**Step 1** **–** **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 step, we will create an Automation account that can be used by OMS when implementing an Automation Solution.

1. Launch **Azure Portal** at [http://portal.azure.com](http://portal.azure.com/)
2. Sign in using your Microsoft Azure credentials.
3. Click **New+,** click **Management**, and click **Automation Account**.
4. In the Add Automation Account blade, in Name, type **AzureOMSAutomation**.
5. Click **Resource group**.
6. Click **Create a new resource group**.
7. In Name, type **AzureOMSResourceGroup** and click **OK**.
8. Click **Region** and select the closest region to you. At the time of writing this post, the following regions are available:
   * Japan East
   * East US 2
   * West Europe
   * Southeast Asia
   * South Central US

I will choose **West Europe**

1. Click **Create** as shown in the following screenshot.

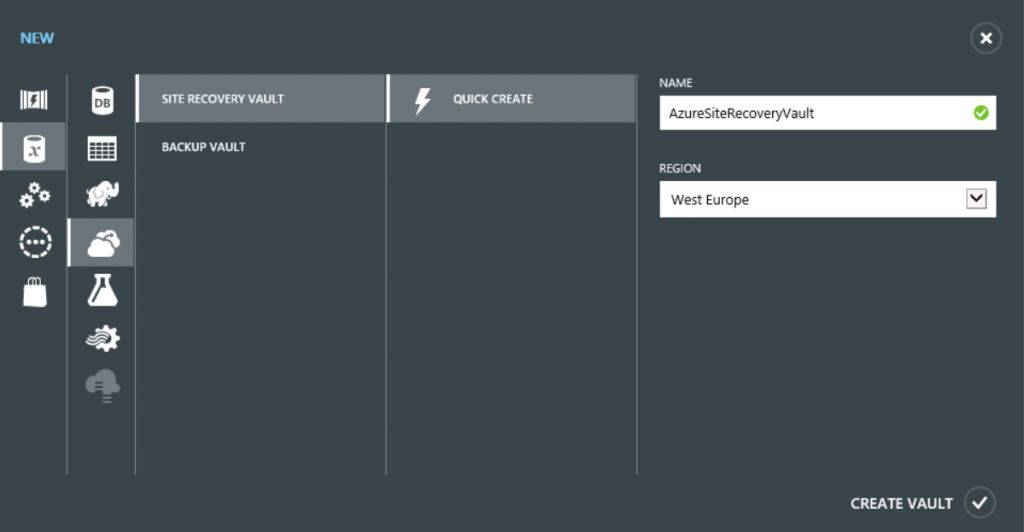
(Note the details of the account for use in future steps).

**Step 2** **–** **Create Microsoft Azure Recovery Services Vaults (Backup and Recovery Site)**

To back up files and data from your [Windows Server](https://www.starwindsoftware.com/reduce-disaster-recovery-and-business-continuity-expenses-video) or System Center Data Protection Manager (SCDPM) to Azure or when backing up IaaS VMs to Azure, you must create a backup vault in the geographic region where you want to store your data.

A Microsoft Azure Site Recovery Vault is used to replicate your virtual machines to a cloud service for disaster recovery purposes.

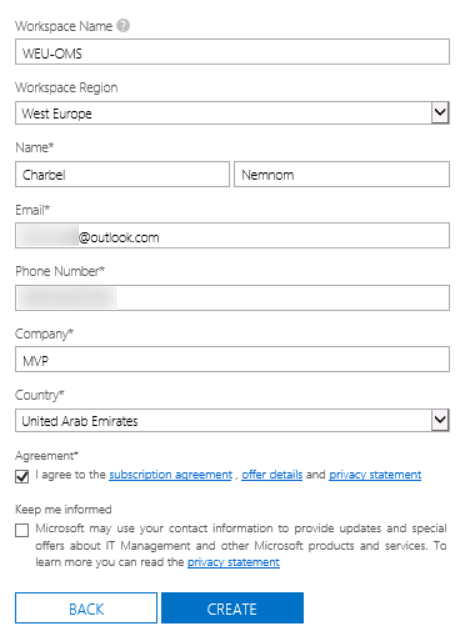
In this step, we will create both a Microsoft Azure Backup vault and a Microsoft Azure Site Recovery Vault.

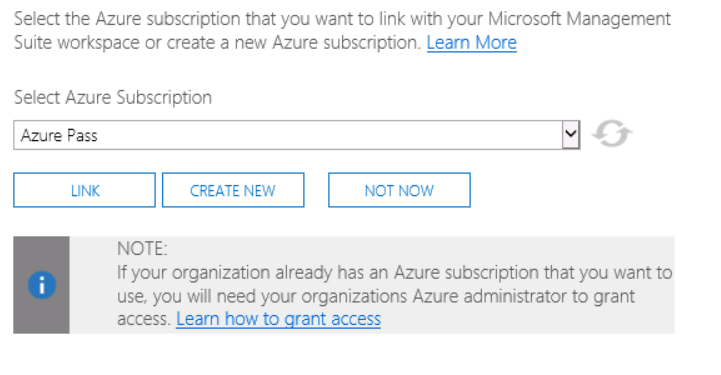
1. Click Create a resource.
2. Click **Storage.**
3. From the Storage blade, click Backup and Site Recovery (OMS).
4. In the NAME field, type **AzureBackupVault**
5. From the Region drop-menu, select the closest region to you.
6. Click **CREATE VAULT** as shown in the following screenshot.
7. Click **+NEW**.
8. Click **SITE RECOVERY VAULT**.
9. Click **QUICK CREATE**.
10. In the **NAME** field, type **AzureSiteRecoveryVault**
11. From the Region drop-menu, select the same region you used before.
12. Click **CREATE VAULT** as shown in the following screenshot. [](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/33.png)
13. In the upper right corner of the window, click your user account name and click Switch to **New** **Azure Portal**.

|  |  |
| --- | --- |
|  |  |
|  |

**Step 3** **– Create a Microsoft Operations Management Suite Workspace**

In this step, you will create a new Microsoft Operations Management Suite account, associate it with an existing Microsoft Azure account, and sign in to the Microsoft Operations Management Suite web site.

1. Launch **Operations Management Suite Portal** at [http://www.microsoft.com/en-us/server-cloud/operations-management-suite/overview.aspx](https://www.microsoft.com/en-us/cloud-platform/operations-management-suite)
2. If prompted, click **No thanks**.
3. Click **Create a free account**.
4. On the Operations Management Suite Trial page, click **Get started**.
5. On the Create a New Workspace page, in Workspace Name type a unique name.
6. In Workspace Region, click the **drop-down arrow** and select **East US** or **West Europe**.
7. In the Name, type your full name.
8. In Email, type the email address associated with your Microsoft Azure account.
9. Click **Subscription Agreement**, read the terms and close the window.
10. Select the check box next to I have read the Subscription agreement and agree to its terms and click **CREATE** as shown in the following screenshot. [](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/43.png)
11. In Select Azure subscription, click the **drop-down arrow** and select **Azure Pass**.
12. Click **LINK** as shown in the following screenshot.

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/52.png)

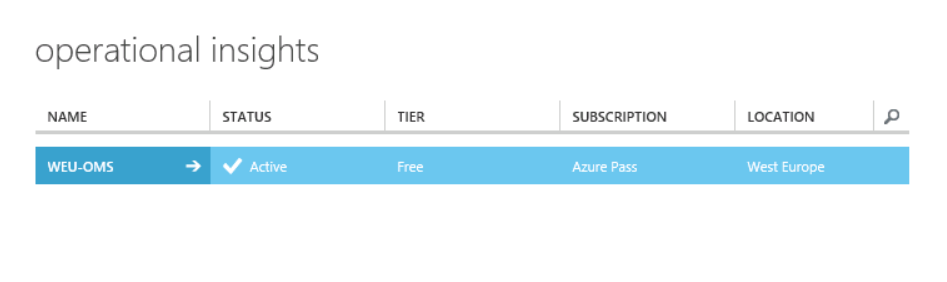
**Step 4** **– Locate Operations Management Suite Workspace Configuration Information**

Operational Insights is an Azure online service that analyzes installations of Microsoft Server software to help administrators identify potential issues.

In this step, we will browse the Microsoft Azure portal to locate information regarding our Operational Insights Workspace.

1. Switch to the old Microsoft Azure Portal window at [https://manage.windowsazure.com](https://manage.windowsazure.com/).
2. In the Browse blade, scroll down and click **Operational Insights.**
3. Record the Name, Resource Group, and Location of your Operational Insights workspace.

This information will be used in later steps as shown in the following screenshot. Write it down.

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/62.png)

1. Close the Azure portal.

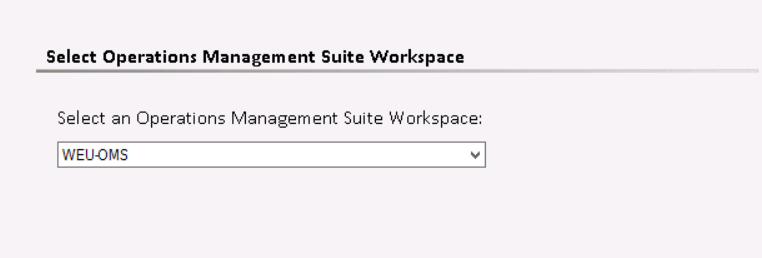
**Step 5** **– Register the Operations Management Suite with SCOM**

System Center Operations Manager now includes Operations Insights as an attached service, which will allow you to add Operations Management Suite monitoring to Windows management servers in your SCOM environment. The services feeds data to your OMS environment.

In this step, you will use the use the SCOM Operations Management Suite Onboarding Wizard to connect the Operational Insights service to SCOM.

Assuming you already have SCOM deployed in your environment.

1. Open the **Operations Manager**
2. On the navigation pane, click **Administration**.
3. Expand **Operations Management Suite** and click **Connection**.
4. Under Get Started, click **Register to Operations Management Suite**.
5. Enter your email and the credentials associated with your OMS Workspace, and click **Sign in**.
6. From the drop-down menu, ensure that your Operations Management Suite workspace is selected as shown in the following screenshot, and click

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/72.png)

1. Click **Create**.
2. Click **Close**.
3. In the Results pane, under **Actions**, click **Add a Computer/Group**.
4. Click
5. Under Available Items, select both your SCOM server and SQL server machine, click
6. In the same window page, Click the drop-down menu for **Options**, select **All Instance Groups**, and click **Search**.
7. Select **Universal Linux Instances Group** and click
8. Click **OK**.
9. In the Navigation pane, click **Managed Computers** to check all managed computers are listed.
10. In the Navigation pane, click **Monitoring** and expand the **Operations Management Suite node.**

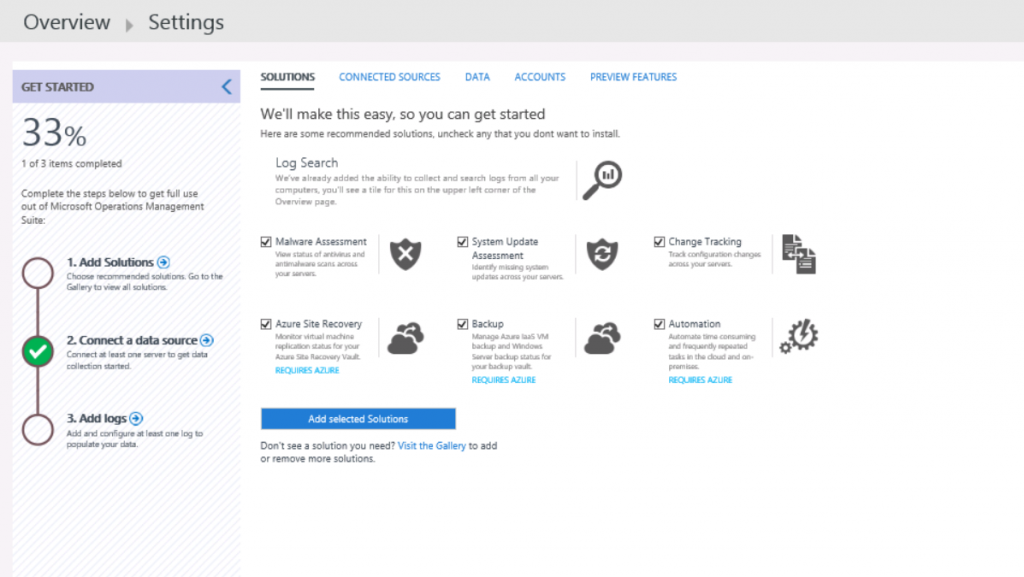
(*Configuration Alerts and Health State nodes exist for monitoring the Operations Management Suite environment*).

**Getting Started with Microsoft Operations Management Suite**

**Step 1** **–** **Configure OMS Settings**

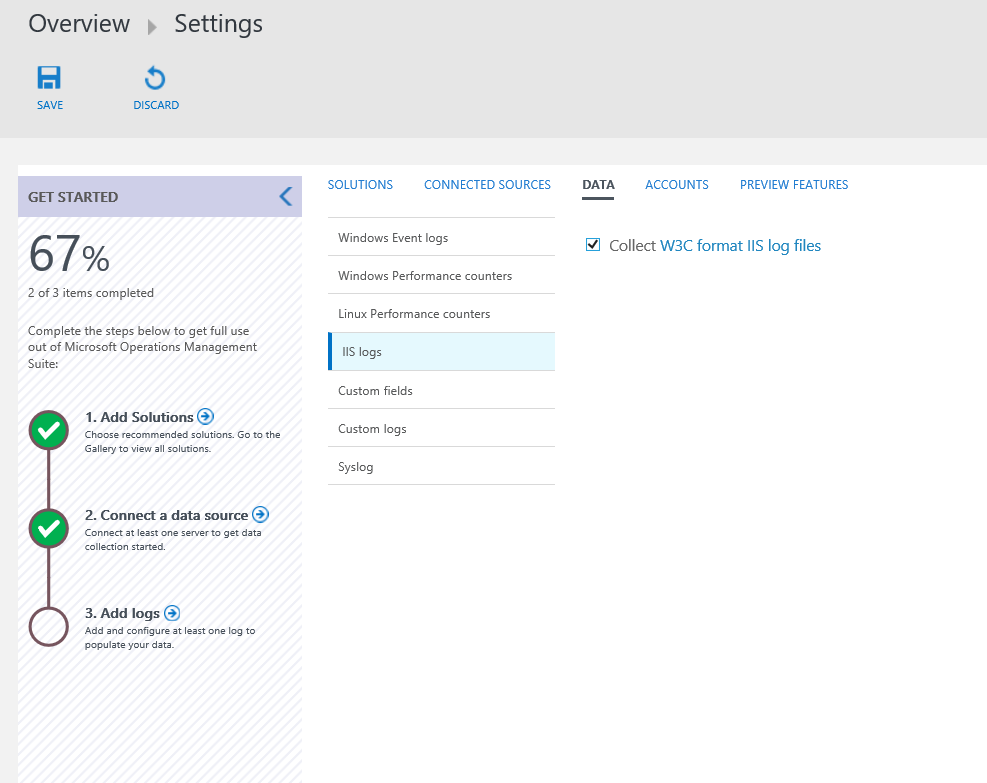
In this step, you will use the OMS Settings tile which allows you to configure Solutions, Logs, and Accounts.

1. Launch Operations Management Suite Portal at [http://www.microsoft.com/en-us/server-cloud/operations-management-suite/overview.aspx](https://www.microsoft.com/en-us/cloud-platform/operations-management-suite)
2. Click **Sign in**, enter the credentials associated with OMS, and click **Sign in**
3. Click the OMS Workspace name. The OMS Portal will open (you may be asked to confirm your email address).
4. Switch to the Operations Management Suite Portal.
5. On the Overview blade, scroll to the right and click the **Settings**
6. Ensure all available solutions are selected and click **Add Selected Solutions** as shown in the following screenshot:

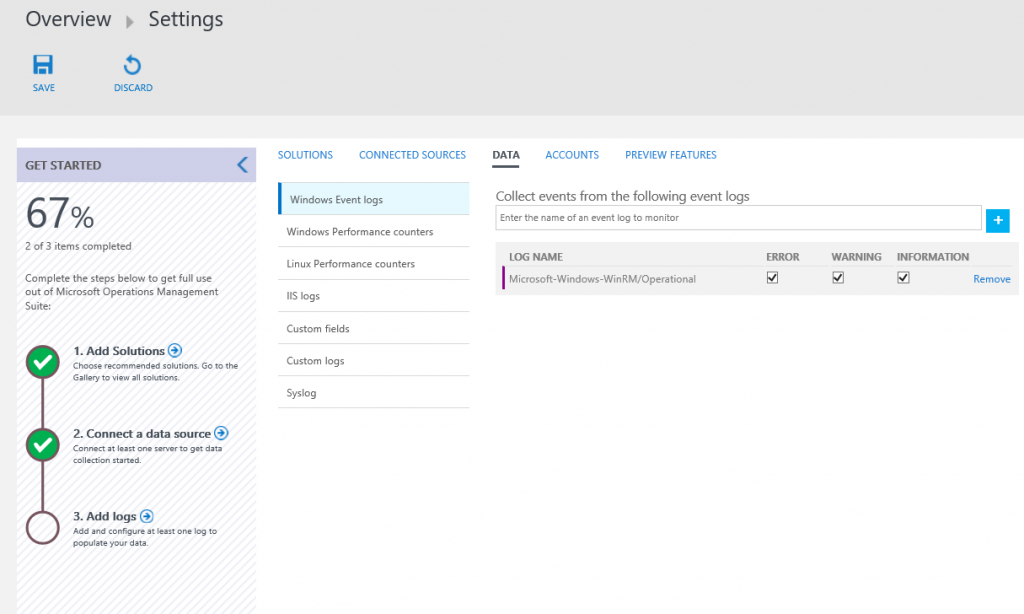
[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/115.png)

*Basic solutions are added to the console: Log Search, Automation, Azure Site Recovery, Backup, Change Tracking, Malware Assessment, and System Update Assessment.*

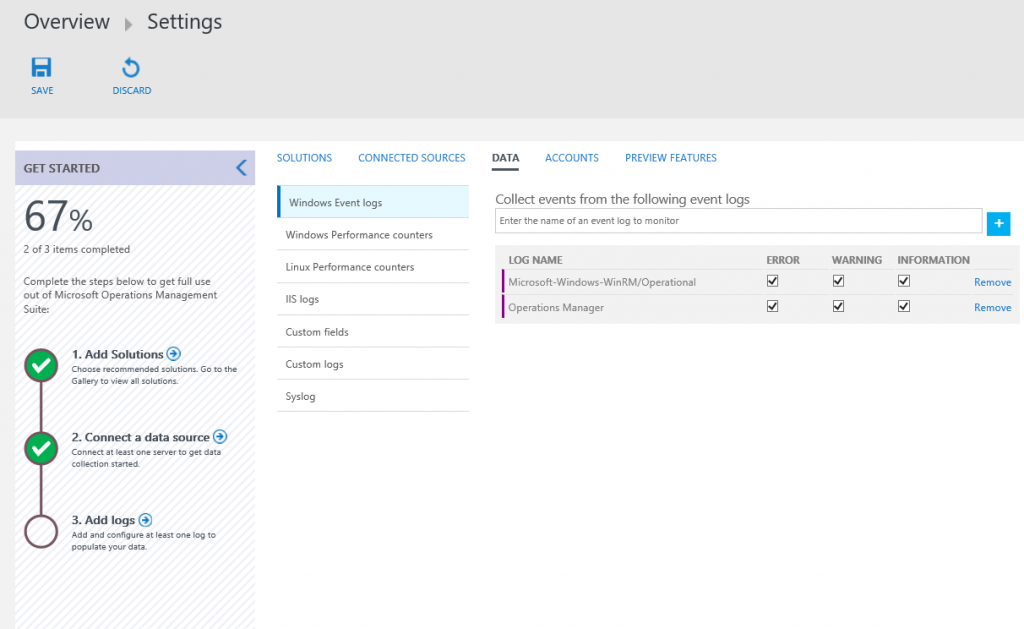
1. On the Settings page, click **Add LOGS**.
2. Select **IIS Logs**.
3. Select the check box next to **Collect W3C format IIS log files** as shown in the following screenshot:

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/214.png)

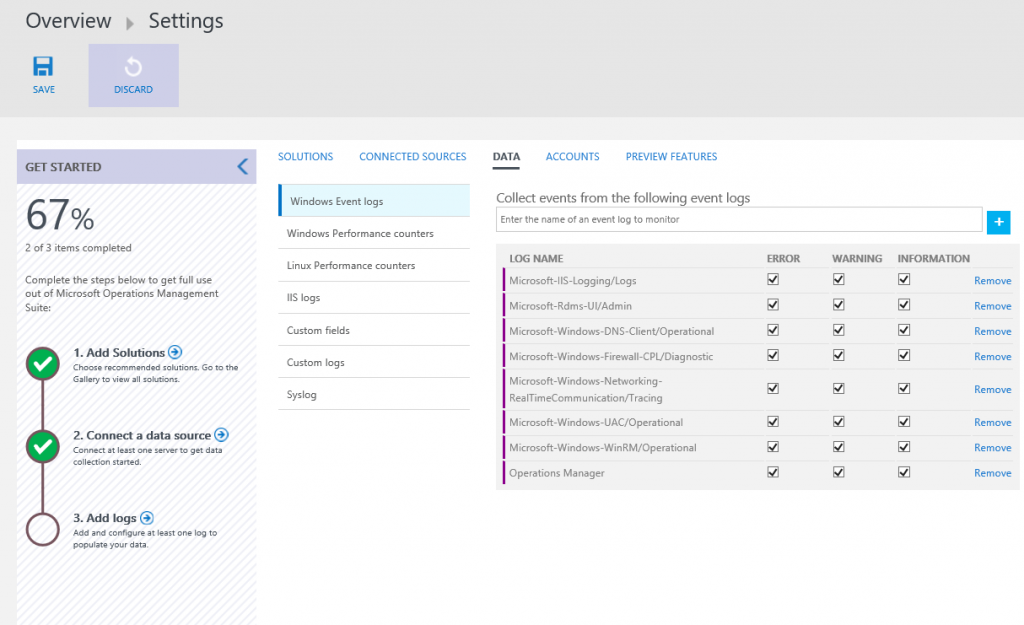
1. Under **Windows Event Logs**, click **Enter the name of an event log to monitor**.
2. Type **Microsoft-Windows-WinRM/Operational** and click the plus sign.
3. Select the check boxes next to **ERROR**, **WARNING**, and **INFORMATION** as shown in the following screenshot:

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/35.png)

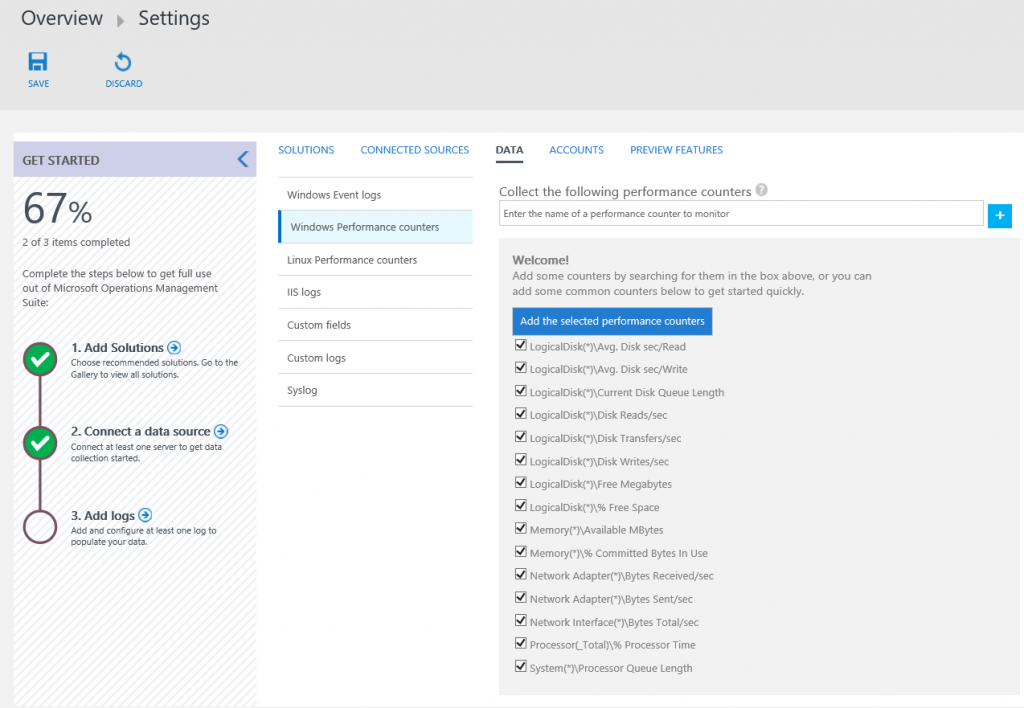
1. Click **Enter the name of an event log to monitor**, type **Operations**, select **Operations Manager**, and click the plus sign.
2. Select the check boxes next to **ERROR**, **WARNING**, and **INFORMATION** as shown in the following screenshot:

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/46.png)

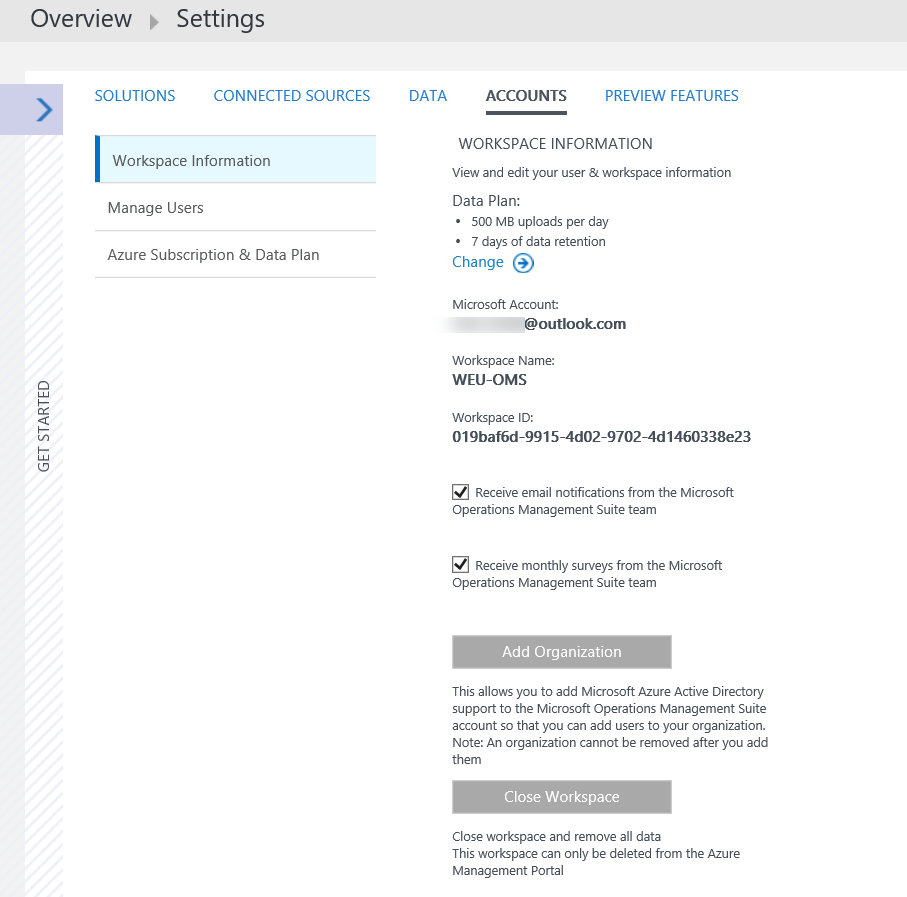
1. Click **Enter the name of an event log to monitor,** type **Microsoft-**, select another log, and click the plus sign.
2. Select the check boxes next to **ERROR**, **WARNING**, and **INFORMATION** as shown in the following screenshot:

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/53.png)

1. Add several more logs and configure the levels to be collected.
2. Under **Windows Performance Counters**, review the available counters and click **Add the selected performance counters** as shown in the following screenshot:

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/63.png)

1. Click **SAVE**.
2. On the Settings blade, click **ACCOUNTS** as shown in the following screenshot (this page provides the ability to configure your workspace(s) and manage OMS user accounts):

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/73.png)

|  |  |
| --- | --- |
| https://www.starwindsoftware.com/blog/wp-content/uploads/2016/10/xStarWind-HCA_blue-300x300.png.pagespeed.ic.tMYFSY41IB.png | **StarWind HyperConverged Appliance** is a turnkey, entirely software-defined hyperconverged platform purpose-built for intensive virtualization workloads. Bringing the desired performance and reducing downtime, the solution can be deployed by organizations with limited budgets and IT team resources. Also, it requires only one onsite node to deliver HA for your applications that make the solution even more cost-efficient. |
| Find out more about  [StarWind HyperConverged Appliance](https://www.starwindsoftware.com/starwind-hyperconverged-appliance" \t "_blank) |

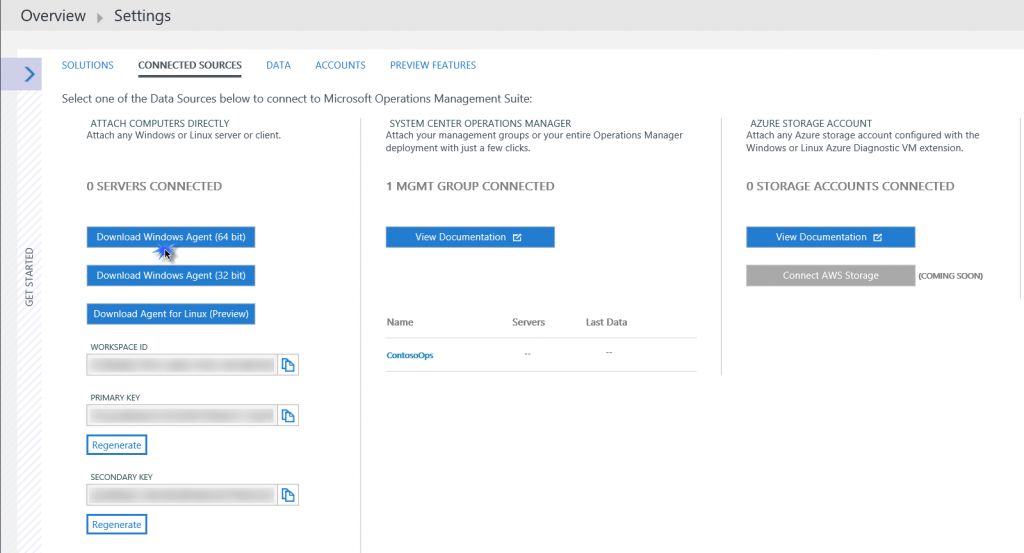
**Step 2** **– Configure Domain Controller as a Connected Source via a Direct Agent**

In this step, you will use the OMS Settings tile to configure your domain controller as a Connected Source via a direct connection.

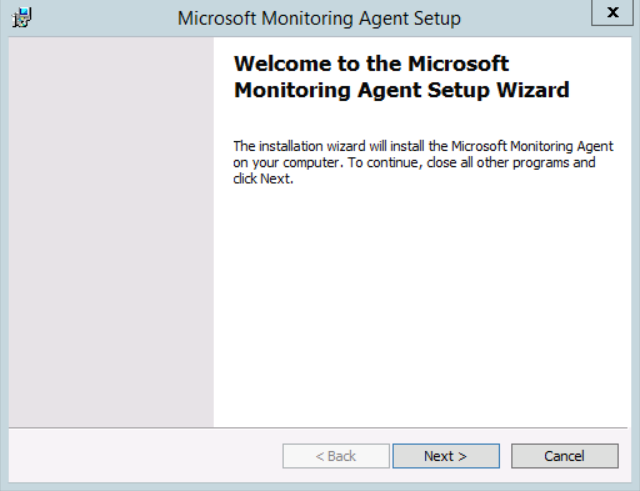
1. Launch **Operations Management Suite Portal** at [http://www.microsoft.com/en-us/server-cloud/operations-management-suite/overview.aspx](https://www.microsoft.com/en-us/cloud-platform/operations-management-suite)
2. Click **Sign in.**
3. Enter the credentials associated with OMS, and click **Sign in**
4. Click the OMS Workspace name.
5. On the dashboard, scroll to the right and click the **Settings**
6. On the Settings blade, click **CONNECTED SOURCES**.

*You have three options for connecting your server environment to OMS: you can attach any Windows server or 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.*

1. Under ATTACH COMPUTERS DIRECTLY, click **Download Windows Agent (64 bit)** as shown in the following screenshot.

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/82.png)

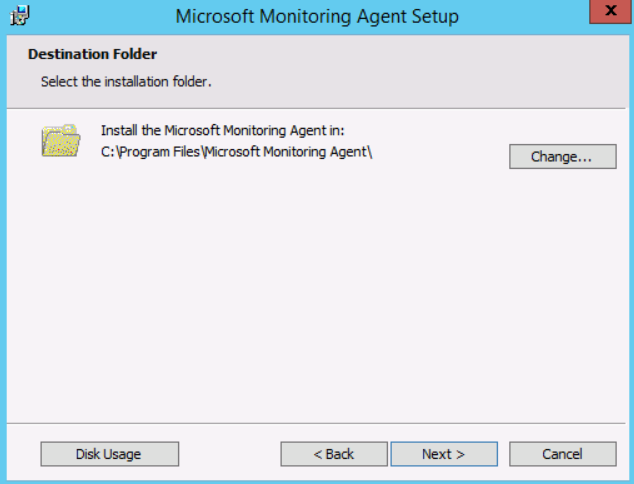
1. Make sure you copy the **MMASetup-AMD64.exe** over your domain controller and Click to Run.
2. In the Microsoft Monitoring Agent Setup Wizard, click **Next**.

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/92.png)

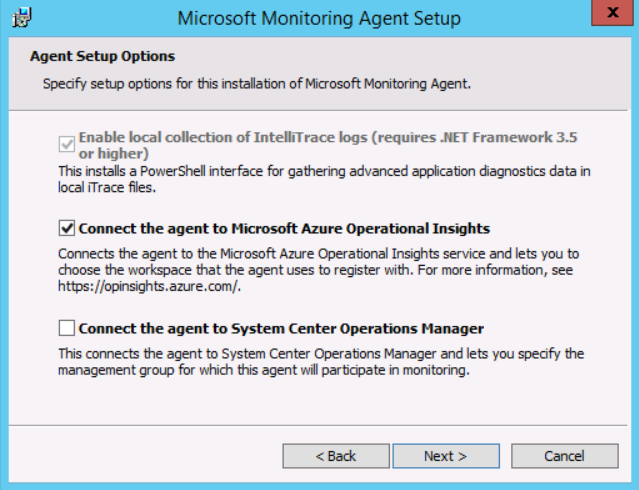
1. Click **I Agree**.

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/102.png)

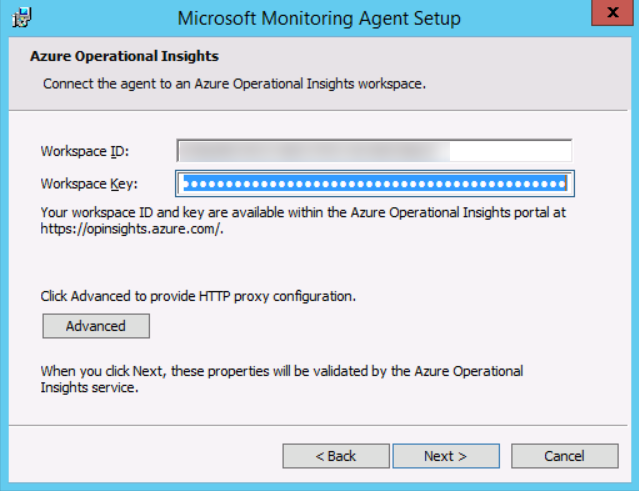
1. On the Destination Folder page, click **Next**.

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/116.png)

1. Click the checkbox next to **Connect the agent to Microsoft Azure Operational Insights** and click **Next**.

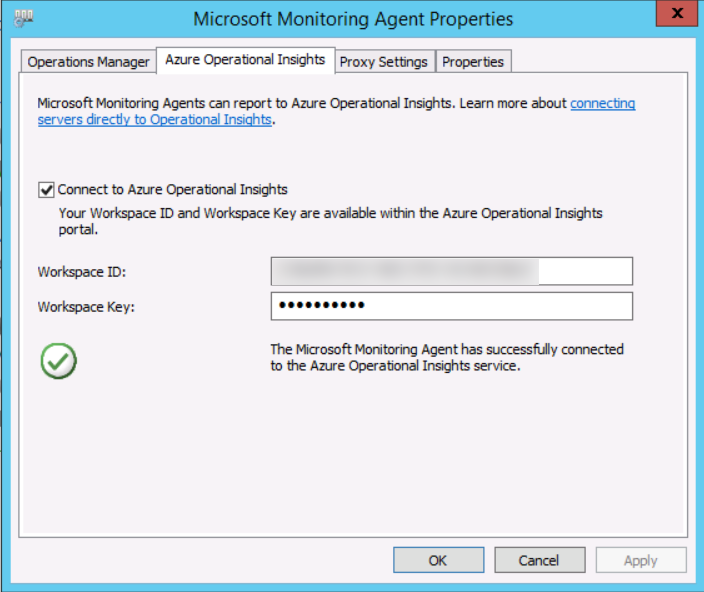
[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/122.png)

1. Switch to the OMS Settings blade, click the **Copy** icon next to **WORKSPACE ID,** and click **Allow access.**
2. Switch to the Microsoft Monitoring Agent Setup Wizard, click in the **Workspace ID** field in the Wizard, and press CTRL-V.
3. Switch to the OMS Settings blade, click the **Copy** icon next to **PRIMARY KEY,** and click **Yes**.
4. Switch to the Microsoft Monitoring Agent Setup Wizard, click in the **Workspace Key** field in the Wizard, and press CTRL-V.

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/131.png)

1. Click **Next**.
2. Click **Install**.
3. Click **Finish**.
4. Right-click **Start** and click **Control Panel**.
5. Click **Microsoft Monitoring Agent**.
6. Click the [**Azure**](https://www.starwindsoftware.com/save-10kon-sql-deployment-in-microsoft-azure) **Operational Insights**

*Note that the Connect to Azure Operational Insights checkbox is selected and the Workspace ID and Workspace Key are configured, per the earlier steps in OMS.*

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/141.png)

1. Click **Cancel**.

**Step 3** **– Configure SQL Server as a Direct Connection Connected Source**

It is possible to configure a machine to report to both OMS and SCOM at the same time. If you recall, in [Part I](https://www.starwindsoftware.com/blog/introduction-to-microsoft-operations-management-suite-oms-part-i), we are monitoring the [SQL server](https://www.starwindsoftware.com/resource-library/critical-sql-server-databases-provide-ha-with-sql-server-failover-clustering-and-cluster-shared-volumes) using SCOM on-premises, so it is already reporting to SCOM.

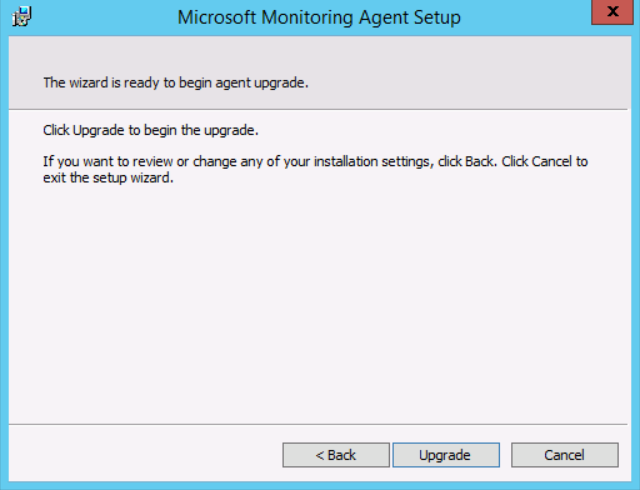
In this step, you will use the OMS Settings tile to configure [SQL Server](https://www.starwindsoftware.com/critical-sql-server-databases-provide-ha-with-sql-server-failover-clustering) as a Connected Source via a direct connection.

1. Login into your [SQL Server](https://www.starwindsoftware.com/microsoft-sql-server-deployment-price-reduced-by-3-times-with-starwind-virtual-san).
2. Click **Start** and click **Control Panel**.
3. Click **Microsoft Monitoring Agent**, as you can see in the following screenshot that the agent is configured to send data to SCOM.

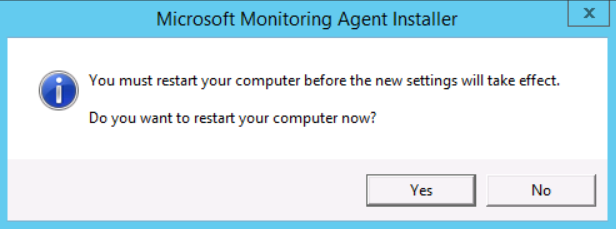
[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/151.png)

The following steps are similar to the steps described in the previous section.

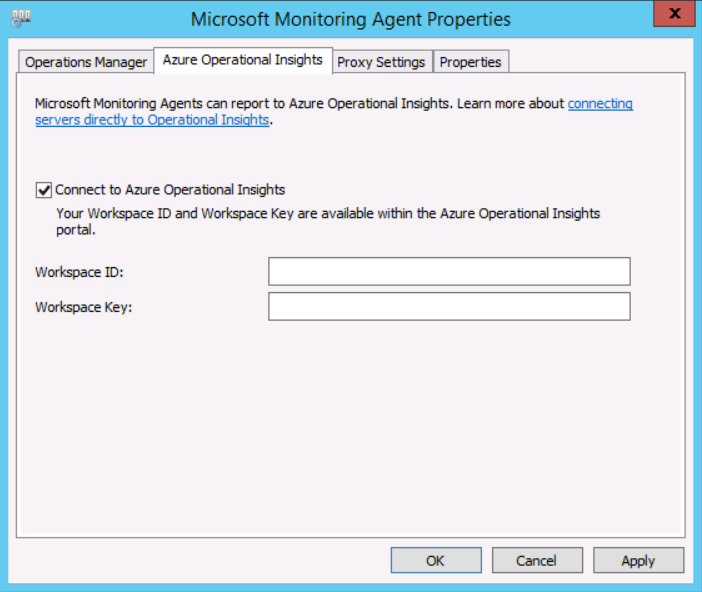
1. Switch to **Operations Management Suite Portal** at [http://www.microsoft.com/en-us/server-cloud/operations-management-suite/overview.aspx](https://www.microsoft.com/en-us/cloud-platform/operations-management-suite)
2. On the Settings blade, click **CONNECTED SOURCES**.
3. Under ATTACH COMPUTERS DIRECTLY, click **Download Windows Agent (64 bit).**
4. Click **RUN** on **MMASetup-AMD64.exe**
5. In the Microsoft Monitoring Agent Setup Wizard, click **Next**.
6. Click **I Agree** (*because the agent is already deployed on the machine, you must upgrade it to add OMS direct connection capabilities*).

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/161.png)

1. Click **Upgrade**.
2. Click **Finish**.
3. Click **Yes** to restart the computer.

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/171.png)

1. After the reboot is completed, log on again to your SQL Server.
2. Click **Start**, click **Control Panel**, and click **Microsoft Monitoring Agent**.
3. Click on the **Azure Operational Insights**
4. Click the checkbox next to **Connect to Azure Operational Insights**.

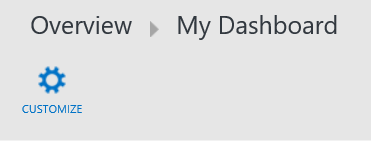
[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/181.png)

1. Leave the agent configuration window open.
2. Open Internet Explorer and sign in using your OMS account credentials.
3. Click **Settings** and click on **Connected Sources**.
4. Click the **Copy** icon next to **WORKSPACE ID** and click **Allow access**.
5. Switch to the Microsoft Monitoring Agent properties, click in the **Workspace ID** field and press CTRL-V.
6. Switch to the OMS Settings blade again, click the **Copy** icon next to **PRIMARY KEY**.
7. Switch to the Microsoft Monitoring Agent properties, click in the **Workspace Key** field and press CTRL-V.
8. Click **OK** (*the agent will stop and start* *automatically*).

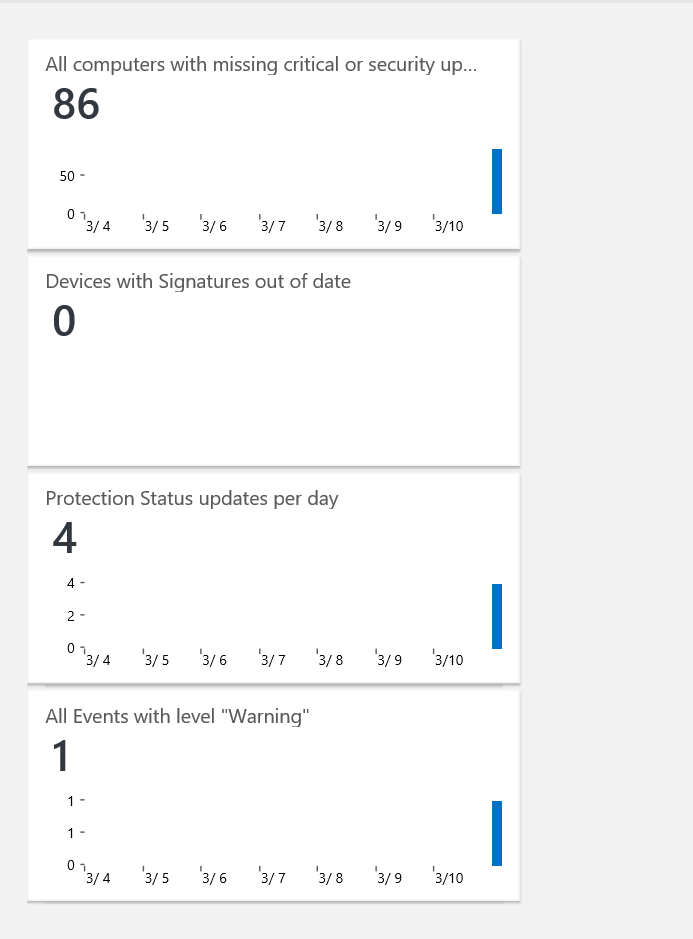
**Step 4** **– Customize the OMS Dashboard**

In this step, we will customize the OMS **My Dashboard** tile.

1. Open **Operations Management Suite Portal** at [http://www.microsoft.com/en-us/server-cloud/operations-management-suite/overview.aspx](https://www.microsoft.com/en-us/cloud-platform/operations-management-suite)
2. In the OMS Portal, to the left of **Overview | Settings**, click the **Overview icon**.
3. Click **My Dashboard**[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/191.png)
4. 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*).

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/201.png)

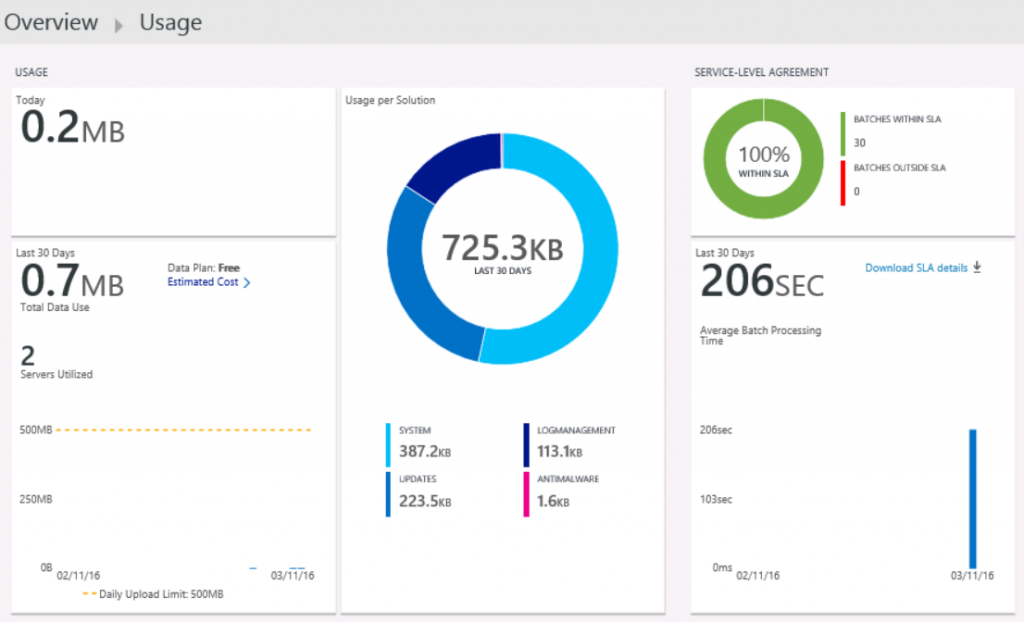
1. From the menu on the right, under Change Tracking, select **All Configuration Changes** and drag it onto **My Dashboard**.
2. Under **System Update Assessment** on the right hand side, select **All computers with missing or Security Updates** and drag it onto **My Dashboard**.
3. Drag several additional items to **My Dashboard** as shown in the following screenshot:

**[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/215.png)**

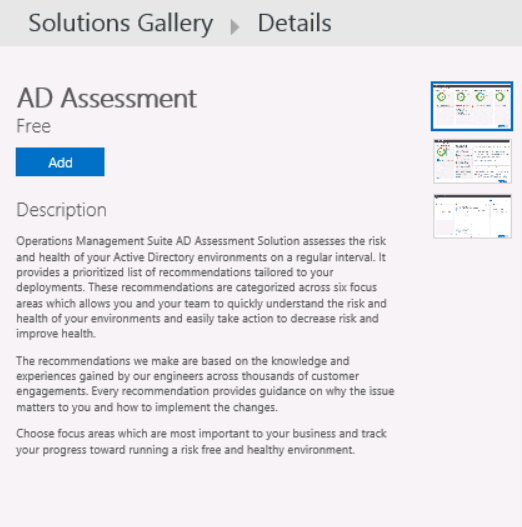
**Step 5** **– Added Microsoft Operations Management Suite Solutions to the OMS Console**

In this step, you will explore several tiles on the OMS dashboard that can assist you in gaining deeper insight into your environment such as Security and Audit, SQL Assessment, and Automation.

1. Open **Operations Management Suite Portal** at [http://www.microsoft.com/en-us/server-cloud/operations-management-suite/overview.aspx](https://www.microsoft.com/en-us/cloud-platform/operations-management-suite)
2. In OMS portal, click the **Overview icon**.
3. Click the **Usage** Review the type of data revealed in the tile.

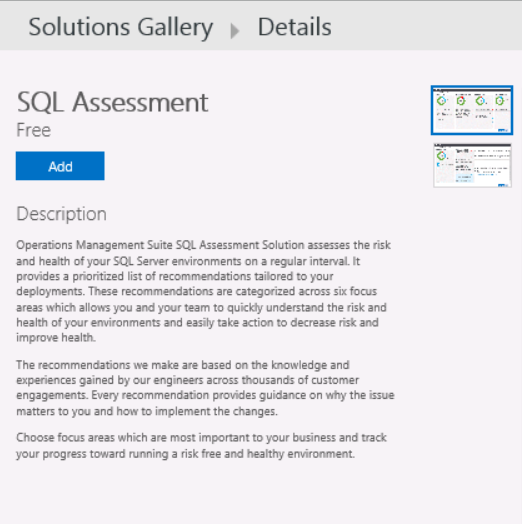
[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/221.png)

1. Click the **Overview icon**.
2. Click the **Solutions Gallery**
3. Click **AD Assessment**.
4. Click **Add** (there will not yet be data populating the solution, it can take up to 4 hours for recommendations to appear).

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/231.png)

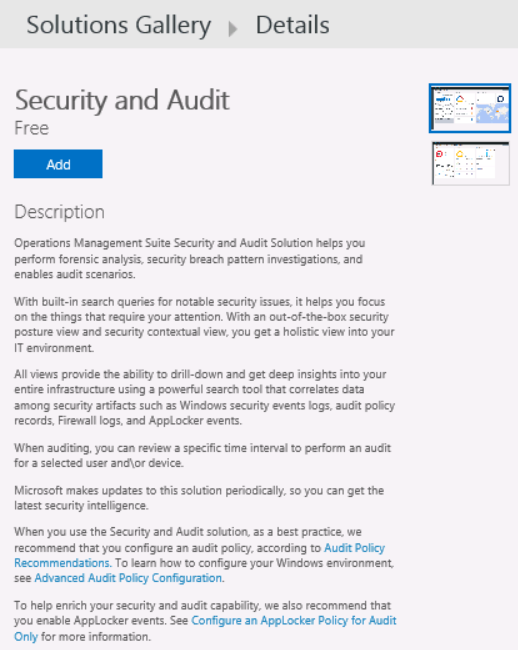
*The AD Assessment tile is now added to the dashboard*

1. Click **Solutions Gallery**.
2. Click **SQL Assessment** and click

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/241.png)

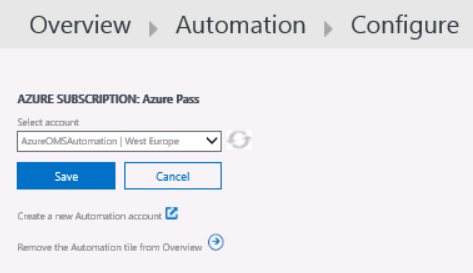
*The SQL Assessment tile is now added to the dashboard*

1. Click the **Overview icon**.
2. Click the **Solutions Gallery**
3. Click **Security and Audit** and click **Add**.

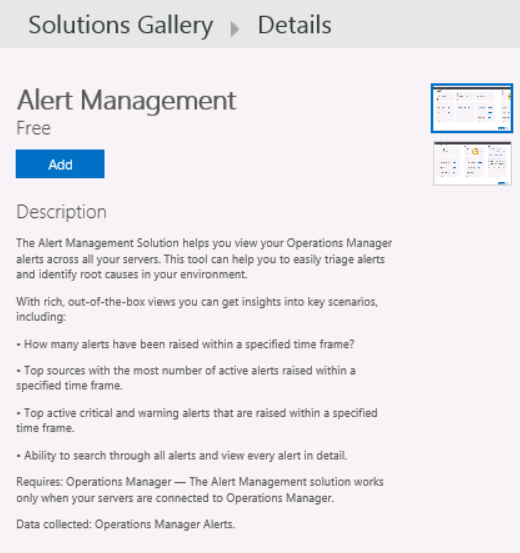
[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/251.png)

*The Security and Audit tile is now added to the dashboard*

1. Click the **Overview icon**.
2. Click the **Automation**
3. Ensure your [Azure](https://www.starwindsoftware.com/blog/azure-execute-an-azure-automation-runbook-from-an-asp-net-website) Pass is listed as the account and click **Save**.

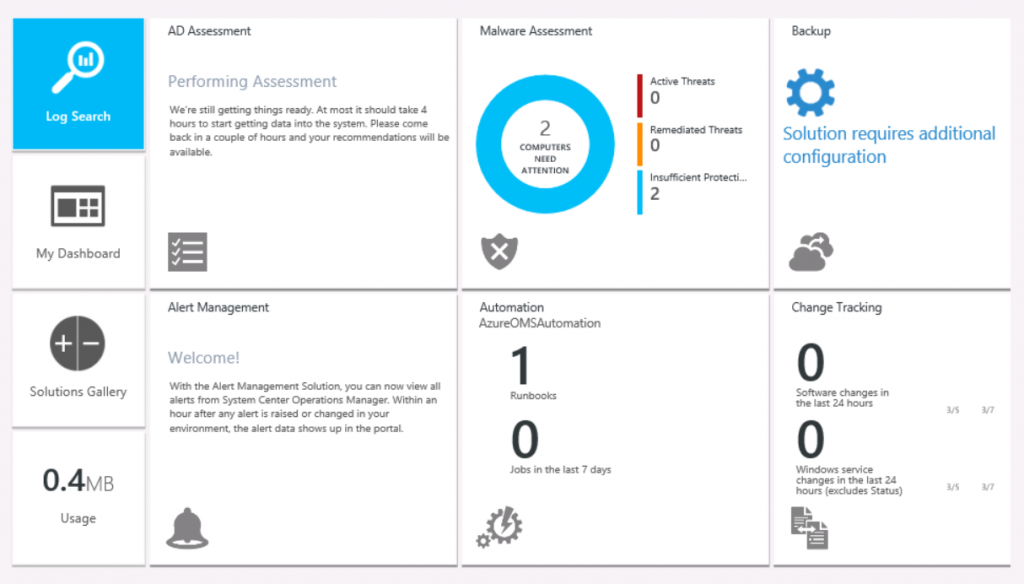
[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/261.png)

1. Click the **Overview**
2. Click the **Solutions Gallery**
3. Click **Alert Management** and click **Add**.

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/271.png)

*The Alert Management tile is now added to the dashboard*

1. Click the **Overview**
2. You will see the solutions that we just added them in this section (you can move the blade to the right hand side to view the complete OMS solutions).

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/281.png)

*Note: 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 twice per day and updated to OMS.*

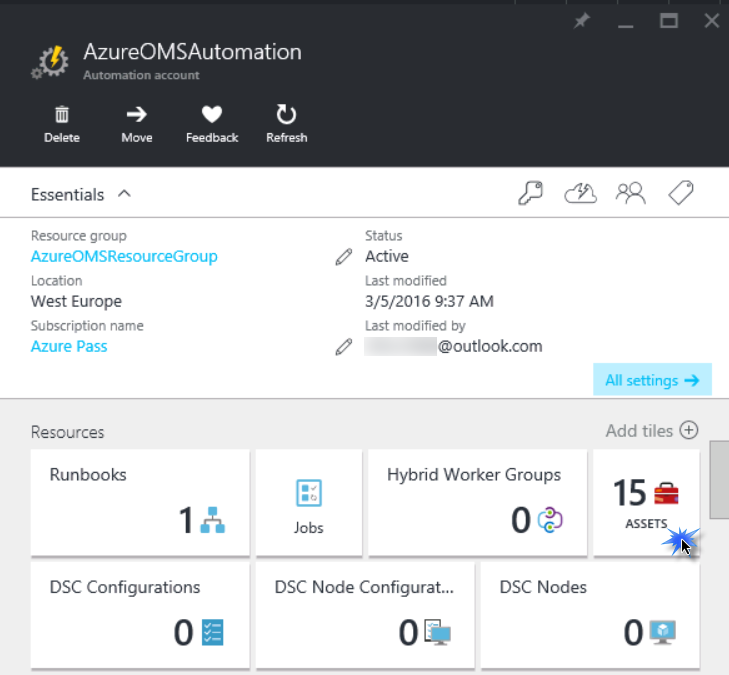
**Introduction to OMS Runbooks**

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

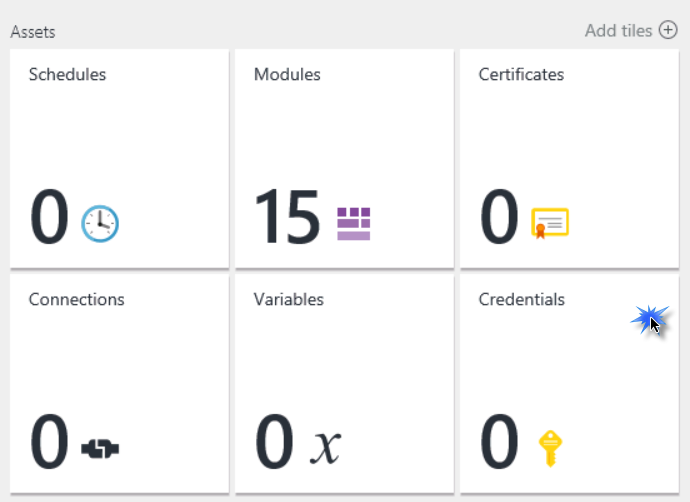
**Step 1** **–** **Configure Azure Automation Assets**

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

1. Login to your [SQL Server](https://www.starwindsoftware.com/microsoft-sql-server-deployment-price-reduced-by-3-times-with-starwind-virtual-san)
2. Sign in Operations Management Suite Portal at [http://www.microsoft.com/en-us/server-cloud/operations-management-suite/overview.aspx](https://www.microsoft.com/en-us/cloud-platform/operations-management-suite)
3. On the OMS Overview blade, click **Automation**. If you recall, this is the account we created in **Part I**.
4. Click the **Runbooks** [Microsoft Azure Portal](https://portal.azure.com/) will open.
5. On the Assets blade, click **AzureOMSAutomation**
6. Under **Resources**, click **Assets** as shown in the following screenshot.

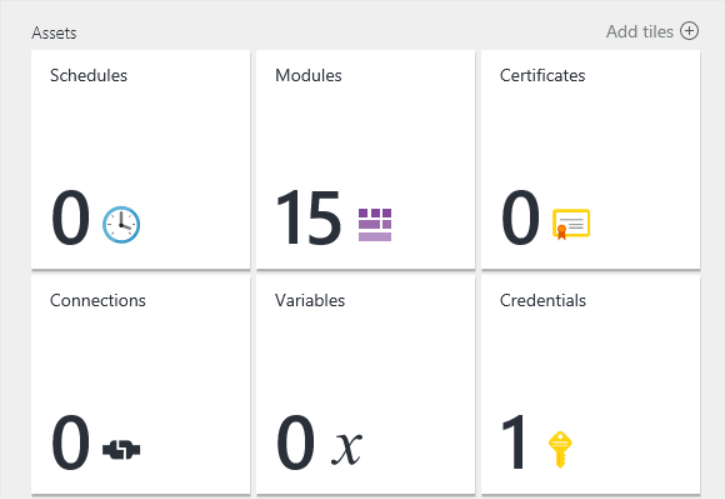
[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/120.png)

1. On the Credential blade, click **Credentials**.

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/218.png)

1. Click **+Add a credential**.
2. In the name field, type **OMS Account**.
3. In the User name and password fields, type the credentials used to log in to OMS and click **Create**.

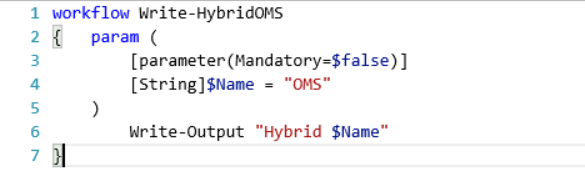
*Note: In a production environment, you would need to use an organizational account. The Credential asset will not function correctly when a Microsoft account (i.e., outlook.com or live.com) is used.*

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/37.png)

1. Close all blades and return to the Start board.

**Step 2** **– Create a Runbook from Scratch**

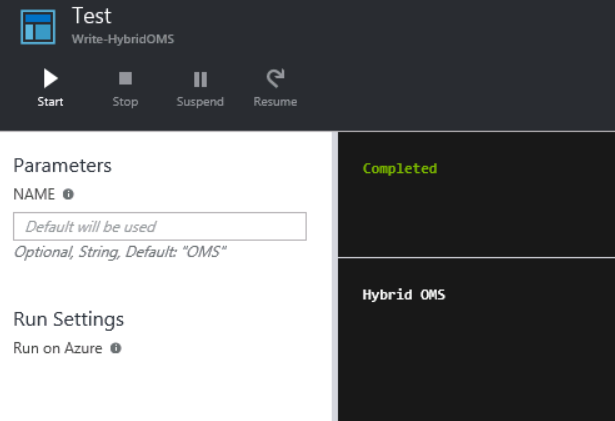
In this section, you will create a runbook from scratch.

1. Login to your SQL Server machine.
2. Sign in to **Operations Management Suite Portal** at [http://www.microsoft.com/en-us/server-cloud/operations-management-suite/overview.aspx](https://www.microsoft.com/en-us/cloud-platform/operations-management-suite)
3. Switch to the **OMS Portal**, **OMS Automation**
4. Click **Create a runbook**. [Microsoft Azure Portal](https://portal.azure.com/) will open.
5. On the Assets blade, click **AzureOMSAutomation**
6. Under Resources, click **Runbooks**.
7. On the Runbook page, click **+Add a runbook**.
8. On the Add Runbook page, click **Create a new runbook**.
9. In the Runbook blade, type **Write-HybridOMS** as a Name.
10. From the Runbook type drop-down menu, select **PowerShell Workflow**, click **Create**.
11. Ensure that the correct Automation account, subscription, and region are selected and click **Create**.
12. In the script area, edit the text to match the following:[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/48.png)
13. Click **Save**.

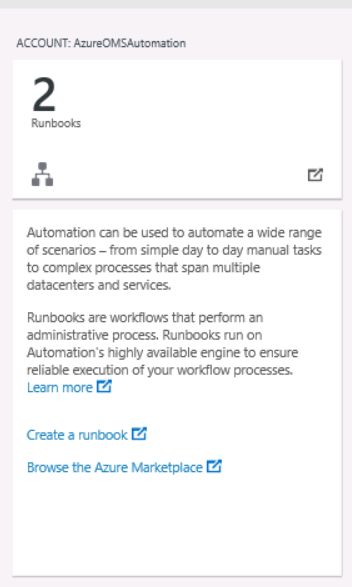
**Step 3** **– Test and Publish a Runbook**

In this step, we will test and publish a runbook.

1. In the Edit PowerShell Workflow Runbook blade for Write-HybridOMS, click **Test Pane**.
2. Click **Start**.
3. When you click, 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 actually starts running. Please note it will take couple of minutes to complete.
4. When the runbook job completes, its output is displayed as shown in the following screenshot. In this case, you should see **Hybrid OMS**.

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/55.png)

1. Close the Test blade to return to the canvas.
2. Switch to the Edit PowerShell Workflow Runbook blade in the Azure Portal.
3. Click **Publish** and then click **Yes**. The runbook will be published.
4. Switch to the OMS Portal, click on **Automation**. As you can see in the following screenshot, we have additional runbook now.

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/65.png)

|  |  |
| --- | --- |
| https://www.starwindsoftware.com/blog/wp-content/uploads/2017/02/StarWind-Virtual-SAN-300x300.png | **StarWind Virtual SAN** eliminates any need for physical shared storage just by mirroring internal flash and storage resources between hypervisor servers. Furthermore, the solution can be run on the off-the-shelf hardware. Such design allows StarWind Virtual SAN to not only achieve high performance and efficient hardware utilization but also reduce operational and capital expenses. |
| Learn more about [StarWind Virtual SAN](https://www.starwindsoftware.com/starwind-virtual-san). |

**Step 4** **– Edit a Runbook**

In this step, we will edit a runbook.

1. Login to your [SQL Server](https://www.starwindsoftware.com/new-microsoft-storage-best-practices-for-hyper-v-and-sql-server-smb-3-0-video)
2. Switch to the Edit PowerShell Workflow Runbook blade in the Azure Portal.
3. In the **Write-HybridOMS** blade, Click **Edit**.
4. Change **“$Name = OMS”** to **“$Name = Azure”**.
5. Click **Save**.
6. Click **Revert to published** and click **Yes**. This will discard all changes you have made and revert to the last published version.
7. Close the **Write-HybridOMS** blade**.**

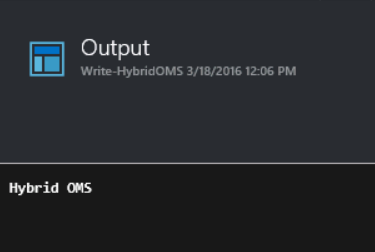
**Step 5** **– Start a Runbook**

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

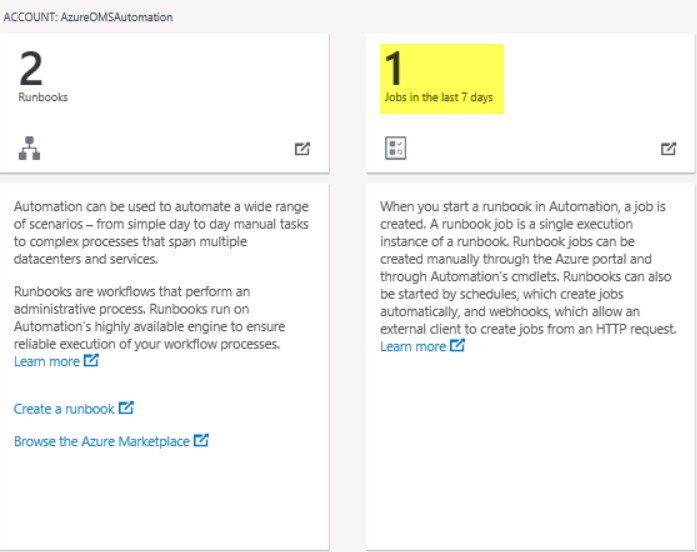
1. Login to your [SQL Server](https://www.starwindsoftware.com/new-microsoft-storage-best-practices-for-hyper-v-and-sql-server-video)
2. Switch to Runbook blade in the Azure Portal, Click on **Write-HybridOMS**
3. In the **Write-HybridOMS** blade, Click **Start**.
4. In the Start Runbook blade, click **OK**.

When the runbook starts, a job pane is opened for the runbook job that you just created. The job status is shown in Job Summary and matches the statuses that you saw when you tested the runbook.

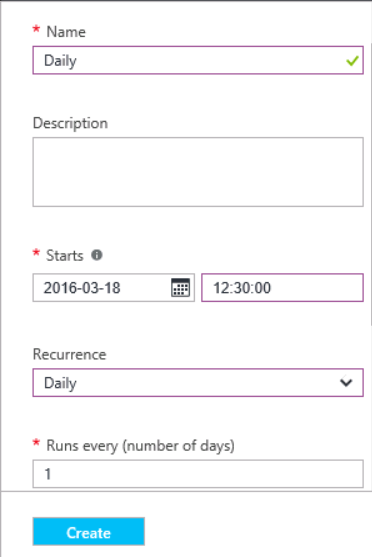
1. When the job completed, click **Output**.
2. The Output blade is opened; you can see **“*Hybrid OMS”*** as shown in the following screenshot

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/75.png)

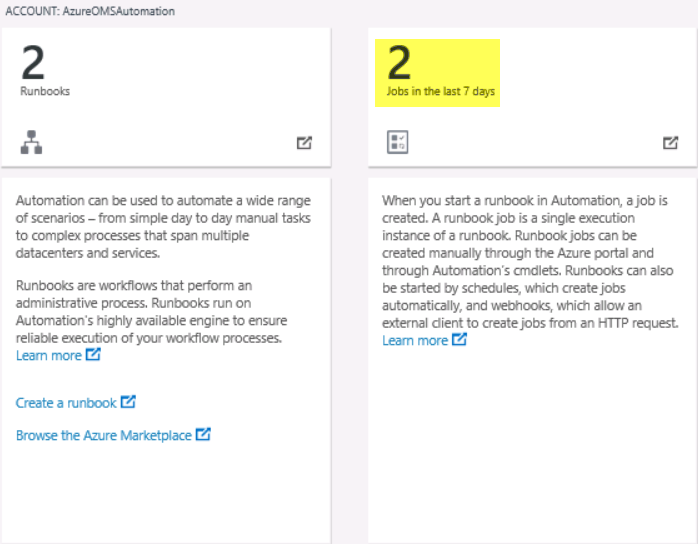
1. Close the Output blade and the Job blade.
2. Switch to the OMS Portal and click on the **Overview** In the Automation tile, “Jobs in the last 7 days” will have increased by 1 as shown in the following screenshot.

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/84.png)

1. Switch to the Job blade in the Microsoft Azure Portal.
2. Close the Job blade.
3. In the **Write-HybridOMS** blade, click **Schedule**.
4. In the Schedule Runbook blade, click **Link a schedule to your runbook**.
5. Click **+Create a new schedule**.
6. In Name, type **Daily**.
7. 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.
8. From the Recurrence drop-menu, select **Daily**.
9. Click **Create.**

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/94.png)

1. 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, so the total will be 2 as shown below:

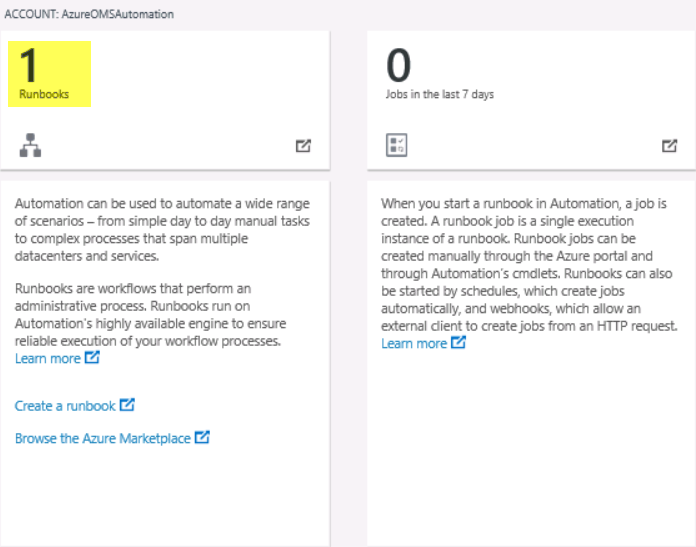
[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/103.png)

1. Leave the Microsoft Azure portal window open for the next steps.

**Step 6** **– Delete a Runbook**

In this step, we will delete a runbook.

1. Login to your SQL Server machine.
2. Sign in to Operations Management Suite Portal at [http://www.microsoft.com/en-us/server-cloud/operations-management-suite/overview.aspx](https://www.microsoft.com/en-us/cloud-platform/operations-management-suite)
3. Switch to the OMS Portal, OMS **Automation**
4. Click the **Runbooks** [Microsoft Azure Portal](https://portal.azure.com/) will open.
5. Select **Write-HybridOMS**.
6. In the **Write-HybridOMS** blade, click **Delete** and click **Yes**. The runbook is removed from the list of Runbooks.
7. Switch to the OMS Portal and lick the **Overview** In the Automation tile, the number of runbooks is reduced by 1.

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/1110.png)

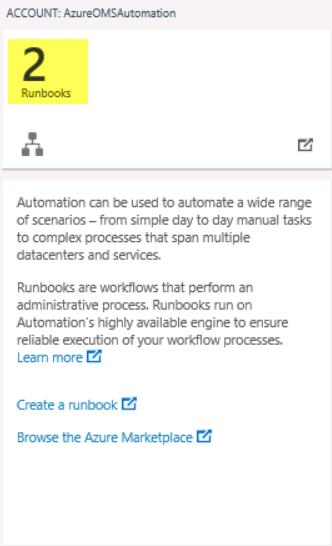
**Step 7** **– Import a Workflow to an OMS Runbook**

In this step, we will import an existing workflow from the Microsoft Marketplace.

1. Login to your [SQL Server](https://www.starwindsoftware.com/the-high-availability-features-in-sql-server-2016-standard-edition)
2. Sign in to Operations Management Suite Portal at [http://www.microsoft.com/en-us/server-cloud/operations-management-suite/overview.aspx](https://www.microsoft.com/en-us/cloud-platform/operations-management-suite)
3. Click the **Automation** tile and note the number of Runbooks, we have one runbook.
4. Click **Runbooks**. [Microsoft Azure Portal](https://portal.azure.com/) will open.
5. On the Dashboard blade, click **AzureOMSAutomation**.
6. Under **Resources**, click
7. On the Runbooks blade, click **Browse gallery**. Note that a larger number of runbooks are available from this location, as runbooks provided by community members are included in this view.
8. In the Search box, type **Create**.
9. In the results, click **Create a new Virtual (VM) on Azure**. Note that you can preview the contents of the runbook.

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/123.png)

1. In the Create a new Virtual Machine (VM) on Azure blade, click **Import**.
2. In the import blade, click **OK**.
3. Close open blades to return to the **Runbooks**
4. Click **New-AzureVMSample**.
5. In the **New-AzureVMSample** blade, click **Edit**. Note additional parameters are required for this runbook. Due to the fact that this is a new Azure environment, we have not yet created the virtual network necessary in Azure to support the creation of Virtual Machines.
6. In the Runbook blade, click **Publish** and click **Yes**.
7. Close the Azure Portal.
8. In the OMS Portal, click the **Overview** Note the Automation tile, “Runbook” has increased by 1.

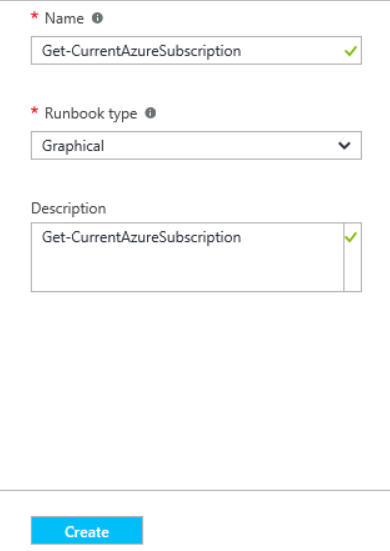
[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/132.png)

**Creating a Graphic-Style Runbook**

In this section, we will create a simple graphic-style runbook designed to obtain Azure Subscription information.

**Step 1** **– Create a Graphical Runbook**

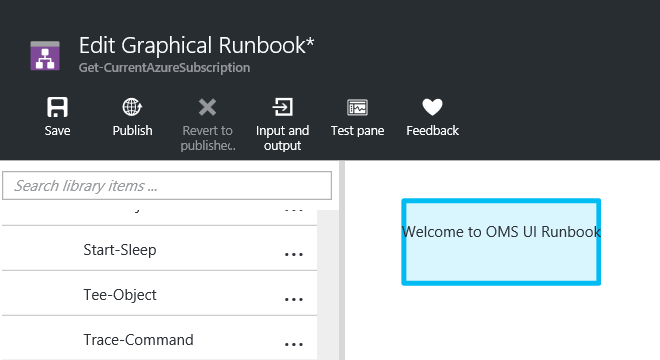
In this step, we will create a new graphical runbook.

1. Login to your SQL Server machine.
2. Sign in to Operations Management Suite Portal at [http://www.microsoft.com/en-us/server-cloud/operations-management-suite/overview.aspx](https://www.microsoft.com/en-us/cloud-platform/operations-management-suite)
3. Click the **Automation**
4. Click **Create** **a** **Runbook**. [Microsoft Azure Portal](https://portal.azure.com/) will open.
5. On the Dashboard, click **AzureOMSAutomation**.
6. Under **Resources**, click
7. In the Azure Portal, in the Runbooks blade, click **+Add a runbook**.
8. Select **Create a new runbook**.
9. In the Name, type **Get-CurrentAzureSubscription**.
10. From the Runbook type drop-down menu, select **Graphical**. [](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/142.png)
11. Click **Create**.

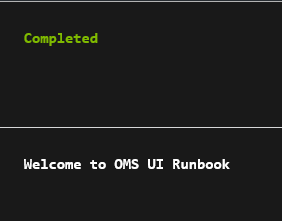
**Step 2** **– Add Activities to a Graphical Runbook**

In this step, we will use Library controls to add activities to the runbook.

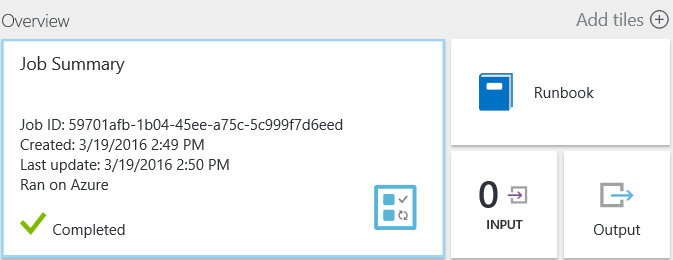
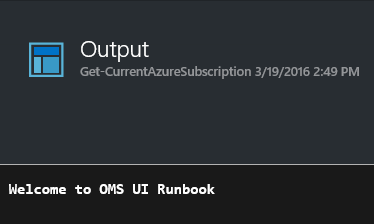
1. In the Azure Portal, in the Runbooks blade, click on **Get-CurrentAzureSubscription**
2. In the **Get-CurrentAzureSubscription** blade, click on **Edit**.
3. In the Library control, expand **Cmdlets** | **PowerShell.Utility**.
4. Scroll down to the bottom of the list, right-click **Write-Output**, and click **Add to canvas**.
5. Click on the **Write-Output** activity on the canvas. This opens the Configuration control which allows you to configure the activity.
6. Change the label to **Welcome to OMS UI Runbook**.
7. Click **Parameters** to provide values for the cmdlet’s parameters.
8. Select the **InputObject** This is the parameter where we will specify the text to send to the output stream.
9. In the Data source dropdown, select **PowerShell expression**.
10. In the Expression box, type **“Welcome to OMS UI Runbook”** (including the double quotes) and then click **OK** twice to return to the canvas.

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/152.png)

1. Save the runbook by clicking **Save**.
2. Click **Test pane**.
3. Click **Start**.
4. When the runbook job completes, its output is displayed. In this case, you should see ***Welcome to OMS UI Runbook***.

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/162.png)

1. Close **Test**
2. In the Edit Graphical Runbook **Get-CurrentAzureSubscription** blade, click **Publish**.
3. In the **Get-CurrentAzureSubscription** blade, click **Start** and click **Yes**.
4. Once the runbook status shows Completed, click **Output**. The Output pane is opened, and you can see ***Welcome to OMS UI Runbook***.

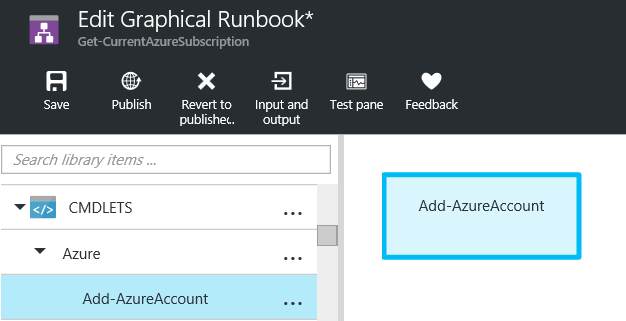
[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/172.png) [](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/182.png)

1. Close the **Output**
2. Click **All Logs** to open the Streams pane for the runbook job. You should only see Hello World in the output stream, but this can show other streams for a runbook job such as Verbose and Error if the runbook writes to them.
3. Close the Streams pane and the Job pane to return to the **Get-CurrentAzureSubscription**
4. Click **Jobs** to open the Jobs pane for this runbook. This lists all of the jobs status created by this runbook. You can click on any job to open it. This allows you to go back in time and view the details of any job that was created for a particular runbook.
5. Close the **Jobs**

**Step 3** **– Add Authentication to Manage Azure resources**

In this step, we will use the **Add-AzureAccount** cmdlet to allow the runbook to authenticate in order to manage Azure resources.

1. In the Azure Portal, in the Runbooks blade, click on **Get-CurrentAzureSubscription**
2. In the **Get-CurrentAzureSubscription** blade, click on **Edit**.
3. Right-click on **Welcome to OMS UI Runbook** and select Delete.
4. In the Library control, expand **Cmdlets | Azure**.
5. Right-click **Add-AzureAccount** and click **Add to canvas**.
6. Select **Add-AzureAccount**.
7. In the Configuration pane, click **Configure Parameters**. **Add-AzureAccount** has multiple parameter sets, so you need to select one before you can provide parameter values.
8. Click **Choose a Parameter set** and select the **User** parameter set. Once you select the parameter set, the parameters are displayed in the Activity Parameter Configuration pane.
9. Under Parameter set, click **Credential**.
10. From the Data source drop-down menu, select **Credential asset**.
11. Select **Credential asset** and click the **OMS Account** you created earlier in **Part I**.
12. Click **OK** twice to return to the canvas.

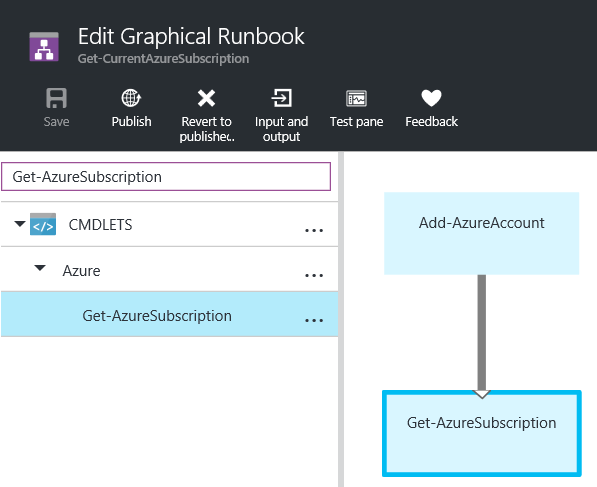
[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/192.png)

1. Click **Save**.

**Step 4** **– Add Activity to Graphical Runbook**

In this step, you will add a **Get-AzureSubscription** activity to your Runbook.

1. In the Azure Portal, in the Runbooks blade, click on **Get-CurrentAzureSubscription**
2. In the **Get-CurrentAzureSubscription** blade, click on **Edit**.
3. Under **Cmdlets | Azure**, right-click **Get-AzureSubscription** and click **Add to canvas**.
4. Click and drag **Get-AzureSubscription** underneath **Add-AzureAccount**.
5. Hover over **Add-AzureAccount** until a circle appears on the bottom of the shape.
6. Click the circle and drag the arrow to **Get-AzureSubscription**. The arrow that you just created is a link. The runbook will start with **Add-AzureAccount** and then run **Get-AzureSubscription**.
7. Click **Get-AzureSubscription** and click **Configure Parameters**.
8. Click **Choose a Parameter set** and click **ByName**.
9. Select **SUBSCRIPTIONNAME**.
10. From the **Data source** drop-down menu, select **Credential asset** and click the **OMS Account** you created earlier in **Part I**.
11. Click **OK** twice to return to the canvas.

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/202.png)

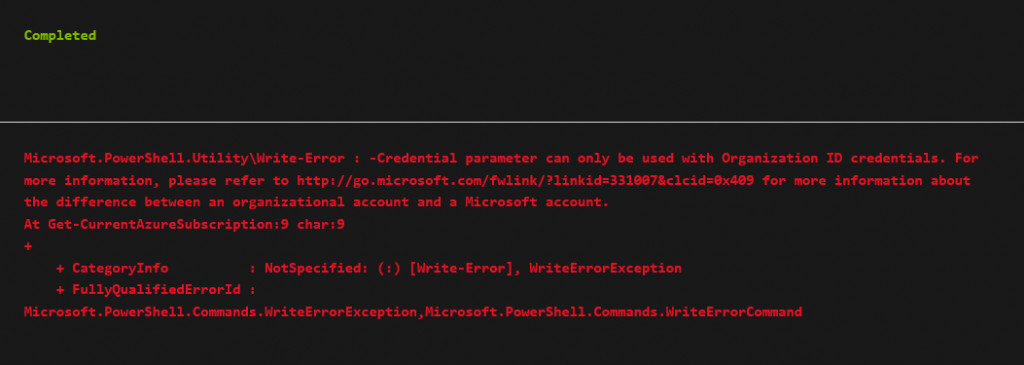
1. Click **Save**.

**Step 5** **– Finalize Your Graphical Runbook**

In this step, we will test, run and publish the graphical runbook.

1. In the Azure Portal, in the Runbooks blade, click on **Get-CurrentAzureSubscription**
2. In the **Get-CurrentAzureSubscription** blade, click on **Edit**.
3. Click **Test pane**.
4. Click **Start**.

*Note: The job will run with the following expected error. The error is produced because you are using a Microsoft account during this clinic. Credential asset can only be used with an Organizational account.*

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/219.png)

1. Close the **Test pane** to return to the canvas.
2. Close the **Edit** In production environment, you would edit the runbook to use your organizational account credentials, re-test the runbook, and then publish it.

## ****Performing Log Analytics with OMS****

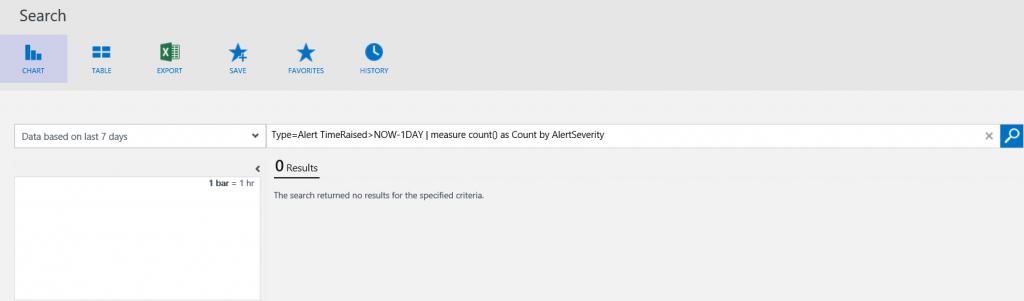
### Using OMS Search

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

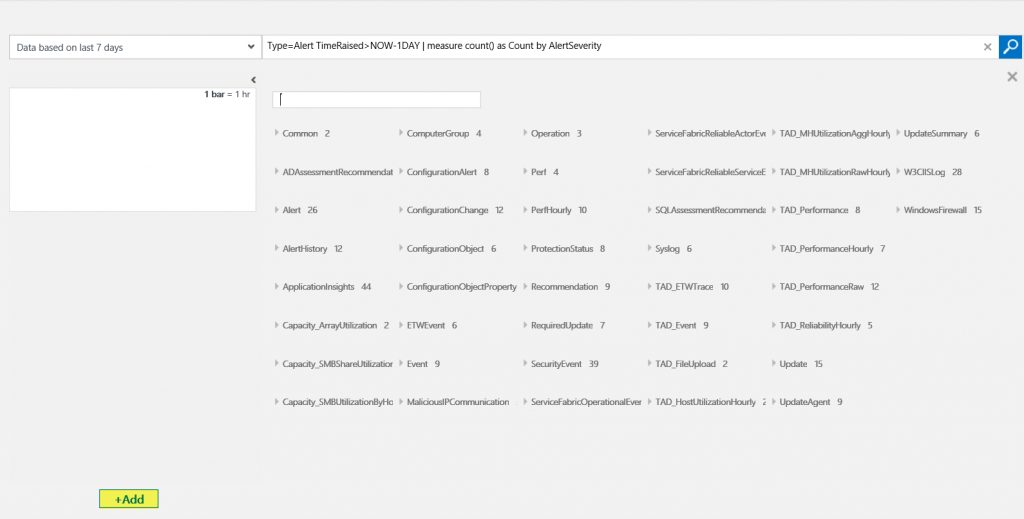
**Step 1** **–** **Examine OMS Search Capabilities and Syntax**

In this step, we will explore the basics of the OMS Log Search feature.

1. Login to your [SQL Server](https://www.starwindsoftware.com/the-high-availability-features-in-sql-server-2016-standard-edition)
2. Sign in to Operations Management Suite Portal at <https://www.microsoft.com/en-us/cloud-platform/operations-management-suite>
3. In the OMS Portal, On the OMS Overview blade, click **Log Search**.
4. Click the down arrow next to **Data based on last 7 days**. Note that you can scope searches by 6 hours, 1 day, 7 days or Custom.
5. Click **OK**.
6. On the right side of the blade next to **SHOW QUERIES**, click **ON**.
7. Under “Saved Searches” locate the **Alert Management** category and click **Alerts raised during the past 1 day grouped by their severity**. The left side of the blade is called the Facet Panel. It uses context to pre-populate appropriate areas for further drill-down. This panel contents change based upon the ongoing selections made during drill-down exploration.

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/124.png)

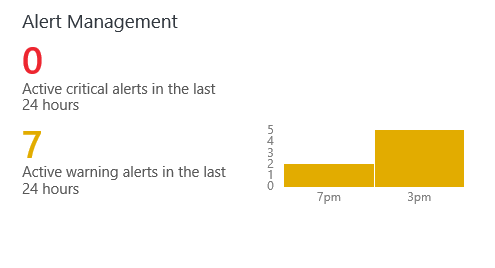
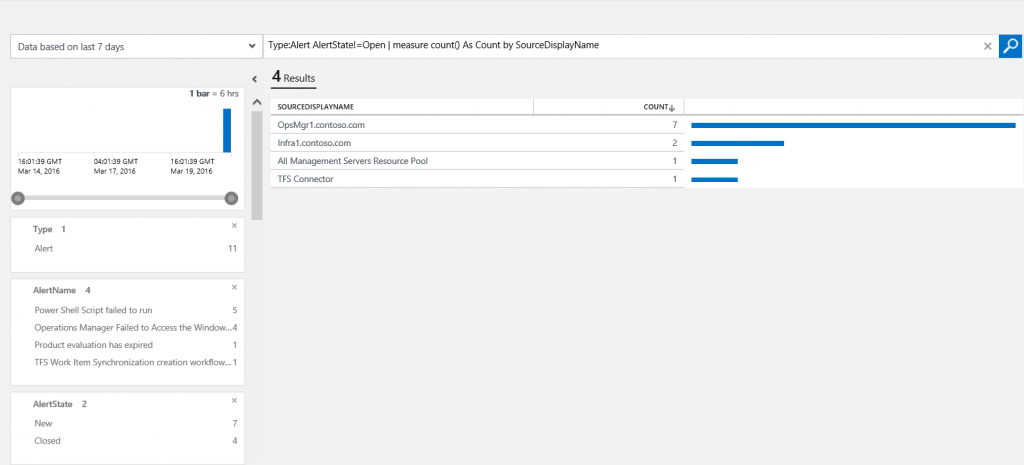
1. In the diagram at the top of the Facet Panel, hover over a bar. A pop-up will display the time frame under which the associated alerts were gathered.
2. Click on a bar to display data based on that custom time range.
3. Scroll through the Facet Panel to become familiar with the data being displayed.
4. Click **+Add**.
5. Review the items that can be added to the Facet Panel.

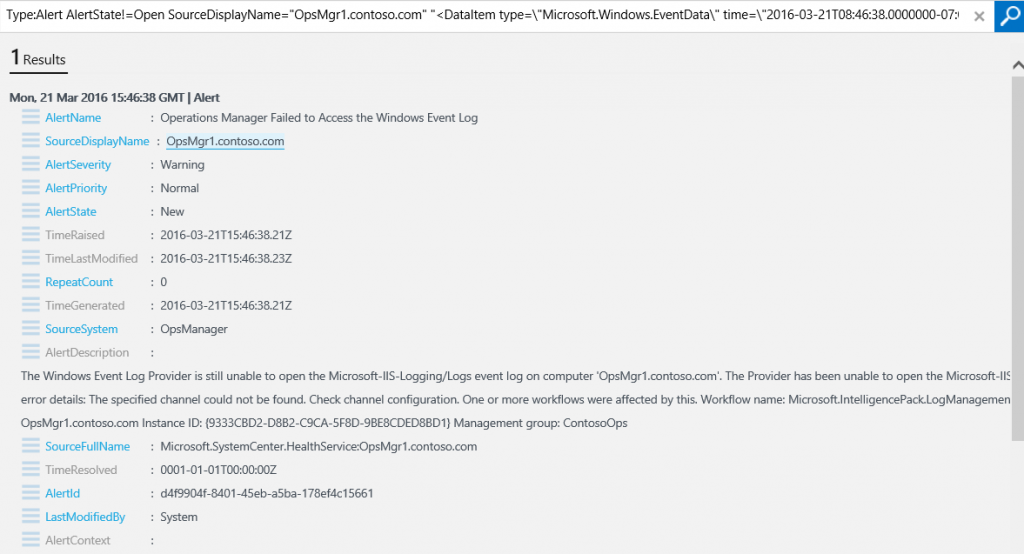
[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/220.png)

1. Close the **Add**

**Step 2** **– Examine Alert Data**

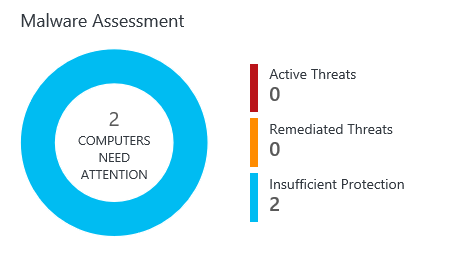
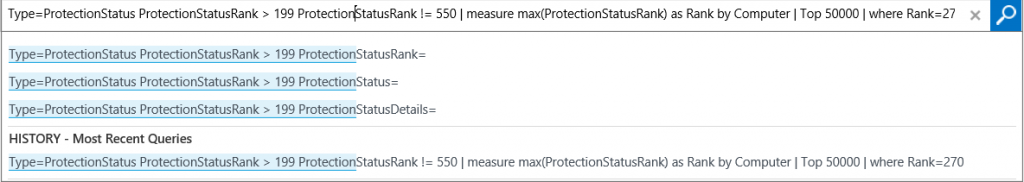
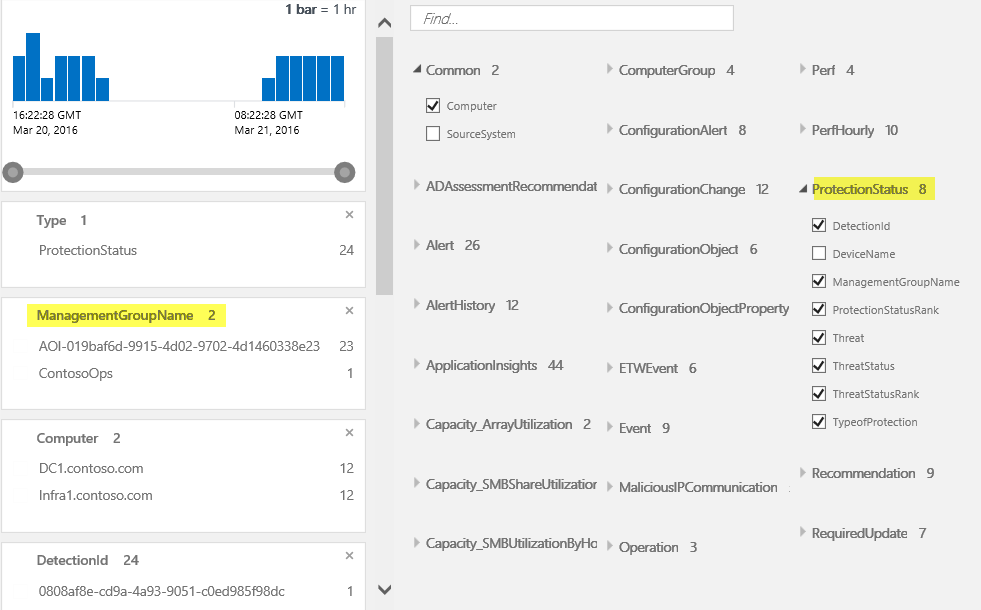
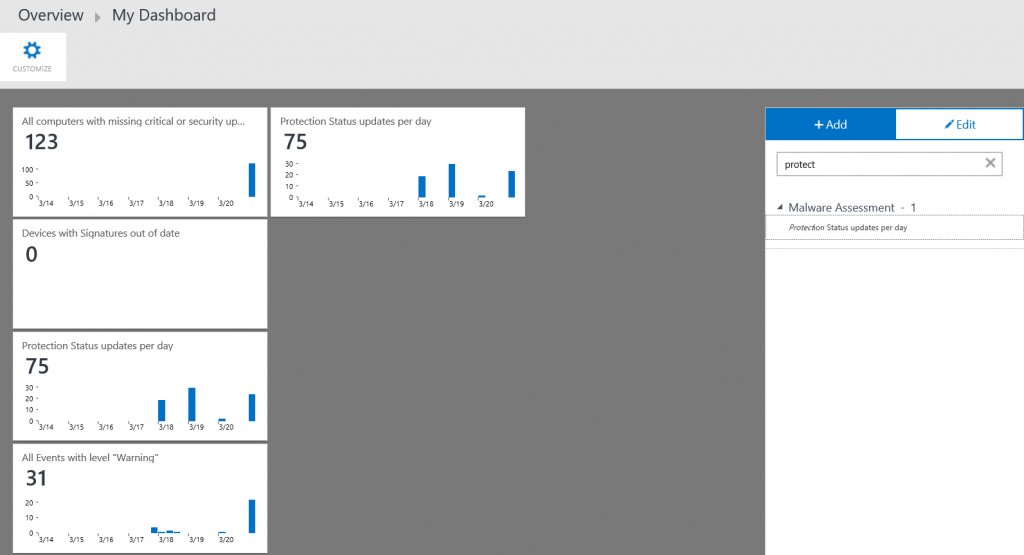
In this step, we will use OMS Search to drill down into data produced by the Alert Management Solution.

1. Login to your [SQL Server](https://www.starwindsoftware.com/save-10kon-sql-deployment-in-microsoft-azure)
2. Sign in to **Operations Management Suite Portal** at [http://www.microsoft.com/en-us/server-cloud/operations-management-suite/overview.aspx](https://www.microsoft.com/en-us/cloud-platform/operations-management-suite)
3. In the OMS Portal, Click the **Overview**
4. Click the **Alert Management                                    [](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/38.png)**
5. Under “ACTIVE ALERTS”, under the **Active out of xxx Critical Alerts Raised** tile, click **SEE ALL**.
6. Note the query string is searching for all alerts where the Alert State is Closed. Edit the query to change the Alert State to **Open** and click the **Search** icon as shown in the following screenshot. [](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/49.png)
7. In the Facet Panel under **AlertName**, click on the top alert.
8. In the result pane, click the top result.
9. Under the top alert, click **[+] show more**.
10. Note the various types of data provided. As you can see in the following screenshot, you know the source of the alert, the time it occurred, and other details of the alert. This information can be used as a starting point for troubleshooting.

**[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/56.png)**

**Step 3** **– Examine Malware-Related Data**

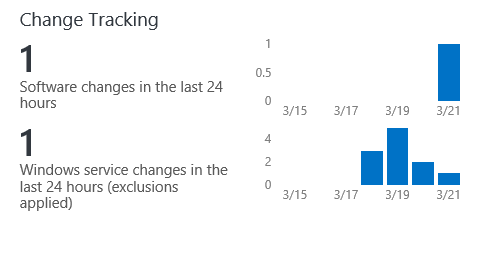
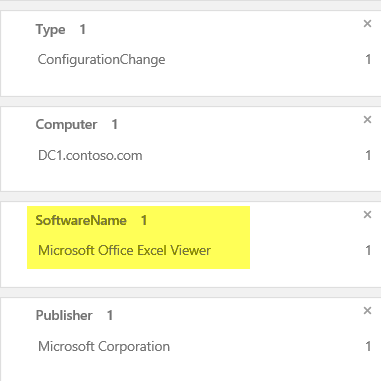
In this step, we will use OMS Search to drill down into data produced by the Malware Assessment Solution.

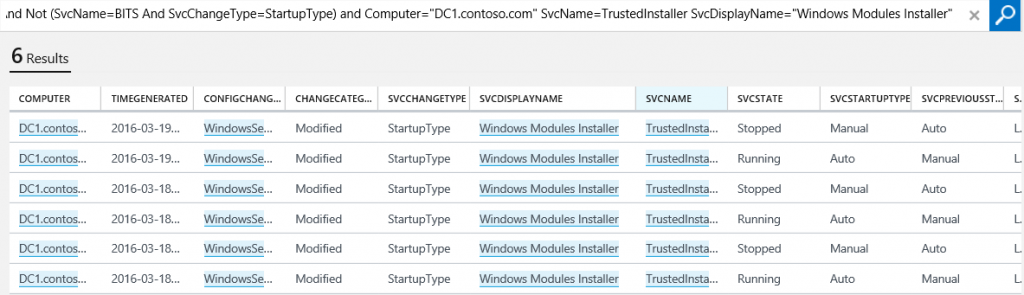
1. Login to your [SQL Server](https://www.starwindsoftware.com/critical-sql-server-databases-provide-ha-with-sql-server-failover-clustering)
2. Sign in to Operations Management Suite Portal at [http://www.microsoft.com/en-us/server-cloud/operations-management-suite/overview.aspx](https://www.microsoft.com/en-us/cloud-platform/operations-management-suite)
3. In the OMS Portal, Click the **Overview**
4. Click the **Malware Assessment                                       [](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/66.png)**
5. Under “PROTECTION STATUS”, click **No Real Time Protection**.
6. 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.
7. 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. [](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/76.png)
8. At the bottom of the Facet Panel, click **+Add**.
9. 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. [](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/85.png)
10. Edit the query to delete “DeviceName=’DC1.contoso.com’ and click the **Search**
11. Click **Save**.
12. In the name field, type **Protection Status by Device.**
13. In the Category field, type **Security and Audit**.
14. Click **Save**.
15. At the bottom of the page, click **HISTORY**. On the right side of the Search blade, previous searches are displayed and can be executed again.
16. Click **Favorites** and note that the Saved Searches displays on the right side of the blade.
17. In the Saved Searches query box, type **Protection Status**. Notice your saved search appears in the results.
18. Click the **Overview**
19. Click the **My Dashboard**
20. Click **Customize**.
21. Click the Find search box and type **Protect**.
22. Click and drag the **Protection Status by Device** saved the search to My Dashboard. [](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/95.png)
23. Click **Customize**.

|  |  |
| --- | --- |
| https://www.starwindsoftware.com/blog/wp-content/uploads/2017/02/xStarWind-Virtual-SAN-300x300.png.pagespeed.ic.zu0zybGxdM.png | **StarWind Virtual SAN** eliminates any need for physical shared storage just by mirroring internal flash and storage resources between hypervisor servers. Furthermore, the solution can be run on the off-the-shelf hardware. Such design allows StarWind Virtual SAN to not only achieve high performance and efficient hardware utilization but also reduce operational and capital expenses. |
| Learn more about [StarWind Virtual SAN](https://www.starwindsoftware.com/starwind-virtual-san). |

**Step 4** **– Examine Data Related to Software and Service Changes**

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

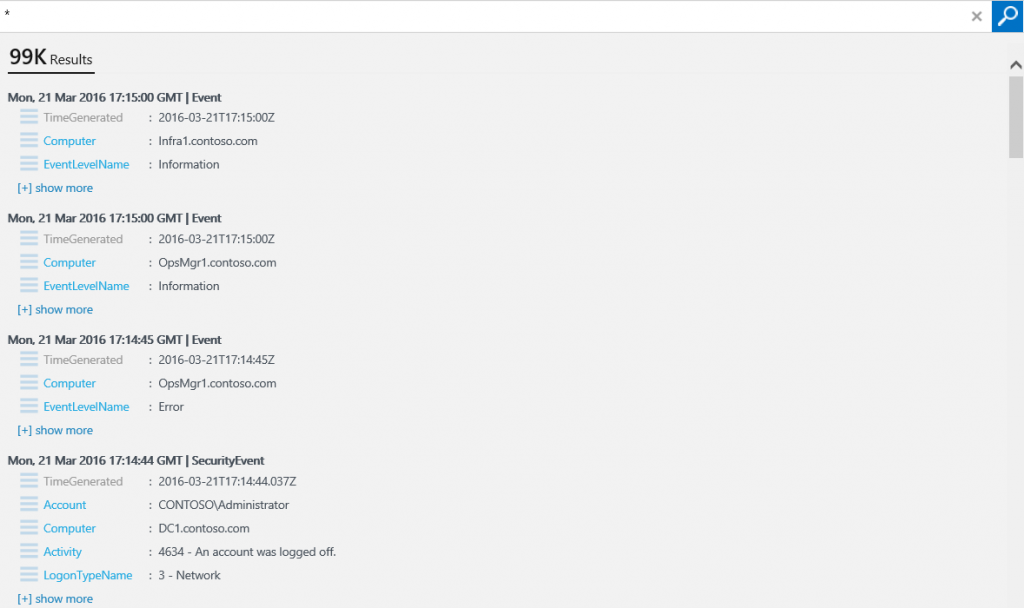
1. Login to your [SQL Server](https://www.starwindsoftware.com/new-microsoft-storage-best-practices-for-hyper-v-and-sql-server-smb-3-0-video)
2. Sign in to Operations Management Suite Portal at [http://www.microsoft.com/en-us/server-cloud/operations-management-suite/overview.aspx](https://www.microsoft.com/en-us/cloud-platform/operations-management-suite)
3. In the OMS Portal, Click the **Overview**
4. Click the **Change Tracking                                         [](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/104.png)**
5. Under SOFTWARE CHANGES, click **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 the 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 IT administrators.                                                               [](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/1111.png)
6. Click the back arrow in your browser window to return to the Change Tracking solution.
7. Under **WINDOWS SERVICE CHANGES**, click **contoso.com**.
8. 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.

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/125.png)

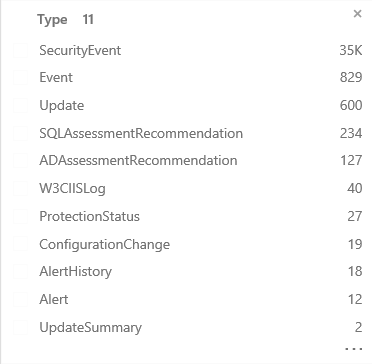
**Step 5** **– Examine Update Data in OMS**

In this step, we will investigate the types of data OS captures with OMS.

1. Login to your [SQL Server](https://www.starwindsoftware.com/new-microsoft-storage-best-practices-for-hyper-v-and-sql-server-video)
2. Sign in to Operations Management Suite Portal at [http://www.microsoft.com/en-us/server-cloud/operations-management-suite/overview.aspx](https://www.microsoft.com/en-us/cloud-platform/operations-management-suite)
3. In the OMS Portal, Click the **Overview**
4. Click the **Log Search**
5. In the query field, type **\*** and click **Search**. Note the number of associated logs and number of metrics are presented. At the time of writing this post, we have 99K associated logs.

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/133.png)

1. In the Facet Panel under **Type**, click **UpdateSummary**. This will filter the search to only Update-Summary related data.

[](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/143.png)

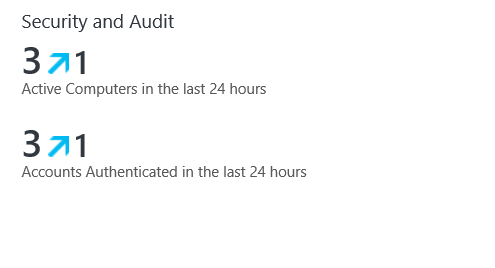
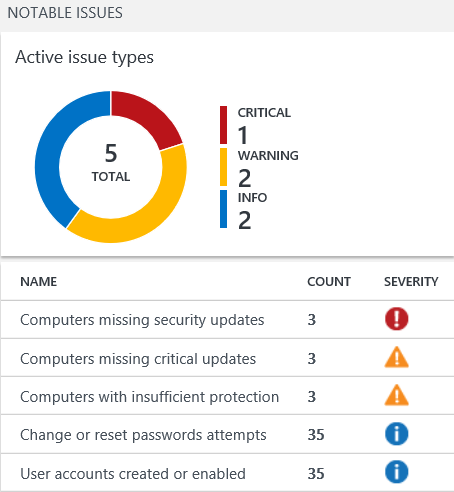
1. To the right of the graph for each solution, click on the **[+]** plus sign to expand the graph.
2. Drill down through the various items to see how they are displayed.

## ****Using the Security and Audit Solution in OMS****

In this section, we will explore the Security and Audit Solution in OMS.

**Step 1** **– Explore Security and Audit Solution Data**

In this step, we will explore common queries available through the Security and Audit solution.

1. Login to your SQL Server machine.
2. Sign in to Operations Management Suite Portal at [http://www.microsoft.com/en-us/server-cloud/operations-management-suite/overview.aspx](https://www.microsoft.com/en-us/cloud-platform/operations-management-suite)
3. In the OMS Portal, Click the **Overview** icon
4. Click the **Security and Audit** tile.                                 [](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/153.png)
5. Under “COMMON SECURITY QUERIES”, click **Logon Activity by Computer**.
6. In the Facet Panel, locate the Account facet and note the number of accounts that have logon activity. To display the entire list, click **…** at the bottom of the facet.
7. In the Account facet, click on **CONTOSO\DC1$**.
8. Scroll down to locate the **LogonTypeName** In a demo environment, you may only see “interactive” logon listed.
9. In the results pane, click **contoso.com**. Each individual logon activity is enumerated with its details.
10. 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.
11. Click the back arrow in Internet Explorer to return to the Security and Audit solution.
12. On the OMS Security and Audit Solution blade, under “NOTABLE ISSUES”, click **Computers missing security updates. [](https://www.starwindsoftware.com/blog/wp-content/uploads/2016/03/163.png)**
13. In the detail pane of Search results, click on **contoso.com**. Note all missing security updates on DC1.
14. Click **Save**.
15. In the Name field, type **Missing Updates on DC1**.
16. In the Category field, type **Security and Audit**.
17. Click **Save**.
18. To export search results, at the bottom of the Search page, click **Export**.
19. **Save** the **.csv** file to the desktop as **SearchResults**.
20. On the desktop, right-click **SearchResult**s and click **Open with**.
21. Select **ExcelViewer**.
22. Review the contents and close the viewer.

**Step 2** **– Use OMS Search to Investigate Suspicious Executables**

Please continue to explore the various types of data provided by OMS.

In the Security and Audit solution, under **NOTABLE ISSUES**, you can check **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 which user 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 file hash.

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.