Introduction

3 minutes

Imagine you are the server administrator for a regional fire department (RFD) covering dozens of stations. Your department has recently migrated their on-premises systems to the cloud; specifically, they've migrated existing servers to virtual machines hosted in Azure. The department has public-facing and private websites supporting email, patient records, and internal applications.

As a part of your effort to keep your infrastructure secure, you need to ensure that the virtual machines in your cloud environment are up-to-date with the latest security and critical updates.

You will learn about Azure Update Management. You will learn how to deploy Update Management to a virtual machine and how to schedule automatic deployment of critical and security updates.

Learning objectives

In this module, you will:

- Deploy Update Management to a virtual machine
- Schedule recurring security updates
- Schedule recurring critical updates

Prerequisites

- Experience administering Azure resources using the Azure portal

Note

You will need your own Azure subscription to complete the exercises in this module.

Next unit: Update Management solution on a virtual machine

Continue >

Update Management solution on a virtual machine

5 minutes

The Public Information Officer (PIO) in your department maintains a non-public facing website for use by the local media. Your PIO uses her mobile device to update content on the media website so that local media outlets can stay informed about current events. To prevent unauthorized or incorrect information being presented to the media, this site must be as secure as possible. As the administrator, one approach you can take to improve security is to keep the site current with the latest updates.

Here, we'll introduce the Update Management solution for Azure.

Update Management overview

The Update Management solution allows you to manage and install operating system updates and patches for both Windows and Linux virtual machines that are deployed in Azure, on-premises, or even in other cloud providers. You can assess the status of available updates on computers and manage the process of installing required updates for servers.

There are several advantages to the Update Management solution:

1. There are no agents or additional configuration within the virtual machine.
2. You can run updates without logging into the VM. You also don't have to create passwords to install the update.
3. The Update Management solution lists missing updates and provides information about failed deployments in an easy-to-read format.

Update Management can be used to natively onboard machines in multiple subscriptions in the same tenant. To manage machines in a different tenant, you must onboard them as non-Azure machines.

Supported Operating Systems

Update Management solution supports Windows and Linux, specifically:

- Windows Server (2008 and newer)
- CentOS 6 (x86/X64) and CentOS 7
- Red Hat Enterprise 6 (x86/x64) and 7 (x64)
- SUSE Linux Enterprise Server 11 (x86/x64) and 12 (x64)
- Ubuntu 14.04 LTS, 16.04 LTS and 18.04 (x86/x64)

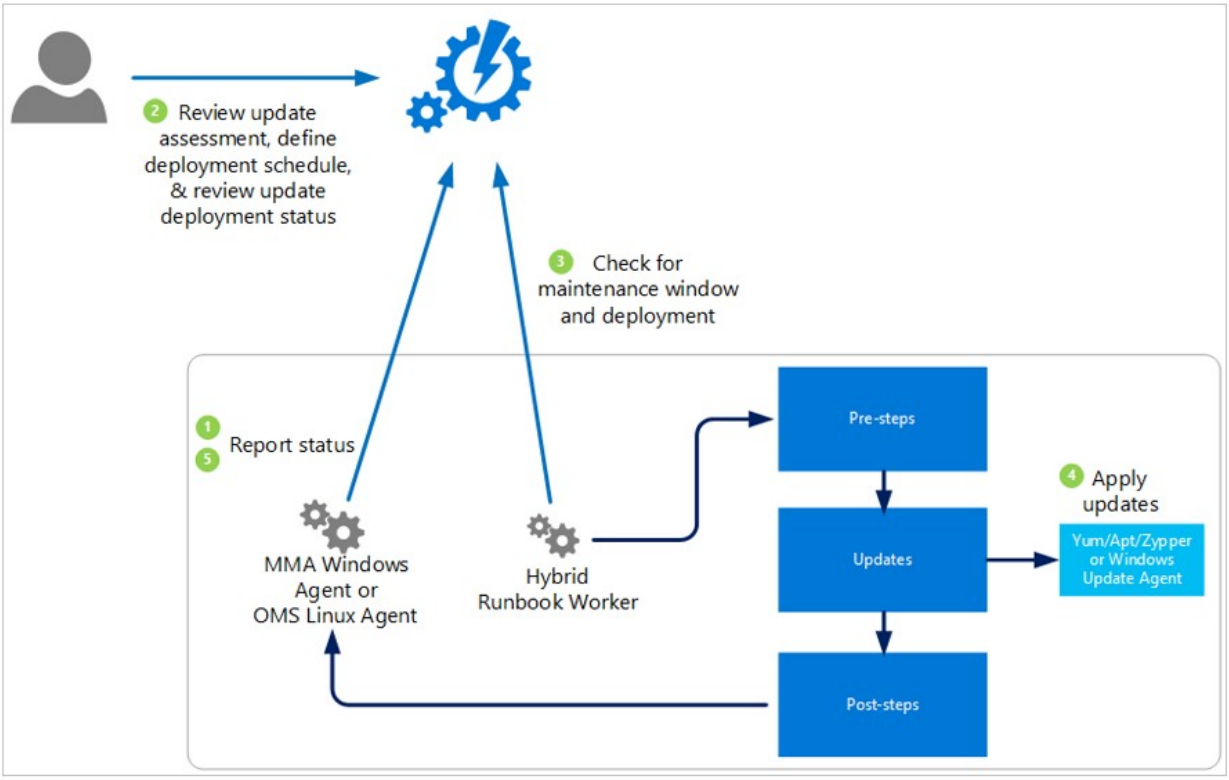
In this module, we'll work with Windows Server 2016 virtual machine deployed in Azure.

Components Used by Update Management

The following configurations are used to perform assessment and update deployments:

- Microsoft Monitoring Agent (MMA) for Windows or Linux.
- PowerShell Desired State Configuration (DSC) for Linux.
- Automation Hybrid Runbook Worker.
- Microsoft Update or Windows Server Update Services (WSUS) for Windows computers.

The following diagram shows a conceptual view of the behavior and data flow with how the solution assesses and applies security updates to all connected Windows Server and Linux computers in a workspace.



Hybrid Worker Groups

Windows computers that are directly connected to your Log Analytics workspace are automatically configured as a Hybrid Runbook Worker to support the runbooks that are included in this solution. Each Windows computer that's managed by the solution is listed in the Hybrid worker groups pane as a System hybrid worker group for the Automation account. The solutions use the naming convention Hostname FQDN_GUID.

Operations Manager Management Packs

If your System Center Operations Manager management group is connected to a Log Analytics workspace, the following management packs are installed in Operations Manager. These management packs are also installed on directly connected Windows computers after you add the solution. You don't need to configure or manage these management packs.

- Microsoft System Center Advisor Update Assessment Intelligence Pack
- Microsoft.IntelligencePack.UpdateAssessment.Configuration
- Update Deployment MP

Next unit: Exercise - Use Update Management on a virtual machine

Continue

100 XP

Exercise - Use Update Management on a virtual machine

12 minutes

Your PIO wants to set up a virtual machine to serve as a web resource for local media outlets. It is imperative that this virtual machine is as protected as it can be to prevent unauthorized access. As part of your security profile, you want to implement Update Management on this VM so that you can ensure that it is always up-to-date with the latest security patches.

Create a virtual machine

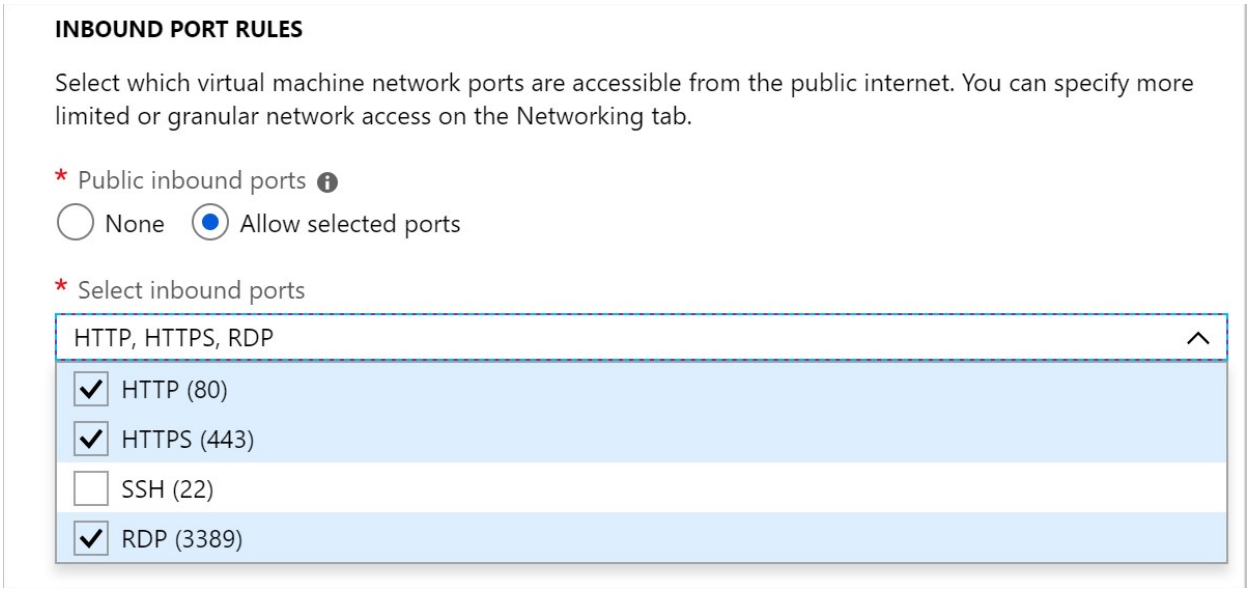
Here you will create a new virtual machine to serve as a web server for the local media.

1. Sign in to the Azure portal.
2. On the Azure portal menu or from the **Home** page, select **Create a resource**.
3. In the **New** pane, select **Windows Server 2016 Datacenter**.
4. Enter the following values in the **Create a virtual machine** window:

Field	Value
Subscription	*Select your Azure subscription*
Resource group	Create a new resource group named "mslearn-vmupdate"
Virtual machine name	MediaWebServer
Region	*Select the region nearest you*

Field	Value
Availability options	No infrastructure redundancy required
Image	Windows Server 2016 Datacenter
Size	Select **Change size** and select **B2s** from the list
Username	*Create a username of your choice and note it for later*
Password	*Create a password of your choice and note it for later*

5. In the **INBOUND PORT ROLES** section, choose **Allow selected ports** in the **Public inbound ports** field. Select HTTP, HTTPS, and RDP as shown below.



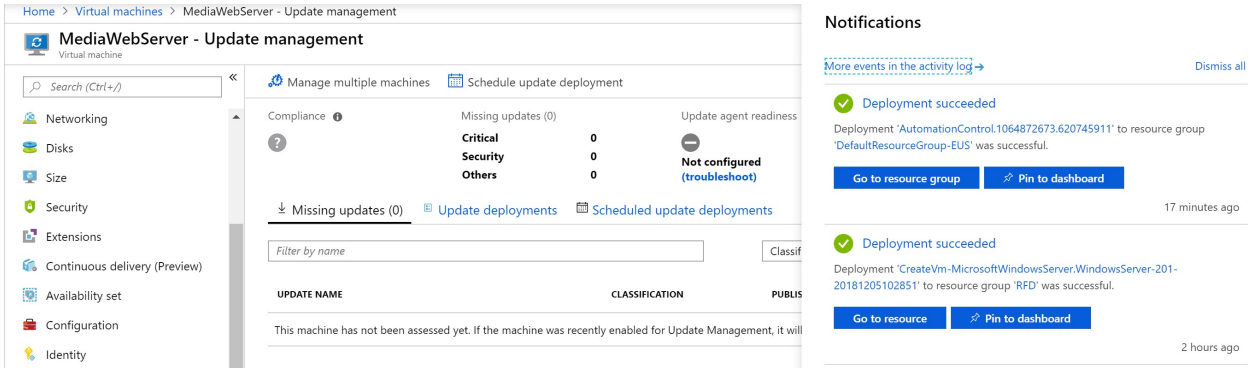
6. Select **Review + create** and then select **Create**. Wait for the VM to be created. You can select the Bell icon in the upper right corner of the portal to monitor the progress.

Onboard Update Manager to the VM

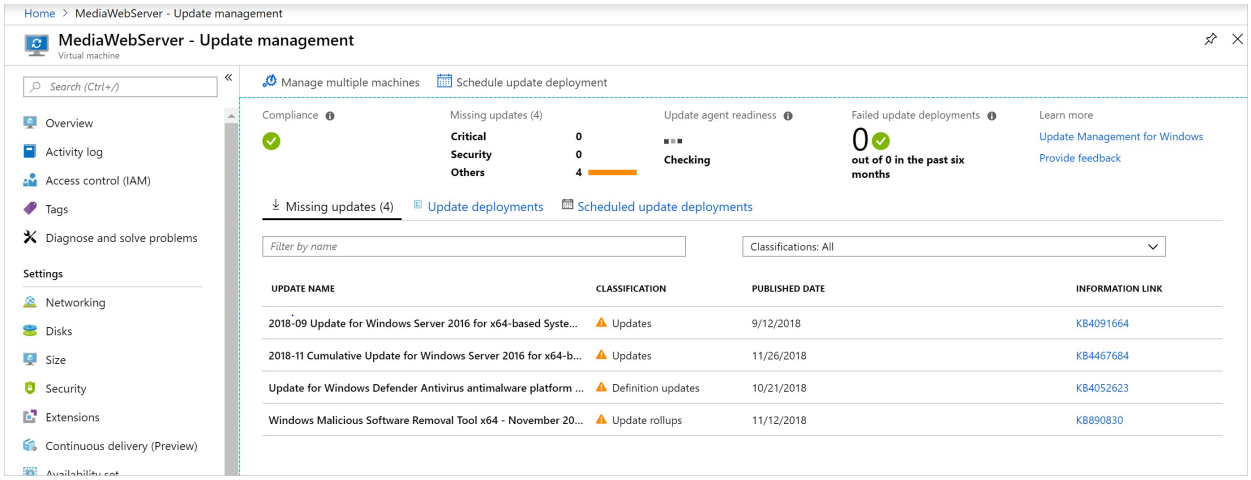
Here you'll enable Update Manager on the virtual machine you created.

1. In the left pane, select **Virtual machines**.

2. In the **Virtual machines** pane, select the virtual machine from the list. In this example, select **MediaWebServer**.
3. In the MediaWebServer pane, scroll down the list to **Operations**, and then select **Update management**.
4. In the **Update Management** pane, ensure that the **Enable for this VM** radio button is selected. Note that a default **Log Analytics workspace** and **Automation account** will be created. Accept the remaining defaults, and then select **Enable**.
5. In the upper left corner, select the Notification bell and wait for deployment to finish.
6. When Update Management deployment has completed, the Update Management menu will appear as shown below.



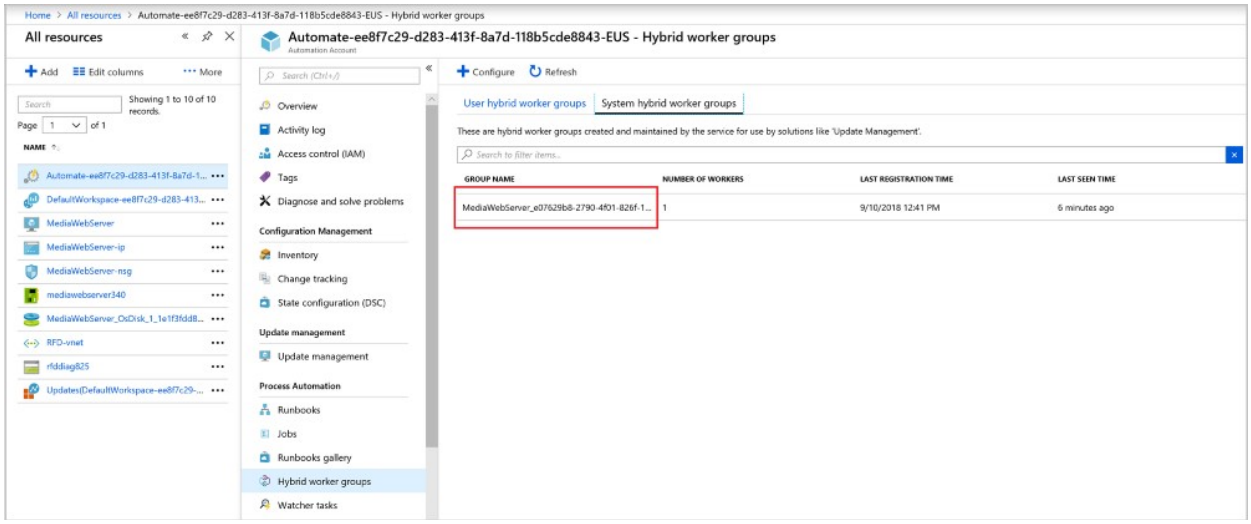
7. Wait for at least 15 minutes while Update Management configures the virtual machine.
8. When Update Management configuration is complete, the Update Management pane will appear as shown below.



9. **Compliance** is now complete, that the **Failed update deployments** counter is now configured, and that in this example, Update Management has identified that there is a Cumulative Update for Windows Server available. To the right of the notification of the Cumulative Update, under **INFORMATION LINK** that there is a link to the knowledge base article for this Cumulative Update.

Examine Hybrid Worker Groups

1. On the Azure portal menu or from the **Home** page, select **All resources**.
2. In the **All resources** pane, examine the **TYPE** column to find the resource of type **Automation Account**, and then select the Automation account.
3. In the Automation account pane, scroll down to the **Process Automation** section and in there, select **Hybrid worker groups**.
4. In the Hybrid worker groups pane, select the **System hybrid worker groups** tab.
5. The virtual machine you created is listed as shown below.



Next unit: Verify agent connectivity and schedule recurring updates

Continue >

Verify agent connectivity and schedule recurring updates

5 minutes

In addition to a public facing web site, the department uses web sites for in-house content such as dispatch and patient care records. These sites must be as secure as possible.

Here, you'll learn how to assess agent connectivity, and schedule a recurring update.

Components used by Update Management

The following configurations are used to perform assessment and update deployments:

- Microsoft Monitoring Agent (MMA) for Windows or Linux.
- PowerShell Desired State Configuration (DSC) for Linux.
- Automation Hybrid Runbook Worker.
- Microsoft Update or Windows Server Update Services (WSUS) for Windows computers.

Compliance scan

Update Management will perform a scan for update compliance. A compliance scan is by default, performed every 12 hours on a Windows computer and every 3 hours on a Linux computer. In addition to the scan schedule, a compliance scan is initiated within 15 minutes if the MMA is restarted, before update installation, and after update installation. After a computer performs a scan for update compliance, the agent forwards the information in bulk to Azure Log Analytics.

It can take between 30 minutes and 6 hours for the dashboard to display updated data from managed computers.

Recurring Updates

You can create a scheduled and recurring deployment of updates. With scheduled deployment you can define what target computers receive the updates, either by explicitly specifying computers or by selecting a computer group that's based on log searches of a specific set of computers. You also specify a schedule to approve and designate a period of time during which updates can be installed.

Updates are installed by runbooks in Azure Automation. You can't view these runbooks, and the runbooks don’t require any configuration. When an update deployment is created, the update deployment creates a schedule that starts a master update runbook at the specified time for the included computers. The master runbook starts a child runbook on each agent to perform installation of required updates.

Next unit: Exercise - Use azure log analytics and schedule updates

Continue

100 XP

Exercise - Use azure log analytics and schedule updates

8 minutes

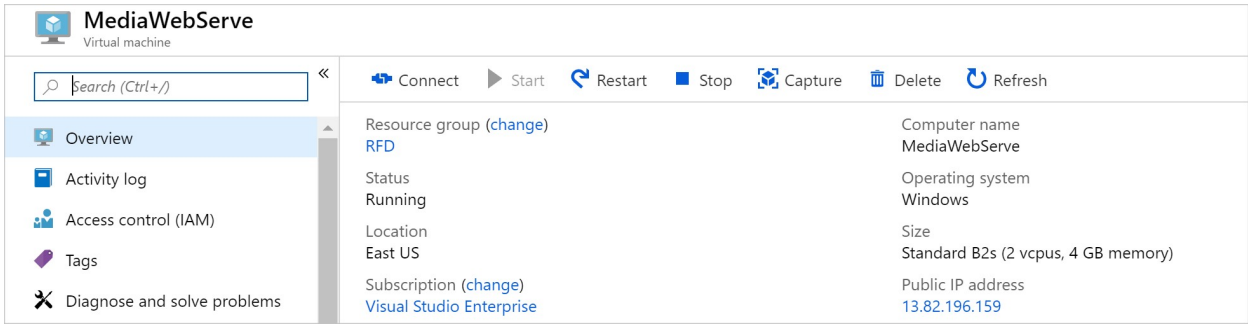
Recently your department moved all of their infrastructure to Azure. There are many VMs serving up web sites and email functions. You have been tasked to keep these VMs up-to-date with the latest patches and security releases. You decide to roll out the Update Management solution to all of the VMs in your enterprise.

In the following exercise you will review the agent connectivity to log analytics and, learn how to schedule update deployments.

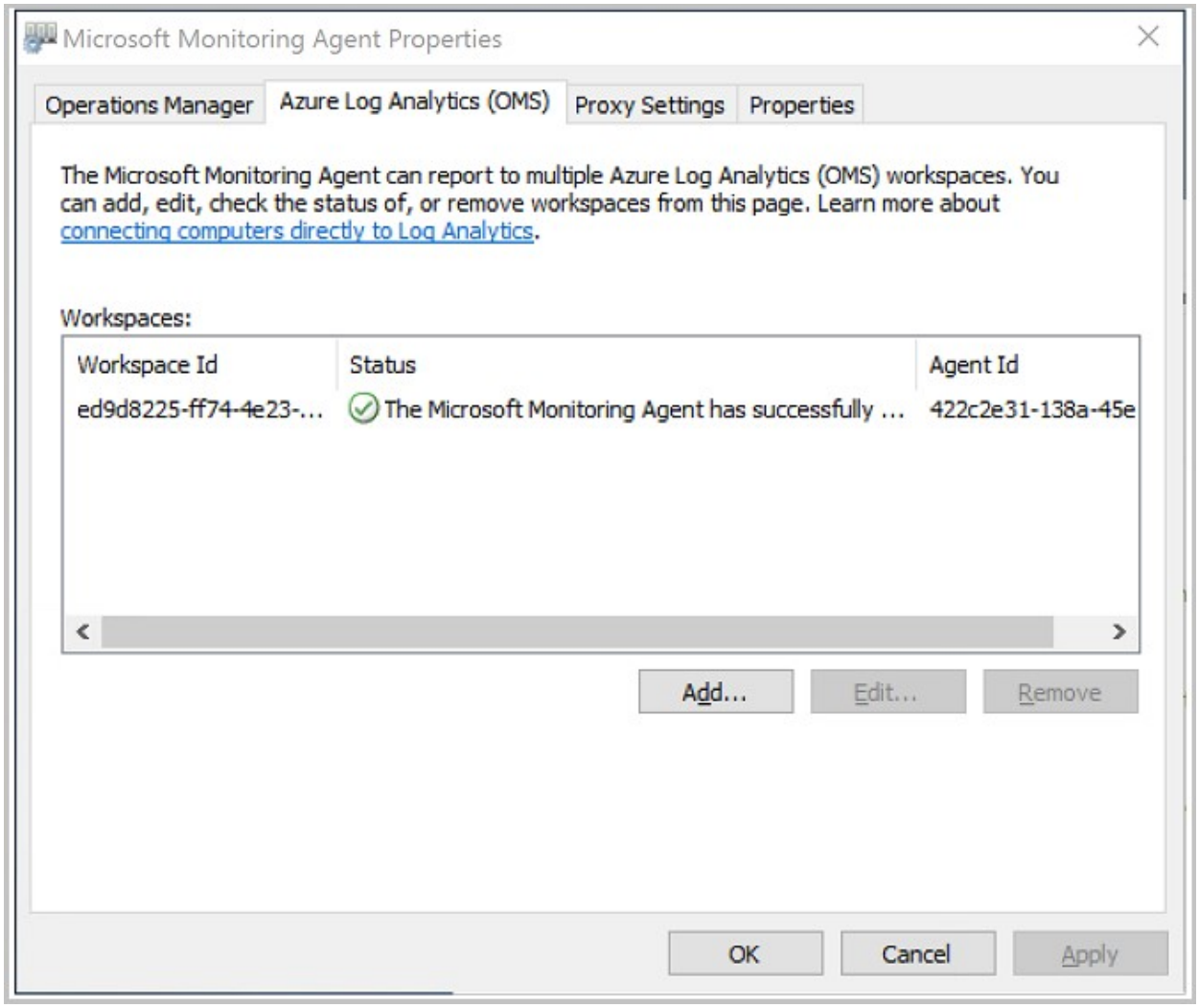
Review Agent Connectivity to Log Analytics

Perform the following steps in the Azure portal to assess if connectivity between the agent and log analytics has taken place. Start by signing into the Azure portal using the same account with which you activated the sandbox.

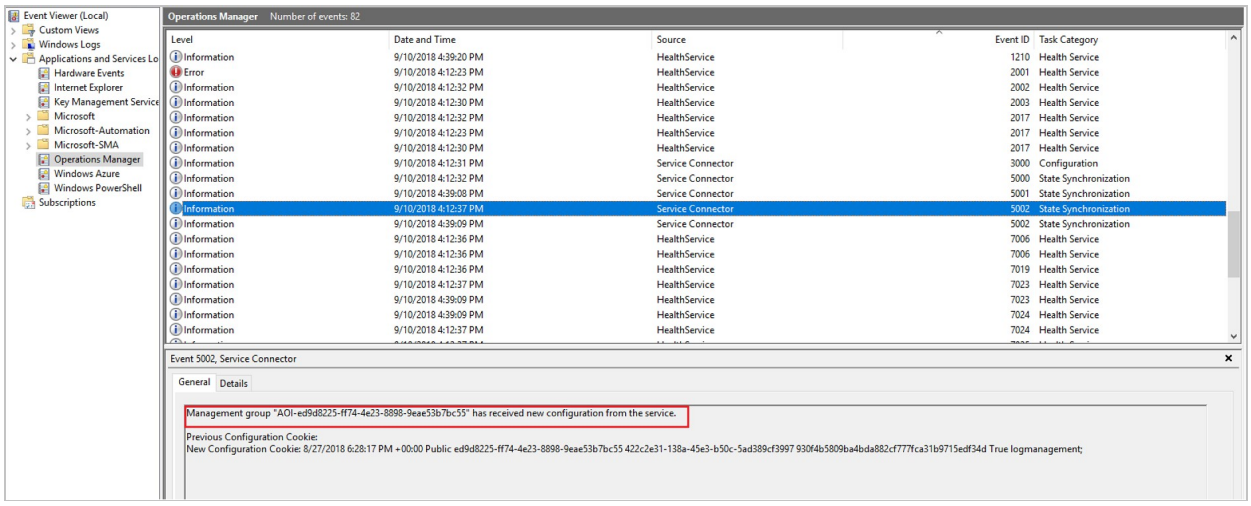
1. On the Azure portal menu or from the **Home** page, select **Virtual machines** option in the left pane and select on the newly created virtual machine.
2. Select the **Overview** menu option.
3. In the virtual machine page, make note of the **Public IP Address** as shown below.



4. On your local computer, select the Windows icon and type **Remote Desktop Connection** then select the **Remote Desktop Connection** app.
5. In the **Remote Desktop Connection** app, type the public IP address into the **Computer** field, and then select **Connect**.
6. In the **Enter your credentials** dialog box, type the password that you specified when you created the virtual machine, and then select **OK**.
7. In the certificate warning dialog, select **Yes**.
8. On the remote machine, select the Windows icon, and then select the **Control Panel** tile.
9. In Control Panel, open **Microsoft Monitoring Agent** and then select on the **Azure Log Analytics (OMS)** tab.
10. Observe that the agent displays the following message: **The Microsoft Monitoring Agent has successfully connected to Microsoft Operations Management Suite service.** as shown below.



11. Select **OK** to close the **Microsoft Monitoring Agent Properties** window.
12. In the **All Control Panel Items** window, select **Administrative Tools**.
13. In the **Administrative Tools** window, double-click **Event Viewer**.
14. Expand **Applications and Services Logs**, and then select **Operations Manager**, and then maximize the **Event Viewer** window.
15. In the **Operations Manager** view, select the **Event ID** column heading to sort the list by Event ID.
16. Observe Event IDs 3000 and 5002. These events indicate that the computer has registered with the Log Analytics workspace and is receiving configuration. Event ID 5002 is shown below.



17. Close the Event Viewer and all other windows that were opened.
18. Close the Remote Desktop Connection application.

Schedule Update Deployments

Here you will learn how to schedule updates for the virtual machine.

1. In the **MediaWebServer - Update management** pane, select **Schedule update deployment** tab.
2. In the **Name** field, type **Critical and Security Updates**
3. In the **Update classifications** drop down list, check only **Critical updates** and **Security updates**.
4. In the **Schedule settings** field, under **Starts** increment the time up one hour.
5. In the **Recurrence** field, select **Recurring**.

6. In the **Recur every** field, configure update to occur once every week on Sunday as shown below, and then select **OK**.

... > MediaWebServe - Update management > New update deployment > Schedule Settings

New update deployment

MediaWebServe

* Name

Critical and Security Updates

Update classifications

2 selected

Include/exclude updates

Click to Configure

* Schedule settings

Click to Configure

Pre-scripts + Post-scripts (preview)

Click to Configure

Maintenance window (minutes)

120

Reboot options

Reboot if required

Create

Schedule Settings

* Starts

2018-12-10 | 1:47 PM

United States - Eastern Time

Recurrence

Once | Recurring

* Recur every

1 | Week

On these days

- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday
- [x] Sunday

Set expiration

Yes | No

Expires

Never

OK

7. In the **New update deployment** pane, select **Create**.

Next unit: Summary

Continue

Summary

2 minutes

In this module, you've seen how a large department can keep all of their Azure virtual machines patched and up-to-date.

In addition, you have seen how Update Management can generate a report indicating which machines are compliant with the latest updates. And finally, you have seen how Update Management can be configured to update deployments on a scheduled basis.

Cleanup

Delete the `mslearn-vmupdate` resource group to clean up your subscription.

Module complete:

Unlock achievement