Microsoft

Operations Management Suite

-Log Analytics Labs

6/14/2017 12:56:00 PM

Version 1.2 Final

Prepared by

Peggy Pinelo Merchan & Patrick Mandemaker
Global Black Belts TSP – Hybrid Management / Hybrid Storage WE

Contributors

Gustav Kaleta

Document Revision

Change Record

Date	Author	Version	Change Reference
January 26, 2017	Patrick Mandemaker	0.2	
March 9, 2017	Cenk Ersoy		
June 6, 2017	Patrick & Anthony	1.2	Changed the order

Reviewers

Name	Version Approved	Position	Date
Patrick Mandemaker	1.2		06/06/2017

Table of Contents

Introduction

Estimated time to complete this lab

240 minutes

Objectives

During this lab, you will learn how to use Microsoft Operations Management Suite (OMS) to:

- Protect heterogeneous environments.
- Respond proactively to changing business needs.
- Simplify IT management.
- Gain immediate, actionable insights.
- Provide all-in-one cloud management.

Prerequisites

- Laptop/computer with Internet browser
- You can only install the OMS MMA on computers running Windows Server 2008 SP 1 or later or Windows 7 SP1 or later.
- You'll need an OMS subscription (free tier). For additional information, see Get started with Log Analytics.
- Each Windows computer must be able to connect to the Internet using HTTPS. This connection can be direct, via a proxy, or through the OMS Log Analytics Forwarder.
- You can install the OMS MMA on stand-alone computers, servers, and virtual machines. If you want to connect Azure-hosted virtual machines to OMS, see Connect Azure virtual machines to Log Analytics.
- The agent uses HTTPS (port 443) for various resources. For more information, see Configure proxy and firewall settings in Log Analytics.

Note regarding pre-release software

Portions of this lab may include software that is not yet released, and as such may still contain active or known issues. While every effort has been made to ensure this lab functions as written, unknown or unanticipated results may be encountered because of using pre-release software.

Note regarding user account control

Some steps in this lab may be subject to user account control. User account control is a technology which provides additional security to computers by requesting that users confirm actions that require administrative rights. Tasks that generate a user account control confirmation are denoted using a shield icon. If you encounter a shield icon, confirm your action by selecting the appropriate button in the dialog box that is presented.

Note regarding resource location West Europe

Throughout this lab, we suggest location West Europe. Of course, you are free to choose the location nearest to you as long all the resources reside in the same location.

Student Materials

All student materials are available for download here:

Https://aka.ms/omslabs

Activity 1: Getting Started

Estimated time to complete this activity

110 minutes

Objectives

In this activity, you will create the various accounts necessary to perform this lab:

- An Outlook.com email account (Microsoft Account).
- An Azure Pass account.
- A Microsoft Operations Management Suite (OMS) account.

You will then associate the OMS account with the Microsoft Azure account, and sign in to the Microsoft Operations Management Suite web site. You will perform initial configuration tasks to connect your servers to OMS.

You will perform tasks necessary to integrate OMS with System Center Operations Manager 2012 R2.

Finally, you will be introduced to OMS Solutions, which will assist you in gaining deeper insight into your environment.

Exercise 1: Prepare for Operations Management Suite (OMS) Environment

In this exercise, you will create a Microsoft Security Account and a Microsoft Azure account and then link it to a newly created Microsoft Operations Management Suite Workspace. You will be introduced to Operational Insights, an online service that analyzes installations of Microsoft Server software and see how it integrates with System Center Operations Manager and OMS.

📌 You can use existing Azure/OMS accounts, but it is recommended that you use an account created specifically for these OMS labs.

📌 We also strongly recommend that you use InPrivate browsing to ensure that you are not automatically logged on with other credentials during the registration / activation process.

Create a New Outlook.com Account

In this task, you will create an email account to be associated with Microsoft Azure and OMS.

> ◈ We strongly recommend that you create a new Microsoft ID account specifically for this lab. The domain name suffix for your email account must be either outlook.com or hotmail.com. These instructions will allow you to create a new Outlook account.

1. On the taskbar, right-click **Internet Explorer** and click **Start InPrivate Browsing**.
2. In the Address Bar, type **http://www.outlook.com** and press ENTER.
3. Click **Sign up**.
4. On the Create an account page, complete the information and click **Create account**.
5. Click on the welcoming pages. Then click on "**Let's Go**" button.
6. Close the Outlook.com window.

Establish a Microsoft Azure Account Using a Promo Code

In this task, you will create a Microsoft Azure Account using a Promo Code **if you don't have a subscription already**. The Azure Pass (promo code) is available upon request by the trainer delivering this workshop.

> ◈ the Microsoft Azure Pass Subscription has a CPU Core limitation of 10. Therefore, after deployment of 3 SharePoint VMs you **MUST** resize the VMs to be able to deploy the 4th Linux VM.

1. On the taskbar, right-click **Internet Explorer** and click **Start InPrivate Browsing**.
2. In the Internet Explorer address bar, type http://www.microsoftazurepass.com and press ENTER.
3. From the drop-down menu, select the country you are in.
4. Type a promo code and click **Submit**.

> 📌 A promotional code will be provided in the Content Tab of the Lab Console. Once you have submitted the promotional code, it will take a few minutes for the account to become activated. Only one promo code can be redeemed per the life of the Microsoft ID.

5. Click **Sign in**.
6. In the email or phone field, type the email address for the Outlook.com account you just created.
7. Type the account password and click **Sign in**.
8. Click **Submit**.
9. Click **Activate**.

◈ Azure Pass activation may take several minutes. DO NOT close the browser.

10. If prompted for a Contact phone number, enter **555-555-5555** or provide the same phone number you used when creating the outlook account.
11. Click **I agree to the subscription agreement, offer details, and privacy statement**.
12. Click **Sign up**.

   ⚠ Wait until the Azure setup process completes. DO NOT close the browser.

13. Click **“Get Started with your Azure subscription”**
14. Click through the Windows Azure Tour or close it.
15. Close Internet Explorer.

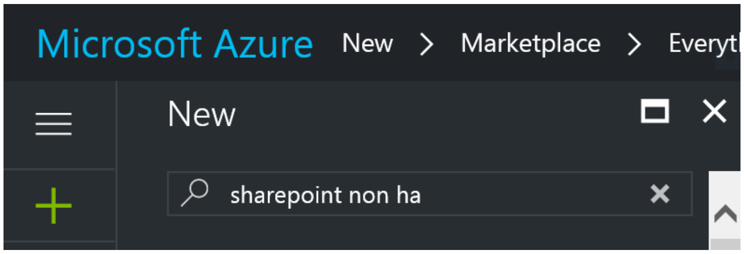
Deploy a SharePoint 2013 Farm via Azure Marketplace

The SharePoint 2013 non-HA Farm template deploys a SharePoint Server 2013 two-tier farm topology including Active Directory Domain Services and Microsoft SQL Server with three servers and 10 cores (using default virtual machine sizes). The completed deployment consists of a Windows Server 2012 R2 domain controller, a SQL Server 2014 server, and a SharePoint 2013 server.

1. On the Internet Explorer Favorites Bar, click **Azure Portal**.

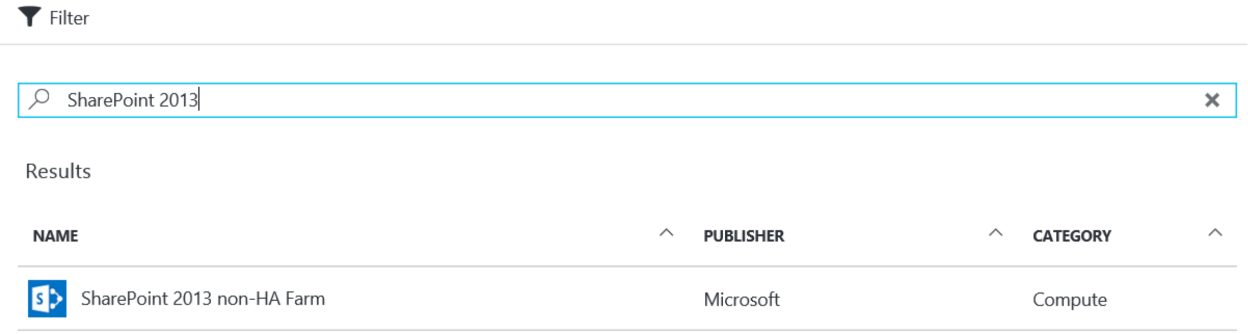
   📌 The Microsoft Azure Portal will open from http://portal.azure.com.

2. Click “+New” in the upper left corner and type **SharePoint 2013 non** and press Enter.



sharepoint non ha

3. The filter view will show the templates available in Marketplace. We’re only interested in **SharePoint 2013 non-HA Farm** so select that one.



SharePoint 2013

Results

NAME	PUBLISHER	CATEGORY
SharePoint 2013 non-HA Farm	Microsoft	Compute

📌 This wizard creates everything from scratch for your new farm; a new virtual network in Azure, Active Directory, SQL Server(s), and all the SharePoint servers.

4. Click the Create button and in the Create Wizard
5. Fill in the details and make sure you set:

PS: If you are sharing an Azure subscription with other people in your organization, you must select a different Resource Group name (such as “omslab1”, “omslab2” etc). If that name in all future steps.

Resource Group=	**omslab**
Location =	**West Europe**
Username=	**AdAdministrator**
All passwords =	**Passw0rd2017!**
Storage account name prefix =	**<pick something random but unique, all lower case>**
Storage account type =	**Change to “L Locally Redundant”**
Virtual Network Name =	**<default>**
Forest root domain name =	**Contoso.com**
Active Directory Virtual Machine Size =	**<default>**
SQL Server Virtual Machine Size =	**<default>**
Service account password =	**Passw0rd2017!**
SharePoint Server Public IP:	**<default>**
DNS label =	**< pick something random but unique, all lower case>**
Setup user account password =	**Passw0rd2017!**
Server farm account password =	**Passw0rd2017!**
Server farm passphrase =	**Passw0rd2017!**
Content site template =	**<default>**

📌 To reduce costs, we suggest Standard LRS.

6. In the “Summary/Validate” view, one the button turns blue, click “**OK**”
7. In the **Purchase** pane, click purchase at the bottom. Deployment will take approximately **30-60 minutes**.
8. **Check occasionally** of the 3 VMs have been created. Even when status is still deploying you can continue to the next activity.

◇ If you are using a Microsoft Azure Pass Subscription you MUST resize the VMs after deployment by selecting the VM and clicking the size tab. Select a VM with 2 cores. Do this for all 3 VMs.

Create a Microsoft Azure Automation Account.

Microsoft Azure Automation accounts are used to automate the deployment, monitoring, and maintenance of resources in Azure. An Automation Account is a container for your Azure Automation resources. It provides a way to separate your environments or further organize your Automation workflows and resources.

In this task, you will create an Automation account that can be used by OMS when implementing an Automation Solution.

1. On the taskbar, right-click **Internet Explorer**.
2. On the Internet Explorer Favorites Bar, click **Azure Portal**.

   The Microsoft Azure Portal will open from http://portal.azure.com.

3. Sign in using your Microsoft Azure credentials.
4. Click **+New**, then click **Monitoring + Management,** and click **Automation Account** or search for **"Automation"**.
5. In the "Add Automation Account" blade, in Name, type **MyAutomation**.
6. Select existing **Resource group**, click "**Use Existing**" and then select "omslab" in the pull down menu
7. Create Azure **RunAs** account **Yes.**
8. Click **Region** and select **West Europe**.
9. Click "**Pin to Dashboard**"
10. Click **Create.**

    Record the details of the account for use in future tasks.

Exercise 2: Establish a Microsoft Operations Management Suite (OMS) Environment

Sign up for existing Workspace (OMS Experience Center)

In this exercise, you will sign up for the Microsoft Experience center workspace. With this environment, you can see how Operations Management Suite works, and what kind of services OMS can deliver for your organization without installing anything. It's a live environment ready for demo purposes. Later you will also create your own workspace, so you will gain a full understanding and have full permissions.

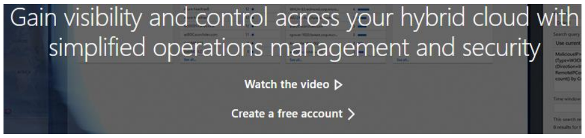
Later you will create your own workspace as well.

In this task, you will sign in to the OMS web site.

1. On the taskbar, click **Internet Explorer**.

   The home page is http://www.microsoft.com/oms

2. Click **on Create a free account**.



Gain visibility and control across your hybrid cloud with simplified operations management and security

3. Click the sign up for the experience and provide your details.
4. Select **Insight and Analytics** scenario after clicking on Sign up for the Experience. A PDF is downloaded during sign up.

5. You can now access the environment which contains 500 servers, running on-premises as well as the cloud – in both Azure and AWS. The on-premises system is managed by System Center, and the key workloads being monitoring include; Exchange, SharePoint, SQL, and even MySQL running on Linux.

Create a free new OMS Workspace using Microsoft Azure

1. On the taskbar, click **Internet Explorer** and open the Azure Portal.

📌 The home page is https://portal.azure.com

2. Click **+New**, then click **Monitoring + Management,** and browse the list of services, and then select **Log Analytics.**
3. Click **Add,** then make sure you set:

   OMS Workspace = **<pick a unique name>**
   Resource Group = click on **“Use Existing”** and select **“omslab”** in the pull down list
   Location = **West Europe**

   Pricing Tier = **Free**

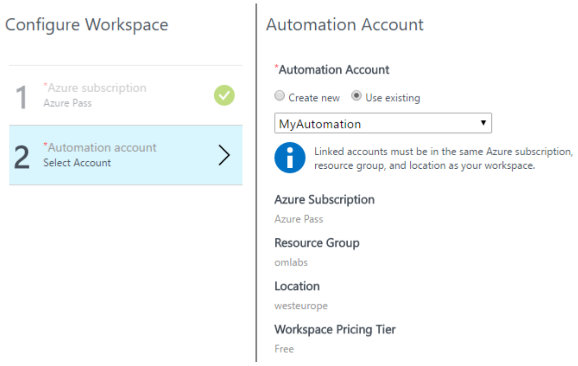
4. Click on “**Pin to Dashboard**”. Then click **OK .** Do not close the blade until you see “Validation Successful” button at the bottom**.**

5. On the Azure Portal, click on the “**Resource Groups**” icon (). Then click on “omslabs” resource group. From the drop down list, click on the name of the workspace you created to see the details.

Configure the OMS Workspace

1. On the taskbar, right-click **Internet Explorer** and click **Start InPrivate Browsing**.
2. Go to **http://mms.microsoft.com** and sign in
3. Select the OMS workspace you created earlier by clicking on the arrow on the right. If prompted to confirm the email, you may click on “Skip This Step” option. Wait until the workspace is displayed.
4. Click **Solution Gallery** button**,** add the solution “**Automation & Control**” by clicking on it.

5. In the **“Configure Workspace”** step, select **“Use existing”,** and select the **Automation Account** you created earlier. Click on “**OK**”. This links the automation account to the OMS Workspace.



Configure Workspace

1 *Azure subscription
Azure Pass

2 *Automation account
Select Account

Automation Account

*Automation Account

○ Create new ● Use existing

MyAutomation

Linked accounts must be in the same Azure subscription, resource group, and location as your workspace.

Azure Subscription
Azure Pass

Resource Group
omlabs

Location
westeurope

Workspace Pricing Tier
Free

6. Click on “**Close**”.

Activity 2: Getting started with Insight & Analytics

Estimated time to complete this activity

75 minutes

Exercise 1: Configure Insights & Analytics

In this exercise, you will become familiar with the OMS console. You will learn how to configure OMS to collect data. In addition, you will learn how to customize your OMS dashboard and how to provide feedback to Microsoft regarding suggested improvements to OMS. You will also see how to access OMS documentation from the Azure Portal.

Sign in to Microsoft Operations Management Suite via Azure Portal

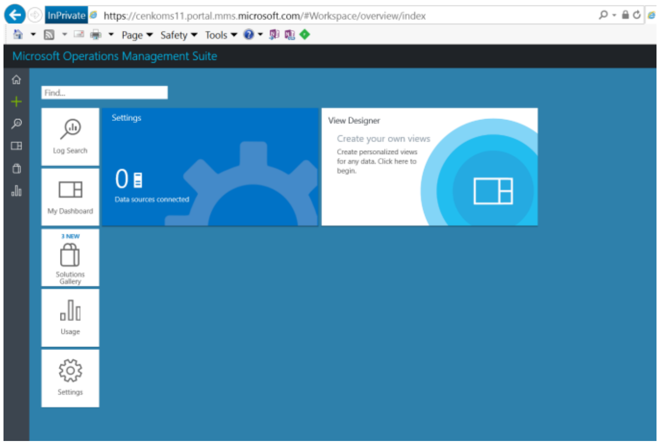
1. Right click on **Internet Explorer** and open the browser in "InPrivate Browsing" mode.
2. On the Internet Explorer Favorites Bar, click **Azure Portal**.

   📌 The Microsoft Azure Portal will open from http://portal.azure.com.

3. Sign in using your Microsoft Azure credentials.
4. In the Azure portal, click on the "**Resource Groups**" icon (⬢). Then click on "omslabs" resource group. Browse the list of services, and then select **Log Analytics**. Then click on the "OMS Portal" view.

Another method to reach the OMS portal is to use the "http://mms.microsoft.com" site. This method is shown in the next section.

Connect Windows computers directly to OMS.


InPrivate
https://cenkoms11.portal.mms.microsoft.com/#Workspace/overview/index
Page
Safety
Tools
Microsoft Operations Management Suite
Find...
Log Search
My Dashboard
3 NEW
Solutions Gallery
Usage
Settings
Settings
0
Data sources connected
View Designer
Create your own views
Create personalized views for any data. Click here to begin.

There are 3 options how you can connect your server environment to gather data.

- One of the options is to Connect any Server or client directly by installing an agent.
- The other is using your existing System Center Operations Manager to attach your management groups or your entire Operations Manager deployment.
- Last, you can use an Azure storage account configured with the Windows or Linux Azure diagnostic VM extension. In the following section, we detail the steps for direct agent connect only.

To connect computers directly to OMS you need to download the agent. In the OMS portal, on the **Overview** page, click the **Settings** tile. You can pick a windows server within your own environment, Azure IaaS or even install directly on your own device.

1. Right click on **Internet Explorer** and open the browser in “InPrivate Browsing” mode.
2. Go to the following site:

📌 The home page is http://mms.microsoft.com

3. Click **Sign in**

   ⚠ If you see any existing account credentials, click Use another account.

4. Enter the credentials associated with OMS, and click **Sign in** again.
5. Click on the right arrow next to the OMS Workspace name.

   📌 The OMS Portal will open.

6. On the dashboard, click the **Settings** tile.
7. On the Settings blade, click **Connected Sources**.

   📌 You have multiple options for connecting your server environment to OMS: You can attach any Windows server or Linux client directly; attach your management groups or your entire Operations Manager deployment; or attach any Azure storage account configured with the Windows or Linux Azure Diagnostic VM extension.

8. Under “Windows Servers”, click **Download Windows Agent (64 bit)**.
9. Click **Run**.
10. In the Microsoft Monitoring Agent Setup Wizard, click **Next**.

11. Click **I Agree**.
12. On the Destination Folder page, click **Next**.
13. Click the checkbox next to **Connect the agent to Microsoft Azure Operational Insights** and click **Next**.
14. Switch to the OMS Settings blade, click the **Copy** icon next to **WORKSPACE ID,** and click **Allow access.**
15. Switch to the Microsoft Monitoring Agent Setup wizard, click in the **Workspace ID** field in the Wizard, and press CTRL-V.
16. Switch to the OMS Settings blade, click the **Copy** icon next to **PRIMARY KEY** and click **Yes**.
17. Switch to the Microsoft Monitoring Agent Setup wizard, click in the **Workspace Key** field in the Wizard, and press CTRL-V.
18. Click **Next**.
19. Click **Install**.
20. Click **Finish**.
21. Right-click **Start** and click **Control Panel**.
22. Click **Microsoft Monitoring Agent**.

    ◈ If necessary, switch View by: to Small icons.

23. Click the **Azure Log Analytics (OMS)** tab.

    📌 Note that the **Connect to Azure Operational Insights** checkbox is selected, and Microsoft Monitoring Agent has successfully connected to the Operations Management Suite Service.

24. Click **Cancel**.
25. Deploy the agent on remaining systems created (VMs of the SharePoint farm, “spfarm-ad”, ‘spfarm-sql” and “spfarm-sp”) via Log Analytics extension screen in the Azure portal:

    a Sign into the Azure portal.
    b On the “Search Resources” line at the top type in **Log Analytics** and press Enter.
    c In your list of Log Analytics workspaces, select the one that you want to use.
    d Under **Log Analytics Management,** select **Virtual machines** under “Workspace Data Sources” section.
    e In the list of **Virtual machines,** select the virtual machines on which you want to install the agent. The **OMS connection status** for the VM indicates that it is **Not connected.**
    f Click on the “Not Connected” in the details for your virtual machine, select **Connect.**
    g Close the blade and repeat for the other VMs of the SharePoint farm.

Alternatively, you can use the script provided with the lab: **AddOMSExtension.ps1**

26. When complete, the status of the OMS connection will change to connected.

Create and connect a Linux computer to OMS

BEFORE THE FOLLOWING STEPS, MAKE SURE THAT YOU HAVE REDUCED THE SIZE OF THE VMS OF THE SHAREPOINT FARM BY FOLLOWING THESE STEPS:

1. In the Azure Portal, click on "**Virtual Machines**" icon (🖥) on the left.
2. Select the desired VM ("spfarm-sql") and then click on "**Size**" under "Settings"
3. Change the size from DS3 (4 cores) to DS2 (2 cores).
4. Repeat the same steps for "spfarm-sp".

In this exercise, you use a template which deploys an Ubuntu VM with the OMS extension installed and onboarded to your workspace.

1. In the Azure Portal, click "**+New**" to open **Azure MarketPlace.**
2. Type **CentOS** and press Enter. Then select **CentOS-Based 7.3** by Rogue Wave Software
3. Verify at the bottom that the deployment model is **Resource Manager** and then click **Create.**
4. Fill in the **details** and make sure you set:

Name =	**lx-centos**
VM Disk Type:	**HDD**
Username=	**lxadministrator**
Authentication Type=	**Password**
Password =	**Passw0rd2017!**
Location =	**West Europe**
Resource Group=	**omslab**
VM Type=	**DS1_V2**

5. In **Settings**, leave the defaults for Storage and Network values, and click **OK.**
6. Once the "Validation Passed" state is reached, click **OK.**
7. Once the VM is created, click the **overview blade** (select using "Virtual Machines" on the left) and note the **public IP** in the "Essentials" section.
8. If you are on a Windows workstation, you need to use PuTTY, MobaXTerm or Cygwin to **SSH to** Linux.
9. Login with Putty or another terminal program to **validate if you can connect to the VM**. Type "exit" to close the SSH session.
10. Deploy the agent via Log Analytics in the Azure portal:
    a. On the "Search Resources" line at the top type in **Log Analytics** and press Enter.
    b. In your list of Log Analytics workspaces, select the one that you want to use.
    c. Under **Log Analytics Management,** select **Virtual machines** under "Workspace Data Sources" section.

   d. In the list of **Virtual machines,** select the Linux virtual machine on which you want to install the agent. The **OMS connection status** for the VM indicates that it is **Not connected.**
   e. Click on the “Not Connected” in the details for your virtual machine, select **Connect.**

11. Once the agent is installed it will take 5-10 minutes before it reports to the workspace.

Configure Workspace Settings

In this task, you will use the OMS Settings tile which allows you to configure Solutions, Logs, and Accounts.

1. Sign in to the **OMS Portal** using your Azure subscription.
2. Go to http://mms.microsoft.com
3. Go to **Settings**.
4. Select **Data.**
5. Click **Windows Event logs**
6. You can add an event log by typing in the name of the log and **clicking +** on the far right. If the (+) does not show, reduce the zoom on your browser**.** *As you type the name of an event log, Log Analytics provides suggestions of common event log names.*
7. Add **System** and **Application**
8. Make sure you’ve selected the check boxes next to **ERROR**, **WARNING**, and **INFORMATION**
9. Click the **SAVE** button in the upper left.
10. Click **Windows Performance Counters** and select **Add the selected Performance Counters** button.
11. Click **Linux Performance Counters** and select **Add the selected Performance Counters** button.
12. Click the **SAVE** button in the upper left.
13. Click IIS.
14. Select the check box next to **Collect W3C format IIS log files**.
15. Go to **SysLog**
16. You can add an event log by typing in the name of the log and **clicking +.** *As you type the name of an event log, Log Analytics provides suggestions of common event log names will appear.*
17. Add **auth, authpriv, cron, daemon, kern, local0, local1, mail, syslog and user.**
18. Select **ALL** the check boxes such as **EMERGENCY**, **ALERT**, and **CRITICAL.**
19. Click the **SAVE** button in the upper left.
20. On the “Settings” blade, review the **ACCOUNTS**.

   📌 This page provides the ability to configure your workspace(s) and manage OMS user accounts.

(OPTIONAL) Configure Custom Logs

In this task, you will add a custom log parse each record in the log into individual fields using the Custom Fields feature of Log Analytics. Many applications log information to text files instead of standard logging services such as Windows Event log or Syslog.

✏ Begin this task logged on to **Spfarm-ad** as **Contoso\AdAdministrator** with the password **Passw0rd2017!** using RDP.

a. On the “Search Resources” line at the top type in **spfarm-ad** and press Enter.
b. In your list of VMs, select the one that you want to use.
c. Click on **Connect**.
d. Open the RDP program at the bottom of your screen to RDP to the virtual machine.
e. Click **Connect**
f. Click on **More Choices**
g. Select “**Use a Different Account**” option
h. Use “\AdAdministrator” (with a back slash) as user and provide the password (**Passw0rd2017!**)
i. Click on **Yes**
j. The initial login may take several minutes. Wait until you see the Server Manager desktop.
k. Close the “Server Manager”.

1. Copy the script **Customlog-Transactions** to the desktop of **Spfarm-ad.**

2. Right-click **Customlog-Transactions** and click **Run with PowerShell.**

   📌 For our test scenario, we simulate a customer facing application that logs information about each critical transaction at a frequent basis into a text file in the following format: 2016-06-21

3. On the taskbar of this server (not your desktop! Bu the “spfarm-ad” VM that you have RDP), click **Internet Explorer** and open operations management suite page.
   - 📌 The home page is http://mms.microsoft.com
   - 📌 You might want to turn off IE Enhanced Security by starting “Server Manager”, going into “Local Server”

4. Click **Sign in**

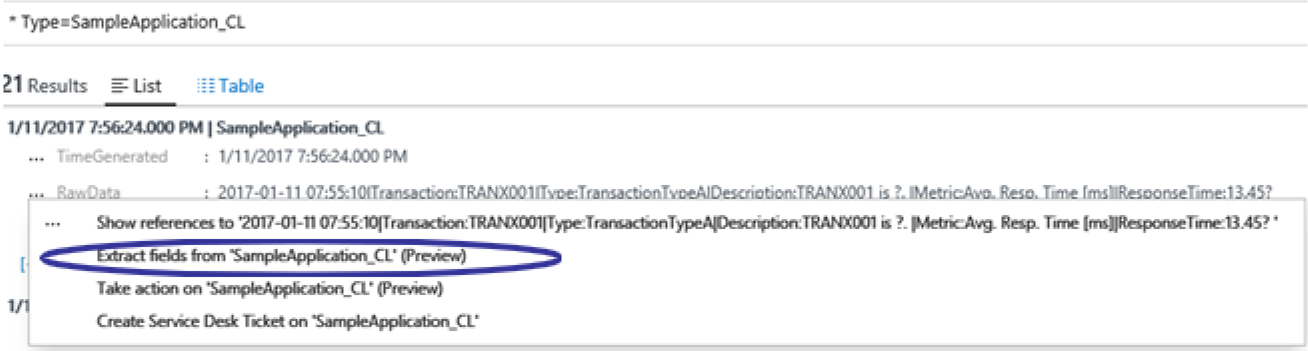
3 Open **Settings**
4 Select **Data**, and select the **Custom Logs** option. Click on “**+Add**” and click to browse to "**C:\TempLogs\SampleApplication.log"**
5 Leave the default **New Line** and click Next
6 Add the log collection path: **C:\TempLogs\SampleApplication.log**
7 Name it **SampleApplication** and click Done.

8 Right-click **Customlog-Transactions** and click **Run with PowerShell** for the 2nd time.

📌 We run the script again to simulate a scenario where the text file is updated with application transaction information.

9 Wait 5-10 minutes and validate that the data in the text file is being collected successfully and searchable in OMS Log Analytics by running a search query of **Type=SampleApplication_CL**

10 Use the context menu option (click on **…**) to **Extract fields** to begin creating custom fields



* Type=SampleApplication_CL

21 Results   List   Table

1/11/2017 7:56:24.000 PM | SampleApplication_CL

… TimeGenerated : 1/11/2017 7:56:24.000 PM

… RawData : 2017-01-11 07:55:10|Transaction:TRANX001|Type:TransactionTypeA|Description:TRANX001 is ?. |Metric:Avg. Resp. Time [ms]|ResponseTime:13.45?

… Show references to '2017-01-11 07:55:10|Transaction:TRANX001|Type:TransactionTypeA|Description:TRANX001 is ?. |Metric:Avg. Resp. Time [ms]|ResponseTime:13.45? '

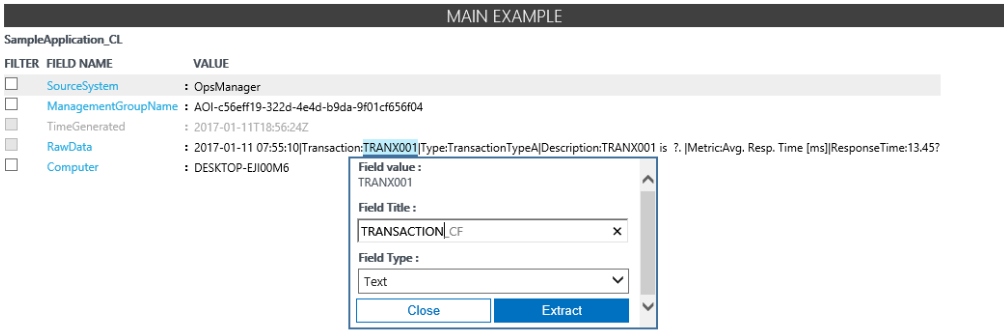
Extract fields from 'SampleApplication_CL' (Preview)

Take action on 'SampleApplication_CL' (Preview)

Create Service Desk Ticket on 'SampleApplication_CL'

11 Create searchable fields **by highlighting and extracting the words or strings of interest** in the raw data field. Make sure to:

Select field type of **Text** for **TRANSACTION**



MAIN EXAMPLE

SampleApplication_CL

FILTER	FIELD NAME		VALUE
☐	SourceSystem	:	OpsManager
☐	ManagementGroupName	:	AOI-c56eff19-322d-4e4d-b9da-9f01cf656f04
☐	TimeGenerated	:	2017-01-11T18:56:24Z
☐	RawData	:	2017-01-11 07:55:10|Transaction:TRANX001|Type:TransactionTypeA|Description:TRANX001 is ?. |Metric:Avg. Resp. Time [ms]|ResponseTime:13.45?
☐	Computer	:	DESKTOP-EJI00M6

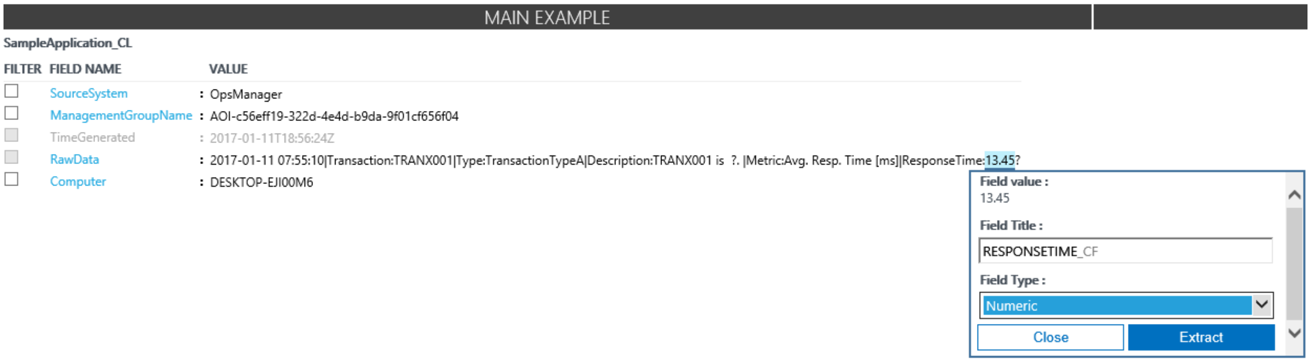
Field value : TRANX001

Field Title : TRANSACTION_CF

Field Type : Text

On the right site the result will appear. Click **Save Extraction** to confirm.

Select field type of **Numeric** for **RESPONSETIME**



MAIN EXAMPLE

SampleApplication_CL

FILTER	FIELD NAME		VALUE
☐	SourceSystem	:	OpsManager
☐	ManagementGroupName	:	AOI-c56eff19-322d-4e4d-b9da-9f01cf656f04
☐	TimeGenerated	:	2017-01-11T18:56:24Z
☐	RawData	:	2017-01-11 07:55:10|Transaction:TRANX001|Type:TransactionTypeA|Description:TRANX001 is ?. |Metric:Avg. Resp. Time [ms]|ResponseTime:13.45?
☐	Computer	:	DESKTOP-EJI00M6

Field value : 13.45

Field Title : RESPONSETIME_CF

Field Type : Numeric

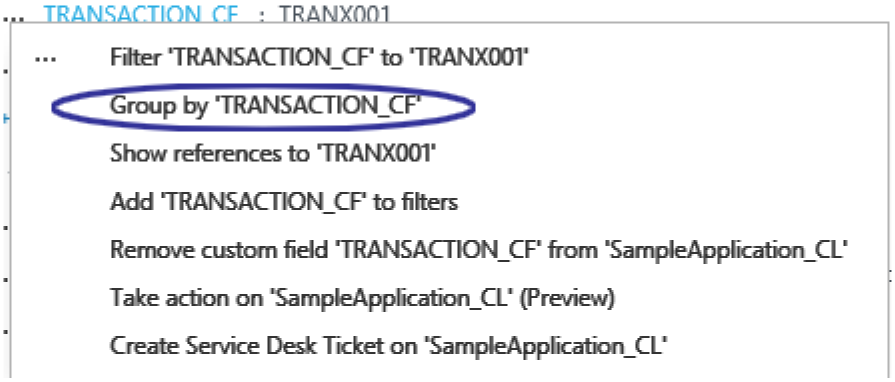
On the right site the result will appear. Click **Save Extraction** to confirm.

12 Right-click **Customlog-Transactions** and click **Run with PowerShell** for the 3rd time.

> 📌 Custom fields will only show up on data that comes into OMS after you configure them to be extracted. It does not retroactively extract custom fields hence we run the script again.

13 Wait a few minutes and validate the fields are visible and searchable in OMS Log Analytics by running a search query of **Type=SampleApplication_CL**

14 Use the context menu option **…** and select **Group by TRANSACTION_CF** to see all the transaction types in a glance.


... TRANSACTION_CF : TRANX001
...
Filter 'TRANSACTION_CF' to 'TRANX001'
Group by 'TRANSACTION_CF'
Show references to 'TRANX001'
Add 'TRANSACTION_CF' to filters
Remove custom field 'TRANSACTION_CF' from 'SampleApplication_CL'
Take action on 'SampleApplication_CL' (Preview)
Create Service Desk Ticket on 'SampleApplication_CL'

15 With the **Custom Logs** and **Custom Fields** features configured, and data being collected successfully from the text file every time new data is written to it, the records can be visualized and analyzed using search queries in the OMS Log Analytics workspace portal. **Here are some examples:**

a. A query to display the maximum response time recorded (in ms) for each transaction over time on a performance view on an hourly interval: **Type=SampleApplication_CL | measure max(RESPONSETIME_CF) by TRANSACTION_CF interval 1HOUR**

b. A query to compare the average response time recorded (in ms) for each transaction in sortable order within a specific time period: **Type=SampleApplication_CL | measure avg(RESPONSETIME_CF) by TRANSACTION_CF**

c. Type=SampleApplication_CL RESPONSETIME_CF > 30 | measure count() by TRANSACTION_CF

Provide Feedback to Microsoft

In this task, you will use the Feedback button to vote on existing suggestions and provide new ones.

1. In the OMS Portal, on top of the page, click the smiley face ☺

2. Click **See more ideas in the forum**.

   - Microsoft provides transparency to existing suggestions, allows you to vote on them, and keeps you informed on the current status of the suggestion.

Get Documentation and Support

In this task, you will learn how to obtain support and documentation on OMS.

1. In the OMS Portal, on top of the page, click the question mark (?).

Exercise 2: Introduction to Solutions

Solutions are a collection of logic, visualization, and data acquisition rules that can help you investigate and resolve issues, collect data, and be proactive with important planning and security activities.

In this exercise, you will learn how Microsoft Operations Management Suite uses Solutions to deliver insights into your log data by providing a cost-effective, all-in-one cloud management solution so you can better protect guest workloads in Azure, AWS, Windows Server, Linux, VMWare, and Open Stack.

- The amount of time it takes to populate data to a solution tile varies based on the specific solution. For example, an initial AD Assessment can take up to 4 hours before the OMS dashboard is populated with data; thereafter, AD Assessment data is collected once per 7 days and updated to OMS.

- The purpose of this exercise is to familiarize you with the types of solutions available and how to add them to your environment. Analysis of available data will be accomplished in later exercises after it has begun to populate; however, you will likely not see data in all the solutions reviewed.

Add Microsoft Operations Management Suite Solutions to the OMS Console

In this task, you will add several solutions to your OMS dashboard that can assist you in gaining deeper insight into your environment.

1. In OMS, click the **Overview (Home) icon**.
2. Click the **Usage** tile. Review the type of data revealed in the tile.
3. Click the **Overview (Home) icon**.
4. Click the **Solutions Gallery** tile.
5. Click **Agent Health** and read the description.

   - The Agent Health solution visualizes your agent heartbeat events and agent distribution statistics across your environment.

6. Click **Add**.
7. Click the **Agent Health** tile.

   - There may not yet be data populating the solution; therefore, the tile may not open immediately. If that is the case, skip to next step.

8. Click the **Overview (Home) icon**.
9. Click the **Solutions Gallery** tile.
10. Click **AD Assessment** and read the description.
11. Click **Add**.

    - The AD Assessment Solution now appears on the dashboard. The tile displays a basic count of security and health issues. You can open the solution to gain deeper insight.

12. Click the **AD Assessment** tile.

    - There may not yet be data populating the solution; therefore, the tile may not open immediately. If that is the case, skip to next step.

    - The solution is divided into Five focus areas with prioritized recommendations: Security and Compliance; Availability and Business Continuity; Performance and Scalability; Upgrade, Migration and Deployment; and Operations and Monitoring. It can take up to 4 hours for recommendations to appear.

    - The recommendations in the AD Assessment Solution are based on the knowledge and experience of Active Directory engineers across thousands of customer engagements. Recommendations are prioritized and include suggested actions with step-by-step instructions for remediating issues. They also provide context and guidance to help you understand why an issue is important to your datacenter.

13. Click the **Overview (Home) icon**.
14. Click **Solutions Gallery**.
15. Click **SQL Assessment** and read the description.

    - The SQL Assessment Solution regularly assesses the risk and health of your SQL Server environments and offers prioritized recommendations based on insights gained from customer interactions. These recommendations are tailored to your deployments and categorized according to different focus areas so that you can quickly take action to decrease risk and improve health. Focus areas include: Security and Compliance; Availability and Business Continuity; Performance and Scalability; Upgrade, Migration and Deployment; Operations and Monitoring; and Change and Configuration Management. It can take several hours for data to appear.

16. Click **Add**.

    - The SQL Assessment tile is now added to the dashboard.

17. Click the **SQL Assessment** tile.

    ⚠ There may not yet be data populating the solution; therefore, the tile may not open immediately. If that is the case, skip to next step.

18. Click the **Overview (Home) icon**.
19. Click the **Solutions Gallery** tile.
20. Click **Security and Audit** and read the description.
21. Click **Add**.
22. Add Solutions **Office365 Analytics** and **Network Performance in** the same manner.

    📌 The Security and Audit Solution helps you explore security-related data and perform forensic, audit, and breach analysis. With built-in search queries for notable security issues, you can focus on those issues that require immediate attention. You can see both a Security Posture view and a Context view for a more holistic understanding of our IT environment.

    📌 For data to populate to this solution, there are policy changes that must be configured at the machine level. The description for this Solution provides links to articles that provide details regarding how to configure these policies: Audit Policy settings and AppLocker Policy for Audit Only.

23. Click the **Security and Audit** tile.

    ⚠ There may not yet be data populating the solution; therefore, the tile may not open immediately.

24. Click the **Solutions Gallery** tile.
25. Click **Update Management** and read the description.

    📌 This Solution helps you identify missing system updates across all of your servers whether they are running in your data center or in a public cloud. Systems that are missing security updates can become targets of intrusions in your network and data. With simple, out-of-the-box dashboards you can quickly assess which servers need your immediate attention.

26. Click **Add**.
27. Click the **Update Management** tile.

    ⚠ There may not yet be data populating the solution; therefore, the tile may not open immediately. If that is the case, skip to next step.

28. Click the **Overview (Home)** icon.
29. Click the **Overview (Home)** icon.
30. Click the **Solutions Gallery** tile.
31. Click **Wire Data 2.0** and read the description.

📌 This solution helps you perform an analysis of your network traffic. Wire data is a rich data source that shows what is happening within an IT environment. Combined with machine-generated data, such as logs, wire data provides another dimension to gain operation insights.

32. Click **Add**.
33. Click the **Wire Data 2.0** tile.

⚠ There may not yet be data populating the solution; therefore, the tile may not open immediately. If that is the case, skip to step 41.

34. Click the **Overview (Home)** icon.
35. Click the **Solutions Gallery** tile.
36. Click **Capacity and Performance** and read the description.

📌 This solution helps you optimize virtual machine placement investigates "what if" scenarios, pinpoint capacity shortages, identify stale and over-allocated VMs and allows you to plan CPU, memory, network, and storage needs for your Hyper-V infrastructure.

37. Click **Add**.
38. Click the **Capacity and Performance** tile**.**
39. Click the **Overview (Home)** icon.
40. Click the large **Security & Compliance** tile on the left.
41. Click **Add.**

📌 This solution provides information regarding detected threats and reports on the protection status of reporting servers.

42. Click the **Update Management** tile.

This solution provides one stop visualization for Windows and Linux patch status

43. Click **Add.**
44. Click the **Overview (Home)** icon.
45. Click the **Change Tracking** tile**.**
46. Click **Add.**

Activity 3: Performing Insight & Analytics with OMS

- Before starting this activity, ensure that Activity #1 of this lab has been successfully completed.

Estimated time to complete this activity

45 minutes

Objectives

In Exercise 1, you will learn how to use the search feature of OMS to perform powerful queries against data being collected by OMS in support of your log analytic efforts for several different OMS Solutions.

In Exercise 2, you will use OMS Search in conjunction with the Security and Audit Solution.

Exercise 1: Using OMS Search

In this exercise, you will explore OMS Search capabilities and be introduced to the query syntax.

Perform Tasks to Generate Data to OMS

OMS will only collect log data from machines for activities that occur AFTER the client connection has been established.

In this task, you will perform activities to generate data to OMS. Each action in this task will result in data that will be analyzed in Activity #3 of this lab.

Begin this task logged on to **spfarm-ad** as **Contoso\AdAdministrator** with the password **Passw0rd2017!**

a. On the “Search Resources” line at the top type in **spfarm-ad** and press Enter.
b. In your list of VMs, select the one that you want to use.
c. Click on **Connect**.
d. Open the RDP program at the bottom of your screen to RDP to the virtual machine.
e. Click **Connect**
f. Click on **More Choices**
g. Select “**Use a Different Account**” option
h. Use “\AdAdministrator” (with a back slash) as user and provide the password (**Passw0rd2017!**)
i. Click on **Yes**
j. The initial login may take several minutes. Wait until you see the Server Manager desktop.
k. Close the “Server Manager”.

1. Copy the script **AddADUsers** to a convenient location on **spfarm-ad** VM.
2. Right-click **AddADUsers** and click **Run with PowerShell.**

   This script will add multiple accounts to Active Directory.

3. Open **Server Manager**.
    - a Click on **Manage** and choose **Add roles and features**
    - b Click through the wizard until **Features**
    - c Go to **Remote Server Administration Tools** and expand it
    - d Select **AD DS and AD LDS Tools**
    - e Select **AD DS Tools** and AD **LDS Snap ins**
    - f Click **Next**
    - g Click **Install**
    - h When installation completed click **Close**
4. On the **Tools** menu of the Server Manager, click **Active Directory Users and Computers**.
5. Expand **Contoso.com** and click **Users**.

    📌 The script will create new accounts in Active Directory.

6. In the **Users** container, locate the **Guest** account which is disabled by default.
7. Right-click **Guest** and click **Enable Account**.
8. Click **OK**.
9. Close “Active Directory Users and Computers”.
10. Click **Start**, click **Administrator** and click **Sign out**.
11. In the Azure menu, click **Virtual Machines**
12. Select the virtual machine from the list.
13. On the blade for the virtual machine, **click Connect**
14. Clicking **Connect** creates and downloads a Remote Desktop Protocol file (.rdp file). Click **Open** to use this file and connect to the machine.
15. **Log** on as **Contoso\Peggy** using password: **Passw0rd2017!**
16. Start Internet Explorer on the spfarm-ad VM, download and install Excel Viewer. (https://www.microsoft.com/download/details.aspx?id=10)
17. Follow the prompts to install the viewer.
18. Open **Server Manager**.
19. On the **Tools** menu, click **Active Directory Users and Computers**.
20. Navigate to **Users**, right-click **Guest** and click **Add to a group…** .
21. Type **Domain Admins** and click **OK**.
22. Click **OK**.

    📌 Peggy is a Domain administrator who is performing actions not in line with security best practices. She has given the Guest account credentials to a 3rd-party vendor who is performing work for Contoso. The

    Vendor was having lunch with colleagues and was overheard to say that he was using the Contoso Guest account for his work and that he had administrative rights in the domain.

23. Click **Start**, click **Administrative Tools**, and double-click **Services**.

24. Right-click **File Replication** and click **Properties**.
25. Change Startup type to **Automatic** and click **OK**.
26. Click **Start**, click **Peggy** and click **Sign out**.
27. Attempt to sign on multiple times as **Contoso\Guest**, using the wrong password.

📌 A “bad guy” overheard Peggy at lunch and is attempting to hack the Guest account to gain access to the domain.

Customize the OMS Dashboard

In this task, you will customize the OMS My Dashboard tile.

1. In the OMS Portal, click on the **Overview (Home)** icon.
2. Click the **My Dashboard** tile.
3. Click **CUSTOMIZE**.

📌 By customizing your dashboard, you can quickly visualize the data sets that are most important to you and gain valuable insight into your datacenter.

4. From the menu on the right, under “Change Tracking”, select **All Configuration Changes** and drag it onto **My Dashboard**.
5. Under System Update Assessment, select **Missing Critical Security Updates** and drag it onto **My Dashboard**.
6. Drag several additional items to **My Dashboard**.
7. On My Dashboard, click **All Configuration Changes**.
8. Under TILE VISUALIZATION, click **123**.

📌 You can control the visualization of each tile and set custom thresholds. You can drill into any tile to gain more insight into your data.

9. Under THRESHOLD, click **on**.
10. In value, type **2**.
11. Click **Add**.

Examine OMS Search Capabilities and Syntax

In this task, you will explore the basics of the OMS Log Search feature.

- Log Analytics Search is **Case Sensitive**

1. On the OMS Overview blade, click **Log Search**.
2. In the query field, type ***** and press enter.
3. Click the down arrow next to **Data based on last x days**.

   - Note that you can scope searches by 6 hours, 1 day, 7 days or CUSTOM. The choices are driven by the specific OMS subscription being used.

4. Click **OK**.

   - This page will display all existing saved searches, including those provided automatically by OMS and those saved by you. From here you can click on any saved search to execute it.

5. Click on the Log Analytics search bar.

   - Note that the actual query syntax for each saved search is displayed.
   - The first part of a search query (before any “|” vertical pipe character, is always a *filter*. This is like a WHERE clause in TSQL – it determines what subset of data to pull from the OMS data store. The most basic kinds of filters you can use are *keywords*, such as ‘error’ or ‘timeout’, or a computer name.

     Additional filters can be added using OR, AND, and Boolean operators.

   - The portion of the query to the right of the “|” vertical pipe character is the query to be performed. For a walkthrough of the Search syntax, see https://azure.microsoft.com/enus/documentation/articles/operational-insights-search.

Examine Malware-Related Data

In this task, you will use OMS Search to drill down into data produced by the Alert Management Solution.

1. Open a browser on a machine that is monitored by your workspace (your local machine or any on the created VMs) and browse to: http://www.eicar.org/download/eicar.com. If this does not work, go to this URL and download one of the files: http://www.eicar.org/85-0-Download.html

   - Depending on security settings of your device the eicar executable will be detected and reported as a threat.

2. Click the **Overview (Home)** icon on the OMS workspace.
3. Click the **Antimalware Assessment** tile.

   - It might take several hours before data is populated for the first time.

4. Under PROTECTION STATUS, click **No Real Time Protection (Not Reporting?)**.

5. In the Query field, position the cursor to the right of **Measure**.

   📌 Note the associated query is displayed. Measure is one of the most versatile commands in OMS. It allows you to apply statistical functions to your data and aggregate results grouped by a given field.

   There are multiple statistical functions that Measure supports.

6. Position the cursor at various places in the query string.

   📌 Note the suggestions that provide additional strings available to add to the preceding portion of the query. This greatly assists in learning the query language. In addition, a history of the most recent queries is displayed. Clicking on an item under HISTORY reruns the query.

7. In the “Facet Panel” om the left, under Type, click **Protection Status**.
8. Click “Protection Status”.
9. In the list that opens, click the … before Computer and select **Group by Computer**.
10. On the left click on spfarm-ad.contoso.com and click the **List** icon that appears.
11. Click **Filter ‘DeviceName’ to ‘spfarm-ad.contoso.com’**.
12. At the bottom of the Facet Panel, click **+Add**.
13. Scroll to locate the ProtectionStatus fields and click the checkbox next to **Management Group Name**.

    📌 On the Facet Panel, note that ManagementGroupName has been added as a facet.

14. Edit the query to delete “DeviceName=’Spfarm-ad.contoso.com’ and click the **Search** icon.
15. Click **Save**.
16. In the name field, type **Protection Status by Device**.
17. In the Category field, type **Security and Audit**.
18. Click **Save**.
19. In the top bar, click **Favorites** and note that the Saved Searches displays on the right side of the blade.
20. In the Saved Searches query box, type **Protection Sta**.

    📌 Notice your saved search appears in the results.

21. Click the **Overview (Home)** icon.
22. Click the **My Dashboard** tile.
23. Click **Customize**.
24. Click the Find search box and type **Protect, hit enter**.
25. Click and drag the **Protection Status by Device** saved search to My Dashboard.
26. Click **Customize**.

Examine Data Related to Software and Service Changes

In this task, you will use OMS Search to drill down into data produced by the Change Tracking solution.

1. Click the **Overview** icon.
2. Click the **Change Tracking** tile.

   📌 Note that there is a software change for SPFARM-AD, which is unexpected in your production environment.

3. Under SOFTWARE CHANGES, click **spfarm-ad.contoso.com**.

   📌 The SOFTWARENAME column of the results indicates that Microsoft Office Excel Viewer has been installed on the domain controller, which is a violation of your corporate policy. Knowing this will allow you to remove the application from the domain controller, and take steps to ensure that the policy is known by all administrators. In addition, you might elect to initiate a technical solution such as AppLocker to ensure compliance.

4. Click the back arrow in your browser window to return to the Change Tracking solution.
5. Under WINDOWS SERVICE CHANGES, click **spfarm-ad.contoso.com**.
6. Click the SVCDISPLAYNAME column header to sort the field.

   📌 Note the records that reflect the change you made to the File Replication Service Startup property.

Examine Performance Data in OMS

In this task, you will investigate the types of data OS captures from Performance Counters.

1. In the OMS Portal, click the **Overview (Home)** icon.
2. Click the **Log Search** tile.
3. In the query field, type ***** and click **Search**.

   📌 The number of associated logs and number of metrics are presented.

4. In the Facet Panel on the left, under Type, click **Perf** and hit **Apply**

   📌 This will filter the search to only performance-related data.

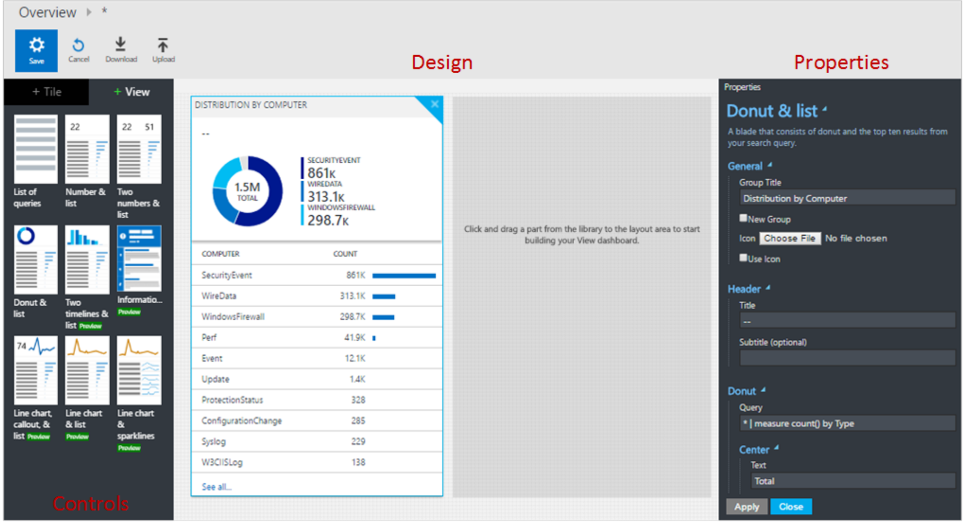
5. At the top of the Results Panel, click **Metrics xx** (where xx is the number of metrics available).
6. To the right of the graph for each solution, click on the [+] plus sign to expand the graph.
7. Drill down through the various items to see how they are displayed.
8. In the query pane **Type=Perf.**
9. **More Examples:**

Query	Description
Type=Perf ObjectName=Processor CounterName="% Processor Time" CounterValue>90	alert when the processor runs over 90% for 30 minutes
Type=Perf ObjectName=LogicalDisk CounterName="Current Disk Queue Length" Computer="MyComputerName" | measure Avg(Average) by InstanceName	Average Current Disk Queue length across all the instances of a given computer
Type=Perf ObjectName=Memory (CounterName="Available MBytes") | measure avg(CounterValue) by Computer Interval 1HOUR	Memory usage the last 7 days divided into hourly intervals

Create a customized View

In this task, you will create a customized view. The View Designer allows you to create custom views in the OMS console that contain different visualizations of data in the OMS repository.

1. In the OMS Portal, click the **View Designer** tile or the **green colored (+)** under the Home icon.



DISTRIBUTION BY COMPUTER

--

COMPUTER	COUNT
SecurityEvent	861K
WireData	313.1K
WindowsFirewall	298.7K
Perf	41.9K
Event	12.1K
Update	1.4K
ProtectionStatus	328
ConfigurationChange	285
Syslog	229
W3CIISLog	138

Click and drag a part from the library to the layout area to start building your View dashboard.

Properties

Donut & list

A blade that consists of donut and the top ten results from your search query.

General

Group Title: Distribution by Computer

□ New Group

Icon: Choose File No file chosen

□ Use Icon

Header

Title: --

Subtitle (optional):

Donut

Query: * | measure count() by Type

Center

Text: Total

2. Select the **+Tile tab** in the Control pane to select **Donut & List**.
3. Enter the title, description, and search query in the specified Properties fields on the right side of the page
4. The query specified in the Query field will determine the data presented in the tile. In this case, we are using:

   *** | measure count() by Computer**

5. Click on **"Apply"**
6. **Save** your changes.

Import customized Views

You can import an omsview file that you exported from another management group. In this exercise, you will import an existing view, by clicking the Import button and select the omsview file.

1. In the OMS Portal, click the **View Designer** tile or the **green colored (+)** under the Home icon.
2. In the upper left overview pane, click the **Import** button.
3. In the upload from computer, browse to **dashboards\ Front End Services.omsview**
7. Leave default title, description, and search query in the specified Properties fields on the right side of the page, click **Save and then close**.
8. Note in the main OMS screen you will have a new **Front End Services Tile.**

Examine Events in OMS

In this task, you will investigate the types Events and query for a specific type.

1. In the OMS Portal, click the **Overview (Home)** icon.
2. Click the **Log Search** tile.
3. In the query field, type * and hit <enter>.

   The number of associated logs and number of metrics are presented.

4. In the “Facet Panel” on the left, under “Type”, click “**+More**” and the select **Event** and click **Apply**.

   This will filter the search to only Event related data.

   Notice that the query now shows “ * | (Type=Event) “

5. For example, Unexplained reboots cause an event with a source from USER32 and eventID 1074. You can find these by using a query like:

Query	Description
Type=Event EventID=1074	Unexplained reboots
Type=Event EventLog=System Source=User32	Unexplained reboots

6. Other Event Queries:

Query	Description
Type=Event	All Windows events.
Type=Event EventLevelName=error	All Windows events with severity of error.
Type=Event | measure count() by Source	Count of Windows events by source.

Query	Description
Type=Event EventLevelName=error | measure count() by Source	Count of Windows error events by source.

Examine SysLog Events in OMS

In this task, you will investigate the Linux Events and query for a specific type.

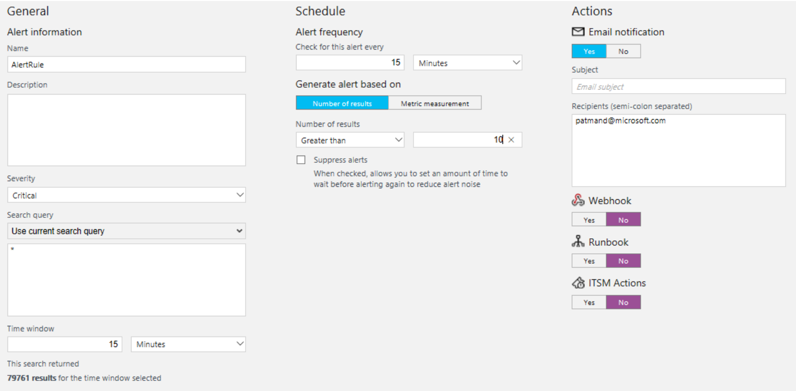
1. In the OMS Portal, click the **Overview (Home)** icon.
2. Click the **Log Search** tile.
3. In the query field type the query **Type=Syslog**.
4. Other examples:

Query	Description
Type=Syslog SeverityLevel=error	All Syslog records with severity of error.
Type=Syslog | measure count() by Computer	Count of Syslog records by computer.
Type=Syslog | measure count() by Facility	Count of Syslog records by facility.

Create an Alert Rule

In this task, you will create an alert rule. You start by creating a log search for the records that should invoke the alert. The Alert button will then be available, so you can create and configure the alert rule.

1. From the OMS Overview (Home) page, click **Log Search** tile.
2. Either create a new log **search query** or select a saved log search.
3. Click **Alert** at the top of the page to open the Add Alert Rule screen.
4. Configure the desired settings



General

Alert information

Name: AlertRule

Description:

Severity: Critical

Search query: Use current search query

*

Time window: 15 Minutes

This search returned

79761 results for the time window selected

Schedule

Alert frequency

Check for this alert every: 15 Minutes

Generate alert based on: [✓ Number of results] Metric measurement

Number of results: Greater than 10

□ Suppress alerts

When checked, allows you to set an amount of time to wait before alerting again to reduce alert noise

Actions

Email notification: [✓ Yes] No

Subject: Email subject

Recipients (semi-colon separated): patmand@microsoft.com

Webhook: Yes [✓ No]

Runbook: Yes [✓ No]

ITSM Actions: Yes [✓ No]

5. When you provide the time window for the alert rule, the number of existing records that match the search criteria for that time window will be displayed. This can help you determine the frequency that will give you the number of results that you expect.
6. Click **Save** to complete the alert rule. It will start running immediately.
7. To see all Alert, go to “Settings” tile and click “Alerts”.

Create an Alert Rule Service Stop and Trigger Runbook

TBD

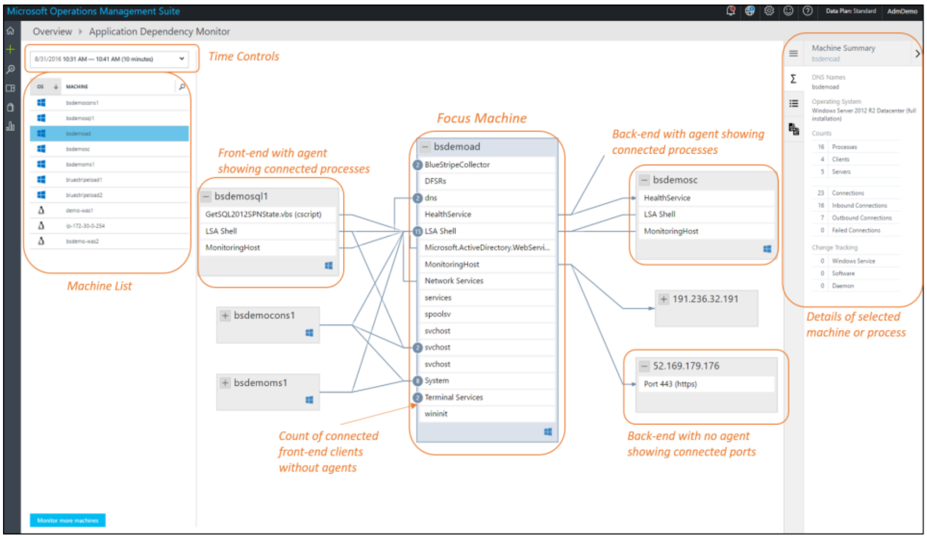
Exercise 2: Exploring Service Map

In this task, you will install and configure the Service Map solution. Service Map automatically discovers application components on Windows and Linux systems and maps the communication between services.

1. On the taskbar, click **Internet Explorer** and open the Microsoft Operations Management Suite workspace.

📌 The home page is http://mms.microsoft.com

2. On the Overview (Home) blade, Open the **Solutions Gallery**.
3. You will see the **Service Map** solution available, Click the tile and click **Add.**
4. Click on the Overview (Home) icon
5. In the overview blade click on the **Service Map** tile. This may take a while to appear. Refresh the browser as required.
6. On the bottom, left click the button **Monitor more machines**.
7. Download the windows agent and run it on the 3 Windows SharePoint VMs.
8. Follow the wizard to **install the agent**. Once the agent is installed on a server reporting to OMS, dependency maps will appear within 10 minutes.
9. To validate that the data is being collected successfully and searchable in OMS Log Analytics type the query **Type=ServiceMapComputer_CL.**
10. On the Overview blade, click **Service Map**.
11. Select **SPContoso-sp.** You will see it's dependency map.
12. Machines can be expanded in the map to show the running processes with active network connections during the selected time range.



Time Controls

Machine List

Front-end with agent showing connected processes

Focus Machine

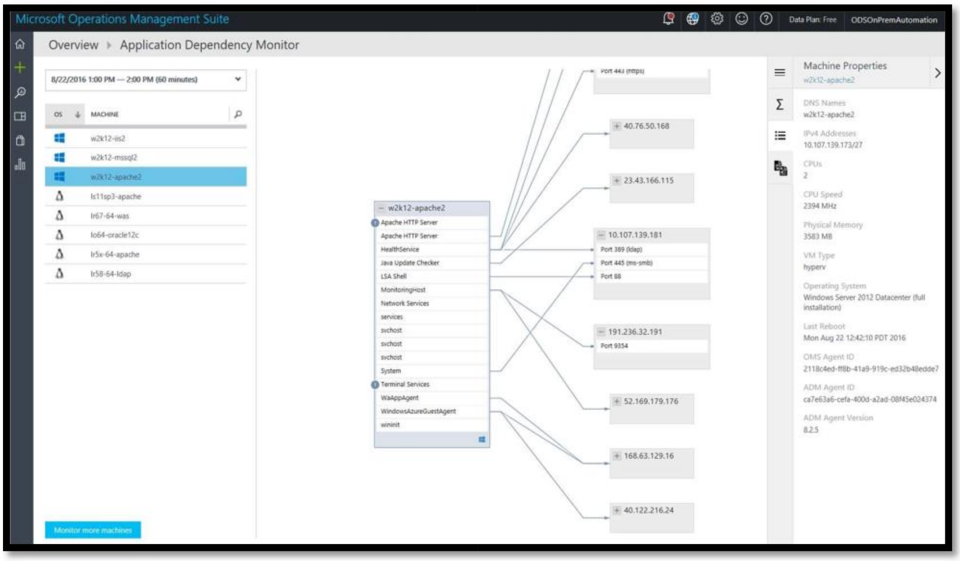
Back-end with agent showing connected processes

Count of connected front-end clients without agents

Back-end with no agent showing connected ports

Details of selected machine or process

13. By default, Service Map maps show the last 10 minutes of dependency information. Using the time controls in the upper left, maps can be queried for historical time ranges, up to one-hour wide, to show how dependencies looked in the past, e.g. during an incident or before a change occurred.



8/22/2016 1:00 PM — 2:00 PM (60 minutes)

Machine Properties
w2k12-apache2

DNS Names
w2k12-apache2

IPv4 Addresses
10.107.139.173/27

CPUs
2

CPU Speed
2394 MHz

Physical Memory
3583 MB

VM Type
hyperv

Operating System
Windows Server 2012 Datacenter (full installation)

Last Reboot
Mon Aug 22 12:42:10 PDT 2016

OMS Agent ID
2118c4ed-ff8b-41a9-919c-ed32b48edde7

ADM Agent ID
ca7e63a6-cefa-400d-a2ad-08f45e024374

ADM Agent Version
8.2.5

Exercise 3: Using the Security and Audit Solution in OMS

In this exercise, you will explore the Security and Audit Solution in OMS.

Explore Security and Audit Solution Data

In this task, you will explore common queries available through the Security and Audit solution.

.

1. In the OMS Portal, click the **Overview** icon.
2. Click the **Security and Audit** tile.
3. Scroll to the right. Under COMMON SECURITY QUERIES, click **Logon Activity by Computer**.
4. In the Facet Panel, locate the "Account" facet and note the number of accounts that have logon activity. To display the entire list, click **"+More"** at the bottom of the facet.
5. In the Account facet, click on **CONTOSO\Peggy**. The click on "**Apply**"
6. Scroll down to locate the **LogonTypeName** facet.

   📌 In the lab environment, you may only see "RemoteInteractive" and "Network" logons listed.

7. In the results pane, click **Spfarm-ad.contoso.com**.

   📌 Each individual logon activity is enumerated with its details.

8. To display the entire list of details for an event, click **[+}show more**. Scroll through the data to become familiar with the type of data provided.

   📌 In particular, note the Event ID and Event Data, TargetUserName, Process ID, etc.

9. Click the back arrow in Internet Explorer to return to the "Security and Audit" solution.
10. On the OMS "Security and Audit Solution" blade, under NOTABLE ISSUES, click "**Accounts Failed to logon**"
11. In the detail pane of Search results, click **Contoso\Guest.**

    📌 Note that an event has been recorded for each time you failed to log on to the Guest account.

    📌 The pattern of failed interactive logon attempts on SPFARM-AD (4625 – An account failed to logon) indicates that an unauthorized attempt may have been made to access the account.

12. Click **Save**.
13. In the Name field, type **Failed Logon Attempts by Guest on SPFARM-AD**.
14. In the Category field, type **MySearches**.
15. Click **Save**.
16. To export search results, at the top of the Search page, click **Export**.
17. **Save** the .csv file to the desktop as **SearchResults**.
18. On the desktop, right-click **SearchResults** and click **Open with**.

19. Select **WordPad**.

    ⟐ If you would like to see a more graphic display of the results, download and install the Excel Viewer.

20. Review the contents and close WordPad.
21. Return to the OMS Portal, click on the “Log Search” blade.
22. In the query field, edit the query to read **Type=SecurityEvent EventID=4769** and click the **Search** icon.

    📌 You can create and save searches for specific Event IDs and add the saved searches to My Dashboard. In this way, you can easily track ongoing issues you are monitoring. A spreadsheet detailing the security audit events for Windows 8 and Windows Server 2012 can be downloaded from https://www.microsoft.com/en-us/download/details.aspx?ID=35753.

23. Click on the Overview (Home) and then click the **Security and Audit** tile.
24. Under SECURITY DOMAINS click **“Identity Access”.**
25. Click the back arrow on the browser to return to the “Security and Audit” solution.
26. Under SECURITY DOMAINS, note the “**Network Security**” tile.

    📌 OMS provides you a centralized view showing all the known malicious IP’s your managed server/client may be communicating with. Working with the Microsoft trustworthy computing team (TwC), the same group responsible for securing the Microsoft Azure data centers. OMS is able to get hourly updates on the latest known malicious IP’s and inform you if any of your servers may be compromised. The TwC team works with various 3rd party threat intelligence partners to gather and provide this consolidated list to OMS.

27. Click the back arrow on the browser to return to the “Security and Audit” solution.
28. Under NOTABLE ISSUES, click **Computers missing security updates.**

    📌 In the lab environment, you may not see any missing updates listed; however, it should be noted that when a missing update is reported, the UpdateTitle asset in the Facet Panel will report the exact name of the missing update.

29. Click the back arrow in Internet Explorer to return to the “Security and Audit” solution.

Use OMS Search to Investigate Suspicious Executables

In this task, you will use the Operational Insights Search capabilities in the OMS Portal to identify the path of a potential security attack.

.

1. In the “Security and Audit” solution, under NOTABLE ISSUES, click **Suspicious Executables**.

   - Search displays detailed information about the process, including the computers where the process ran, the user account that the process ran under, the date and time that an event was created for the process, and the name of the process. You can see that Peggy has executed a Command Prompt on the domain controller which would not be unusual for an administrator. However, the file has been reported as being suspicious because the file has been edited resulting in a change in the filehash,

   - Search displays detailed information about the process, including all the computers where the process ran, etc. In the lab environment, the executable was only run on a single machine.

   - Using the information that you find, you can take corrective action as needed. For example, if you determine that the executable is malware then you'll want to take action to remove it from all the computer systems that it affects. After the executable is removed and OMS receives updated log and audit events for your computer systems, values on the NOTABLE ISSUES blade will change on the following day.

2. Click the back button in the browser to return to the “Security and Audit” solution.
3. As time permits, continue to explore the various types of data provided.

Trigger Advanced Detection simulation

The advanced detection is analyzing many patterns that might indicate a threat. The full list of detections is not disclosed to protect our customers. If the full list is revealed, attackers would have easier time finding techniques to avoid it. In this task you will perform two examples for detections that are being evaluated. These examples could also be used by you to test OMS Security advance detections on your environment.

1. **RDP** to a machine that is monitored by your workspace.
2. Select an EXE file (for example the excel viewer) that is not part of the OS (not under c:\windows). Copy this file to a different folder (e.g. c:\temp)
3. Change the name of this file to “**something.pdf.exe**” and execute it.
4. Then, change the name of this file to “**svchost.exe”** and execute it.
5. If all goes well, in few minutes, you would have two detections on your dashboard.

Another detection that you can simulate is clearing the security event log. On these machines, you can clear the event log but take into account the following:

1. To avoid false-positives, detection is triggered only when there is more than one event like that.
2. If you clear the event log too frequently, OMS agent will not be able to pick up all these events. Wait 5-10 between these events.

Activity 4: Configuring Automation for OMS

Estimated time to complete this activity

75 minutes

Objectives

Runbooks are workflows that perform an administrative process. You do not have to create all runbooks from scratch. Workflows can be uploaded to Azure from the Azure Runbook Gallery, the Microsoft Script Center, Microsoft MSDN and TechNet libraries, and the Azure community forums. OMS solution leverages the runbook capabilities of Microsoft Azure.

After completing this activity, you will be able create and manage runbooks.

- Before starting this activity, ensure that Activity #1 of this lab has been successfully completed

Exercise 1: Introduction to OMS Runbooks

In this exercise, you will learn how to create and manage runbooks.

Configure Azure Automation Assets

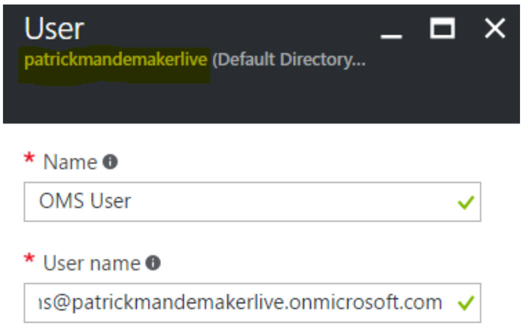
In this task, you will create a credential asset for use in the creation of runbooks.

Microsoft accounts cannot be used for automation to logon non-interactively, so we must use an organizational account. If you don't use a Microsoft Account, you can skip the "create a user" steps.

Create a new user

1. In the **Azure Portal** (http://portal.azure.com), in the "Search Resources" line at the top, search for **Azure Active Directory**
2. Under **Manage,** open **Users and Groups**
3. Again, under **Manage,** click **All Users**
4. Click the **+Add** button to create a new user

   In the new user blade **note the directory name**, this is displayed right under **User.**



User

patrickmandemakerlive (Default Directory...

* Name: OMS User

* User name: ıs@patrickmandemakerlive.onmicrosoft.com

Name=	**OMS User**
User name=	OMS@<directory name>.onmicrosoft.com
Directory role=	Change to **Global administrator**
Profile=	<default>
Properties=	<defaults>
Groups=	<defaults>

5. Click **Show Password** radio button and note the password.
6. Click on "**Create**"
7. Logout of the Azure Portal. Start Internet Explorer in "InPrivate Browsing Mode". Then login with the user created as OMS@<directory name>.onmicrosoft.com and the password. A change your password prompt will pop-up.
8. **Change the password,** log out and log back in with your normal Microsoft Account using the "Private Browsing Mode".

Assign Subscription Permissions to the Newly Created User

The newly created user OMS@<directory name>.onmicrosoft.com does not have permissions on the subscription or resources yet.

1. In Azure Portal (http://azure.microsoft.com) , on the bottom left click on "**More Services**" icon (›) and then select **Subscriptions**
2. Select the subscription you use and click **Access Control (IAM)**
3. Click "**+Add**", then click on the OMS@<directory name>.onmicrosoft.com user.
4. In the "Role" pull down list on the right, select "**Owner**"
5. Click on "**Save**"

Create the Automation Asset

1. In the Azure Portal (http://azure.microsoft.com), click on the "**Resource Groups**" icon ( ). Then click on "omslabs" resource group.
2. From the pull-down list, open **MyAutomation** account

   - This is the account you created in Activity #1.

3. Under **Resources**, click **Assets**.

   - Assets are used to build Runbooks.

4. On the "Assets" blade, click **Credentials**.
5. Click **+Add a credential**.
6. In the name field, type **DefaultAzureCredential**.

7. In the User name and password fields, type the user credentials you created earlier (OMS@<directory name>.onmicrosoft.com)
8. Close all blades and return to main screen.

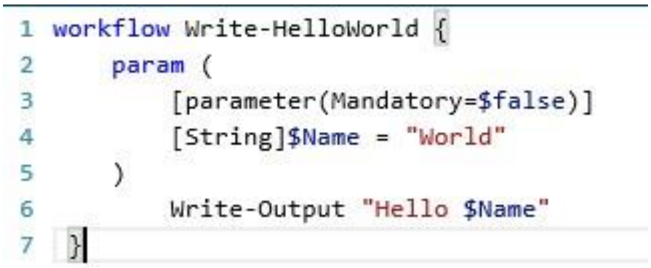
Exercise 2: Create/Edit/Run Workbooks

Create a Runbook from Scratch

In this task, you will create a runbook from scratch.

1. In the Azure Portal (http://azure.microsoft.com), click on the "**Resource Groups**" icon (). Then click on "omslabs" resource group.
2. Open **MyAutomation** account, then click on **Runbooks**
3. Click **Add a runbook**, and then click **Quick Create**
4. In the Azure Portal, in the Runbook blade, type **Write-HelloWorld** as the name.
5. From the Runbook type, drop-down menu, select **PowerShell Workflow**.
6. Ensure that the correct Automation account, subscription, and region are selected and click **Create**.

7. In the script area, edit the text to match the following:



```
workflow Write-HelloWorld {
    param (
        [parameter(Mandatory=$false)]
        [String]$Name = "World"
    )
        Write-Output "Hello $Name"
}
```

8. Click **Save**.

Test and Publish a Runbook

In this task, you will test and publish a runbook.

1. In the Edit blade for Write-HelloWorld, click **Test pane**.
2. Click **Start.**

📌 A runbook job is created and its status displayed in the pane. The job status will start as *Queued* indicating that it is waiting for a runbook worker in the cloud to come available. It will then move to *Starting* when a worker claims the job, and then *Running* when the runbook starts running.

3. When the runbook job completes, its output is displayed.

   📌 In this case, you should see *Hello World*.

4. Close the Test blade to return to the canvas.
5. Switch to the Edit blade in the Azure Portal.
6. Click **Publish** and click **Yes.**

📌 When you import or create a runbook, it is in in a draft state until you explicitly promote it to a published state. After being published, the runbook is eligible to be called by other runbooks. In your environment, a runbook should never be published until it is successfully tested.

If you scroll left to view the runbook in the **Runbooks** pane now, it will show an **Authoring Status** of *Published*.

Edit a Runbook

In this task, you will edit a runbook.

1. In the Write-HelloWorld blade, click **Edit**.
2. Change **$Name = “World”** to **$Name = “Everyone”**.
3. Click **Save**.
4. Click **Revert to published** and click **Yes**.
5. Click **Edit**.

   📌 **$Name = “Everyone”** is now **$Name = “World”**.

6. Close the Write-HelloWorld blade.

Start a Runbook

In this task, you will start a runbook manually and as a scheduled task.

1. In the Write-HelloWorld blade, click **Start**.
2. In the Start Runbook blade, click **OK**.

   📌 The options across the top allow you to start the runbook, schedule it to start at some time in the future, or create a webhook so it can be started through an HTTP call.

📌 A job pane is opened for the runbook job that you just created. You could close this pane, but in this case leave it open so you can watch the job's progress. The job status is shown in **Job Summary** and matches the statuses that you saw when you tested the runbook.

3. When the job completes, click **Output**.
4. The **Output** blade is opened, and after a while you can see *Hello World*.
5. Close the “Output” blade and the “Job” blade.
6. In the monitoring part, you will see the “Job Statistics”.

📌 In the MyAutomation blade you’ll see the “Jobs in the last 7 days” will have increased by 1.

7. Switch to the “Job” blade in the Microsoft Azure Portal.
8. Close the “Job” blade.
9. In the Write-HelloWorld blade, click **Schedule** (🕒 Schedule) (not “Schedules” !)
10. In the Schedule Runbook blade, click **Link a schedule to your runbook**.
11. Click **Create a new schedule**.
12. In Name, type **Daily**.
13. Change the time to **5** minutes from the current time.

📌 The start time must be at least 5 minutes after the time you create the schedule.

14. From the Recurrence drop-menu, select **Daily**.
15. Click **Create**.
16. In the Schedule Runbook blade, click **OK**.

📌 The runbook will launch according to the schedule. When the job completes, “Jobs in the last 7 days” will increase by 1.

17. Leave the Microsoft Azure portal window open for future tasks.

Delete a Runbook

In this task, you will delete a runbook.

1. In the Azure Portal (http://azure.microsoft.com), click on the “**Resource Groups**” icon ( ). Then click on “omslabs” resource group.
2. Open **MyAutomation** account
3. Click the **Runbooks** tile.
4. Select **Write-HelloWorld**.
5. In the Write-HelloWorld blade, click **Delete** and click **Yes**.

📌 The runbook is removed from the list of Runbooks.

6. Click **Home**.

   📌 The deleted runbook tile now displays “Error loading tile”.

7. Right-click the tile of the deleted runbook and click **Unpin from Startboard**.

   📌 In the MyAutomation blade, the number of runbooks is reduced by 1.

Import a Workflow to an OMS Runbook

In this task, you will import an existing Runbook from the Runbook Gallery.

1. In the Azure Portal (http://azure.microsoft.com), click on the “**Resource Groups**” icon (). Then click on “omslabs” resource group.
2. Open MyAutomation account.
3. Under **Process Automation**, open the **Runbook Gallery**
4. Search for some Runbooks.
5. More automation Runbooks are available on https://www.powershellgallery.com/profiles/AzureAutomationTeam/

   📌 Read the text under ATTENTION: “Each runbook is licensed to you under a license agreement by its owner, not Microsoft. Microsoft is not responsible for runbooks provided and licensed by the community members and does not screen for security, compatibility or performance. The runbooks are not supported under any Microsoft support program or service. The runbooks are provided AS IS without warranty of any kind.”

Exercise 3: (OPTIONAL) Start/Stop VMs after off-hours (OPTIONAL)

◇ Exercises marked as (OPTIONAL) mean they are not mandatory or related to the remaining of the labs. You can decide to return and perform them later.

In this exercise, you will schedule startup and shutdown of Azure virtual machines. You will implement granular power schedules for your virtual machines using simple tag metadata.

Import the Runbook

1. In the Azure Portal (http://azure.microsoft.com), click on the “**Resource Groups**” icon (). Then click on “omslabs” resource group.

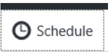
2. Open **MyAutomation** account which will contain the runbook
3. Click on **Runbooks** from the Resources section
4. Select **Browse gallery**
5. Search for **Shutdown**
6. Click the runbook named **Shutdown/Start VMs (ASM and ARM) by resource group**.
7. Click **Import,** then click **“Ok”.**
8. Click on **Edit** and then click on **Publish**. Click on **“Yes”** to publish the runbook.
9. Confirm the runbook now shows a status of **Published**

Now you can test the runbook by clicking run. In the Run Settings you can have to define the resource group (omslab) and shutdown true or false to start.

Create Variable for Subscription Name

1. In the Azure Portal (http://azure.microsoft.com), click on the “**Resource Groups**” icon (). Then click on “omslabs” resource group.
2. Open the **MyAutomation** Account which will contain the runbook
3. Open the **Assets** view from the Resources section
4. Open the **Variables** view.
5. Click **Add a variable** from the top menu
6. Give the variable the name **MySubscription**, and enter the **subscription name** (for example Azure Pass) as the variable’s value. Leave “Encrypted” as “No”. Click **Create.**

Schedule the runbook

1. Back in the runbooks list, open the new runbook **Shutdown-Start-VMs-By-Resource-Group**.
2. Click on **Schedule** () (not “Schedules” !)

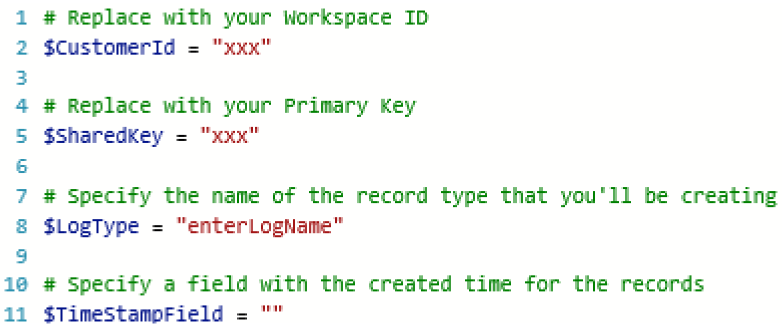
3. Under “Parameter and Run Settings” section, add the resource group **omslab** and the shutdown parameter true or false. Click “OK”.
4. Under **Link a schedule to your runbook** you can create a schedule
5. Click **Create a new schedule.**
6. Provide a name like **Shutdown Resource Group**.
7. Set the **start time** to time you want to first run to shut down the machines. For example, 8pm.
8. You can create a second schedule to start the VMs again in the morning.

Exercise 4: ADVANCED SCENARIOS

Send data to Log Analytics with the HTTP Data Collector API

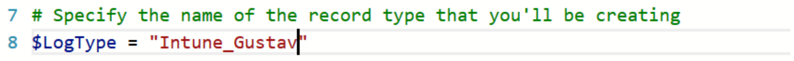
In this exercise, you will learn how to use the HTTP Data Collector API to send data to Log Analytics from a REST API client. It describes how to format data collected by your script or application, include it in a request, and have that request authorized by Log Analytics. When data is ingested into the Log Analytics API it needs to be in JSON format. The following example is an example where we ingest simulated JSON format that has Intune telemetry data in it.

1. Copy the script **Log Analytis-Api** to a convenient location on a machine where **Azure PowerShell Modules** are installed.
2. Right-click **Log Analytis-Api** and click **Edit.**
3. The header to validate your POST will be generated with your **Workspace ID** and your **Workspace Key,** referred to as $customerId and $sharedKey here. These can be found under **Settings > Connected Sources > Windows Servers.**



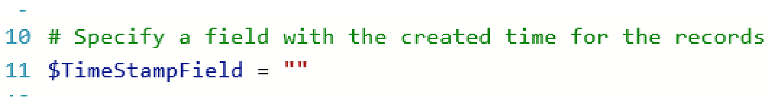
```
# Replace with your Workspace ID
$CustomerId = "xxx"

# Replace with your Primary Key
$SharedKey = "xxx"

# Specify the name of the record type that you'll be creating
$LogType = "enterLogName"

# Specify a field with the created time for the records
$TimeStampField = ""
```

4. Next, we need to give the data you're sending a **Custom Log Type,** just like the kind we create in **Custom Logs.** In the screendumps, you see Intune_Gustav. **Name it Intune_yourname.** The last part, _CL, is added by Log Analytics, so they system marks it as a custom log.



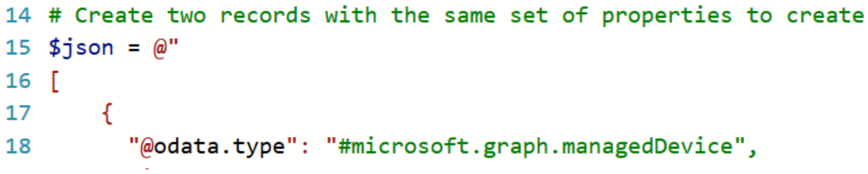
```
# Specify the name of the record type that you'll be creating
$LogType = "Intune_Gustav"
```

5. You can set your own **Timestamp** field with $TimeStampField. Whatever field you set to be your Timestamp field will permanently become the field that will replace TimeGenerated in your events. In this case, **we leave it blank,** so it defaults to the time this data is ingested.



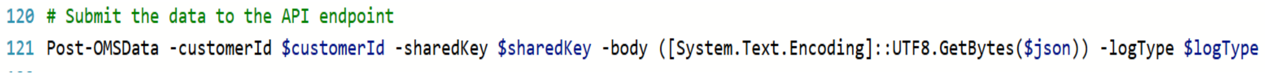
```
# Specify a field with the created time for the records
$TimeStampField = ""
```

6. To define the data, we created a **JSON Payload** using the "Using the Microsoft Graph APIs" from Intune. **Don't change** anything here.



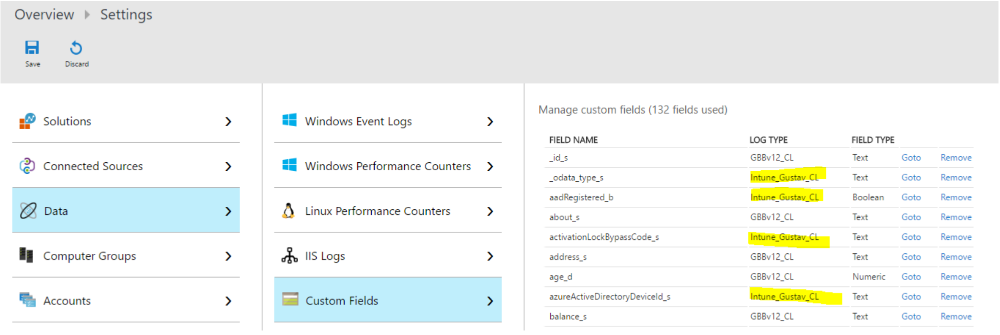
```
# Create two records with the same set of properties to create
$json = @"
[
    {
      "@odata.type": "#microsoft.graph.managedDevice",
```

7. Finally, we make the call to PostData with our **Workspace ID, Workspace Key, JSON Payload**, and the name of our **Custom Log Type.**



```
# Submit the data to the API endpoint
Post-OMSData -customerId $customerId -sharedKey $sharedKey -body ([System.Text.Encoding]::UTF8.GetBytes($json)) -logType $logType
```

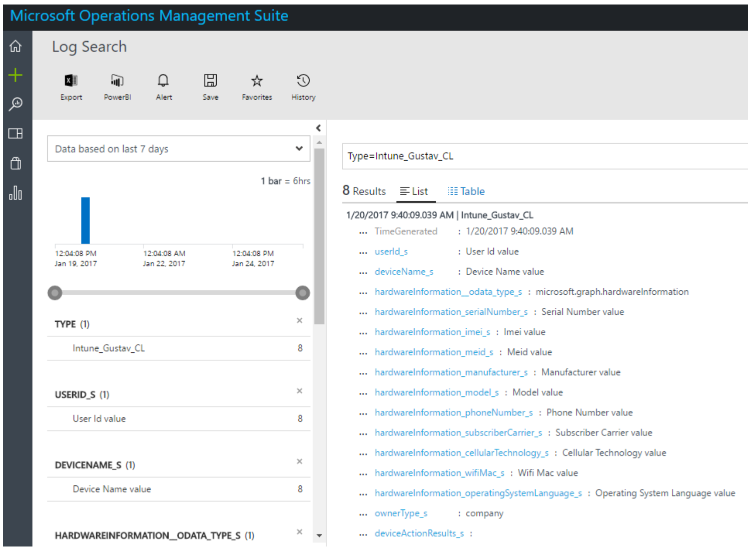
8. Right-click **Log Analytis-Api** and choose **Run with PowerShell.** The HTTP status code 200 means that the request has been received for processing by Log Analytics service. On https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-data-collector-api you will find a complete table with status codes.
9. When a request is successfully submitted, you will see it in the Custom Fields view in the OMS Portal via **Settings | Data | Custom Logs.**



Manage custom fields (132 fields used)

FIELD NAME	LOG TYPE	FIELD TYPE		
_id_s	GBBv12_CL	Text	Goto	Remove
_odata_type_s	Intune_Gustav_CL	Text	Goto	Remove
aadRegistered_b	Intune_Gustav_CL	Boolean	Goto	Remove
about_s	GBBv12_CL	Text	Goto	Remove
activationLockBypassCode_s	Intune_Gustav_CL	Text	Goto	Remove
address_s	GBBv12_CL	Text	Goto	Remove
age_d	GBBv12_CL	Numeric	Goto	Remove
azureActiveDirectoryDeviceId_s	Intune_Gustav_CL	Text	Goto	Remove
balance_s	GBBv12_CL	Text	Goto	Remove

10. You can now perform a search for **Type=Intune_yourname_CL.**



TYPE (1)	
Intune_Gustav_CL	8
USERID_S (1)	
User Id value	8
DEVICENAME_S (1)	
Device Name value	8
HARDWAREINFORMATION__ODATA_TYPE_S (1)	

Type=Intune_Gustav_CL

8 Results

```
1/20/2017 9:40:09.039 AM | Intune_Gustav_CL
  ... TimeGenerated        : 1/20/2017 9:40:09.039 AM
  ... userId_s             : User Id value
  ... deviceName_s         : Device Name value
  ... hardwareInformation__odata_type_s : microsoft.graph.hardwareInformation
  ... hardwareInformation_serialNumber_s : Serial Number value
  ... hardwareInformation_imei_s : Imei value
  ... hardwareInformation_meid_s : Meid value
  ... hardwareInformation_manufacturer_s : Manufacturer value
  ... hardwareInformation_model_s : Model value
  ... hardwareInformation_phoneNumber_s : Phone Number value
  ... hardwareInformation_subscriberCarrier_s : Subscriber Carrier value
  ... hardwareInformation_cellularTechnology_s : Cellular Technology value
  ... hardwareInformation_wifiMac_s : Wifi Mac value
  ... hardwareInformation_operatingSystemLanguage_s : Operating System Language value
  ... ownerType_s          : company
  ... deviceActionResults_s :
```

Integrating OMS and Power BI

This section will cover the steps required to create a missing update report and a dashboard through Power BI functionality.

Create Power BI workspace

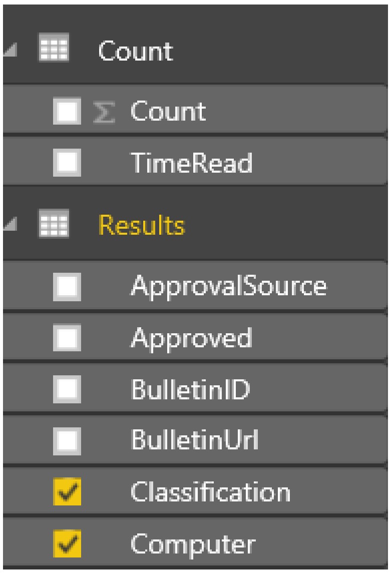
In this task, you will create a Power BI workspace.

1. On the taskbar, right-click **Internet Explorer** and click **Start InPrivate Browsing**.
2. In the Address Bar, type https://powerbi.microsoft.com and press ENTER.
3. Click **Get started free**.
4. On the Get Started page page, choose **Power BI** and click "**Sign Up**".

Connect OMS to Power BI

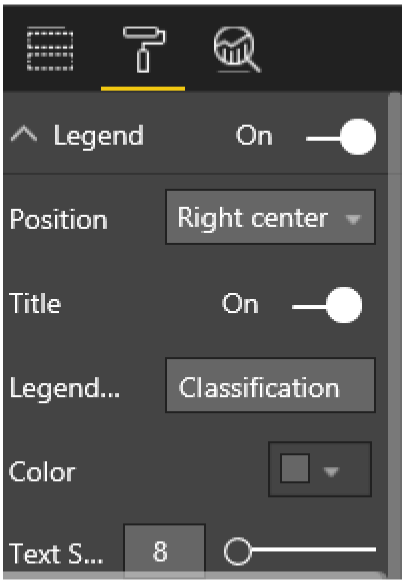
1. In the **OMS Portal,** Click the **Settings** tile.
2. Click **Preview Features**
3. Switch the **PowerBI Integration** to **Enabled**
4. Refresh the OMS Portal, Click on "**Settings**" tile. Click on "**Accounts**", followed by "**Workspace Information"**. Theb click on **"Connect Power BI Account"**
5. **Sign in** by using your Office 365 or work account, and you are all set for the Power BI integration.
6. In the **OMS Portal,** Click the **"Log Search"** tile and enter the query:

   Type=Update
7. Select the **PowerBI** button in the upper bar.
8. Give the name **Missing Updates** to the saved query and a name to the dataset (it will appear in Power BI workspace with this name), set the schedule to 24 hours, and save it.
9. **Refresh** the OMS Portal
10. If the query is successfully saved it will appear in **"Settings"** tile. Click on **"Power BI".** *Wait few minutes and the dataset should sync with the Power BI workspace.*
11. Go to **PowerBI.com,** and sign in with your Office 365 account.
12. After you are logged in, select the menu button (☰) at the upper left, to bring out the **dataset view.**
13. Scroll down to "Datasets" section and select your created dataset.
14. Under "Visualizations", select the "Table" model ▦
15. On the right site under **Fields | Results** then check **Computer, KBID, Product** and **Classification**



- Count
  - □ Count
  - □ TimeRead
- Results
  - □ ApprovalSource
  - □ Approved
  - □ BulletinID
  - □ BulletinUrl
  - ☑ Classification
  - ☑ Computer

16. Now we want to create a diagram containing information on the updates per computer Select the **Pie Chart** model, and then under **Fields | Results**, check **Classification**
17. On the right, drag **Classification** field to **Values.**
18. Select the format icon to the right, turn on **Legend,** set “Position” to **Right center**, and give it an appropriate name in the “Legend” field.



Legend On

Position: Right center

Title On

Legend...: Classification

Color

Text S...: 8

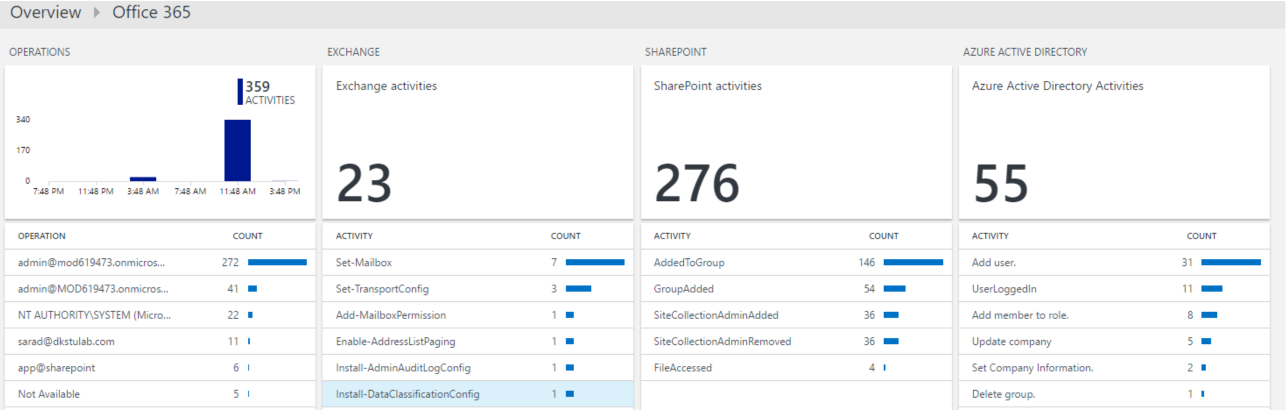
19. Now you can hover over a field with your mouse, and you will see more information.
20. **Save** your report for future use.
21. At this point, the report is available through a dashboard, so you can click the **Share** Button and share with others

O365, SharePoint, Azure AD and Exchange Online - Enabling monitoring of productivity

This section will cover the steps required to monitor Azure AD, Office 365, SharePoint Online and Exchange Online.

When enabling O365, it is good practices to create a service account and give that specific user Global Admin right. When the first connection has been made and data starts flowing into the Log Analytics dashboard, de-promote the service account and remove the global admin and they are only used for establishing first connection.

Office 365 Overview



Overview ▸ Office 365

OPERATIONS

OPERATION	COUNT
admin@mod619473.onmicros...	272
admin@MOD619473.onmicros...	41
NT AUTHORITY\SYSTEM (Micro...	22
sarad@dkstulab.com	11
app@sharepoint	6
Not Available	5

EXCHANGE

Exchange activities

23

ACTIVITY	COUNT
Set-Mailbox	7
Set-TransportConfig	3
Add-MailboxPermission	1
Enable-AddressListPaging	1
Install-AdminAuditLogConfig	1
Install-DataClassificationConfig	1

SHAREPOINT

SharePoint activities

276

ACTIVITY	COUNT
AddedToGroup	146
GroupAdded	54
SiteCollectionAdminAdded	36
SiteCollectionAdminRemoved	36
FileAccessed	4

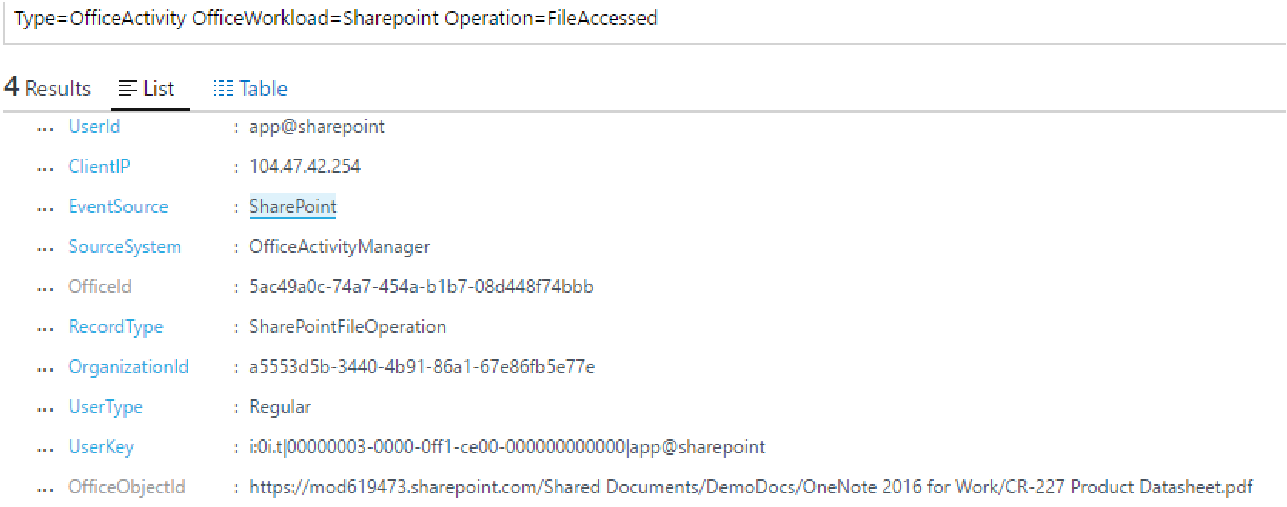
AZURE ACTIVE DIRECTORY

Azure Active Directory Activities

55

ACTIVITY	COUNT
Add user.	31
UserLoggedIn	11
Add member to role.	8
Update company	5
Set Company Information.	2
Delete group.	1

Files accessed



```
Type=OfficeActivity OfficeWorkload=Sharepoint Operation=FileAccessed
```

UserId	app@sharepoint
ClientIP	104.47.42.254
EventSource	SharePoint
SourceSystem	OfficeActivityManager
OfficeId	5ac49a0c-74a7-454a-b1b7-08d448f74bbb
RecordType	SharePointFileOperation
OrganizationId	a5553d5b-3440-4b91-86a1-67e86fb5e77e
UserType	Regular
UserKey	i:0i.t|00000003-0000-0ff1-ce00-000000000000|app@sharepoint
OfficeObjectId	https://mod619473.sharepoint.com/Shared Documents/DemoDocs/OneNote 2016 for Work/CR-227 Product Datasheet.pdf

Create a custom view based on hard deletion based on the following query:

Type=OfficeActivity OfficeWorkload=Exchange Operation=HardDelete | measure count() by UserId

In case that a user hard deletes a document, it will show what document was deleted and what user did it.