MICROSOFT SYSTEM CENTER OPERATIONS MANAGER (SCOM) SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 1

09 March 2021

Developed by Microsoft and DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. INTRODUCTION

1.1 Executive Summary

Microsoft System Center Operations Manager (SCOM) is a monitoring platform designed for enterprise customers. It allows system administrators to deploy, configure, and monitor the operations, services, and applications of multiple enterprise Information Technology (IT) systems from one console. SCOM is a multi-platform tool that can monitor Windows, macOS, and Unix-based operating systems (including Linux) and uses management packs developed by third-party vendors to extend its monitoring capability.

1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that "all IT that receives, processes, stores, displays, or transmits DoD information will be […] configured […] consistent with applicable DoD cybersecurity policies, standards, and architectures" and tasks that Defense Information Systems Agency (DISA) "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DoDI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 Microsoft SCOM Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Cyber Exchange website at https://cyber.mil/. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DoD Certificates can obtain the STIG from https://public.cyber.mil/.

1.5 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable will be included in the final STIG. A report marked For Official Use Only (FOUO) will be available for those items that did not meet requirements. This report will be available to component Authorizing Official (AO) personnel for risk assessment purposes by request via email to: disa.stig_spt@mail.mil.

1.6 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DoD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.7 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible AO. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the DoD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied at both the device hardening level and the architectural level due to the fact that some settings may not be configurable in environments outside the DoD architecture.

1.8 Product Approval Disclaimer

The existence of a STIG does not equate to DoD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DoD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with Cybersecurity controls/control enhancements, which supports system Assessment and Authorization (A&A) under the DoD Risk Management Framework (RMF). DoD AOs may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval in accordance with (IAW) DoD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (https://www.niap-ccevs.org/) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (https://www.disa.mil/network-services/ucco) IAW DoDI 8100.04

2. ASSESSMENT CONSIDERATIONS

2.1 Security Assessment Information

This Microsoft SCOM STIG was written based on a Windows platform using the Network Device Management SRG controls. Since SCOM is integrally interwoven into the Windows operating system, many of the controls were inherently met by the Windows operating system and are thus relying on the Windows operating system STIGs to be in compliance. This SCOM STIG also contains requirements that will be validated by reviewing the Windows Active Directory or monitored devices.

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

3.1 Microsoft SCOM Components

Microsoft SCOM is software that monitors services, devices, and operations for many computers, all from a single console. Figure 3-1 shows an example of a single-server configuration.

3.1.1 Management Server

The management server's role is to administer the management group configuration, administer and communicate with agents, and communicate with the databases in the management group.

Additional capacity and availability can be accomplished with a management group of multiple management servers configured as part of a resource pool. The workload will be distributed among the members. If any fail, the others will pick up the workload.

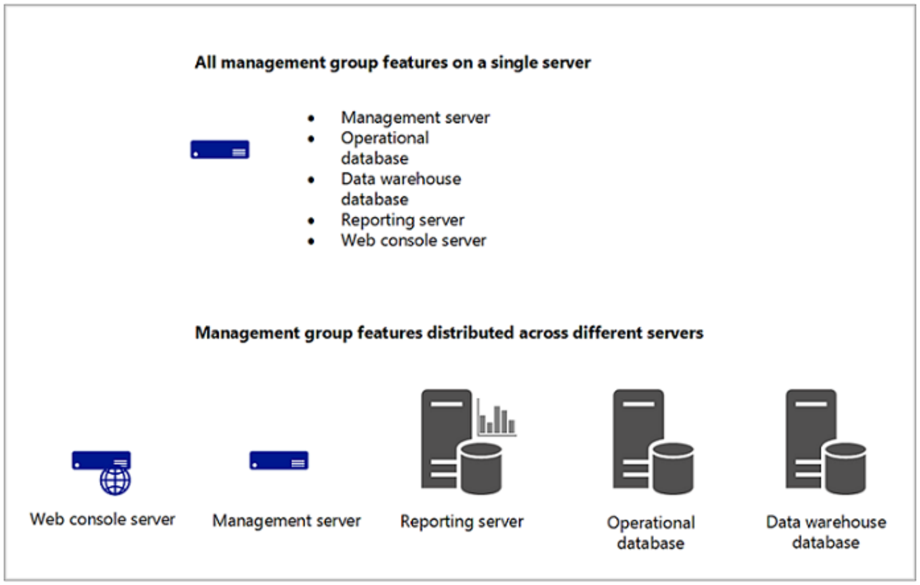
3.1.2 Operational Database

The operational database is a SQL server database that contains the configuration data for the management group. It also stores all monitoring data collected and processed by the management group. This operational database retains short-term data.

3.1.3 Data Warehouse Database

The data warehouse database is a SQL Server database that stores historical monitoring and alerting data. Data that is written to the operations manager database is also written to the data warehouse database, so reports always contain current data. The data warehouse database retains long-term data.

Figure 3-1: Single Server SCOM Configuration



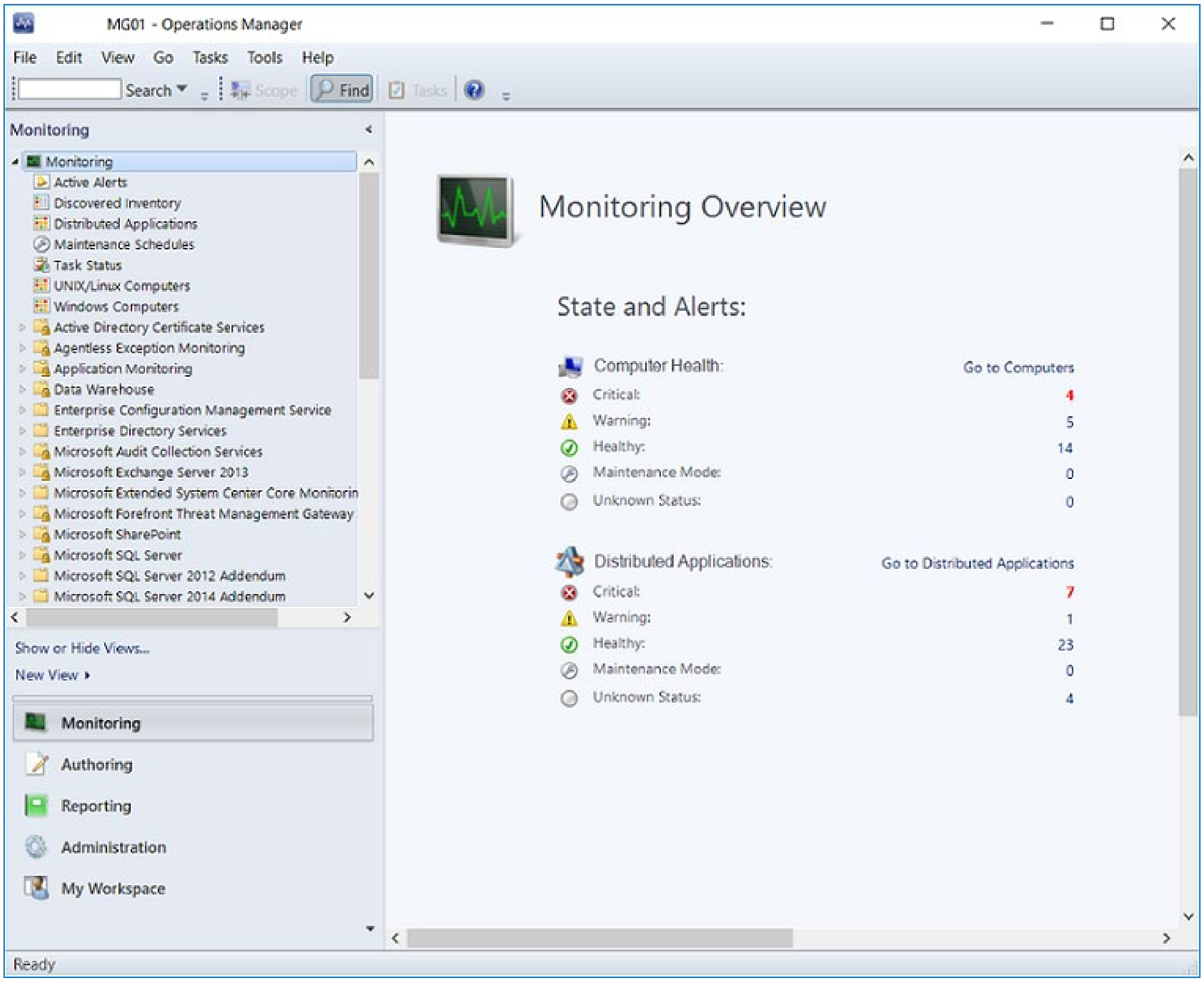
3.1.4 SCOM Consoles

SCOM comes with two consoles. Figure 3-2 shows a sample console.

The Operations console is the primary tool used for managing the deployment of agents and interacting with the alerts and monitoring data, managing and editing monitoring configuration, generating and viewing reports, and administering management group settings.

The Web console is a web-based user interface that provides access to all the monitoring data and tasks that can be run against monitored computers from the Operations console. It does not have full functionality of the Operations console and only provides access to the Monitoring and workspace views.

Figure 3-2: SCOM Console


MG01 - Operations Manager
File
Edit
View
Go
Tasks
Tools
Help
Search
Scope
Find
Tasks
Monitoring
Monitoring
Active Alerts
Discovered Inventory
Distributed Applications
Maintenance Schedules
Task Status
UNIX/Linux Computers
Windows Computers
Active Directory Certificate Services
Agentless Exception Monitoring
Application Monitoring
Data Warehouse
Enterprise Configuration Management Service
Enterprise Directory Services
Microsoft Audit Collection Services
Microsoft Exchange Server 2013
Microsoft Extended System Center Core Monitorin
Microsoft Forefront Threat Management Gateway
Microsoft SharePoint
Microsoft SQL Server
Microsoft SQL Server 2012 Addendum
Microsoft SQL Server 2014 Addendum
Show or Hide Views...
New View
Monitoring
Authoring
Reporting
Administration
My Workspace
Ready

Monitoring Overview

State and Alerts:

Computer Health:	Go to Computers
Critical:	4
Warning:	5
Healthy:	14
Maintenance Mode:	0
Unknown Status:	0

Distributed Applications:	Go to Distributed Applications
Critical:	7
Warning:	1
Healthy:	23
Maintenance Mode:	0
Unknown Status:	4

3.1.5 Agents

Agents, also known as Monitoring Agent or Health Service, are installed on monitored computers. The agent collects data, compares sampled data to predefined values, creates alerts, and responds to alerts. An agent has a designated primary management server to which it reports and from which it receives configuration changes.

The agent calculates the health of the monitored computer and objects on the monitored computer. When the health changes or meets a preconfigured criteria, an alert is generated and sent to the management server.

The agent runs as a service on the monitored computer and will continue to collect performance data, execute tasks, etc., based on its configuration, even if it cannot communicate with the management server. Once a connection is restored, the data is sent to the management server.

3.1.6 Services

Management servers also run the Monitoring Agent as well as the Monitoring Host process service.

In addition, the management server runs the System Center Data Access services, which provide access for the Operation console to the operational database and write data to the database.

The System Center Management Configuration services manage the management group configuration and handle distribution of management packs to monitor systems.

3.1.7 Management Packs

Management packs are distributed to monitored systems and define what information the agent collects and returns to the management server.

3.1.8 Communication Between Agents and Management Servers

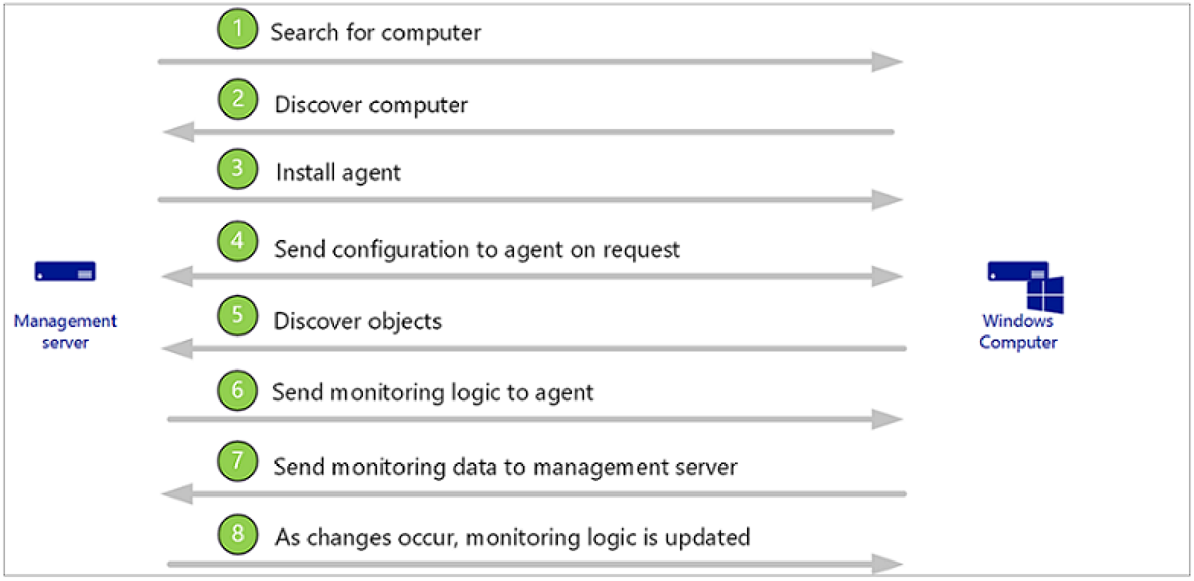
The Operations Manager agent sends alerts and discovery data to the primary management server. The agent also sends event, performance, and state data. In addition, all agents send a heartbeat to the management server on a regular basis to validate the availability of the agent and communication between the agent and the management server.

3.1.9 How Objects Are Discovered and Monitored

The Operations Manager is configured to search for computers with predefined criteria to manage. An Operations Manager agent is then installed on the found computer. Once installed, the agent will request configuration data from, and send its status to, the management server. When configuration data is received, the agent compares the configuration to its current configuration and identifies any objects it discovers, such as its operating system version. It returns that data to the management server. The management server sends monitoring logic specific to the objects discovered. The agent then applies the monitoring logic, runs any workflows, and returns data to the management server.

Figure 3-3 is a simplified illustration of how objects are discovered and monitored.

Figure 3-3: Objects Discovery and Monitoring


1 Search for computer
2 Discover computer
3 Install agent
4 Send configuration to agent on request
5 Discover objects
6 Send monitoring logic to agent
7 Send monitoring data to management server
8 As changes occur, monitoring logic is updated
Management server
Windows Computer