Enterprise-ready cloud

Hands-on lab step-by-step

March 2018

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The names of manufacturers, products, or URLs are provided for informational purposes only and Microsoft makes no representations and warranties, either expressed, implied, or statutory, regarding these manufacturers or the use of the products with any Microsoft technologies. The inclusion of a manufacturer or product does not imply endorsement of Microsoft of the manufacturer or product. Links may be provided to third party sites. Such sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

© 2018 Microsoft Corporation. All rights reserved.

Microsoft and the trademarks listed at <https://www.microsoft.com/en-us/legal/intellectualproperty/Trademarks/Usage/General.aspx> are trademarks of the Microsoft group of companies. All other trademarks are property of their respective owners

Contents

[Enterprise-ready cloud hands-on lab step-by-step 1](#_Toc510785946)

[Abstract and learning objectives 1](#_Toc510785947)

[Overview 1](#_Toc510785948)

[Requirements 1](#_Toc510785949)

[Solution architecture 2](#_Toc510785950)

[Before the hands-on lab 3](#_Toc510785951)

[Task 1: Validate global admin access to Azure AD tenant 3](#_Toc510785952)

[Task 2: Setup a development environment 4](#_Toc510785953)

[Exercise 1: Create the policy for Enterprise IT 5](#_Toc510785954)

[Help references 5](#_Toc510785955)

[Task 1: Create a Management Group 5](#_Toc510785956)

[Task 2: Apply the service catalog policy 7](#_Toc510785957)

[Task 3: Restrict the creation of ExpressRoute circuits 9](#_Toc510785958)

[Task 4: Restrict the creation of resources in regions 10](#_Toc510785959)

[Task 5: Create and apply a naming convention 12](#_Toc510785960)

[Task 6: Test the policies 17](#_Toc510785961)

[Exercise 2: Configure delegated permissions 23](#_Toc510785962)

[Help references 23](#_Toc510785963)

[Task 1: Create groups in Azure AD for delegation 23](#_Toc510785964)

[Task 2: Create user accounts in Azure AD for delegation 24](#_Toc510785965)

[Task 3: Enable a business unit administrator for the subscription 26](#_Toc510785966)

[Task 4: Enable project-based delegation and chargeback 28](#_Toc510785967)

[Exercise 3: Create the environment for the e-commerce team 31](#_Toc510785968)

[Help references 31](#_Toc510785969)

[Task 1: Create a new virtual network 31](#_Toc510785970)

[Task 2: Configure secure VPN for connectivity 34](#_Toc510785971)

[Task 3: Create an Azure DevTest lab environment 36](#_Toc510785972)

[Task 4: Test access to the DevTest labs environment 41](#_Toc510785973)

[Task 5: Finish configuring secure connectivity 45](#_Toc510785974)

[After the hands-on lab 52](#_Toc510785975)

[Task 1: Remove resources and configuration created during this lab 52](#_Toc510785976)

## Enterprise-ready cloud hands-on lab step-by-step

## Abstract and learning objectives

Create an Azure cloud governance plan to advise a manufacturing company of the features available in Azure. Discover features to bring governance to their Azure deployments, distributed administration, and allowance for secure remote connectivity and development work for their offshore developers. Attendees will be better able to design a governance plan to showcase the security and governance features of Azure and control costs. In addition,

* Provide for cost tracking by business unit, environment, and project
* Provide for a distributed administration model
* Put a service catalog in place to prevent deployment of unsupported Azure services
* Put controls in place to allow deployment of services only in specific regions

## Overview

In this hands-on lab, you are working with Trey Research to setup some best practices regarding policies, permissions, and remote access to their network. Some tasks will include creating scripts that Enterprise IT will use to automatically set policy and delegate permissions when a new subscription is created. You will also help them solve a critical problem for onboarding new developers and controlling access to what they can access on the network.

## Requirements

* Local machine or a virtual machine configured with:
  + Visual Studio 2015 or 2017 Community Edition or VS Code
* Full global admin access to the Azure AD tenant associated with your Azure subscription.

## Solution architecture



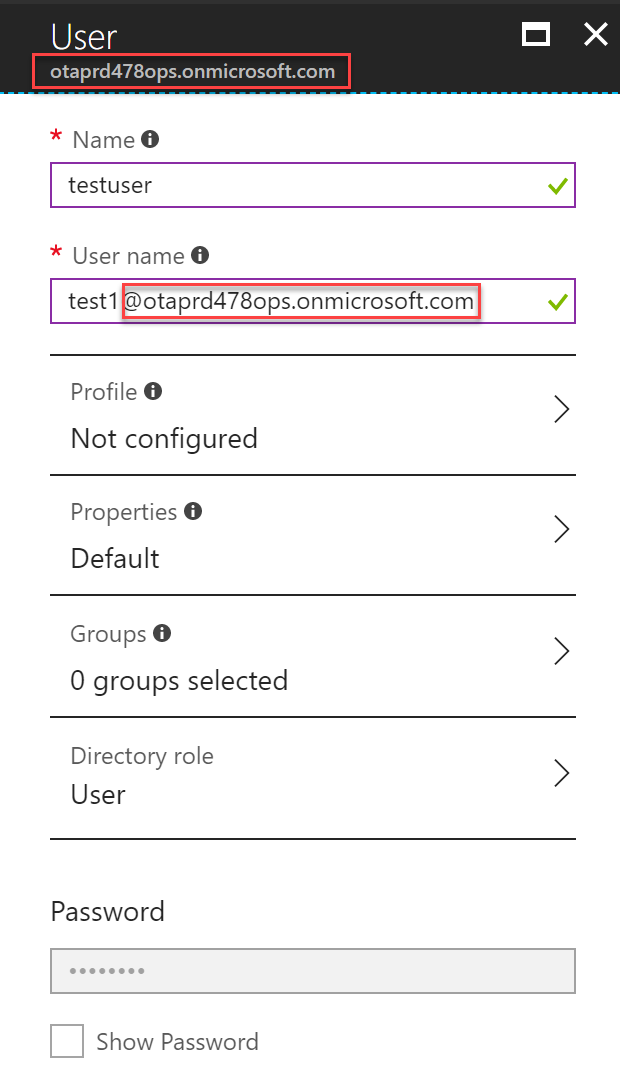
## Before the hands-on lab

Duration: 15 minutes

To complete this lab, you must have full global admin access to the Azure AD tenant associated with your Azure subscription.

#### Task 1: Validate global admin access to Azure AD tenant

1. Login to <http://portal.azure.com>, click on **All Services**, and type in **Azure Active Directory**.
2. Open the Azure Active Directory tenant. Click Users -> New User.
3. Create a new user called testuser/test1. Use the tenant name on the header for the domain name of the email.



**If you can create the user, you will enough permissions in Azure AD to complete the lab. If you cannot, you will need more permissions before proceeding.**

#### Task 2: Setup a development environment

If you do not have a machine set up with Visual Studio complete this task, and use this VM to complete the remainder of the Lab.

1. Create a DS2\_V2 Azure Virtual Machine using the Visual Studio Community 2017 image from the Azure Marketplace.

## Exercise 1: Create the policy for Enterprise IT

Duration: 60 minutes

In this exercise, you first create a Management Group for your Azure subscription(s). You will apply several of the built-in Azure Policy definitions to that Management Group to ensure that users stay within the scope of supported services for Enterprise IT. Finally, you will create a new policy initiative defining a multi-resource naming convention, and apply that initiative to the Management Group.

#### Help references

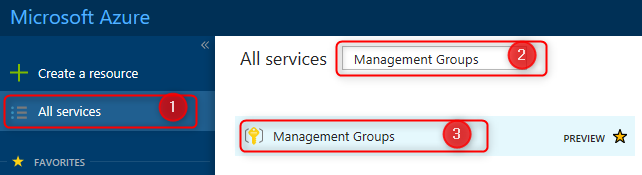
|  |  |
| --- | --- |
| Azure Policy | https://docs.microsoft.com/azure/azure-policy/azure-policy-introduction |
| Azure Management Groups | https://docs.microsoft.com/azure/azure-resource-manager/management-groups-overview |

#### Task 1: Create a Management Group

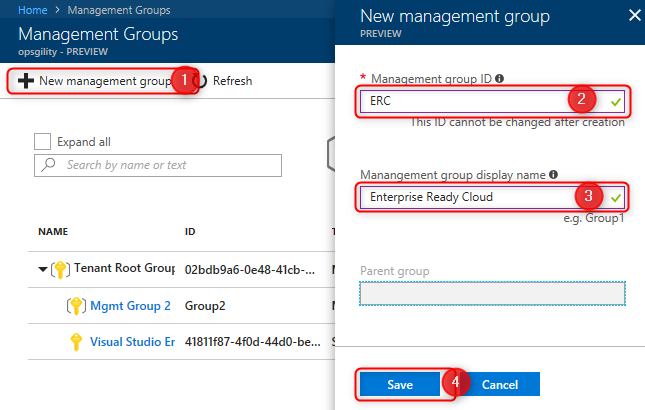
In this Task, you will create a new Management Group, and move a subscription into this Management Group. We’ll later assign Azure Policy using the Management Group scope, so that it applies automatically to all subscriptions under that scope.

Note: We’ll use our own Management Group, if you have permissions you could also use the Tenant Root Management Group.

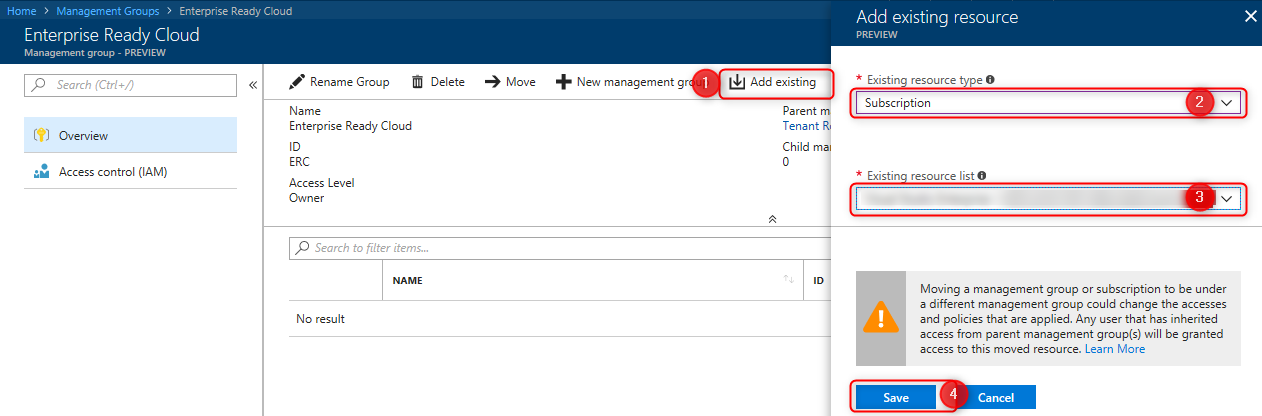
1. Launch the Azure Management Portal, and navigate to **Management Groups** under **All services**:



1. Click **New management group**, then fill in the management group ID and display name (we’ll use ‘ERC’ as the management group ID). Leave the Parent group blank (so our new group will sit under the Tenant Root Management Group), and click **Save**.



1. Click on the newly-created management group, then click **Add existing**. Select ‘Subscription’ as the existing resource type, and choose your subscription from the drop-down list, then click **Save**.



#### Task 2: Apply the service catalog policy

In this exercise, you will apply one of the built-in Azure Policies to restrict services to the supported list provided by Trey Research.

1. First, we need to build a list of resource types which will be permitted, and their corresponding resource providers. We’ll do that using PowerShell. Start PowerShell ISE, and log in to your Azure subscription:

Login-AzureRmAccount -Subscription "{subscription name or id}"

1. Enter the following script into the edit window, and run the script:

$FormatEnumerationLimit = -1

Get-AzureRmResourceProvider `

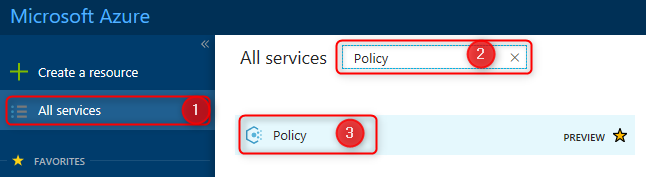
| Select-Object ProviderNamespace, ResourceTypes `

| Format-List

1. Review the list, and identify the resource providers and resource types for each of the following:

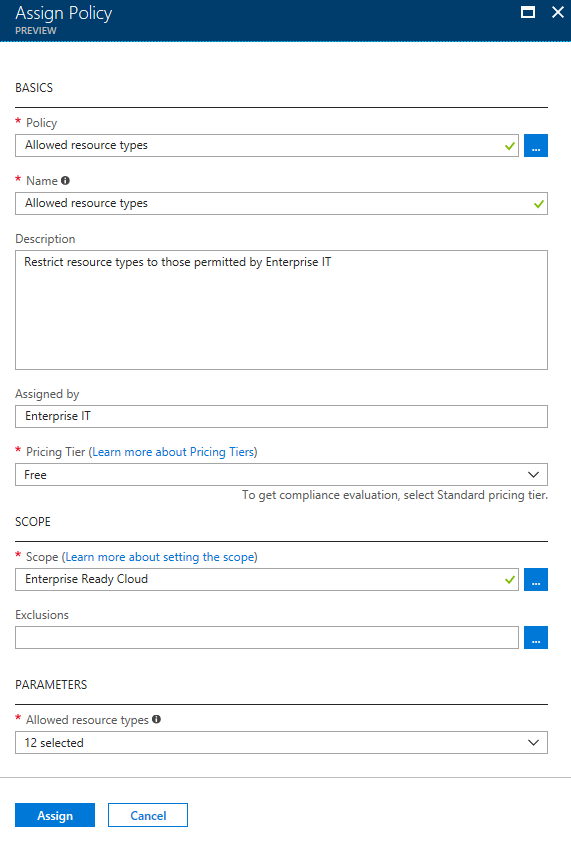
|  |
| --- |
| Resource Name |
| Resource Group |
| Virtual Machines |
| Disk |
| Network Interface |
| Public IP Address |
| Network Security Group |
| Virtual Networks |
| Virtual Network Gateways |
| ExpressRoute Circuits |
| VPN Gateways |
| Storage Accounts |
| Backup Vault |
| Site Recovery Vault |
| DevTest Labs |
| Key Vault |
| Web Apps |
| SQL Database |

1. Launch the Azure Management portal, and navigate to **Policy** under **All services**:



1. Click **Assignments**, then **Assign Policy**. Complete the form as follows:
   1. Policy: Select ‘Allowed resource types’
   2. Name: Service Catalog policy
   3. Description: Restrict resource types to those permitted by Enterprise IT
   4. Assigned by: Enterprise IT
   5. Pricing Tier: Standard
   6. Scope: Enterprise Ready Cloud (ERC) management group, as created in Task 1
   7. Exclusions: None
   8. Parameters | Allowed resource types: Choose the resource types identified in Step 3. (You may need to include some additional types, such as for NICs, Public IP Addresses, NSGs, etc.)

The assignment form should look like this:

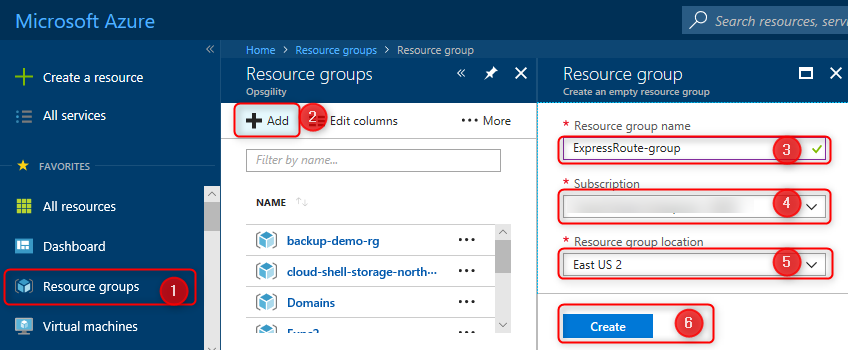


When complete, click **Assign** to create the policy assignment.

#### Task 3: Restrict the creation of ExpressRoute circuits

In this exercise, you will apply another built-in Azure policy to restrict the creation of ExpressRoute circuits. For this policy, we’ll use an exclusion scope for the resource group in which Enterprise IT will create the permitted ExpressRoute circuits.

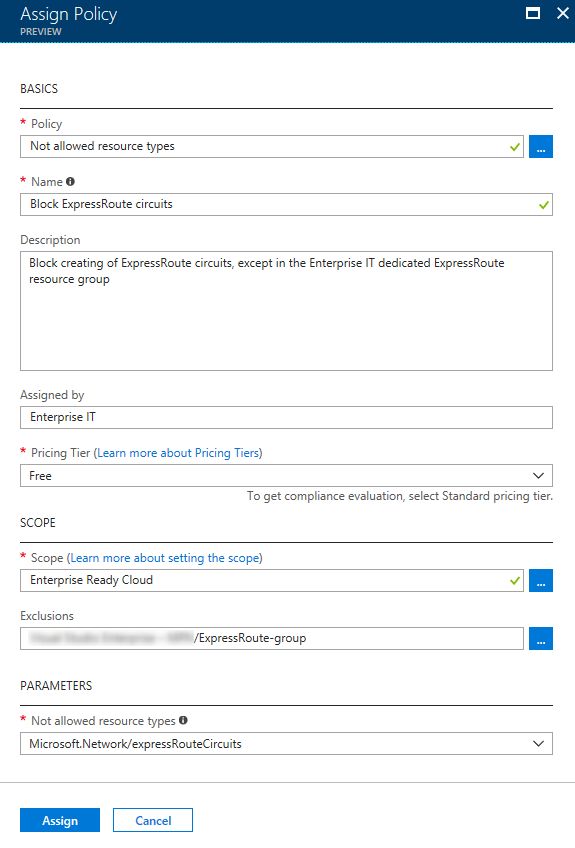
1. First, we’ll create the resource group for the exclusion scope. Click **Resource groups**, then **Add**, then fill in the resource group name, select your subscription, and choose a resource group location:



Once complete, click **Create**.

1. Return to the **Policy** blade in the Azure portal. Click **Assignments**, then **Assign Policy**. Complete the form as follows:
   1. Policy: Not allowed resource types
   2. Name: Block ExpressRoute circuits
   3. Description: Block creating of ExpressRoute circuits, except in the Enterprise IT dedicated ExpressRoute resource group
   4. Assigned by: Enterprise IT
   5. Pricing Tier: Standard
   6. Scope: Enterprise Ready Cloud (the management group created earlier)
   7. Exclusions: The resource group created in Step 1 above. Select the management group, subscription, and resource group.
   8. Parameters | Not allowed resource types: Microsoft.Network/expressRouteCircuits

The assignment form should look like this:



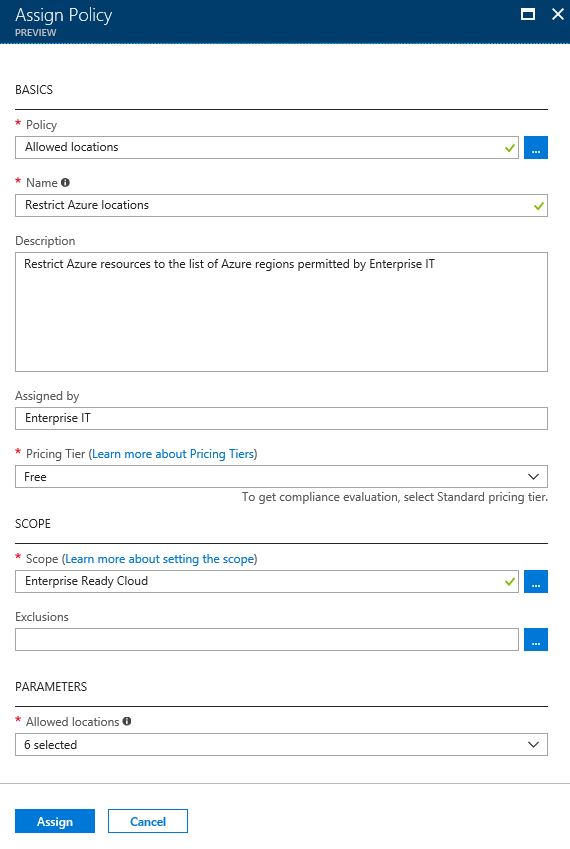
When complete, click **Assign** to create the policy assignment.

#### Task 4: Restrict the creation of resources in regions

In this exercise, you will create a new Azure Policy assignment that restricts which regions resources can be created in.

1. In the Azure portal, navigate to **Policy**, then click **Assignments**, then **Assign Policy**. Complete the form as follows:
   1. Policy: Allowed locations
   2. Name: Restrict Azure locations
   3. Description: Restrict Azure resources to the list of Azure regions permitted by Enterprise IT
   4. Assigned by: Enterprise IT
   5. Pricing Tier: Free
   6. Scope: Enterprise Ready Cloud (the management group created earlier)
   7. Exclusions: None
   8. Parameters | Allowed locations: East US, West US, North Europe, West Europe, Japan East, Japan West

The assignment form should look like this:



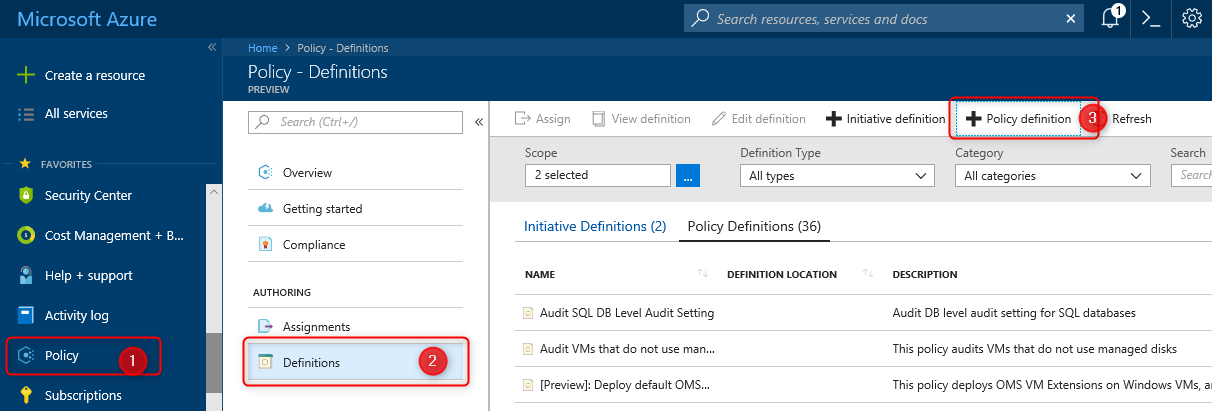
When complete, click **Assign** to create the policy assignment.

#### Task 5: Create and apply a naming convention

In this task, we will define a simple naming convention for Azure resources. We shall simply require that virtual machine names end with ‘-vm’, virtual networks end with ‘-vnet’, and so on across the various resource types. We shall implement this naming convention using custom policy definition and policy initiative, assigned at the management group scope.

First, we shall create a generic policy definition that restricts resources of a given type to have a given name suffix. The resource type and name suffix shall be specified using parameters.

1. In the Azure portal, open the **Policy** blade, then click **Definitions**, then **+ Policy definition**.



1. Complete the Policy definition form as follows:
   1. Definition location: Enterprise Ready Cloud (the Management Group created earlier)
   2. Name: Restrict Resource Name Suffix
   3. Description: Restrict resources of a given type to have a name ending with a given suffix. The resource type and suffix are parameterized.
   4. Category: Create New, “Naming”
   5. Policy rule and paramters: As shown below:

{

"properties": {

"mode": "all",

"parameters": {

"resourceType": {

"type": "string",

"metadata": {

"displayName": "Resource Type",

"description": "The resource type for this policy",

"strongType": "resourceTypes"

}

},

"nameSuffix": {

"type": "string",

"metadata": {

"displayName": "Resource Name Suffix",

"description": "The suffix that must be appended"

}

}

},

"policyRule": {

"if": {

"allof": [

{

"field": "type",

"equals": "[parameters('resourceType')]"

},

{

"not": {

"field": "name",

"like": "[concat('\*-', parameters('nameSuffix'))]"

}

}

]

},

"then": {

"effect": "deny"

}

}

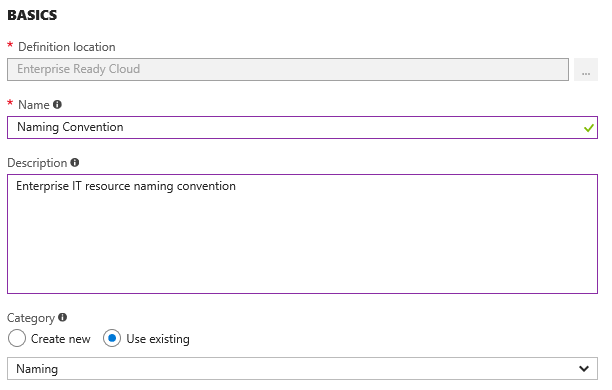
}

}

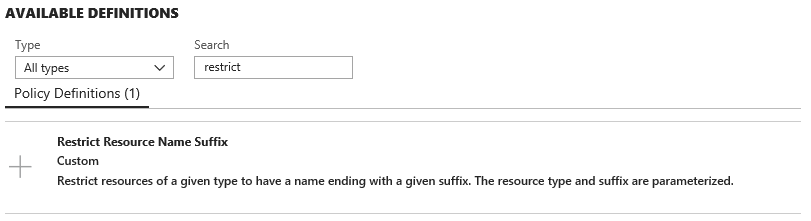
Once the policy definition is complete, click **Save**.

Next, we shall create a policy initiative comprising multiple instances of our policy definition (one per resource type).

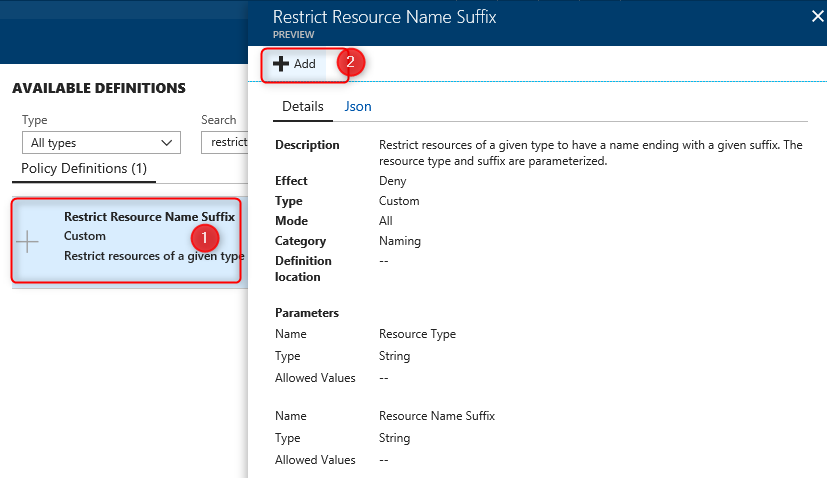
1. From the **Policy** blade, on the **Definitions** panel, click **+Initiative Defintion**.
2. Fill in the Initiative Definition form as follows (but don’t click Save yet)
   1. Definition location: Enterprise Ready Cloud (the Management Group created earlier)
   2. Name: Naming Convention
   3. Description: Trey Research resource naming convention
   4. Category: Use Existing | Naming



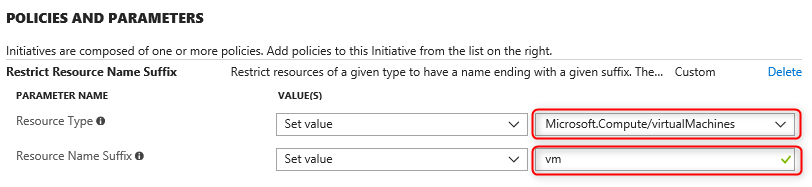
1. Under ‘Available Definitions’, find the ‘Restrict Resource Name Suffix’ policy definition created in Step 2.



1. Click on the policy definition, then click **+Add** to add the Policy Definition to the Policy Initiative.



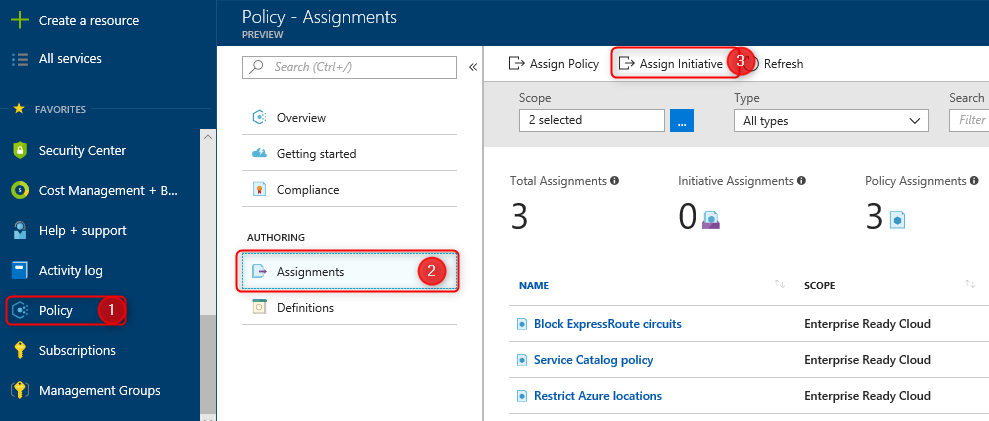
1. Select the resource type and name suffix. In this case, we’ll choose **Microsoft.Network/virtualMachines** as the resource type, and **vm** as the name suffix.



1. Repeat steps 6 and 7 above for each of the resource types you wish to include in the naming convention.
2. Once you’ve added each resource type, click **Save**.

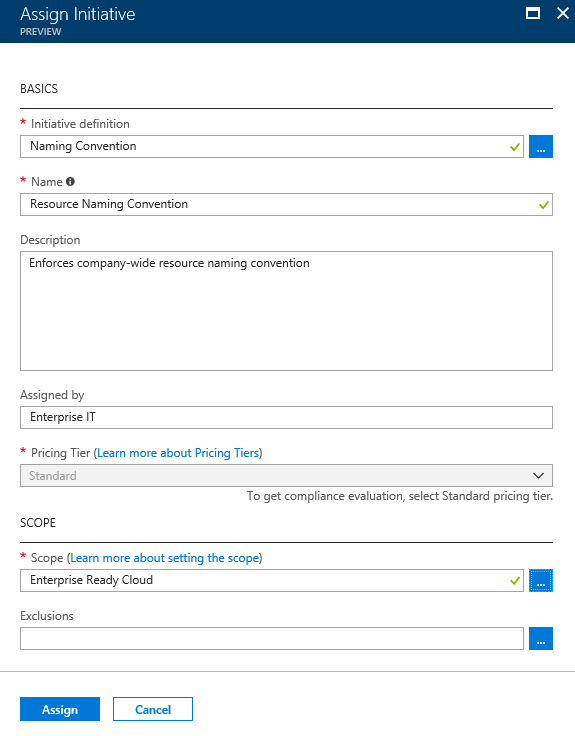
Finally, we will apply the policy initiative across all subscriptions in the Management Group by creating an assignment at the Management Group scope.

1. On the **Policy** blade, click **Assignments**, then **Assign Initiative**.



1. Complete the Assign Initiative form as follows:
   1. Initiative definition: Naming Convention (the initiative definition we just created)
   2. Name: Resource Naming Convention
   3. Description: Enforces company-wide resource naming convention
   4. Assigned by: Enterprise IT
   5. Pricing Tier: Standard
   6. Scope: Enterprise Ready Cloud (the Management Group created earlier)
   7. Exclusions: None

The assignment form should look like this:



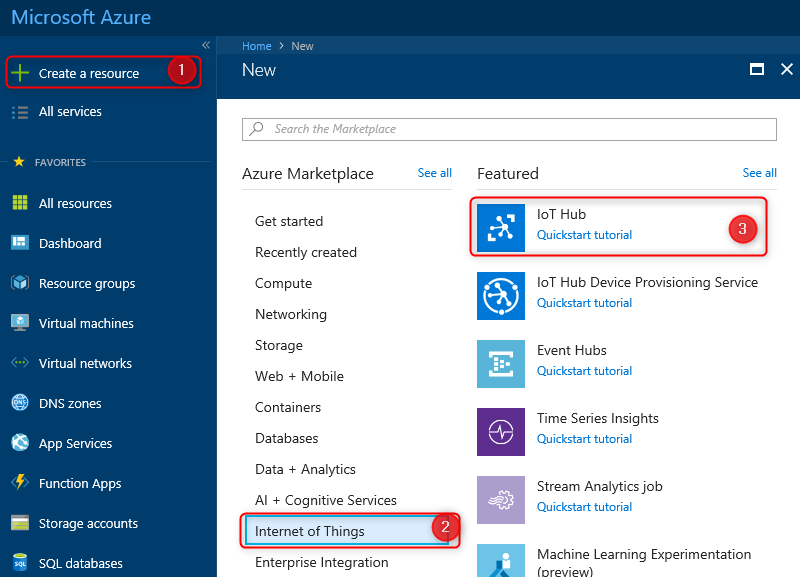
When complete, click **Assign** to create the policy initiative assignment.

#### Task 6: Test the policies

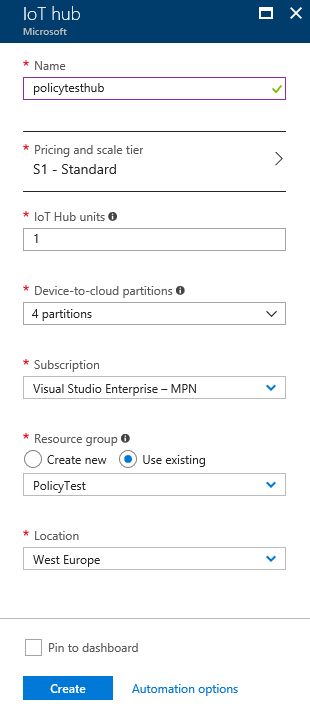
In this task, you will use the Azure management portal to validate each of the policies created so far, and to understand how to identify policy events.

**Subtask 1: Test the service catalog policy**

1. Navigate to the Azure management portal in a browser <http://portal.azure.com>, and sign in.
2. Click **Create a Resource > Internet of Things > IoT Hub**

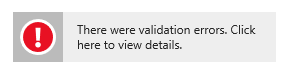


1. Specify a unique name for the IoT Hub, and choose an existing resource group. Choose a permitted location (we are only testing the Service Catalog policy at this time).

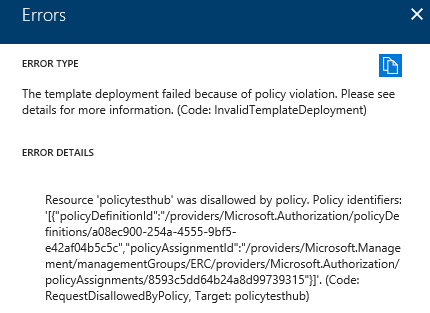


Once all the settings have been filled in, click **Create**.

1. The IoT Hub creation blade should show an error:

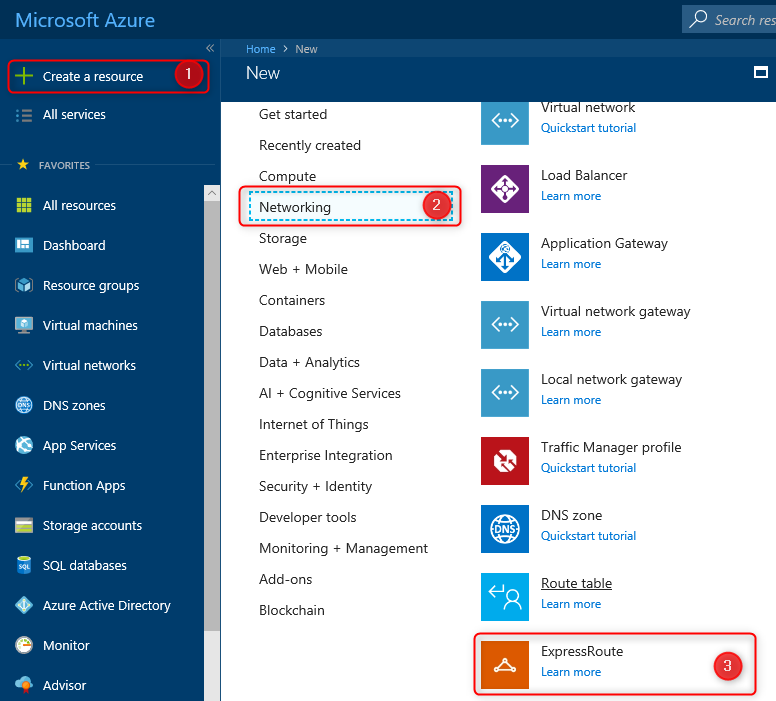


1. Click on the error. The following error details are displayed:



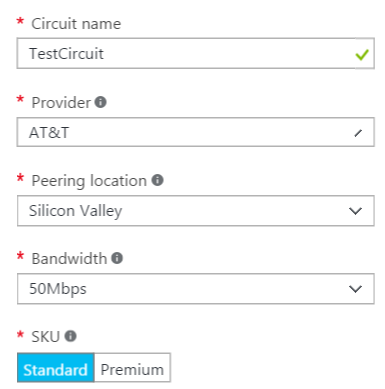
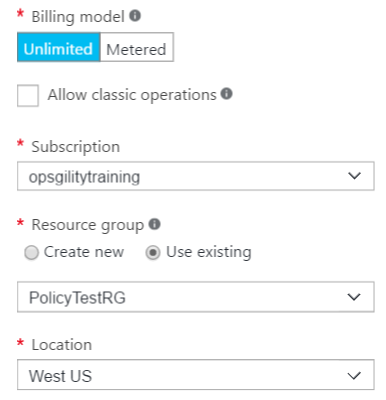
**Subtask 2: Test the ExpressRoute circuit policy**

1. Click **New** **>** **Networking** **>** **ExpressRoute**.

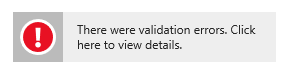


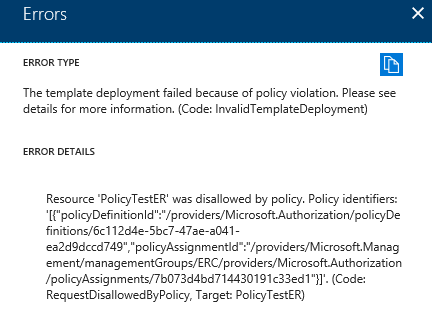
1. Specify the following configuration for the circuit and click **Create**.

Note: you may have to specify an alternate region if West United States is not supported with your subscription.

1. As with the Service Catalog policy, you should see an error in the Create ExpressRoute Circuit blade, which when clicked shows error details:





**SubTask 3: Test the resource location policy**

1. Testing the resource location policy follows a similar pattern. Attempt to create a permitted resource, with a permitted name, but in a not-permitted region. For example, create a virtual network named ‘erc-vnet’ in South Central US. This should be rejected by the ‘Restrict Azure locations’ policy.
2. To test further, change to a permitted location (e.g. East US) and try again—this time, the virtual network should be created OK. Note: you may need to refresh browser to release caching on policies.

**SubTask 4: Test the naming convention policy**

1. Attempt to create a permitted resource, in a permitted location, with a not-permitted name. For example, create a virtual network named ‘erc-network’ in East US. This should be rejected by the ‘Resource Naming Convention’ policy.
2. To test further, change to a permitted name (e.g. ‘erc-network-vnet’) and try again—this time, the virtual network should be created OK. Note: you may need to refresh browser to release caching on policies.

## Exercise 2: Configure delegated permissions

Duration: 60 minutes

In this exercise, you will configure delegated permissions for users in the Trey Research business unit. You will extend a PowerShell script to automatically provision a limited access user with the configuration of the subscription.

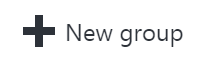
#### Help references

|  |  |
| --- | --- |
| Add new users to Active Directory | https://docs.microsoft.com/azure/active-directory/add-users-azure-active-directory |
| How Subscriptions are associated with Azure AD | https://docs.microsoft.com/azure/active-directory/active-directory-how-subscriptions-associated-directory |
| Managing Azure AD Security Groups | https://docs.microsoft.com/azure/active-directory/active-directory-groups-create-azure-portal |
| Role Based Access Control | https://docs.microsoft.com/azure/active-directory/role-based-access-control-configure |
| Manage RBAC with PowerShell | https://docs.microsoft.com/azure/active-directory/role-based-access-control-manage-access-powershell |

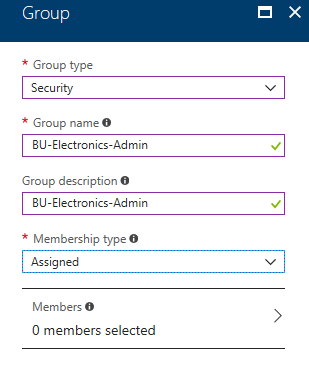
#### Task 1: Create groups in Azure AD for delegation

In this task, you will create two groups in Azure AD that you will use for testing delegated access control. You will add the users created in the previous task to the groups.

1. Open the Azure Active Directory console under the Azure Management portal in your browser (<https://portal.azure.com>).
2. Click **Groups**, and click **New group**.



1. Specify the **Security** as the Group type, **BU-Electronics-Admin** as the **Name** and **Description**, and change the Membership type to **Assigned**. Then, click **Create**.



1. Repeat the process, and create another group named **BU-Electronics-Users.**

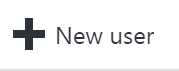
#### Task 2: Create user accounts in Azure AD for delegation

In this task, you will create two user accounts in Azure AD that you will use for testing delegated access control.

1. Navigate to **All services -> Azure Active Directory**, and click on **Custom domain names** to find out the name of your Azure AD tenant (this will be needed in the next step).



1. Click **Users**, and click **+New user**.



1. Specify the following configuration for the new user:

|  |  |
| --- | --- |
| **Name**  Electronics Admin  **User name:** [ElectronicsAdmin@[yourtenant].onmicrosoft.com](mailto:ElectronicsAdmin@[yourtenant].onmicrosoft.com)  **Groups**  Add the user to the BU-Electronics-Admin group.  **Password**  Check the Show password checkbox and note the password for later. | In the New User dialog box, the Name, User name, and Groups fields are circled, and set to the previously defined settings. At the bottom, the check box for Show Password is selected and circled. |

1. Create a second user with the following configuration:

|  |  |
| --- | --- |
| **Name**  Electronics User  **User name:** [ElectronicsUser@[yourtenant].onmicrosoft.com](mailto:ElectronicsUser@[yourtenant].onmicrosoft.com)  **Groups**  Add the user to the BU-Electronics-User group.  **Password**  Check the Show password checkbox and note the password for later. | In the New User dialog box, the Name, User name, and Groups fields are circled, and set to the previously defined settings. At the bottom, the check box for Show Password is selected and circled. |

#### Task 3: Enable a business unit administrator for the subscription

In this task, you will update a script to automatically add a user to the contributor role of the subscription.

1. Open PowerShell ISE, and log in to your Azure account

Login-AzureRmAccount

1. Create a new script **ConfigureSubscription.ps1** in PowerShell ISE.
2. Add the following code to script, and save the file. This code will retrieve the object ID for the Active Directory group passed in and assign the group to the Contributor role on the subscription.

param([string]$SubscriptionId, [string]$AdGroupName)

Select-AzureRmSubscription -SubscriptionId $SubscriptionId

$scope = "/subscriptions/$SubscriptionId"

$groupObjectId = (Get-AzureRmADGroup -SearchString $AdGroupName).Id.Guid

Write-Host "Adding group to contributor role" -ForegroundColor Green

New-AzureRmRoleAssignment -Scope $scope `

-RoleDefinitionName "Contributor" `

-ObjectId $groupObjectId

This code will add an Azure AD security group to the contributor role at the subscription scope.

1. Create a local variable containing your Subscription ID (you can copy your subscription ID from the Azure portal, or obtain it using Get-AzureRmSubscription):

Paste this under the param section of the script and save.

$SubscriptionId = "{your subscription id}"

1. Execute the script passing in the -SubscriptionID and -AdGroupName parameters:

.\ConfigureSubscription.ps1 -SubscriptionId $SubscriptionId -AdGroupName "BU-Electronics-Admin"

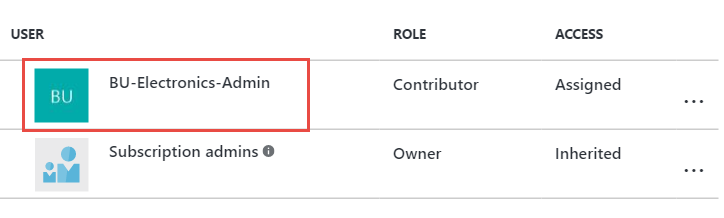
1. Close all instances of your browser (or switch to a different type of browser) and re-launch In-Private or Incognito mode.
2. Navigate to the Azure management portal in a browser <http://portal.azure.com>, and sign in using the **ElectronicsAdmin** credentials created earlier. When prompted to change your password, specify a strong password you will remember.
3. You will need to configure a method of resetting your account. You can choose either a phone call or email.
4. Click **All services**, then **Subscriptions**.



1. Click the name of the subscription you have been working on.
2. Click the **Access control (IAM)** tile:



1. You should see the BU-Electronics-Admin group assigned to the contributor role.



Users in the contributor role scoped at the subscription have full access to all resources within the subscription but cannot grant access to others or change policies on the subscription.

#### Task 4: Enable project-based delegation and chargeback

In this task, you will create a script that will create a new resource group, assign ‘Owner’ rights over the resource group to a given AD group, and apply a policy to enforce an ‘IOCode’ tag with a given value.

1. Using PowerShell ISE, click **File > New**, and save the file in the **C:\Hackathon\ERC** folder. Name the file **CreateProjectResourceGroup.ps1**.
2. Add the following code to the script, and **Save** the file.

param(

[string]$SubscriptionId,

[string]$ResourceGroupName,

[String]$Location,

[String]$IOCode,

[string]$AdGroupName

)

Select-AzureRmSubscription -SubscriptionId $SubscriptionId

# Create resource group

New-AzureRmResourceGroup -Name $ResourceGroupName -Location $Location

$scope = "/subscriptions/$subscriptionId/resourceGroups/$resourceGroupName"

# Assign Owner role to given group

$groupObjectId = (Get-AzureRmADGroup -SearchString $AdGroupName).Id.Guid

New-AzureRmRoleAssignment -Scope $scope `

-RoleDefinitionName "Owner" `

-ObjectId $groupObjectId

# Assign policy to apply IOCode tag

$definition = Get-AzureRmPolicyDefinition | where {$\_.Properties.displayName -eq "Apply tag and its default value"}

$parameters = @{

tagName = 'IOCode'

tagValue = $IOCode

}

New-AzureRmPolicyAssignment -Name "AppendIOCode" `

-Scope $scope `

-DisplayName "Append IO Code" `

-PolicyDefinition $definition `

-PolicyParameterObject $parameters

This code creates a new resource group in the specified region. It then assigns the group to the owner role definition just for the resource group. It will allow users in the group to have full ownership of resources within the resource group only. This code then applies a built-in policy to append a tag with name ‘IOCode’ and the given tag value to any resource created in the resource group.

1. In the **Console** pane, create a new variable called **$location**, and specify a region name to deploy to the resource group to. This location must be one of the supported regions in your previously created policy.

$location = "West US"

1. In the **Console** pane, create a new variable called **$resourceGroupName**, and specify the value as **DelegatedProjectDemo**. Also, make sure you create a **$SubscriptionId** variable as you did earlier.

$resourceGroupName = "DelegatedProjectDemo"

$SubscriptionId = "{your subscription id}"

1. In the **Console** pane, execute the following command to create a new resource group with delegated permissions and IO Code policy.

.\CreateProjectResourceGroup.ps1 -SubscriptionId $SubscriptionId -ResourceGroupName $resourceGroupName -Location $location -IOCode "1000150" -AdGroupName "BU-Electronics-Admin"

1. Create a new storage account in the resource group (choose a unique name) to validate the ioCode tag was applied (replace uniquestorageaccount with a unique value).

New-AzureRmStorageAccount -ResourceGroupName $resourceGroupName `

-Name "uniquestorageaccount" -SkuName Standard\_LRS `

-Location $location

You should see the ioCode tag applied in the output.

Screenshot of the Console Pane displaying the following line of code:  Tags  : {[ioCode, 1000150]}

1. Switch back to the Azure Management portal using the ElectronicsAdmin credentials.
2. Click **Resource Groups.**
3. Click the **DelegatedProjectdemo** resource group.

Screenshot of the DelegatedProjectdemo resource group.

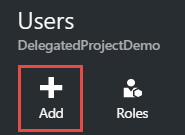
1. Click the **Access** icon.

Screenshot of the Access icon.

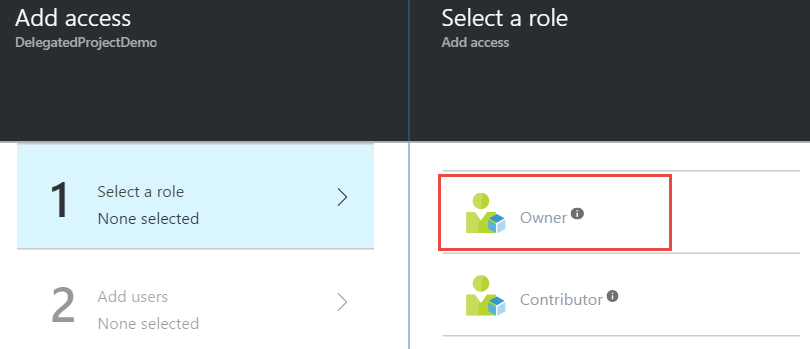
1. Note the BU-Electronics-Admin role is set as owner for the resource group.



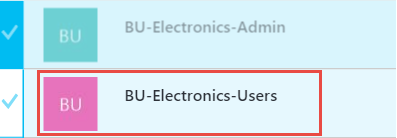
1. Click **Add**.



1. Select **Owner**.



1. Click the **BU-Electronics-Users group** > **Select** > **OK** to add the group to the role.



## Exercise 3: Create the environment for the e-commerce team

Duration: 75 minutes

In this exercise, you will configure a new environment for the developers of the e-commerce team. You will configure access to a subnet where other developer resources are available and provide secure access to the network for the developers.

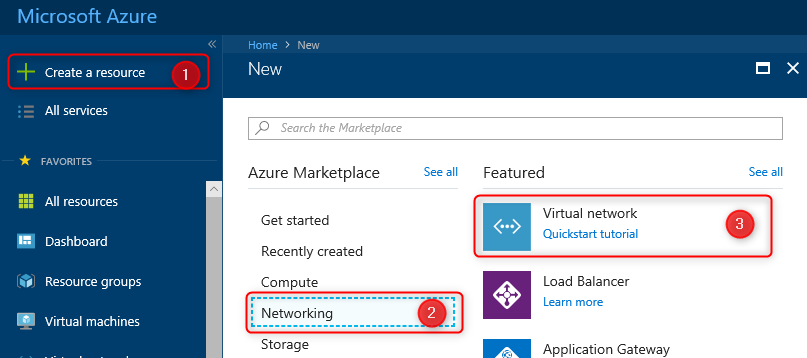
#### Help references

|  |  |
| --- | --- |
| Configuring Point-to-Site Secure VPN | https://docs.microsoft.com/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal |
| Network Security Groups | https://docs.microsoft.com/azure/virtual-network/virtual-networks-nsg |
| Azure DevTest Labs | https://docs.microsoft.com/azure/devtest-lab/ |
| MakeCert.exe | <https://cloudworkshop.blob.core.windows.net/enterprise-ready-cloud/makecert.exe> |

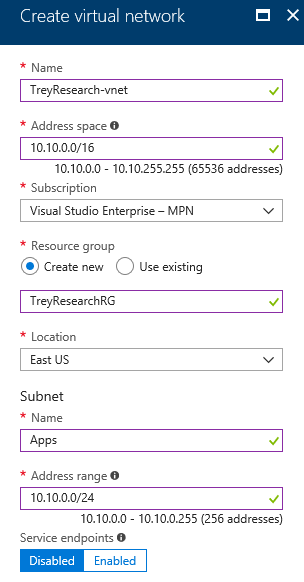
#### Task 1: Create a new virtual network

In this task, you will create a new virtual network for Trey Research.

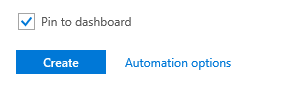
1. Sign in to the Azure Management portal using the subscription owner user account.
2. Click **New** **> Networking >** **Virtual Network**.



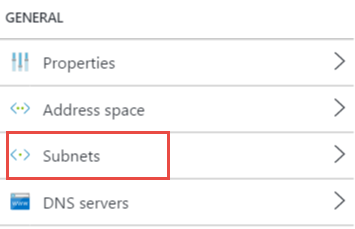
1. Specify the following configuration for the virtual network:
   1. Name: TreyResearch-vnet
   2. Address Space: 10.10.0.0/16
   3. Resource Group: TreyResearchRG (Create New)
   4. Location: Choose one of the supported regions.
   5. Subnet Name: Apps
   6. Subnet Address Range: 10.10.0.0/24
   7. Service endpoints: Disabled



1. Select Pin to dashboard, and click **Create**.



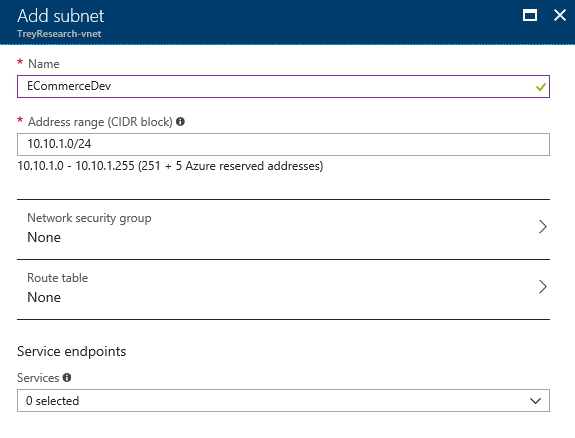
1. After the virtual network is open, click **Subnets.**



1. Click **+Subnet**.



1. Name the subnet **ECommerceDev**, and specify the Address Range as **10.10.1.0/24**.



1. Click **+ Gateway subnet** to add a gateway subnet to the virtual network. Note: VPN gateway and ExpressRoute gateway could be co-existing at Gateway subnet. We recommend that you create a gateway subnet of /27 or larger (/27, /26, /25 etc.)

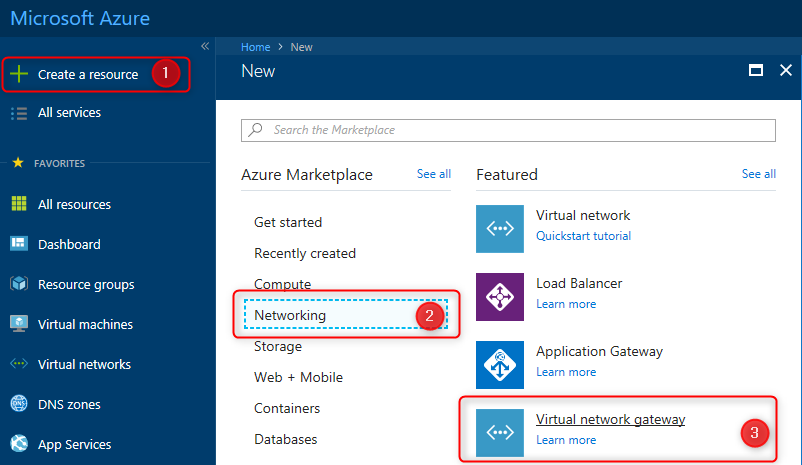


1. Click **OK** on the new blade that opens to create the Gateway subnet with default settings.

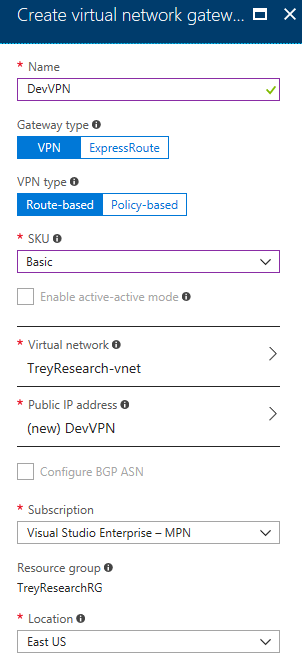
#### Task 2: Configure secure VPN for connectivity

In this task, you will start provisioning of a VPN gateway that will be used for secure connectivity for Trey Research.

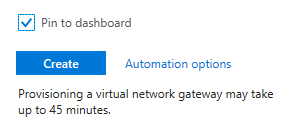
1. Click **Crate a resource** > **Networking** **>** **Virtual network gateway.**



1. Name the VPN Gateway **DevVPN**, select the existing **TreyResearchVNET** virtual network, specify the Basic SKU, and specify a new Public IP address named **DevVPN** (again, with the Basic SKU). Note: The Basic SKU is considered a legacy SKU. The Basic SKU has certain feature limitations, it is for Dev-test or proof of concept. You can't resize a gateway that uses a Basic SKU to one of the new gateway SKUs.



1. Select **Pin to dashboard**, and click **Create** to start provisioning the VPN gateway.

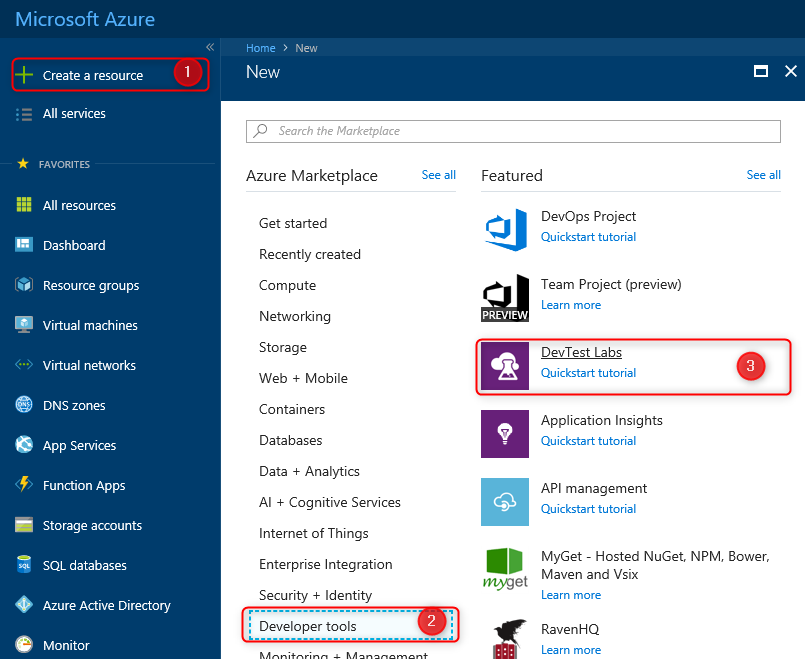


This step will take up to 45 minutes to complete. Continue to the next task. Gateway configuration will be continued in a later task.

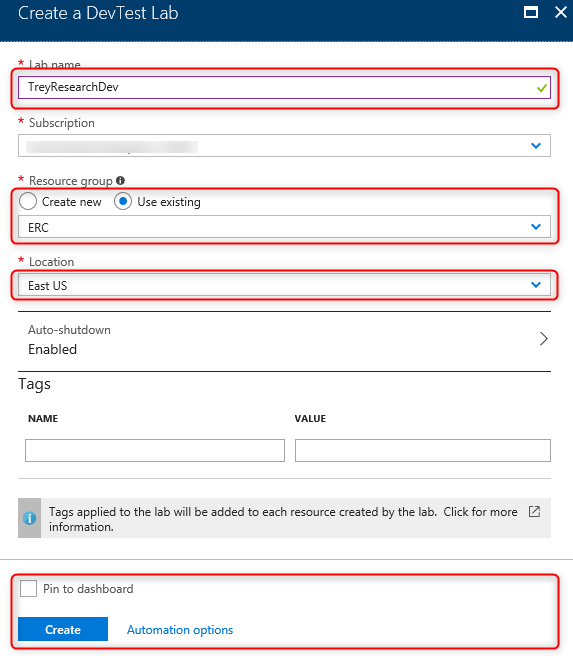
#### Task 3: Create an Azure DevTest lab environment

In this task, you will create and configure a new development environment for Trey Research developers and contingent staff.

1. Click **Create a resource** **>** **Developer tools >** **DevTest Labs**.

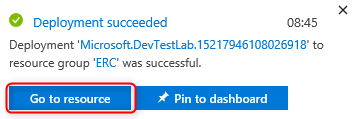


1. Name the lab **TreyResearchDev-vnet**, and specify the same region you deployed the virtual network to.

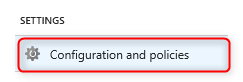


When done, click **Create**.

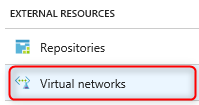
1. Open the DevTest lab environment following the completion of provisioning.



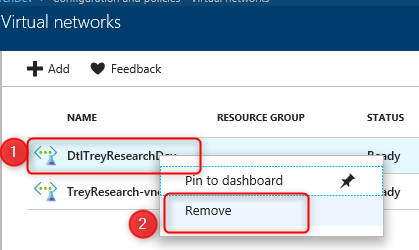
1. Open **Settings > Configuration and policies**.



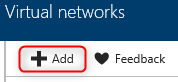
1. Click **Virtual Networks**.



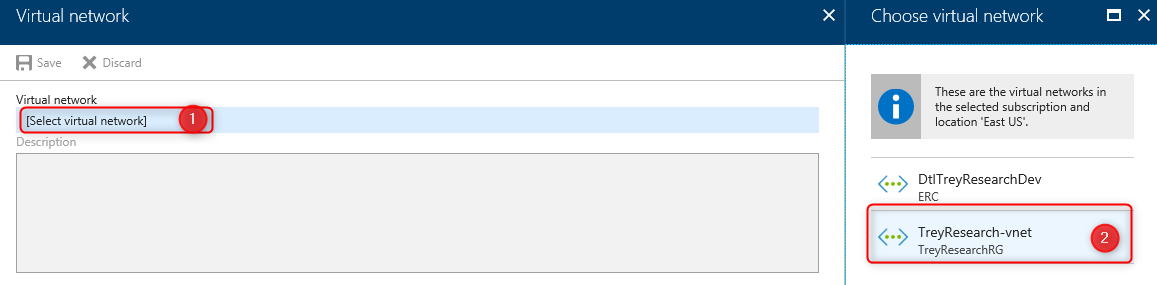
Right-click the default virtual network created for the DevTest lab environment, and click **Remove**.



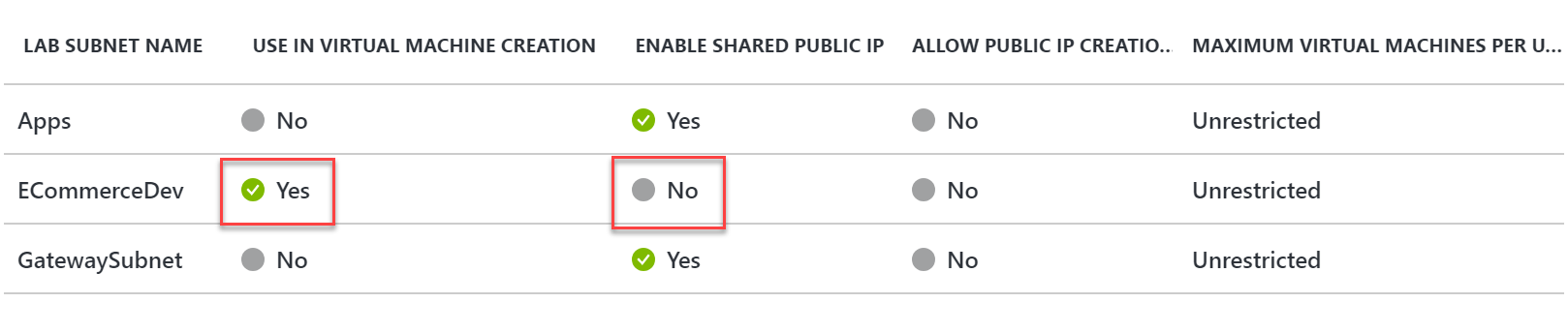
1. Click the **Add** button.



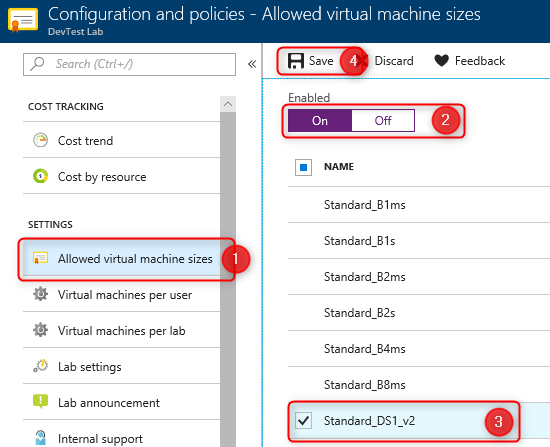
1. Click **[Select virtual network]**, and select **TreyResearch-vnet**



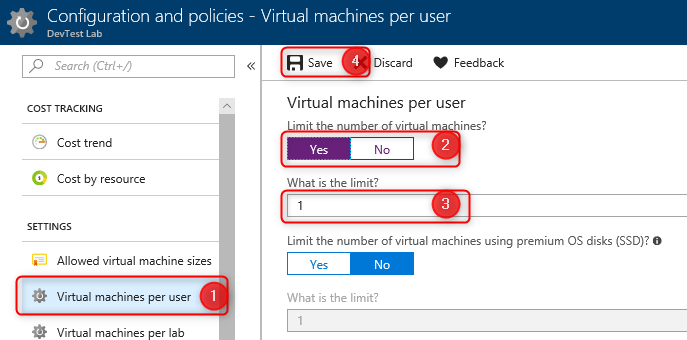
1. Configure the ECommerceDev subnet to **allow** **USE IN VIRTUAL MACHINE CREATION**, and to **disable ENABLE SHARED PUBLIC IP**. Then, click **Save** and close the blade.



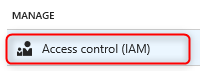
1. Configure a virtual machine policy for this DevTest lab by clicking **Allowed virtual machine sizes**, select **Standard\_DS2\_v2 (or Standard\_DS2)**, and click **Save**.



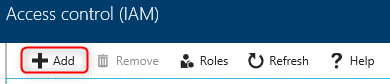
1. Enable the virtual machines per user policy. Set a maximum number of virtual machines per user to one, and click **Save**.



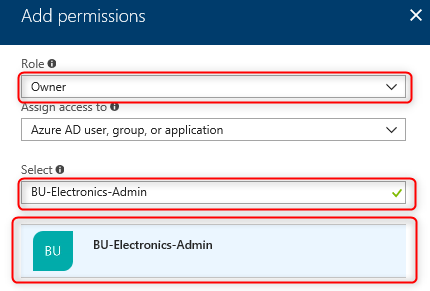
1. Allow access to the DevTest labs users by **Access control** icon within Configuration and Policies.



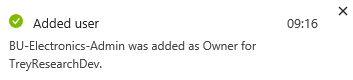
1. Click **+Add**



1. Select **Role** as **Owner**, type ‘BU-Electronics-Admin into the search field and select the **BU-Electronics-Admin** group.



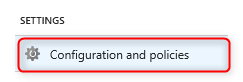
Then click **Save**.



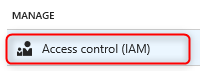
#### Task 4: Test access to the DevTest labs environment

In this task, you will use the ElectronicsAdmin user account to grant access to the developer environment. Then, you will validate as a user whether access was successfully granted.

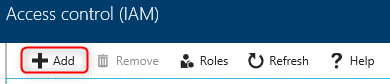
1. Sign in to the Azure Management Portal as the **ElectronicsAdmin** user account.
2. Open the DevTest labs environment by clicking **All services** **>** **DevTest Labs** **>** **TreyResearchDev**.
3. Click **Configuration and policies.**



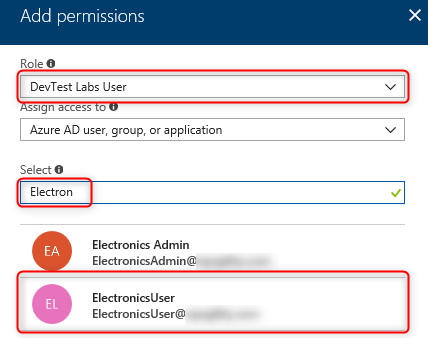
1. Allow access to the DevTest Labs users by clicking the **Access** **control** icon within Configuration and Policies.



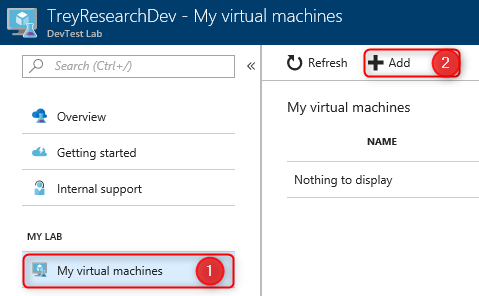
1. Click **+Add**



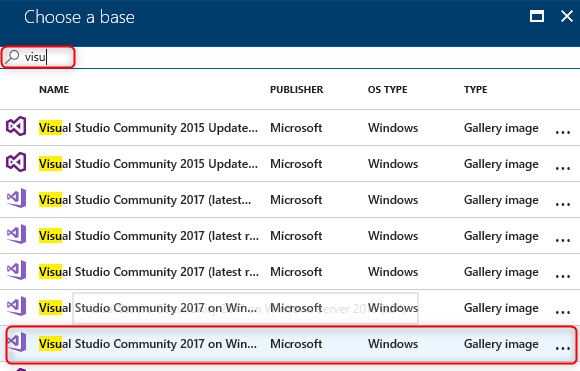
1. Specify the **Role** as **DevTest Labs User**. Use the search field to find the **ElectronicsUser** account, and select it. Then **Save**.



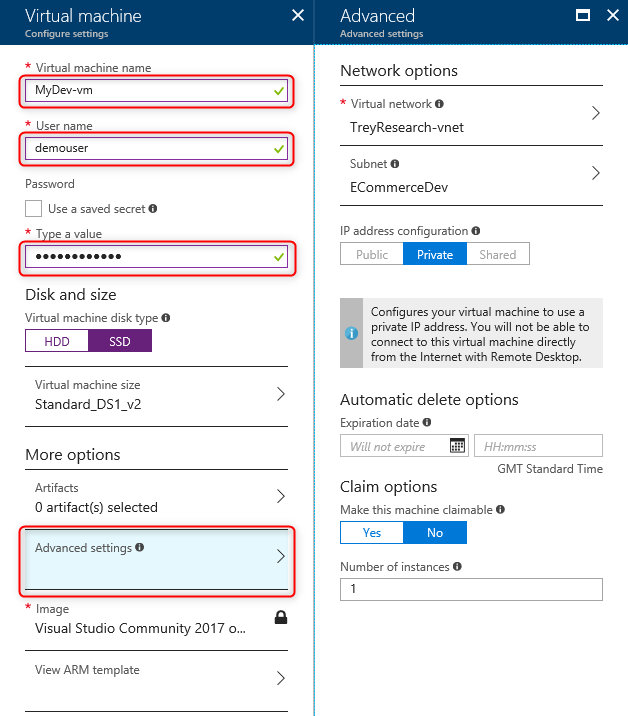
1. Close your browser and sign in with the **ElectronicsUser** account. You will have to change your password and setup a recovery mechanism with this account.
2. Open the DevTest labs environment by clicking **All services** **>** **DevTest Labs** **>** **TreyResearchDev**.
3. Click **My virtual machine**s, then **+Add** provision a virtual machine for the developer.

****

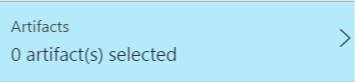
1. On the **Choose a Base** blade, select the **Visual Studio Community 2017 on Windows Server 2016 (x64)** image.



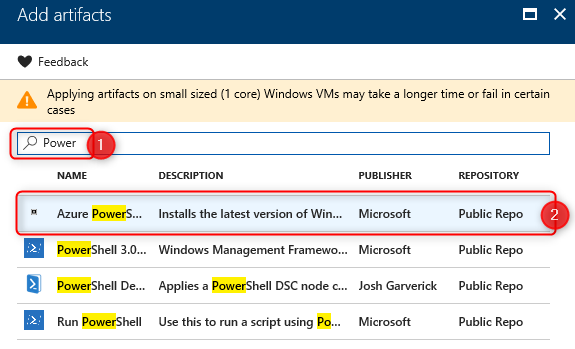
1. Specify the **virtual machine name** as well as a **user name** and **password**. Click **Advanced Settings** and note the VM size, IP address configuration, virtual network, and subnet are not changeable by the user.



1. Click **Artifacts**.



1. Add **Azure PowerShell** to the artifacts of the VM by selecting their names and clicking **ADD**. Click **OK** at the bottom of the **Add artifacts** blade when complete.



1. Click **Create** to provision the virtual machine.

NOTE: If you receive a Policy Error make sure that the VM Auto Shutdown Policy is enabled in your Allowed Resources.

#### Task 5: Finish configuring secure connectivity

In this task, you will configure certificates for the VPN gateway and for the end users as well as complete configuration of the VPN gateway. You will then configure and test access to the development environment.

**Subtask 1: Create certificates for point-to-site VPN**

1. Download makecert.exe from: <https://cloudworkshop.blob.core.windows.net/enterprise-ready-cloud/makecert.exe> and save it to the C:\Hackathon\ERC folder.
2. Launch a command prompt (run cmd.exe), and navigate to the **C:\Hackathon\ERC** folder by typing in the following command:

CD C:\Hackathon\ERC

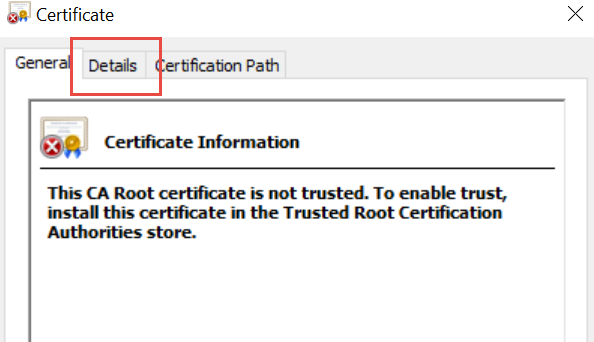
1. Execute the following command to generate a root certificate for configuring a point-to-site VPN gateway.

makecert -sky exchange -r -n "CN=P2SROOT" -pe -a sha1 -len 2048 -ss My .\P2SRoot.cer

1. Execute the following command to generate a client certificate:

makecert.exe -n "CN=P2SClient" -pe -sky exchange -m 96 -ss My -in "P2SRoot" -is my -a sha1

1. Using **File Explorer**, navigate to the C:\Hackathon\ERC folder, and double-click the **P2SRoot.cer** file.
2. Click the **Details** tab of the certificate.

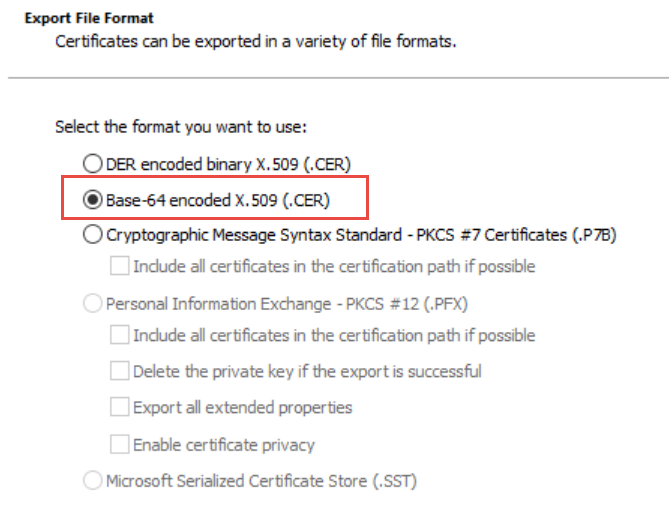


1. Click **Copy to File**.

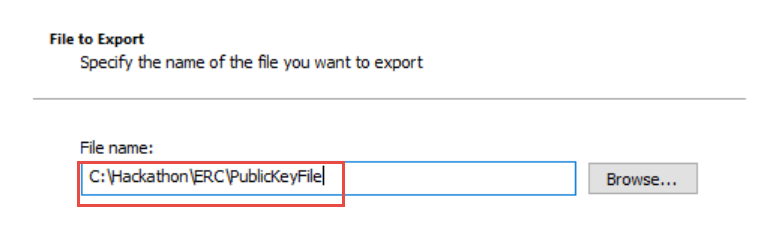
Screenshot of the Copy to file button.

Click **NEXT**

1. Change the encoding type to **Base-64 encoded X.509 (.CER)**, and click **Next**.



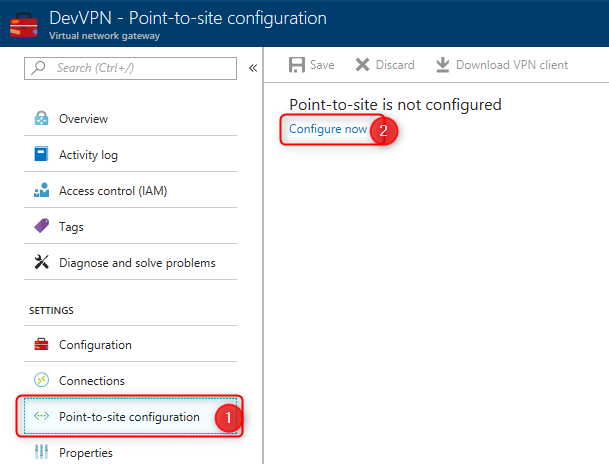
1. Specify the filename as **C:\Hackathon\ERC\PublicKeyFile**. Click **Next** and **Finish**.



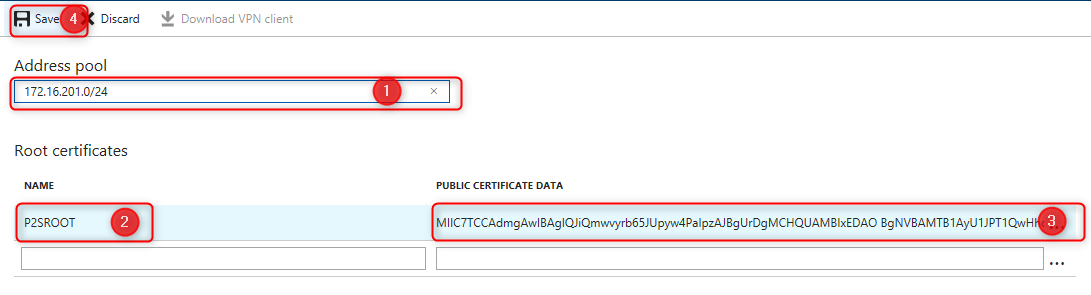
1. Open the newly created PublicKeyFile in Notepad, and copy the certificate text to the clipboard. Do NOT copy the first and last lines (containing -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----).

**Subtask 2: Configure the VPN gateway**

1. In the Azure Portal, make sure you are logged in as ElectronicsAdmin. Then, navigate to **All services** > **Virtual Network Gateways**, and click on the **DevVPN** gateway created earlier
2. Click **Point to site configuration**, and then **Configure Now**



1. In the **DevVPN – Point to site configuration** blade, enter the following details:
   1. Address pool: 172.16.201.0/24
   2. Under Root Certificates, enter
      1. Name: P2SROOT
      2. Public Certificate Data: Paste the certificate data copied to the clipboard earlier



Once complete, click **Save**.

**Subtask 3: Configure and test the client**

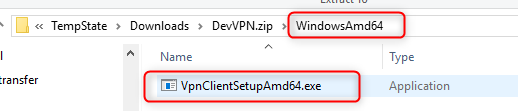
1. Once the P2S configuration has been saved, click **Download VPN Client**.



1. Click **Open**



1. Windows Explorer should open, showing the contents of the downloaded ZIP file. Open the **WindowsAmd64folder**, and copy the **VpnClientSetupAmd64.exe** file to the desktop.

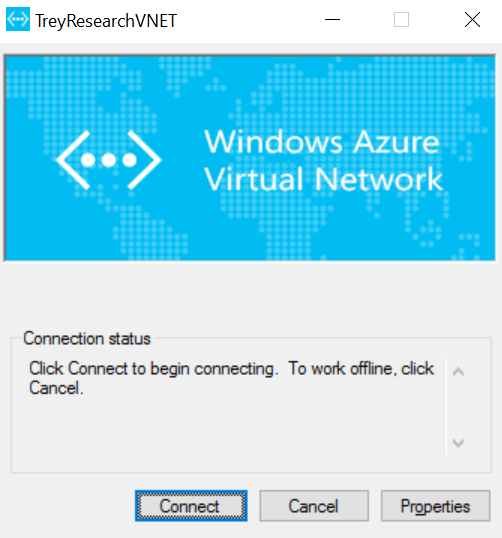


1. Run the **VpnClientSetupAmd64.exe** installer from the desktop. Accept any confirmation prompts.
2. The client computer should now have a new connection option in the same location as new wireless connections. Click the **TreyResearchVNET** icon to launch the connection.

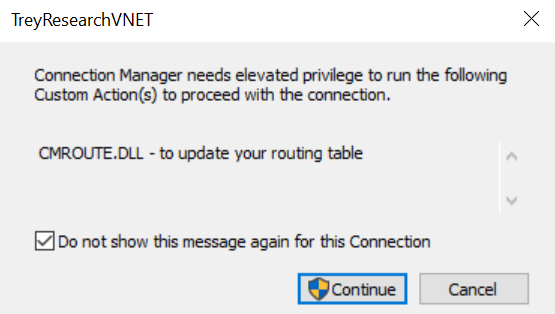


1. Click **Connect** to initiate connection.

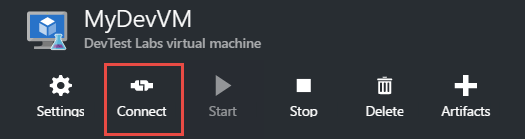




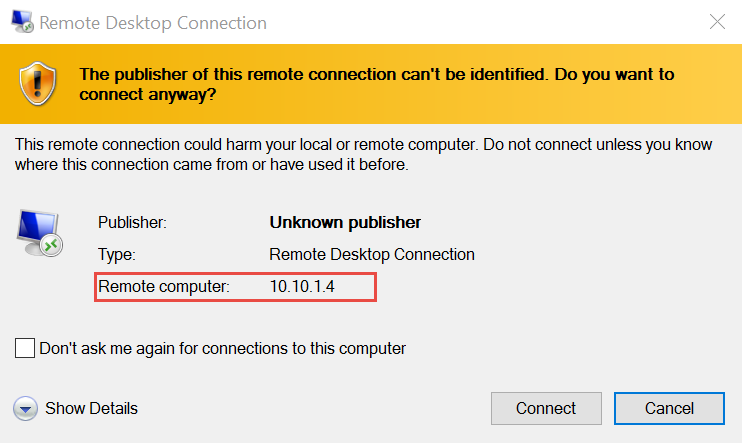
1. Select **Do not show this message again for this Connection**,and click **Continue**.



1. After you are successfully connected, switch back to the Azure Management Portal using the **ElectronicsUser** account.
2. Browse to **DevTest Labs**, open **TreyResearchLab**, and click **MyDevVM**.
3. Click **Connect** to initiate a connection with the virtual machine.



1. Note the remote computer is connecting over a Private IP address.



## After the hands-on lab

Duration: 10 minutes

After completing the hands-on lab, you will remove the policies on your subscription.

#### Task 1: Remove resources and configuration created during this lab

You should follow all steps provided *after* attending the hands-on lab.

1. Log in to the Azure portal.
2. Navigate to the **Policy** blade.
3. Click on **Assignments** and delete all policy assignments created during this lab
4. Click on **Definitions** and delete any policy definitions or initiative definitions created during this lab
5. Navigate to the **Management Groups** blade.
6. Remove any Management Groups crated during this lab.
7. Navigate to the **Resource Groups** blade.
8. Remove any resource groups created during this lab. This will also delete any resources in those resource groups.
9. Navigate to the **Azure Active Directory** blade
10. Remove any users and groups created during this lab.