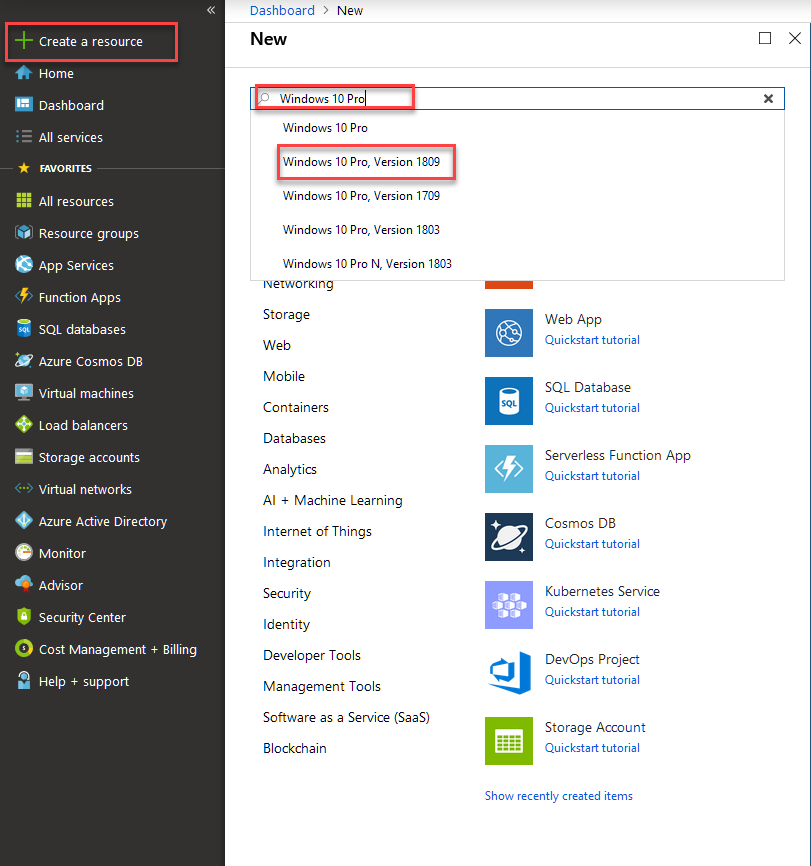
**LABS Day 1**

Version 1.2

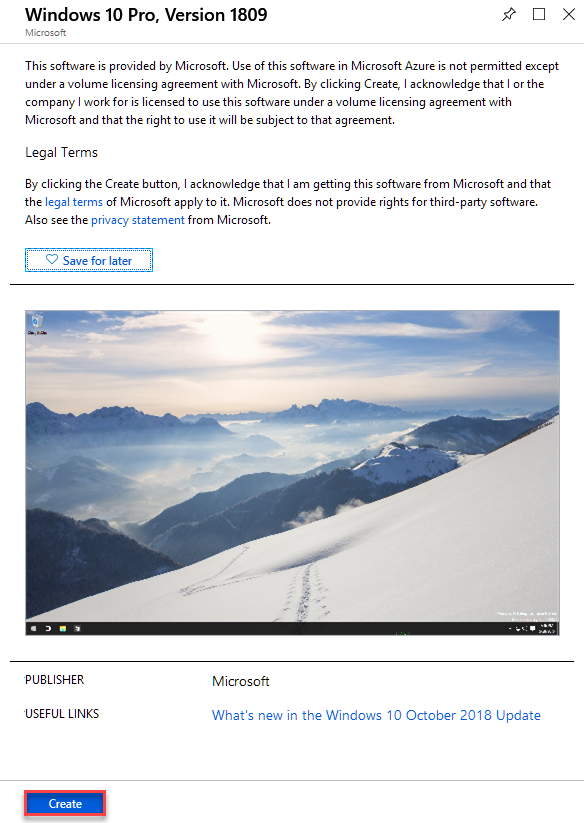
**Lab 0 Install Windows 10 VM and Azure Powershell**

**Task1 Install Windows 10 VM**

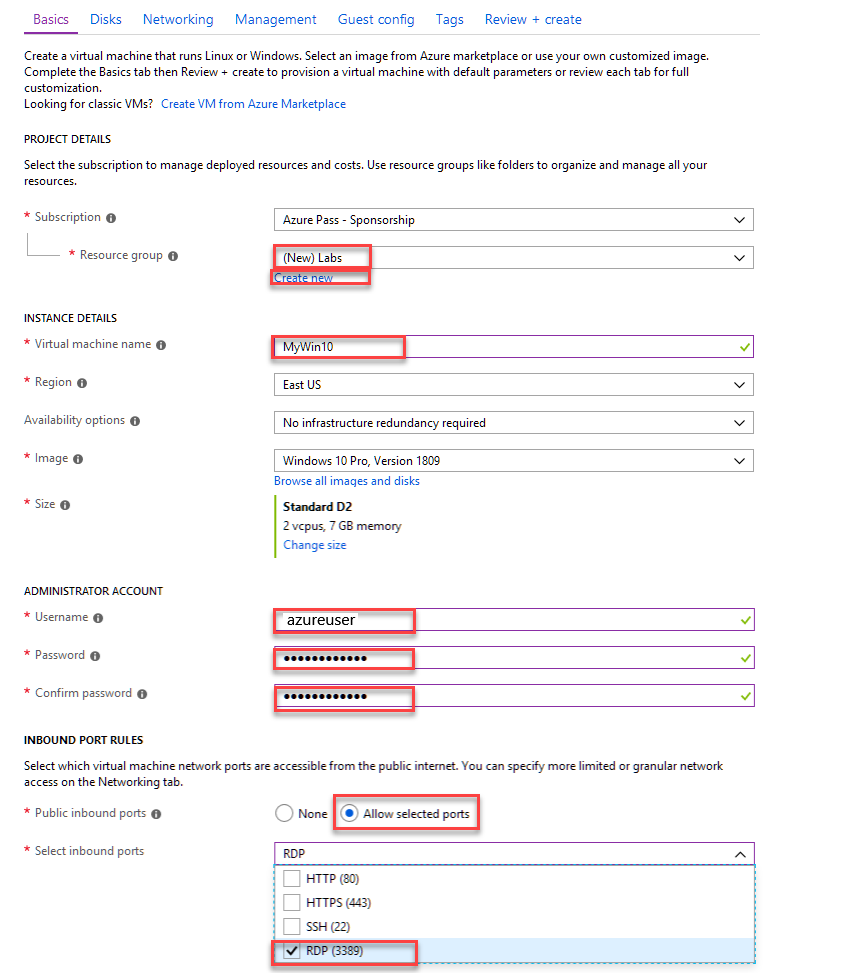
1. Go to <http://portal.azure.com>
2. Select **+Create a resource**
3. Type Windows 10 Pro in the Search box



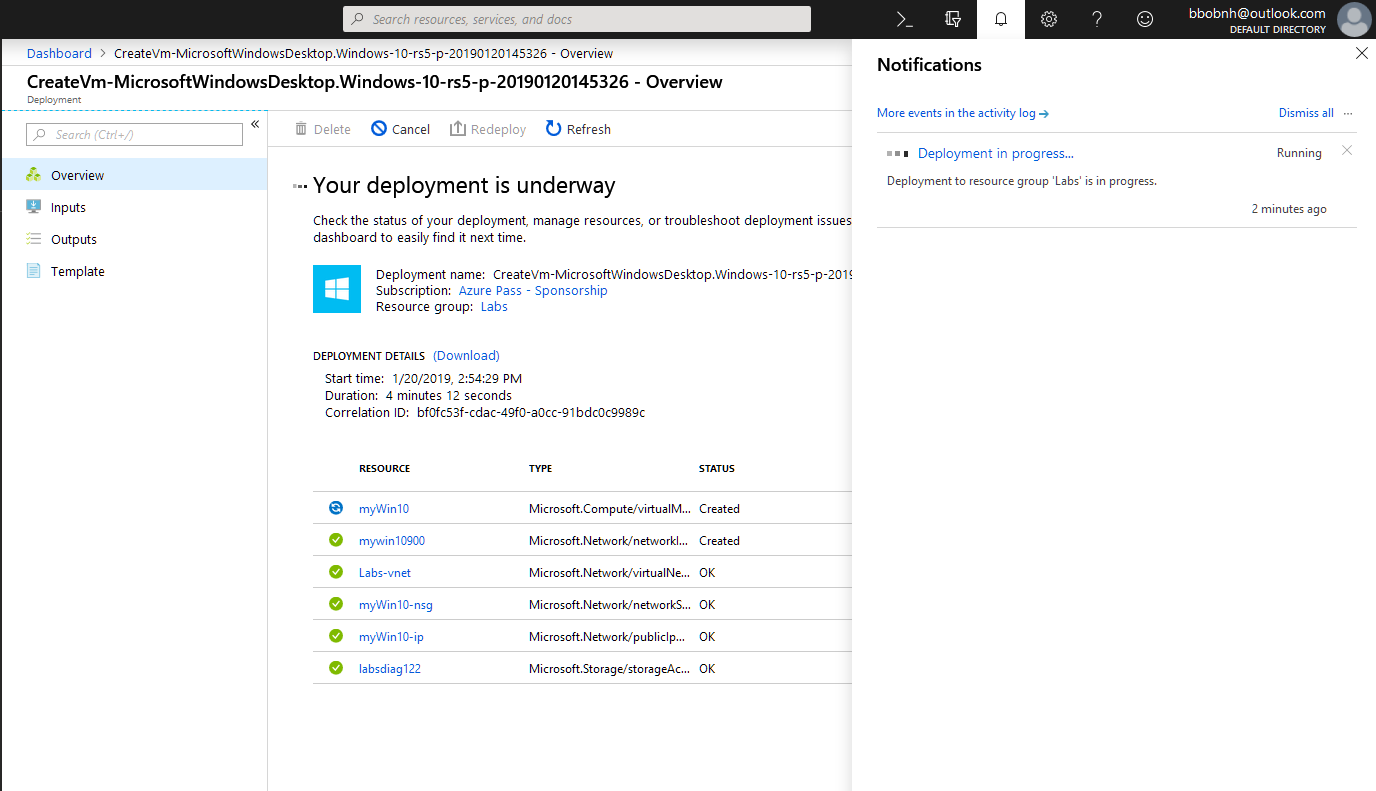
1. Choose **Windows 10 Pro** and the lastest version select **Create**



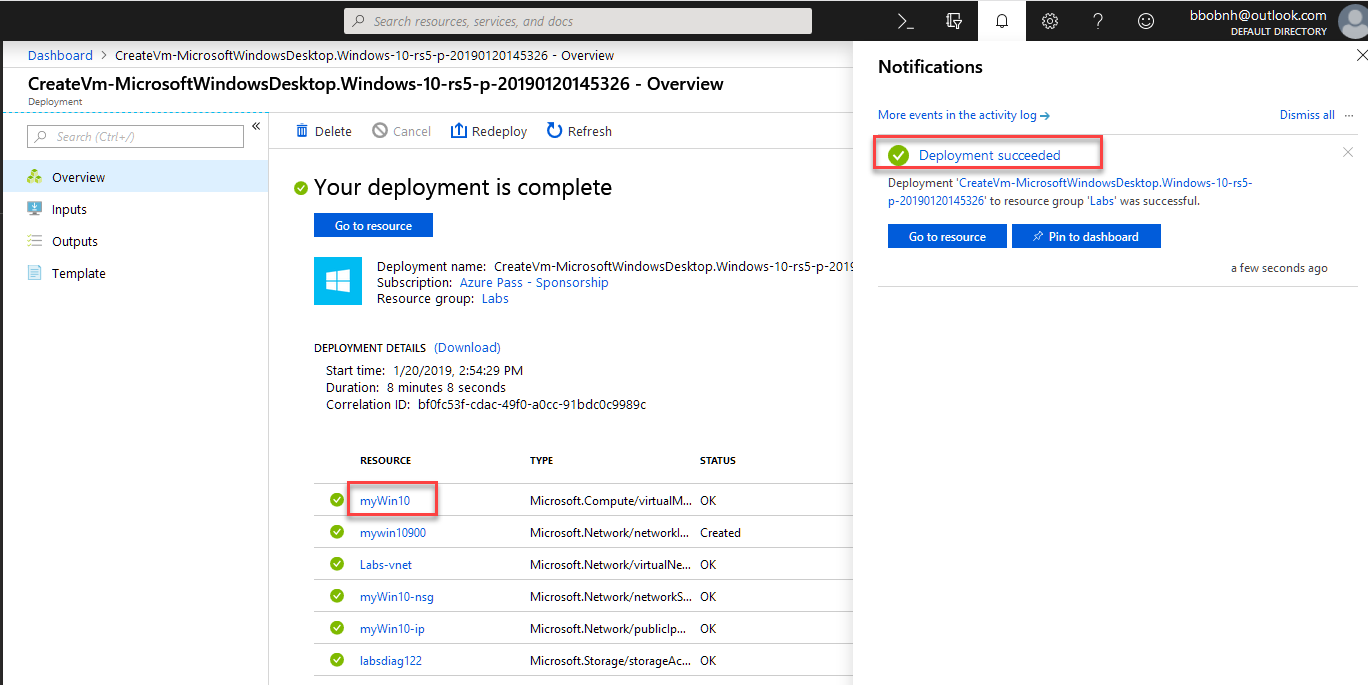
1. Fill out the Create a Virtual Machine as shown in the below graphic
   1. For password use **Pa55w.rd1234**



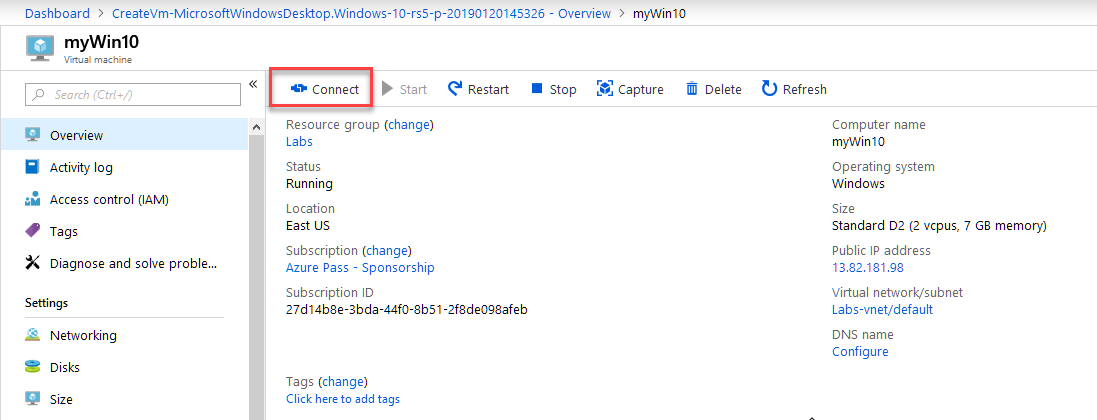
1. Select **Review + Create** then select **Create**
2. Wait until the Windows 10 VM deployment is done it will take a few minutes



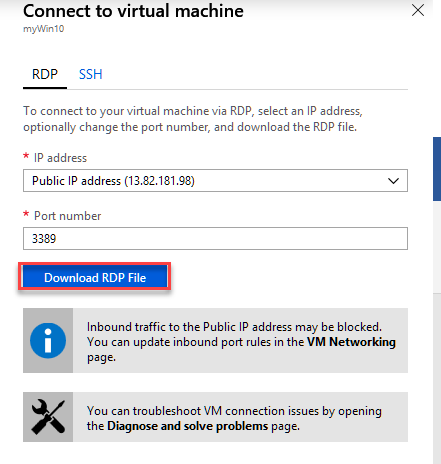
1. When the deployment has completed select **myWin10** vm



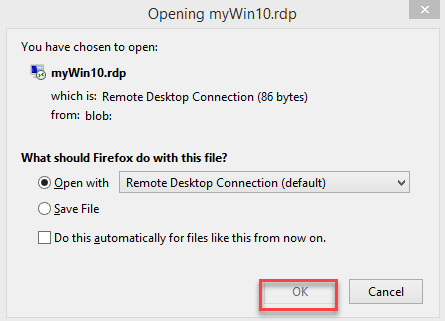
1. Then select the **Connect** Button



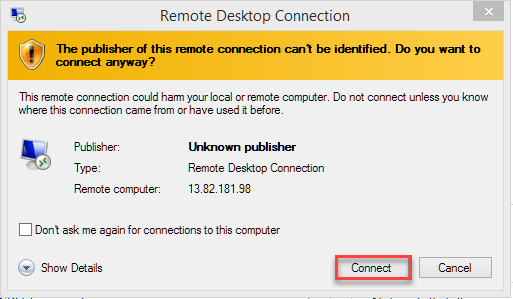
1. The select **Download RDP File**



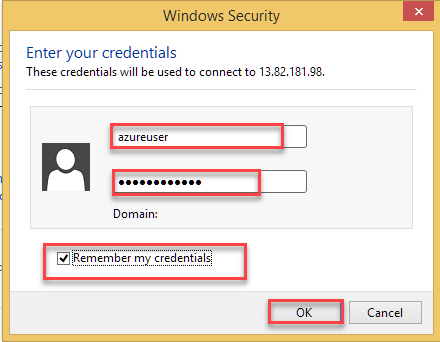
1. In the Opening myWin10.rdp dialog Select **OK**



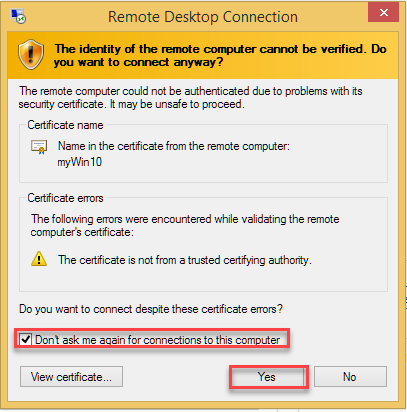
1. In the Remote Desktop Connection dialog select **Connect**



1. Enter your User name and Password and then select **Ok**

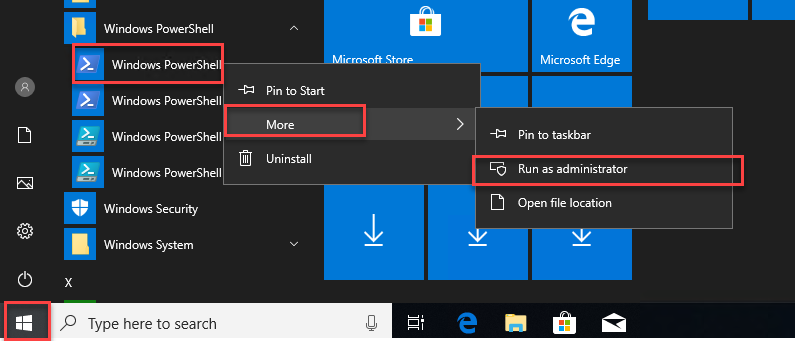


1. In the Remote Desktop Connection dialog select the **checkbox** then **Yes**

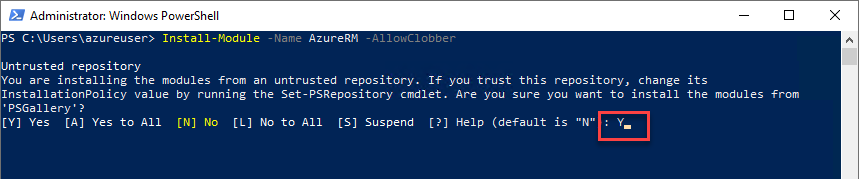


**Task 2 Install Azure PowerShell**

* + 1. Open Powershell as Administrator



* + 1. Run the following Powershell cmd
       - Install-Module -Name AzureRM -AllowClobber
       - Type Y to accept the download and hit enter



**Lab1 Download or view your Azure billing invoice and daily usage data**

For most subscriptions, you can download your invoice from the [Azure portal](https://portal.azure.com/#blade/Microsoft_Azure_Billing/SubscriptionsBlade) or have it sent in email. If you're an Azure customer with an Enterprise Agreement (EA customer), you can't download your organization's invoices. Invoices are sent to whoever is set up to receive invoices for the enrollment.

If you want to download usage as an EA customer, it's available in the [Azure portal](https://portal.azure.com/) > **Cost Management + Billing** > **Usage + charges**. For other subscriptions, go to the [Azure Account Center](https://account.azure.com/Subscriptions).

Only certain roles have permission to get billing invoice and usage information, like the Account Administrator, or Enterprise Administrator. To learn more about getting access to billing information, see [Manage access to Azure billing using roles](https://docs.microsoft.com/en-us/azure/billing/billing-manage-access).

**Note**

This Lab provides steps for how to delete personal data from the device or service and can be used to support your obligations under the GDPR. If you’re looking for general info about GDPR, see the [GDPR section of the Service Trust portal](https://servicetrust.microsoft.com/ViewPage/GDPRGetStarted).

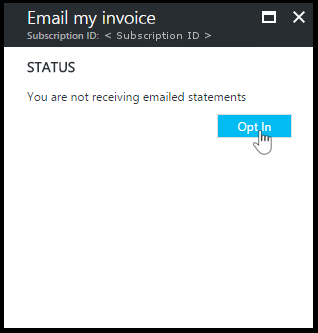
**Download or view your invoice**

If you're an EA customer, you can't download your organization's invoices. Invoices are sent to whoever is set up to receive invoices for the enrollment. For other subscriptions, you can get your invoice in email or download it from the Azure portal.

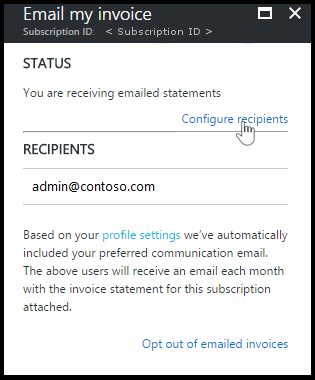
You can opt in and configure additional recipients to receive your Azure invoice in an email. This feature may not be available for certain subscriptions such as support offers, Enterprise Agreements, or Azure in Open.

**Task 1**

1. Goto <http://azure.portal.com>
2. From the left hand menu select **All Services**
3. Then click **Subscriptions**
4. Select your subscription from the Subscriptions page.
5. Click **Invoices** then **Email invoice**.
6. Click **Opt in** and accept the terms.



1. Once you've accepted the agreement, you can configure additional recipients. When a recipient is removed, the email address is no longer stored. If you change your mind, you need to re-add them.

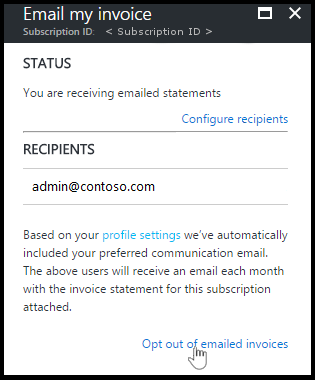


**Note**

If you are using free account you will not get an invoice.

**Opt out from getting your invoice in email**

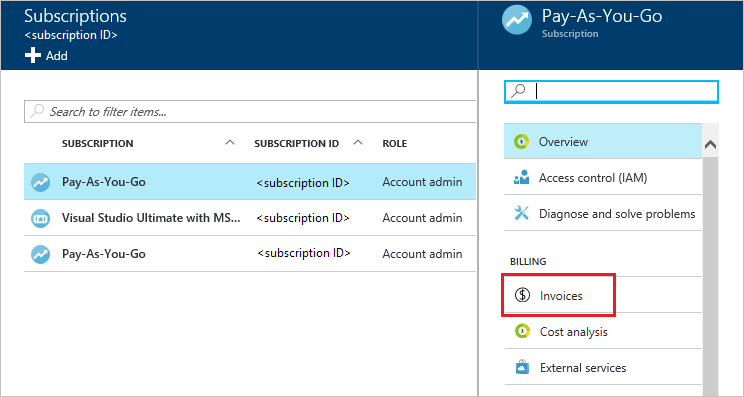
If you don't want to get your invoice in email, click **Opt out of emailed invoices**. This option removes any email addresses set to receive invoices in email. If you opt back in, you will have to reconfigure recipients.



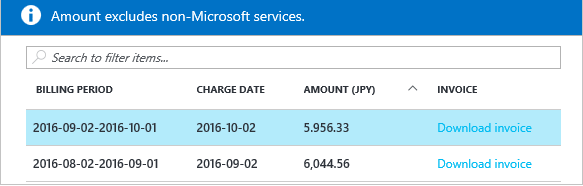
**Task 2 Optional**

If you have a **Pay as You GO** account you can follow the rest of the instructions

1. Select your subscription from the [Subscriptions page](https://portal.azure.com/#blade/Microsoft_Azure_Billing/SubscriptionsBlade) in Azure portal as [a user with access to invoices](https://docs.microsoft.com/en-us/azure/billing/billing-manage-access).
2. Select **Invoices**.



1. Click **Download Invoice** to view a copy of your PDF invoice. If it says **Not available**, see [Why don't I see an invoice for the last billing period?](https://docs.microsoft.com/en-us/azure/billing/billing-download-azure-invoice-daily-usage-date#noinvoice)



1. You can also view your daily usage by clicking the billing period.

For more information about your invoice, see [Understand your bill for Microsoft Azure](https://docs.microsoft.com/en-us/azure/billing/billing-understand-your-bill). For help managing your costs, see [Prevent unexpected costs with Azure billing and cost management](https://docs.microsoft.com/en-us/azure/billing/billing-getting-started).

**Why don't I see an invoice for the last billing period?**

There could be several reasons that you don't see an invoice:

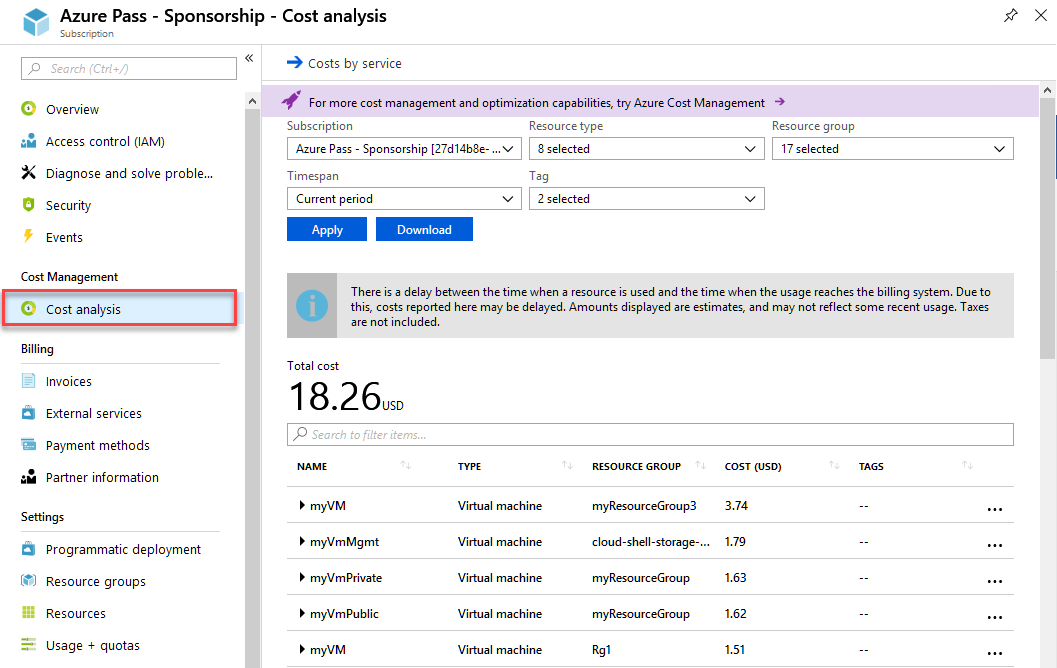
* You have a monthly credit amount with your subscription that you didn't exceed or you have a Free Trial. An invoice is only generated when you owe money.
* It's less than 30 days from the day you subscribed to Azure.
* The invoice isn't generated yet. Wait until the end of the billing period.
* If you're not the Account Administrator, older invoices may not be available to you.

**Download usage**

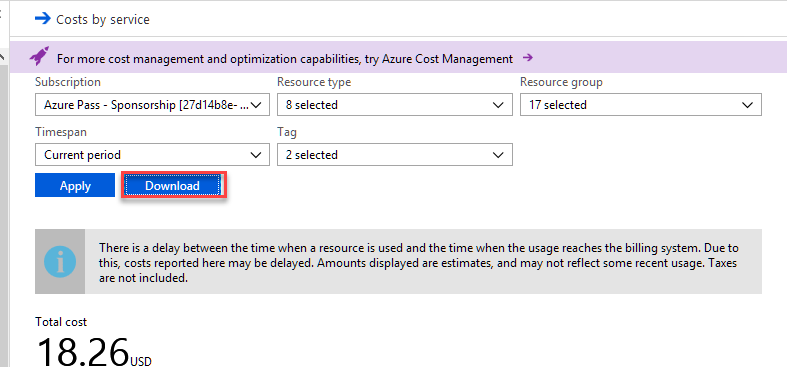
**Download usage from the Account Center (.csv)**

**Task 3**

1. Sign into the portal.
2. Select **All Services**, then select the subscription for which you want the usage information.
3. Select **Cost Analysis** under **Cost Management**.



1. Then click Download and view the file in Notepad.



**Lab 2**

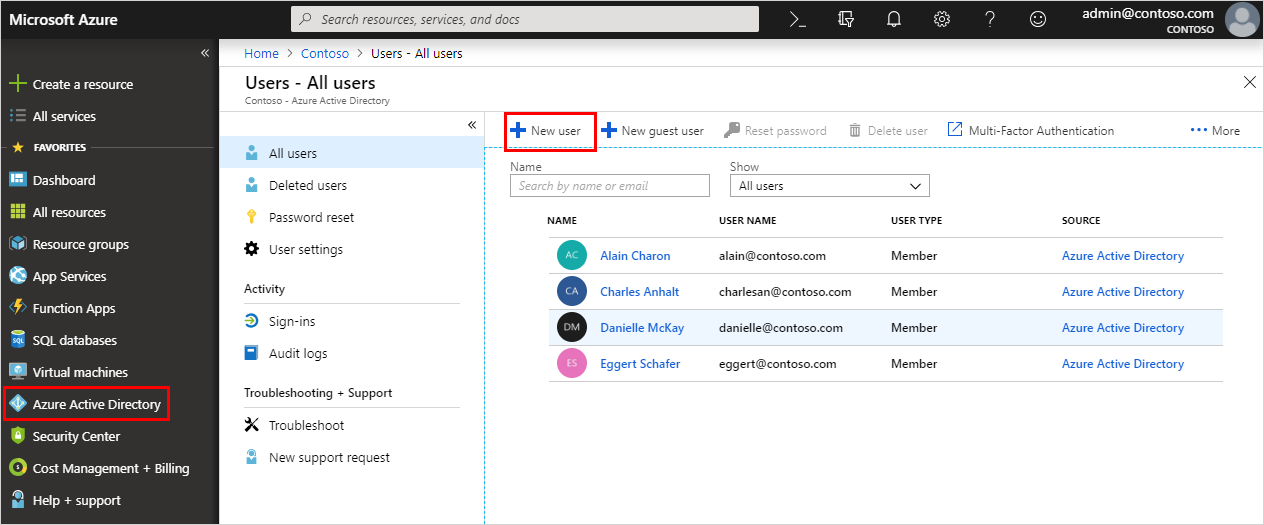
**Exercise 1**

**Add or delete users using Azure Active Directory**

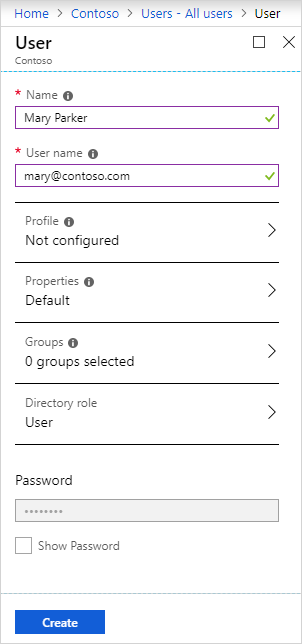
‎ **Task 1 Add a new user**

**To add a new user**

1. Sign in to the [Azure portal](https://portal.azure.com/) as a Global administrator or user administrator for the directory.
2. Select **Azure Active Directory**, select **Users**, and then select **New user**.



1. On the **User** page, fill out the required information.



* + **Name (required).** The first and last name of the new user. For example, Mary Parker.
  + **User name (required).** The user name of the new user. For example, [mary@<*yourdomainname*>.onmicrosoft.com](mailto:mary@%3cyourdomainname%3e.onmicrosoft.com)
    1. Yourdomainname is you user name + domain for example
       1. [bbobnh@outlook.com](mailto:bbobnh@outlook.com) the account used to create the Azure account would be mary@bbobnhoutlook.onmicrosoft.com

**Note**

The domain part of the user name must use either the initial default domain name, <*yourdomainname*>.onmicrosoft.com, or a custom domain name, such as contoso.com. For more information about how to create a custom domain name, see [How to add a custom domain name to Azure Active Directory](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-custom-domain).

* + **Profile.** Optionally, you can add more information about the user. You can also add user information at a later time. For more information about adding user info, see [How to add or change user profile information](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-profile-azure-portal).
  + **Groups.** Optionally, you can add the user to one or more existing groups. You can also add the user to groups at a later time. For more information about adding users to groups, see [How to create a basic group and add members](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-create-azure-portal).
  + **Directory role.** Optionally, you can add the user to a directory role. You can assign the user to be a global administrator, or to one or more of the other administrator roles in Azure AD. For more information about assigning roles, see [How to assign roles to users](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-assign-role-azure-portal).

1. Copy the auto-generated password provided in the **Password** box by selecting **Show Password**. You'll need to give this password to the user for the initial sign-in process.
2. Select **Create**.

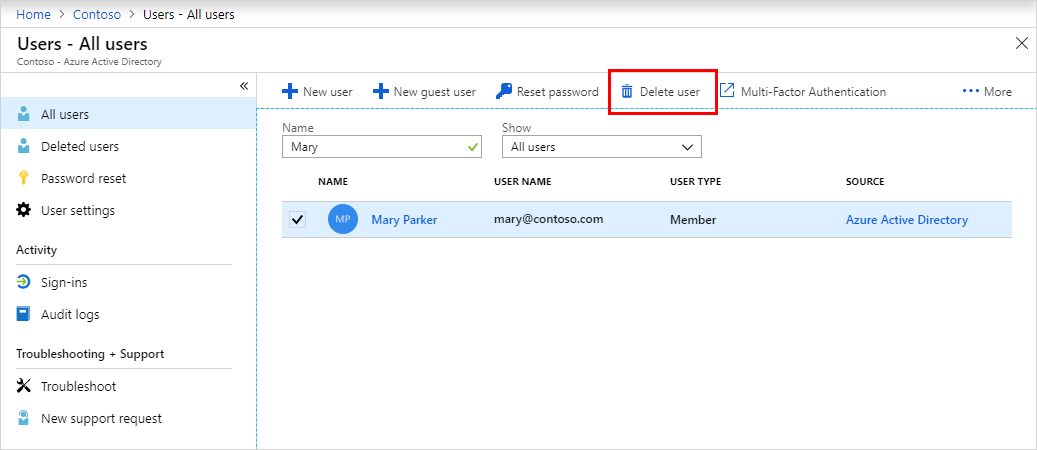
The user is created and added to your Azure AD tenant.

**Add a new user within a hybrid environment**

If you have an environment with both Azure Active Directory (cloud) and Windows Server Active Directory (on-premises), you can add new users by syncing the existing user account data. For more information about hybrid environments and users, see [Integrate your on-premises directories with Azure Active Directory](https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-hybrid-identity).

**Task 2 Delete a user**

1. Select **Azure Active Directory**, select **Users**, and then search for and select the user you want to delete from your Azure AD tenant. For example, *Mary Parker*.
2. Select **Delete user**.



The user is deleted and no longer appears on the **Users - All users** page. The user can be seen on the **Deleted users** page for the next 30 days and can be restored during that time.

**Task 3 Restore User**

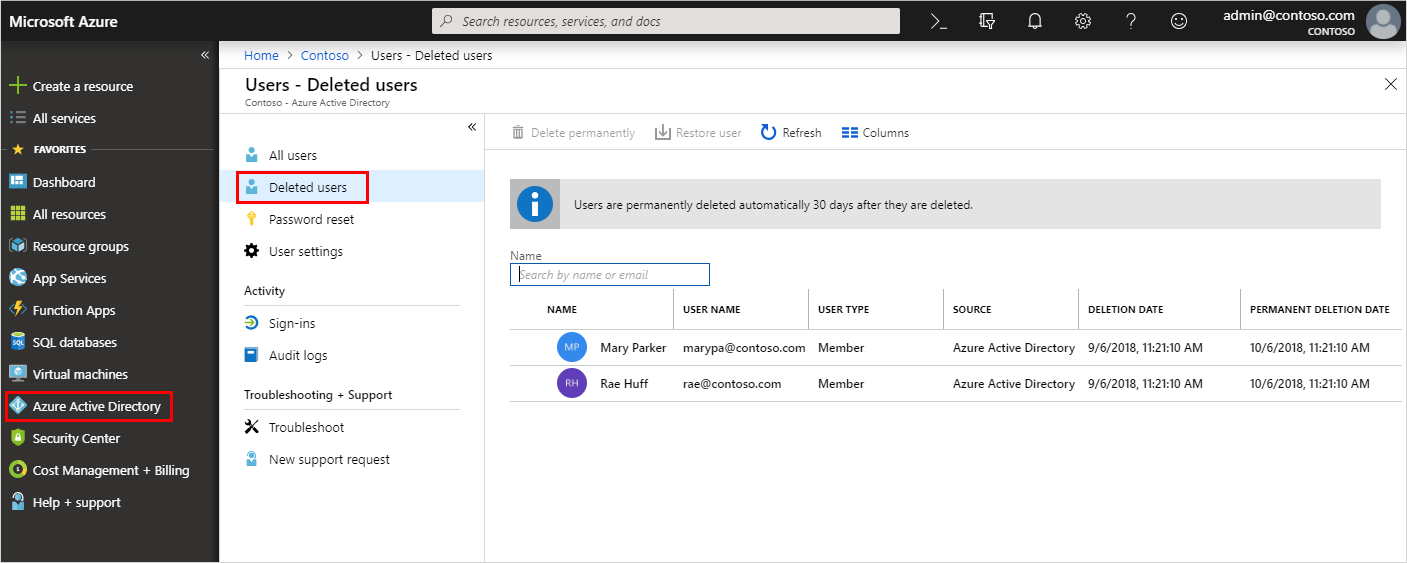
## View your restorable users

You can see all the users that were deleted less than 30 days ago. These users can be restored.

### To view your restorable users

1. Sign in to the [Azure portal](https://portal.azure.com/) using a Global administrator account for the directory.
2. Select **Azure Active Directory**, select **Users**, and then select **Deleted users**.

Review the list of users that are available to restore.

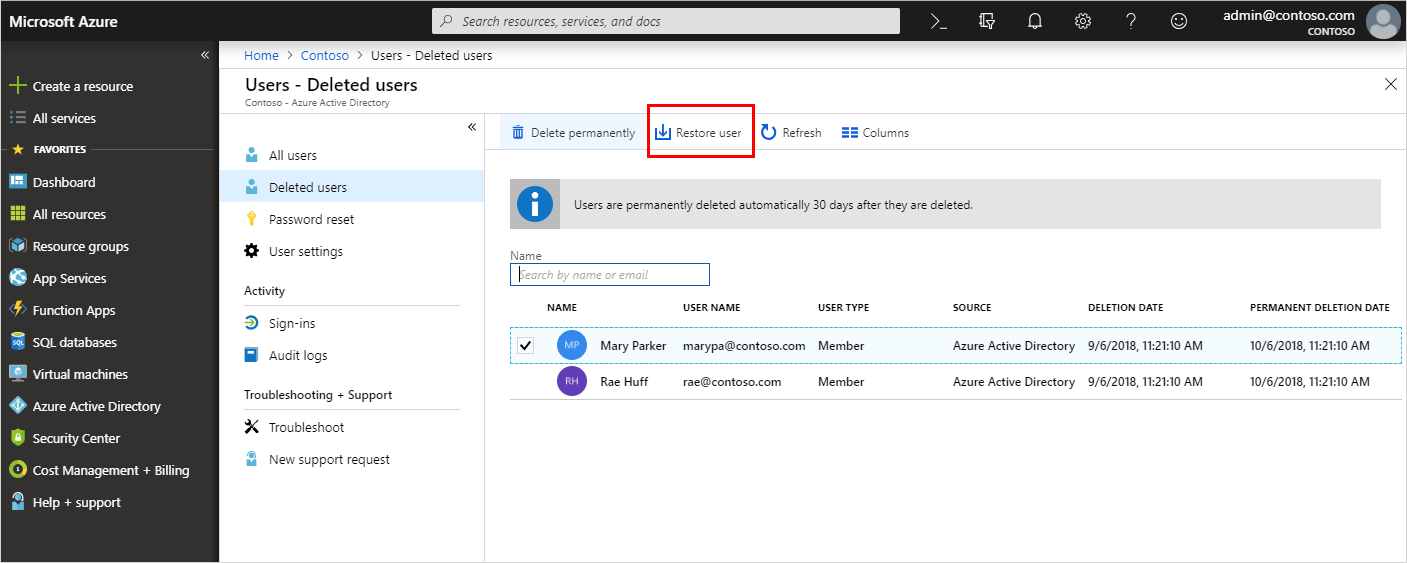


## Restore a recently deleted user

While a user's account is suspended, all the related directory information is preserved. When you restore a user, this directory information is also restored.

### To restore a user

1. On the **Users - Deleted users** page, search for and select one of the available users. For example, Mary Parker.
2. Select **Restore user**.

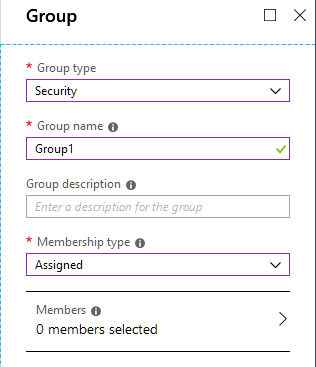


**Exercise 2**

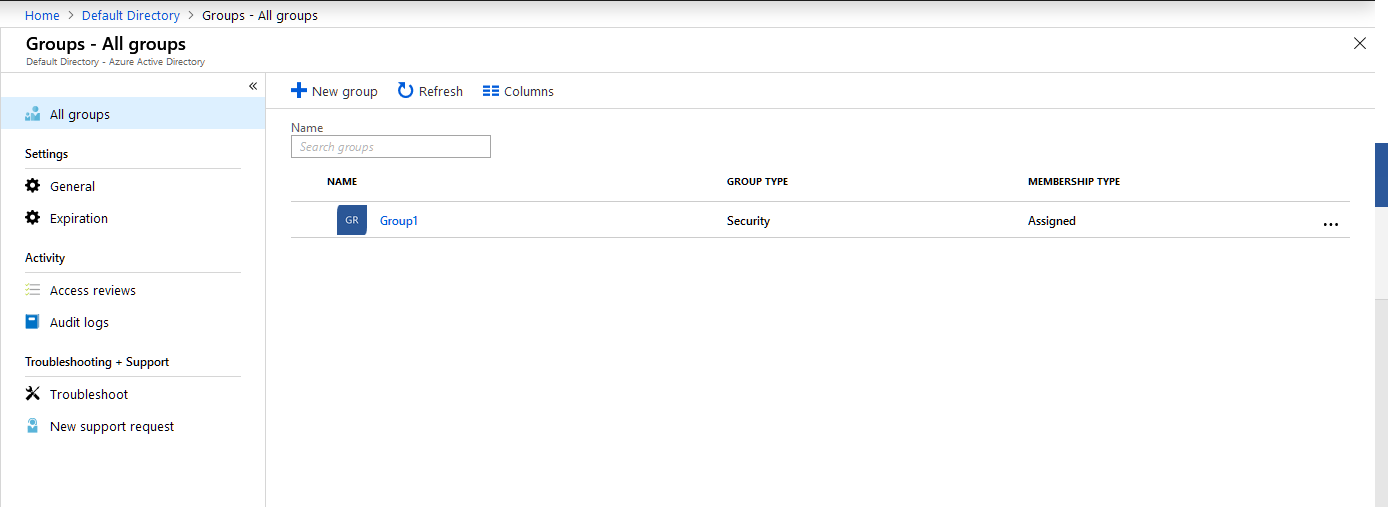
**Add or remove group members using Azure Active Directory**

**Task1 Add group members**

1. Select **Azure Active Directory**, and then select **Groups**.
2. Click **New Group** and Create a new Group by clicking the **Create button.**
   1. Group Type *Security*
   2. Group Name *Group1*

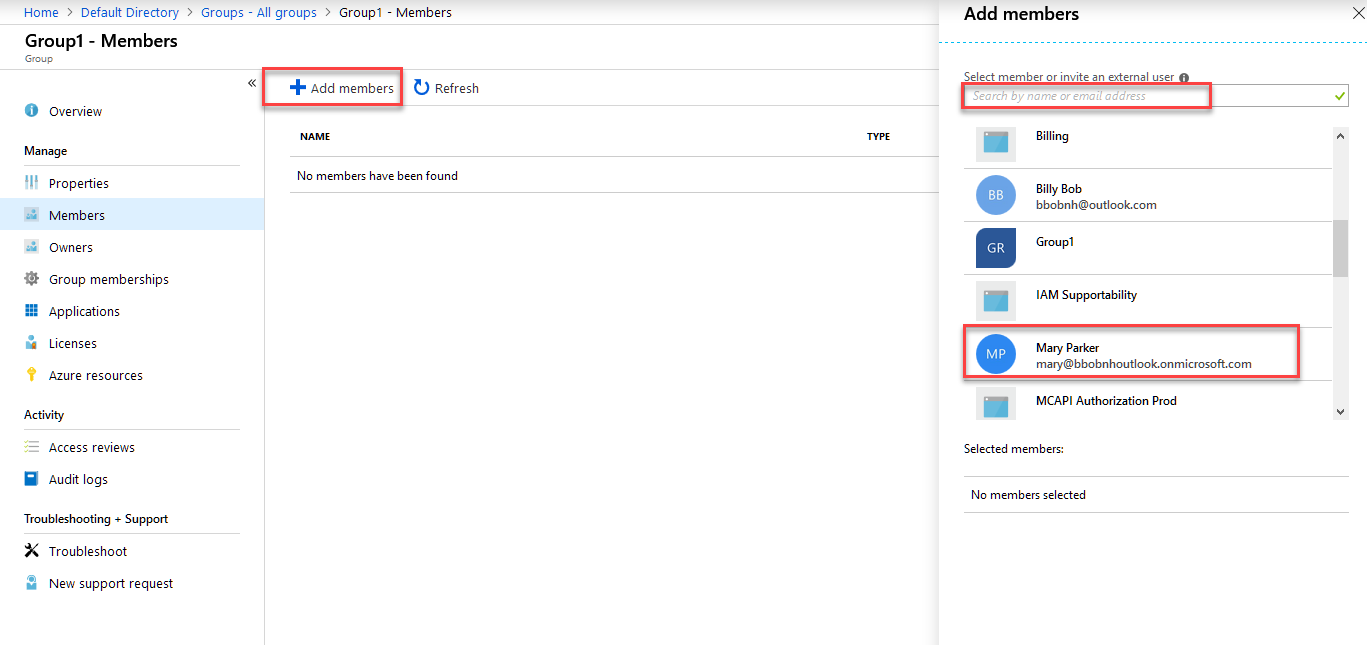


1. From the **Groups - All groups** page, search for and select the group you want to add the member to. In this case, use our previously created group, *Group1*.



1. From the **Group1** page, select **Members** from the **Manage** area.
2. Select **Add members**, and then search and select each of the members you want to add to the group, and then choose **Select**.

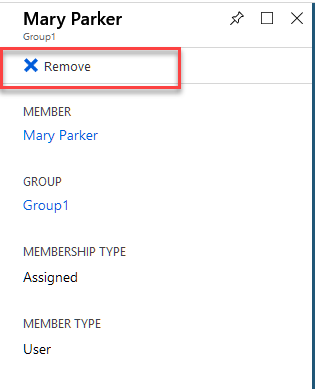
You'll get a message that says the members were added successfully.



1. Refresh the screen to see all of the member names added to the group.

**Task 2 To remove group members**

1. From the **Groups - All groups** page, search for and select the group you want to remove the member from. Again we'll use, **Group1**
2. Select **Members** from the **Manage** area, search for and select the name of the member to remove, and then select **Remove**.



# Exercise 3 Add or update a user's profile information using Azure Active Directory

* ‎Add user profile information, including a profile picture, job-specific information, and some settings using Azure Active Directory (Azure AD). For more information about adding new users, see [How to add or delete users in Azure Active Directory](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory).

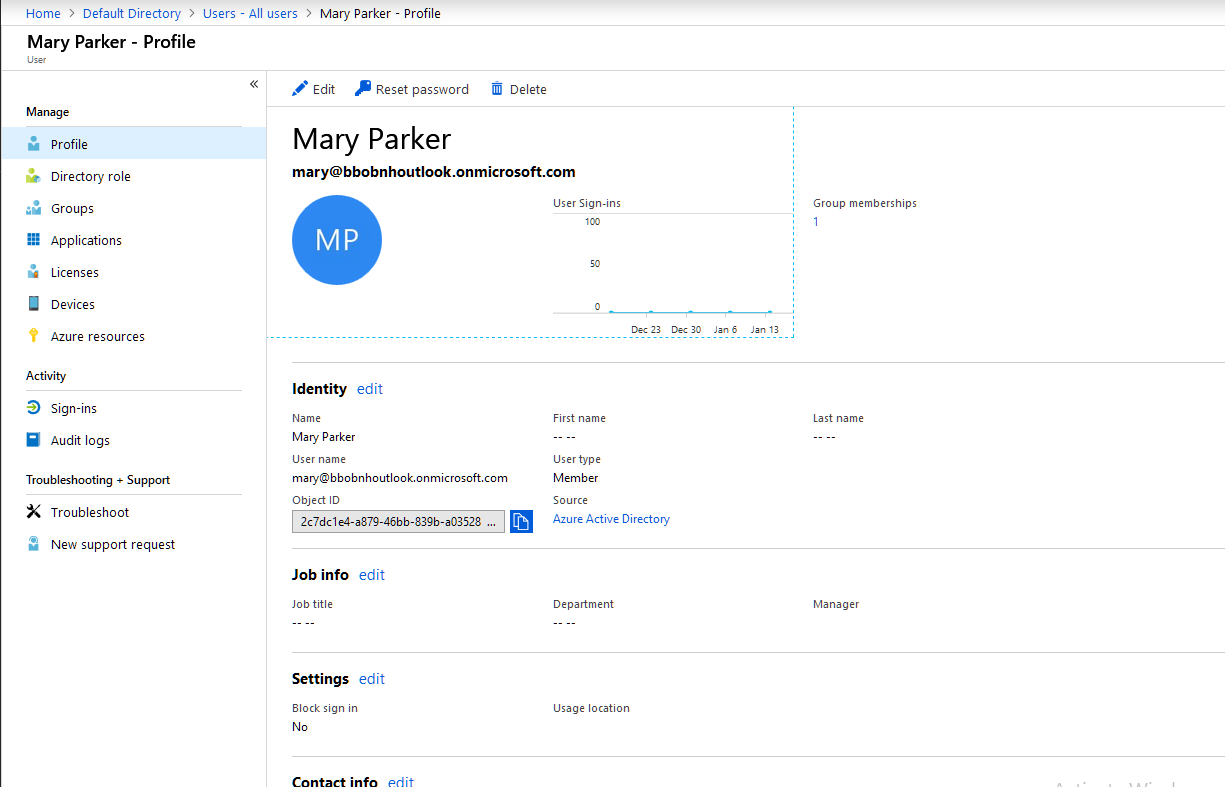
**Add or change profile information**

As you'll see, there's more information available in a user's profile than what you're able to add during the user's creation. All this additional information is optional and can be added as needed by your organization.

**Task 1 To add or change profile information**

1. Select **Azure Active Directory**, select **Users**, and then select a user. For example, *Mary Parker*.

The **Mary Parker - Profile** page appears.



1. Select **Edit** to optionally add or update the information included in each of the available sections.
   * 1. **Job info.**
        1. job title Azure *Admin*
        2. department *IT*
        3. manager *Bill Smith*.
2. Select **Save**.

All your changes are saved for the user.

**Lab 3A**

**Exercise 1**

**Audit and receive notifications about important actions in your Azure subscription**

* ‎The **Azure Activity Log** provides a history of subscription-level events in Azure. It offers information about *who* created, updated, or deleted *what* resources and *when* they did it. You can create an **Activity Log alert** to receive email, SMS, or webhook notifications when an activity occurs that match your alert conditions. This Quickstart steps through creating a simple network security group, browsing the Activity Log to understand the event that occurred, and then authoring an Activity Log alert to become notified when any network security group is created going forwards.

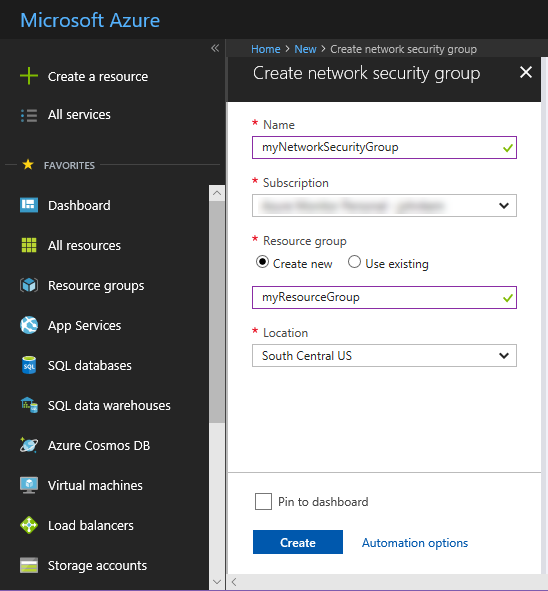
If you don't have an Azure subscription, create a [free](https://azure.microsoft.com/free/) account before you begin.

**Task 1 Log in to the Azure portal**

* 1. Log in to the [Azure portal](https://portal.azure.com/).

**Task 2 Create a network security group**

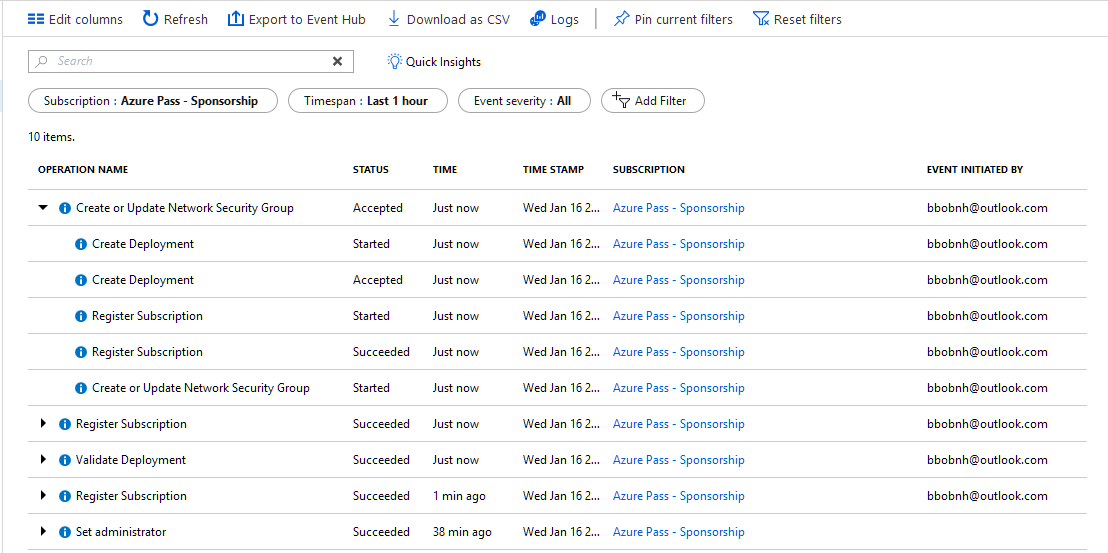
1. Click the **Create a resource** button found on the upper left-hand corner of the Azure portal.
2. Select **Networking**, select **Network security group**.
3. Enter "myNetworkSG" as the **Name** and create a new resource group named **myResourceGroup**. Click the **Create** button.



**Task 3 Browse the Activity Log in the portal**

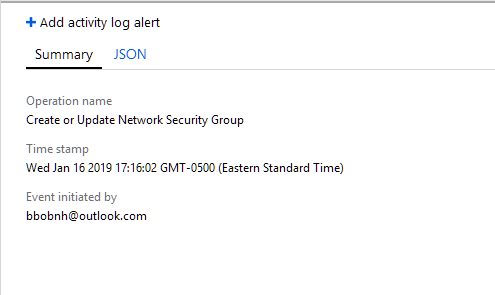
An event has now been added to the Activity Log that describes the creation of the network security group. Use the following instructions to identify that event.

1. Click the **Monitor** button found on the left-hand navigation list. It opens to the Activity Log section. This section contains a history of all actions that users have performed on resources in your subscription, filterable by several properties such as the **Resource Group**, **Timespan**, and **Category**.
2. Click **Add Filter** and select **Resource Group** to filter by **Resource Group**
3. In the **Activity Log** section, click the **Resource Group** dropdown and select **myResourceGroup**. Change the **Timespan** dropdown to **Last 1 hour**. Click **Apply**.
4. Click on the **Create or Update NetworkSecurityGroups** event in the table of events shown.

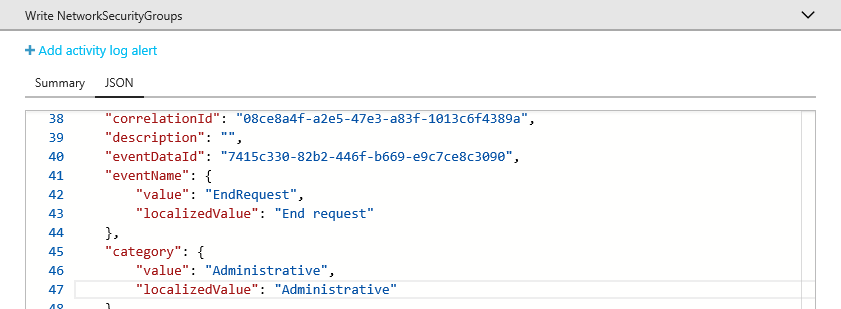


**Browse an event in the Activity Log**

The section that appears contains basic details of the operation that was performed, including the name, the timestamp, and the user or application that performed it.



Click on the **JSON** tab to view the full event details. This includes the details of how the user or application was authorized to perform the operation, the event category and level, and the status of the operation.



**Exercise 2 View activity logs to audit actions on resources**

* ‎Through activity logs, you can determine:
* what operations were taken on the resources in your subscription
* who initiated the operation (although operations initiated by a backend service do not return a user as the caller)
* when the operation occurred
* the status of the operation
* the values of other properties that might help you research the operation

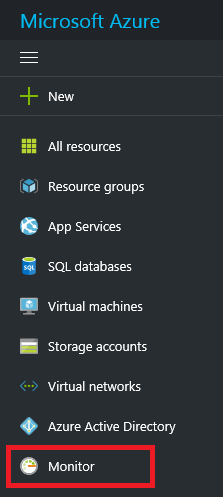
The activity log contains all write operations (PUT, POST, DELETE) performed on your resources. It does not include read operations (GET). For a list of resource actions, see [Azure Resource Manager Resource Provider operations](https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations). You can use the audit logs to find an error when troubleshooting or to monitor how a user in your organization modified a resource.

Activity logs are retained for 90 days. You can query for any range of dates, as long as the starting date is not more than 90 days in the past.

You can retrieve information from the activity logs through the portal, PowerShell, Azure CLI, Insights REST API, or [Insights .NET Library](https://www.nuget.org/packages/Microsoft.Azure.Insights/).

**Task 1 Portal**

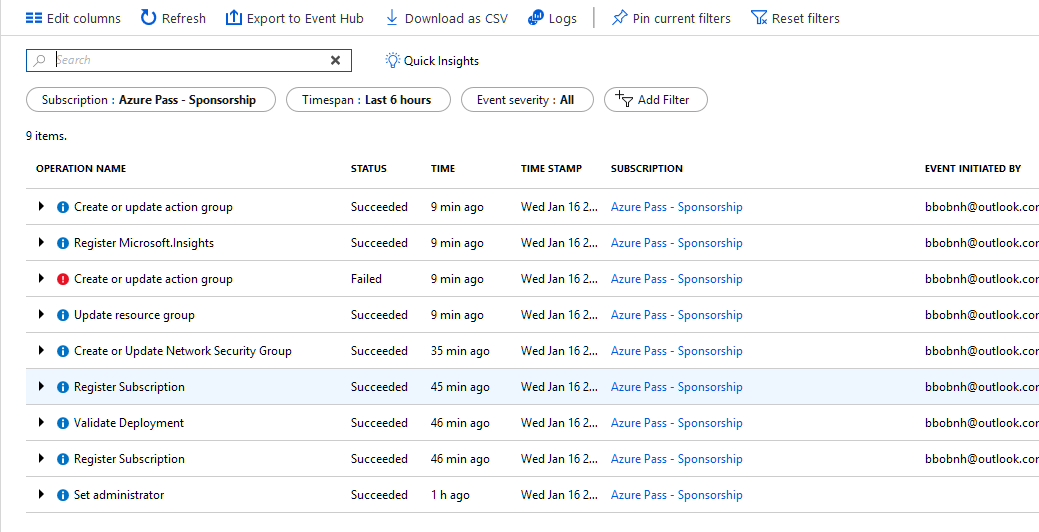
1. To view the activity logs through the portal, select **Monitor**.



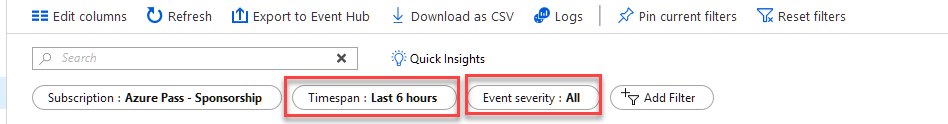
**Note**

To automatically filter the activity log for a particular resource or resource group, select **Activity log**. Notice that the activity log is automatically filtered by the selected resource.

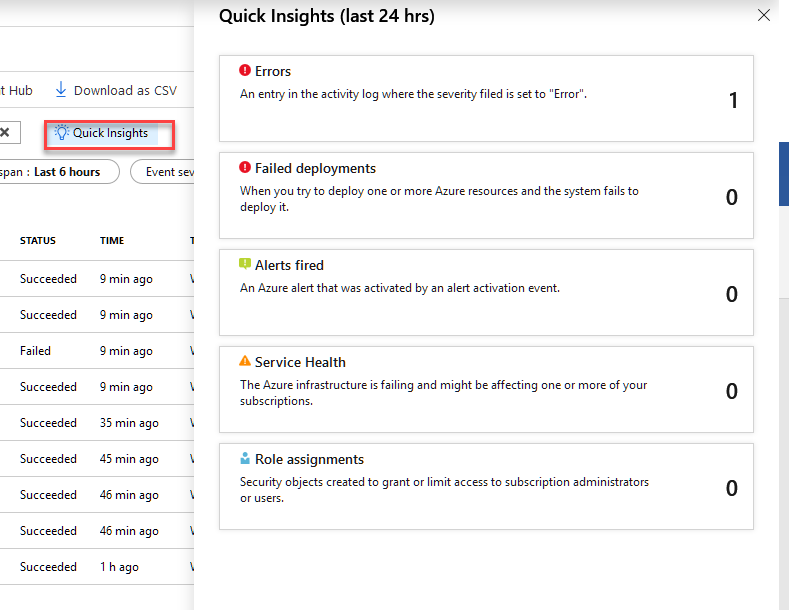
1. In the **Activity Log**, you see a summary of recent operations.



1. To restrict the number of operations displayed, select different conditions. For example, the following image shows the **Timespan** and **Event initiated by** fields changed to view the actions taken by a particular user or application for the past month. Select **Apply** to view the results of your query.



1. Click on Quick Insights to view details on Activities.

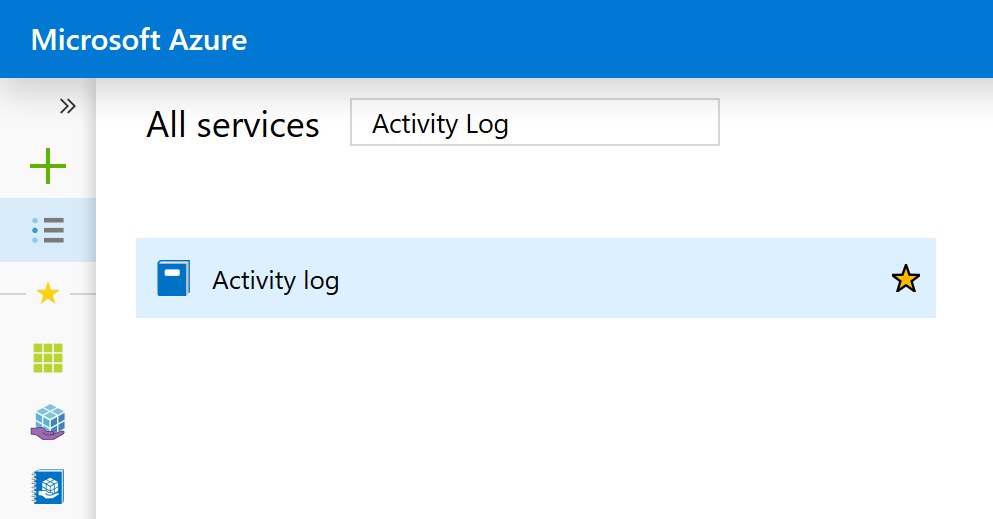


**Exercise 3**

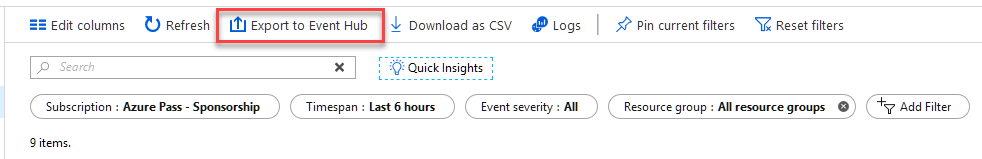
### Task 1 Configure log profiles using the Azure portal

You can stream the Activity Log to an Event Hub or store them in a Storage Account by using the “Export to Event Hub” option in the Azure portal.

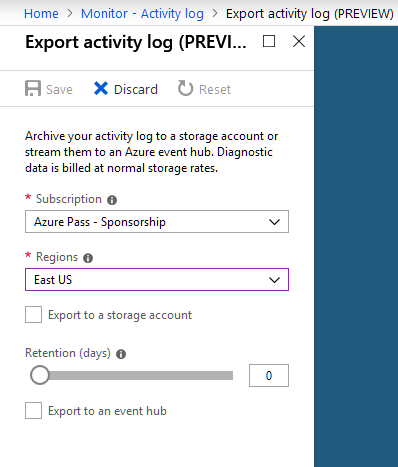
1. Navigate to **Activity Log** using the menu on the left side of the portal.



1. Click the **Export to Event Hub** button at the top of the blade.



1. In the blade that appears, you can select:
   * regions for which you would like to export events
   * the Storage Account to which you would like to save events
   * the number of days you want to retain these events in storage. A setting of 0 days retains the logs forever.
   * the Service Bus Namespace in which you would like an Event Hub to be created for streaming these events.



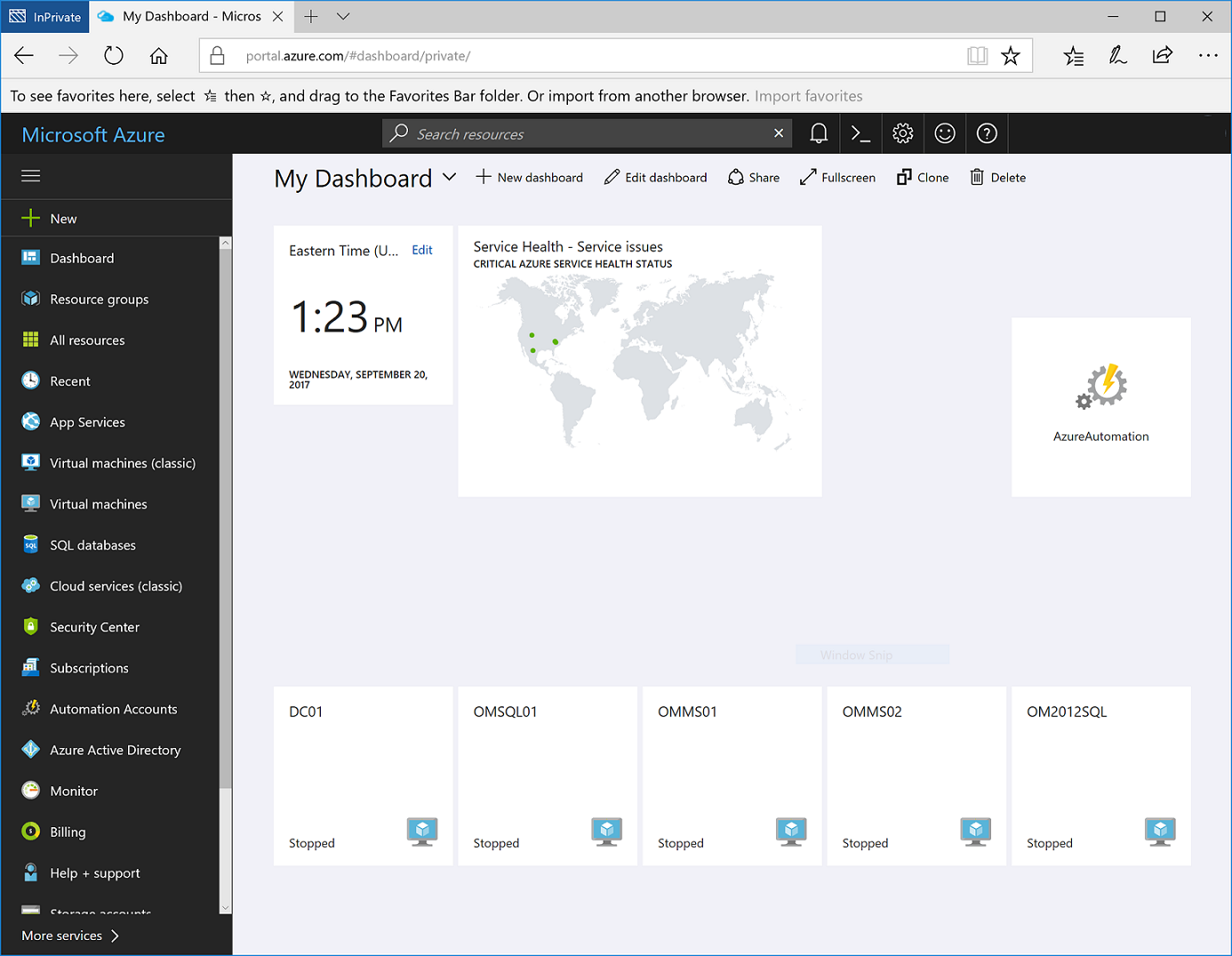
1. Click **Save** to save these settings. The settings are immediately be applied to your subscription.

## Lab 4A Create and share dashboards of Log Analytics data

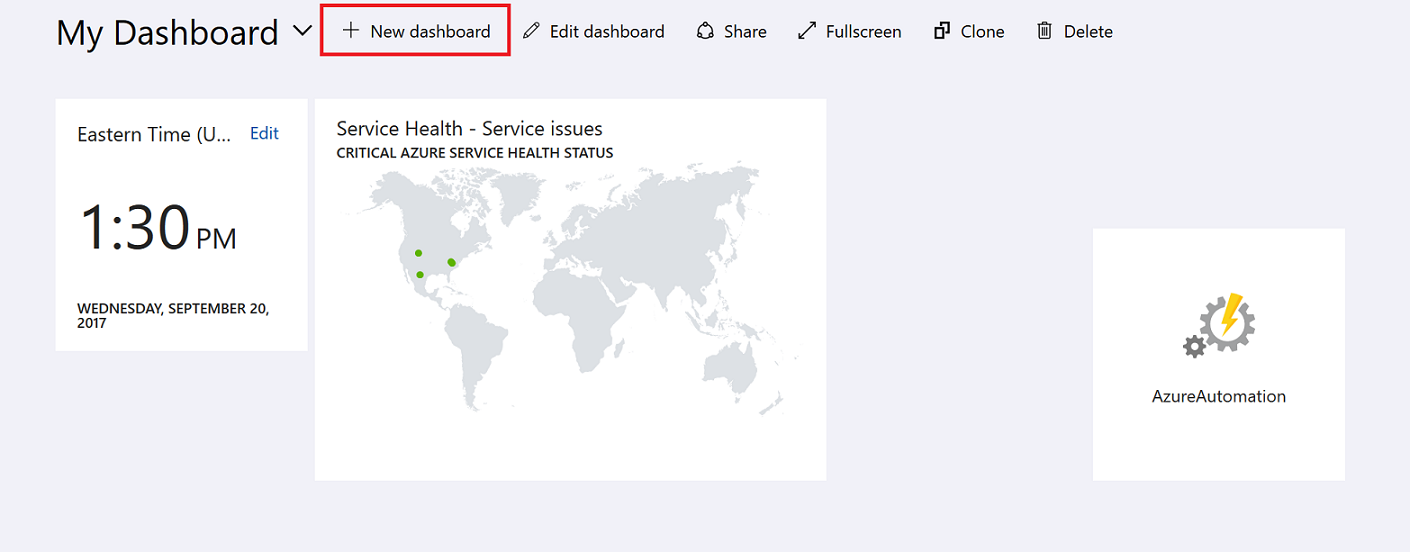
* ‎Log Analytics dashboards can visualize all of your saved log searches, giving you the ability to find, correlate, and share IT operational data in the organization. This tutorial covers creating a log search that will be used to support a shared dashboard that will be accessed by your IT operations support team. You learn how to:
* Create a shared dashboard in the Azure portal
* Visualize a performance log search
* Add a log search to a shared dashboard
* Customize a tile in a shared dashboard

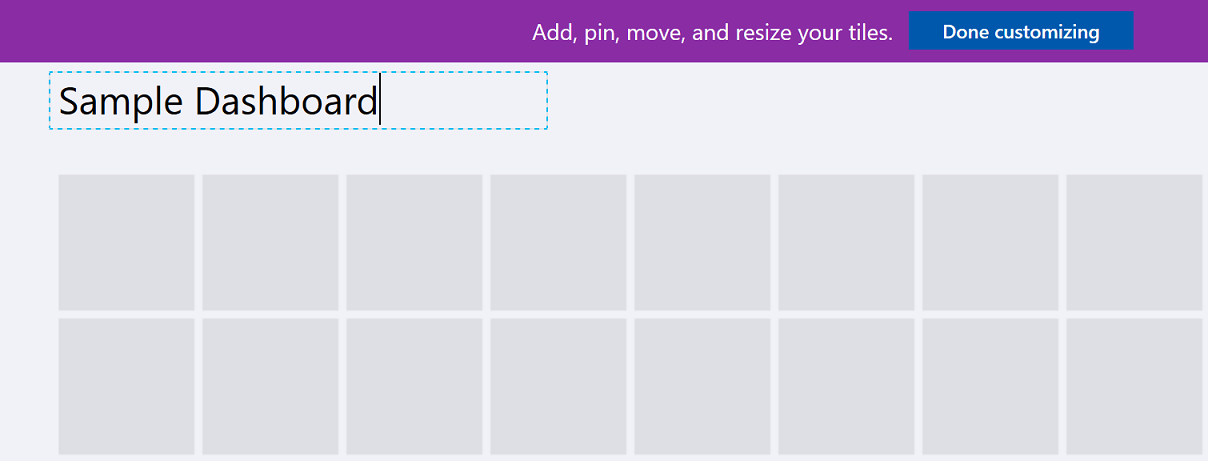
To complete the example in this tutorial, you must have an existing virtual machine [connected to the Log Analytics workspace](https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-azurevm).

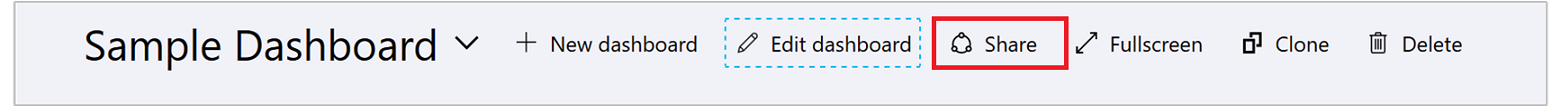
## Task 1 Create a shared dashboard

The first thing you see after you sign in to the Microsoft Azure portal is a [dashboard](https://docs.microsoft.com/en-us/azure/azure-portal/azure-portal-dashboards).  


Here you can bring together operational data that is most important to IT across all your Azure resources, including telemetry from Azure Log Analytics. Before we step into visualizing a log search, let's first create a dashboard and share it. This allows us to get it out of the way before we take our example performance log search, which will render as a line chart, and add it to the dashboard.

To create a dashboard, select the **New dashboard** button next to the current dashboard's name.  


This action creates a new, empty, private dashboard and puts you into customization mode where you can name your dashboard and add or rearrange tiles. Edit the name of the dashboard and specify Sample Dashboard for this tutorial and then select **Done customizing**.  
  


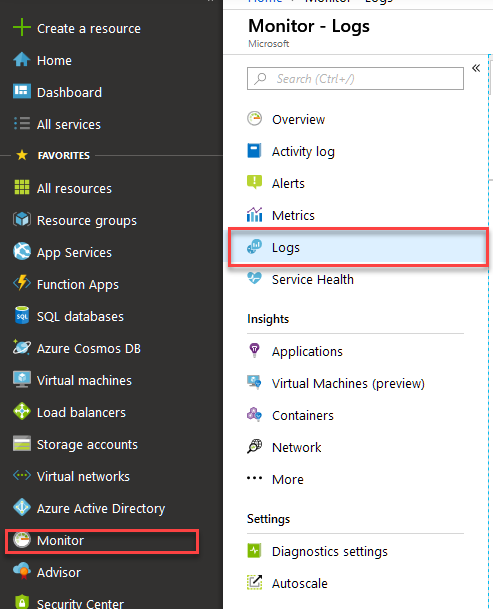
When you create a dashboard, it is private by default, which means you are the only person who can see it. To make it visible to others, use the **Share** button that appears alongside the other dashboard commands.  


You are asked to choose a subscription and resource group for your dashboard to be published to. For convenience, the portal's publishing experience guides you towards a pattern where you place dashboards in a resource group called **dashboards**. Verify the subscription selected and then click **Publish**. Access to the information displayed in the dashboard is controlled with [Azure Resource Based Access Control](https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal).

## Task 2 Visualize a log search

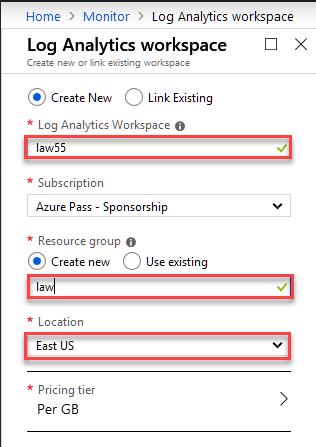
You can create basic queries on a single line from the Log Search portal in the Azure portal. The Log Search portal can be used without launching an external portal, and you can use it to perform a variety of functions with log searches including creating alert rules, creating computer groups, and exporting the results of the query.

The [Log Analytics portal](https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/get-started-portal) is a dedicated portal that provides advanced functionality not available in the Log Search portal. Features include the ability to edit a query on multiple lines, selectively execute code, context sensitive Intellisense, and Smart Analytics. In the Advanced Analytics portal, you will create a performance view in graphical form, save it for a future search, and pin it to the shared dashboard created earlier.

1. You launch the Advanced Analytics portal from a link in the Log Search portal.  


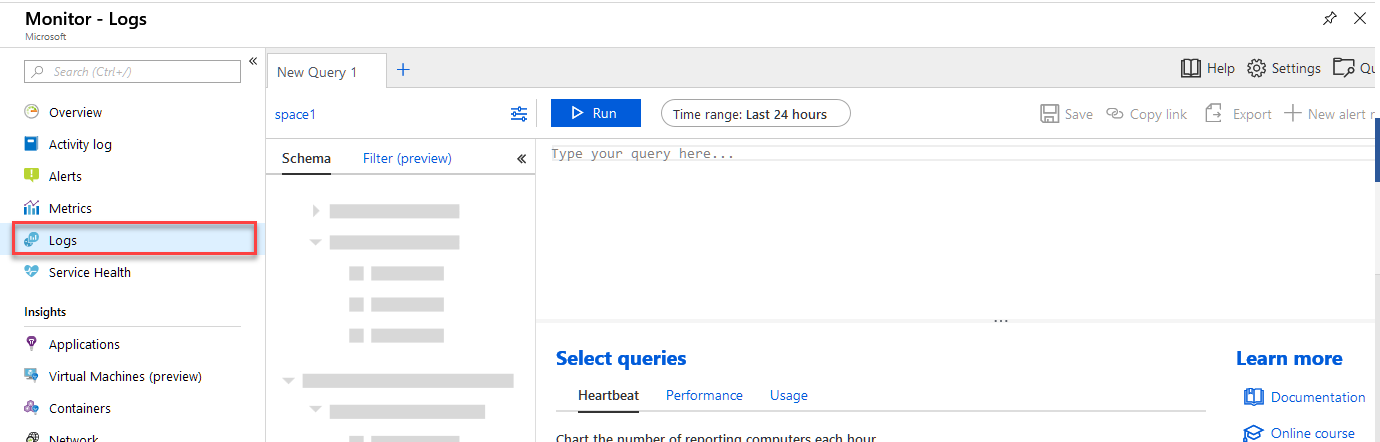
2. Create a new **Log Analytics Workspace**

* + The workspace name must be unique
  + Type a name for a new Resource Group
  + Select the East Us Location



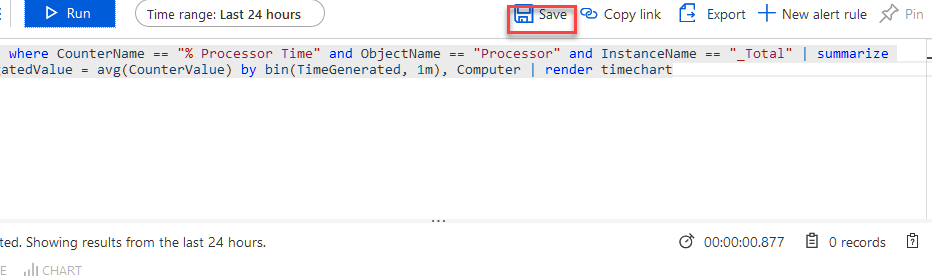
3. After filling in the values Click **OK**

4. After the Workspace is created you may need to go back click **Logs** Again



5. In the Analytics portal, enter the following query to return only processor util4ization records for both Windows and Linux computers, grouped by Computer and TimeGenerated, and displayed in a visual chart:

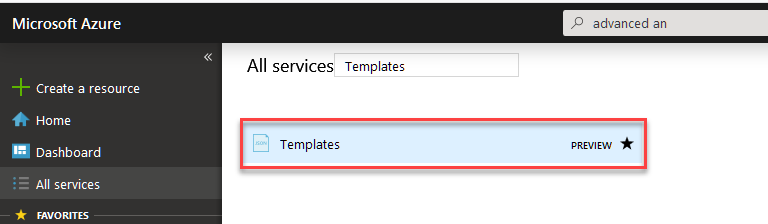
Perf | where CounterName == "% Processor Time" and ObjectName == "Processor" and InstanceName == "\_Total" | summarize AggregatedValue = avg(CounterValue) by bin(TimeGenerated, 1m), Computer | render timechart

**Save the query by selecting the Save query button from the top-right corner.**  
  
In the **Save Query** control panel, provide a name such as Azure VMs - Processor Utilization and then click **Save**. This way you can create a library of common queries to search with or modify it without having to re-write it entirely.

## Lab 5A Create a Windows virtual machine from a Resource Manager template

**Task 1 Create new Template**

1 From **All Services** Type Templates and the Select **Templates**



## 2 Click Add to add a new Template giving it a naming it “DeployServer” and a description “Deploy SQL Server 2016”

## 3 Add Template by copying the Json below. You must the value of domainNameLabel with your own unique name.

{

"$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",

"contentVersion": "1.0.0.0",

"parameters": {

"adminUsername": { "type": "string" },

"adminPassword": { "type": "securestring" }

},

"variables": {

"vnetID": "[resourceId('Microsoft.Network/virtualNetworks','myVNet')]",

"subnetRef": "[concat(variables('vnetID'),'/subnets/mySubnet')]"

},

"resources": [

{

"apiVersion": "2016-03-30",

"type": "Microsoft.Network/publicIPAddresses",

"name": "myPublicIPAddress",

"location": "[resourceGroup().location]",

"properties": {

"publicIPAllocationMethod": "Dynamic",

"dnsSettings": {

"domainNameLabel": "myresourcegroupdns1"

}

}

},

{

"apiVersion": "2016-03-30",

"type": "Microsoft.Network/virtualNetworks",

"name": "myVNet",

"location": "[resourceGroup().location]",

"properties": {

"addressSpace": { "addressPrefixes": [ "10.0.0.0/16" ] },

"subnets": [

{

"name": "mySubnet",

"properties": { "addressPrefix": "10.0.0.0/24" }

}

]

}

},

{

"apiVersion": "2016-03-30",

"type": "Microsoft.Network/networkInterfaces",

"name": "myNic",

"location": "[resourceGroup().location]",

"dependsOn": [

"[resourceId('Microsoft.Network/publicIPAddresses/', 'myPublicIPAddress')]",

"[resourceId('Microsoft.Network/virtualNetworks/', 'myVNet')]"

],

"properties": {

"ipConfigurations": [

{

"name": "ipconfig1",

"properties": {

"privateIPAllocationMethod": "Dynamic",

"publicIPAddress": { "id": "[resourceId('Microsoft.Network/publicIPAddresses','myPublicIPAddress')]" },

"subnet": { "id": "[variables('subnetRef')]" }

}

}

]

}

},

{

"apiVersion": "2016-04-30-preview",

"type": "Microsoft.Compute/virtualMachines",

"name": "myVM",

"location": "[resourceGroup().location]",

"dependsOn": [

"[resourceId('Microsoft.Network/networkInterfaces/', 'myNic')]"

],

"properties": {

"hardwareProfile": { "vmSize": "Standard\_B2ms" },

"osProfile": {

"computerName": "myVM",

"adminUsername": "[parameters('adminUsername')]",

"adminPassword": "[parameters('adminPassword')]"

},

"storageProfile": {

"imageReference": {

"publisher": "MicrosoftSQlServer",

"offer": "SQL2016SP1-WS2016",

"sku": "Enterprise",

"version": "latest"

},

"osDisk": {

"name": "myManagedOSDisk",

"caching": "ReadWrite",

"createOption": "FromImage"

}

},

"networkProfile": {

"networkInterfaces": [

{

"id": "[resourceId('Microsoft.Network/networkInterfaces','myNic')]"

}

]

}

}

}

]

}

4 Once copied select **OK** then **Add**

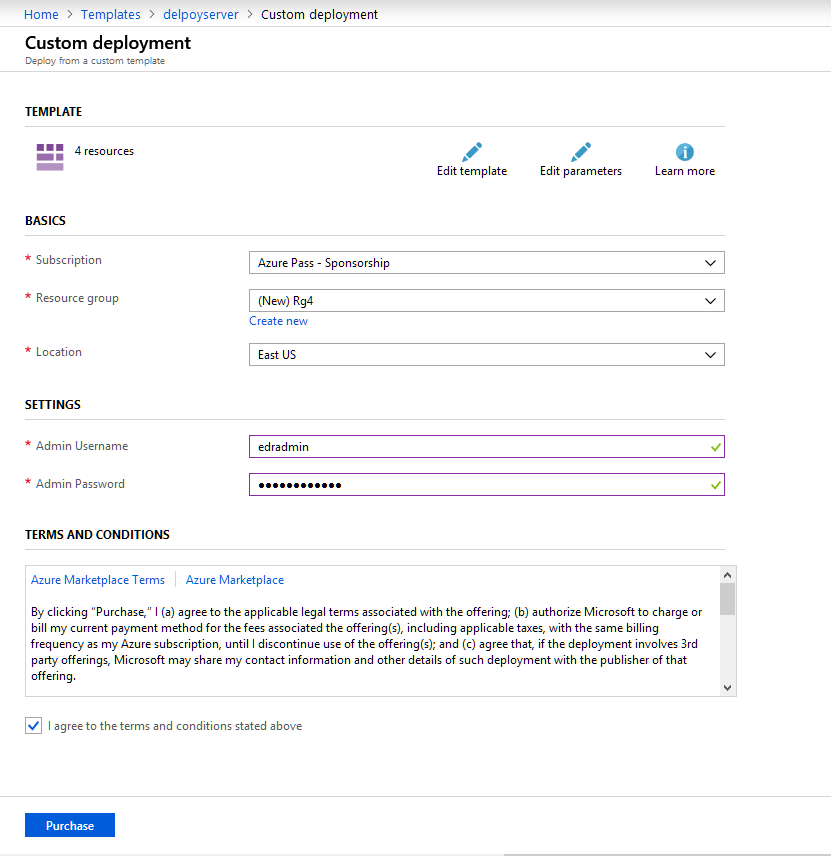
5 Select Refresh, then select the deployserver template

6 Select Deploy

7 Create a new Resource Group and name it **Rg4**

8 Add the credentials, user name **AnAdmin**, pwd **Pa55w.rd1234**

9 Select the **I agree** checkbox



10 Click **Purchase**

You Just deployed a VM using a Template.

**Lab 5 B**

**Exercise 1 Lock resources to prevent unexpected changes**

In this Lab, how locks are appliedWho can create or delete locks in your organizationPortalTemplatePowerShellAzure CLIREST APINext steps

As an administrator, you may need to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. You can set the lock level to CanNotDelete or ReadOnly. In the portal, the locks are called Delete and Read-only respectively.

CanNotDelete means authorized users can still read and modify a resource, but they can't delete the resource.

ReadOnly means authorized users can read a resource, but they can't delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

How locks are applied

When you apply a lock at a parent scope, all resources within that scope inherit the same lock. Even resources you add later inherit the lock from the parent. The most restrictive lock in the inheritance takes precedence.

Unlike role-based access control, you use management locks to apply a restriction across all users and roles. To learn about setting permissions for users and roles, see Azure Role-based Access Control.

Resource Manager locks apply only to operations that happen in the management plane, which consists of operations sent to https://management.azure.com. The locks do not restrict how resources perform their own functions. Resource changes are restricted, but resource operations are not restricted. For example, a ReadOnly lock on a SQL Database prevents you from deleting or modifying the database, but it does not prevent you from creating, updating, or deleting data in the database. Data transactions are permitted because those operations are not sent to https://management.azure.com.

Applying ReadOnly can lead to unexpected results because some operations that seem like read operations actually require additional actions. For example, placing a ReadOnly lock on a storage account prevents all users from listing the keys. The list keys operation is handled through a POST request because the returned keys are available for write operations. For another example, placing a ReadOnly lock on an App Service resource prevents Visual Studio Server Explorer from displaying files for the resource because that interaction requires write access.

Who can create or delete locks in your organization

To create or delete management locks, you must have access to Microsoft.Authorization/\* or Microsoft.Authorization/locks/\* actions. Of the built-in roles, only Owner and User Access Administrator are granted those actions.

**Task 1 Portal**

1 In the Settings blade for the resource, resource group, or subscription that you wish to lock, select **Locks**.

2 Select **Add**. If you want to create a lock at a parent level, select the parent. The currently selected resource inherits the lock from the parent. For example, you could lock the resource group to apply a lock to all its resources.

3 Give the lock a name and lock level. Optionally, you can add notes that describe the lock.

4 Delete the lock, select the **ellipsis** and **Delete** from the available options.

**Example Template**

The following **example** shows a template that creates an app service plan, a web site, and a lock on the web site. The resource type of the lock is the resource type of the resource to lock and /providers/locks. The name of the lock is created by concatenating the resource name with /Microsoft.Authorization/ and the name of the lock.

JSON

{

"$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",

"contentVersion": "1.0.0.0",

"parameters": {

"hostingPlanName": {

"type": "string"

}

},

"variables": {

"siteName": "[concat('ExampleSite', uniqueString(resourceGroup().id))]"

},

"resources": [

{

"apiVersion": "2016-09-01",

"type": "Microsoft.Web/serverfarms",

"name": "[parameters('hostingPlanName')]",

"location": "[resourceGroup().location]",

"sku": {

"tier": "Free",

"name": "f1",

"capacity": 0

},

"properties": {

"targetWorkerCount": 1

}

},

{

"apiVersion": "2016-08-01",

"name": "[variables('siteName')]",

"type": "Microsoft.Web/sites",

"location": "[resourceGroup().location]",

"dependsOn": [

"[resourceId('Microsoft.Web/serverfarms', parameters('hostingPlanName'))]"

],

"properties": {

"serverFarmId": "[parameters('hostingPlanName')]"

}

},

{

**"type": "Microsoft.Web/sites/providers/locks",**

**"apiVersion": "2016-09-01",**

**"name": "[concat(variables('siteName'), '/Microsoft.Authorization/siteLock')]",**

"dependsOn": [

"[resourceId('Microsoft.Web/sites', variables('siteName'))]"

],

"properties": {

"level": "CanNotDelete",

"notes": "Site should not be deleted."

}

}

]

}

**Exercise 2 To deploy this example template with PowerShell**

**1. Open Cloud Shell**

|  |  |
| --- | --- |
| Open Cloud Shell in your browser. | <https://shell.azure.com/powershell> |
| Click the **Cloud Shell** button on the menu in the upper right of the Azure portal. | [Cloud Shell in the portal](https://portal.azure.com/) |

2. **Create Resource Group**

*New-AzureRmResourceGroup -Name sitegroup -Location eastus*

3. ***Deploy using GitHub***

*New-AzureRmResourceGroupDeployment -ResourceGroupName sitegroup -TemplateUri https://raw.githubusercontent.com/Azure/azure-docs-json-samples/master/azure-resource-manager/lock.json -hostingPlanName plan0103*

**PowerShell**

You can lock deployed resources with Azure PowerShell by using the New-AzureRmResourceLock command.

To lock a resource, provide the name of the resource, its resource type, and its resource group name.

**4. Azure PowerShell**

*New-AzureRmResourceLock -LockLevel CanNotDelete -LockName LockSite -ResourceName examplesite -ResourceType Microsoft.Web/sites -ResourceGroupName sitegroup*

To lock a resource group, provide the name of the resource group.

**5. Azure PowerShell**

*New-AzureRmResourceLock -LockName LockGroup -LockLevel CanNotDelete -ResourceGroupName sitegroup*

To get information about a lock, use Get-AzureRmResourceLock. To get all the locks in your subscription, use:

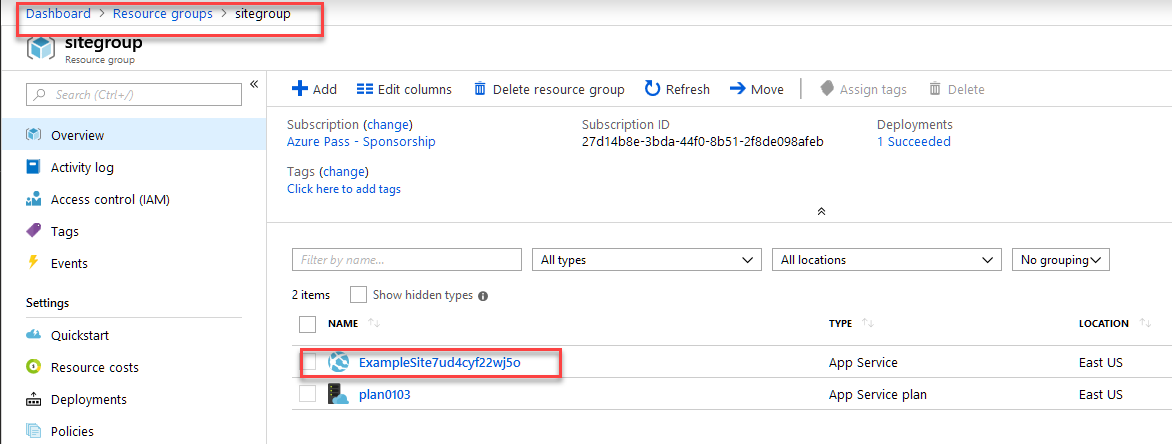
**6. Azure PowerShell**

*Get-AzureRmResourceLock*

To get all locks for a resource, use:

**7 Azure PowerShell**

* + - 1. Replace ***examplesite*** *with your site name which will be unique.*



*Get-AzureRmResourceLock -ResourceName* ***examplesite*** *-ResourceType Microsoft.Web/sites -ResourceGroupName sitegroup*

To get all locks for a resource group, use:

**8 Azure PowerShell**

*Get-AzureRmResourceLock -ResourceGroupName sitegroup*

To delete a lock, use:

**9 Azure PowerShell**

*$lockId = (Get-AzureRmResourceLock -ResourceGroupName sitegroup -ResourceName* ***examplesite*** *-ResourceType Microsoft.Web/sites).LockId*

*Remove-AzureRmResourceLock -LockId $lockId*