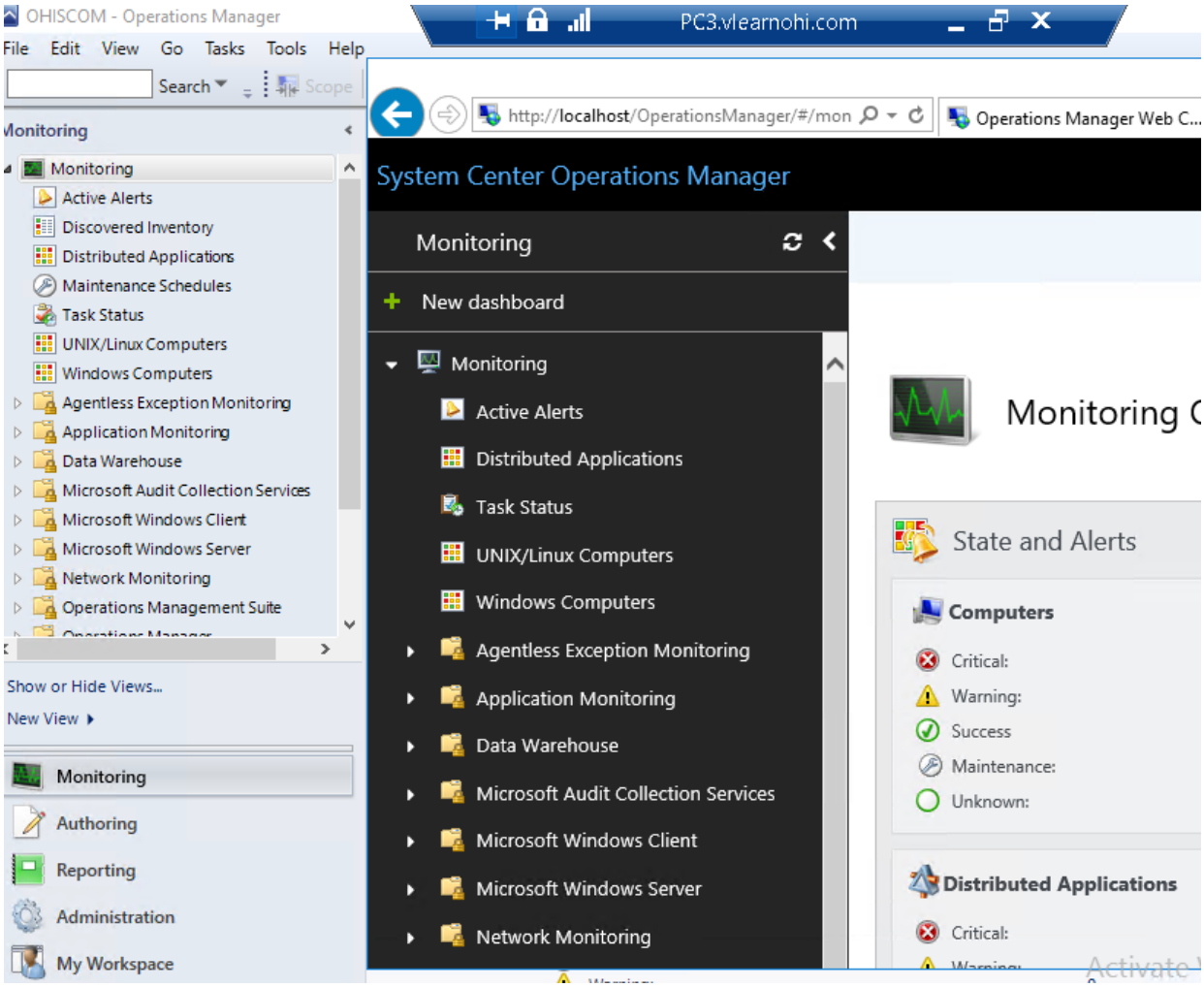


4. **Deploy SCOM Agents**
    - Use the SCOM console to deploy agents to the target computers.
    - Navigate to the "Administration" pane, and under "Device Management," select "Agent Managed."
    - Use the "Discovery Wizard" to discover and deploy agents to Windows and Linux computers.
    - Ensure the account used for agent deployment has administrative privileges on the target computers.
    - Verify that the agents are deployed and communicating with the management server.
5. **Configure Management Packs**
    - Import and configure management packs for the applications and services you want to monitor.
    - Navigate to the "Administration" pane, and under "Management Packs," select "Import Management Packs."
    - Browse and import the necessary management packs from the SCOM catalog or local storage.
6. **Set Up Dashboards and Reports**
    - Configure dashboards and reports to visualize monitoring data.
    - Navigate to the "Monitoring" pane to create and customize dashboards.
    - Use the "Reporting" pane to generate and schedule reports.

Post Installation Tasks and Configurations

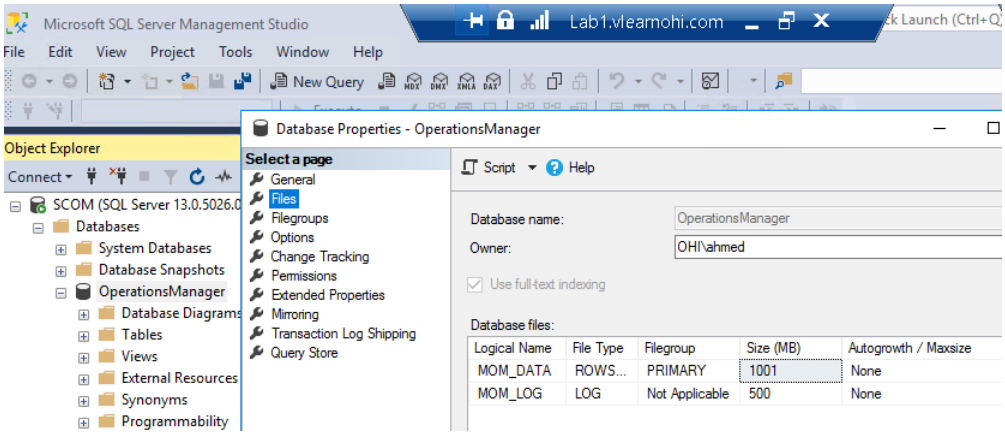
Operations Manager and Web Consoles

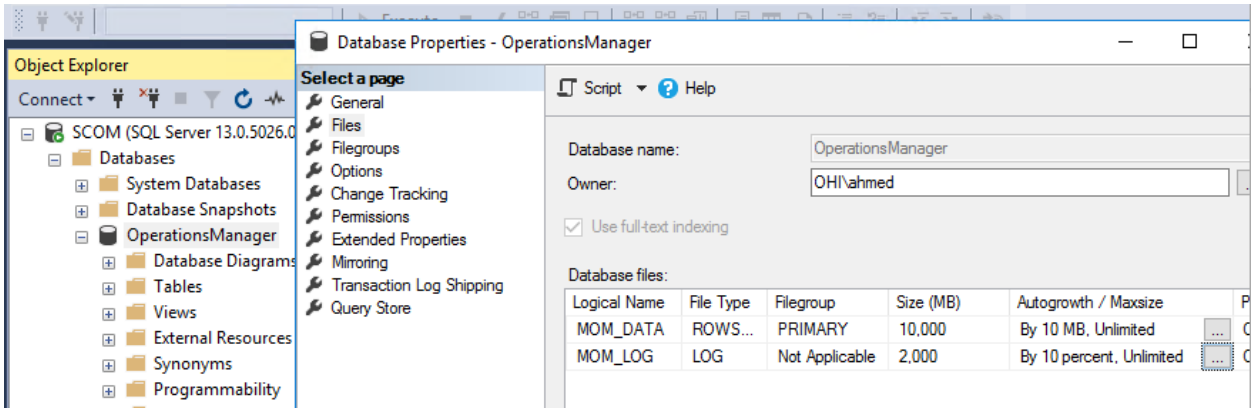
- **Web Console Access**: You can connect to SCOM through any web browser from any location.
- **Limited Administration Capabilities**: The web interface offers limited administration capabilities. For instance, you cannot create rules, alerts, or monitors through the web console.
- **Use for Monitoring**: The web interface is primarily used for monitoring purposes.
- **Differences Between Consoles**:
    - **Graphic Console**: Allows for configuration options for alerts.
    - **Web Console**: Does not allow configuration options for alerts.



Extending the SQL Operational Database Size

1. **Identify the Issue**:
   - After a week of running SCOM 2012 R2, you received errors indicating "Ops DB Free Space Low."
   - The default setting for the Operations Manager database is Autogrowth = None, which is not suitable for production environments.
2. **Steps to Resolve**:
   - **Change Autogrowth Settings**:
     - Open SQL Server Management Studio (SSMS).
     - Connect to your SCOM database instance.
     - Navigate to the OperationsManager database.
     - Right-click the database and select Properties.
     - Go to the Files page.
     - Locate the database files (e.g., MOM_DATA and MOM_LOG).
     - Set appropriate Autogrowth settings for each file. For example:
       - **MOM_DATA**: Change initial size to a larger value (e.g., 50 GB) and set autogrowth by a specific MB increment (e.g., 10 MB) or percentage.
       - **MOM_LOG**: Set an appropriate initial size and autogrowth setting similar to the data file.
3. **Example Configuration**:
   - **Data File (MOM_DATA)**:
     - Initial Size: 10,000 MB
     - Autogrowth: By 10 MB, Unlimited
   - **Log File (MOM_LOG)**:
     - Initial Size: 2,000 MB
     - Autogrowth: By 10%, Unlimited
4. **Implementation**:
   - Apply these settings during the initial installation or adjust them afterward to prevent running out of space.
   - Monitor the database size regularly to ensure it remains within acceptable limits.

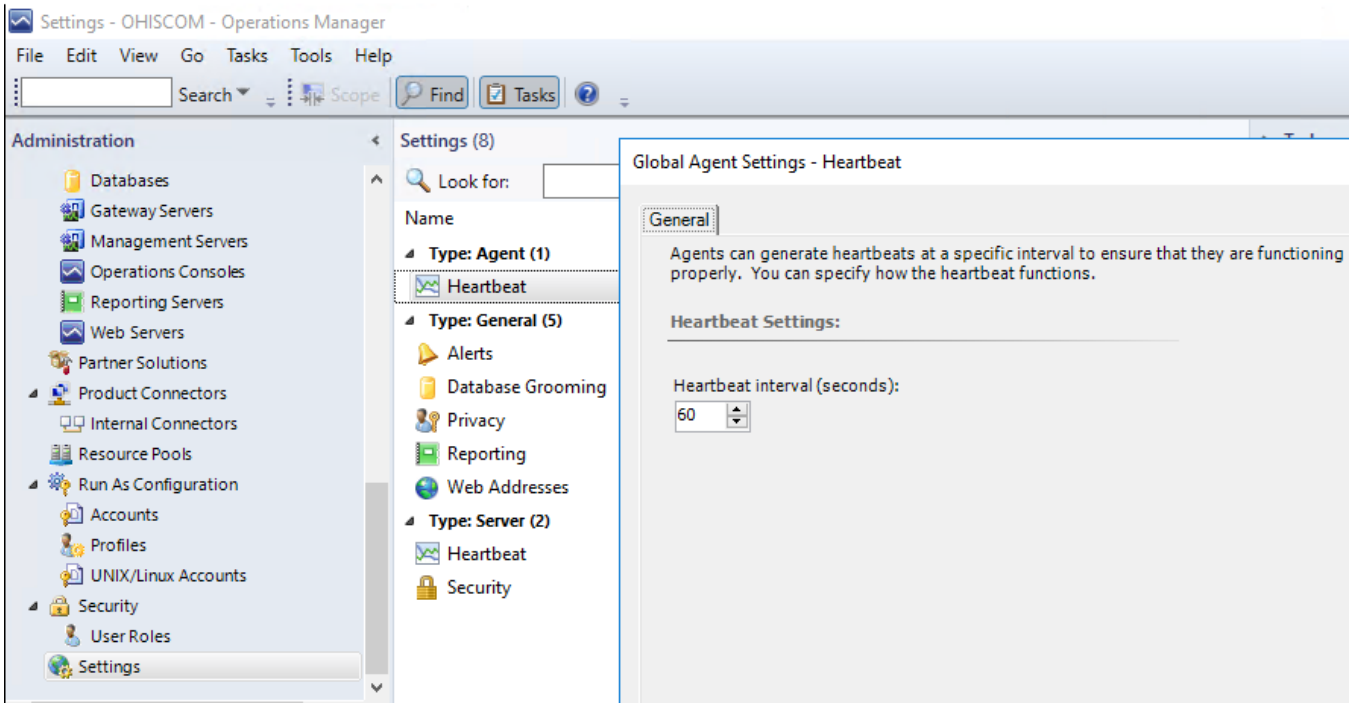


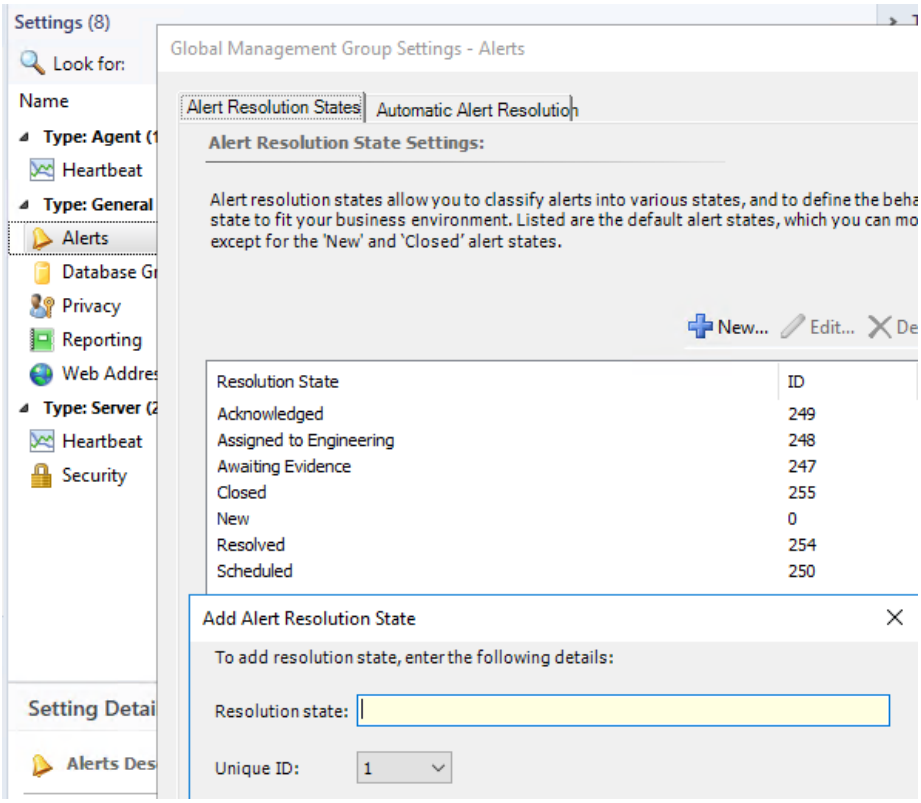


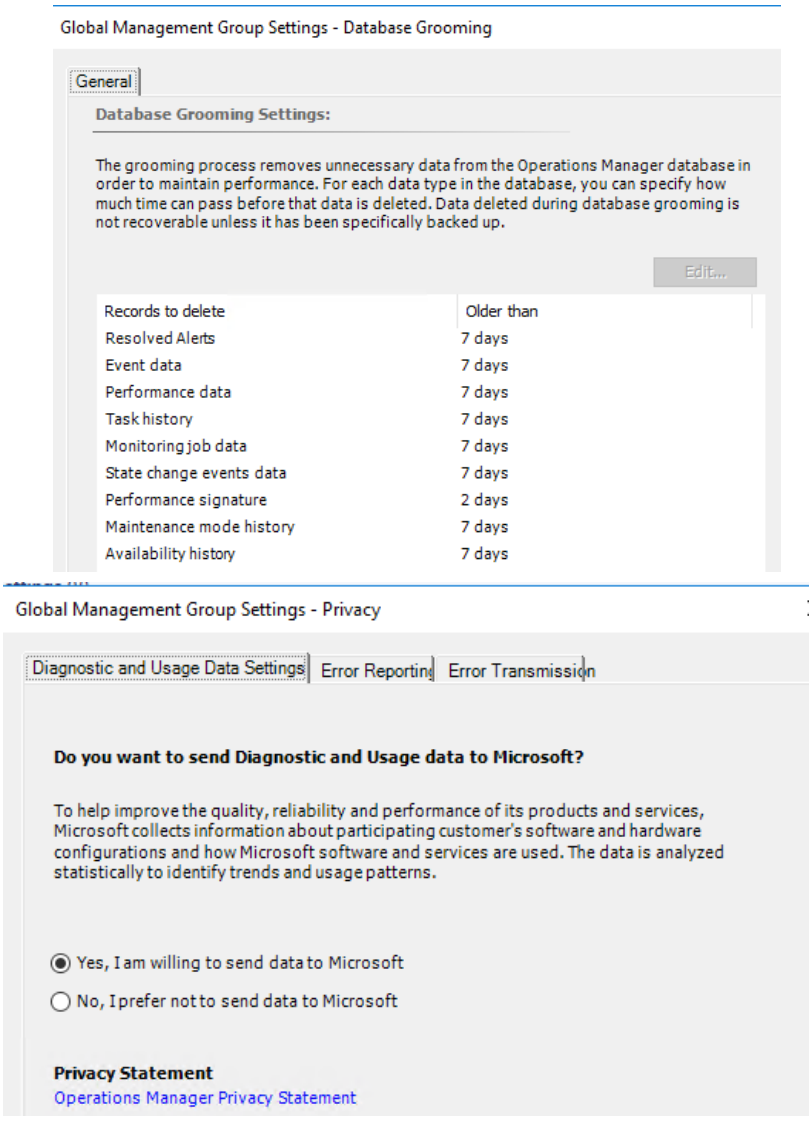
Configuring Global Settings in SCOM

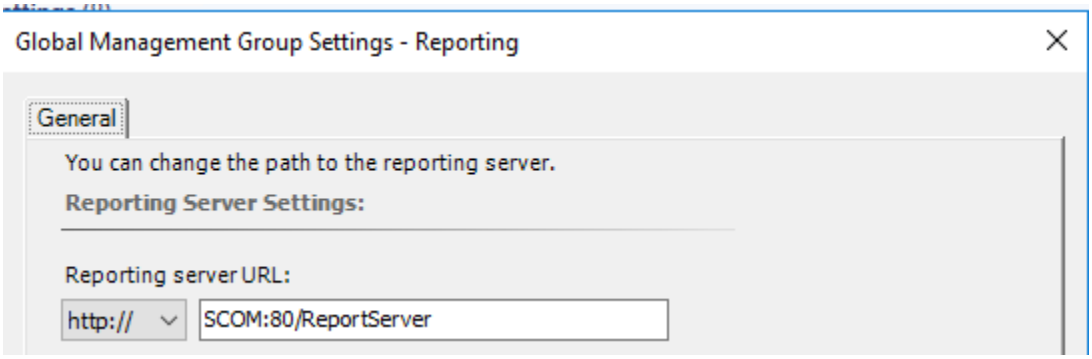
1. **Heartbeat Interval**:
   - Navigate to **Global Management Server Settings** > **Heartbeat**.
   - Set the number of missed heartbeats allowed before an alert is triggered. In your case, it's set to 3.
   - This setting ensures that the management server can ping the computer to diagnose issues if the agent stops sending heartbeats.
2. **Manual Agent Installations**:
   - Go to **Global Management Server Settings** > **Security**.
   - Choose how you want to handle manual agent installations:
     - **Reject new manual agent installations**: Ensures that only approved agents can be installed.
     - **Review new manual agent installations in pending management view**: Allows you to manually approve each new agent installation.
3. **Web Console and Alerts**:
   - Under **Global Management Group Settings** > **Web Addresses**:
     - Change the web console and online product knowledge URLs from HTTP to HTTPS for enhanced security.
     - For example:
       - Web console: https://SCOM.ohi.com/OperationsManager
       - Online product knowledge: https://SCOM.ohi.com/OperationsManager
     - Test the URLs to ensure they are correctly configured and accessible.
4. **Database Grooming**:
   - Determine how much operational data should be retained in the database to manage storage effectively.

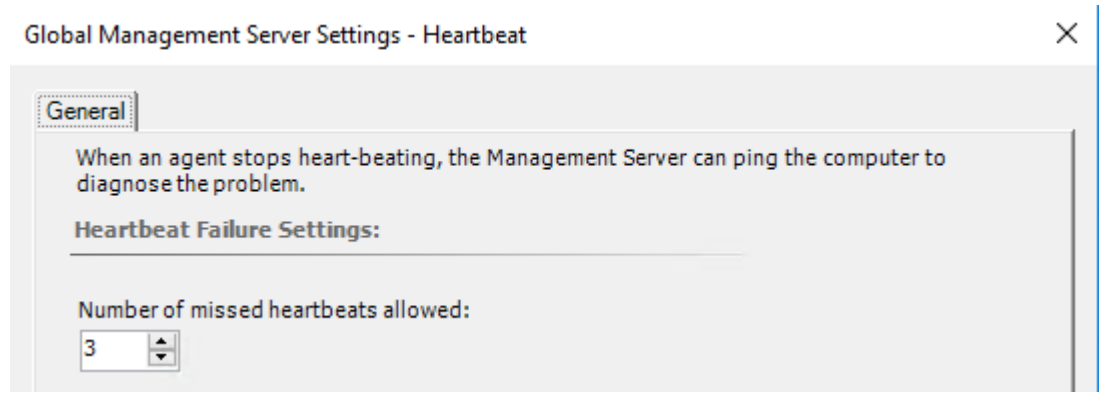
- Adjust the settings to groom old data from the database, ensuring it remains within manageable sizes and performance is optimized.

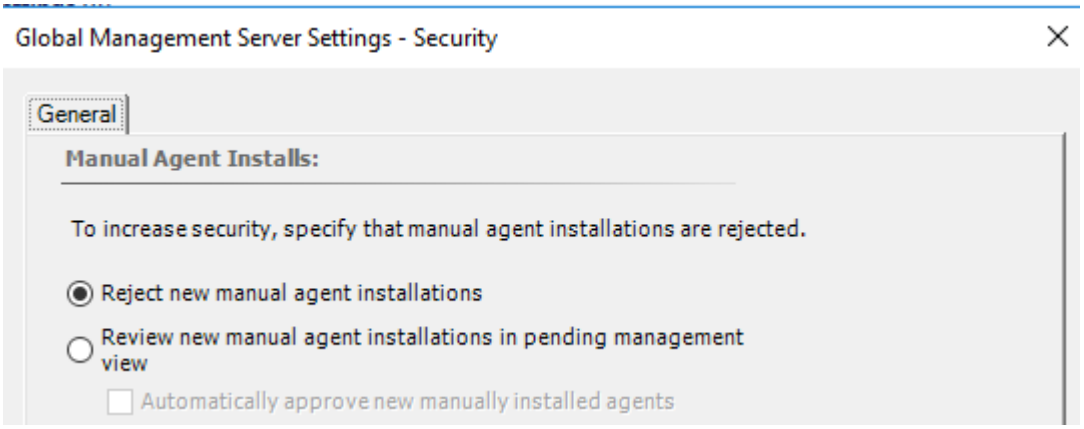


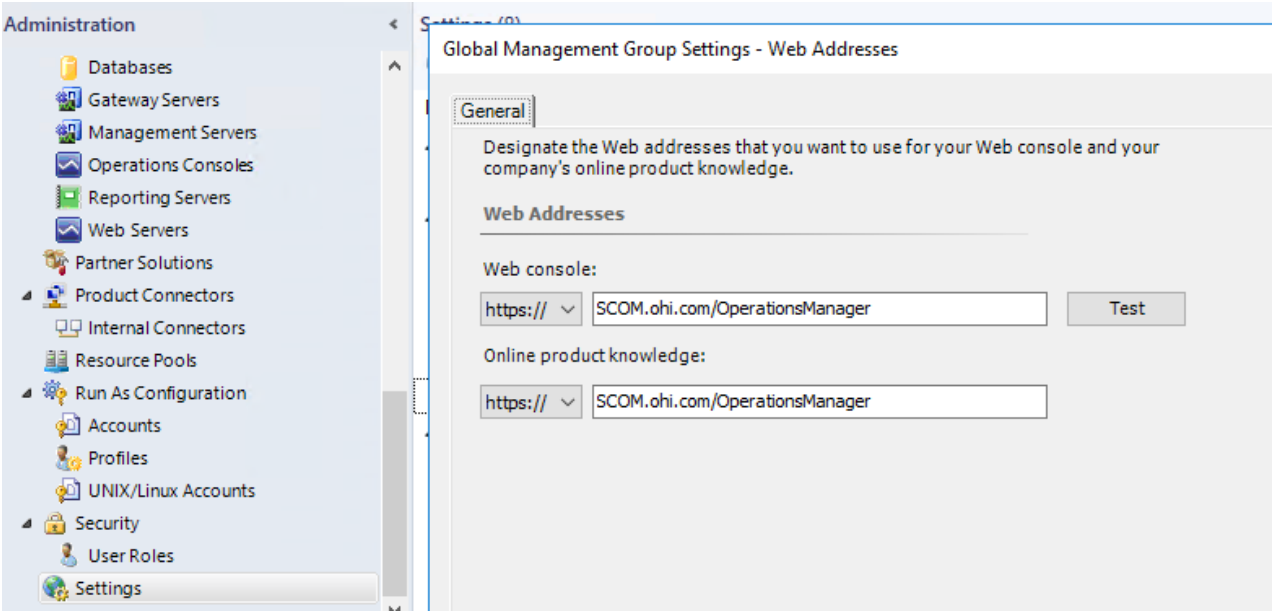



Global Management Group Settings - Database Grooming
General
Database Grooming Settings:
The grooming process removes unnecessary data from the Operations Manager database in order to maintain performance. For each data type in the database, you can specify how much time can pass before that data is deleted. Data deleted during database grooming is not recoverable unless it has been specifically backed up.
Edit...
Records to delete
Older than
Resolved Alerts
7 days
Event data
7 days
Performance data
7 days
Task history
7 days
Monitoring job data
7 days
State change events data
7 days
Performance signature
2 days
Maintenance mode history
7 days
Availability history
7 days
Global Management Group Settings - Privacy
Diagnostic and Usage Data Settings
Error Reporting
Error Transmission
Do you want to send Diagnostic and Usage data to Microsoft?
To help improve the quality, reliability and performance of its products and services, Microsoft collects information about participating customer's software and hardware configurations and how Microsoft software and services are used. The data is analyzed statistically to identify trends and usage patterns.
Yes, I am willing to send data to Microsoft
No, I prefer not to send data to Microsoft
Privacy Statement
Operations Manager Privacy Statement


Global Management Group Settings - Reporting
General
You can change the path to the reporting server.
Reporting Server Settings:
Reporting server URL:
http://
SCOM:80/ReportServer

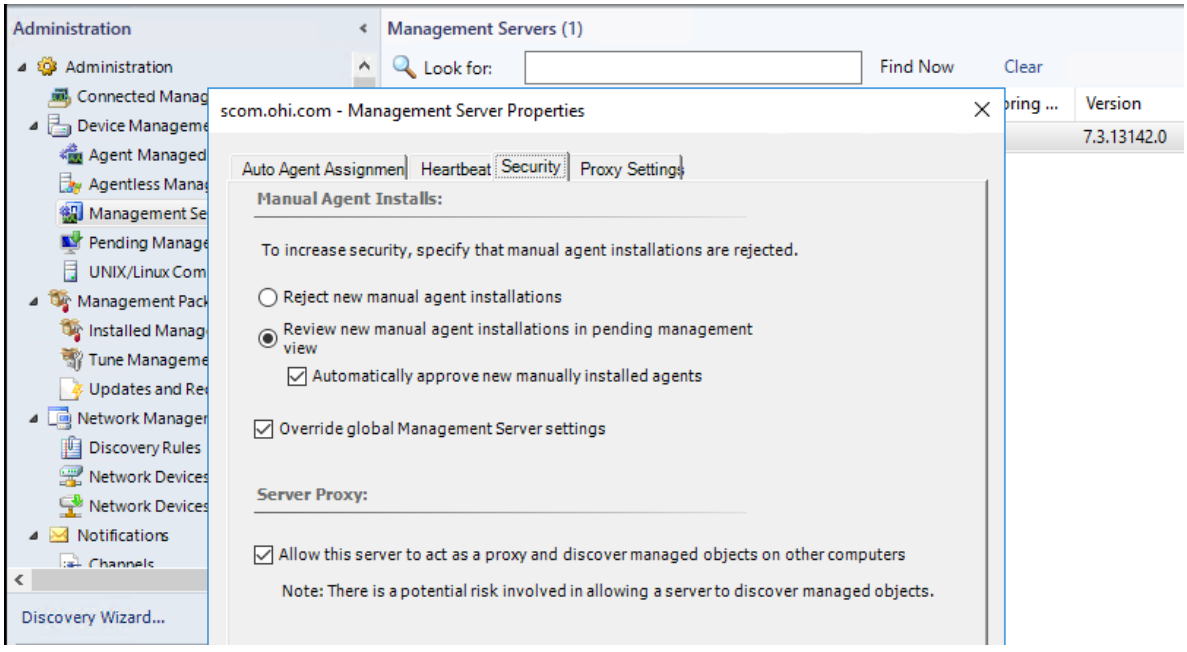

Global Management Server Settings - Heartbeat
General
When an agent stops heart-beating, the Management Server can ping the computer to diagnose the problem.
Heartbeat Failure Settings:
Number of missed heartbeats allowed:
3


Global Management Server Settings - Security
General
Manual Agent Installs:
To increase security, specify that manual agent installations are rejected.
Reject new manual agent installations
Review new manual agent installations in pending management view
Automatically approve new manually installed agents


Administration
Databases
Gateway Servers
Management Servers
Operations Consoles
Reporting Servers
Web Servers
Partner Solutions
Product Connectors
Internal Connectors
Resource Pools
Run As Configuration
Accounts
Profiles
UNIX/Linux Accounts
Security
User Roles
Settings
Global Management Group Settings - Web Addresses
General
Designate the Web addresses that you want to use for your Web console and your company's online product knowledge.
Web Addresses
Web console:
https://
SCOM.ohi.com/OperationsManager
Test
Online product knowledge:
https://
SCOM.ohi.com/OperationsManager

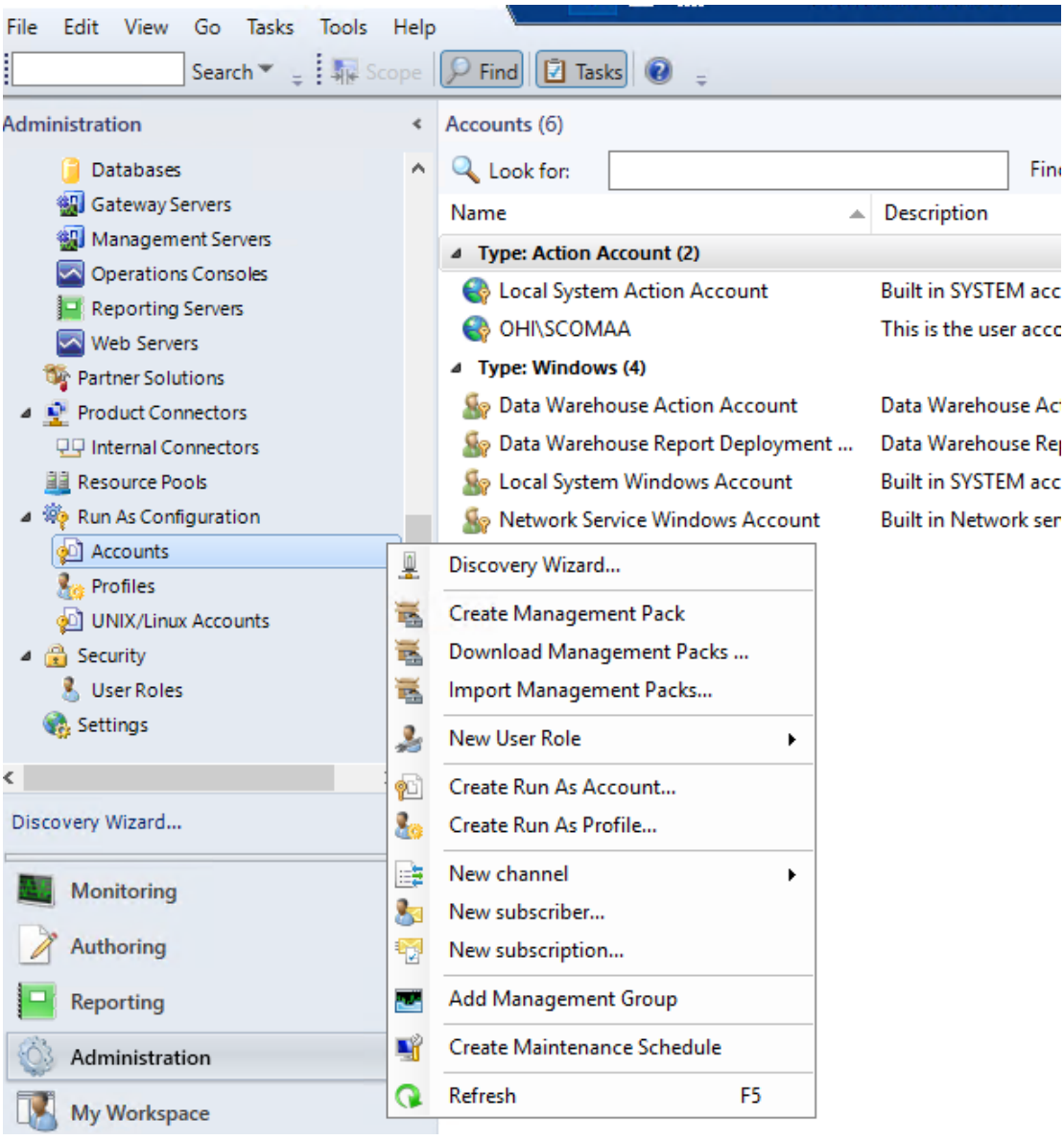
Management Server Properties - Security Settings

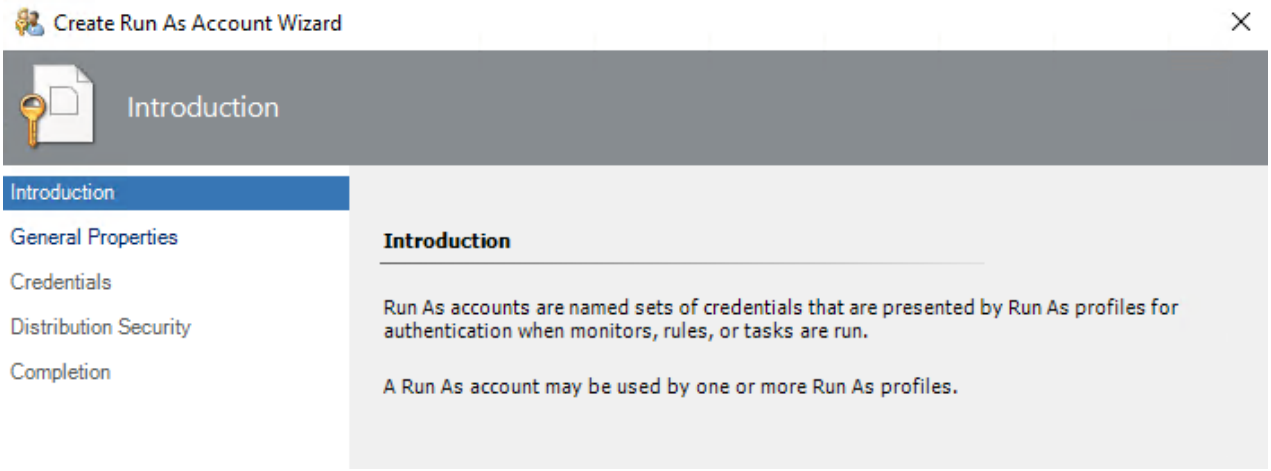
1. **Manual Agent Installs**:
    - **Reject new manual agent installations**: This option increases security by preventing any manual installations of agents that have not been pre-approved.
    - **Review new manual agent installations in pending management view**: Allows administrators to manually approve or reject new agent installations. This option is selected in your screenshot.
        - **Automatically approve new manually installed agents**: If selected, it will automatically approve new agents, but this is not enabled in your configuration.
    - **Override global Management Server settings**: Allows this server's settings to override the global settings for manual agent installations.
2. **Server Proxy:**
    - **Allow this server to act as a proxy and discover managed objects on other computers**: This setting enables the management server to act as a proxy, allowing it to discover and manage objects on other computers. Note the potential security risk involved in enabling this feature as it allows more extensive network discovery.

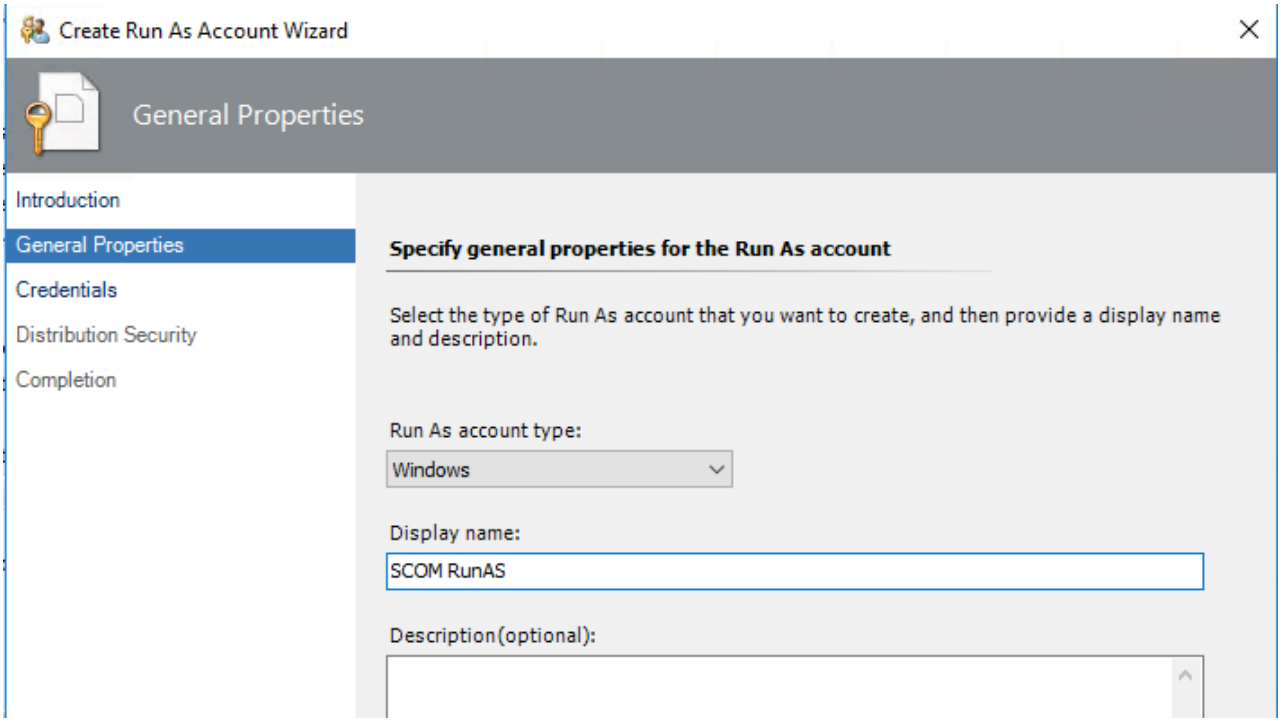


Run As Accounts

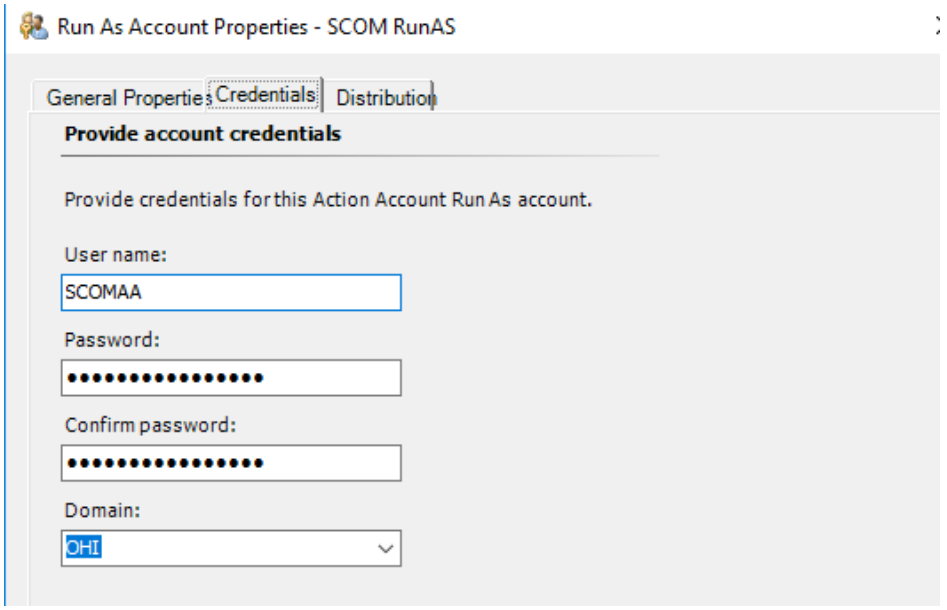
"Run As" accounts define which credentials will be used for specific actions carried out by the Operations Manager agent. These accounts are managed centrally through the Operations console and are assigned to different "Run As" profiles. If a specific action does not have an assigned "Run As" profile, it will default to using the Default Action account.

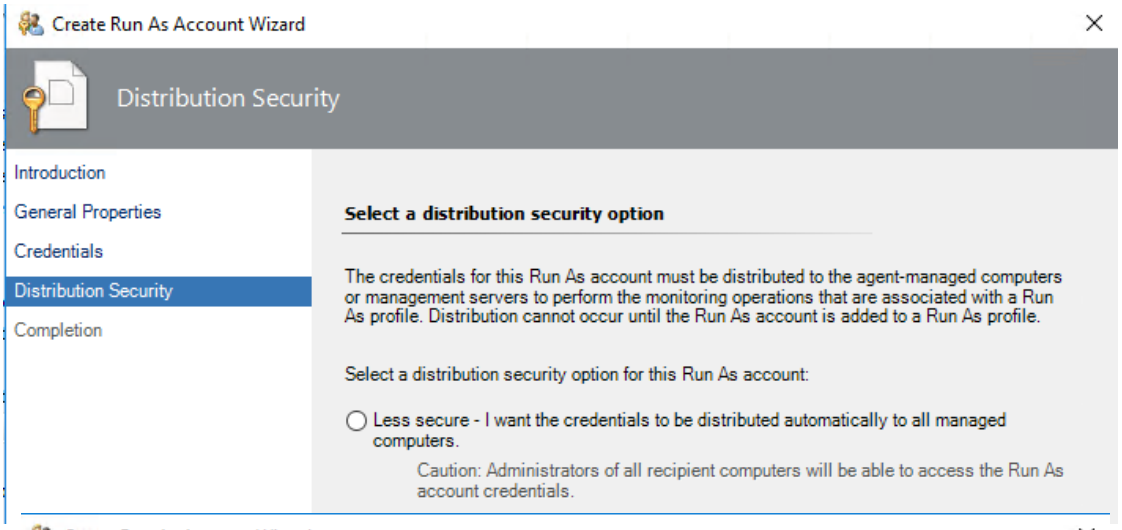


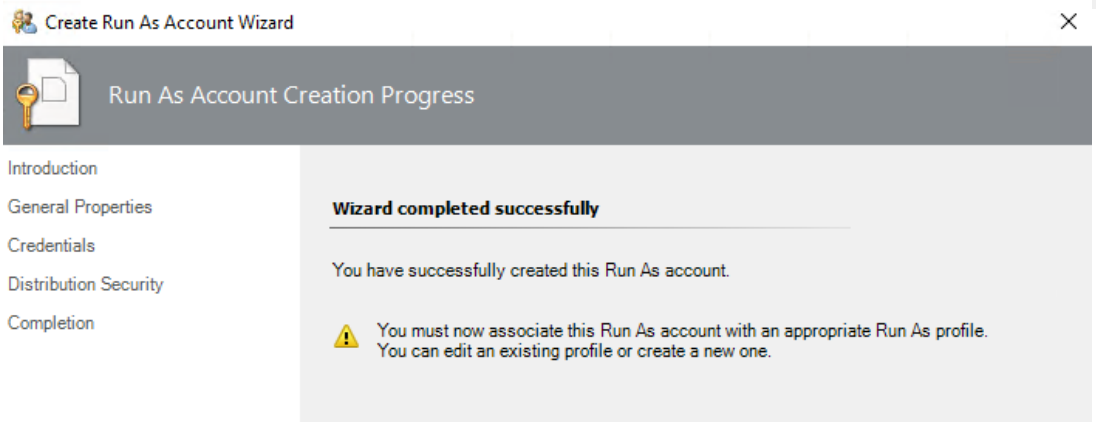

Create Run As Account Wizard
Introduction
Introduction
General Properties
Credentials
Distribution Security
Completion
Introduction
Run As accounts are named sets of credentials that are presented by Run As profiles for authentication when monitors, rules, or tasks are run.
A Run As account may be used by one or more Run As profiles.


Create Run As Account Wizard
General Properties
Introduction
General Properties
Credentials
Distribution Security
Completion
Specify general properties for the Run As account
Select the type of Run As account that you want to create, and then provide a display name and description.
Run As account type:
Windows
Display name:
SCOM RunAS
Description (optional):

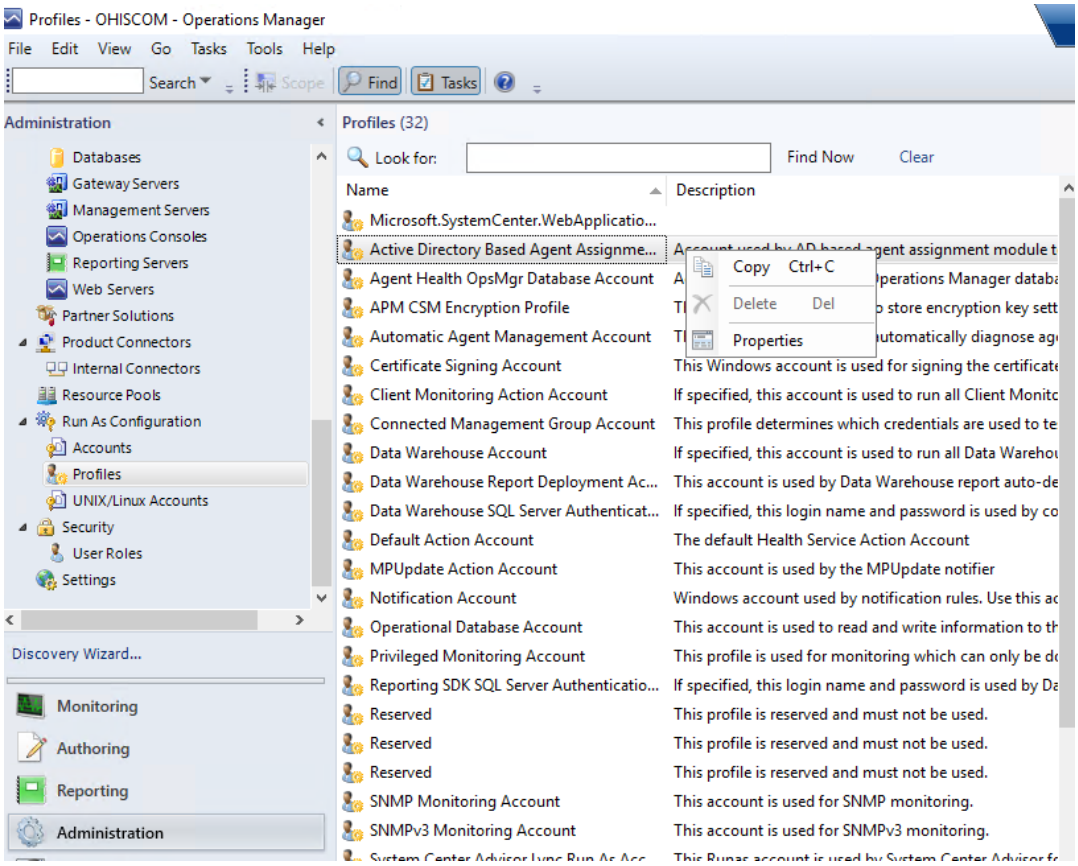
The same Action Acount

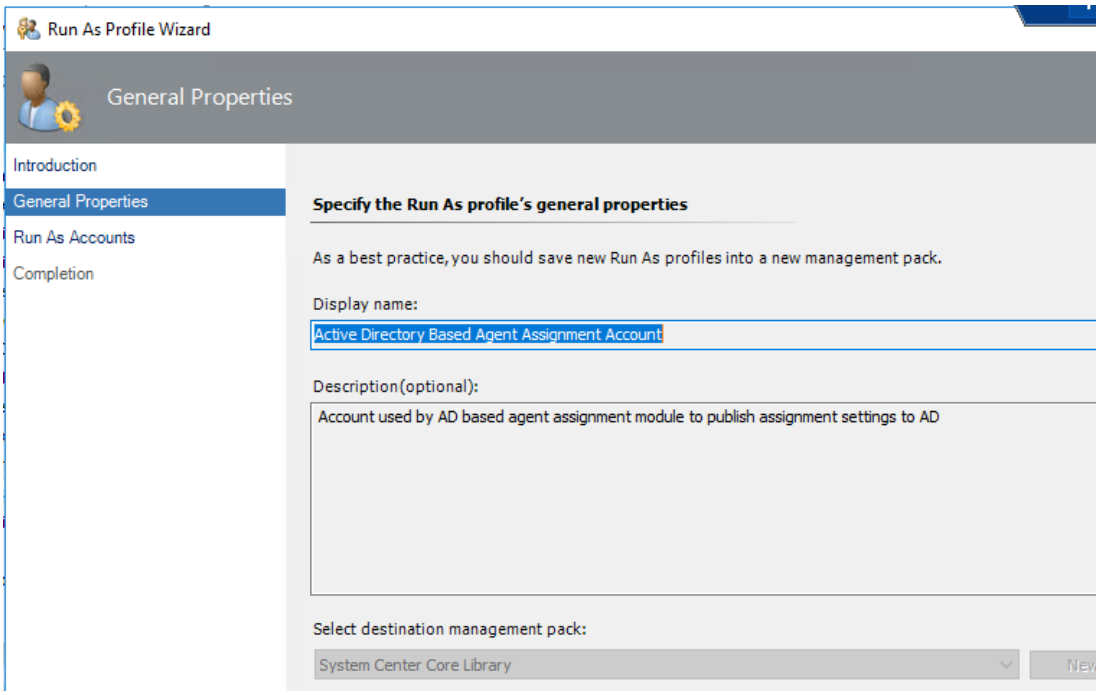


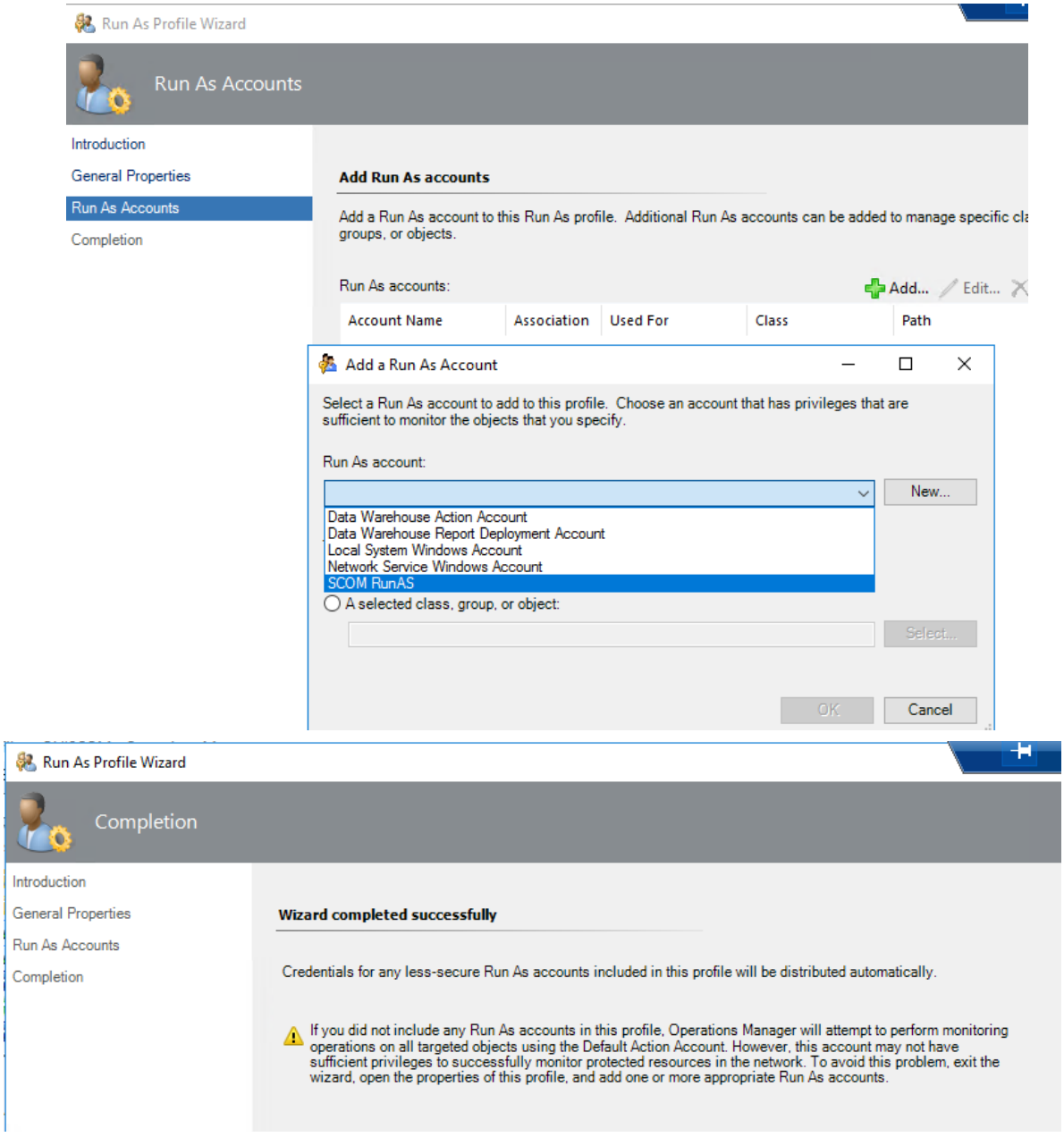




Next, include this account in AD for agent evaluations.






Run As Profile Wizard
Run As Accounts
Introduction
General Properties
Run As Accounts
Completion
Add Run As accounts
Add a Run As account to this Run As profile. Additional Run As accounts can be added to manage specific cla
groups, or objects.
Run As accounts:
Add...
Edit...
Account Name
Association
Used For
Class
Path
Add a Run As Account
Select a Run As account to add to this profile. Choose an account that has privileges that are
sufficient to monitor the objects that you specify.
Run As account:
New...
Data Warehouse Action Account
Data Warehouse Report Deployment Account
Local System Windows Account
Network Service Windows Account
SCOM RunAS
A selected class, group, or object:
Select...
OK
Cancel
Run As Profile Wizard
Completion
Introduction
General Properties
Run As Accounts
Completion
Wizard completed successfully
Credentials for any less-secure Run As accounts included in this profile will be distributed automatically.
If you did not include any Run As accounts in this profile, Operations Manager will attempt to perform monitoring
operations on all targeted objects using the Default Action Account. However, this account may not have
sufficient privileges to successfully monitor protected resources in the network. To avoid this problem, exit the
wizard, open the properties of this profile, and add one or more appropriate Run As accounts.

Installing SCOM Agent

To install the SCOM agent on supported systems, follow these steps:

Prerequisites

1. **Add SCOMAG to Local Admin Group**: Ensure that the SCOMAG account is a member of the local administrators group on all target computers.
2. **Supported Systems**: The installation is supported from Windows Vista SP2 onwards.
3. **Network Configuration**

   Port Requirements

   - **TCP 5723**: For OpsMgr Windows agent communication.
   - **TCP 135**: RPC Endpoint Mapper for push installations.
   - **UDP 137**: NetBIOS Name Service for push installations.
   - **UDP 138**: NetBIOS Datagram Service for push installations.
   - **TCP/UDP 445**: SMB for push installations.
   - **TCP 139**: NetBIOS Session Service for push repairs.

These ports must be open on both Windows Firewall and hardware firewall to facilitate communication and installation processes.

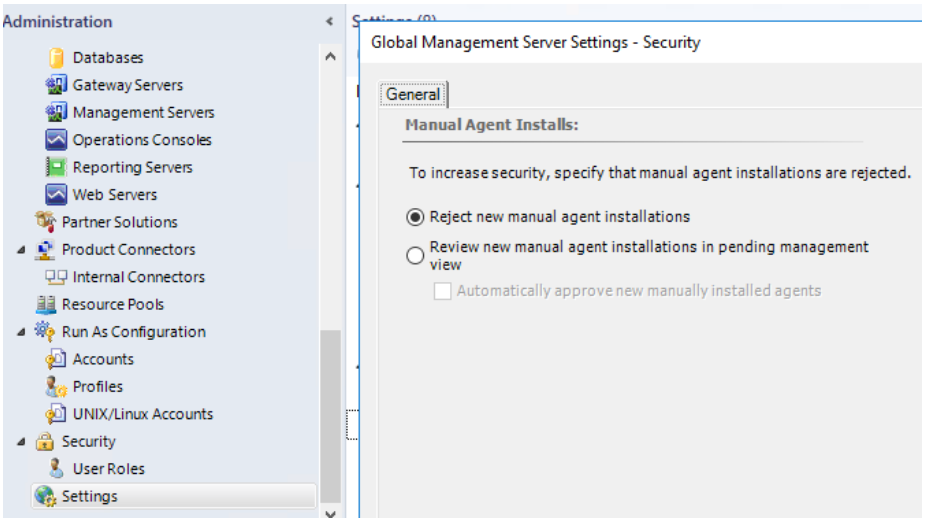
Manual Installation Steps

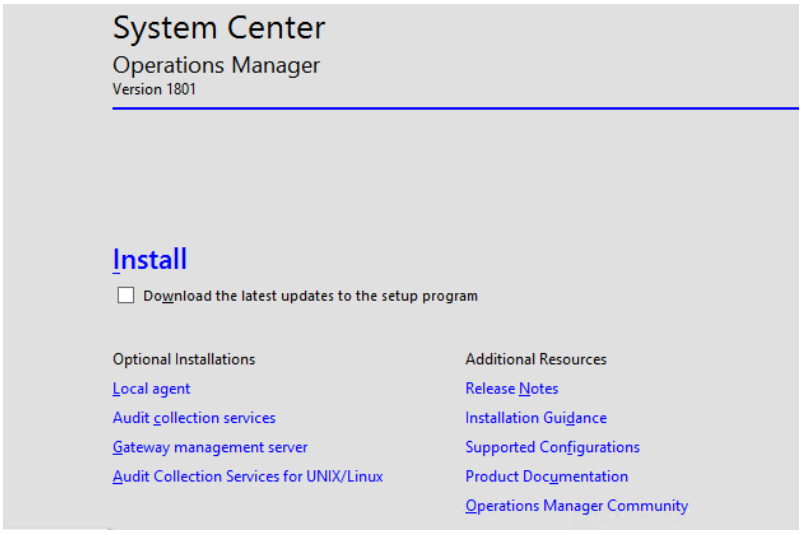
1. **To manually install, you must first activate it from the security settings.**
2. **Navigate to the Installation Directory**:

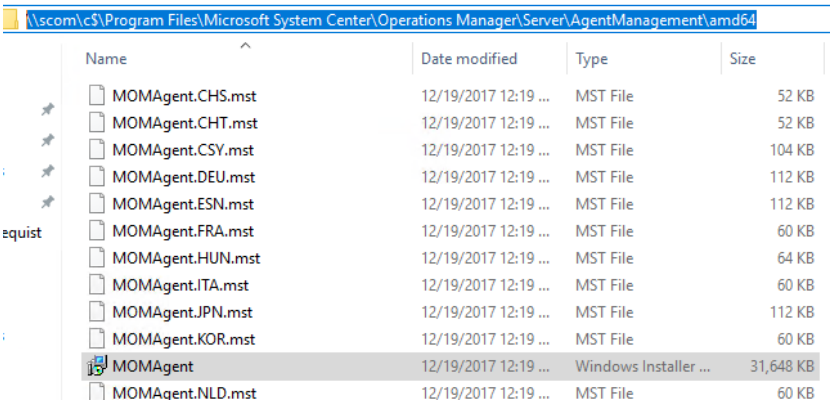
   On the SCOM server, go to the `\agent\momagent` directory where the agent installation files are located. Or from DVD Media run local agent



3. **Run the Installer**:
   - Execute the agent installer `(MOMAgent.msi)` on the target computer.
   - Follow the on-screen instructions to complete the installation.
4. **Configure the Agent**:
   - After installation, configure the agent to communicate with the appropriate SCOM management server.





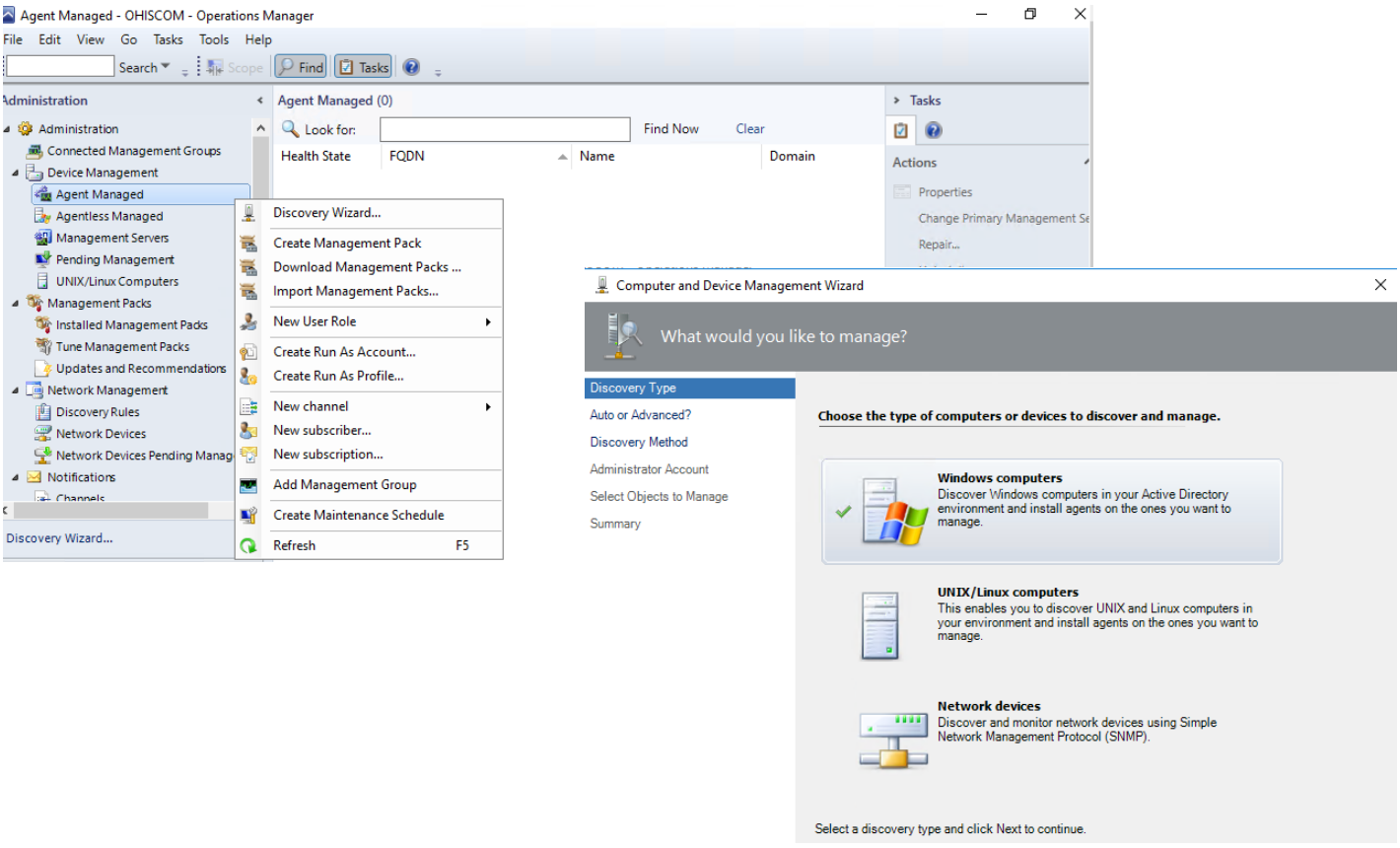


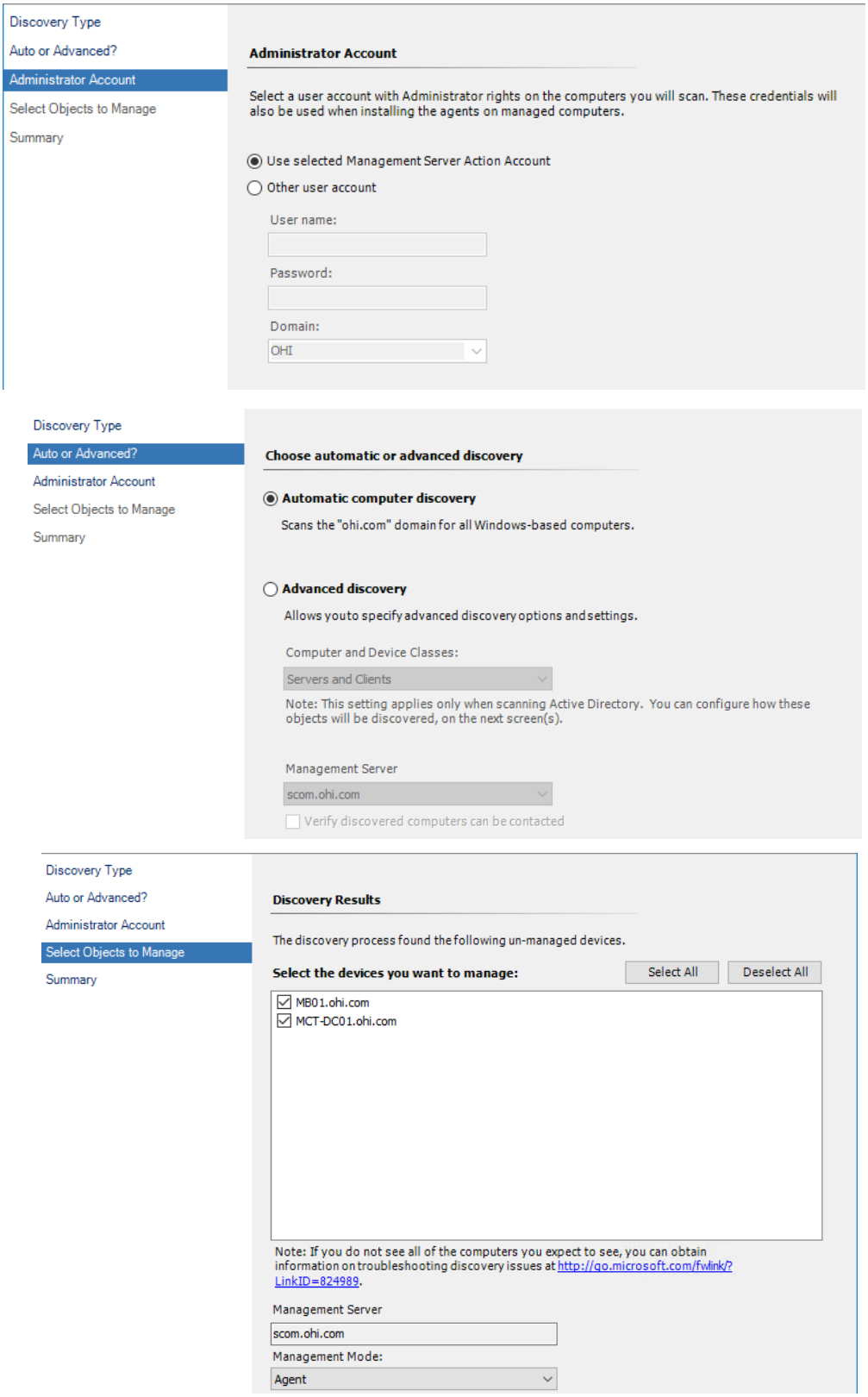
Deploying Agents Using the Discovery Wizard

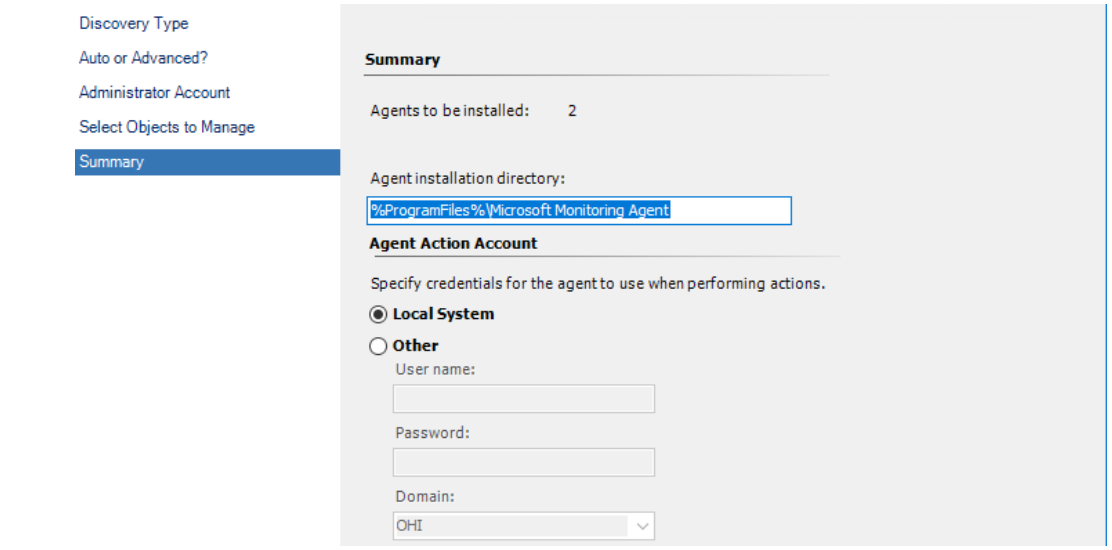
1. **Open Operations Manager Console**:
   - Go to the Administration workspace.
2. **Agent Managed**:
   - In the Administration workspace, click on Agent Managed.
3. **Discovery Wizard**:
   - Click on the Discovery Wizard... option to launch the wizard.
4. **Choose Discovery Type**:
   - Select Windows computers, UNIX/Linux computers, or Network devices depending on the target systems.
5. **Discovery Method**:
   - Choose either Automatic computer discovery to scan the domain or Advanced discovery for specific configurations.
6. **Administrator Account**:
   - Provide credentials with administrator rights for the target computers.

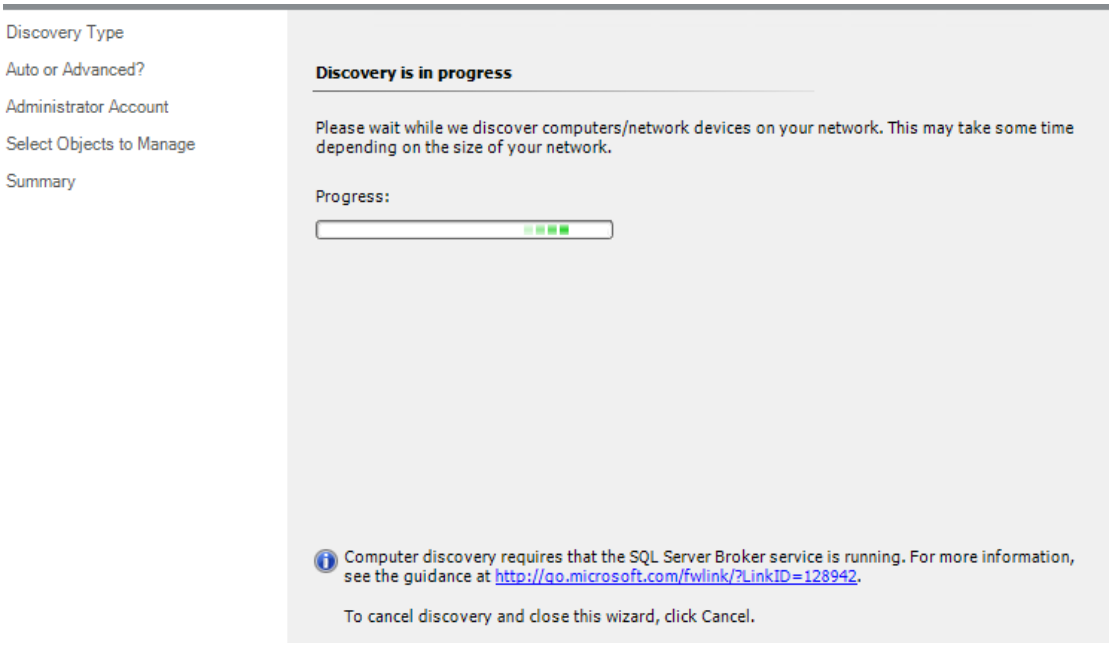
7. **Discovery in Progress**:
    - The wizard will search for computers and network devices on the network.
8. **Select Objects to Manage**:
    - From the discovery results, select the devices you want to manage.

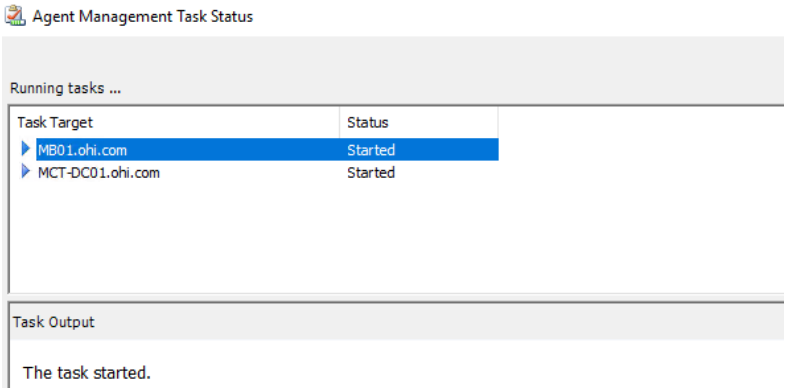
9. **Install Agents**:
    - Confirm the installation directory and agent action account details.
    - Start the installation process.
10. **Monitor Installation**:
    - The status of the agent deployment will be displayed, ensuring that the installation completes successfully.

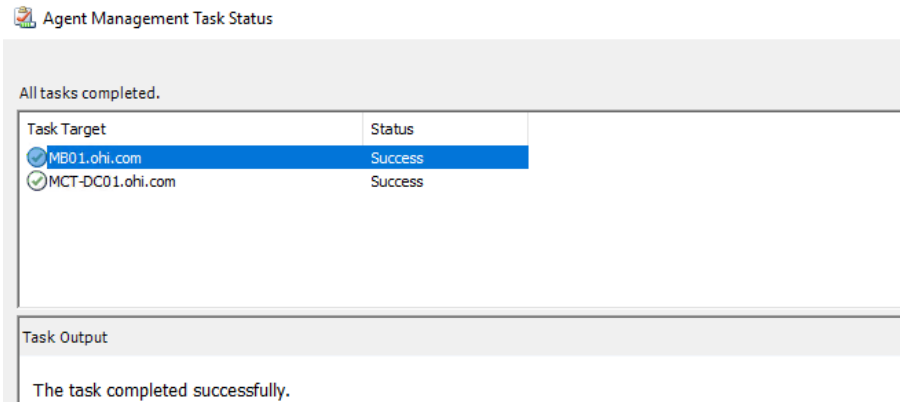



Discovery Type
Auto or Advanced?
Administrator Account
Select Objects to Manage
Summary
Administrator Account
Select a user account with Administrator rights on the computers you will scan. These credentials will also be used when installing the agents on managed computers.
Use selected Management Server Action Account
Other user account
User name:
Password:
Domain:
OHI
Discovery Type
Auto or Advanced?
Administrator Account
Select Objects to Manage
Summary
Choose automatic or advanced discovery
Automatic computer discovery
Scans the "ohi.com" domain for all Windows-based computers.
Advanced discovery
Allows you to specify advanced discovery options and settings.
Computer and Device Classes:
Servers and Clients
Note: This setting applies only when scanning Active Directory. You can configure how these objects will be discovered, on the next screen(s).
Management Server
scom.ohi.com
Verify discovered computers can be contacted
Discovery Type
Auto or Advanced?
Administrator Account
Select Objects to Manage
Summary
Discovery Results
The discovery process found the following un-managed devices.
Select the devices you want to manage:
Select All
Deselect All
MB01.ohi.com
MCT-DC01.ohi.com
Note: If you do not see all of the computers you expect to see, you can obtain information on troubleshooting discovery issues at http://go.microsoft.com/fwlink/?LinkID=824989.
Management Server
scom.ohi.com
Management Mode:
Agent


Discovery Type
Auto or Advanced?
Administrator Account
Select Objects to Manage
Summary
Summary
Agents to be installed: 2
Agent installation directory:
%ProgramFiles%\Microsoft Monitoring Agent
Agent Action Account
Specify credentials for the agent to use when performing actions.
Local System
Other
User name:
Password:
Domain:
OHI


Discovery Type
Auto or Advanced?
Administrator Account
Select Objects to Manage
Summary
Discovery is in progress
Please wait while we discover computers/network devices on your network. This may take some time depending on the size of your network.
Progress:
Computer discovery requires that the SQL Server Broker service is running. For more information, see the guidance at http://go.microsoft.com/fwlink/?LinkID=128942.
To cancel discovery and close this wizard, click Cancel.

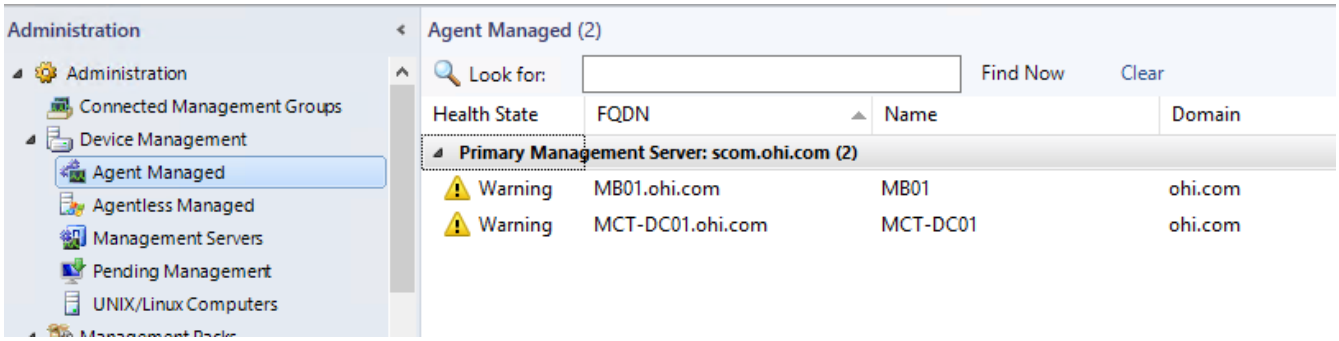

Agent Management Task Status
Running tasks ...
Task Target
Status
MB01.ohi.com
Started
MCT-DC01.ohi.com
Started
Task Output
The task started.

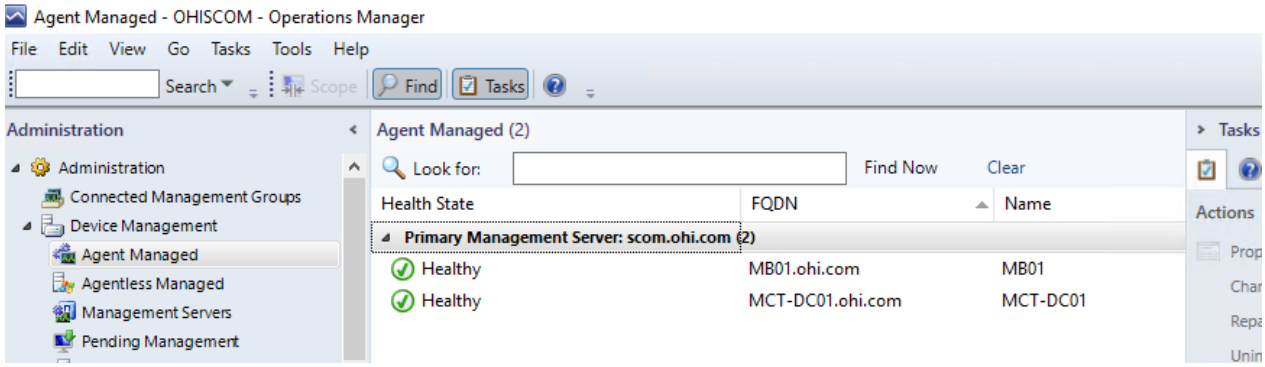


Post-Installation Configuration

After deploying the agents, ensure the following:

- **Agent Assignment**: Configure each agent to report to the correct SCOM management server.
- **Verification**: Check the Operations Manager console to verify that all agents are communicating correctly.





Implementing Active Directory integration

Integrating System Center Operations Manager **(SCOM)** with Active Directory **(AD)** can streamline the management of agent assignments and enhance the monitoring capabilities. Here are the steps to implement AD integration in SCOM:

Prerequisites

1. **Active Directory Domain Services (AD DS)**: Ensure that the AD DS role is installed and configured.
2. **SCOM Administrator Rights**: Ensure you have administrative rights on the SCOM management server.

Step 1: Create AD Container for SCOM

1. **Open Command Prompt as Administrator**:
   - Right-click the Command Prompt and select Run as administrator.
2. **Run the MOMADAdmin.exe Command**:

```
"C:\Program Files\Microsoft System Center 2016\Operations Manager\Server\MOMADAdmin.exe" Path\MOMADAdmin.exe MBOM ohi\OMAdmins ohi\administrator ohi.com
```

   - Adjust the paths, domain names, and organizational unit as necessary for your environment.

Step 2: Delegate Control to SCOM

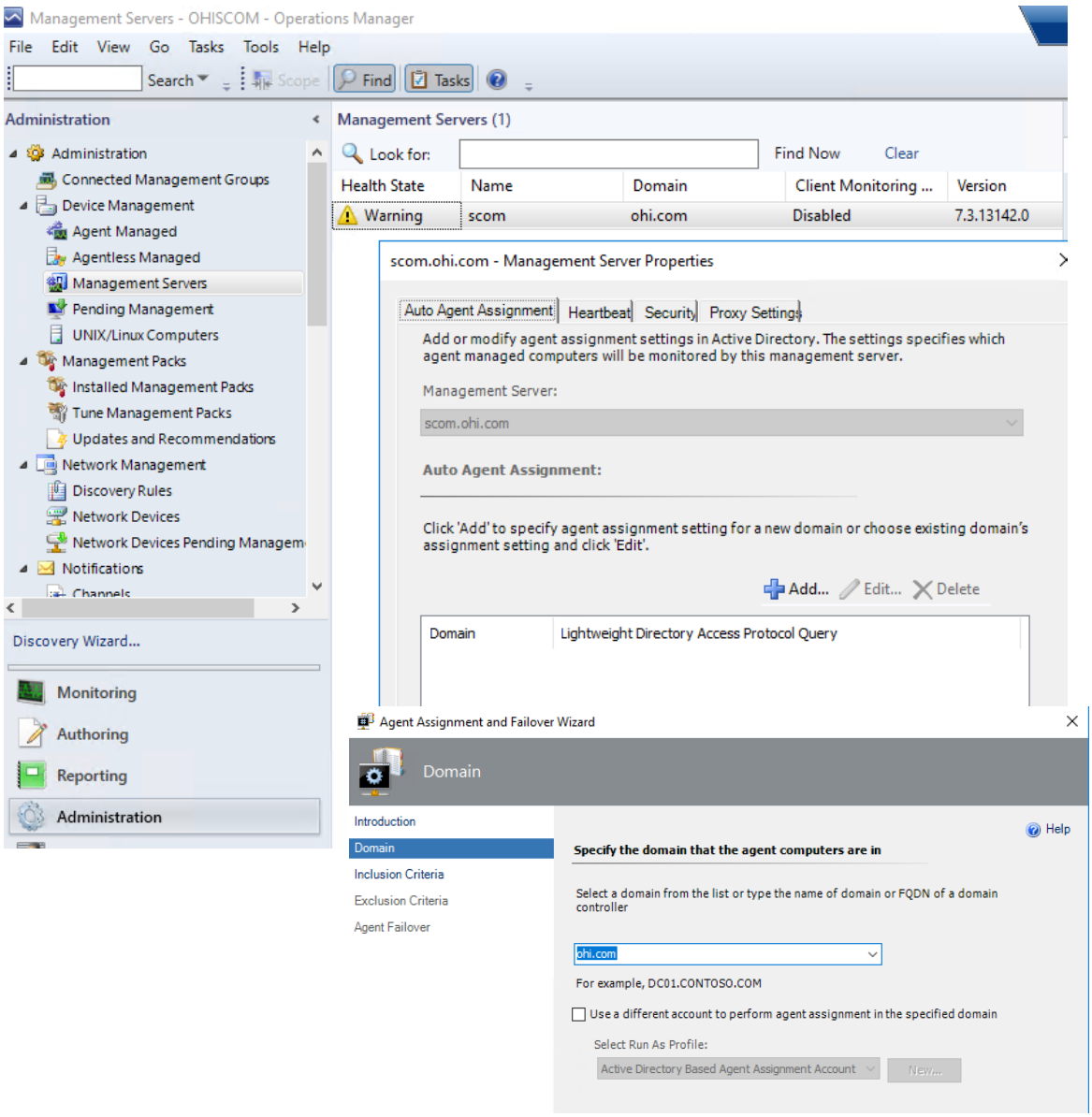
1. **Open Active Directory Users and Computers**:
   - Open the Active Directory Users and Computers console.
2. **Create Organizational Unit (OU)**:
   - Right-click the domain or an existing OU and select New > Organizational Unit.
   - Name the new OU (e.g., SCOM).
3. **Delegate Control**:
   - Right-click the new OU and select Delegate Control.
   - Use the Delegation of Control Wizard to delegate permissions to the SCOM management server's computer account. Grant full control over the container.

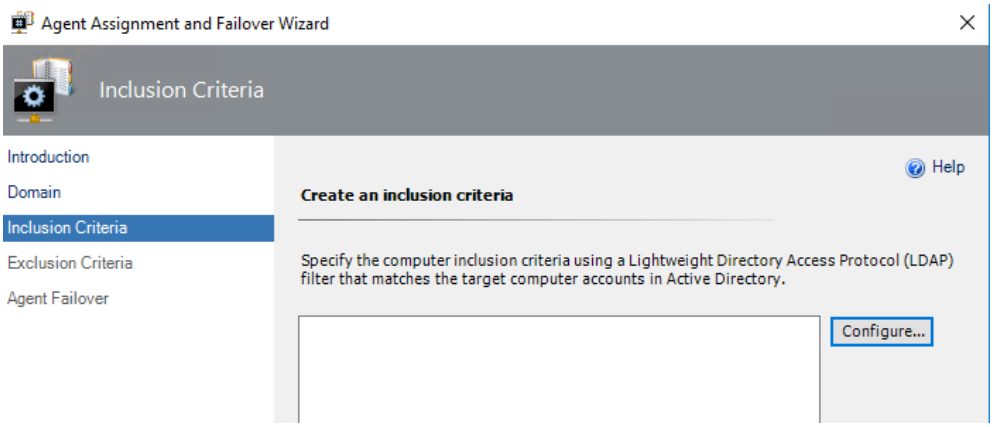
Step 3: Configure AD Integration in SCOM

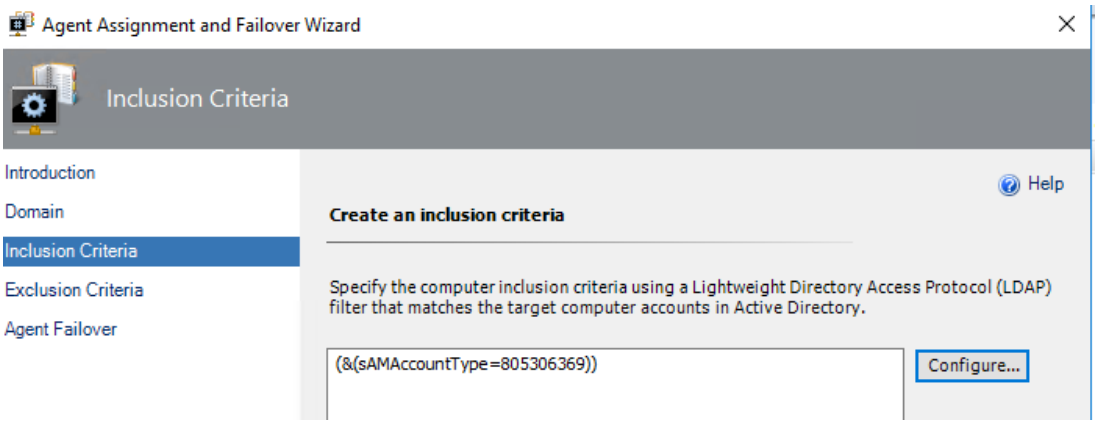
1. **Open Operations Manager Console**:
   - Launch the Operations Manager console.
   - Navigate to the Administration workspace.
2. **Set Up Active Directory Integration Account**:
   - In the Administration workspace, navigate to Run As Configuration > Accounts.
   - Right-click Accounts and select Create Run As Account.
   - Follow the wizard to create an AD Integration Run As Account. Use an account that has appropriate permissions in AD.
3. **Configure AD Integration**:
   - In the Administration workspace, navigate to Active Directory Integration.
   - Right-click and select Create Active Directory Integration Connection.
   - Follow the wizard to specify the AD container created earlier and the Run As Account.

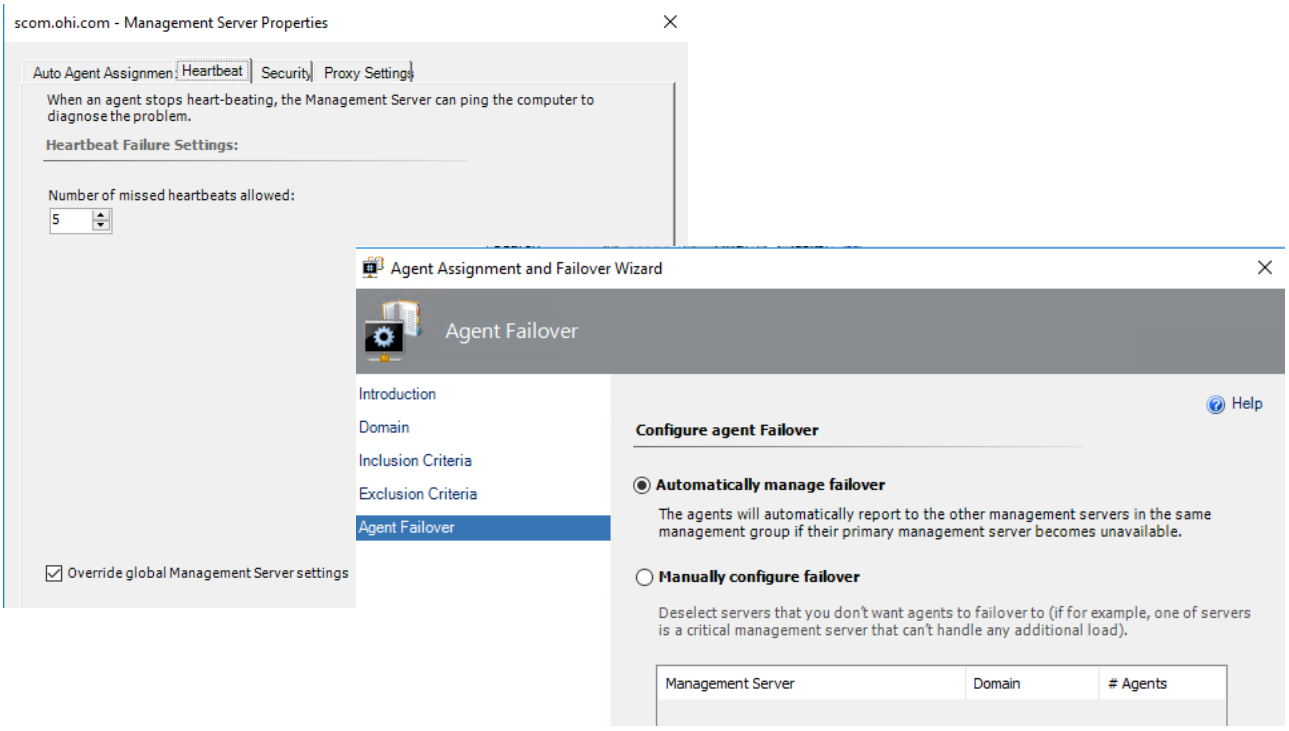
Step 4: Publish SCOM Management Group to AD

1. **Enable Auto Agent Assignment**:
   - In the Administration workspace, select Management Servers.
   - Right-click on the management server and select Properties.
   - Navigate to the Auto Agent Assignment tab.
   - Check the box to enable automatic agent assignment and select the appropriate AD container.
2. **Publish Management Group Information**:
   - In the Administration workspace, navigate to Active Directory Integration.
   - Right-click on Active Directory Integration and select Create Management Group Connection.
   - Follow the wizard to publish the SCOM management group information to the specified AD container.




Agent Assignment and Failover Wizard
Inclusion Criteria
Introduction
Domain
Inclusion Criteria
Exclusion Criteria
Agent Failover
Help
Create an inclusion criteria
Specify the computer inclusion criteria using a Lightweight Directory Access Protocol (LDAP) filter that matches the target computer accounts in Active Directory.
Configure...


Agent Assignment and Failover Wizard
Inclusion Criteria
Introduction
Domain
Inclusion Criteria
Exclusion Criteria
Agent Failover
Help
Create an inclusion criteria
Specify the computer inclusion criteria using a Lightweight Directory Access Protocol (LDAP) filter that matches the target computer accounts in Active Directory.
(&(sAMAccountType=805306369))
Configure...


scom.ohi.com - Management Server Properties
Auto Agent Assignmen
Heartbeat
Security
Proxy Settings
When an agent stops heart-beating, the Management Server can ping the computer to diagnose the problem.
Heartbeat Failure Settings:
Number of missed heartbeats allowed:
5
Override global Management Server settings
Agent Assignment and Failover Wizard
Agent Failover
Introduction
Domain
Inclusion Criteria
Exclusion Criteria
Agent Failover
Help
Configure agent Failover
Automatically manage failover
The agents will automatically report to the other management servers in the same management group if their primary management server becomes unavailable.
Manually configure failover
Deselect servers that you don't want agents to failover to (if for example, one of servers is a critical management server that can't handle any additional load).
Management Server
Domain
Agents

Step 5: Assign Computers to Management Servers Using AD DS

1. **Open Active Directory Users and Computers**:
   - Open the Active Directory Users and Computers console.
2. **Move Computers to SCOM OU**:
   - Move the computers you want to monitor to the SCOM OU you created.
3. **Verify Integration**:
   - Ensure that the management group information is published to AD.
   - Verify that the agents are automatically assigned to the correct management server based on the AD container settings.

Adding a Security Group to the Operations Manager Administrators Group

1. **Open Operations Console**:
   - Launch the Operations Manager console.
   - Select the Administration workspace.
2. **Navigate to User Roles**:
   - Under Security, click on User Roles.
3. **Open Properties for Operations Manager Administrators**:
   - Select Operations Manager Administrators.
   - Click the Properties action or right-click Operations Manager Administrators and select Properties.
4. **Add Security Group**:
   - Click Add to open the Select Group dialog box.
   - Select the desired security group and click OK to close the dialog box.
5. **Close User Role Properties**:
   - Click OK to close the User Role Properties window.

Enable Agent Proxy for All Agents Using PowerShell

If you need to enable the proxy setting for multiple agents, you can use PowerShell to automate the process: System Center Operations Manager (SCOM) relies heavily on agents to collect the data necessary for monitoring and reporting. To enable agents to discover and manage objects on other computers, you need to enable the Agent Proxy setting. This setting is disabled by default, so enabling it can help prevent errors related to agent operations.

Steps to Enable Agent Proxy

1. **Open Operations Manager Console**:
   - Navigate to the Administration workspace.
2. **Select Agent Managed**:
   - In the Device Management section, click on Agent Managed.
3. **Access Agent Properties**:
   - Locate the agent you want to configure. Right-click on the agent's entry and select Properties.
4. **Navigate to the Security Tab**:
   - In the Agent Properties window, go to the Security tab.
5. **Enable Agent Proxy**:
   - Check the box that says "Allow this agent to act as a proxy and discover managed objects on other computers".
   - Click OK to apply the changes.

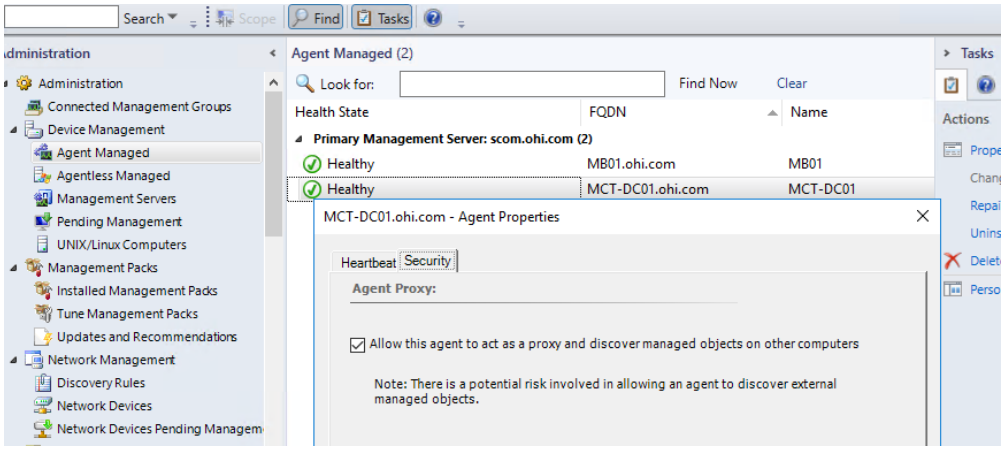
Enabling Agent Proxy for All Agents Using PowerShell

If you need to enable the proxy setting for multiple agents, you can use PowerShell to automate the process:

1. **Open PowerShell**:
   - Open the SCOM Command Shell.
2. **Run the Following Command**:

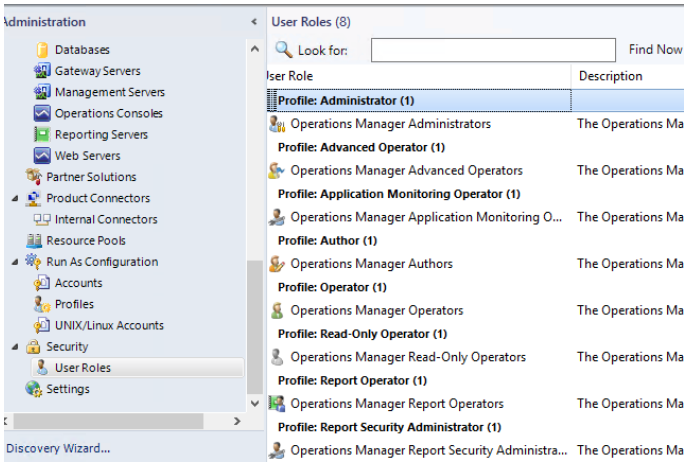
```
get-SCOMagent | where {$_.ProxyingEnabled -match "False"} | Enable-SCOMAgentProxy
```

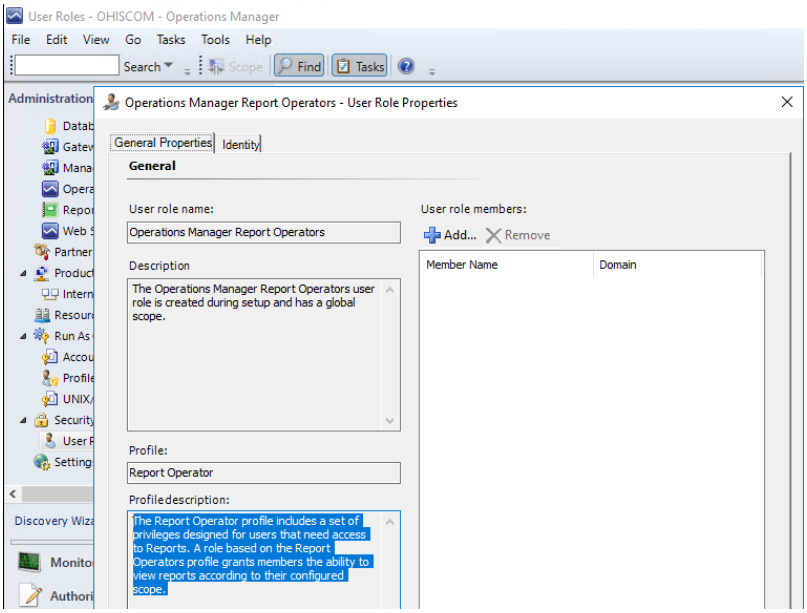
This command retrieves all agents where the proxying is not enabled and then enables the proxy setting for those agents.

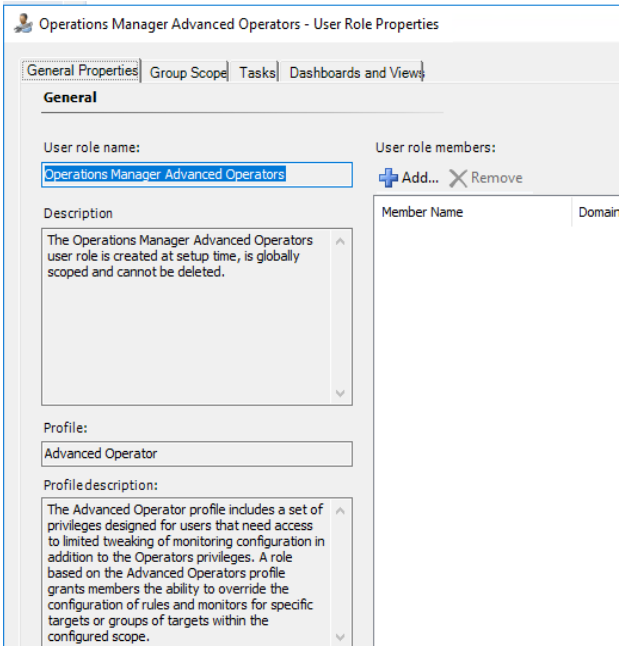


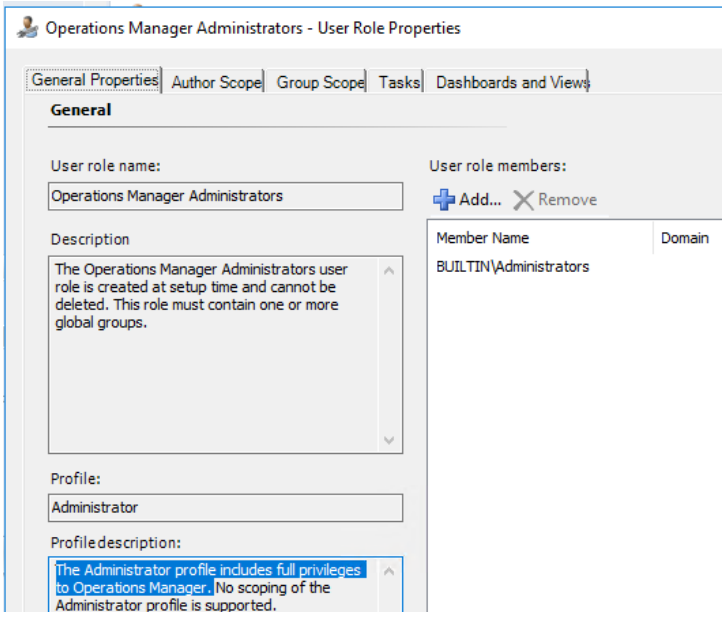
SCOM Administration Roles

- Administrators of Operations Manager have the greatest level of privileges.









Managing SCOM Agent Settings

Managing SCOM agent settings includes configuring multi-homing, repairing agents, and uninstalling agents. Here's a detailed guide based on the provided image:

Multi-Homing Agents

SCOM agents can report to multiple management groups (up to 4). To add management groups to an agent:

1. **Open Control Panel**:
   - Navigate to the Control Panel on the client computer.
2. **Open Microsoft Monitoring Agent**:
   - In the Control Panel, select the Microsoft Monitoring Agent settings.
3. **Add Management Group**:
   - In the Operations Manager tab, click Add to open the Add a Management Group dialog box.
   - Enter the following details:
     - **Management group name**: Name of the management group.
     - **Primary management server**: FQDN of the primary management server.
     - **Management server port**: Default is 5723.
   - Choose the agent action account:
     - **Use the Local System account**: Recommended for most scenarios.
     - **Use the following domain or local account**: Specify the domain\user and password if a different account is needed.
   - Click OK to add the management group.
4. **Enable Automatic Updates from AD**:
   - In the same tab, check the box Automatically update management group assignments from AD to allow the agent to query AD for management group assignments.

Repairing SCOM Agents

If an agent becomes corrupted, unresponsive, or requires settings changes, you can use the repair option:

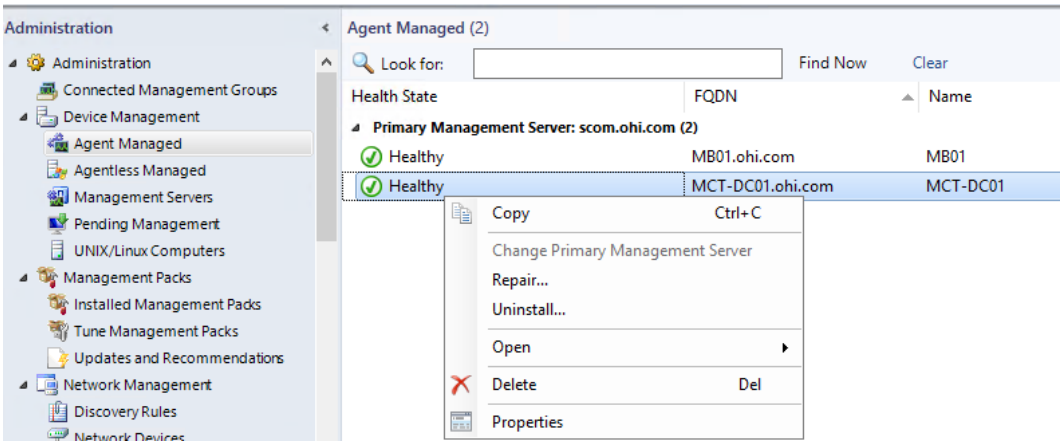
1. **Open Operations Manager Console**:
   - Navigate to the Administration workspace.
2. **Select Agent Managed**:
   - In the Device Management section, click on Agent Managed.
3. **Select Agent**:
   - Right-click on the agent that needs repair and select Repair.
   - Follow the wizard to complete the repair process.

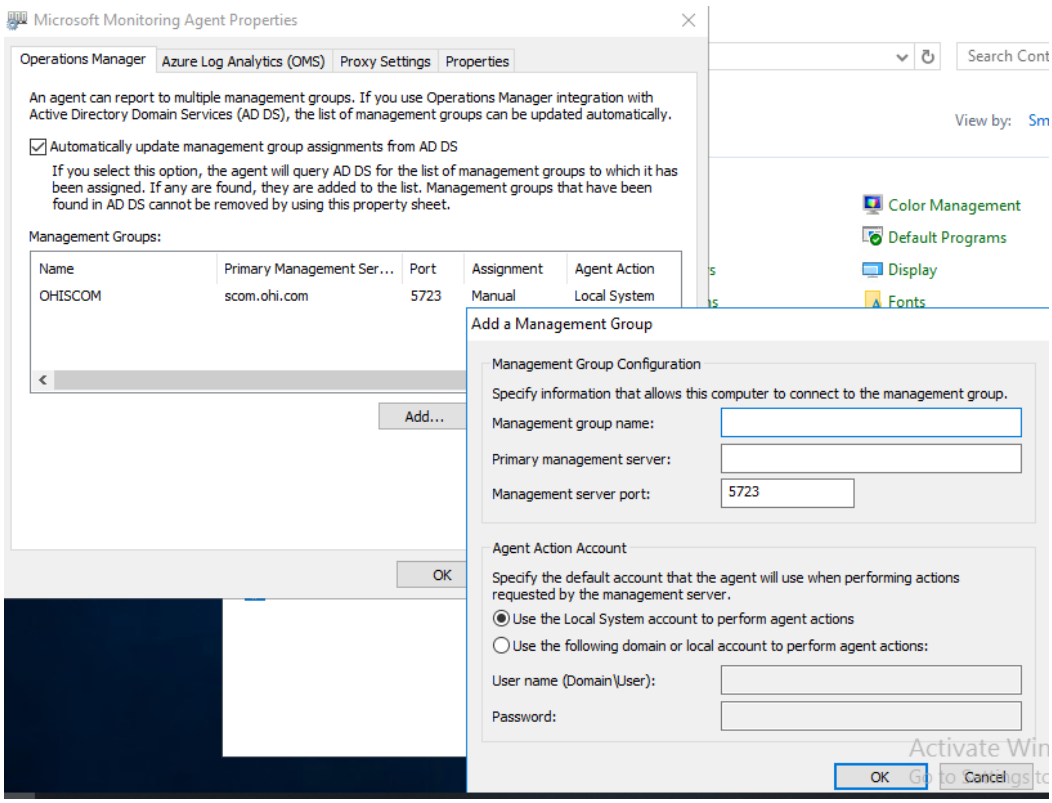
Uninstalling SCOM Agents

To uninstall a SCOM agent:

1. **Open Operations Manager Console**:
   - Navigate to the Administration workspace.
2. **Select Agent Managed**:
   - In the Device Management section, click on Agent Managed.

3. **Uninstall Agent**:
    - Right-click on the agent and select Uninstall.
    - Follow the wizard to complete the uninstallation process.
4. **Manual Uninstallation**:
    - If the agent is uninstalled from the Operations Manager console, you may also need to manually uninstall it from the client computer:
        - Open Programs and Features in the Control Panel.
        - Find Microsoft Monitoring Agent, right-click, and select Uninstall.
5. **Delete from Operations Manager Database**:
    - If you delete the agent entry from the Operations Manager database, make sure to manually uninstall the agent from the client computer as described above.





Importing and Managing Management Packs in SCOM

Management Packs in System Center Operations Manager (SCOM) are essential components that allow SCOM to monitor and manage different applications, services, and systems. They contain predefined rules, monitors, views, and knowledge about the specific applications or services they are designed to monitor.

Steps to Import Management Packs

1. **Open Operations Manager Console**:
    - Navigate to the Administration workspace.
2. **Select Management Packs**:
    - Under Management Packs, click on Installed Management Packs.
3. **Import Management Packs**:
    - Click on Import Management Packs in the Actions pane.
    - In the Import Management Packs dialog box, click Add and choose either:
        - **Add from catalog**: Connects to the Microsoft online catalog to download MPs.
        - **Add from disk**: Allows you to import MPs from a local directory.
4. **Select Management Packs**:
    - If adding from the catalog, browse and select the necessary Management Packs.

- If adding from disk, navigate to the location of the downloaded MPs and select them.

5. **Resolve Dependencies**:
   - If the selected Management Packs have dependencies, a Dependency Warning will appear.
   - Click Resolve to automatically download and import the required dependencies.
6. **Import List**:
   - Ensure that all required Management Packs and their dependencies are listed in the Import list.
   - Click Install to import the selected Management Packs.
7. **Review and Confirm**:
   - Review the import status to ensure that all Management Packs are successfully imported.
   - Click Close once the import process is complete.

Best Practices for Managing Management Packs

- **Monitor Relevant Systems**:
  - Import only the Management Packs that are necessary for monitoring the systems and applications in your environment.
- **Check Dependencies**:
  - Always verify and resolve dependencies for the Management Packs to avoid import errors.
- **Do Not Rename or Change Sealed MPs**:
  - Avoid renaming or modifying settings in sealed Management Packs. Instead, create unsealed MPs for custom changes.
- **Import Gradually**:
  - Import a small number of Management Packs at a time to avoid server stress and ensure proper functioning.
- **Download from Trusted Sources**:
  - Use the Microsoft catalog or trusted sources for downloading Management Packs.

Common Management Packs

Some of the most commonly used Management Packs include:

- DHCP
- DNS
- Active Directory
- SQL Server
- Exchange Server
- IIS and Apache

Downloading Management Packs

You can download Management Packs from the Microsoft Management Packs catalog or the TechNet Wiki. Here is the link for reference: Microsoft Management Packs

Tuning Management Packs

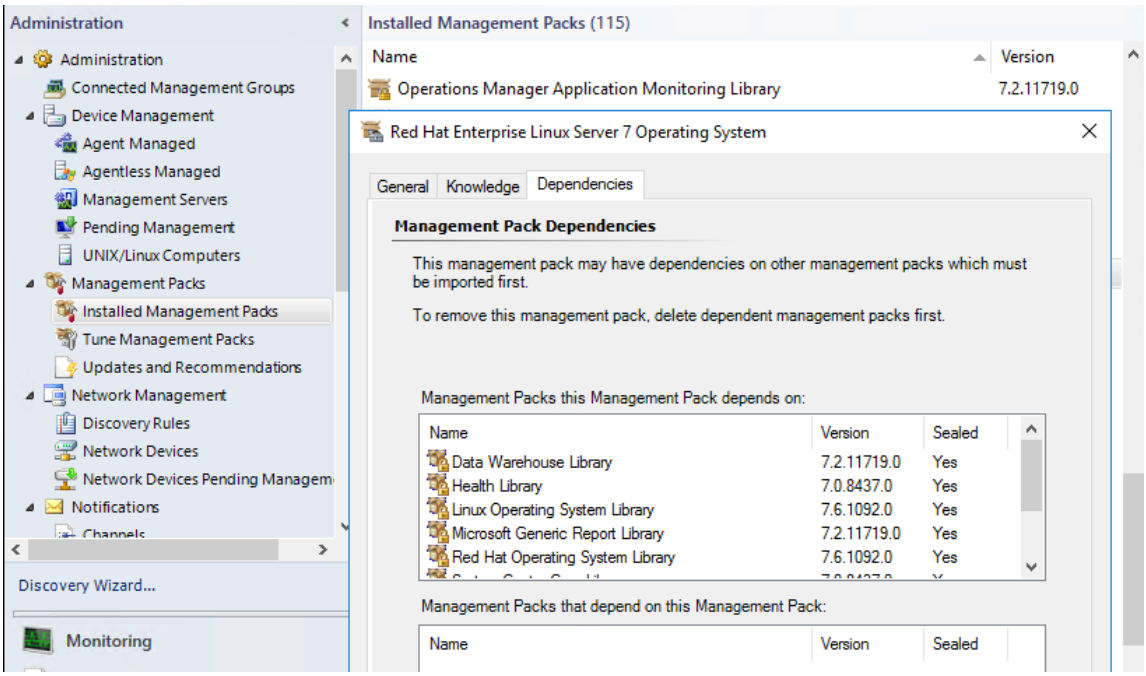
After importing Management Packs, you may need to tune them to fit your monitoring requirements:

1. **Open the Management Pack Properties**:
    - Navigate to Installed Management Packs in the Administration workspace.
    - Select the Management Pack and click Properties.
2. **Adjust Settings**:
    - Modify the rules, monitors, and thresholds as per your requirements.
3. **Create Overrides**:
    - For sealed Management Packs, create overrides in an unsealed Management Pack to customize monitoring settings.

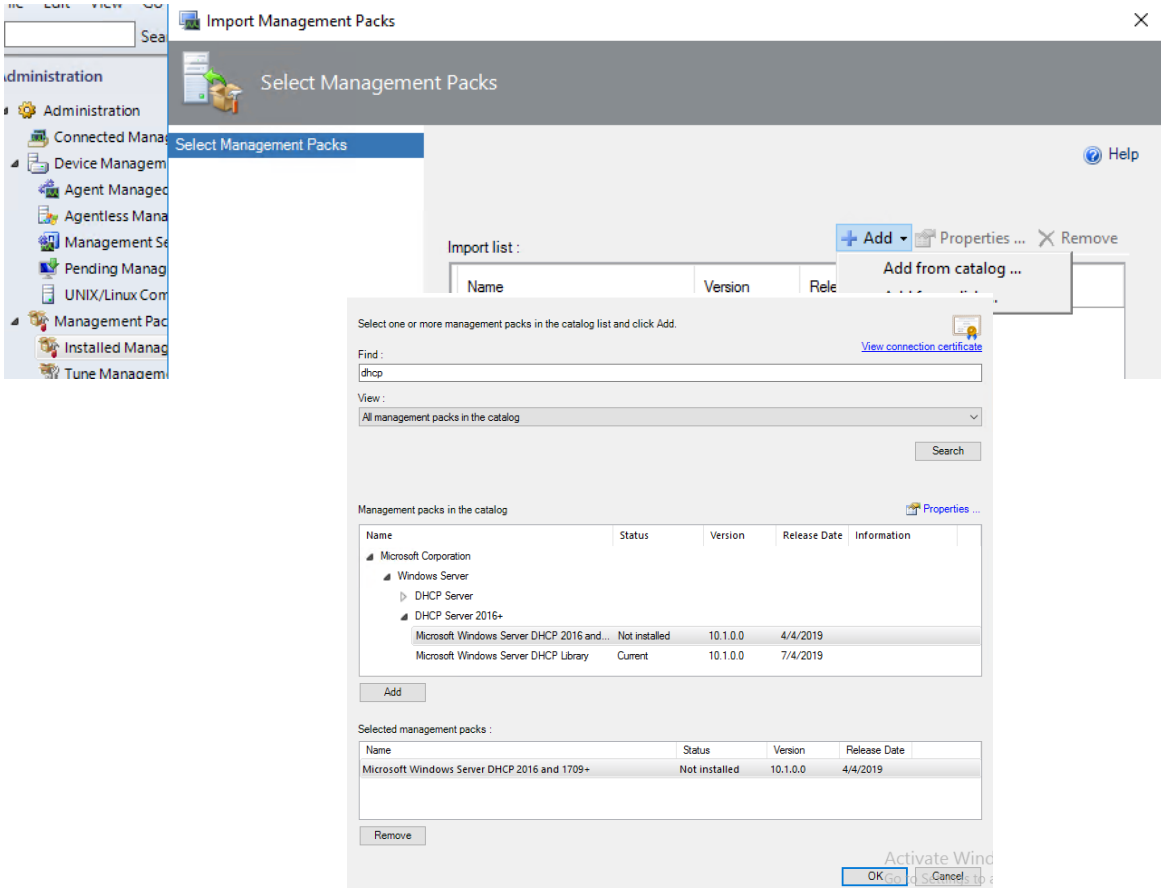
Handling Dependencies

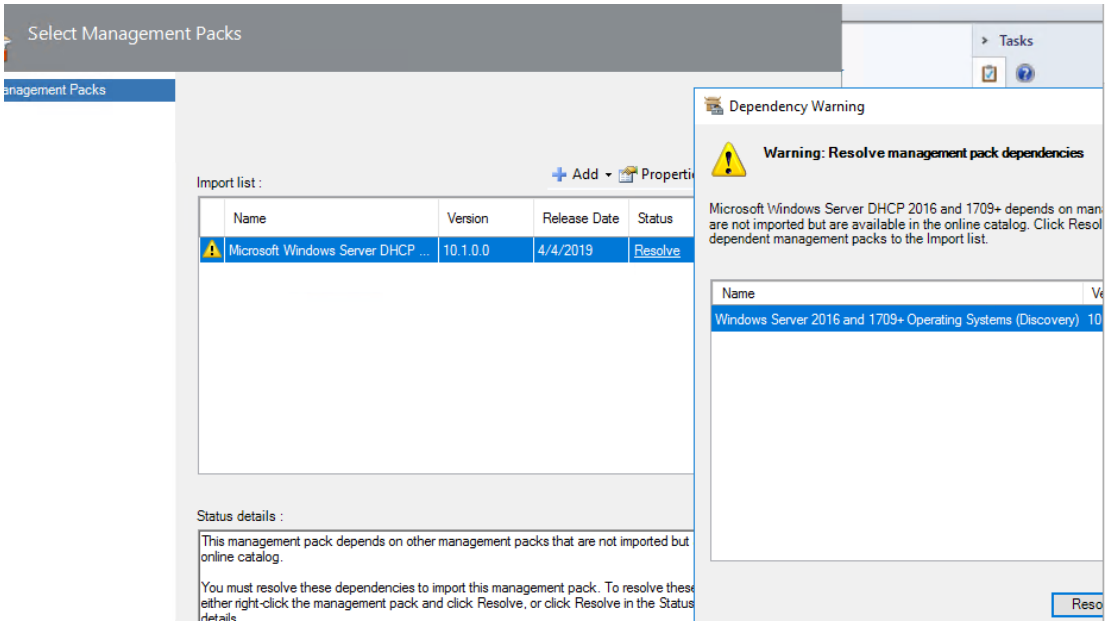
Sometimes, Management Packs require additional dependencies. The provided images illustrate resolving dependencies during the import process:

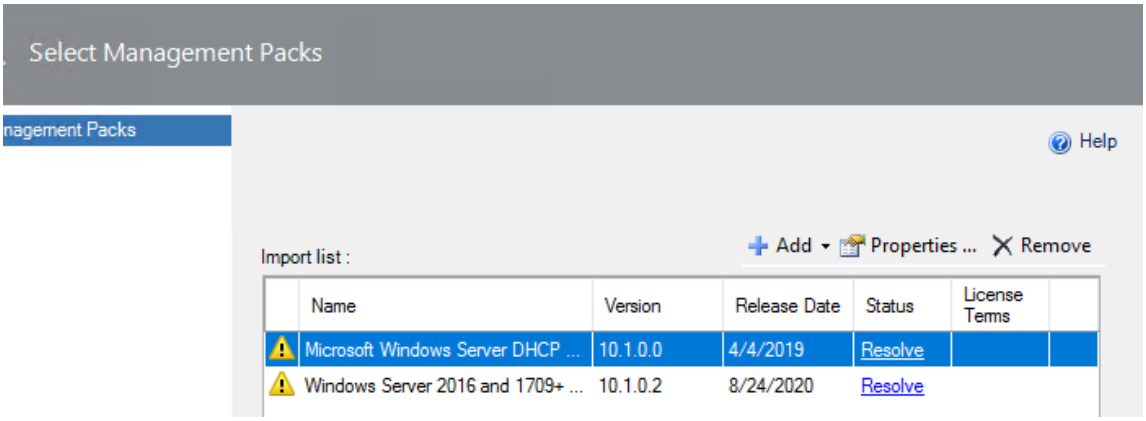
- **Dependency Warning**:
    - When importing a Management Pack, a Dependency Warning might appear if other Management Packs are required.
    - Click Resolve to automatically download and import these dependencies from the catalog.



add New MP


Import Management Packs
Select Management Packs
Select Management Packs
Help
Import list :
Add
Properties ...
Remove
Add from catalog ...
Name
Version
Select one or more management packs in the catalog list and click Add.
View connection certificate
Find :
dhcp
View :
All management packs in the catalog
Search
Management packs in the catalog
Properties ...
Name
Status
Version
Release Date
Information
Microsoft Corporation
Windows Server
DHCP Server
DHCP Server 2016+
Microsoft Windows Server DHCP 2016 and... Not installed 10.1.0.0 4/4/2019
Microsoft Windows Server DHCP Library Current 10.1.0.0 7/4/2019
Add
Selected management packs :
Name
Status
Version
Release Date
Microsoft Windows Server DHCP 2016 and 1709+ Not installed 10.1.0.0 4/4/2019
Remove
OK
Cancel


Select Management Packs
Tasks
Import list :
Add
Name
Version
Release Date
Status
Microsoft Windows Server DHCP ...
10.1.0.0
4/4/2019
Resolve
Status details :
This management pack depends on other management packs that are not imported but
online catalog.
You must resolve these dependencies to import this management pack. To resolve these
either right-click the management pack and click Resolve, or click Resolve in the Status
Dependency Warning
Warning: Resolve management pack dependencies
Microsoft Windows Server DHCP 2016 and 1709+ depends on man
are not imported but are available in the online catalog. Click Resol
dependent management packs to the Import list.
Name
Windows Server 2016 and 1709+ Operating Systems (Discovery) 10


Select Management Packs
Help
Import list :
Add
Properties ...
Remove
Name
Version
Release Date
Status
License Terms
Microsoft Windows Server DHCP ...
10.1.0.0
4/4/2019
Resolve
Windows Server 2016 and 1709+ ...
10.1.0.2
8/24/2020
Resolve

Sealed and Unsealed Management Packs in SCOM

Management Packs (MPs) in System Center Operations Manager (SCOM) come in two types: sealed and unsealed. Understanding the differences between them is crucial for effective management and customization of your monitoring environment.

Sealed Management Packs

Characteristics:

- **File Type**: Binary file with a .mp extension.
- **Immutability**: Cannot be edited directly.
- **Source**: Typically provided by application or hardware vendors, including Microsoft.
- **Usage**: Ensure standardization and integrity of the monitoring definitions provided by vendors.

Customization:

- **Overrides**: While you cannot change the settings directly in a sealed Management Pack, you can customize it by creating overrides.
- **Additional Settings**: You can create additional rules, monitors, and tasks that supersede the default settings.
- **Separate File for Customizations**: All customizations are saved in a separate, unsealed Management Pack.

Referencing:

- **Dependency**: A Management Pack can only reference another Management Pack if the referenced pack is sealed. This ensures the referenced definitions remain consistent and unchanged.

Example:

- **Microsoft SQL Server Management Pack**: You import the sealed Management Pack from Microsoft, then create an unsealed Management Pack to store your overrides and additional configurations.

Unsealed Management Packs

Characteristics:

- **File Type**: XML file with a .xml extension.
- **Editability**: Can be edited directly.
- **Source**: Typically created by users or organizations for custom monitoring needs.
- **Usage**: Used for creating and storing custom rules, monitors, views, tasks, and overrides.

Flexibility:

- **Customization**: You can modify settings as needed to suit specific requirements.
- **Integration**: Often used in conjunction with sealed Management Packs to store overrides and additional configurations.

Example:

- **Custom Application Monitoring**: You create an unsealed Management Pack to monitor a custom application, defining specific rules, monitors, and views tailored to that application.

Practical Application

Working with Sealed Management Packs

1. **Importing**: Import the sealed Management Pack from the vendor.
2. **Creating Overrides**: Create a new unsealed Management Pack to store your customizations.

3. **Applying Customizations**: Define overrides for the settings you want to change. These might include threshold adjustments, enabling/disabling specific monitors, or custom alert definitions.

Creating and Using Unsealed Management Packs

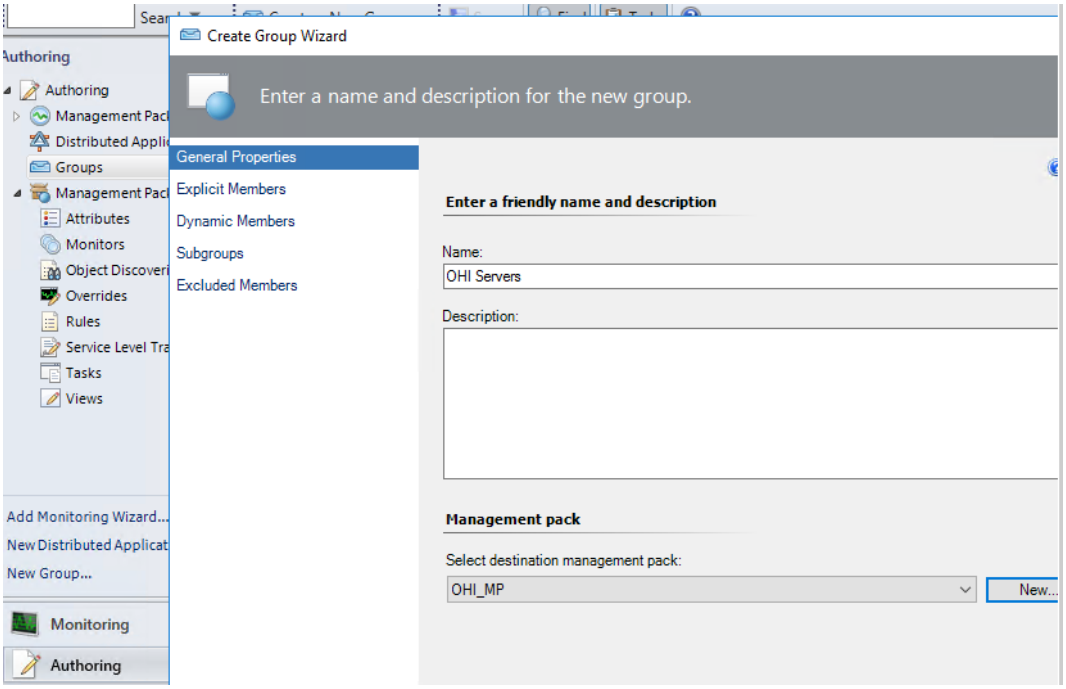
1. **Defining Custom Monitoring**: Use unsealed Management Packs to define monitoring for custom applications or services not covered by existing sealed packs.
2. **Storing Overrides**: Store overrides for sealed Management Packs in an unsealed Management Pack to keep your customizations organized.
3. **Editing Flexibility**: Modify the unsealed Management Pack as needed to update or enhance your monitoring configuration.

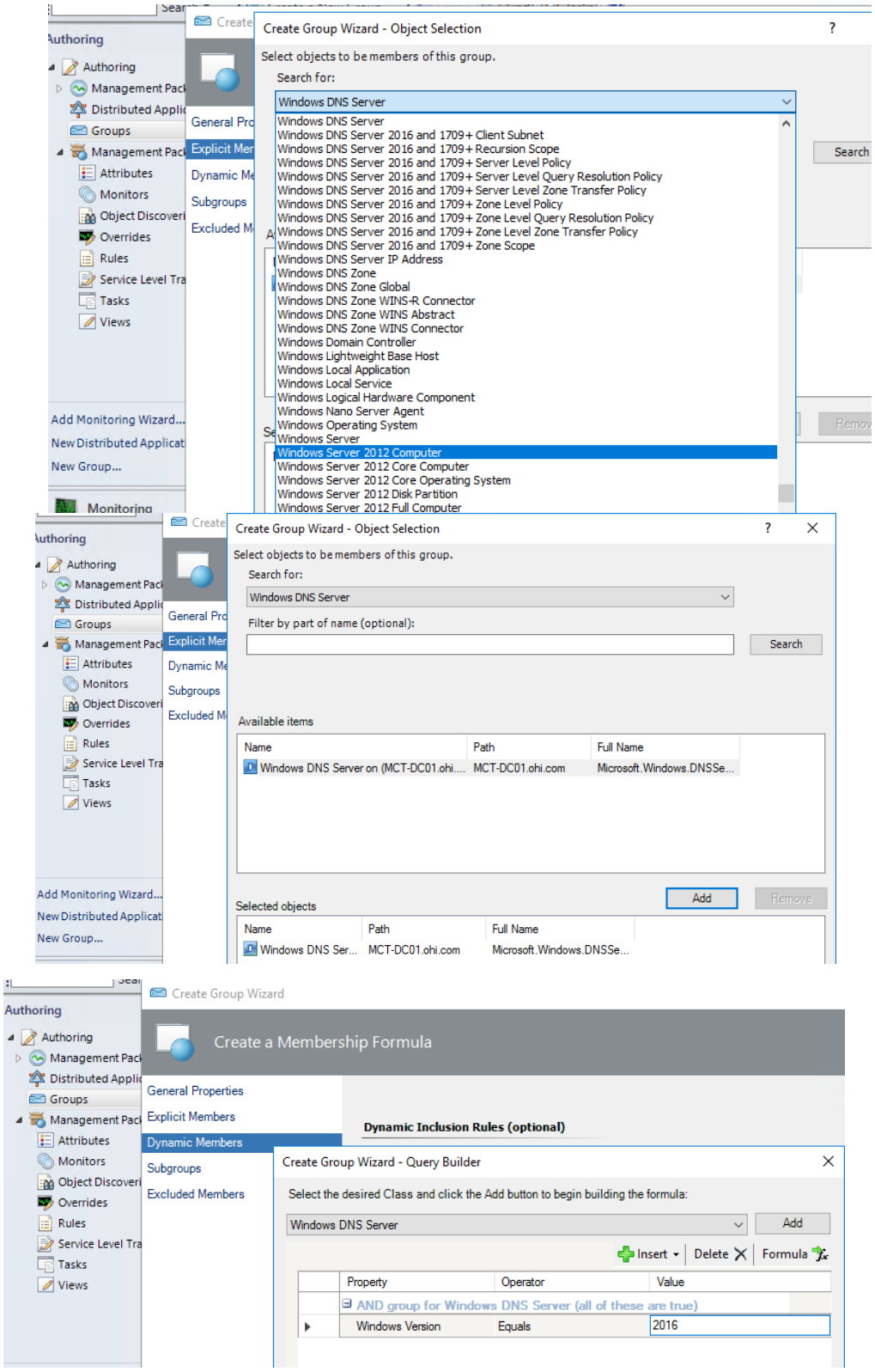
Example Scenario

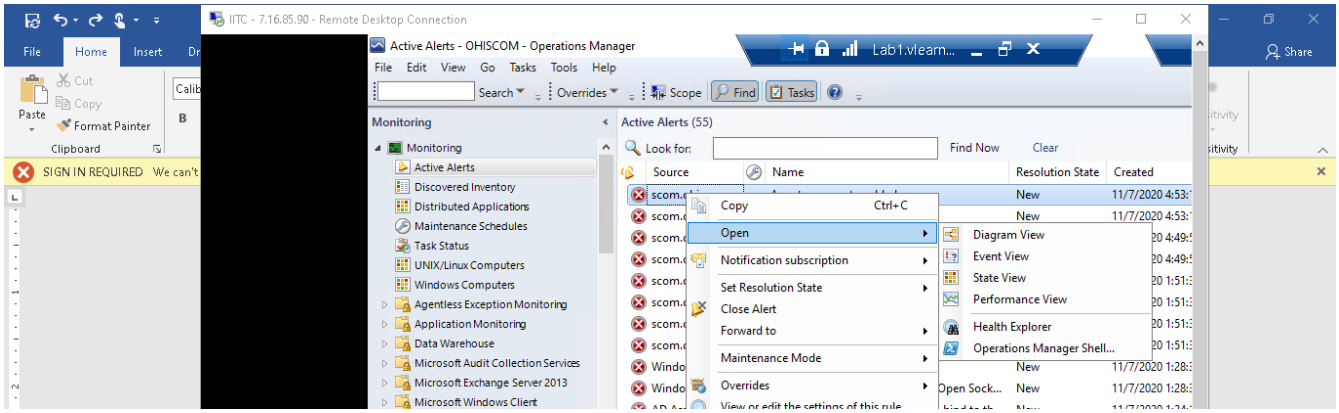
Custom DNS Server Monitoring:

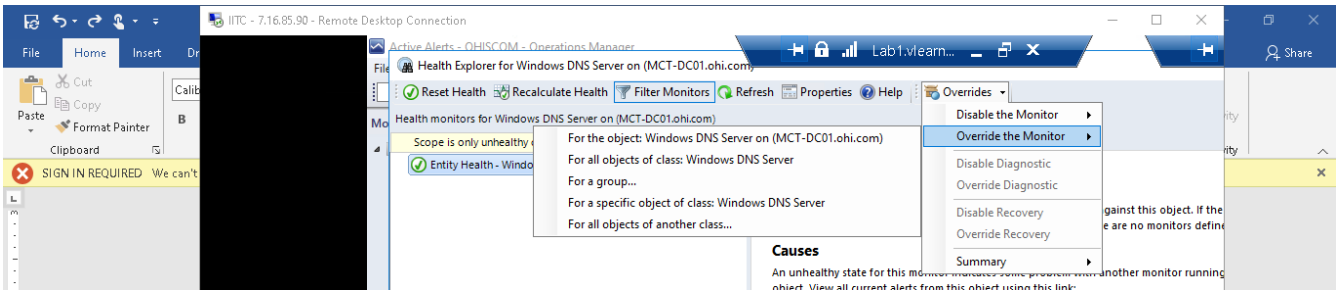
1. **Import Sealed DNS MP**: Import a sealed Management Pack for DNS server monitoring from Microsoft.
2. **Create Unsealed MP for Overrides**: Create an unsealed Management Pack to store your overrides.
3. **Apply Overrides**: Override specific alerts for DNS servers, such as changing the severity or notification settings.
4. **Group Management**: Create a group of DNS servers and apply the overrides to this group, ensuring that only relevant alerts are triggered for this specific set of servers.

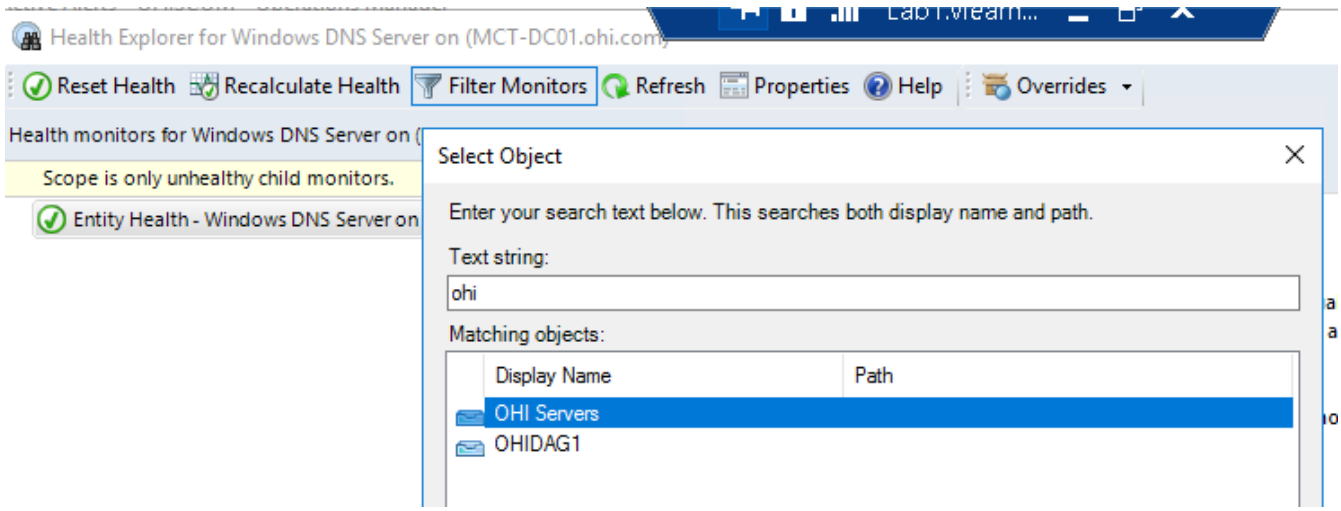
Create Group then apply Overrides

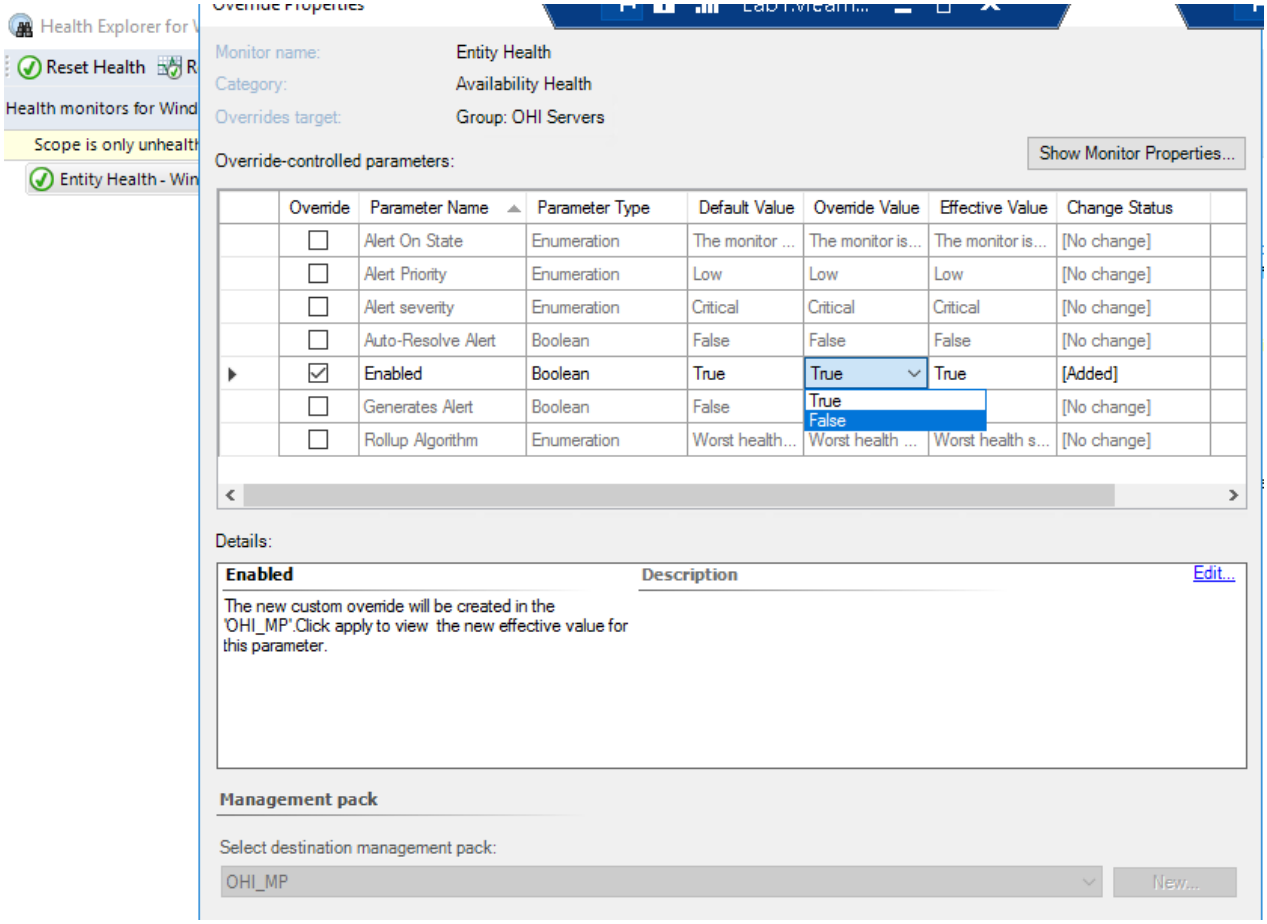



Create Group Wizard - Object Selection
Select objects to be members of this group.
Search for:
Windows DNS Server
Windows DNS Server
Windows DNS Server 2016 and 1709+ Client Subnet
Windows DNS Server 2016 and 1709+ Recursion Scope
Windows DNS Server 2016 and 1709+ Server Level Policy
Windows DNS Server 2016 and 1709+ Server Level Query Resolution Policy
Windows DNS Server 2016 and 1709+ Server Level Zone Transfer Policy
Windows DNS Server 2016 and 1709+ Zone Level Policy
Windows DNS Server 2016 and 1709+ Zone Level Query Resolution Policy
Windows DNS Server 2016 and 1709+ Zone Level Zone Transfer Policy
Windows DNS Server 2016 and 1709+ Zone Scope
Windows DNS Server IP Address
Windows DNS Zone
Windows DNS Zone Global
Windows DNS Zone WINS-R Connector
Windows DNS Zone WINS Abstract
Windows DNS Zone WINS Connector
Windows Domain Controller
Windows Lightweight Base Host
Windows Local Application
Windows Local Service
Windows Logical Hardware Component
Windows Nano Server Agent
Windows Operating System
Windows Server
Windows Server 2012 Computer
Windows Server 2012 Core Computer
Windows Server 2012 Core Operating System
Windows Server 2012 Disk Partition
Windows Server 2012 Full Computer
Search
Authoring
Groups
Attributes
Monitors
Overrides
Rules
Tasks
Views
Add Monitoring Wizard...
New Group...
General Properties
Explicit Members
Dynamic Members
Subgroups
Excluded Members
Filter by part of name (optional):
Available items
Name
Path
Full Name
Windows DNS Server on (MCT-DC01.ohi....
MCT-DC01.ohi.com
Microsoft.Windows.DNSSe...
Selected objects
Add
Remove
Create Group Wizard
Create a Membership Formula
Dynamic Inclusion Rules (optional)
Create Group Wizard - Query Builder
Select the desired Class and click the Add button to begin building the formula:
Insert
Delete
Formula
Property
Operator
Value
AND group for Windows DNS Server (all of these are true)
Windows Version
Equals
2016

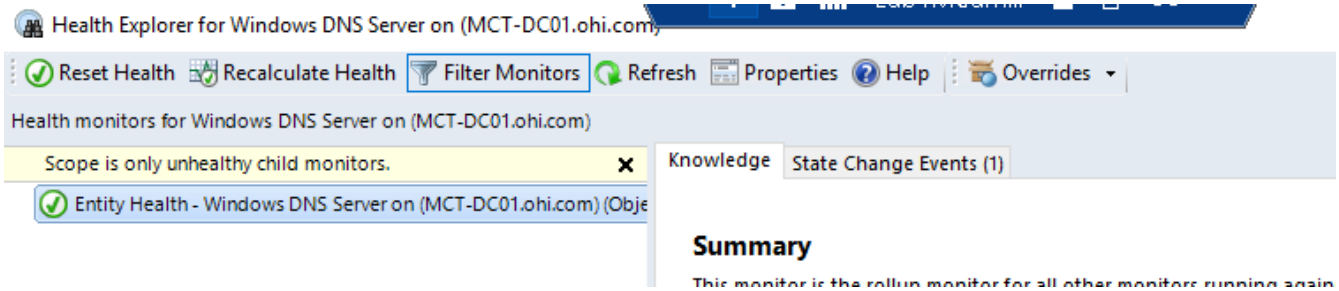

Active Alerts - OHISCOM - Operations Manager
Monitoring
Active Alerts
Discovered Inventory
Distributed Applications
Maintenance Schedules
Task Status
UNIX/Linux Computers
Windows Computers
Agentless Exception Monitoring
Application Monitoring
Data Warehouse
Microsoft Audit Collection Services
Microsoft Exchange Server 2013
Microsoft Windows Client
Active Alerts (55)
Look for:
Find Now
Clear
Source
Name
Resolution State
Created
Copy Ctrl+C
Open
Notification subscription
Set Resolution State
Close Alert
Forward to
Maintenance Mode
Overrides
Diagram View
Event View
State View
Performance View
Health Explorer
Operations Manager Shell...


Health Explorer for Windows DNS Server on (MCT-DC01.ohi.com)
Reset Health
Recalculate Health
Filter Monitors
Refresh
Properties
Help
Overrides
Health monitors for Windows DNS Server on (MCT-DC01.ohi.com)
Scope is only unhealthy
Entity Health - Windo
For the object: Windows DNS Server on (MCT-DC01.ohi.com)
For all objects of class: Windows DNS Server
For a group...
For a specific object of class: Windows DNS Server
For all objects of another class...
Disable the Monitor
Override the Monitor
Disable Diagnostic
Override Diagnostic
Disable Recovery
Override Recovery
Summary
Causes


Health Explorer for Windows DNS Server on (MCT-DC01.ohi.com)
Reset Health
Recalculate Health
Filter Monitors
Refresh
Properties
Help
Overrides
Health monitors for Windows DNS Server on
Scope is only unhealthy child monitors.
Entity Health - Windows DNS Server on
Select Object
Enter your search text below. This searches both display name and path.
Text string:
ohi
Matching objects:
Display Name
Path
OHI Servers
OHIDAG1



Now recalculate Health



Installing SCOM Agent on Linux

Based on the provided screenshots, here is a step-by-step guide for installing the SCOM agent on a CentOS 7 machine:

Prerequisites

1. **SCOM Management Server**: Ensure you have a running SCOM management server.
2. **CentOS 7 Machine**: The machine should be running CentOS 7.
3. **Privileges**: You need root or sudo access on the CentOS machine.
4. **Network Configuration**: Ensure the CentOS machine can communicate with the SCOM server over the network.

Step 1: Prepare the CentOS 7 Machine

- **Update the Package List**:

```
sudo yum update
```

- **Install Required Libraries**:

```
sudo yum install libunwind libicu
```

- **Enable and Start SSH Service**:

```
sudo systemctl start sshd
sudo systemctl enable sshd
sudo systemctl status sshd
```

- **Configure Firewall**:

```
sudo firewall-cmd --add-port=22/tcp --permanent
sudo firewall-cmd --add-port=1270/tcp --permanent
sudo firewall-cmd --reload
```

Step 2: Download and Install the SCOM Agent

- **Download the SCOM Agent Package**:
  - Obtain the SCOM agent package for CentOS from the Microsoft website or your SCOM installation media.
- **Transfer the Package**:
  - Use SCP or another file transfer method to copy the agent package to your CentOS machine.
- **Install the Package**:

```
sudo rpm -ivh scx-1.6.3-476.x86_64.rpm
```

Step 3: Configure the SCOM Agent

- **Run the Agent Configuration Script**:

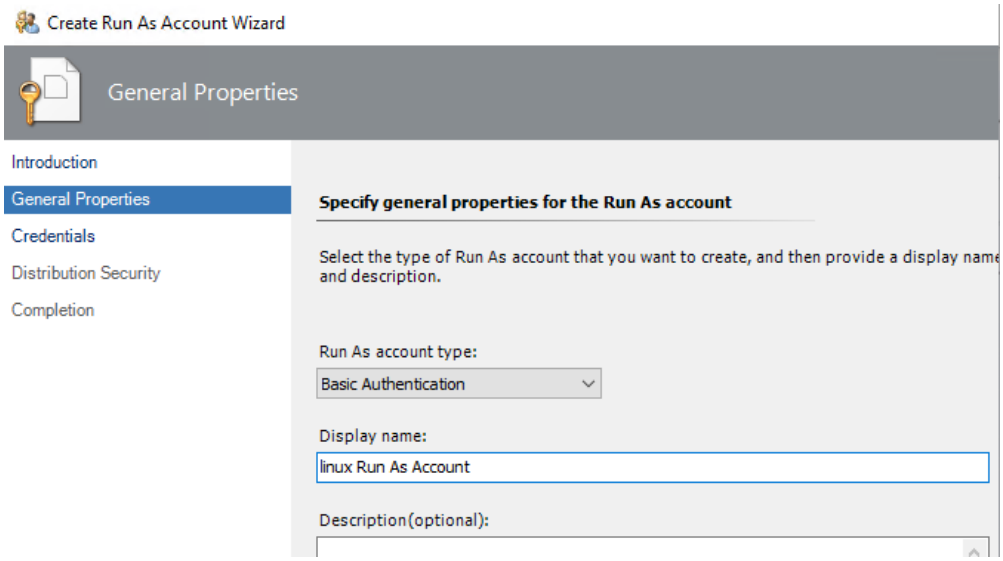
```
sudo /opt/microsoft/scx/bin/tools/scxadmin -install
```

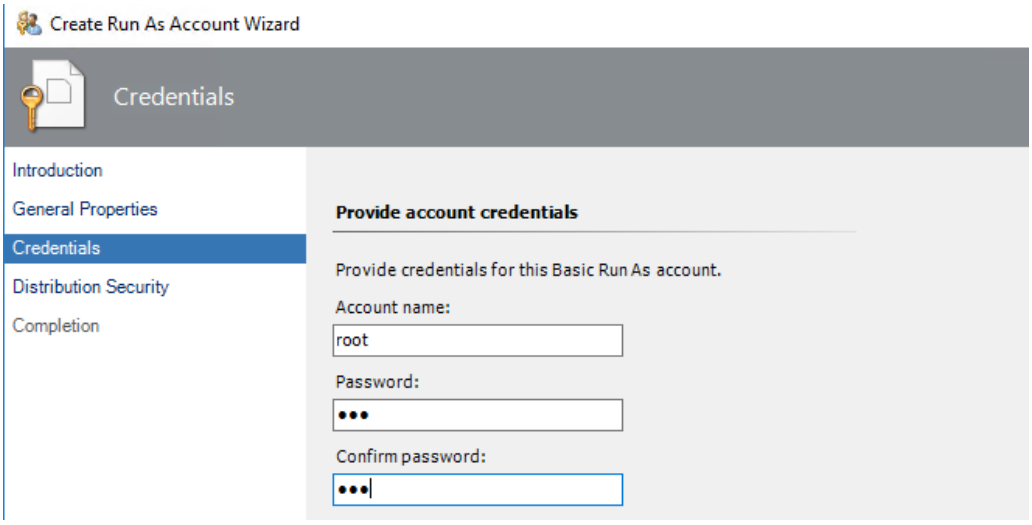
- **Configure the Agent to Communicate with the SCOM Server**:

```
sudo /opt/microsoft/scx/bin/tools/scxsslconfig -h centos7 -d ohi.com -f -v
sudo /opt/microsoft/scx/bin/tools/scxadmin -restart
```

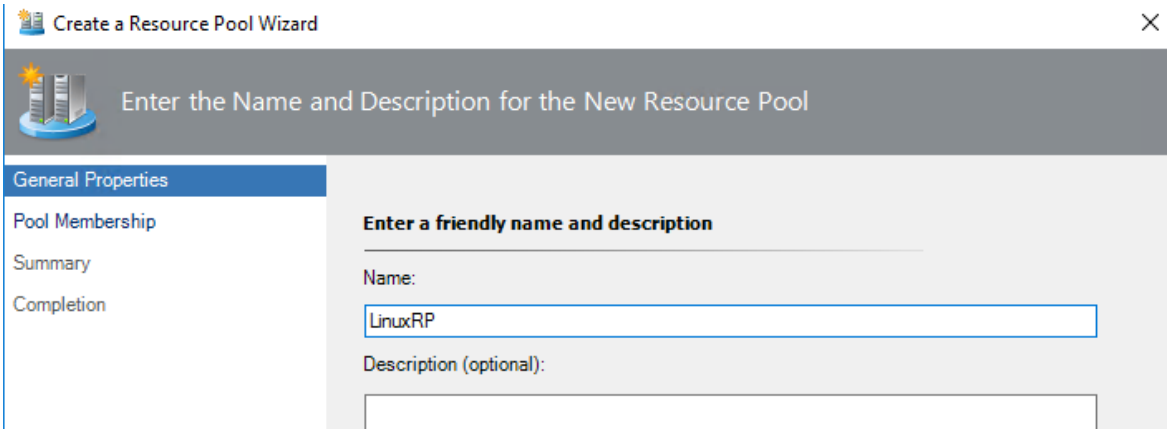
Step 4: Configure SCOM for Linux Monitoring

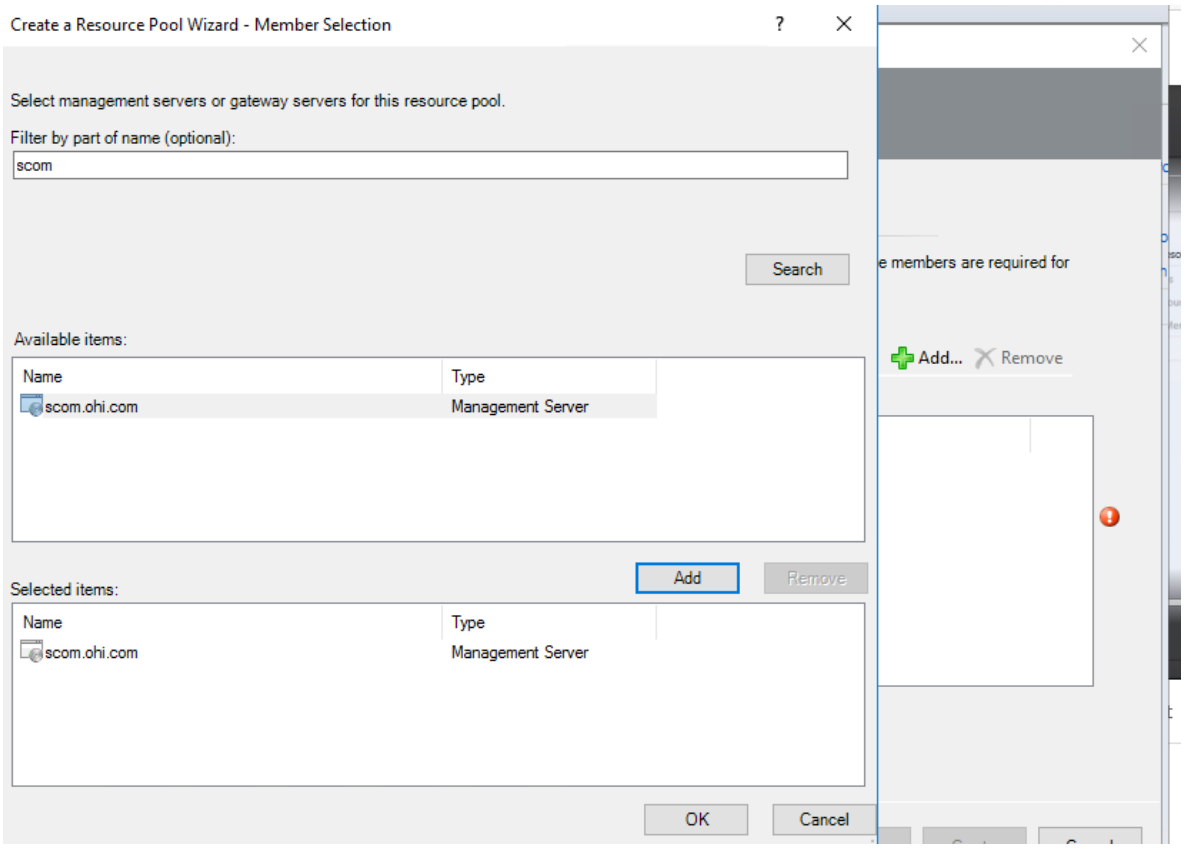
1. **Create a Run As Account**:
    - Open the SCOM console.
    - Navigate to Administration > Run As Configuration > Accounts.
    - Create a new account of type Basic Authentication.
    - Provide a display name, such as Linux Run As Account.
    - Enter the credentials for a user with sufficient privileges on the CentOS machine.





2. **Create a Resource Pool**:
    - Navigate to Administration > Resource Pools.
    - Create a new resource pool, such as LinuxRP.

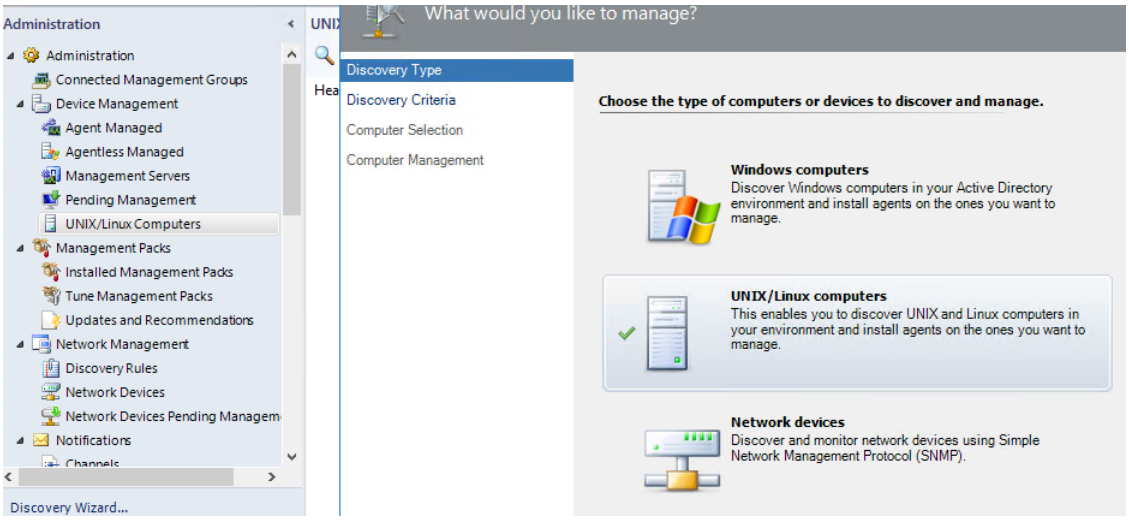




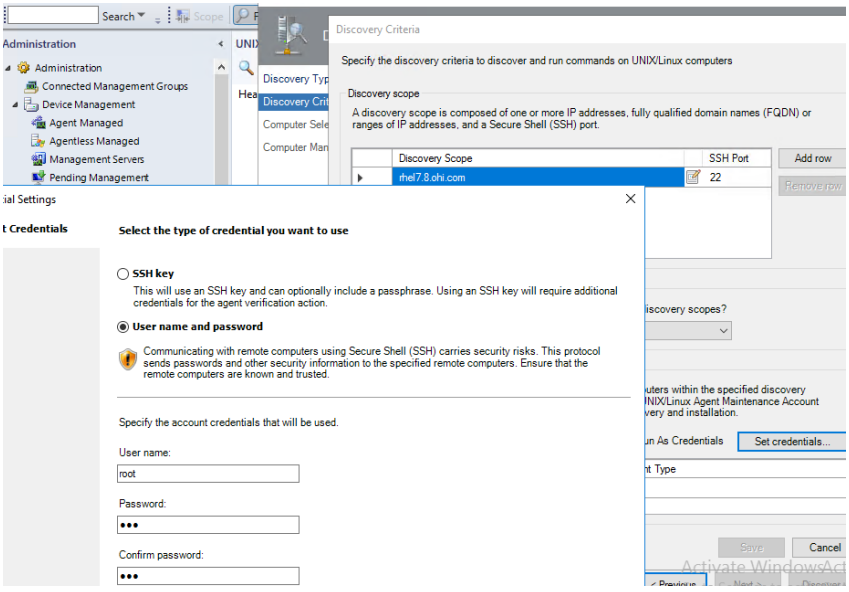
3. **Configure Distribution Security**:
    - Select More secure - I want to manually select the computers to which the credentials will be distributed.

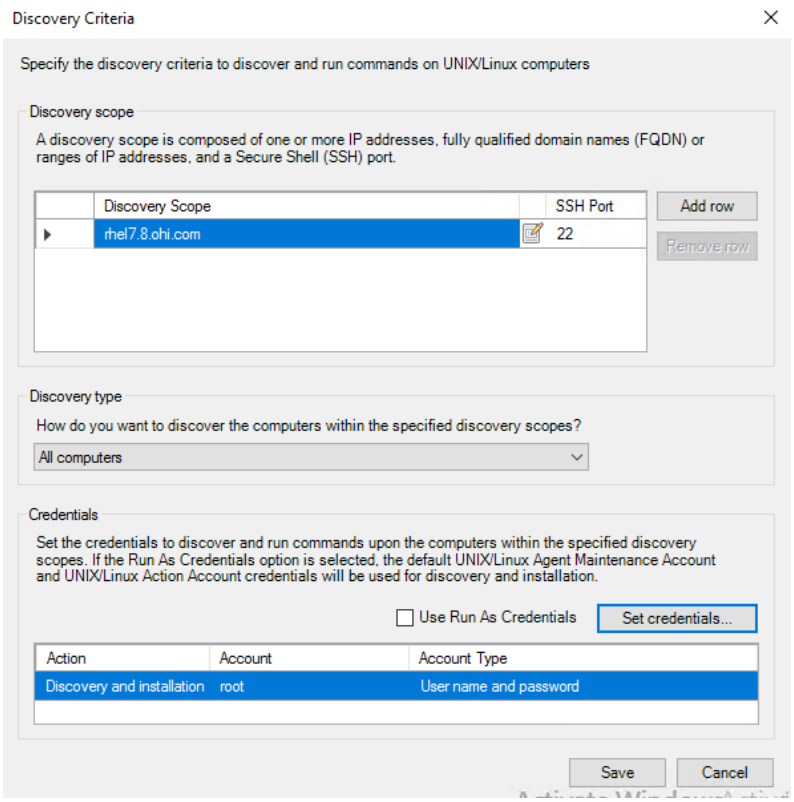
Step 5: Discover and Install the SCOM Agent on CentOS 7

1. **Open the Discovery Wizard**:
    - Navigate to Administration > UNIX/Linux Computers.
    - Start the Discovery Wizard.

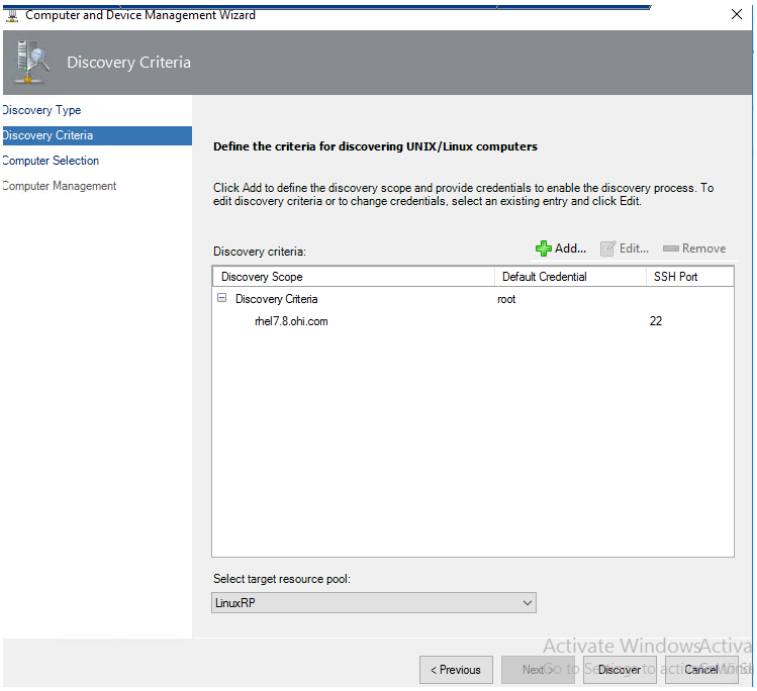


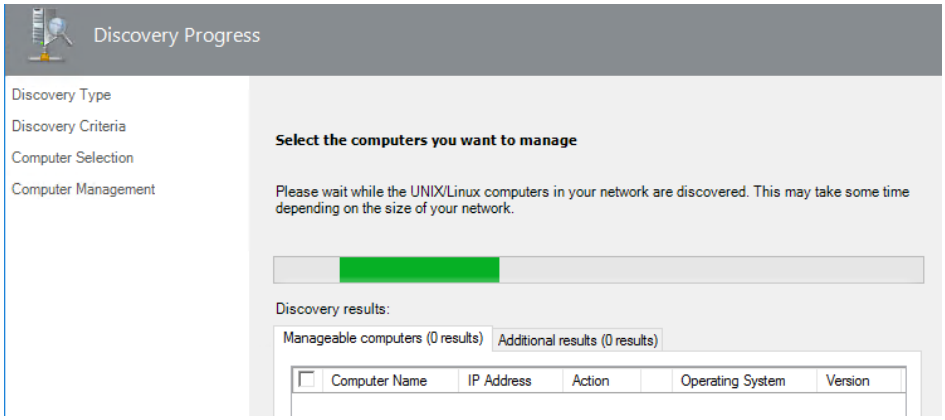
2. **Discovery Criteria**:
    - Specify the discovery scope by adding the FQDN of the CentOS machine, e.g., rhel7.8.ohi.com.
    - Set the SSH port to 22.
3. **Specify Credentials**:
    - Use the credentials created earlier for Discovery and Installation.
    - Set the username and password or SSH key for the root or sudo user.



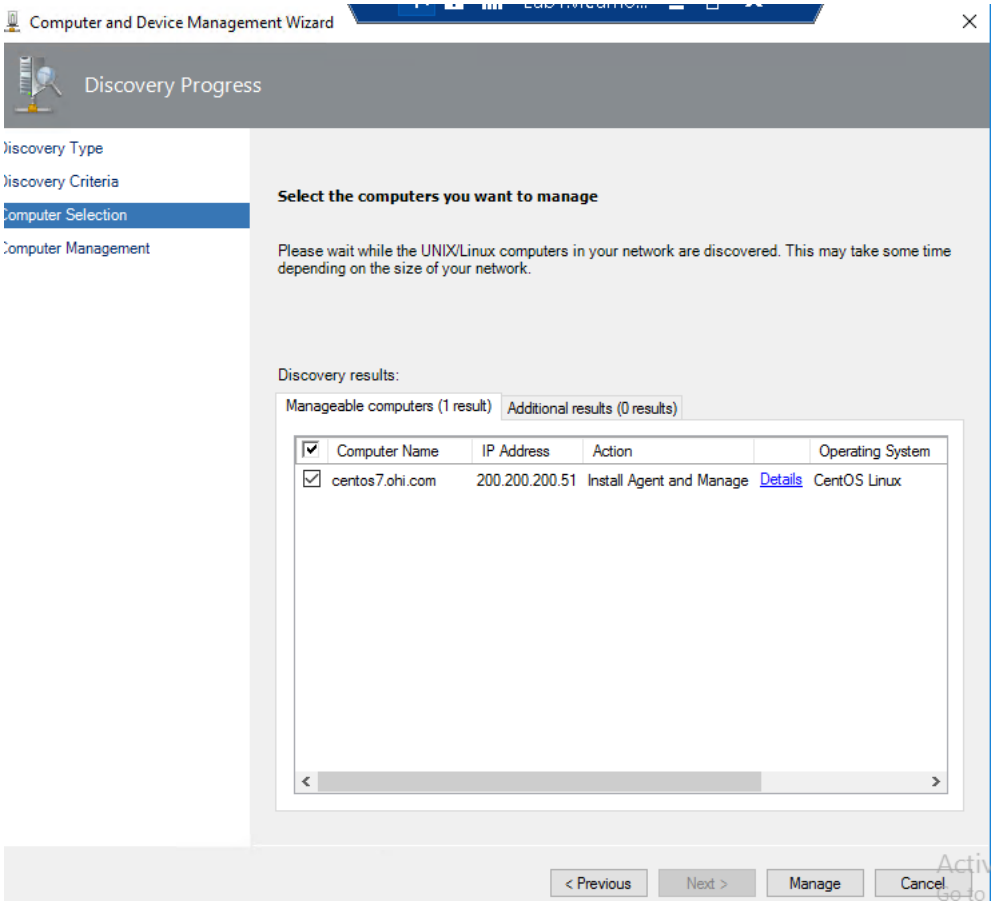


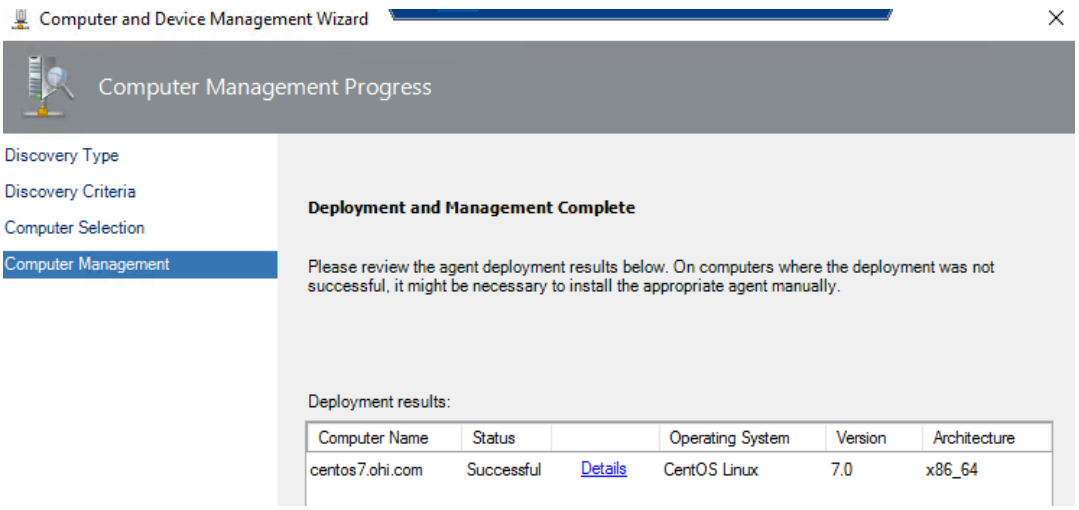
4. **Start Discovery**:
    - Start the discovery process and wait for the CentOS machine to be discovered.



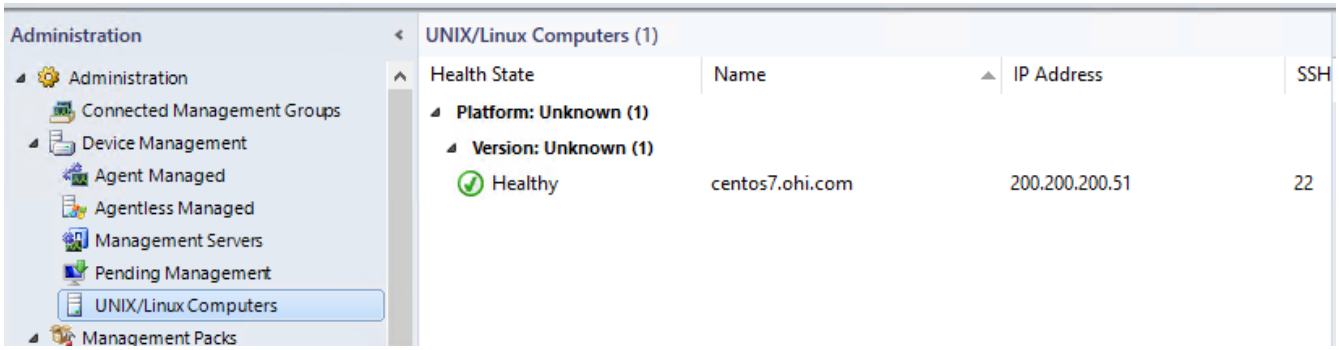


5. **Manage Discovered Computers**:
    - Select the discovered CentOS machine.
    - Install the agent and manage the machine.





6. **Verify the Installation**:
    - Ensure the CentOS machine appears under Administration > UNIX/Linux Computers with a healthy state.



Alerts and Monitoring in SCOM

System Center Operations Manager (SCOM) provides a robust framework for monitoring IT environments and generating alerts based on the health and performance of monitored objects. Alerts are critical in ensuring that IT administrators are aware of issues in real-time and can take corrective actions promptly. Here is a theoretical overview followed by practical steps illustrated in the provided screenshots.

Overview

1. Alerts in SCOM:

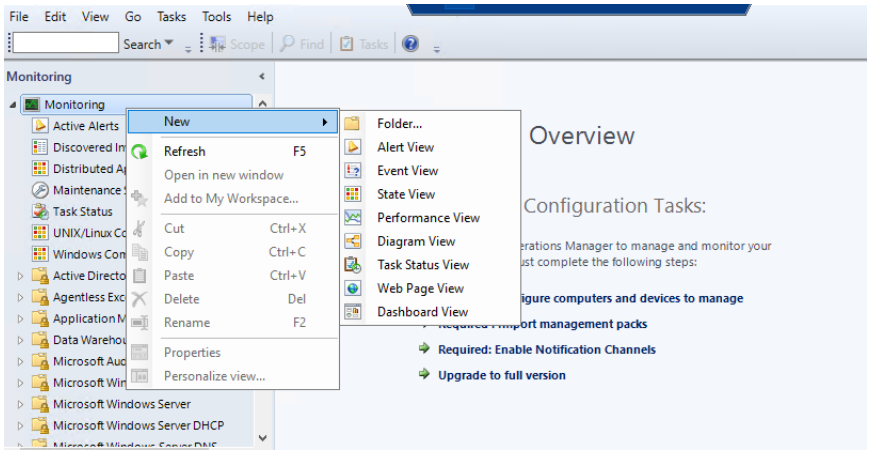
- **Definition:** Alerts are notifications generated by SCOM when a specific condition or threshold is met. They are designed to inform administrators about issues that need attention.
- **Components of an Alert:**
  - **Severity:** Indicates the importance of the alert (e.g., Critical, Warning, Informational).
  - **Priority:** Defines the urgency of the alert.
  - **Resolution State:** Shows the current status of the alert (e.g., New, Acknowledged, Closed).
  - **Source:** The object or rule that generated the alert.
  - **Description:** Provides details about the alert and possible steps for resolution.

2. Monitoring:

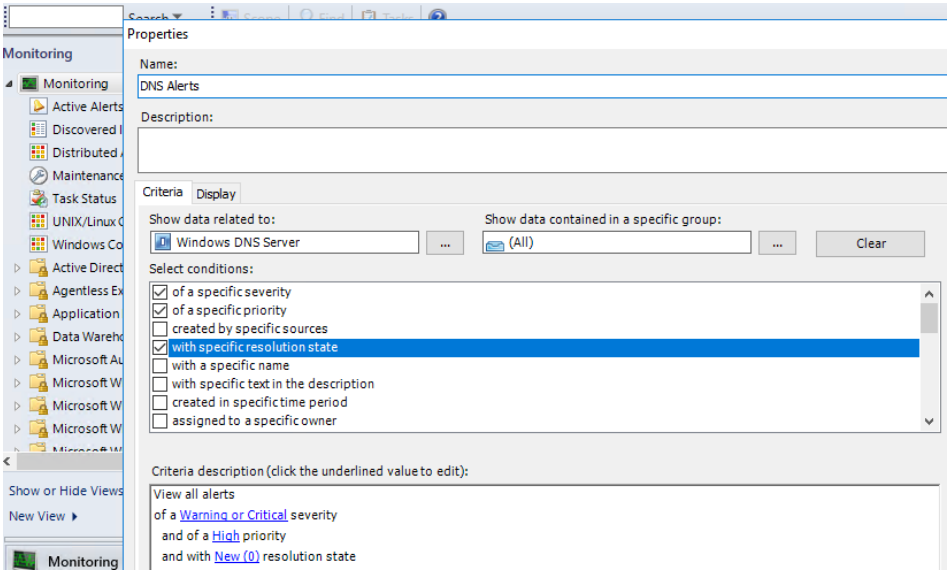
- **Purpose:** Monitoring involves continuously assessing the health and performance of IT infrastructure components, such as servers, applications, and services.
- **Monitoring Components:**
  - **Monitors:** Assess the health state of objects and can trigger alerts.
  - **Rules:** Collect data and generate alerts based on specific conditions.
  - **Views:** Visual representations of monitored data, including alerts, performance, and state views.
  - **Tasks:** Actions that can be executed to remediate or further investigate issues.

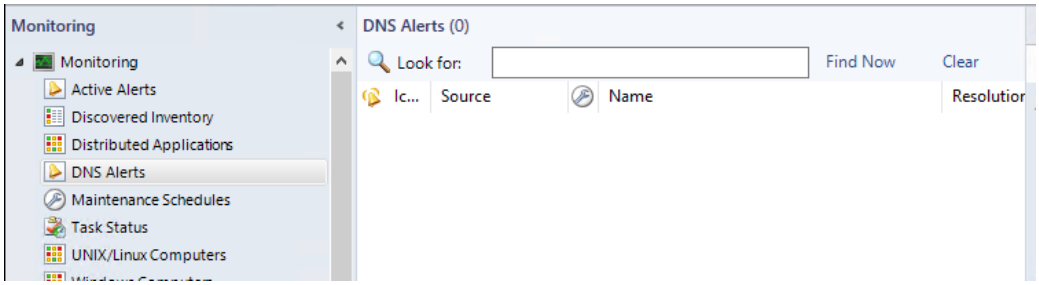
Creating and Managing Alerts in SCOM

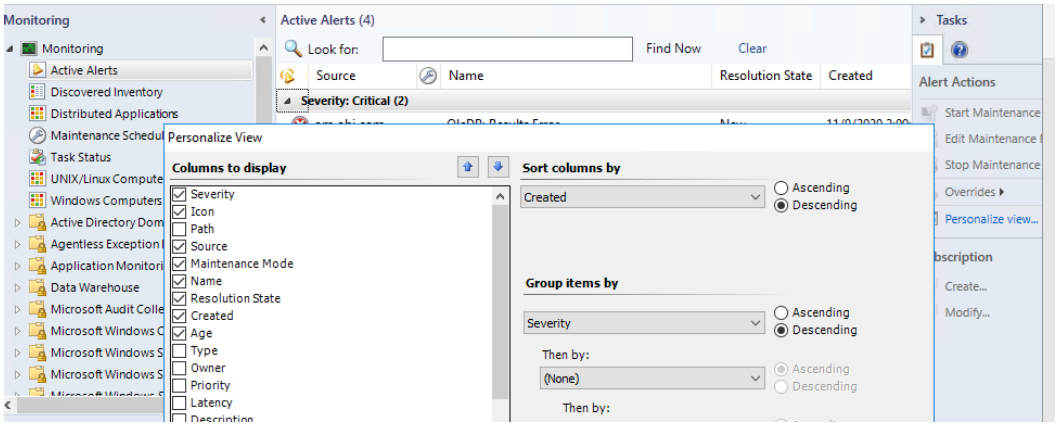
1. **Create a New View for DNS Alerts:**
   - **Step 1:** Navigate to the Monitoring workspace, right-click, and select New > State View.
   - **Step 2:** In the Properties window, configure the view to show data related to Windows DNS Server and set conditions for alerts with specific resolution states.
   - **Step 3:** The new DNS Alerts view will display alerts related to DNS servers.



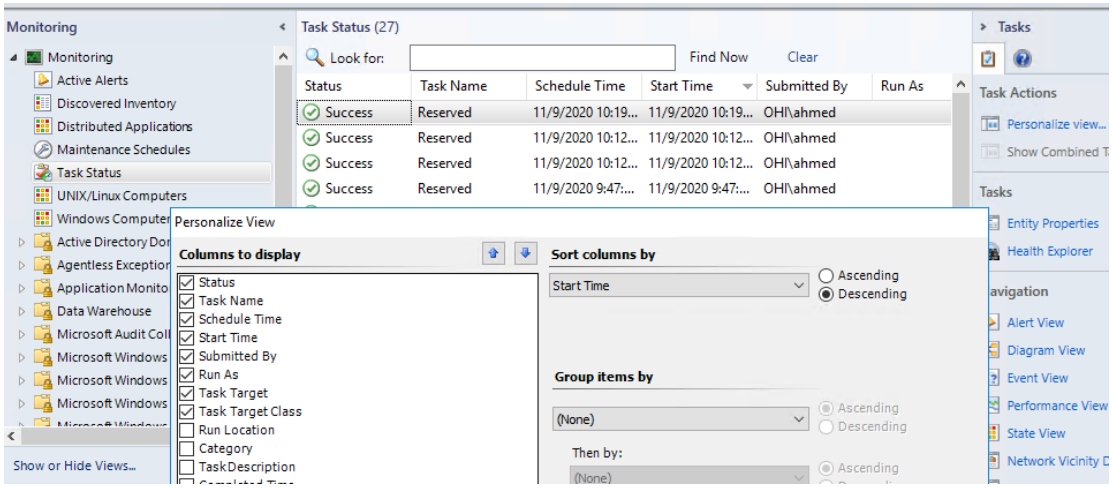
2. **Personalize Alert Views:**
    - **Step 4:** Personalize the Active Alerts view to display relevant columns such as Severity, Source, Name, and Resolution State.







3. **Customize Task Status View:**
    - **Step 5:** Personalize the Task Status view to display information such as Task Name, Schedule Time, Start Time, and Status.



Using "My Workspace" in SCOM

"My Workspace" in System Center Operations Manager (SCOM) is a customizable area where you can create and save personalized views, searches, and dashboards. This feature allows you to tailor the SCOM console to display the most relevant information for your specific needs, improving efficiency and focus.

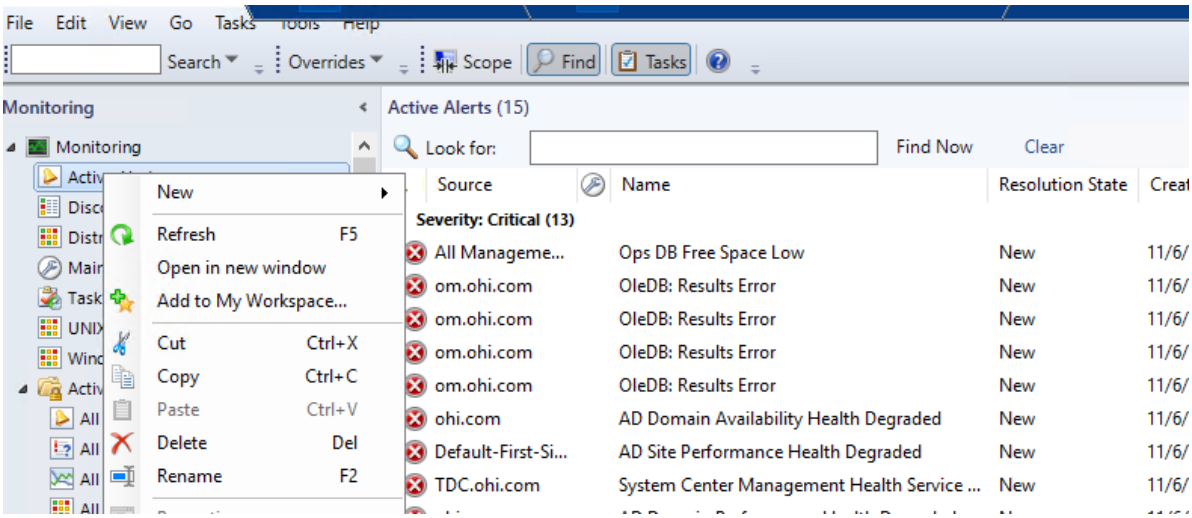
Features of "My Workspace"

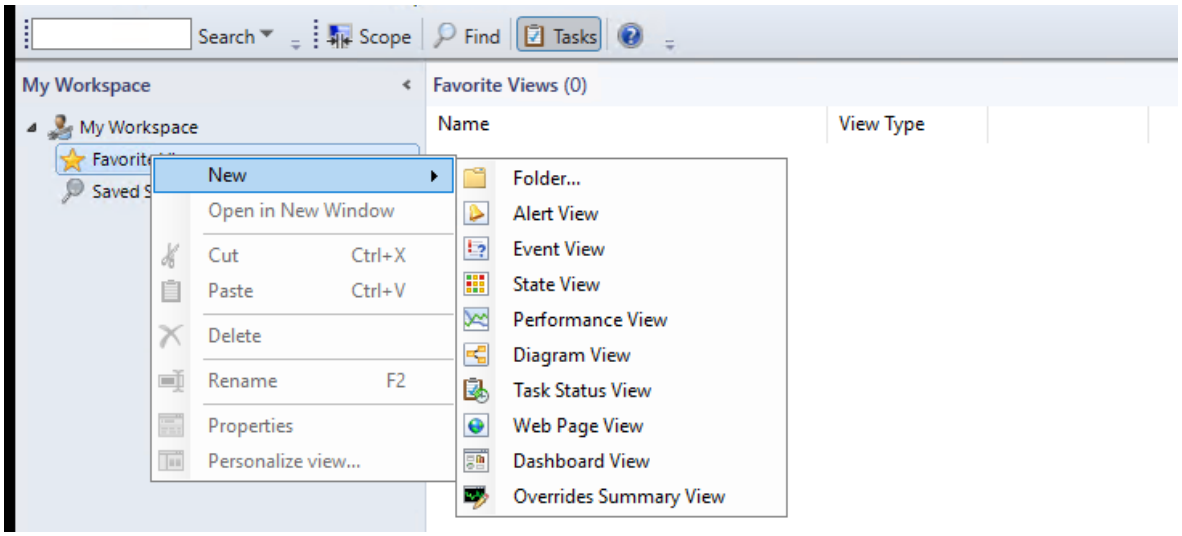
1. **Favorite Views**: Save and organize the views you use most frequently.
2. **Saved Searches**: Create and save searches to quickly find specific alerts, events, or objects.
3. **Dashboards**: Customize dashboards to monitor key performance indicators and health states at a glance.

Example: Creating and Using an Alert View

1. Creating an Alert View:

- **Step 1:** Navigate to "My Workspace" and right-click under "Favorite Views."
- **Step 2:** Select New > Alert View.



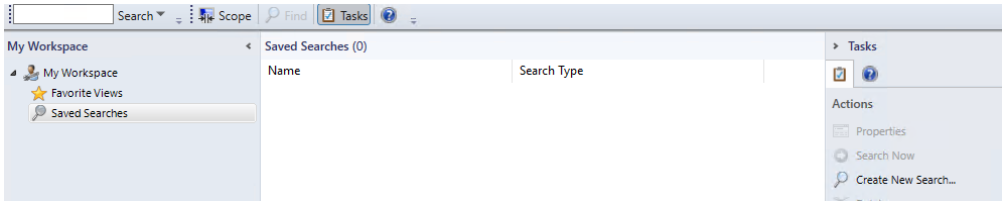


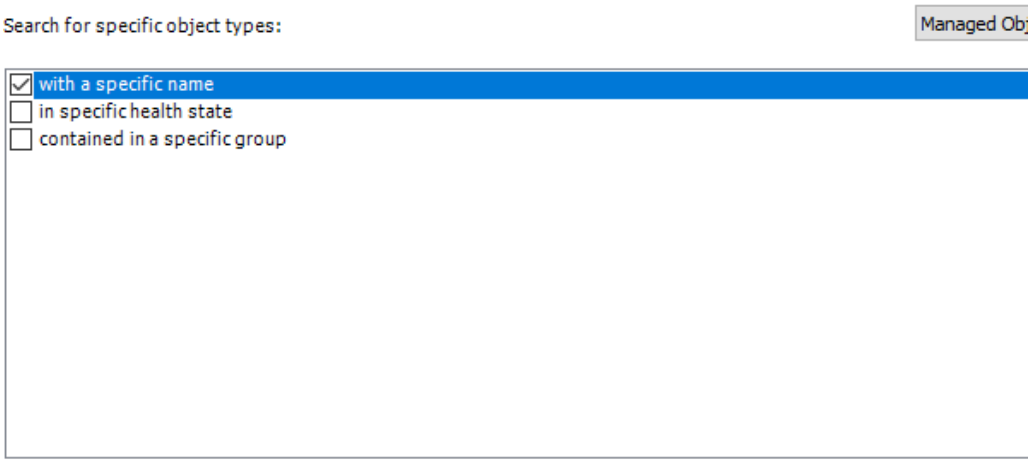
2. Configuring the Alert View:

- **Step 1:** In the properties window, set the criteria for the alert view. For example, you can filter alerts by severity, source, or specific conditions.

3. Accessing the Alert View:

- **Step 1:** Once created, the alert view will be listed under "Favorite Views" in "My Workspace."
- **Step 2:** Click on the alert view to display alerts matching your criteria.





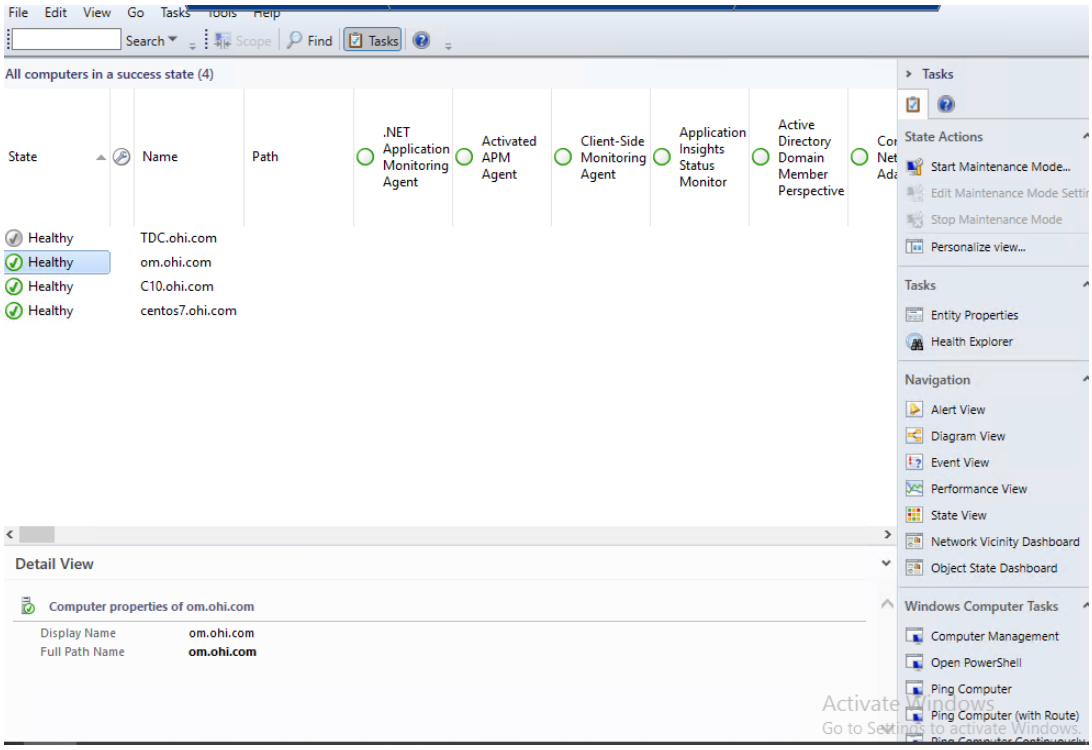


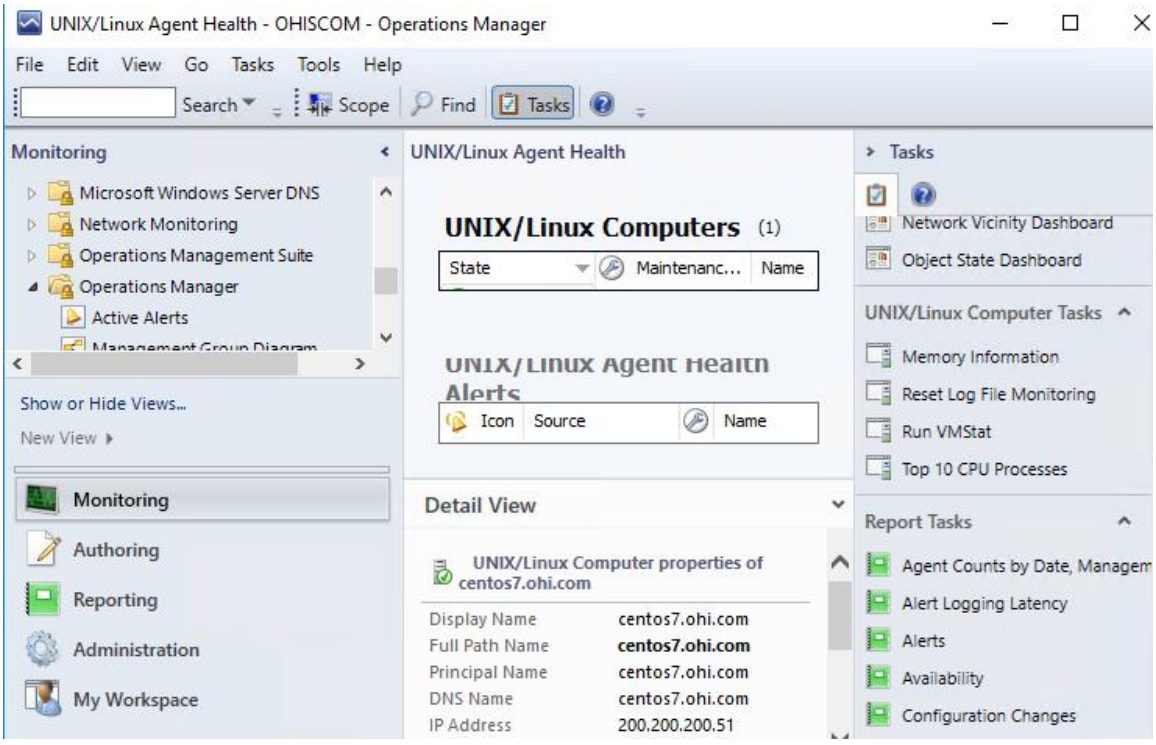
Computer Task Options in SCOM

In System Center Operations Manager (SCOM), various tasks can be performed on monitored computers. These tasks help administrators manage and troubleshoot the health and performance of the systems efficiently. Below are some of the available computer task options, along with examples from the provided screenshots:

Available Computer Task Options

1. **Computer Management**:
   - Opens the Computer Management console for the selected machine.
2. **Open PowerShell:**
   - Launches a PowerShell session on the selected machine for executing commands and scripts remotely.
3. **Ping Computer:**
   - Sends a ping request to the selected machine to check its network connectivity and response time.
   - Two options are usually available:
     - **Ping Computer**
     - **Ping Computer (with Route)**
4. **Navigation Tasks:**
   - Provides quick access to various views such as Alert View, Diagram View, Event View, Performance View, State View, Network Vicinity Dashboard, and Object State Dashboard.
5. **UNIX/Linux Computer Tasks:**
   - Specific to monitoring UNIX/Linux machines, including:
     - **Memory Information**: Displays memory usage details of the selected UNIX/Linux machine.
     - **Reset Log File Monitoring**: Resets the monitoring of log files for the selected UNIX/Linux machine.
     - **Run VMStat**: Executes the vmstat command to provide virtual memory statistics.
     - **Top 10 CPU Processes**: Lists the top 10 processes consuming the most CPU resources.
6. **Report Tasks:**
   - Generates various reports related to the selected computer, including:
     - **Agent Counts by Date, Manager, and Version**: Displays the count of agents based on their installation date, manager, and version.
     - **Alert Logging Latency**: Provides a report on the latency of alert logging.
     - **Alerts**: Lists all alerts generated by the selected computer.
     - **Availability**: Shows the availability report of the selected computer.
     - **Configuration Changes**: Lists configuration changes on the selected computer.


File Edit View Go Tasks Tools Help
Search Scope Find Tasks
All computers in a success state (4)
State
Name
Path
.NET Application Monitoring Agent
Activated APM Agent
Client-Side Monitoring Agent
Application Insights Status Monitor
Active Directory Domain Member Perspective
Healthy TDC.ohi.com
Healthy om.ohi.com
Healthy C10.ohi.com
Healthy centos7.ohi.com
Tasks
State Actions
Start Maintenance Mode...
Edit Maintenance Mode Setti
Stop Maintenance Mode
Personalize view...
Tasks
Entity Properties
Health Explorer
Navigation
Alert View
Diagram View
Event View
Performance View
State View
Network Vicinity Dashboard
Object State Dashboard
Windows Computer Tasks
Computer Management
Open PowerShell
Ping Computer
Ping Computer (with Route)
Detail View
Computer properties of om.ohi.com
Display Name om.ohi.com
Full Path Name om.ohi.com
Activate Windows
Go to Settings to activate Windows.


UNIX/Linux Agent Health - OHISCOM - Operations Manager
File Edit View Go Tasks Tools Help
Search Scope Find Tasks
Monitoring
Microsoft Windows Server DNS
Network Monitoring
Operations Management Suite
Operations Manager
Active Alerts
Show or Hide Views...
New View
Monitoring
Authoring
Reporting
Administration
My Workspace
UNIX/Linux Agent Health
UNIX/Linux Computers (1)
State
Maintenanc...
Name
UNIX/Linux Agent Health Alerts
Icon
Source
Name
Detail View
UNIX/Linux Computer properties of centos7.ohi.com
Display Name centos7.ohi.com
Full Path Name centos7.ohi.com
Principal Name centos7.ohi.com
DNS Name centos7.ohi.com
IP Address 200.200.200.51
Tasks
Network Vicinity Dashboard
Object State Dashboard
UNIX/Linux Computer Tasks
Memory Information
Reset Log File Monitoring
Run VMStat
Top 10 CPU Processes
Report Tasks
Agent Counts by Date, Managem
Alert Logging Latency
Alerts
Availability
Configuration Changes

Configuring SSL for SQL Server Reporting Services (SSRS) on SCOM

Configuring SSL for SQL Server Reporting Services (SSRS) enhances the security of data transmission between clients and the report server. Here's how to set up SSL for SSRS in the context of System Center Operations Manager (SCOM):

Step-by-Step Guide

Prerequisites

1. **SSL Certificate**: Ensure you have a valid SSL certificate installed on the server where SSRS is running.
2. **Administrator Privileges**: You need administrative rights to configure SSRS and bind the SSL certificate.

Step 1: Open Reporting Services Configuration Manager

1. **Launch**: Open the Reporting Services Configuration Manager.
2. **Connect**: Select the SQL Server instance hosting your SSRS and click Connect.

Step 2: Navigate to Web Portal URL

1. **Select Web Portal URL**: In the left pane, select Web Portal URL.

Step 3: Configure HTTP and HTTPS Bindings

1. **HTTP Bindings**:
    - In the Web Portal URL section, you will see the existing HTTP bindings.
    - If needed, you can modify or add additional HTTP bindings.
2. **HTTPS Bindings**:
    - Click Advanced.
    - In the Advanced Multiple Web Site Configuration window, click Add under Multiple HTTPS Identities for the current Reporting Services feature.

Step 4: Add HTTPS Binding

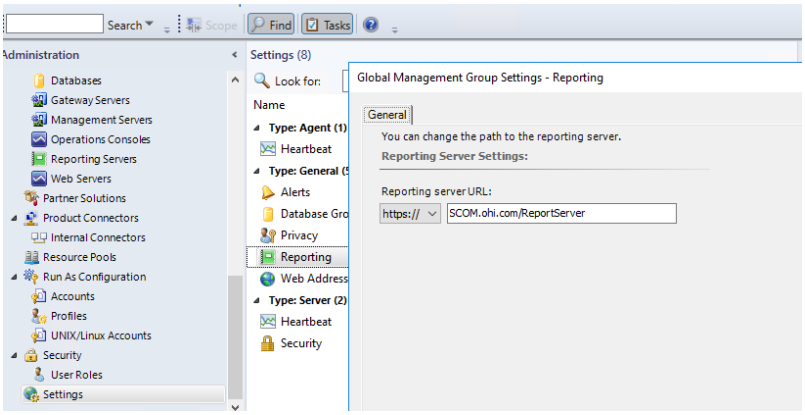
1. **Select IP Address**: From the IP Address drop-down, select the appropriate IP address (e.g., (All IPv4)).
2. **HTTPS Port**: Enter the HTTPS port, typically 443.
3. **Select Certificate**:
    - From the Certificate drop-down, select the installed SSL certificate. Ensure the certificate is correctly installed and recognized by the server.
4. **Host Header**: Enter the fully qualified domain name (FQDN) for the SSRS, e.g., scom.ohi.com.
5. **URL**: The URL field will automatically populate based on the FQDN and port entered, e.g., https://scom.ohi.com:443/Reports.
6. **Confirm**: Click OK to add the HTTPS binding.

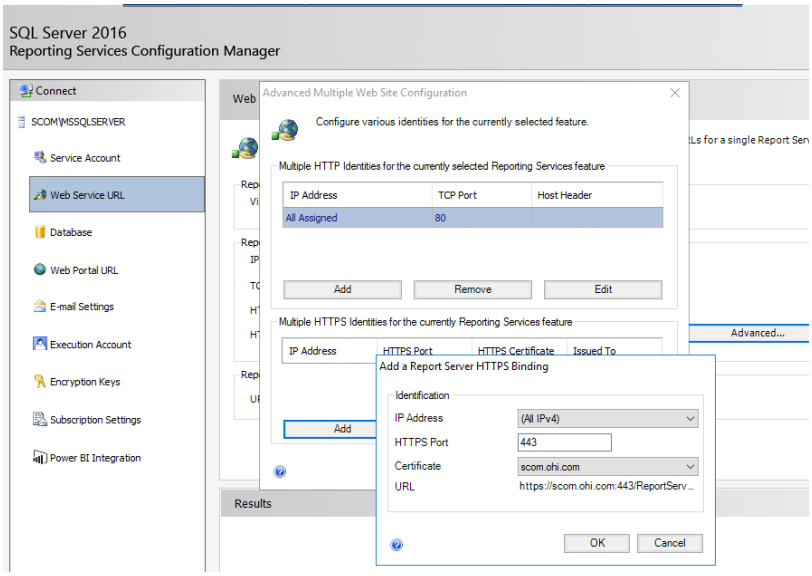
Step 5: Apply Changes

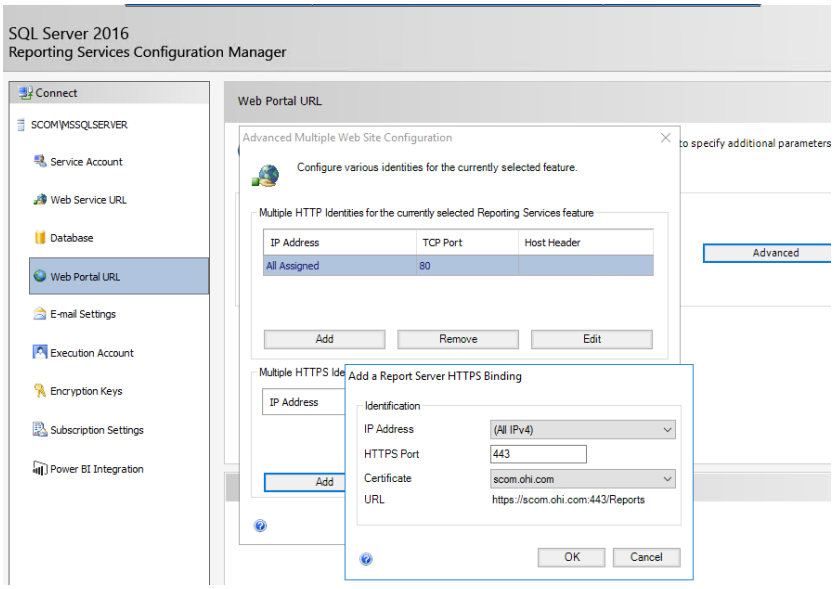
1. **Apply**: Click Apply to save the configuration changes.
2. **Verify**: Ensure that both HTTP and HTTPS bindings are listed and correctly configured.

Step 6: Test the Configuration

1. **Access URL**: Open a web browser and navigate to the SSRS web portal URL using HTTPS, e.g., https://scom.ohi.com:443/Reports.
2. **Verify SSL**: Ensure that the connection is secure and the SSL certificate is correctly applied.


Search
Scope
Find
Tasks
Administration
Databases
Gateway Servers
Management Servers
Operations Consoles
Reporting Servers
Web Servers
Partner Solutions
Product Connectors
Internal Connectors
Resource Pools
Run As Configuration
Accounts
Profiles
UNIX/Linux Accounts
Security
User Roles
Settings
Settings (8)
Look for:
Name
Type: Agent (1)
Heartbeat
Type: General (5
Alerts
Database Gro
Privacy
Reporting
Web Address
Type: Server (2)
Heartbeat
Security
Global Management Group Settings - Reporting
General
You can change the path to the reporting server.
Reporting Server Settings:
Reporting server URL:
https://
SCOM.ohi.com/ReportServer


SQL Server 2016
Reporting Services Configuration Manager
Connect
SCOM\MSSQLSERVER
Service Account
Web Service URL
Database
Web Portal URL
E-mail Settings
Execution Account
Encryption Keys
Subscription Settings
Power BI Integration
Advanced Multiple Web Site Configuration
Configure various identities for the currently selected feature.
Multiple HTTP Identities for the currently selected Reporting Services feature
IP Address
TCP Port
Host Header
All Assigned
80
Add
Remove
Edit
Multiple HTTPS Identities for the currently Reporting Services feature
IP Address
HTTPS Port
HTTPS Certificate
Issued To
Add
Advanced...
Add a Report Server HTTPS Binding
Identification
IP Address
(All IPv4)
HTTPS Port
443
Certificate
scom.ohi.com
URL
https://scom.ohi.com:443/ReportServ...
OK
Cancel
Results


SQL Server 2016
Reporting Services Configuration Manager
Connect
SCOM\MSSQLSERVER
Service Account
Web Service URL
Database
Web Portal URL
E-mail Settings
Execution Account
Encryption Keys
Subscription Settings
Power BI Integration
Web Portal URL
Advanced Multiple Web Site Configuration
Configure various identities for the currently selected feature.
Multiple HTTP Identities for the currently selected Reporting Services feature
IP Address
TCP Port
Host Header
All Assigned
80
Add
Remove
Edit
Advanced
Add a Report Server HTTPS Binding
Identification
IP Address
(All IPv4)
HTTPS Port
443
Certificate
scom.ohi.com
URL
https://scom.ohi.com:443/Reports
OK
Cancel

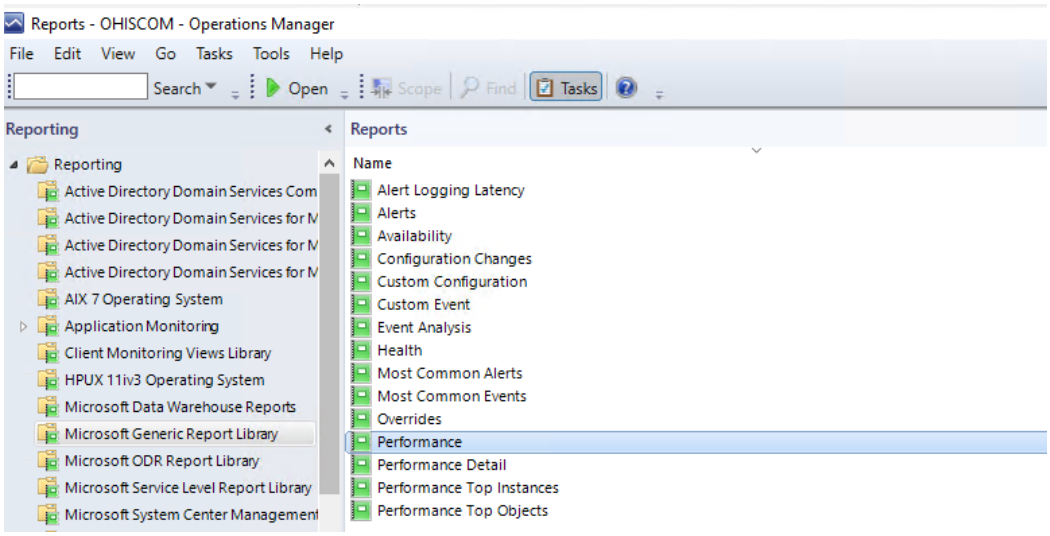
Generating a CPU Utilization Report in SCOM

To generate a CPU utilization report in System Center Operations Manager (SCOM), follow these steps using the provided screenshots as a guide.

Step-by-Step Guide

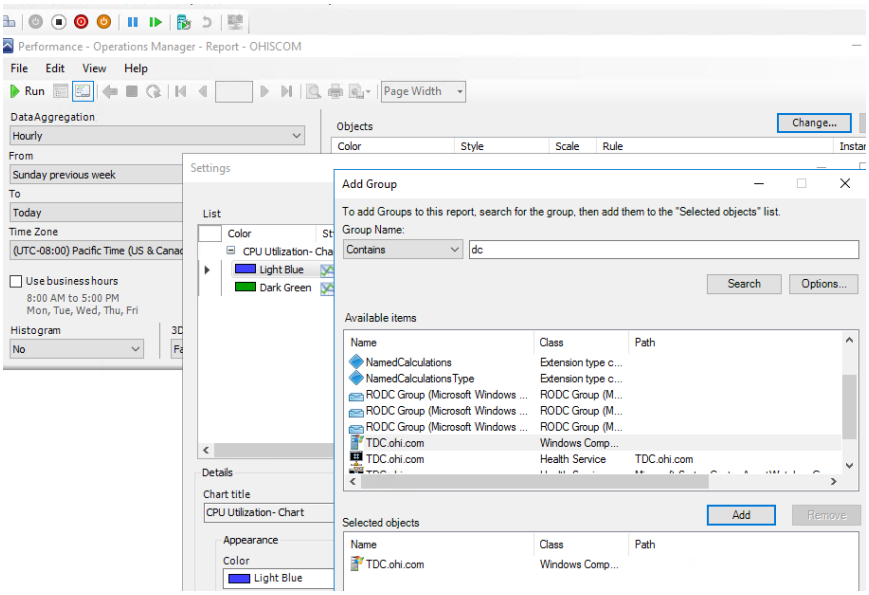
1. Access Reports in SCOM

- Open the SCOM console and navigate to Reporting > Microsoft Generic Report Library.
- Select Performance from the list of available reports.



2. Configure the Report Parameters

- Click Run to open the report configuration window.
- Set the Data Aggregation to Hourly.
- Specify the time range (From and To) for which you want to generate the report.
- Set the Time Zone as needed.

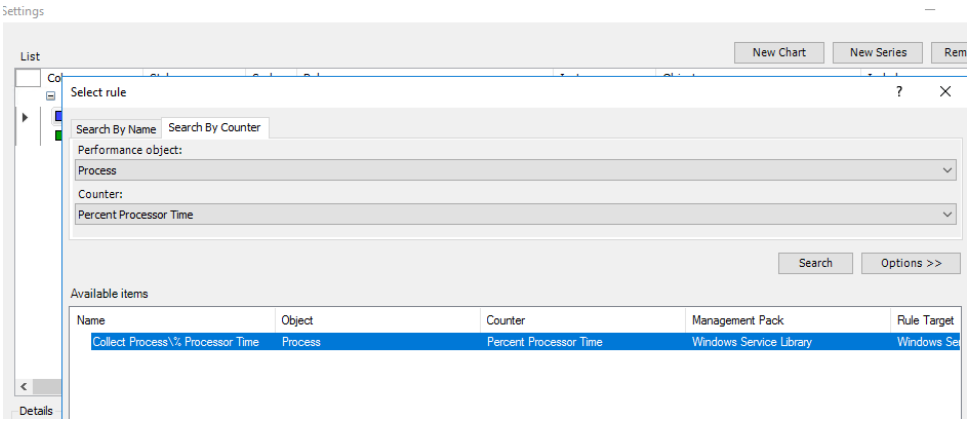


3. Add Groups and Objects

- In the Objects section, click Add Group.
- Search for the desired groups (e.g., DC groups, UNIX/Linux groups) and add them to the report.
- Similarly, click Add Object to include specific computers or instances in the report.

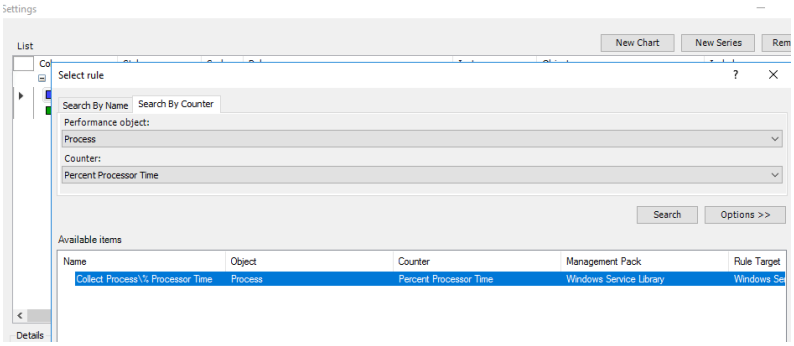
4. Select Performance Counters

- Click Add Counters to open the Select Rule window.
- Search for the Percent Processor Time counter under the Process performance object. Add the Collect Process\% Processor Time rule to the report.



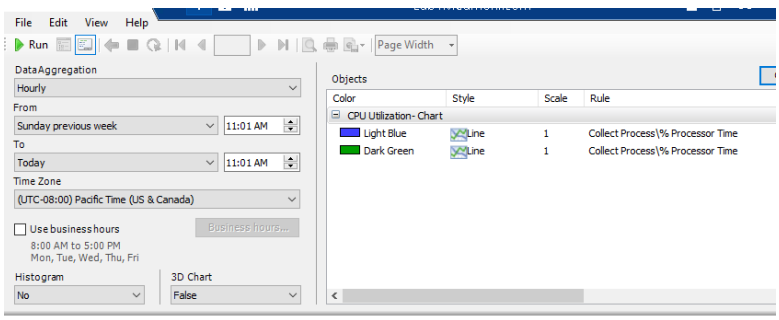
5. Customize Chart Settings

- Configure the appearance of the chart, including color, style, and scale for each performance counter.
- Ensure that the CPU utilization data for the selected objects is displayed in the chart.



6. Run and View the Report

- After configuring all parameters and settings, click Run to generate the report.
- The report will display the CPU utilization data in the specified format and time range.



Troubleshooting Blank Reports in SCOM

If you encounter blank reports in System Center Operations Manager (SCOM), one of the potential solutions involves flushing the health service state and cache for both agents and management servers. This process can help refresh the configurations and resolve any underlying issues. Here are the detailed steps to perform this troubleshooting task:

For Agents

1. Flush Health Service State and Cache from SCOM Console

- **Navigate to Agent Health State**:
  - Go to Monitoring -> OperationsManager -> Agent Details -> Agent Health State.
- **Select the Agent**:
  - Select the particular agent you want to flush.
- **Flush Health Service State and Cache**:
  - From the task pane on the right, click on Flush Health Service State and Cache.
  - This task will clear the cache and state information for the selected agent.



2. Manually Clear Cache

- **Stop the Microsoft Monitoring Agent Service**:

```
sudo systemctl stop HealthService
```

- **Rename the Health Service State Folder**:
  - Navigate to the SCOM installation directory and rename the Health Service State folder.

```
cd /var/opt/microsoft/scx/agent
sudo mv HealthServiceState HealthServiceState_Old
```

- **Start the Microsoft Monitoring Agent Service**:

```
sudo systemctl start HealthService
```

- This manual process ensures the agent reloads its configuration upon restart.

For SCOM Management Server

1. Flush Health Service State and Cache from SCOM Console

- **Navigate to Management Server State**:
  - Go to Monitoring -> OperationsManager -> Management Server -> Management Server State.
- **Select the Management Server**:
  - Select the management server you want to flush.
- **Flush Health Service State and Cache**:
  - From the task pane on the right, click on Flush Health Service State and Cache.
  - This task will clear the cache and state information for the selected management server.

2. Manually Clear Cache

- **Stop the Microsoft Monitoring Agent Service**:
  - Open a command prompt as an administrator and run:

```
net stop HealthService
```

- **Rename the Health Service State Folder**:
  - Navigate to the SCOM installation directory and rename the Health Service State folder.

```
cd "C:\Program Files\Microsoft Monitoring Agent\Agent\Health Service State"
ren "Health Service State" "Health Service State_Old"
```

- **Start the Microsoft Monitoring Agent Service**:
  - Restart the service:

```
net start HealthService
```

- This manual process ensures the management server reloads its configuration upon restart.

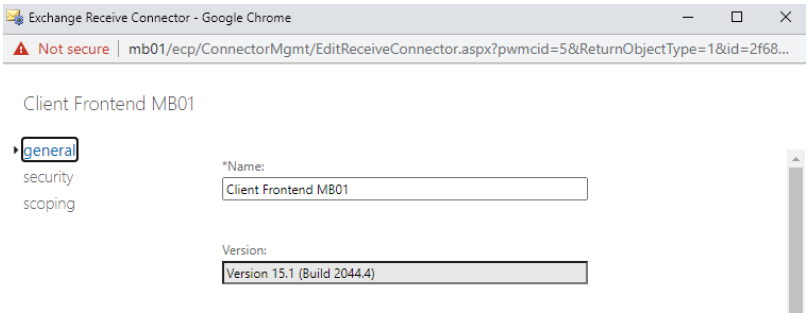
Configuring Exchange SMTP Settings for SCOM

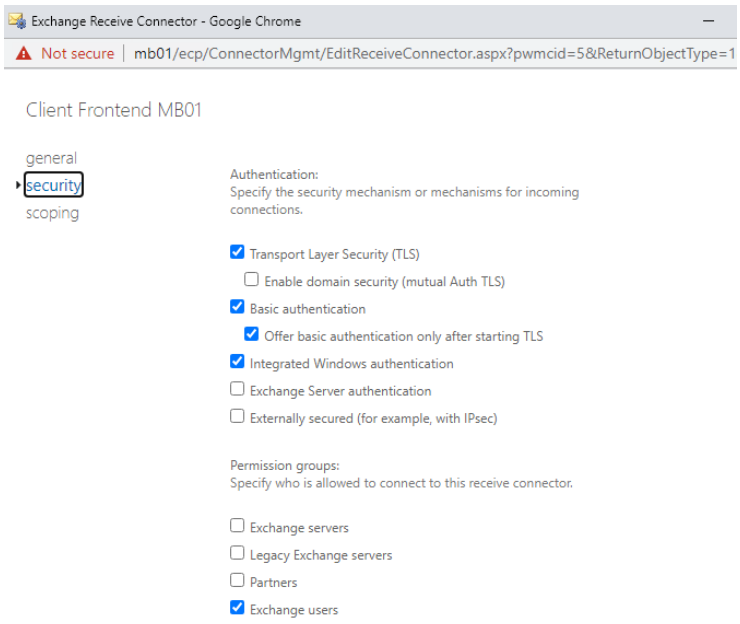
To ensure that System Center Operations Manager (SCOM) can send email notifications, in this lab I going to use Exchange server as SMTP and here is how to configure the Exchange SMTP settings. Here's how you can do this step-by-step.

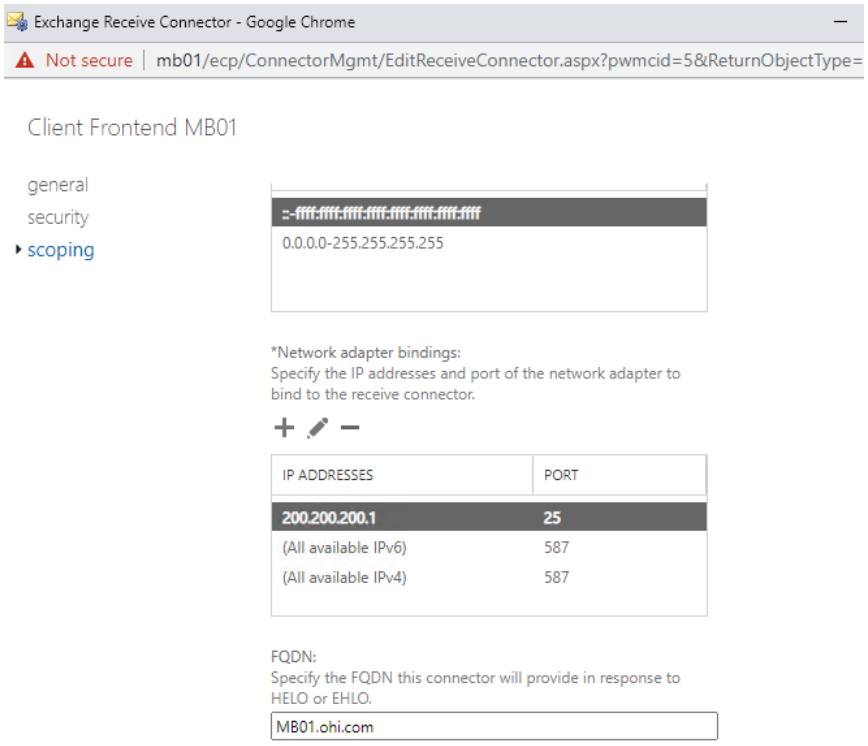
Step-by-Step Guide

1. Configure Receive Connector in Exchange

- **Step 1:** Open the Exchange Admin Center (EAC) and navigate to Mail flow -> Receive connectors.
- **Step 2:** Edit the existing receive connector or create a new one.
    - **Security Settings:**
        - Ensure Transport Layer Security (TLS) is enabled.
        - Enable Basic authentication and Integrated Windows authentication.
        - Under Permission groups, select Exchange users.
    - **Scoping Settings:**
        - Bind the connector to the appropriate IP address and port (e.g., IP: 200.200.200.1, Port: 25).
        - Specify the FQDN that the connector will provide (e.g., MB01.ohi.com).

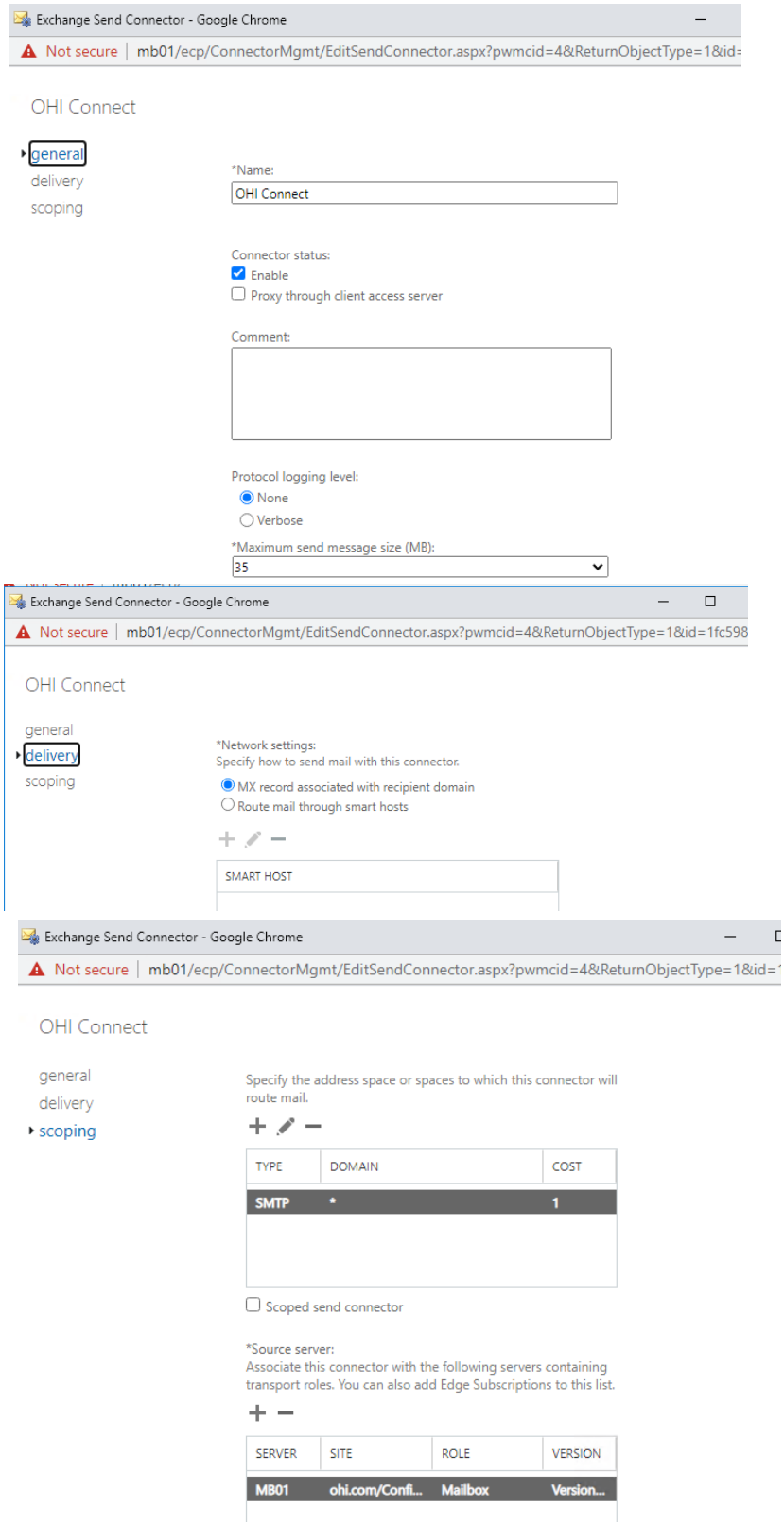






2. Configure Send Connector in Exchange

- **Step 1:** In the EAC, navigate to Mail flow -> Send connectors.
- **Step 2:** Edit the existing send connector or create a new one.
    - **General Settings:**
        - Provide a name for the connector (e.g., OHI Connect).
        - Ensure the connector status is Enabled.
        - Set the Protocol logging level to None or Verbose as needed.
        - Set the Maximum send message size as appropriate (e.g., 35 MB).
    - **Delivery Settings:**
        - Select MX record associated with recipient domain.
    - **Scoping Settings:**
        - Specify the address space (e.g., SMTP with domain *).
        - Associate the connector with the appropriate source server (e.g., MB01).


Exchange Send Connector - Google Chrome
Not secure | mb01/ecp/ConnectorMgmt/EditSendConnector.aspx?pwmcid=4&ReturnObjectType=1&id=
OHI Connect
general
delivery
scoping
*Name:
OHI Connect
Connector status:
Enable
Proxy through client access server
Comment:
Protocol logging level:
None
Verbose
*Maximum send message size (MB):
35
Exchange Send Connector - Google Chrome
Not secure | mb01/ecp/ConnectorMgmt/EditSendConnector.aspx?pwmcid=4&ReturnObjectType=1&id=1fc598
OHI Connect
general
delivery
scoping
*Network settings:
Specify how to send mail with this connector.
MX record associated with recipient domain
Route mail through smart hosts
SMART HOST
Exchange Send Connector - Google Chrome
Not secure | mb01/ecp/ConnectorMgmt/EditSendConnector.aspx?pwmcid=4&ReturnObjectType=1&id=
OHI Connect
general
delivery
scoping
Specify the address space or spaces to which this connector will route mail.
TYPE
DOMAIN
COST
SMTP
*
1
Scoped send connector
*Source server:
Associate this connector with the following servers containing transport roles. You can also add Edge Subscriptions to this list.
SERVER
SITE
ROLE
VERSION
MB01
ohi.com/Confi...
Mailbox
Version...

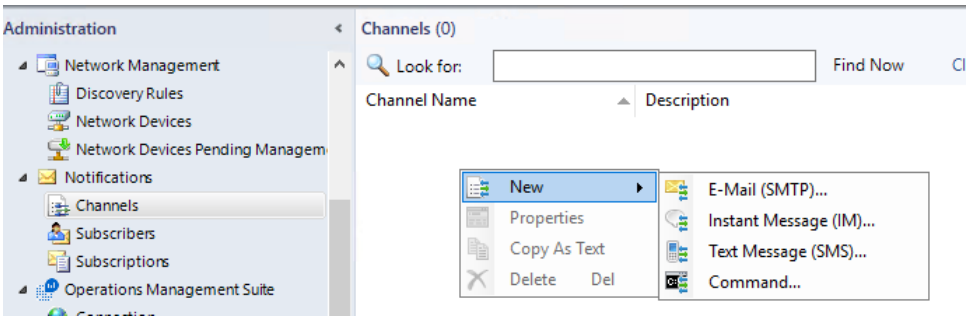
Configuring Notifications in SCOM

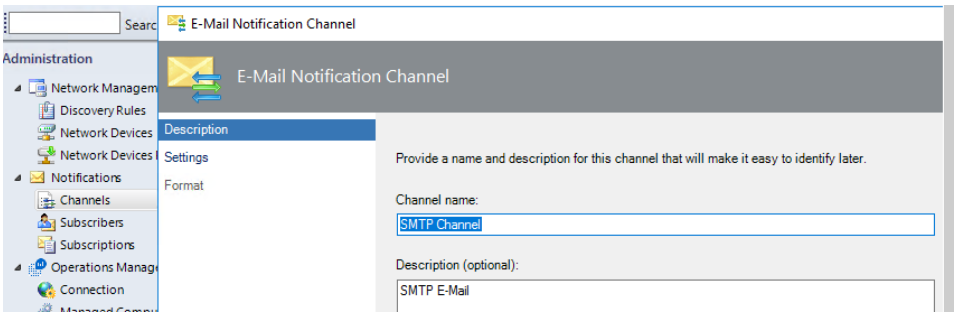
Setting up notifications in System Center Operations Manager (SCOM) allows administrators to receive alerts about critical events in their monitored environment. This guide will walk you through the process of configuring email notifications using the provided screenshots.

Step-by-Step Guide

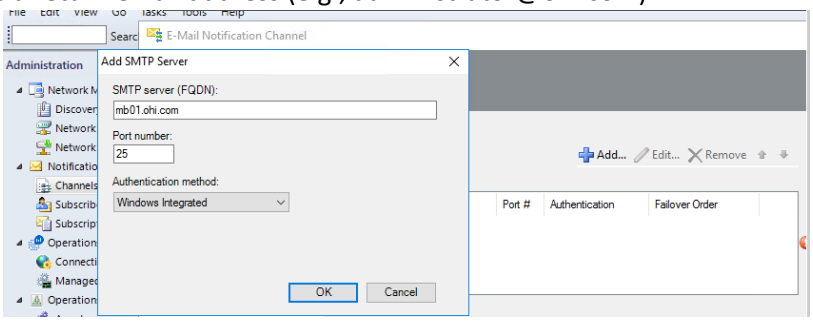
1. Configure the Notification Channel

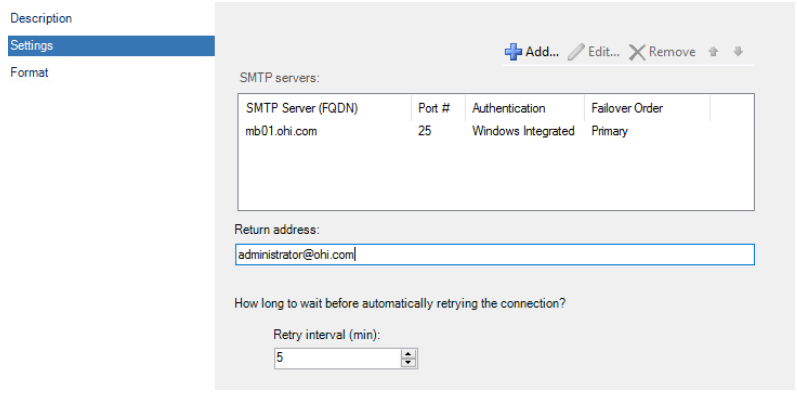
- **Step 1:** Navigate to Administration -> Notifications -> Channels.
- **Step 2:** Right-click and select New -> E-Mail (SMTP)... to create a new email notification channel.
- **Step 3:** Provide a name for the channel, such as SMTP Channel.



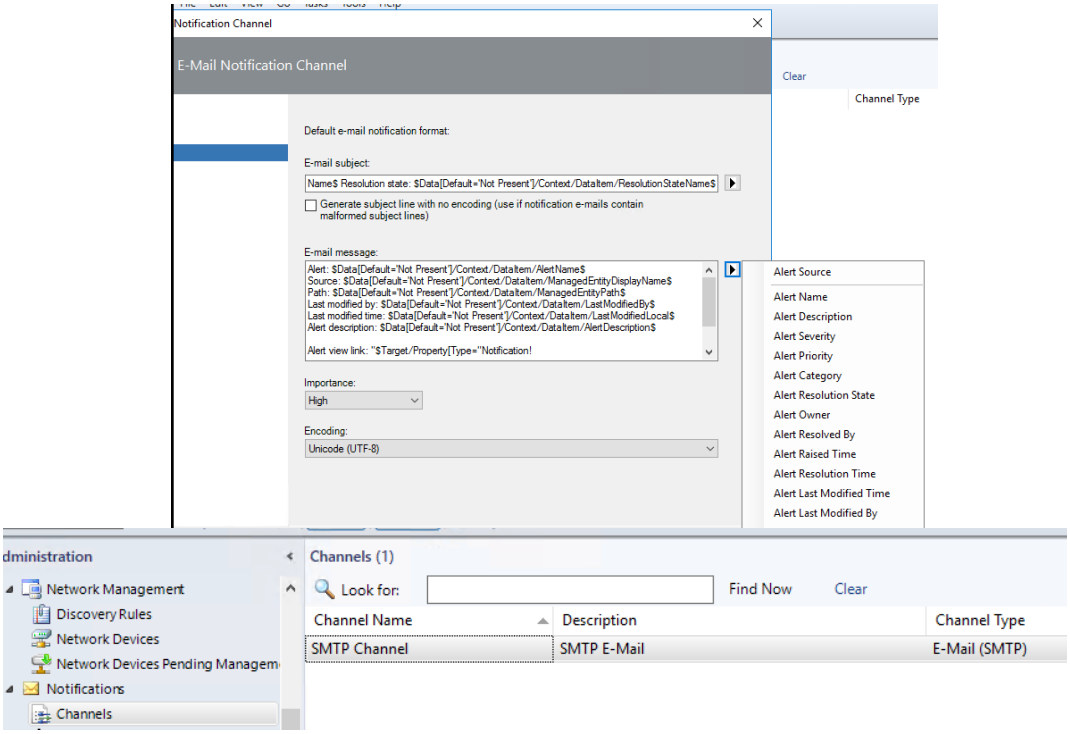


- **Step 4:** Configure the SMTP server settings:
  - Enter the SMTP server FQDN (e.g., mb01.ohi.com).
  - Set the port number to 25.
  - Choose the authentication method (Windows Integrated).
  - Provide a return email address (e.g., administrator@ohi.com).



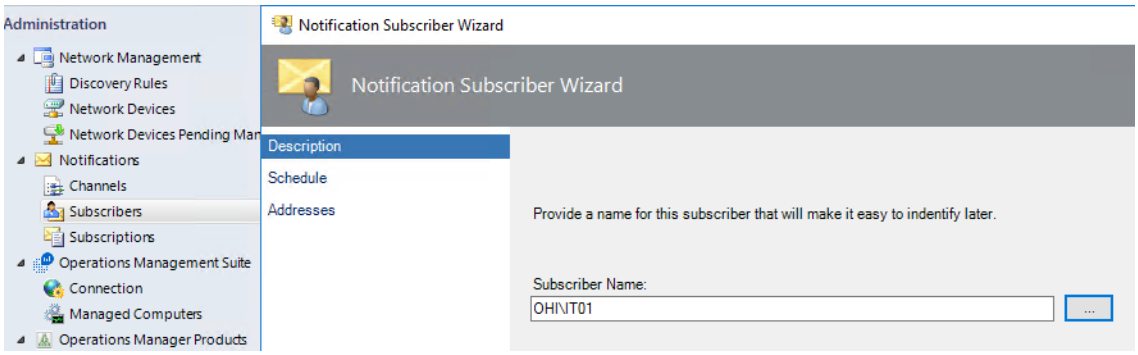


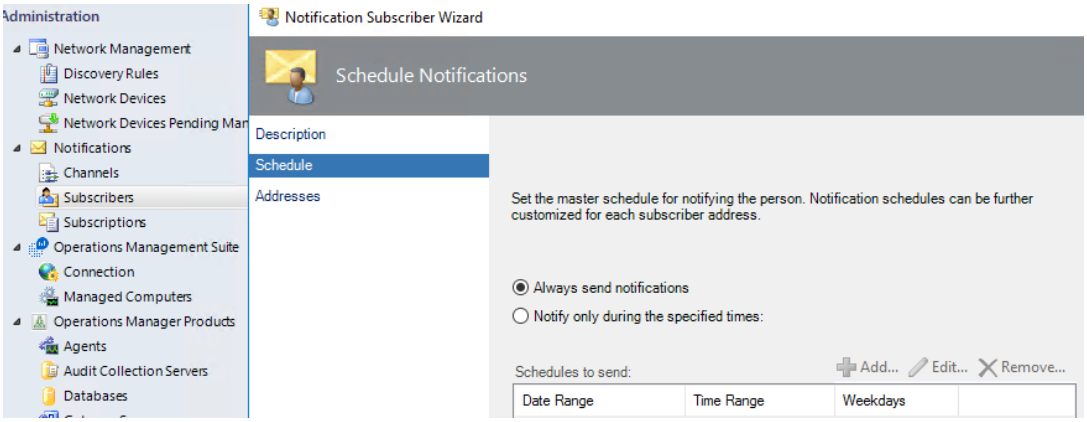
- **Step 5:** Configure the email format:
  - Set the email subject and message format.
  - Use available variables for dynamic content (e.g., Alert Source, Alert Name).

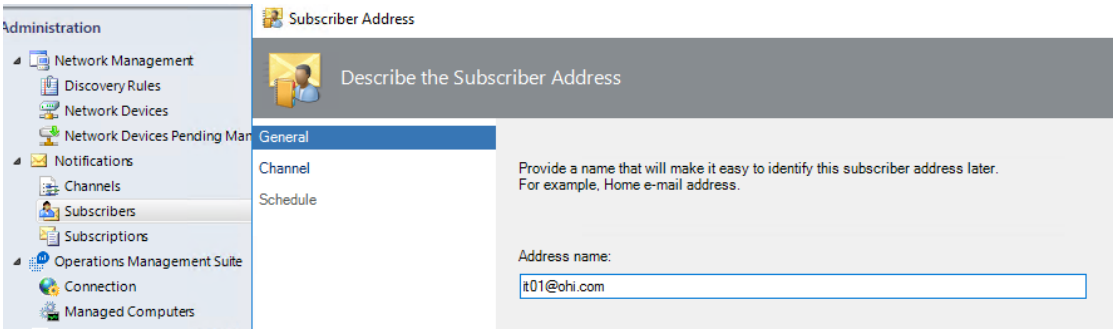


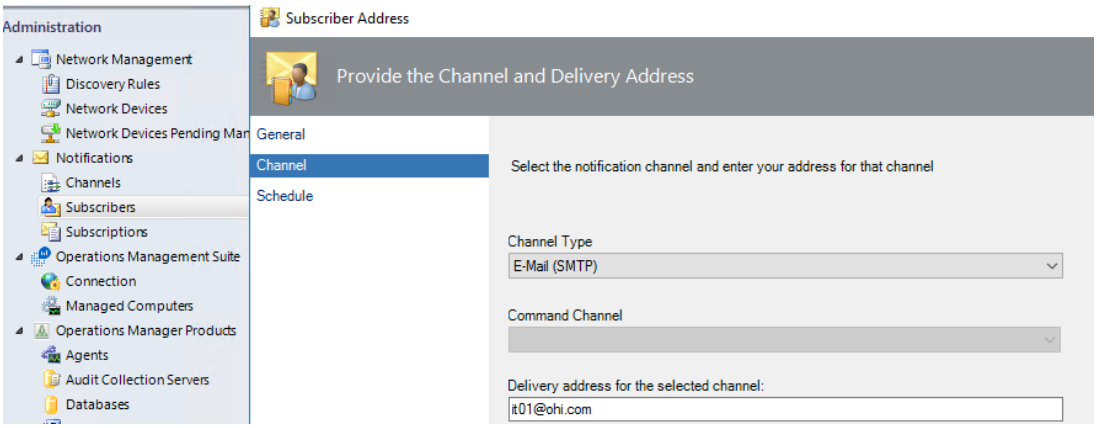
2. Create a Notification Subscriber

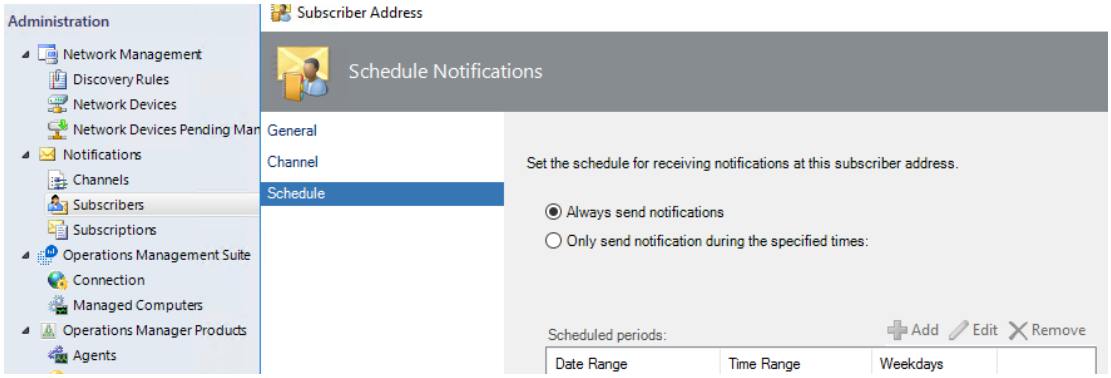
- **Step 1:** Navigate to Administration -> Notifications -> Subscribers.
- **Step 2:** Right-click and select New -> Subscriber... to create a new notification subscriber.
- **Step 3:** Provide a name for the subscriber, such as OHINT01.
- **Step 4:** Configure the notification schedule:
  - Choose Always send notifications or specify a time range for sending notifications.
- **Step 5:** Add the subscriber's email address:
  - Provide an address name (e.g., it01@ohi.com).
  - Select the channel type as E-Mail (SMTP).
  - Enter the delivery address (e.g., it01@ohi.com).

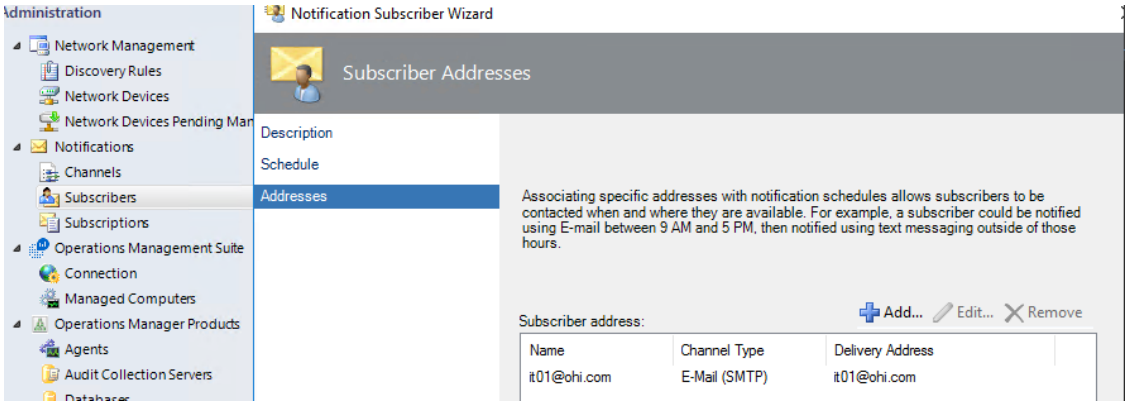






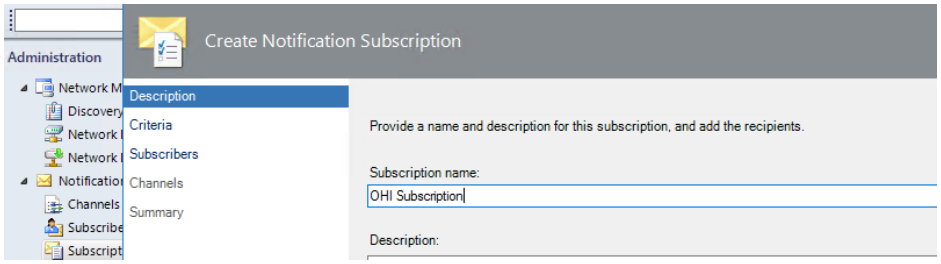

Administration
Network Management
Discovery Rules
Network Devices
Network Devices Pending Mar
Notifications
Channels
Subscribers
Subscriptions
Operations Management Suite
Connection
Managed Computers
Operations Manager Products
Agents
Audit Collection Servers
Databases
Subscriber Address
Provide the Channel and Delivery Address
General
Channel
Schedule
Select the notification channel and enter your address for that channel
Channel Type
E-Mail (SMTP)
Command Channel
Delivery address for the selected channel:
it01@ohi.com

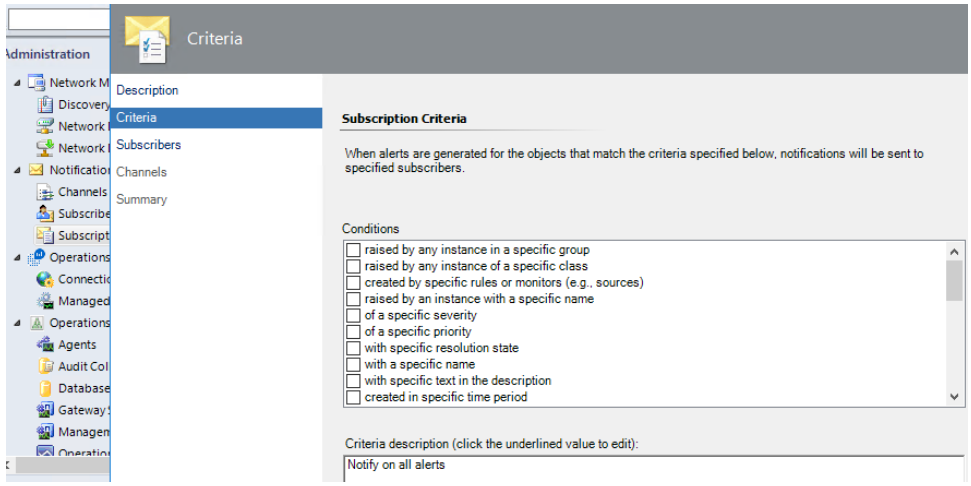

Administration
Network Management
Discovery Rules
Network Devices
Network Devices Pending Mar
Notifications
Channels
Subscribers
Subscriptions
Operations Management Suite
Connection
Managed Computers
Operations Manager Products
Agents
Subscriber Address
Schedule Notifications
General
Channel
Schedule
Set the schedule for receiving notifications at this subscriber address.
Always send notifications
Only send notification during the specified times:
Scheduled periods:
Add
Edit
Remove
Date Range
Time Range
Weekdays

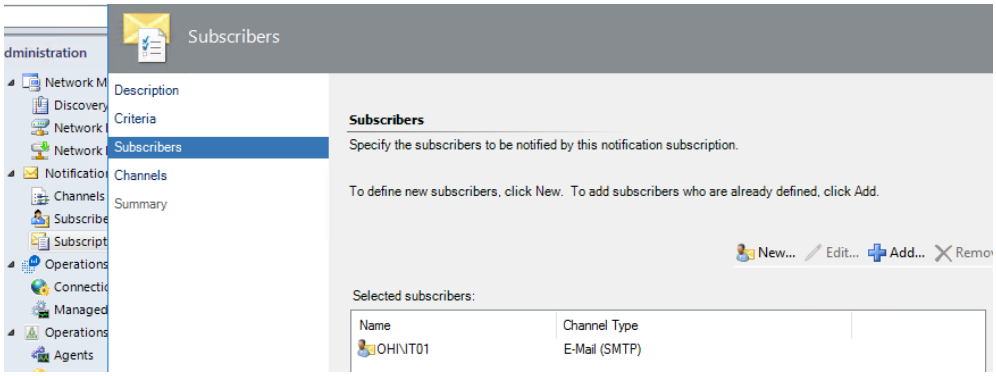

Administration
Network Management
Discovery Rules
Network Devices
Network Devices Pending Mar
Notifications
Channels
Subscribers
Subscriptions
Operations Management Suite
Connection
Managed Computers
Operations Manager Products
Agents
Audit Collection Servers
Notification Subscriber Wizard
Subscriber Addresses
Description
Schedule
Addresses
Associating specific addresses with notification schedules allows subscribers to be contacted when and where they are available. For example, a subscriber could be notified using E-mail between 9 AM and 5 PM, then notified using text messaging outside of those hours.
Subscriber address:
Add...
Edit...
Remove
Name
Channel Type
Delivery Address
it01@ohi.com
E-Mail (SMTP)
it01@ohi.com

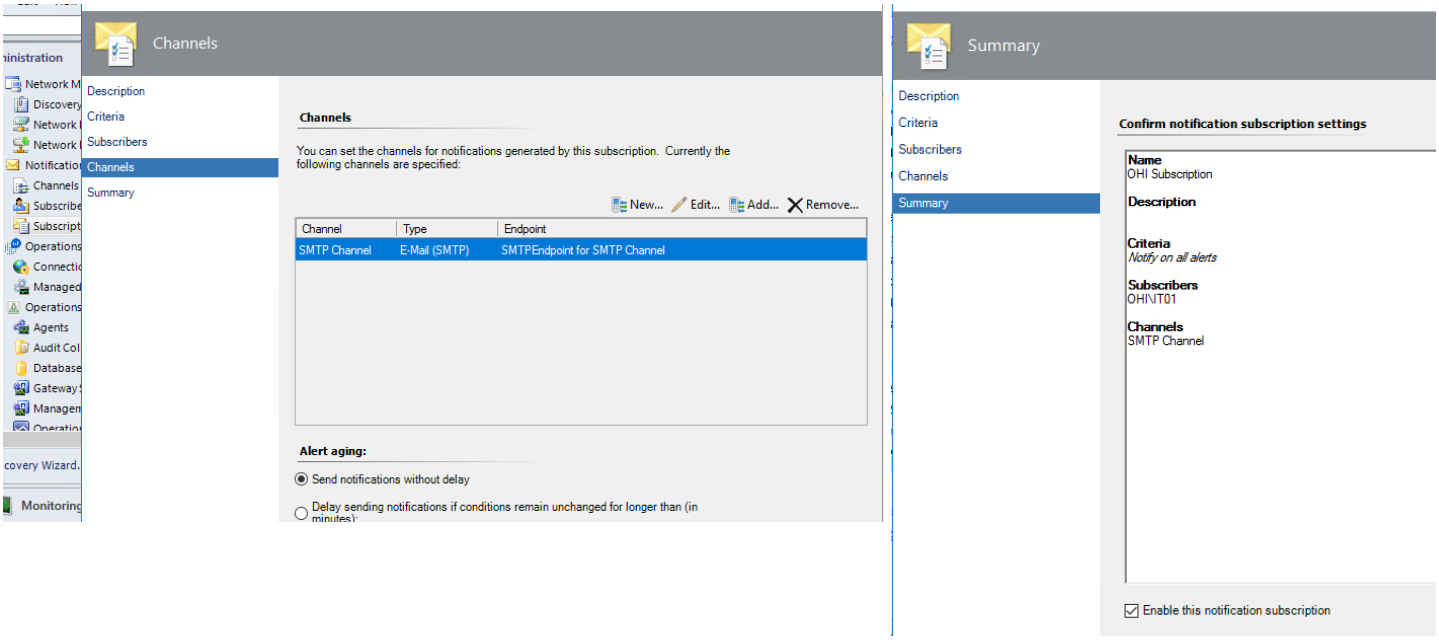
3. Create a Notification Subscription

- **Step 1:** Navigate to Administration -> Notifications -> Subscriptions.
- **Step 2:** Right-click and select New -> Subscription... to create a new notification subscription.
- **Step 3:** Provide a name for the subscription, such as OHI Subscription.
- **Step 4:** Configure the subscription criteria:
  - Define the conditions that will trigger the notification (e.g., notify on all alerts).
- **Step 5:** Add the subscribers to the subscription:
  - Select the previously created subscriber (e.g., OHINT01).
- **Step 6:** Add the notification channels:
  - Select the previously created notification channel (e.g., SMTP Channel).
- **Step 7:** Review and confirm the subscription settings.



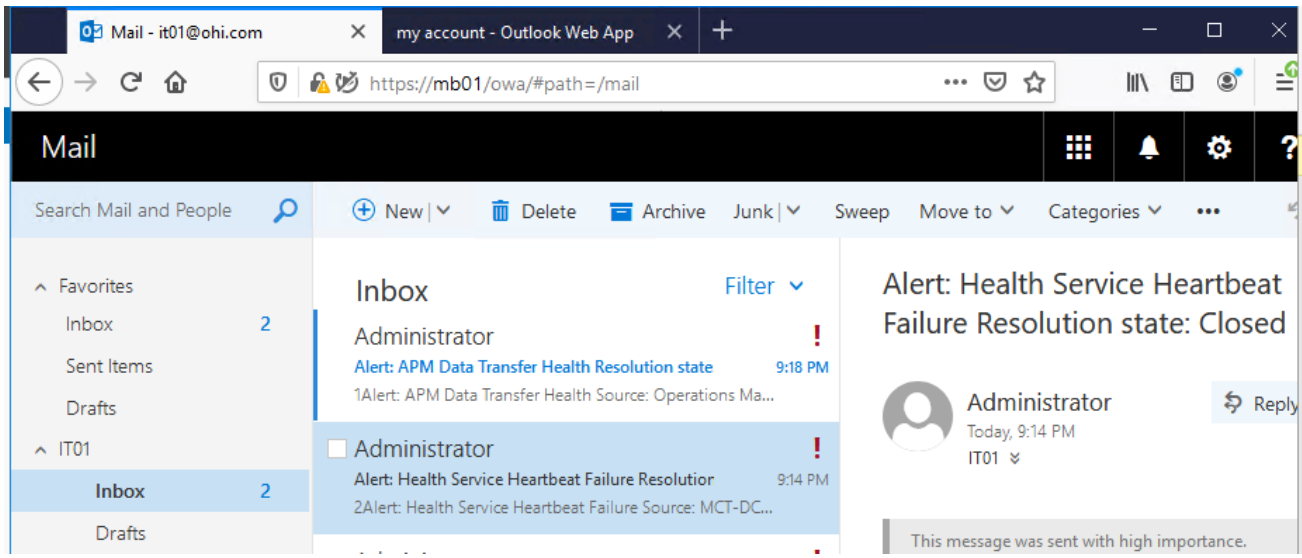






4. Verify the Notification

- **Step 1:** Trigger an alert in SCOM to test the notification setup.
- **Step 2:** Check the subscriber's email inbox for the notification.

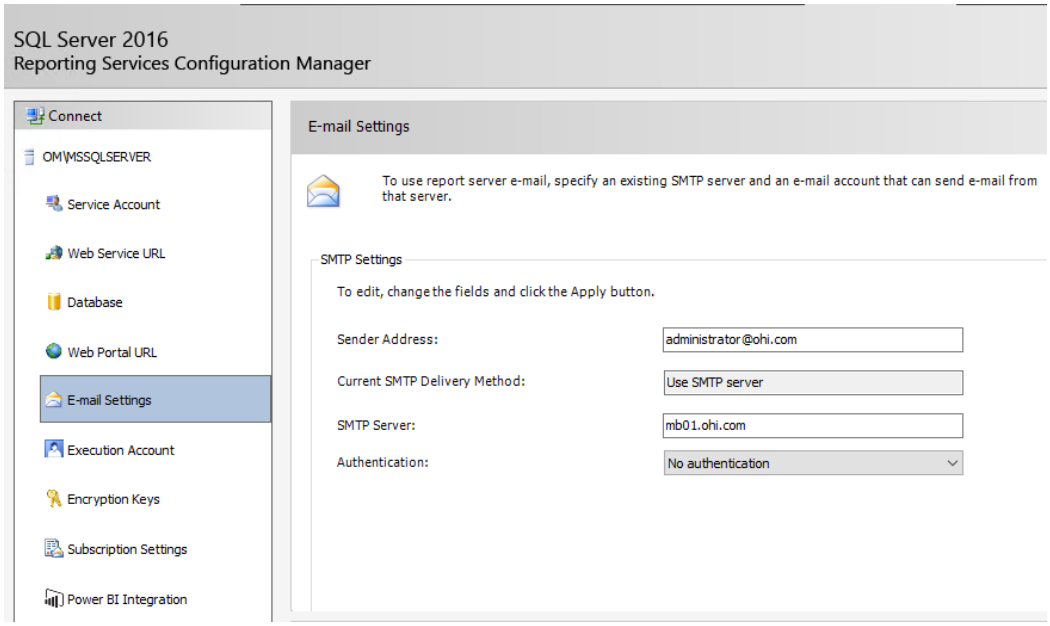


Enabling Email Report Delivery in SQL Server Reporting Services (SSRS)

To enable the delivery of reports via email in SQL Server Reporting Services (SSRS), follow these steps:

Step 1: Configure Email Settings in SSRS

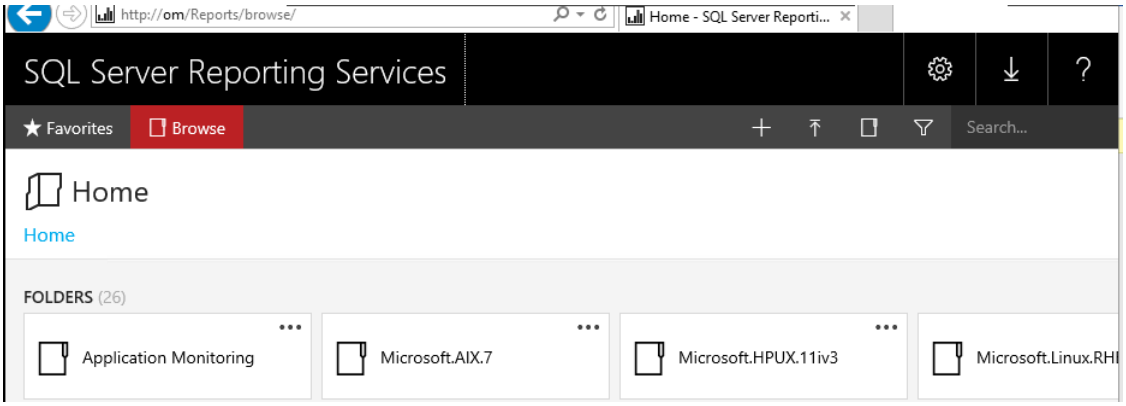
1. **Open Reporting Services Configuration Manager:**
   - Connect to the report server instance.
2. **Navigate to the E-Mail Settings:**
   - Go to the E-Mail Settings section.
3. **Set Up the SMTP Server:**
   - **Sender Address:** Enter the email address from which the reports will be sent (e.g., administrator@ohi.com).
   - **SMTP Server:** Enter the address of your SMTP server (e.g., mb01.ohi.com).
   - **Authentication:** Choose the appropriate authentication method. For this example, No authentication is selected.
   - **Apply the Settings:**

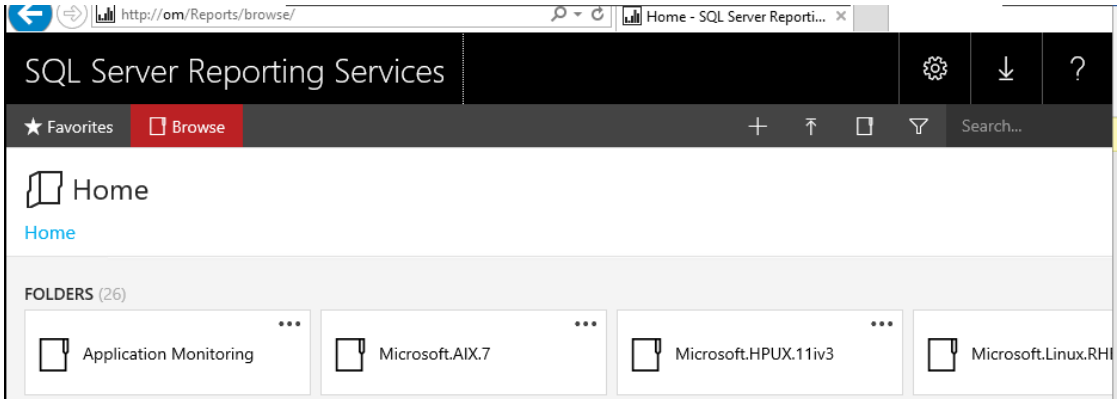


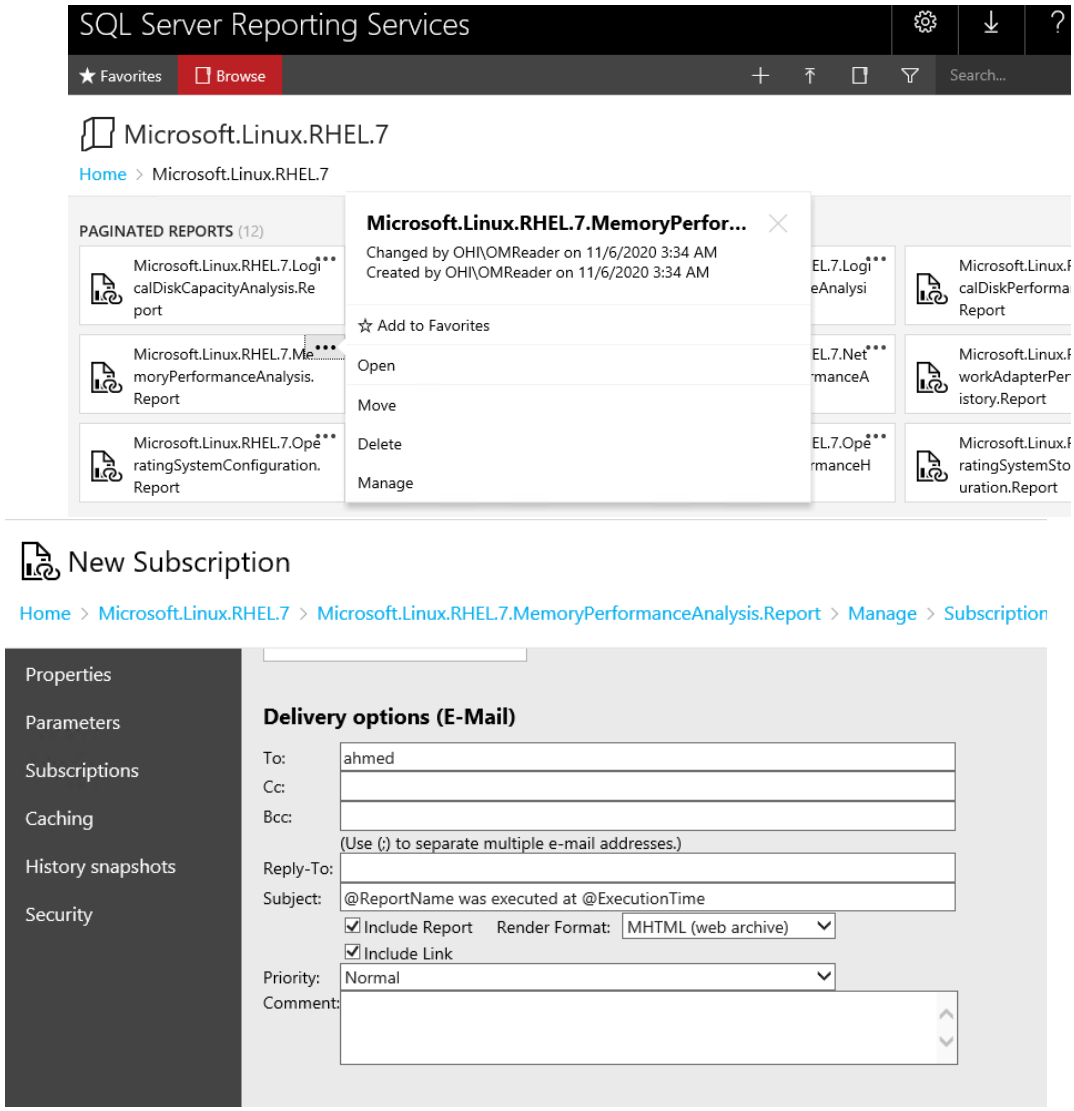
Step 2: Create a Subscription for the Report

1. **Access the SSRS Web Portal:**
   - Navigate to the URL of your SSRS Web Portal (e.g., http://om/Reports).
2. **Select the Report for Subscription:**
   - Locate and select the report you want to send via email (e.g., Microsoft.Linux.RHEL.7.MemoryPerformanceAnalysis.Report).
   - Click on the ellipsis (...) next to the report and select Subscribe.

3. **Configure the Subscription:**
    - **Delivery Options (E-Mail):**
        - **To:** Enter the recipient's email address (e.g., ahmed).
        - **Subject:** Customize the email subject line if necessary.
        - **Include Report:** Check this option if you want the report included in the email.
        - **Render Format:** Choose the format for the report (e.g., MHTML (web archive)).
        - **Include Link:** Optionally, include a link to the report.
        - **Priority:** Set the email priority.
        - **Comments:** Add any additional comments if needed.
    - Save the subscription settings.





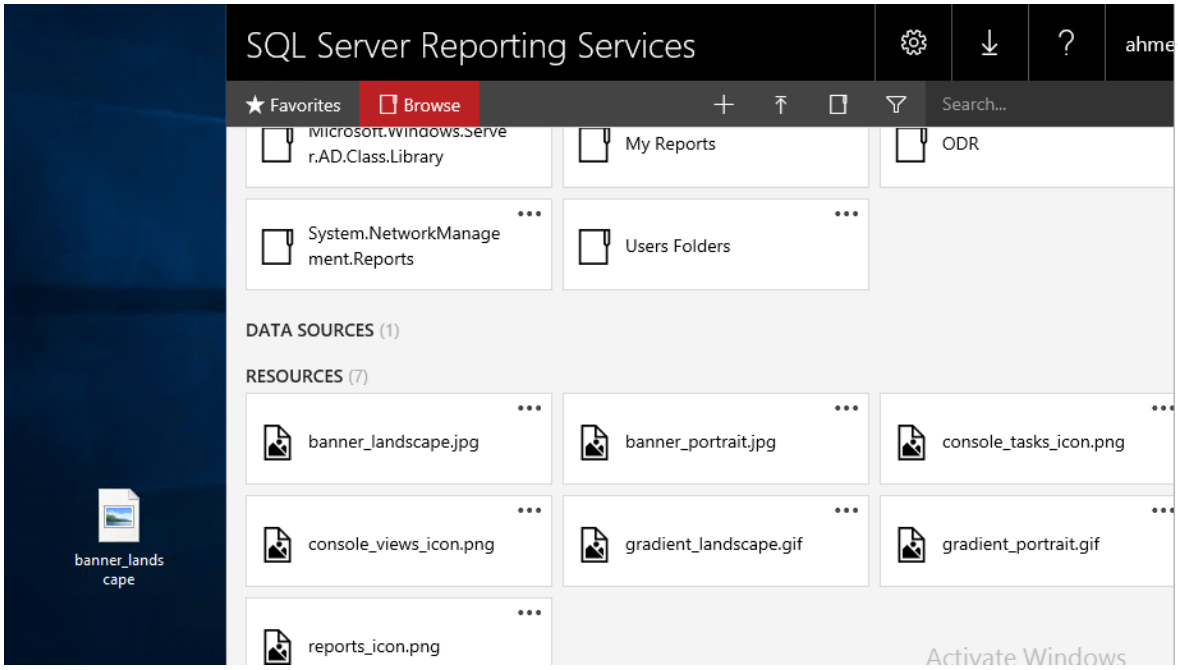


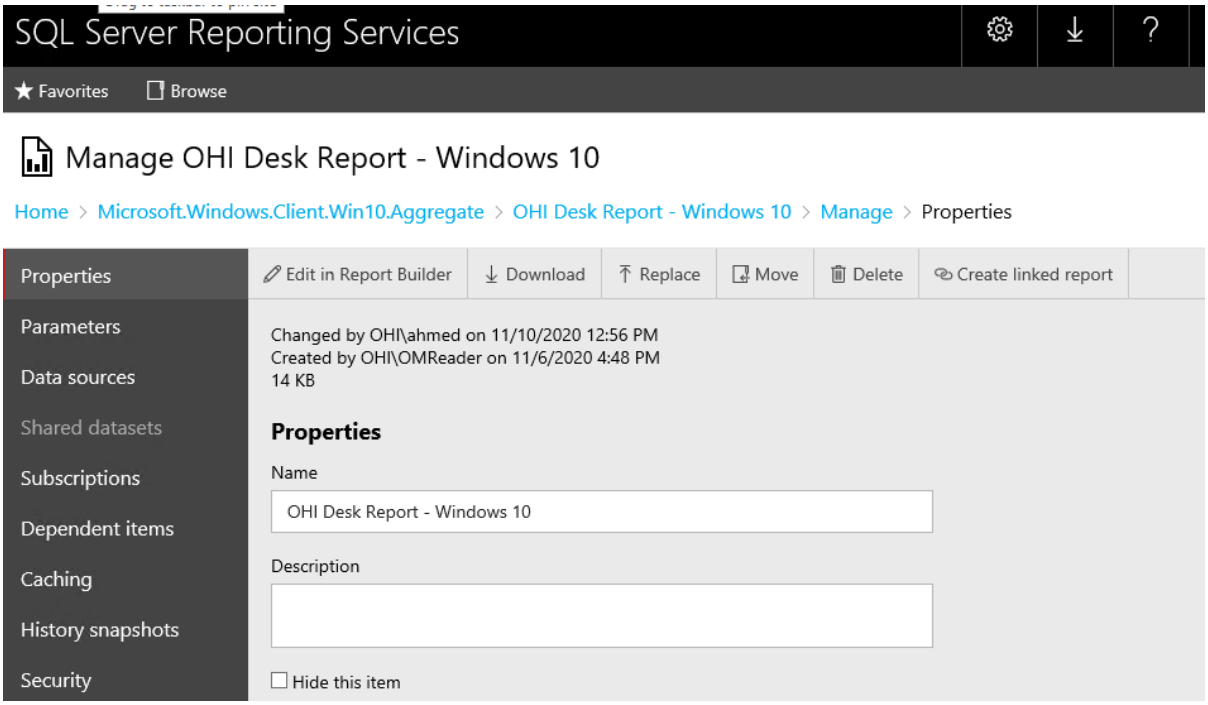
Step 3: Verify Email Delivery

- **Check Email Delivery:**
  - Ensure that the report is delivered to the specified email address at the scheduled time.
  - Verify that the email contains the report in the specified format and includes any additional details configured.

Customizing Reports

- **Step 1:** To customize reports, such as changing the logo, upload the new logo in the SQL Server Reporting Services web portal under Resources.
- **Step 2:** Manage the report properties and replace the existing logo with the newly uploaded one.





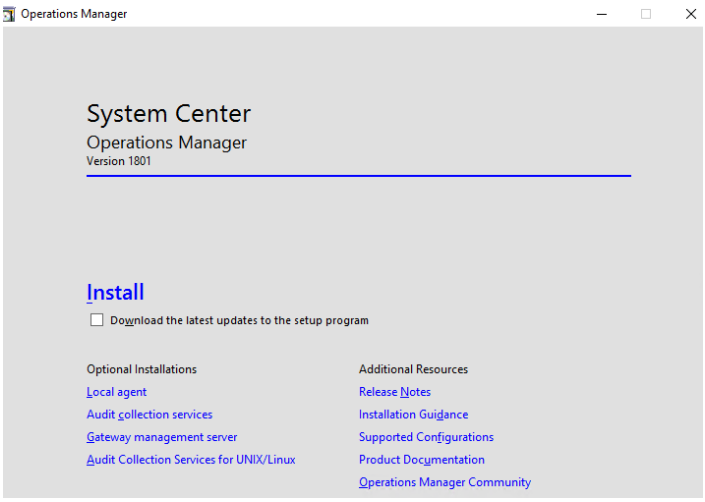
Complete Lab for Audit Collection Services (ACS)

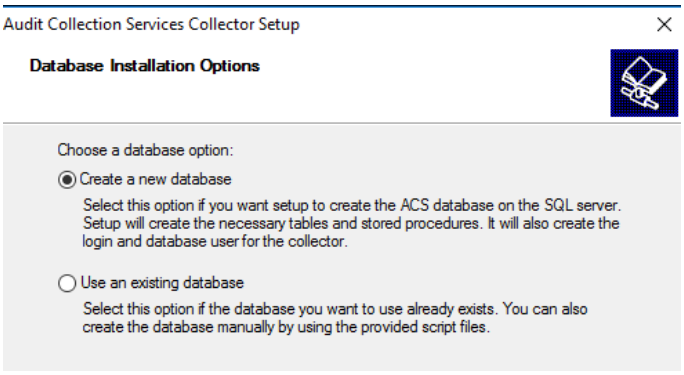
Audit Collection Services (ACS) is a feature in System Center Operations Manager (SCOM) that provides a centralized way to collect, store, and analyze security audit data from Windows servers and clients. ACS helps organizations monitor compliance with security policies, detect potential security breaches, and generate audit reports for analysis and auditing purposes.

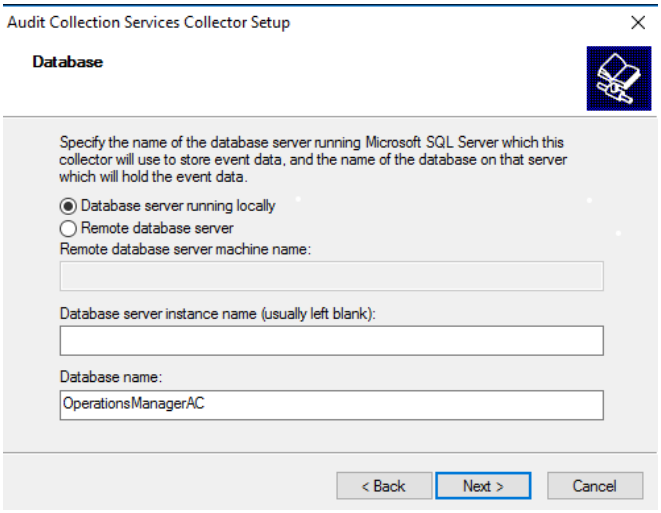
1. Install ACS Collector and Database

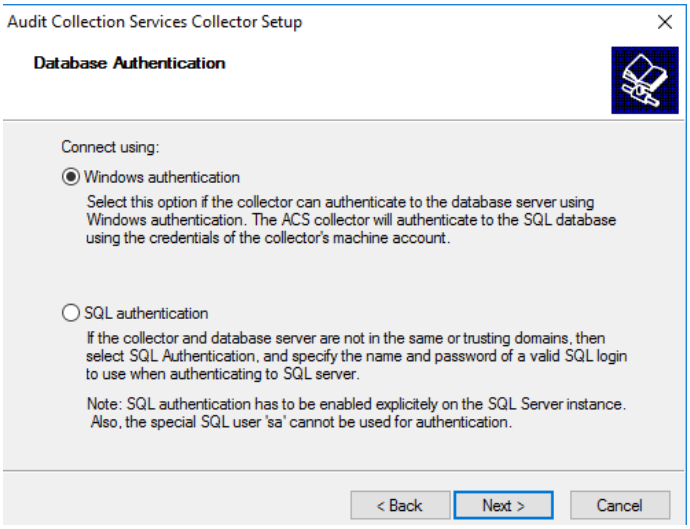
1. Database Installation Options

- Choose to create a new database or use an existing database.
- Specify the name of the database server and database instance.
- Name your database OperationsManagerAC.







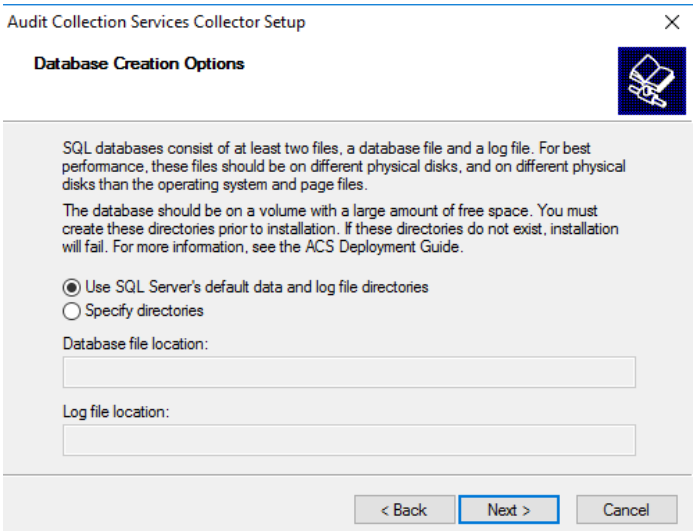


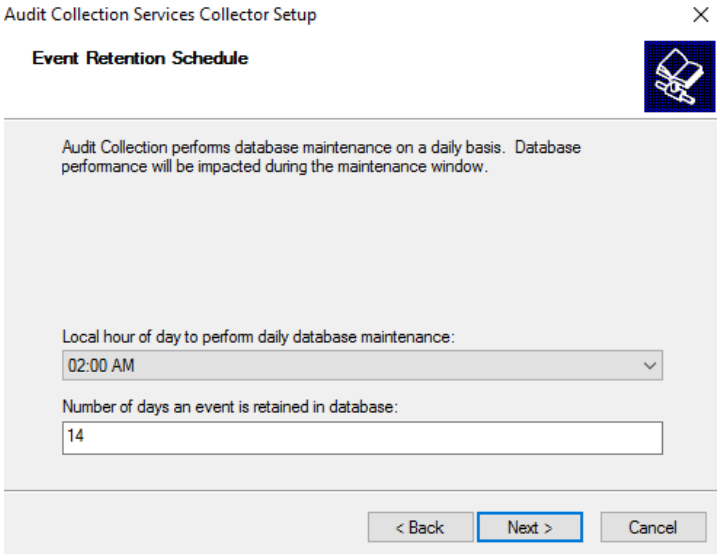
2. Database Configuration

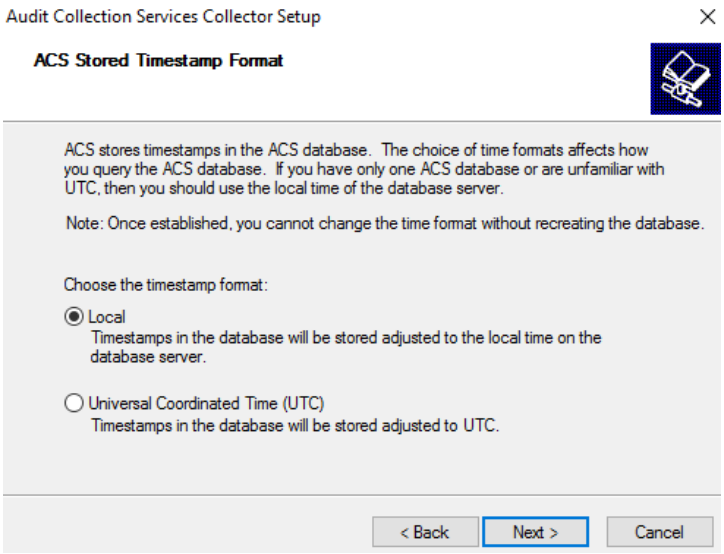
- Select timestamp format (Local or UTC).
- Set the event retention schedule (e.g., 14 days).

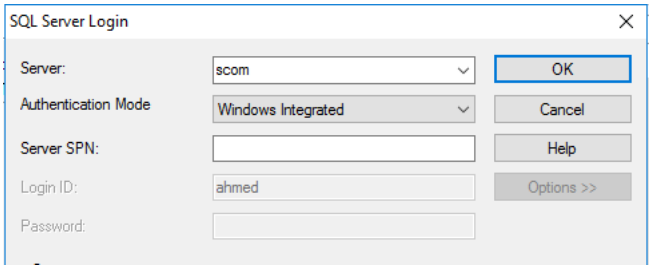
3. SQL Server Login

- Provide credentials for the SQL server.

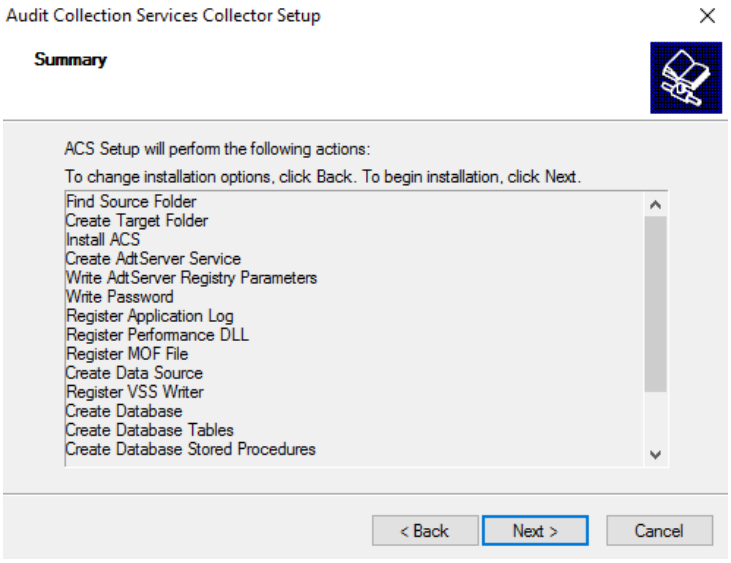


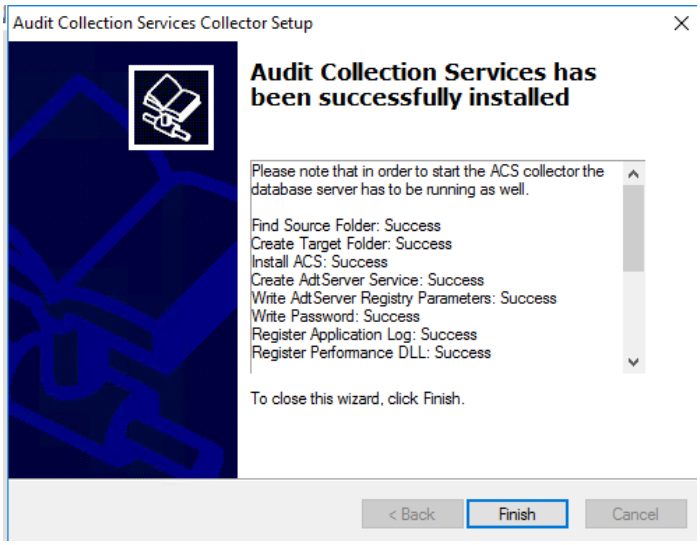

Audit Collection Services Collector Setup
Event Retention Schedule
Audit Collection performs database maintenance on a daily basis. Database performance will be impacted during the maintenance window.
Local hour of day to perform daily database maintenance:
02:00 AM
Number of days an event is retained in database:
14
< Back
Next >
Cancel


Audit Collection Services Collector Setup
ACS Stored Timestamp Format
ACS stores timestamps in the ACS database. The choice of time formats affects how you query the ACS database. If you have only one ACS database or are unfamiliar with UTC, then you should use the local time of the database server.
Note: Once established, you cannot change the time format without recreating the database.
Choose the timestamp format:
Local
Timestamps in the database will be stored adjusted to the local time on the database server.
Universal Coordinated Time (UTC)
Timestamps in the database will be stored adjusted to UTC.
< Back
Next >
Cancel


SQL Server Login
Server:
scom
Authentication Mode
Windows Integrated
Server SPN:
Login ID:
ahmed
Password:
OK
Cancel
Help
Options >>

4. **Summary and Installation**
    - Review the actions and start the installation.
5. **Installation Success**
    - Confirm that ACS has been successfully installed.

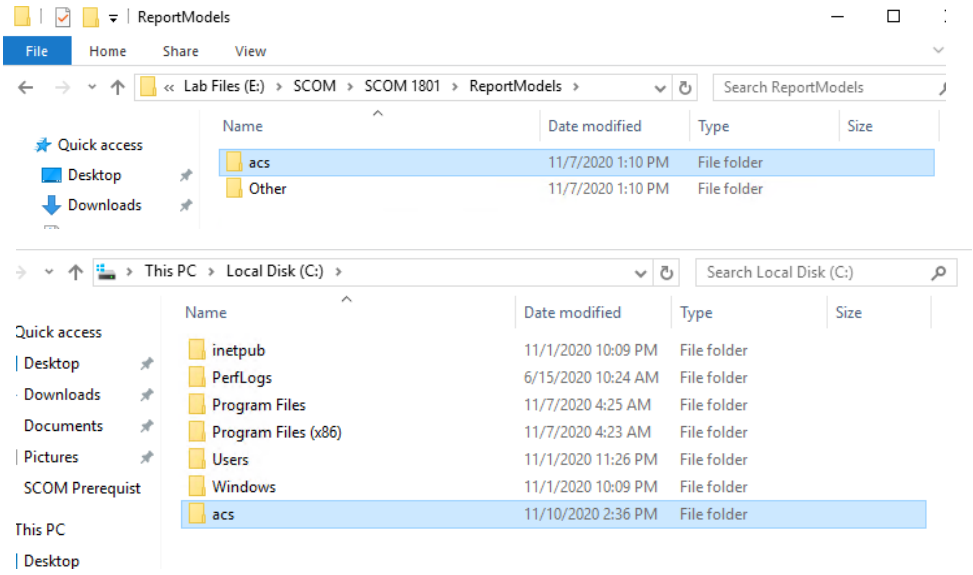




2. Deploy ACS Reporting

1. Upload ACS Reports

- Navigate to the ACS directory and upload the audit reports to the Report Server.
- Command example: .\UploadAuditReports.cmd scom http://scom/reportserver C:\acs




```
PS C:\Windows\system32> cd C:\acs\
PS C:\acs> dir

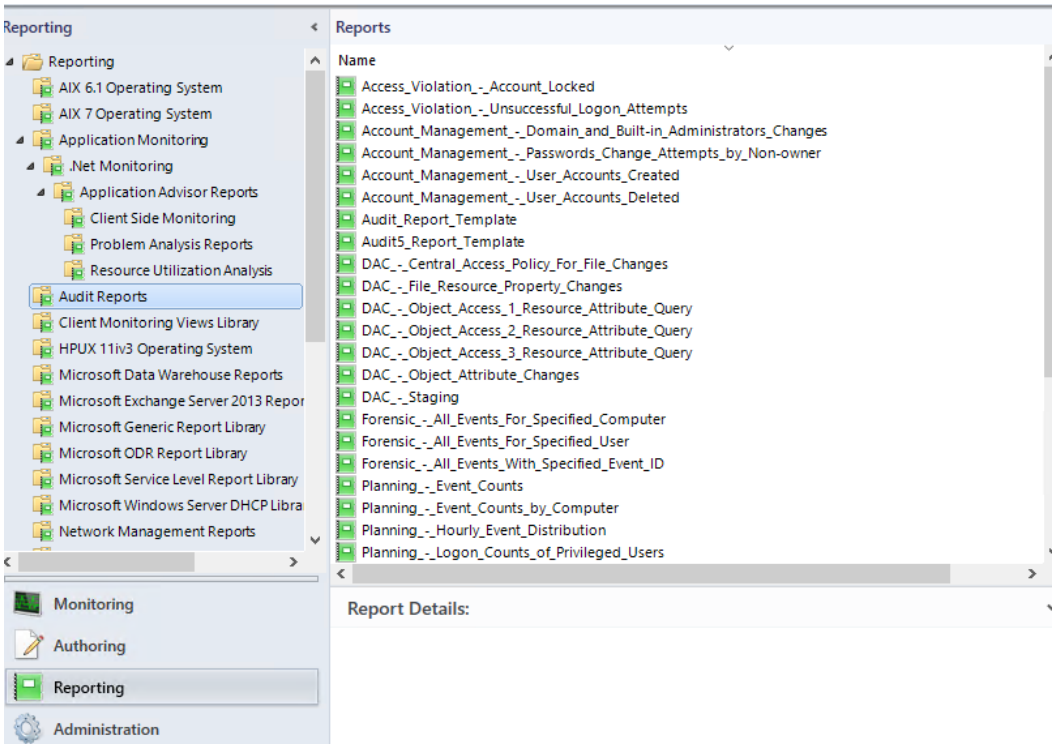

    Directory: C:\acs


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        11/7/2020   1:10 PM                en
d-----       11/10/2020   2:36 PM                Models
d-----       11/10/2020   2:36 PM                Reports
-a----        1/13/2018   7:31 AM         263920 ReportingConfig.exe
-a----       11/20/2017  11:06 AM            158 ReportingConfig.exe.config
-a----       12/19/2017  12:19 AM           1201 UploadAuditReports.cmd
```

```
PS C:\acs> .\UploadAuditReports.cmd scom http://scom/reportserver C:\acs
```

2. Verify Reports in SCOM

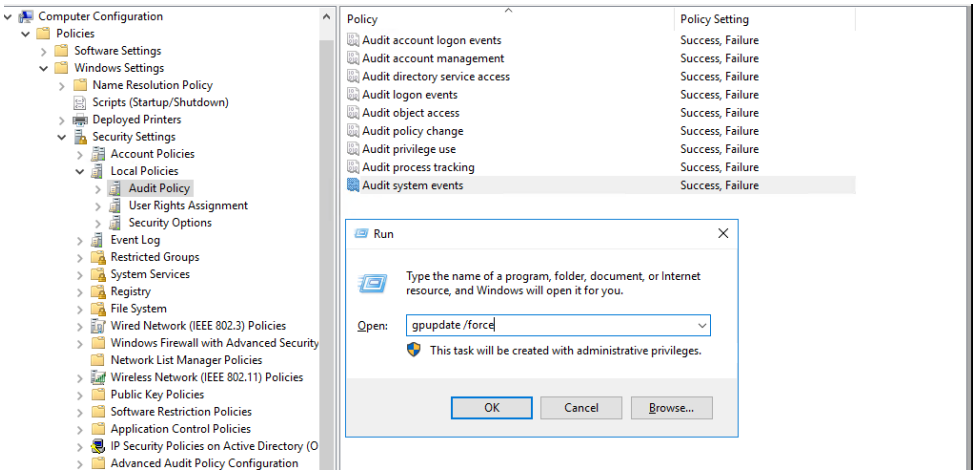
- Check that the audit reports have been successfully uploaded and are visible in the SCOM Reporting pane.



3. Enable ACS Forwarders

1. Configure Group Policy

- Apply audit policies for your domain controllers.
- Go to Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Audit Policy.
- Enable policies like Audit account logon events, Audit logon events, Audit object access, etc.



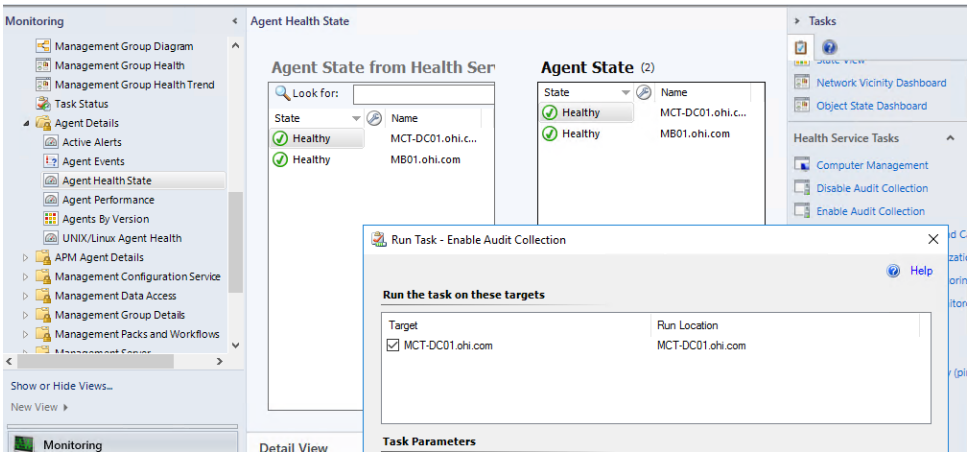
2. **Force Group Policy Update**
    - Run gpupdate /force to apply the policies immediately.

4. Create and Delete Users to Generate Audit Data

1. **Create Users**
    - Use Active Directory Users and Computers to create some test user accounts.
2. **Delete Users**
    - Delete the test user accounts to generate audit data for user deletions.

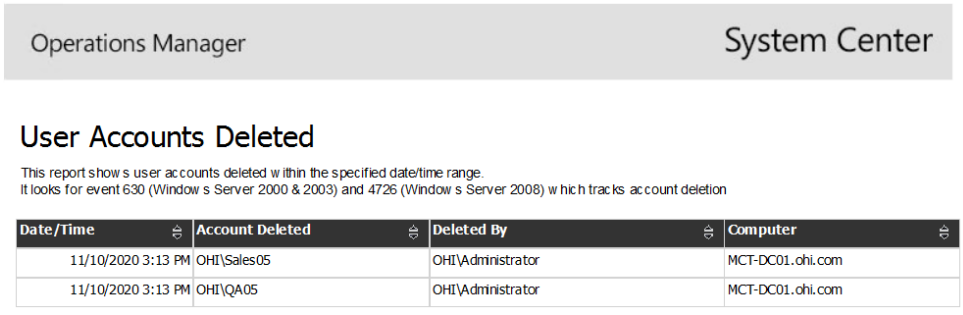
5. Enable ACS from Operations Manager

1. **Enable Audit Collection**
    - Go to Monitoring -> OperationsManager -> Agent Details -> Agent Health State.
    - Select the agent and click on "Enable Audit Collection" from the tasks pane.



6. Run the ACS Report

1. **Run the User Accounts Deleted Report**
    - Navigate to the Reports pane in Operations Manager.
    - Find and run the "User Accounts Deleted" report to view the audit data.



SCOM Maintenance Mode

Maintenance Mode in System Center Operations Manager (SCOM) is an essential feature designed to temporarily suppress monitoring, alerting, and reporting on specific managed objects within the SCOM environment. This functionality is critical during planned maintenance activities, ensuring that routine tasks such as software updates, hardware replacements, or configuration changes do not trigger false alerts and notifications, thereby reducing unnecessary noise and distractions for IT operations teams.

How Maintenance Mode Works:

- **Alert Suppression:** When an object (such as a server, application, or database) is placed into Maintenance Mode, SCOM suspends the generation of alerts, notifications, and other monitoring-related actions for that object. This prevents maintenance activities from being misinterpreted as faults or issues by SCOM.
- **Performance Data Handling:** Depending on the configuration, SCOM can either stop or continue collecting performance data during Maintenance Mode. Administrators can choose to stop performance data collection to focus resources on maintenance tasks or continue collection to analyze the impact of maintenance activities on performance metrics.
- **Health Monitoring:** The health state of the object in Maintenance Mode is not updated based on monitoring data received during this period. This means that the object's health state will remain unchanged, regardless of any issues that might be detected during maintenance.
- **Audit Logging:** SCOM logs the entry and exit of objects from Maintenance Mode, providing a clear audit trail. This logging helps administrators understand when an object was placed in and taken out of Maintenance Mode, ensuring transparency and accountability during maintenance operations.
- **Scheduling:** Maintenance Mode can be scheduled in advance or activated immediately. Scheduled Maintenance Mode allows administrators to plan maintenance activities ahead of time, ensuring that objects enter Maintenance Mode automatically at the designated time without requiring manual intervention.
- **Scope of Maintenance Mode:** Maintenance Mode can be applied at different levels within SCOM:
  - **Individual Objects:** Specific servers, applications, or components can be placed in Maintenance Mode, allowing targeted maintenance without affecting other parts of the infrastructure.
  - **Groups of Objects:** Maintenance Mode can be applied to groups of objects, such as all servers in a specific datacenter or all instances of a particular application, simplifying large-scale maintenance operations.
  - **Dependency Management:** SCOM can be configured to place dependent objects into Maintenance Mode automatically when their parent object enters Maintenance Mode. For example, placing a database in Maintenance Mode can automatically include the applications that depend on it.
- **User Roles and Permissions:** Maintenance Mode can be managed through SCOM's role-based access control. Only users with the appropriate permissions can place objects into or take them out of Maintenance Mode, ensuring that only authorized personnel can control this feature.

Common Use Cases for Maintenance Mode:

- **Software Updates:** During operating system updates, application patches, or antivirus scans, Maintenance Mode prevents these activities from being misinterpreted as faults or issues.
- **Hardware Maintenance:** When performing hardware upgrades, such as adding more memory, replacing a hard drive, or changing network interfaces, Maintenance Mode ensures that these actions do not trigger unnecessary alerts.

- **Configuration Changes:** Firewall rule updates, network reconfigurations, or load balancing adjustments can be performed without generating false alarms by using Maintenance Mode.
- **Routine Checks and Tests:** IT teams can perform regular health checks, diagnostic tests, or other routine maintenance tasks without triggering alerts by temporarily placing the affected objects into Maintenance Mode.

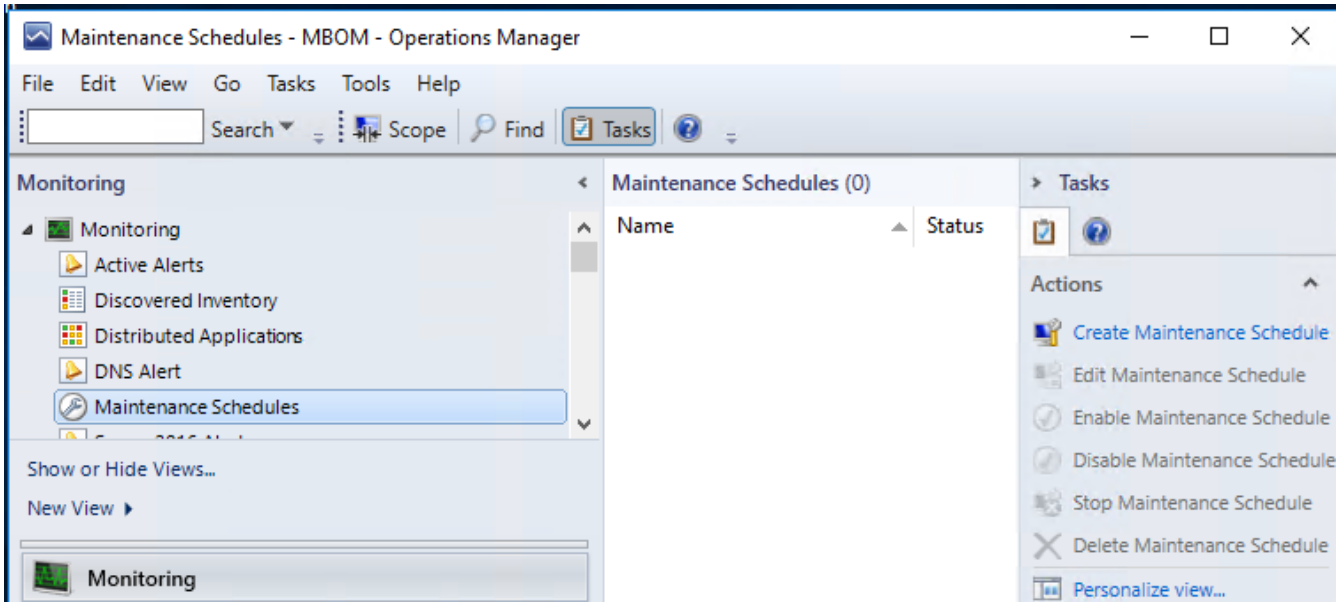
Managing Maintenance Mode:

1. **Manually Starting Maintenance Mode:** Administrators can manually place objects into Maintenance Mode through the SCOM console. This is typically done for ad-hoc maintenance tasks that were not planned in advance.
2. **Scheduling Maintenance Mode:** For planned maintenance, administrators can schedule Maintenance Mode to start and stop at predefined times. This ensures that Maintenance Mode is active during the maintenance window without requiring manual intervention.
3. **Stopping Maintenance Mode:** Once maintenance is completed, objects can be manually or automatically taken out of Maintenance Mode. This resumes normal monitoring and alerting activities.
4. **Automation:** Maintenance Mode can be automated using SCOM PowerShell cmdlets or integrated with other automation tools and processes, allowing for seamless management as part of larger IT workflows.

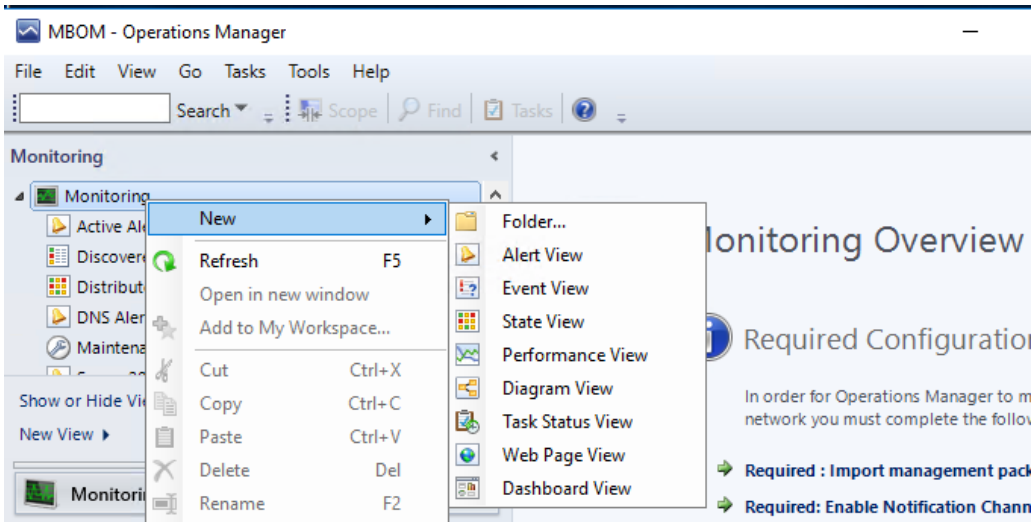
Best Practices:

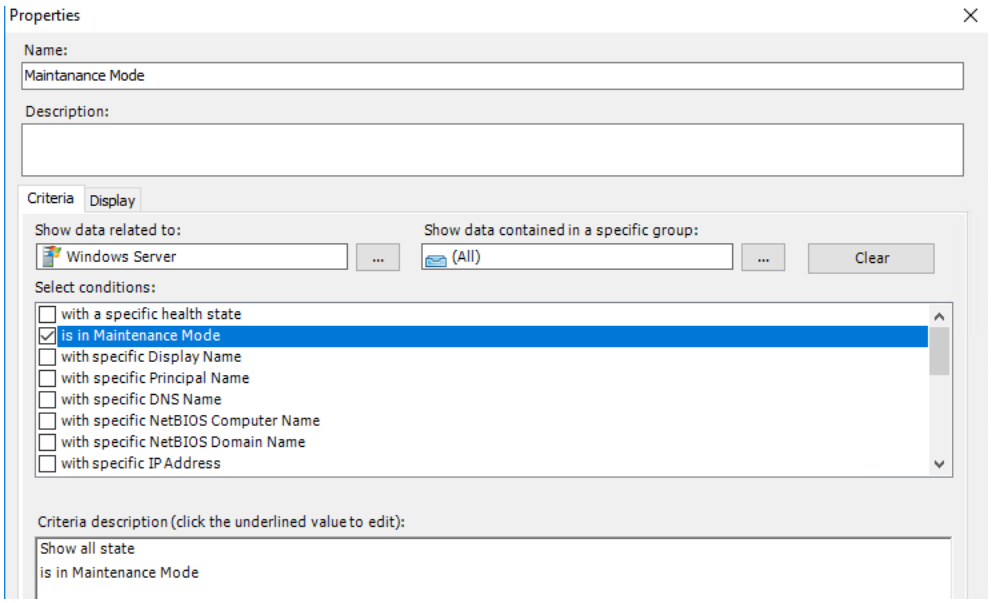
- **Predefine Maintenance Windows:** Set up and regularly update predefined maintenance windows in SCOM for commonly maintained objects to streamline the process.
- **Use Groups for Large-Scale Maintenance:** For large-scale maintenance, place entire groups of objects into Maintenance Mode rather than managing them individually.
- **Automate with Scripts:** Use PowerShell scripts to automate the process of placing objects into and out of Maintenance Mode, reducing the risk of human error and improving efficiency.
- **Monitor and Review:** Regularly review audit logs for Maintenance Mode to ensure that it was applied correctly and that no critical monitoring was missed during the maintenance period.

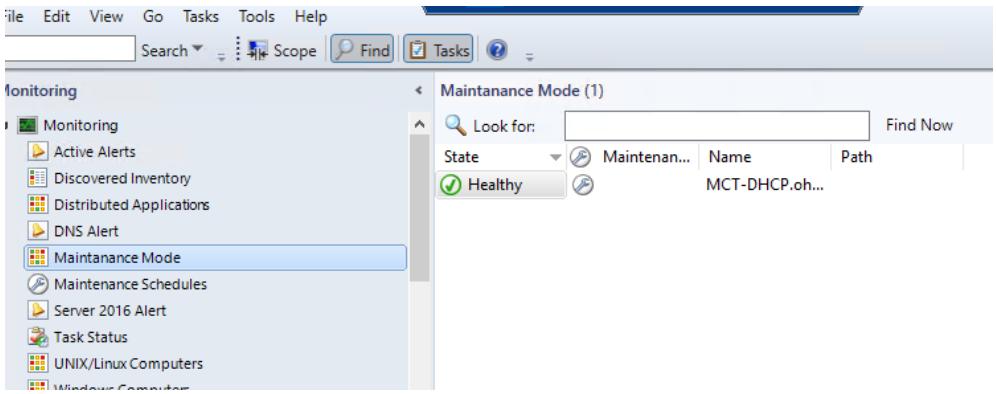
schedule maintenance mode



How to view the objects that are in maintenance mode







SCOM Updates

System Center Operations Manager (SCOM) is a monitoring tool from Microsoft that helps manage and monitor the infrastructure, applications, and services across various environments, including on-premises and cloud. SCOM receives regular updates that bring enhancements, new features, bug fixes, and support for newer technologies. Below is an in-depth look at recent updates and features in SCOM:

1. Latest Features and Improvements

- **Management Pack Updates**: SCOM frequently updates its management packs to provide support for the latest versions of Microsoft products like SQL Server, Exchange, SharePoint, and others. These management packs include monitoring templates, rules, and dashboards tailored to each product.
- **Azure Monitoring Integration**: With the rise of hybrid environments, SCOM updates have enhanced integration with Azure Monitor. This allows organizations to extend their on-premises monitoring to Azure resources, providing a unified monitoring experience.
- **Improved Dashboards**: New updates often include enhancements to SCOM dashboards, making them more user-friendly with improved visualizations and better integration with other Microsoft tools like Power BI.
- **Enhanced Performance and Scalability**: Recent updates have focused on improving SCOM's performance, especially in large environments. Enhancements in the data warehouse, grooming processes, and overall scalability have been significant.
- **Linux/UNIX Monitoring**: SCOM continues to expand its capabilities in monitoring non-Windows environments. Updates include support for more Linux/UNIX distributions and improved monitoring capabilities.

2. Bug Fixes and Stability Improvements

- **Agent and Management Server Stability**: SCOM updates often address issues related to the stability of the SCOM agents and management servers. This includes fixing memory leaks, crashes, and improving the overall reliability of the monitoring services.
- **Alerting and Notification Improvements**: Updates often refine how alerts are generated and handled within SCOM. This includes fixing issues with alerting rules, thresholds, and the delivery of notifications via email or other channels.
- **Database Maintenance**: Regular updates include fixes and optimizations for the SCOM databases (OperationsManager, Data Warehouse). These optimizations help in improving query performance, reducing the size of the databases, and ensuring smooth database maintenance operations.

3. Security Enhancements

- **TLS/SSL Support**: SCOM has enhanced its support for modern TLS/SSL protocols to ensure secure communication between SCOM components, including agents, management servers, and consoles.
- **Role-Based Access Control (RBAC)**: Updates have refined RBAC features, allowing more granular control over who can access and modify various parts of the SCOM environment.

4. Support for New Platforms and Technologies

- **Windows Server and SQL Server**: SCOM updates regularly include support for the latest versions of Windows Server and SQL Server, ensuring that organizations can monitor these environments as soon as they are deployed.
- **Azure Stack Monitoring**: Updates have enhanced the ability to monitor Azure Stack environments, allowing organizations to monitor their hybrid cloud deployments more effectively.

5. SCOM as a Service (SCOMaaS)

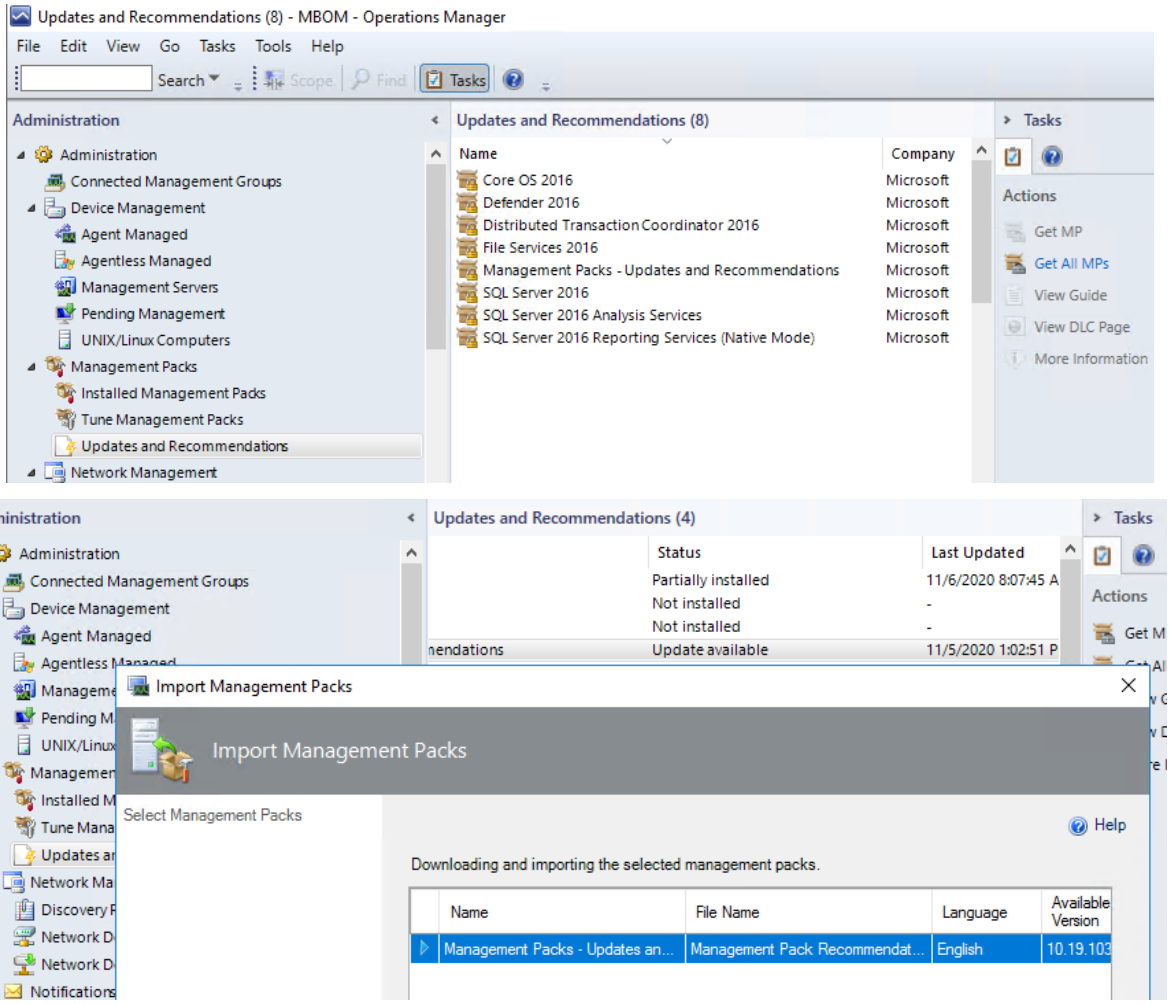
- **Managed Service Providers (MSPs)**: Some updates have focused on improving the capabilities of SCOM for MSPs, making it easier to offer SCOM as a service. This includes multi-tenant capabilities and easier onboarding of new clients.

6. User Experience Enhancements

- **SCOM Web Console**: The web console has seen significant improvements in recent updates, with a more modern UI, faster performance, and better support for different browsers.
- **Native PowerShell Integration**: Updates have expanded the PowerShell cmdlets available for SCOM, allowing for more automation and scripting possibilities.

7. SCOM Roadmap

- **Future Updates**: Microsoft's roadmap for SCOM includes further integration with Azure Monitor, more advanced AI-driven insights, and continued improvements in ease of use, particularly around the deployment and configuration of SCOM in hybrid environments.

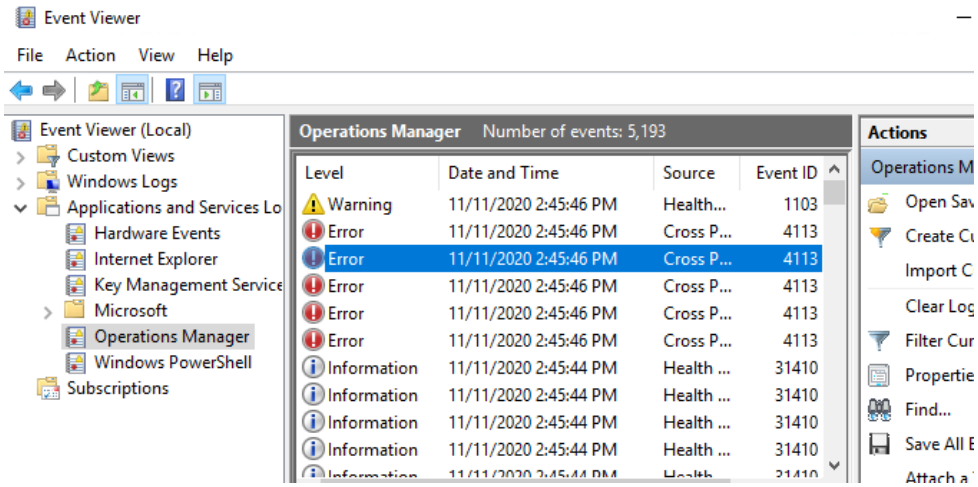


SCOM Upgrade

Pre-Upgrade Tasks

1. Review the Operations Manager Event Logs

- **Purpose**: Check for any existing issues or errors that might affect the upgrade process.
- **Steps**:
    1. Open Event Viewer on the Operations Manager server.
    2. Navigate to **Applications and Services Logs** > **Operations Manager**.
    3. Review any warnings, errors, or critical events, especially related to the HealthService or Data Access services.
    4. Resolve any identified issues before proceeding with the upgrade.



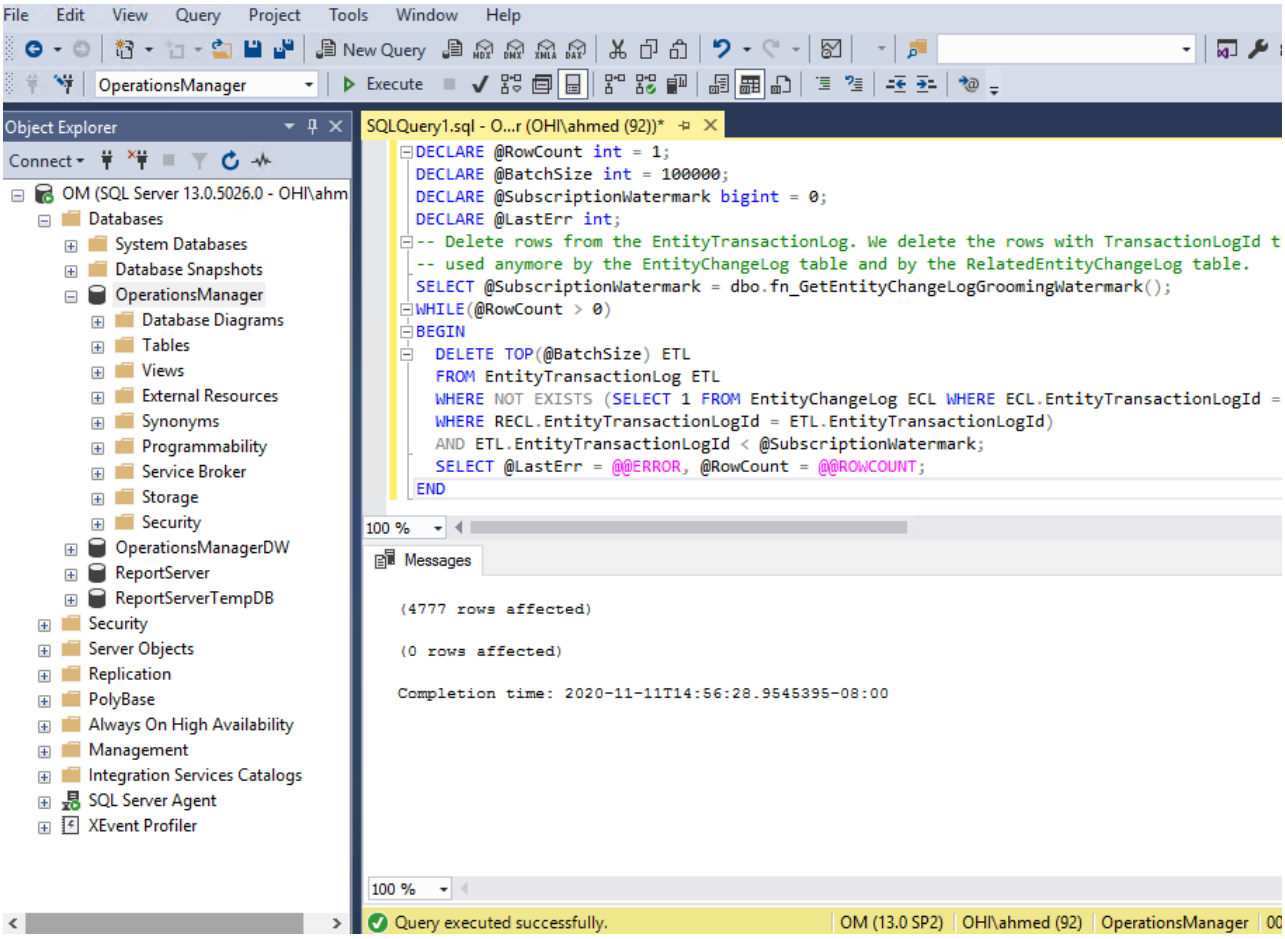
2. Clean up the Database (ETL Table)

- **Purpose**: Cleaning up old rows in the OpsMgr database helps speed up the update process by reducing the size of the database.
- **SQL Script**:

```
DECLARE @RowCount int = 1;
DECLARE @BatchSize int = 100000;
DECLARE @SubscriptionWatermark bigint = 0;
DECLARE @LastErr int;
-- Delete rows from the EntityTransactionLog. We delete the rows with
TransactionLogId that aren't being
-- used anymore by the EntityChangeLog table and by the RelatedEntityChangeLog
table.
SELECT @SubscriptionWatermark = dbo.fn_GetEntityChangeLogGroomingWatermark();
WHILE(@RowCount > 0)
BEGIN
  DELETE TOP(@BatchSize) ETL
  FROM EntityTransactionLog ETL
  WHERE NOT EXISTS (SELECT 1 FROM EntityChangeLog ECL WHERE
ECL.EntityTransactionLogId = ETL.EntityTransactionLogId)
```

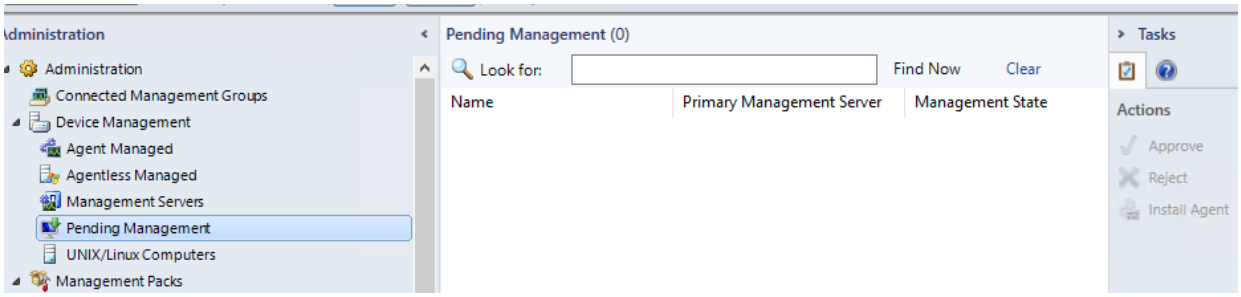
```
    AND NOT EXISTS (SELECT 1 FROM RelatedEntityChangeLog RECL WHERE
RECL.EntityTransactionLogId = ETL.EntityTransactionLogId)
    AND ETL.EntityTransactionLogId < @SubscriptionWatermark;
  SELECT @LastErr = @@ERROR, @RowCount = @@ROWCOUNT;
END
```

- **Steps**:
    1. Launch SQL Server Management Studio.
    2. Connect to the database engine.
    3. Expand **Databases** and select the **OperationsManager** database.
    4. Right-click and choose **New Query**.
    5. Paste the SQL script above into the query window.
    6. Click **Execute** to run the script.



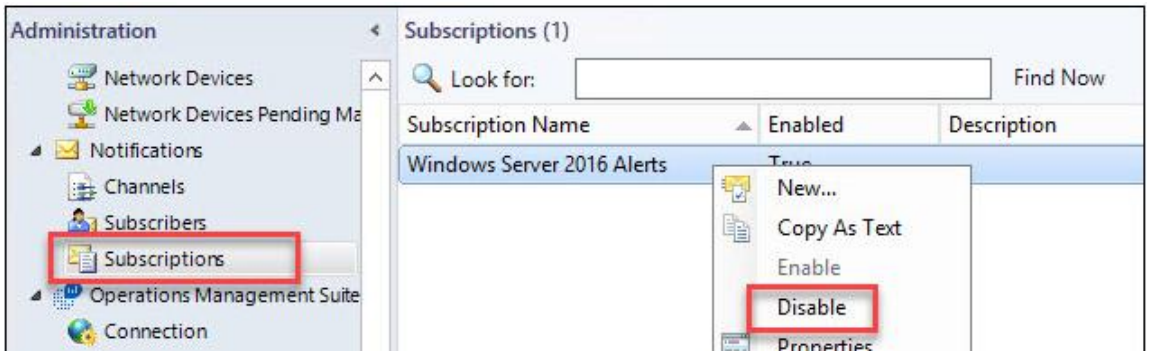
3. Remove Agents from Pending Management

- **Purpose**: Ensure that no agents are in a pending state, which could cause issues during the upgrade.
- **Steps**:
    1. Open the SCOM console.
    2. Navigate to **Administration** > **Pending Management**.
    3. If any agents are listed, either approve or remove them.



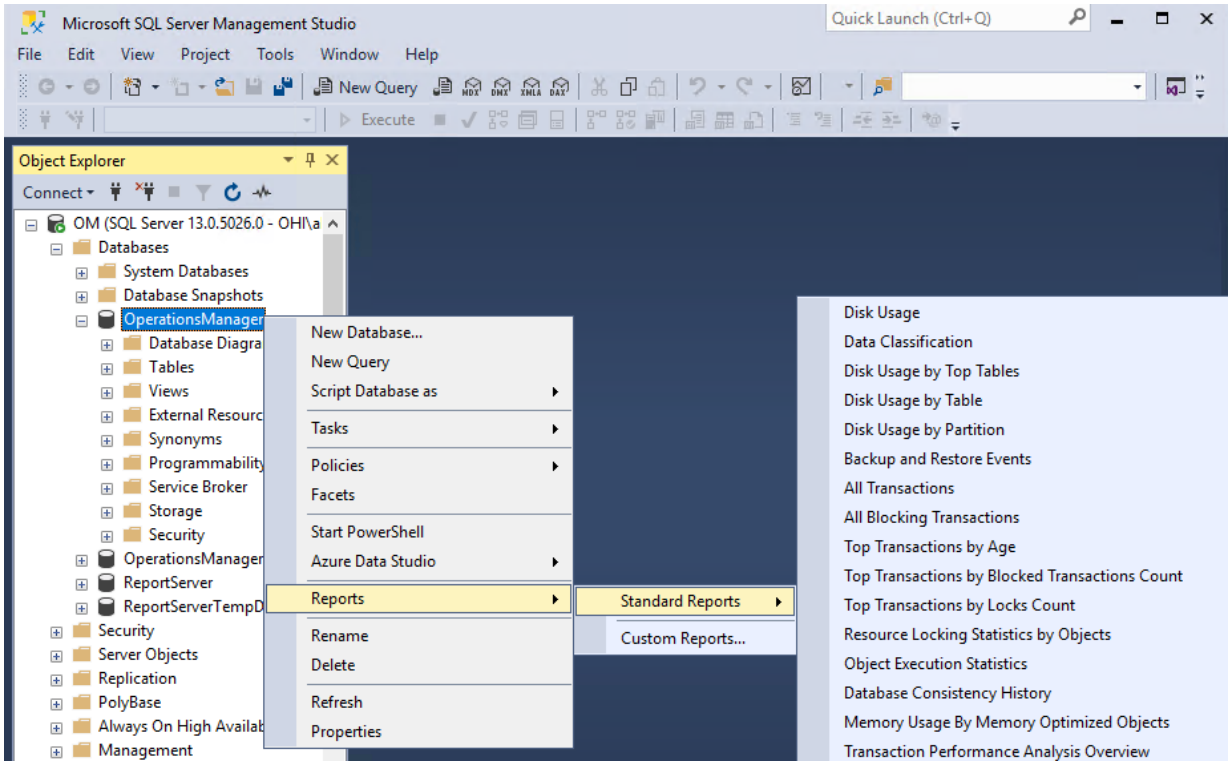
4. Disable SCOM Notification Subscriptions

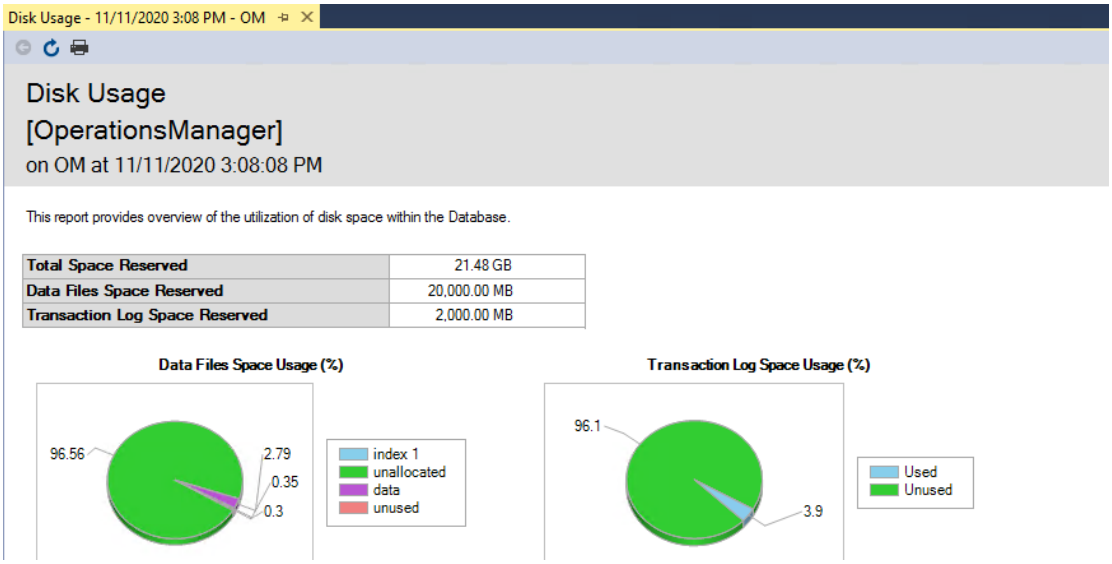
- **Purpose**: Prevent any unnecessary alerts from being sent during the upgrade process.
- **Steps**:
    1. Open the SCOM console.
    2. Navigate to **Administration** > **Notifications** > **Subscriptions**.
    3. Right-click on each subscription and choose **Disable**.



5. Ensure Database Has More Than 50% Free Space

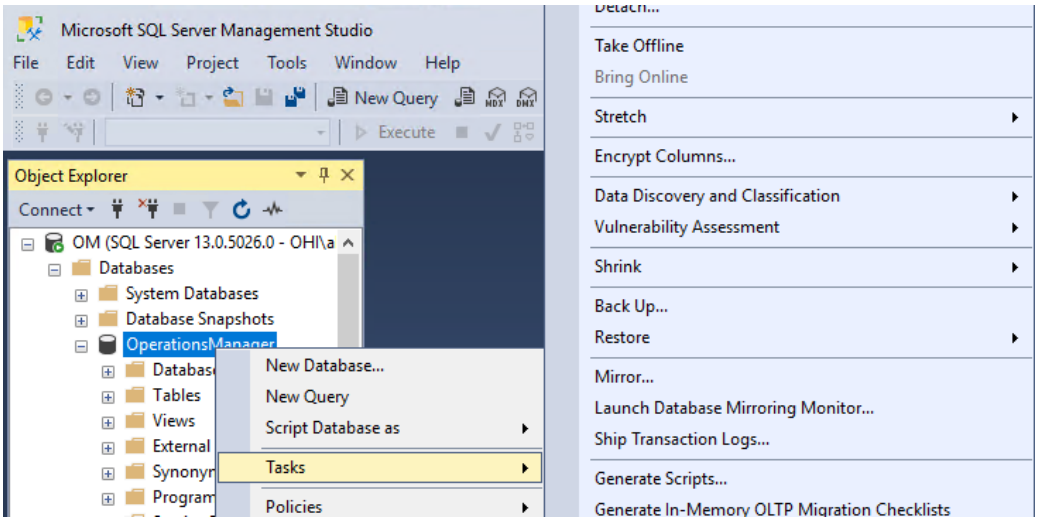
- **Purpose**: Verify that the Operations Manager database has enough free space to handle the upgrade.
- **Steps**:
    1. On the SQL Server hosting the Operations Manager database, open SQL Server Management Studio.
    2. Expand **Databases**, right-click on the **OperationsManager** database, and choose **Reports** > **Standard Reports** > **Disk Usage**.
    3. Review the report to ensure more than 50% of free space is available.

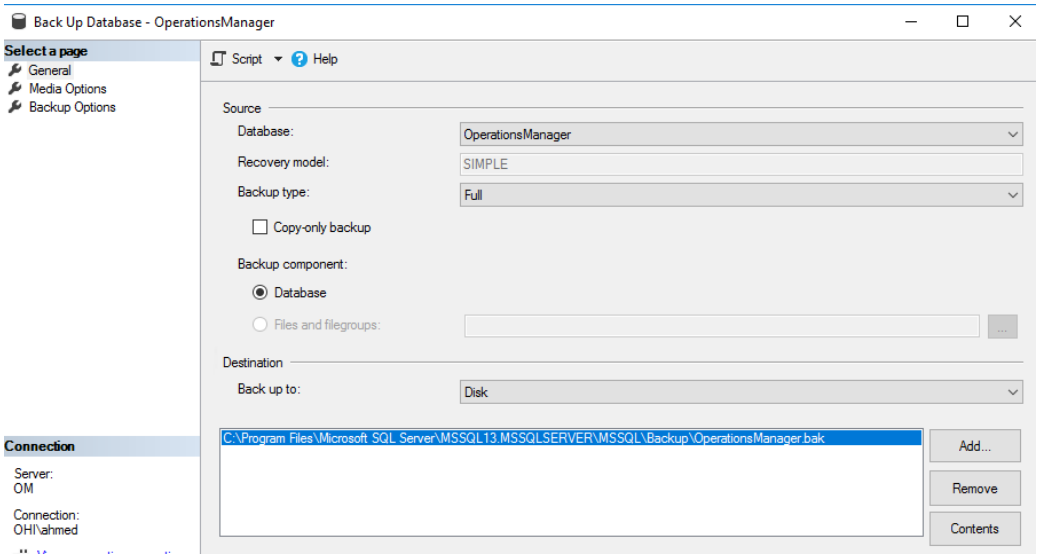

Microsoft SQL Server Management Studio
Quick Launch (Ctrl+Q)
File Edit View Project Tools Window Help
New Query
Execute
Object Explorer
Connect
OM (SQL Server 13.0.5026.0 - OHI\a
Databases
System Databases
Database Snapshots
OperationsManager
Database Diagra
Tables
Views
External Resourc
Synonyms
Programmability
Service Broker
Storage
Security
OperationsManager
ReportServer
ReportServerTempD
Security
Server Objects
Replication
PolyBase
Always On High Availab
Management
New Database...
New Query
Script Database as
Tasks
Policies
Facets
Start PowerShell
Azure Data Studio
Reports
Rename
Delete
Refresh
Properties
Standard Reports
Custom Reports...
Disk Usage
Data Classification
Disk Usage by Top Tables
Disk Usage by Table
Disk Usage by Partition
Backup and Restore Events
All Transactions
All Blocking Transactions
Top Transactions by Age
Top Transactions by Blocked Transactions Count
Top Transactions by Locks Count
Resource Locking Statistics by Objects
Object Execution Statistics
Database Consistency History
Memory Usage By Memory Optimized Objects
Transaction Performance Analysis Overview


Disk Usage - 11/11/2020 3:08 PM - OM
Disk Usage
[OperationsManager]
on OM at 11/11/2020 3:08:08 PM
This report provides overview of the utilization of disk space within the Database.
Total Space Reserved 21.48 GB
Data Files Space Reserved 20,000.00 MB
Transaction Log Space Reserved 2,000.00 MB
Data Files Space Usage (%)
96.56
2.79
0.35
0.3
index 1
unallocated
data
unused
Transaction Log Space Usage (%)
96.1
3.9
Used
Unused

6. Back Up the Operations Manager Databases

- **Purpose**: Ensure a backup is available in case the upgrade fails and a rollback is necessary.
- **Steps**:
    1. In SQL Server Management Studio, expand **Databases**.
    2. Right-click on the **OperationsManager** database and select **Tasks** > **Back Up**.
    3. Choose the destination and backup type (Full), and start the backup process.
    4. Repeat the process for the **OperationsManagerDW** database.





7. Increase Agent HealthService Cache Size

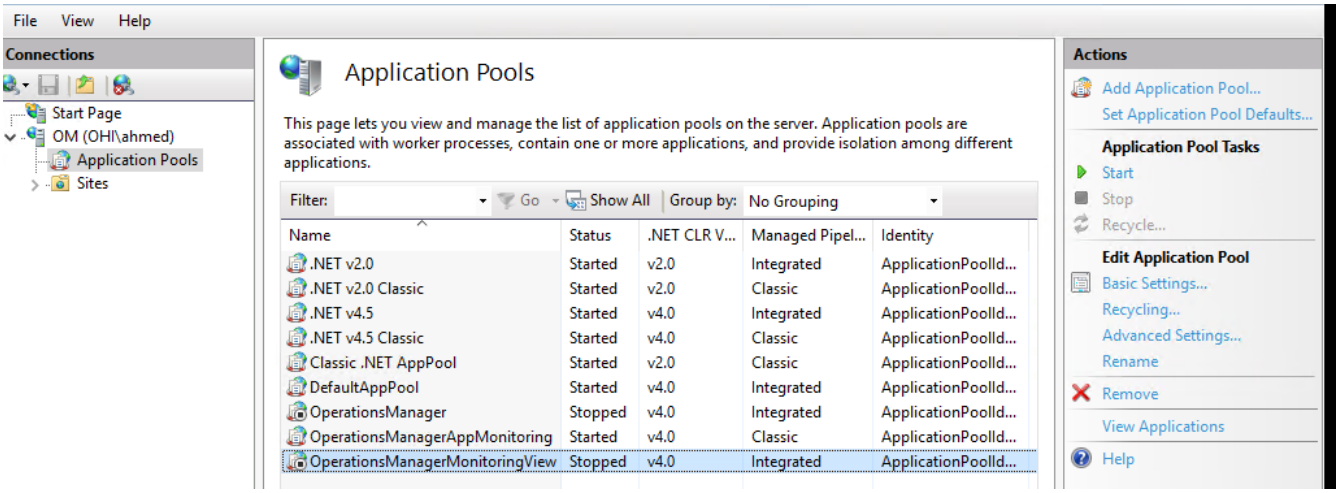
- **Purpose**: Increase the cache size to ensure agents can queue data during the upgrade.
- **Steps**:
    1. Open **Registry Editor** on the SCOM server.
    2. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HealthService\Parameters\Management Groups\<ManagementGroupName>.
    3. Find or create the **maximumQueueSizeKb** DWORD value.
    4. Set its value to **76800** (75 MB) or higher.

8. Stop Operations Manager Services on Management Servers

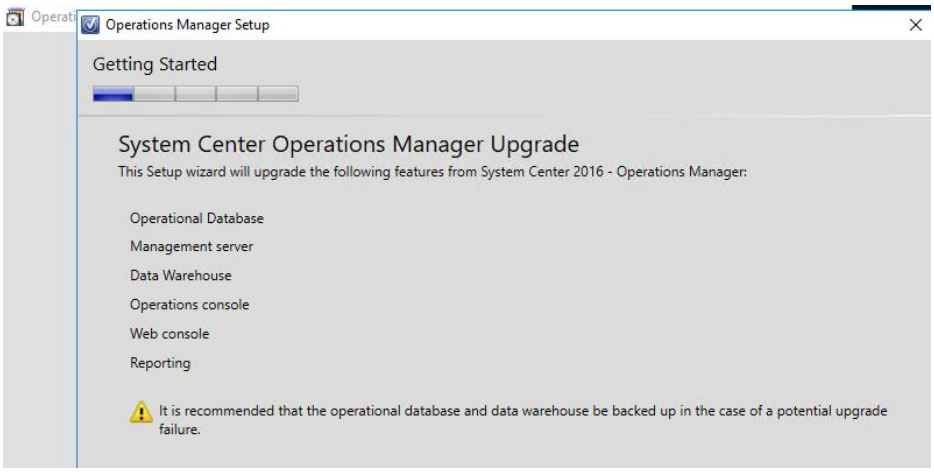
- **Purpose**: Prevent changes or data collection during the upgrade process.
- **Steps**:
    1. On each management server, stop the following services:
        - **System Center Data Access**
        - **System Center Configuration**
        - **Microsoft Monitoring Agent**
    2. Do not stop SQL services on the SQL server hosting the SCOM databases.

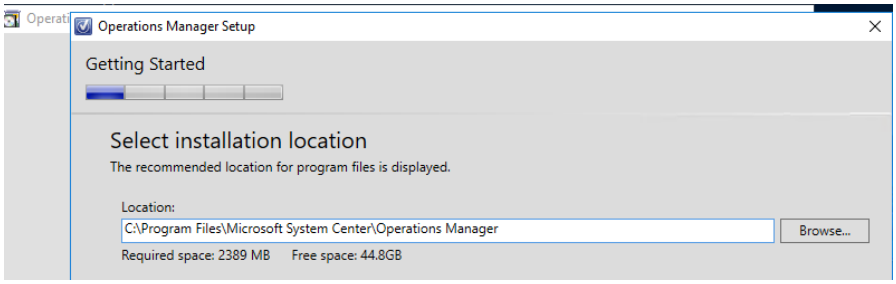
9. Stop the Application Pool of Operations Manager and MonitoringViews in IIS

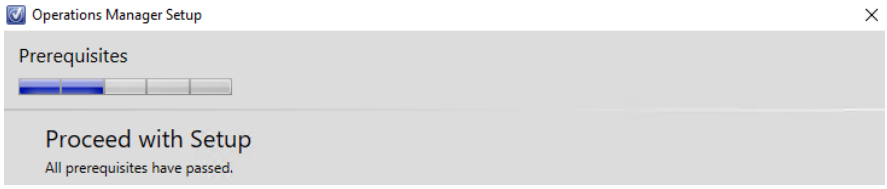
- **Purpose**: Ensure that web components are not running during the upgrade.
- **Steps**:
    1. Open **IIS Manager** on the server hosting the SCOM web console.
    2. Navigate to **Application Pools**.
    3. Right-click on **OperationsManagerMonitoringView** and **OperationsManager** application pools, and select **Stop**.

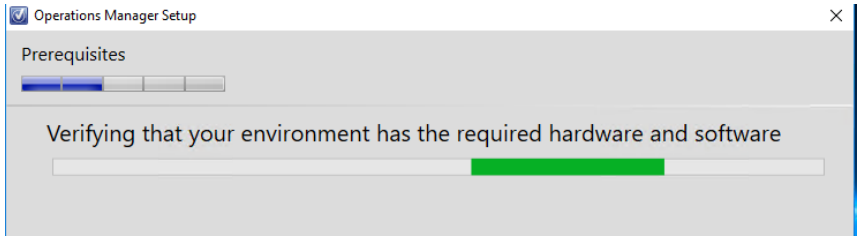


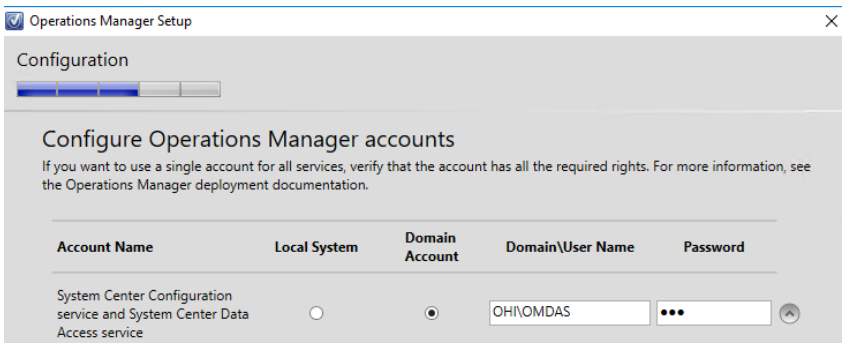
Start Migration

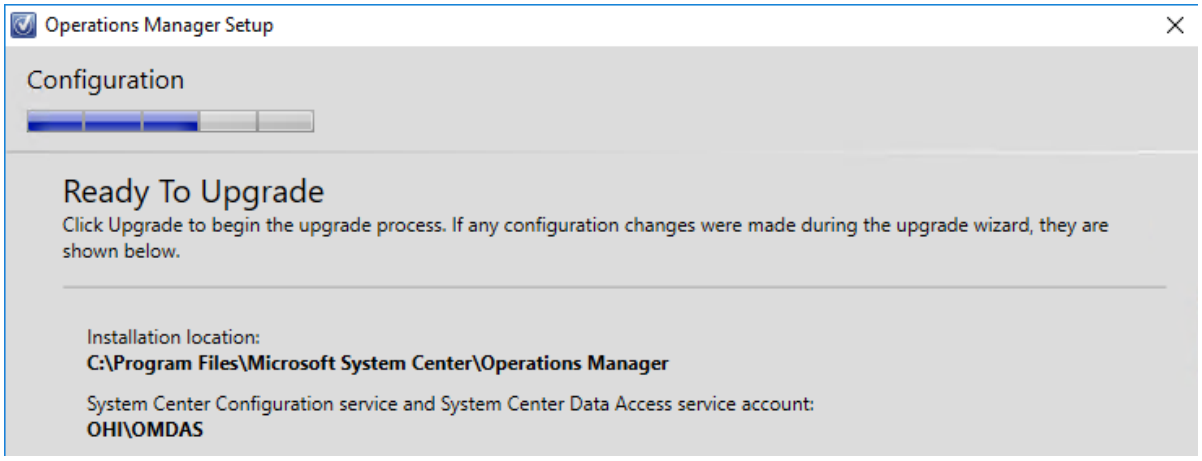


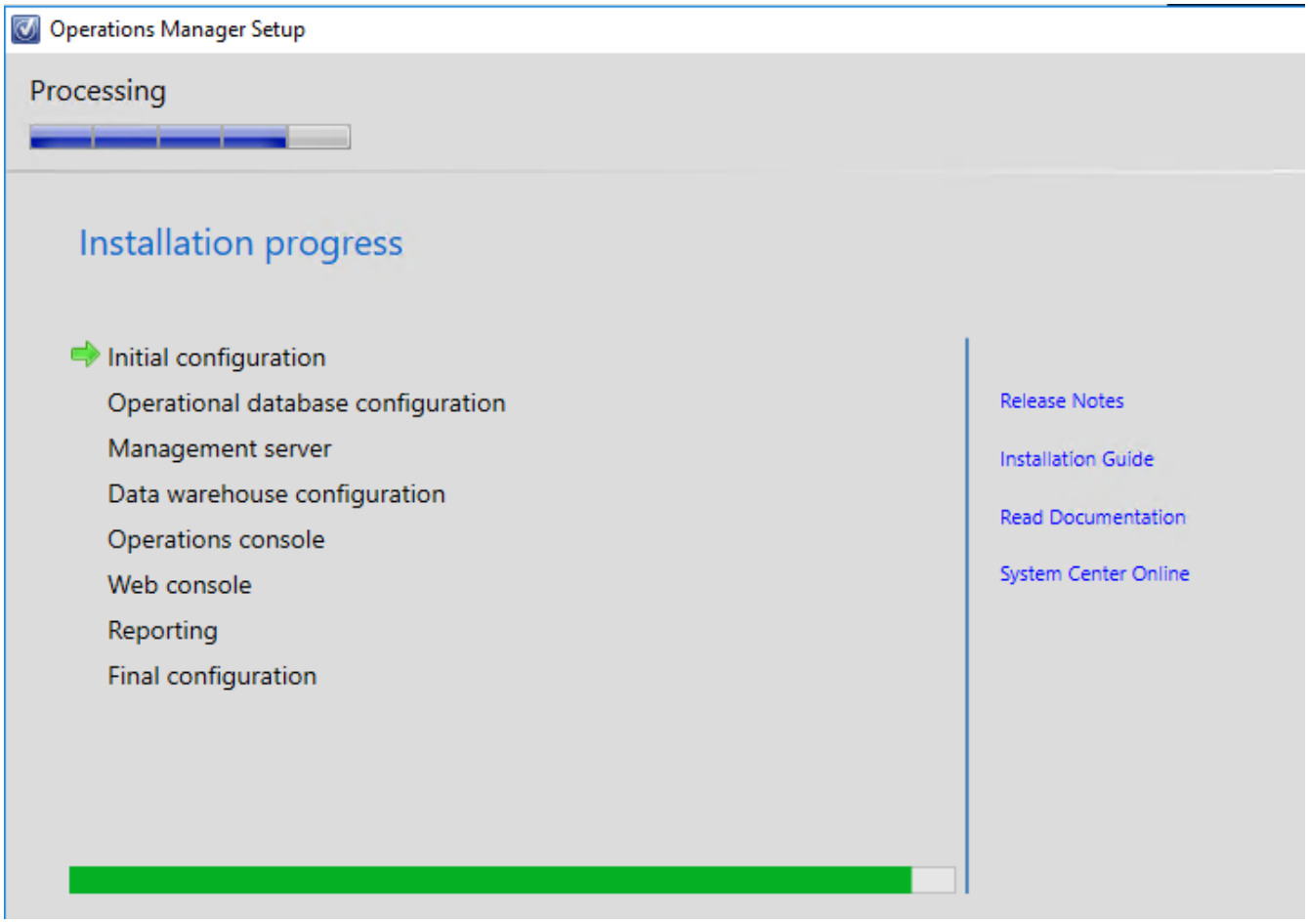


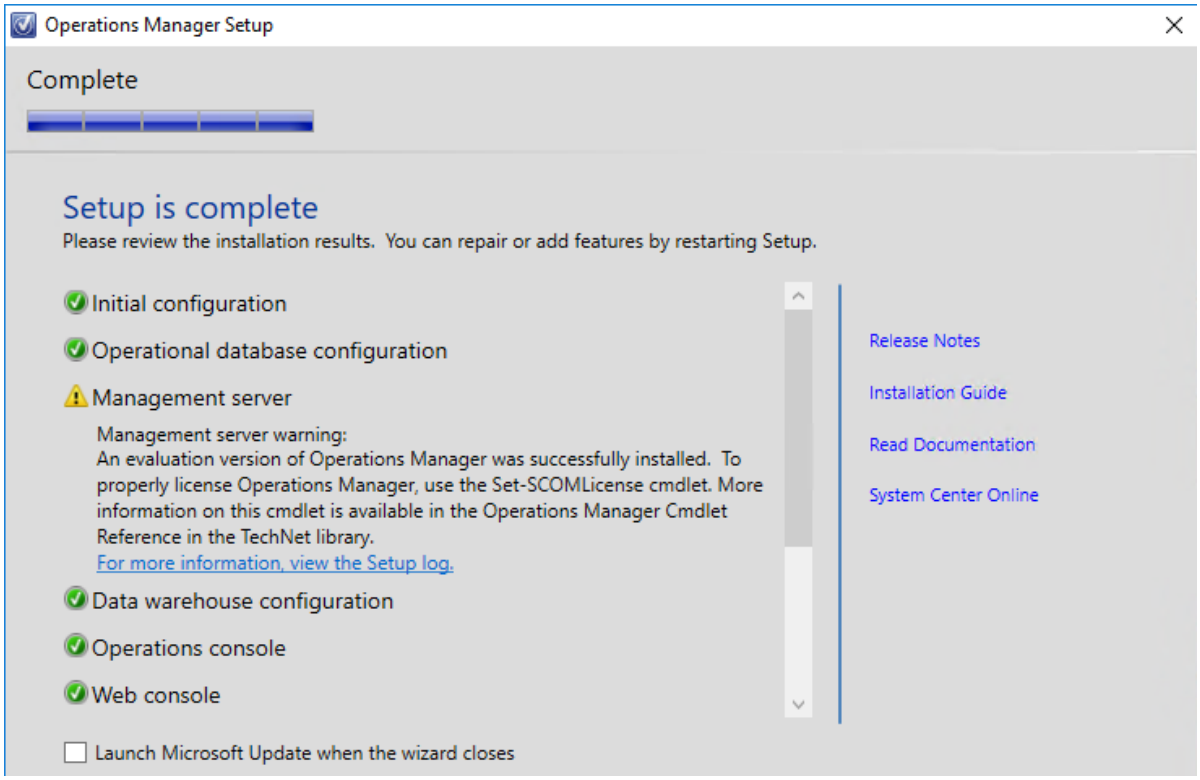







Operations Manager Setup
Configuration
Ready To Upgrade
Click Upgrade to begin the upgrade process. If any configuration changes were made during the upgrade wizard, they are shown below.
Installation location:
C:\Program Files\Microsoft System Center\Operations Manager
System Center Configuration service and System Center Data Access service account:
OHI\OMDAS

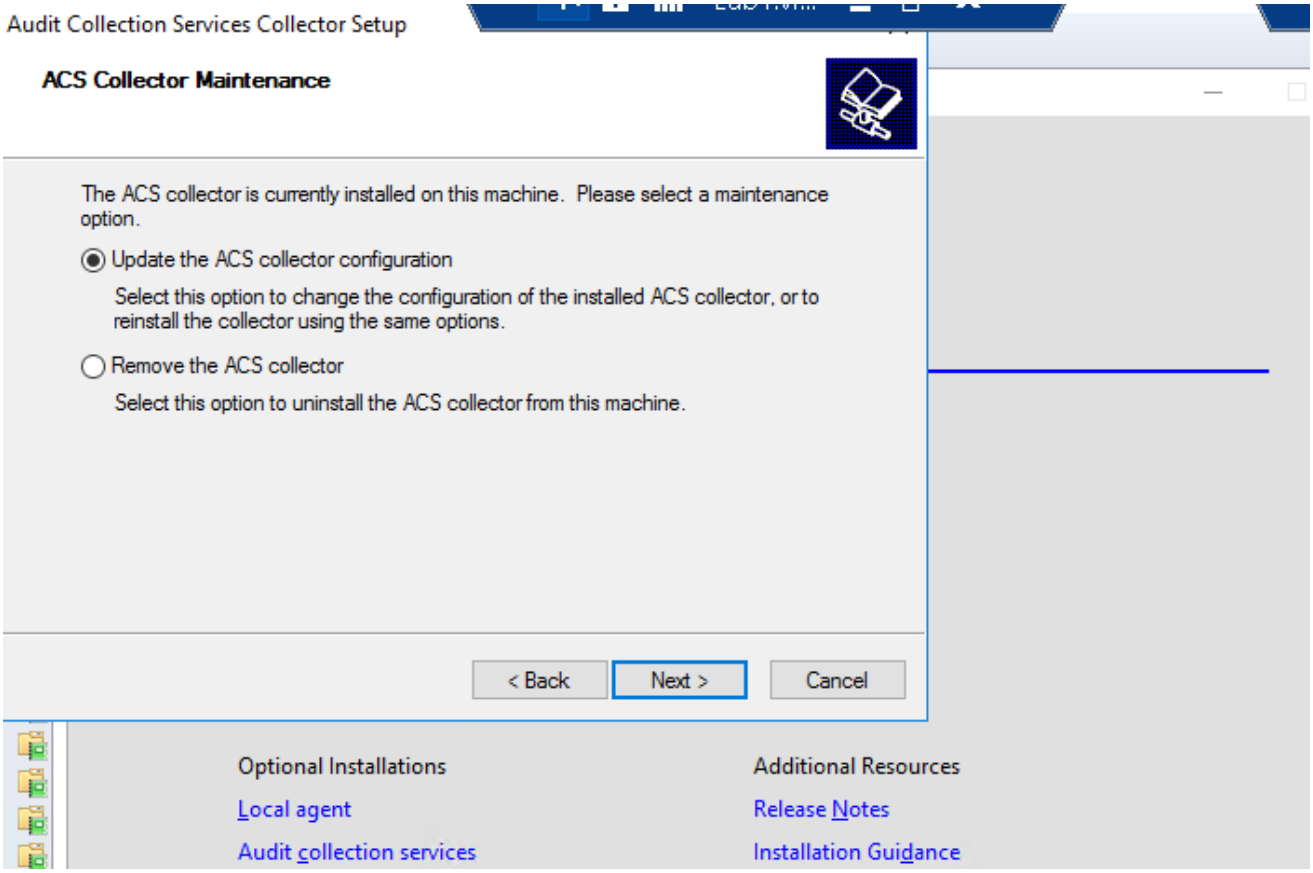

Operations Manager Setup
Processing
Installation progress
Initial configuration
Operational database configuration
Management server
Data warehouse configuration
Operations console
Web console
Reporting
Final configuration
Release Notes
Installation Guide
Read Documentation
System Center Online

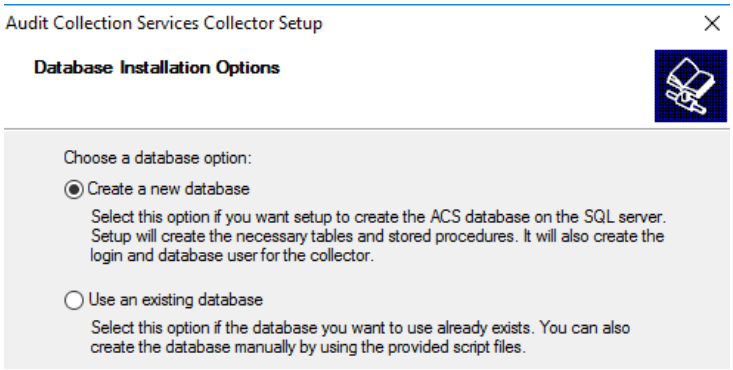


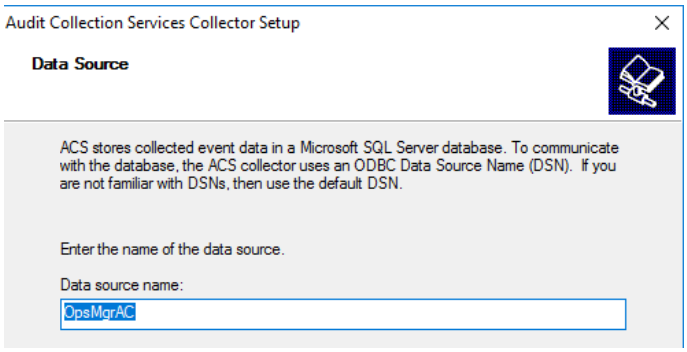
Post-upgrade tasks

- Re-enable the Notification Subscriptions
- Re-enable Audit Collection Services (ACS) on agents that were upgraded
- Reset agent HealthService Cache size
- Verify the upgrade was successful




Audit Collection Services Collector Setup
ACS Collector Maintenance
The ACS collector is currently installed on this machine. Please select a maintenance option.
Update the ACS collector configuration
Select this option to change the configuration of the installed ACS collector, or to reinstall the collector using the same options.
Remove the ACS collector
Select this option to uninstall the ACS collector from this machine.
< Back
Next >
Cancel
Optional Installations
Local agent
Audit collection services
Additional Resources
Release Notes
Installation Guidance


Audit Collection Services Collector Setup
Database Installation Options
Choose a database option:
Create a new database
Select this option if you want setup to create the ACS database on the SQL server. Setup will create the necessary tables and stored procedures. It will also create the login and database user for the collector.
Use an existing database
Select this option if the database you want to use already exists. You can also create the database manually by using the provided script files.


Audit Collection Services Collector Setup
Data Source
ACS stores collected event data in a Microsoft SQL Server database. To communicate with the database, the ACS collector uses an ODBC Data Source Name (DSN). If you are not familiar with DSNs, then use the default DSN.
Enter the name of the data source.
Data source name:
OpsMgrAC

Go with default options

