Microsoft Operations Management Suite
Experience Center
Contents

Introduction ............................................................................................................. 3
Scenario 1 – OMS Dashboard Overview ......................................................... 4
Scenario 2 – OMS Search Queries ................................................................. 11
Scenario 3 – OMS Security and Audit ......................................................... 22
Conclusion ........................................................................................................... 29
Terms of use ........................................................................................................ 30
Microsoft Operations Management Suite (OMS) is an enterprise-class IT management solution for hybrid cloud that enables simplified IT management for any organization. OMS gives you flexibility to manage any instance, whether it’s on-premises or in the cloud, such as Microsoft Azure, Amazon Web Services (AWS), Windows Server, Linux, VMware, or OpenStack.

The purpose of this lab guide is to walk you through OMS and its features, including security, auditing, analytics, and threat intelligence across your IT infrastructure. This lab consists of three scenarios to evaluate different OMS capabilities:

1. **OMS Dashboard Overview** – Introduces the OMS Dashboard and solutions for monitoring different infrastructure services, including alerts, change tracking, updates, and resource utilization.

2. **OMS Search Queries** – Introduces the Log Analytics feature, which allows you to perform search queries on any type of machine data. With a wide range of filters and expressions, you can narrow search results to your specific requirements. You also can perform basic to advanced levels of search queries and initiate alert-based notifications.

3. **OMS Security and Audit** – Introduces security and audit features for performing checks across your infrastructure around antimalware, identity and access, system logs and events, threat detection, and security baselines.
The steps below explore the Microsoft OMS Dashboard, various solutions for monitoring infrastructure services, and ways to customize the Dashboard.

Dashboard Overview

1. Log on to the OMS console.

By default, OMS opens the Dashboard view and displays solution metrics. These solutions are the collection of logic, visualization, and data acquisition rules that provide metrics pivoted around a particular problem area.

2. Note that in the left pane, OMS gives navigation options:
Microsoft Operations Management Suite – Experience Center

1. **Log Search** – Provides enterprise-class search functionalities with data visualization and analytics.

2. **My Dashboard** – Provides the ability to build and check your customized dashboard.

3. **Solutions Gallery** – Covers different problem areas to be monitored. At any time, you can add or remove these solutions on your Dashboard and Overview page.

4. **Usage** – Delivers insights about data being used in OMS, with various filters like data consumed today, last 30 days, and data usage per solution. If you are near or have exceeded your daily usage limit, you can optionally remove a solution to reduce the amount of data sent to the OMS service.

5. **Settings** – Provides the ability to configure various functions, such as solutions, data source connections, data, computer groups, accounts, and alerts.

3. Note that in the top right corner, OMS gives quick-to-click options:

   a. **Alerts** – Gives an at-a-glance view of the number of recently generated alerts.

   b. **Language** – Provides various language options for the OMS console.

   c. **Settings** – Takes you to the Settings page.

   d. **Send Feedback** – Shares your feedback with the Microsoft OMS team.

   e. **Help** – Takes you to OMS help documentation.

   f. **Data Plan** – Provides high-level information about your subscribed OMS plan.
g. **User Options** – Delivers options related to the workspace, support, logging out, and more.

**OMS Solutions**

Microsoft OMS offers a wide range of solutions to monitor and analyze common problem areas in IT environments.

1. In the left pane, click the **Solutions Gallery** tile.

   This page shows the list of available and upcoming OMS solutions across different problem areas. Microsoft frequently provides new solutions for monitoring applications, infrastructure, cloud, security, and so on.

![Solutions Gallery](image)

2. Click the name of the solution that you want to add to OMS.

   This page gives you more information about the solution, including screenshots for better understanding.

3. From this page, click **Add** to enable and add the solution to your Overview page.

   A new tile for the solution appears on the Overview page, and you can start using it after the OMS service processes your data.
4. Go to the **Overview** page to explore some solutions and understand how and what type of data is being collected.

In this part of the scenario, you will look at commonly used solutions. Note that solutions related to security and auditing will be explored in more detail in the **third scenario** of this demonstration.

5. Click the **AD Assessment** tile.

This solution helps you to assess the risk level and health of your server environments at a regular interval.

   ![AD Assessment tile](image)

   a. **Security and Compliance** – Shows recommendations for potential security threats and breaches; corporate policies; and technical, legal, and regulatory compliance requirements.

   b. **Availability and Business Continuity** – Shows recommendations for service availability, infrastructure resiliency, and business protection.

   c. **Performance and Scalability** – Shows recommendations to help IT infrastructure grow, validate that the IT environment meets performance requirements, and ensure that the organization can respond to changing infrastructure needs.

   d. **Upgrade, Migration, and Deployment** – Shows recommendations to help upgrade, migrate, and deploy Active Directory to existing infrastructure.

6. View recommendations and take corrective action: Under **Availability and Business Continuity**, click the **Low Priority Recommendation**.
a. Corrective actions are listed in **Suggested Actions**.

b. Completed corrective actions appear as **Passed Objects**.

7. Go back to the **Overview** page, and then open **Alert Management**.

The Alert Management solution helps you analyze all alerts in your environment. In environments with multiple management groups, this solution provides a consolidated view of alerts across all management groups.

a. **Critical Alerts** – All alerts with a severity of Critical, grouped by alert name. Click an alert name to run a log search returning all records for that alert.

b. **Warning Alerts** – All alerts with a severity of Warning, grouped by alert name. Click an alert name to run a log search returning all records for that alert.

c. **Active SCOM Alerts** – All SCOM alerts with any state other than Closed, grouped by the source that generated the alert.

d. **Common Alert Queries** – At any time, you can call common alert queries from this page, or you can create your own search queries related to the alerts.
8. Go back to the **Overview** page. Note that similar to the above two solutions, OMS provides a range of solutions for individual needs. Learn more about OMS solutions [here](#).

9. From the **Overview** page, click the **Azure Automation** tile.

OMS offers flexibility to collect data from cloud services (like Office 365, Azure Automation, Azure Backup, and Azure Site Recovery) and from on-premises solutions (like System Center).

- **Runbooks** – Provides insights about active runbooks in Azure Automation. You can also initiate the runbook creation process from OMS and browse runbooks from the Azure Marketplace.

- **Jobs** – Gives visibility into the number of runbook jobs created within the last seven days.

  Note that with both the Runbooks and Jobs options, you can directly navigate to the Azure Automation portal.

**Customize the Dashboard**

Microsoft OMS allows you to customize the Dashboard to display all required solutions and information on a single page.

1. From the **Overview** page, click the **My Dashboard** tile.

2. In the top left corner, click **Customize**.

   This functionality allows you to add, remove, and edit solutions in the Dashboard.
For any solution, you can add multiple widgets from the new pane that appears on the right side.

3. Click the **Add** tab, select the widget you want to add to your Dashboard, and then click the plus (+) button.

   A new solution widget appears in your Dashboard.

4. In the right pane, click the **Edit** tab, and then select the widget you want to edit or delete.

   This allows you to change the tile visualization type or delete the widget.

A list of all solutions supported by the Microsoft Monitoring Agent is available [here](#).
Microsoft OMS provides Log Search capabilities through the Log Analytics feature. Log Analytics allows you to combine and correlate any type of machine data from various sources within your IT infrastructure. Solutions are powered by Log Search to deliver metrics pivoted around a particular problem area.

On the Log Search page, you can create a query. When you search, you can filter the results by using facet controls. You can also create advanced queries to transform, filter, and report on your results. This scenario looks at options available on the Log Search page.

Simple Search Queries

In this section, you will explore how to use Log Search for simple search queries and how to use filters and timelines.

1. Log on to the OMS console.

2. In the top left corner, click the Log Search tile.

3. Note that the Log Search page includes:
   a. **Search Bar** – Enables you to create and run search queries. When you click the Search bar to run a query, it shows commands you ran earlier and suggests syntax while you are creating the query.
b. **Predefined Queries** – Provides some predefined search queries to start with. You can modify these queries at any time.

A few more queries to try

- All collected data
- Count of all data collected grouped by Type
- All data collected grouped by 1HOUR interval
- All Configuration Changes
  - Required Solution: Change Tracking
- All computers with missing critical or security updates
  - Required Solution: System Update Assessment
- Computers with guest account logons
  - Required Solution: Security

c. **Favorites** – Allows you to save frequently used search queries for your convenience. This option shows the list of previously saved search queries.
d. **History** – Allows you to check the history of all performed search queries.

With Log Search, you can perform searches on any type of machine data. In this part of the scenario, you will start with a simple search for system events, and then filter your results for critical events against a security baseline.

4. In the Search bar, type **Event**, and then run the query.

This returns a huge amount of results data. Now you will use filters and timelines to get more specific results.

e. **Reference Links** – Enables you to access more information about log searches.

With Log Search, you can perform searches on any type of machine data. In this part of the scenario, you will start with a simple search for system events, and then filter your results for critical events against a security baseline.
5. In the left pane, in the **Type** section, click (+) **More** to get more filter types.

6. Select the **SecurityBaseline** filter.

   a. This filter sorts populated results data specific to events related to the security baselines of the machines.

   b. After you select this filter, the command in the Search bar is automatically modified with the filter.

   You can also add filters from the result itself. For example, say that you now need to check among all security baseline events for how many events are critical.

7. From the first item listed below the Search bar, select **RuleSeverity**.
8. In the left pane, under the new filter for RuleSeverity, select **Critical**.

You can also change the timeline to perform search queries on different timelines.

9. Click the **timeline** dropdown menu.

   a. You have the option to search run queries for data generated within the last six hours, one day, or seven days.

   b. You can also customize the timeline to get results data for various timelines.

Finally, you can add advanced filters with AND and OR operators. Continuing with the above search query, you will now add warning events to critical events.

10. Note that the current search query is:

    \( \text{Event Type=SecurityBaseline RuleSeverity=Critical} \)

11. Modify the command by adding the **OR** filter for warning events:

    \( \text{Event Type=SecurityBaseline (RuleSeverity=Critical OR RuleSeverity=Warning)} \)
The results now display both critical and warning events generated against SecurityBaseline. In the same way, you can add a filter for AND to have two conditions to be positive at the same time.

**Advanced Search Queries**

This part of the scenario examines additional functionalities of Log Search to run more advanced search queries. You will perform queries to track performance across all systems within an environment. Then you will drill down into results with more advanced search queries and alerts.

For this example, you will start by monitoring processor performance for all computers within your environment. To do this, you need to define:

- **Type** of search query as **Perf** (performance).
- **ObjectName** to be monitored as **Processor**.
- **CounterName** to be monitored within ObjectName as “% Processor Time”. The counter shows the percentage of time the processor was busy during the sampling interval.
- **InstanceName** as **_Total** to find the value of total processor utilization across all systems. This counter is equivalent to the Task Manager CPU Usage counter. (See more on [measuring % Processor Time](#) later in this section.)

1. Run this query on data that has been generated in the last seven days. In the Search bar, type:

   ```
   Type=Perf ObjectName=Processor CounterName="% Processor Time" InstanceName=_Total
   ```
2. Note that Log Search gives flexibility to manipulate search results.

Log Search provides the following basic commands:

a. **Sort** – The Sort command allows you to define the sorting order by one or multiple fields. By default, a time-descending order is enforced, so to sort your results data in ascending order, add the following command:

```
Type=Perf ObjectName=Processor CounterName="% Processor Time" InstanceName=_Total | Sort TimeGenerated asc
```

Check this result in Table view for more visibility.

b. **Select** – The Select command returns filtered results that do not have all of their original properties. Instead, only the properties that you specify are selected. To filter your search results with specific property values—in this example, Computer, CounterName, and CounterValue—use the following command:

```
Type=Perf ObjectName=Processor CounterName="% Processor Time" InstanceName=_Total | Select Computer,CounterName,CounterValue
```
Now only these property values will be shown for each search result.

3. Use the **Measure** command with your search queries.

This allows you to apply statistical functions to your data and aggregate results grouped by a given field. The Measure command supports multiple statistical functions, including:

a. **Count** – The Count command helps you to count unique and distinct values for your required field. For example, if you want to count processor time events generated by computers, use the following command:

```
Type=Perf ObjectName=Processor CounterName="% Processor Time" InstanceName=_Total | Measure Count() by Computer
```

All results are now aligned by computer name, so you can identify the number of logs related to % Processor Time for each computer.

b. **Maximum, Minimum, and Average** – There are several scenarios where Measure Max(), Measure Min(), and Measure Avg() are useful. In this example, you can find the maximum, minimum, and average values for % Processor Time with the following commands:
Type=Perf ObjectName=Processor CounterName="% Processor Time" InstanceName=_Total | Measure max(CounterValue) by Computer

Type=Perf ObjectName=Processor CounterName="% Processor Time" InstanceName=_Total | Measure min(CounterValue) by Computer

Type=Perf ObjectName=Processor CounterName="% Processor Time" InstanceName=_Total | Measure avg(CounterValue) by Computer
4. Group multiple parameters to look for various aspects of processor performance within a single search query.

Continuing this example, in addition to the previous search where you were looking for % Processor Time, now you also want to search for events related to % User Time, which is the percentage of time a process was running in user mode. With a single query, you get more visibility into different counters of an object. To run such a search query, use the following command:

```
Type=Perf ObjectName=Processor (CounterName="% User Time" OR CounterName="% Processor Time")
InstanceName=_Total
```

Configure Alerts

Log Search allows you to define alerts on the occurrence of specific events. You can easily bind your search queries with alerts based on the number of occurrences and time window. For example, you can define the threshold on processor performance, and whenever it breaches, an alert is generated, with notification through email.

For this example, you will use your previous command and add more specific filters to it. You will track CPU utilization of a specific computer named azure-ws08-001 and define the threshold for % Processor Time as 90%. Logs will be filtered if the threshold is breached and can be mapped to an alert. To create an alert, follow these steps:

1. Use the following command to run the search query:

```
Type=Perf ObjectName=Processor (CounterName="% User Time" OR CounterName="% Processor Time")
InstanceName=_Total Computer="azure-ws08-001"
CounterValue>90
```
2. After the search query completes, on the top menu, click the **Alert** tab.

3. In the **Add Alert Rule** window, define the following values:
   a. Name and description of alert
   b. Severity level
   c. Time window
   d. Alert frequency
   e. Alert parameter for number of results
   f. Email notification details

4. Click **Save**.
5. Review the alert email notification.

Microsoft OMS provides an end-to-end solution for security and audit. With this solution’s audit controls and best practices across hybrid cloud infrastructure, you can gain deep visibility into the overall security of your IT environment.

Visibility into Security Posture

Microsoft OMS delivers built-in search queries for various areas that commonly require attention, including the following:

- Antimalware Assessment
- Update Assessment
- Identity and Access
- Threat Intelligence
- Notable Issues

In this example, you will start by exploring the Antimalware Assessment solution:

1. On the **Overview** page, click the **Security and Audit** solution tile.
2. Click **Antimalware Assessment**.

You can use the antimalware solution in Log Analytics to report on the status of antimalware protection in your infrastructure.
a. **Threat Status and Detected Threats** – Gives visibility into all active and remediated threats for each computer name.

b. **Protection Status** – Shows computers with insufficient protection like out-of-date signature, no real-time protection (no detection of System Center Endpoint Protection), and other related issues.

c. **Protection Types** – Shows computers with various antimalware protection tools, including System Center Endpoint Protection, Malicious Software Removal Tool, and Windows Defender. If no protection tools are detected on a machine, its name will be listed as such.

3. Go back to the Security and Audit solution, and then click **Update Assessment**.

   This helps you to detect missing system updates across all servers—whether they are running in your datacenter or in a public cloud. In this way, you can easily determine your organization’s overall exposure to potential security problems.

a. **Windows Computers** – Gives visibility into computers with missing updates, including critical, security, and others.

b. **Updates Older Than 30 Days** – Allows you to identify missing updates by their age.
c. **Required Missing Updates** – Provides a list of all missing updates by type.

You can also create and manage update run schedules:

4. Click **CLICK TO SCHEDULE AN UPDATE RUN**, where you can see scheduled, running, and completed update runs.

5. Click **Save** to create a new update run.

6. Go back to the Security and Audit solution, and then click **Identity and Access**.

   With an increasing amount of data and applications running in the cloud, it is important to manage authentication and ensure that access remains secure. With Identity and Access, you can monitor all logon activities, failed logon attempts by user account, and more—so you can take proactive or reactive measures, as needed.

   a. **Identity Posture** – Gives visibility into user accounts and logon attempts, including successful and failed logons, locked accounts, accounts with changed or reset passwords, and active notable issues.

   b. **Failed Logon** – Shows the reason behind each failed logon attempt for user accounts.
c. **Logons Over Time** – Shows number of logon attempts sorted by computer.

7. Go back to the Security and Audit solution, and then select **Threat Intelligence**.

This helps you to visualize all malicious traffic on an interactive map. Yellow location pins indicate incoming traffic, while red indicates outgoing. Under Threat Details, you can see the IP address, threat type, overview of the threat, and more.

8. Go back to the Security and Audit solution, and then select **Notable Issues**.

Notable issues are categorized by severity level and count, making it easy to focus on those that need immediate attention.

**Threat Identification and Remediation**

The threat identification and remediation features of OMS enable you to identify specific security events and define appropriate remediation actions.

In this scenario, you will search an app for its security events. Specifically, you will take a HeavyLoad (stress test tool) app running on an Azure VM and identify its processes from security events that OMS
collects. For remediation against those processes, you will configure alert rules to notify the IT team and define automated actions.

1. On the **Overview** page, click the **Log Search** tile.

![Log Search tile](image)

2. In the Search bar, perform the following query:

   ```plaintext
   Type=SecurityEvent Process="HeavyLoad.exe" | Select Computer,Account,Process,Activity,TimeGenerated
   ```

   In this query, you are identifying any security event for the process HeavyLoad.exe, which can cause high CPU, memory, or I/O. The search query filters the logs to identify computers with the security event and the process.

![Search bar output](image)

   Based on the query, you can define specific actions against the occurrence of the event:

3. On the results page, click **Alert**.
4. On the **Add Alert Rule** page, define the required properties for your alert.

5. Click **Yes** for **Runbook**.

This will fetch a list of active runbooks from your connected Azure Automation account.

In this example, you will stop the Azure VM found to have malicious activity (like a process of HeavyLoad.exe) using a predefined runbook. Runbooks are used to automate tasks and orchestrate actions.
6. From the dropdown menu, select the `stop-myazurevm` runbook to stop the Azure VM when the security event occurs.

7. Click **Save** to save this alert rule.

In this way, you can identify any threat or malicious activity at the user or device level, and perform appropriate remediation actions against a security breach.
This demonstration highlighted specific capabilities and features of Microsoft Operations Management Suite designed to assist you in quickly discovering and remediating performance and security issues.

For more information:
© 2016 Microsoft Corporation. All rights reserved.

By using this Hands-on Lab, you agree to the following terms:

The technology/functionality described in this Hands-on Lab is provided by Microsoft Corporation in a “sandbox” testing environment for purposes of obtaining your feedback and to provide you with a learning experience. You may only use the Hands-on Lab to evaluate such technology features and functionality and provide feedback to Microsoft. You may not use it for any other purpose. You may not modify, copy, distribute, transmit, display, perform, reproduce, publish, license, create derivative works from, transfer, or sell this Hands-on Lab or any portion thereof.

COPYING OR REPRODUCTION OF THE HANDS-ON LAB (OR ANY PORTION OF IT) TO ANY OTHER SERVER OR LOCATION FOR FURTHER REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PROHIBITED.

THIS HANDS-ON LAB PROVIDES CERTAIN SOFTWARE TECHNOLOGY/PRODUCT FEATURES AND FUNCTIONALITY, INCLUDING POTENTIAL NEW FEATURES AND CONCEPTS, IN A SIMULATED ENVIRONMENT WITHOUT COMPLEX SET-UP OR INSTALLATION FOR THE PURPOSE DESCRIBED ABOVE. THE TECHNOLOGY/CONCEPTS REPRESENTED IN THIS HANDS-ON LAB MAY NOT REPRESENT FULL FEATURE FUNCTIONALITY AND MAY NOT WORK THE WAY A FINAL VERSION MAY WORK. WE ALSO MAY NOT RELEASE A FINAL VERSION OF SUCH FEATURES OR CONCEPTS. YOUR EXPERIENCE WITH USING SUCH FEATURES AND FUNCTIONALITY IN A PHYSICAL ENVIRONMENT MAY ALSO BE DIFFERENT.

FEEDBACK. If you give feedback about the technology features, functionality and/or concepts described in this Hands-on Lab to Microsoft, you give to Microsoft, without charge, the right to use, share and commercialize your feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft software or service that includes the feedback. You will not give feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because we include your feedback in them. These rights survive this agreement.

MICROSOFT CORPORATION HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH REGARD TO THE HANDS-ON LAB, INCLUDING ALL WARRANTIES AND CONDITIONS OF MERCHANTABILITY, WHETHER EXPRESS, IMPLIED OR STATUTORY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. MICROSOFT DOES NOT MAKE ANY ASSURANCES OR REPRESENTATIONS WITH REGARD TO THE ACCURACY OF THE RESULTS, OUTPUT THAT DERIVES FROM USE OF THE VIRTUAL LAB, OR SUITABILITY OF THE INFORMATION CONTAINED IN THE VIRTUAL LAB FOR ANY PURPOSE.

DISCLAIMER

Copyright © 2016 Microsoft, Inc. All rights reserved. This document is for informational purposes only. Microsoft makes no warranties, express or implied, with respect to the information presented here.