Create a policy assignment with Azure Policy

Use Case:

In this walkthrough task we will locate an Azure Policy to restrict deployment of Azure resources to a particular Datacenter, and then assign that allowed location policy to a subscription. We will then verify that creating an Azure resource, such as a virtual machine, outside of the allowed location is blocked. We will finally remove the allowed location policy assignment, to allow us deploy resources again to any Datacenter location using that same subscription.

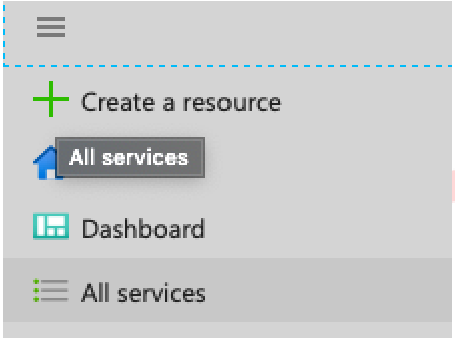
Prerequisites:

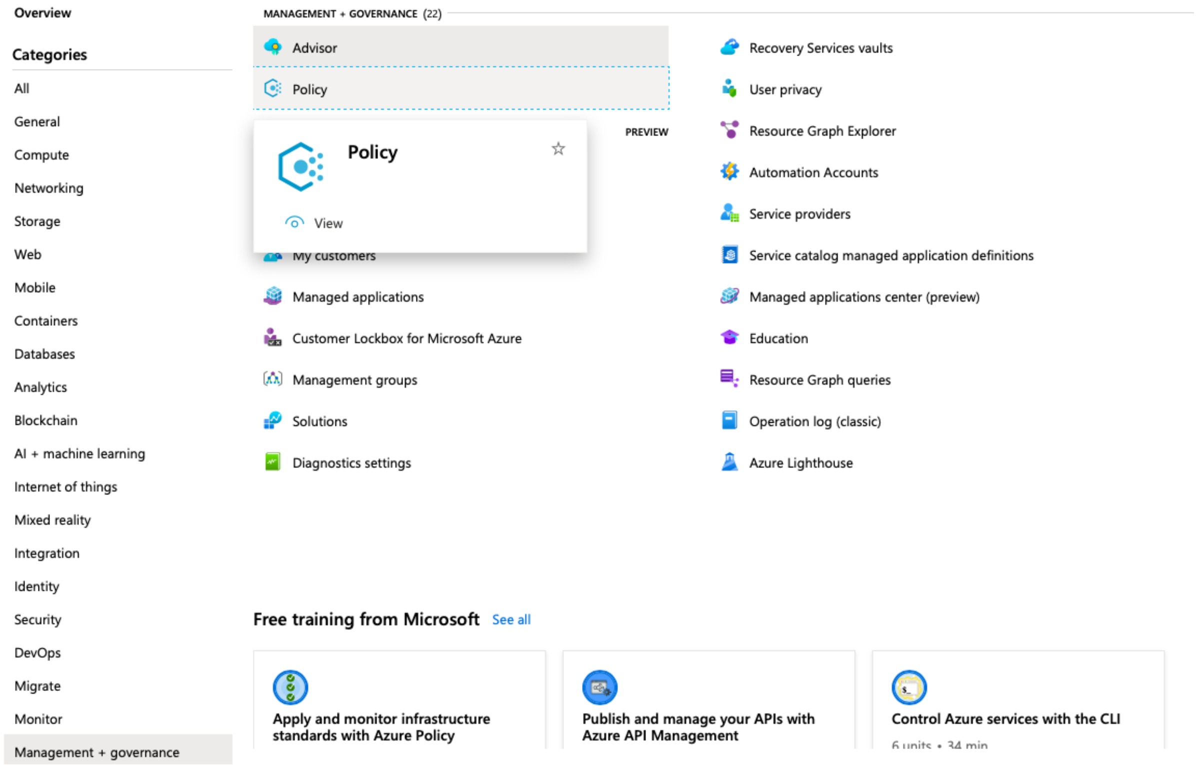
You require need an Azure subscription to perform these steps. If you don't have one you can create one by following the steps outlined on the Create your Azure free account today webpage.

Steps:

Create a Policy assignment:

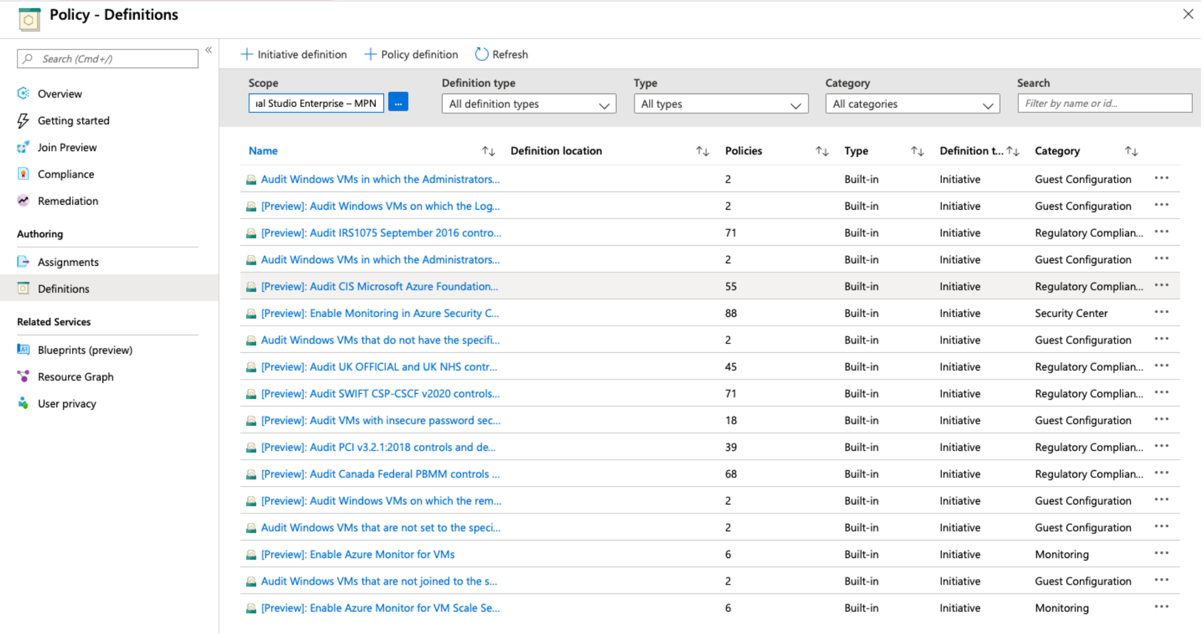
1. Launch the Azure Policy service in the Azure portal by clicking **All services** then, **Everything**, then type **Policy** in the search box and select **Policy**





Note: Azure Policy is also accessible under the **All services > Management + governance** section in the portal.

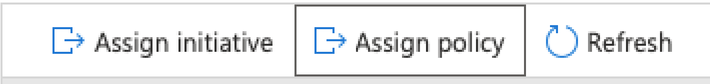
2. Go to **Authoring > Definitions** and take a moment to have a quick browse through the list of built-in policy definitions that are available for you to use.



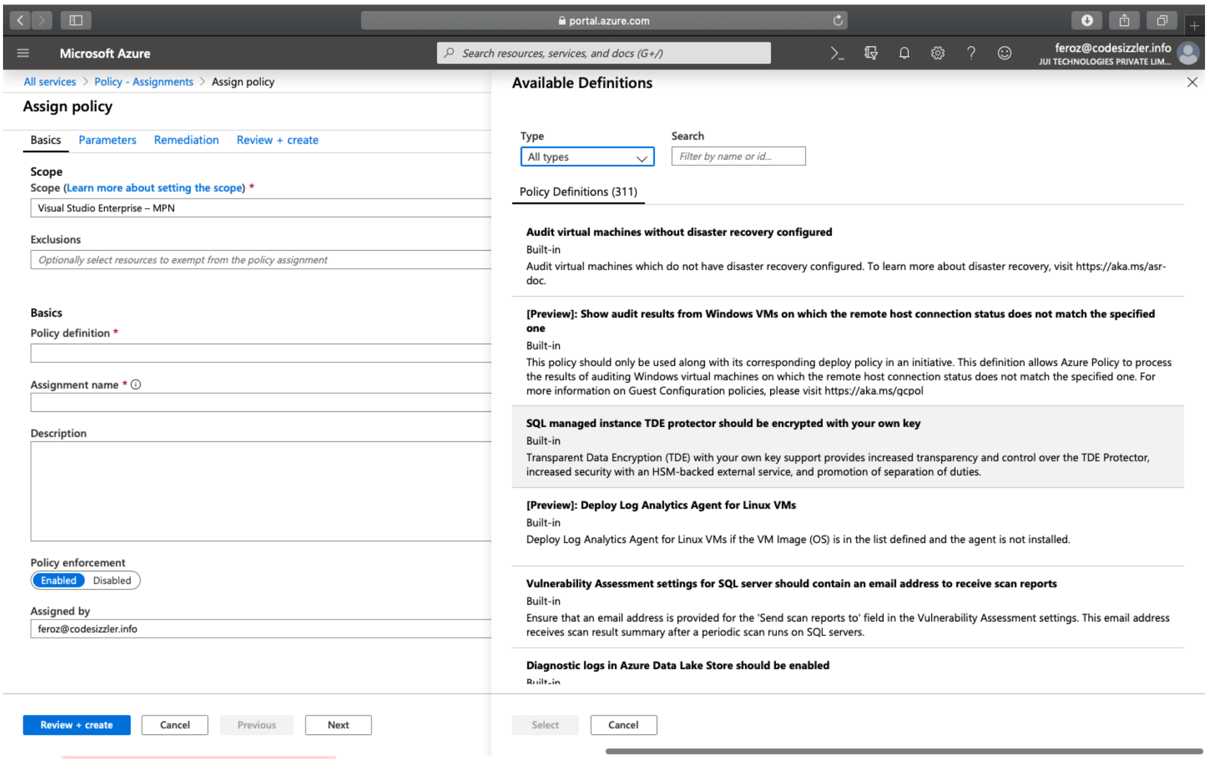
Scope: ıal Studio Enterprise – MPN
Definition type: All definition types
Type: All types
Category: All categories
Search: Filter by name or id...

Name	Definition location	Policies	Type	Definition t...	Category
Audit Windows VMs in which the Administrators...		2	Built-in	Initiative	Guest Configuration
[Preview]: Audit Windows VMs on which the Log...		2	Built-in	Initiative	Guest Configuration
[Preview]: Audit IRS1075 September 2016 contro...		71	Built-in	Initiative	Regulatory Complian...
Audit Windows VMs in which the Administrators...		2	Built-in	Initiative	Guest Configuration
[Preview]: Audit CIS Microsoft Azure Foundation...		55	Built-in	Initiative	Regulatory Complian...
[Preview]: Enable Monitoring in Azure Security C...		88	Built-in	Initiative	Security Center
Audit Windows VMs that do not have the specifi...		2	Built-in	Initiative	Guest Configuration
[Preview]: Audit UK OFFICIAL and UK NHS contr...		45	Built-in	Initiative	Regulatory Complian...
[Preview]: Audit SWIFT CSP-CSCF v2020 controls...		71	Built-in	Initiative	Regulatory Complian...
[Preview]: Audit VMs with insecure password sec...		18	Built-in	Initiative	Guest Configuration
[Preview]: Audit PCI v3.2.1:2018 controls and de...		39	Built-in	Initiative	Regulatory Complian...
[Preview]: Audit Canada Federal PBMM controls ...		68	Built-in	Initiative	Regulatory Complian...
[Preview]: Audit Windows VMs on which the rem...		2	Built-in	Initiative	Guest Configuration
Audit Windows VMs that are not set to the speci...		2	Built-in	Initiative	Guest Configuration
[Preview]: Enable Azure Monitor for VMs		6	Built-in	Initiative	Monitoring
Audit Windows VMs that are not joined to the s...		2	Built-in	Initiative	Guest Configuration
[Preview]: Enable Azure Monitor for VM Scale Se...		6	Built-in	Initiative	Monitoring

3. Select **Assignments** on the left side of the **Policy** page. An assignment is a policy that has been assigned to take place within a specific scope.



4. Select **Assignments** on the left side of the **Policy** page. An assignment is a policy that has been assigned to take place within a specific scope.



Assign policy

Scope

Scope (Learn more about setting the scope) *

Visual Studio Enterprise – MPN

Exclusions

Optionally select resources to exempt from the policy assignment

Basics

Policy definition *

Assignment name *

Description

Policy enforcement

Enabled Disabled

Assigned by

feroz@codesizzler.info

Available Definitions

Type: All types

Search: Filter by name or id...

Policy Definitions (311)

Audit virtual machines without disaster recovery configured
Built-in
Audit virtual machines which do not have disaster recovery configured. To learn more about disaster recovery, visit https://aka.ms/asr-doc.

[Preview]: Show audit results from Windows VMs on which the remote host connection status does not match the specified one
Built-in
This policy should only be used along with its corresponding deploy policy in an initiative. This definition allows Azure Policy to process the results of auditing Windows virtual machines on which the remote host connection status does not match the specified one. For more information on Guest Configuration policies, please visit https://aka.ms/gcpol

SQL managed instance TDE protector should be encrypted with your own key
Built-in
Transparent Data Encryption (TDE) with your own key support provides increased transparency and control over the TDE Protector, increased security with an HSM-backed external service, and promotion of separation of duties.

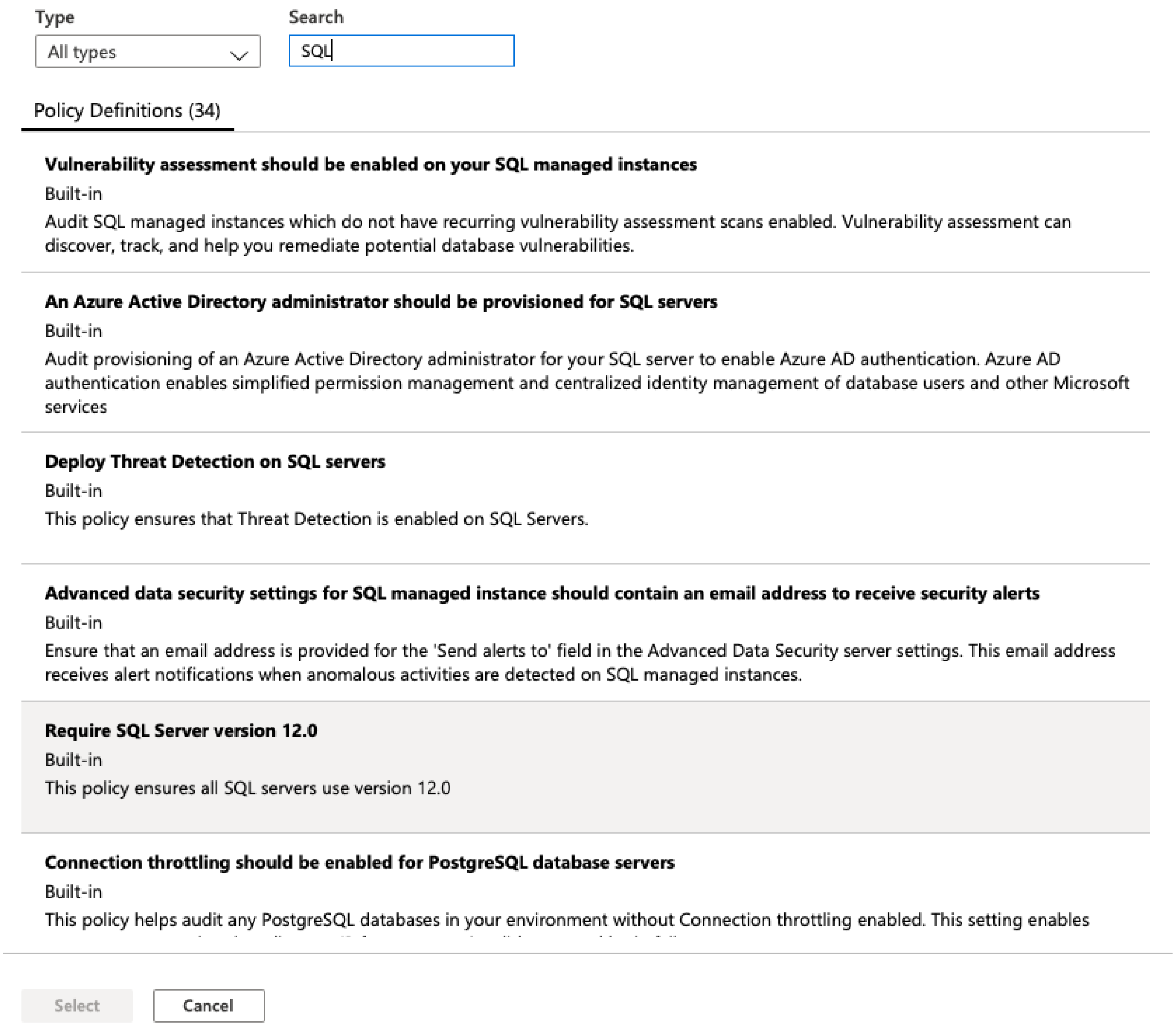
[Preview]: Deploy Log Analytics Agent for Linux VMs
Built-in
Deploy Log Analytics Agent for Linux VMs if the VM Image (OS) is in the list defined and the agent is not installed.

Vulnerability Assessment settings for SQL server should contain an email address to receive scan reports
Built-in
Ensure that an email address is provided for the 'Send scan reports to' field in the Vulnerability Assessment settings. This email address receives scan result summary after a periodic scan runs on SQL servers.

Diagnostic logs in Azure Data Lake Store should be enabled
Built-in

5. Select **Assign Policy** from the top of the **Policy - Assignments** page and on the subsequent **Assign Policy** page, select the Scope selector by clicking the ellipsis and setting the following values, then click **Select** at the bottom of the **Scope** page.
   - **Subscription**: < choose your own subscription >
   - **Resource Group**: < accept the default value i.e. leave blank >

Note: A scope determines what resources or grouping of resources the policy assignment gets enforced on. In our case we could assign this policy to a specific resource group, however we will assign the policy at subscription level. Also, be aware that resources can be excluded based on the Scope. Exclusions are optional.



Vulnerability assessment should be enabled on your SQL managed instances
Built-in
Audit SQL managed instances which do not have recurring vulnerability assessment scans enabled. Vulnerability assessment can discover, track, and help you remediate potential database vulnerabilities.

An Azure Active Directory administrator should be provisioned for SQL servers
Built-in
Audit provisioning of an Azure Active Directory administrator for your SQL server to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services

Deploy Threat Detection on SQL servers
Built-in
This policy ensures that Threat Detection is enabled on SQL Servers.

Advanced data security settings for SQL managed instance should contain an email address to receive security alerts
Built-in
Ensure that an email address is provided for the 'Send alerts to' field in the Advanced Data Security server settings. This email address receives alert notifications when anomalous activities are detected on SQL managed instances.

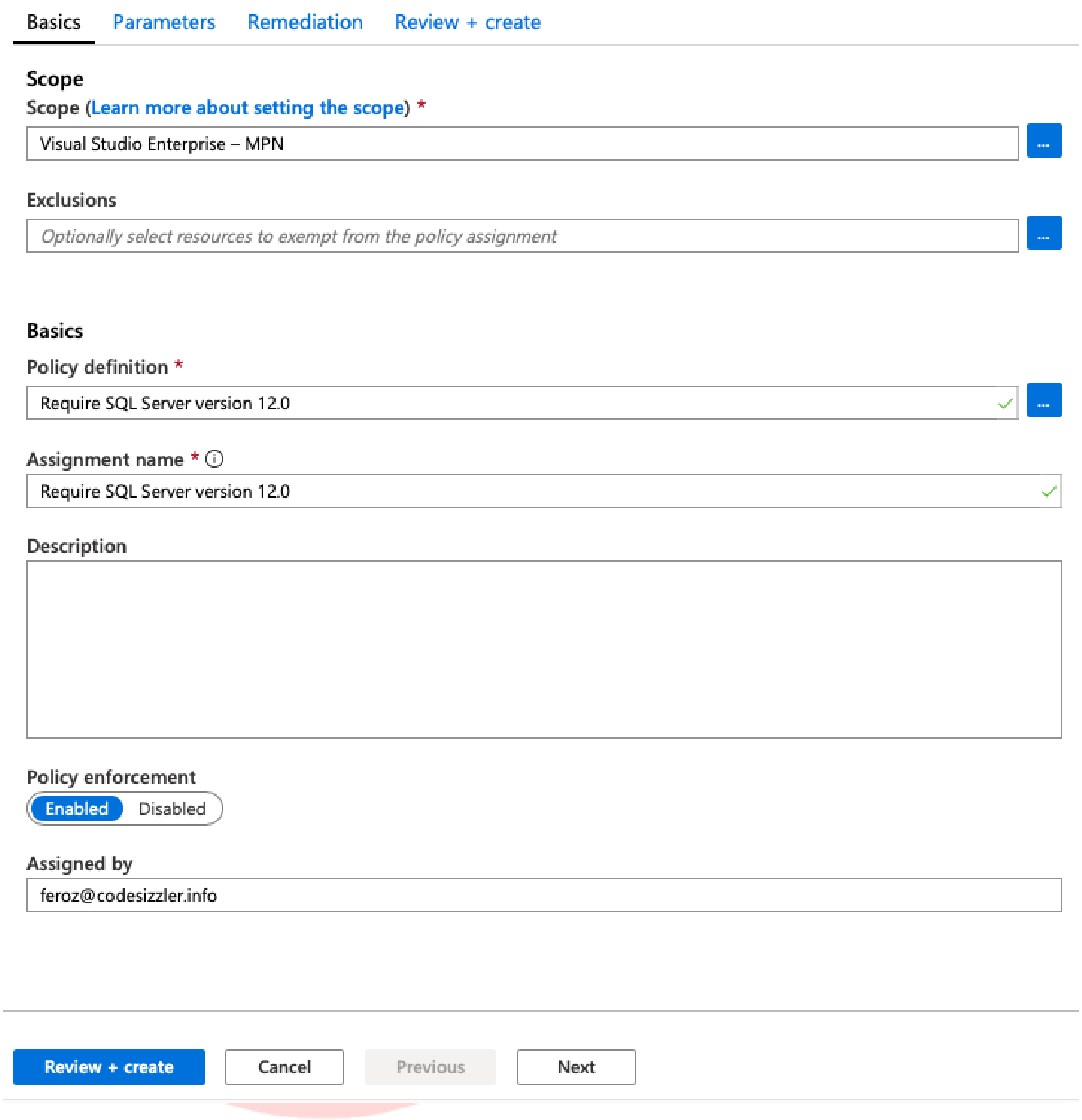
Require SQL Server version 12.0
Built-in
This policy ensures all SQL servers use version 12.0

Connection throttling should be enabled for PostgreSQL database servers
Built-in
This policy helps audit any PostgreSQL databases in your environment without Connection throttling enabled. This setting enables

6. Select the **Policy definition** ellipsis button to open the list of available definitions. Azure Policy comes with built-in policy definitions you can use, this is the same list that we saw earlier in the **Definitions** pane. Many are available, such as the below, but again you can take a quick moment to scroll through and search for ones that may interest you:
   - Require tag and its value
   - Append tag and its value
   - Require SQL Server version 12.0

In the **Available Definitions** pane in the **Search** box type **location** and click on the **Allowed locations** definition, then click **Select**.

Note: This **Allowed Locations** policy definition will specify a location into which all resources must be deployed. If a different location is chosen deployment will not be allowed. For a partial list of available built-in policies, you can also see them at the https://docs.microsoft.com/en-us/azure/governance/policy/samples/index page.



Scope

Scope (Learn more about setting the scope) *

Visual Studio Enterprise – MPN

Exclusions

Optionally select resources to exempt from the policy assignment

Basics

Policy definition *

Require SQL Server version 12.0

Assignment name *

Require SQL Server version 12.0

Description

Policy enforcement

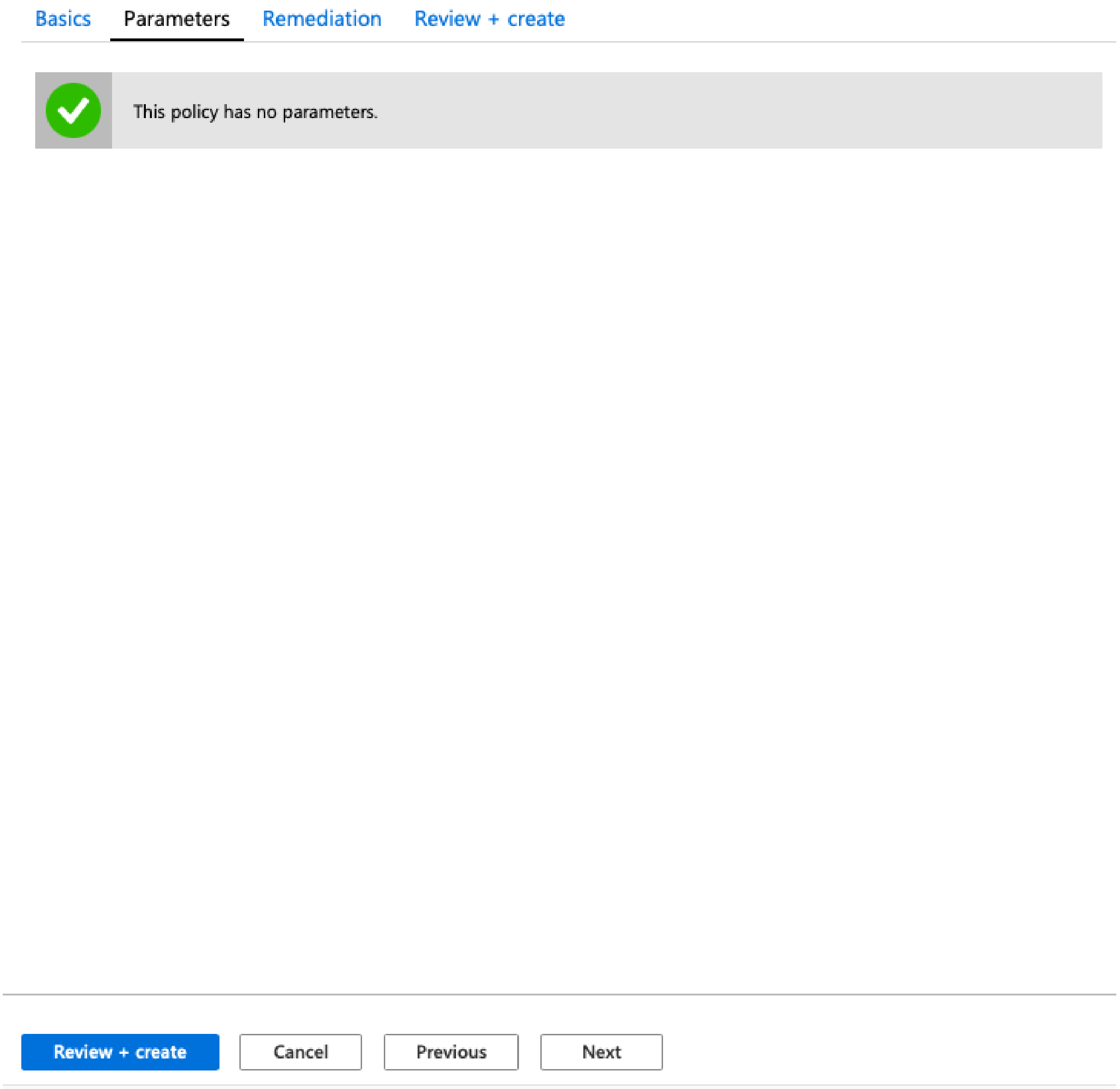
[✓ Enabled] Disabled

Assigned by

feroz@codesizzler.info

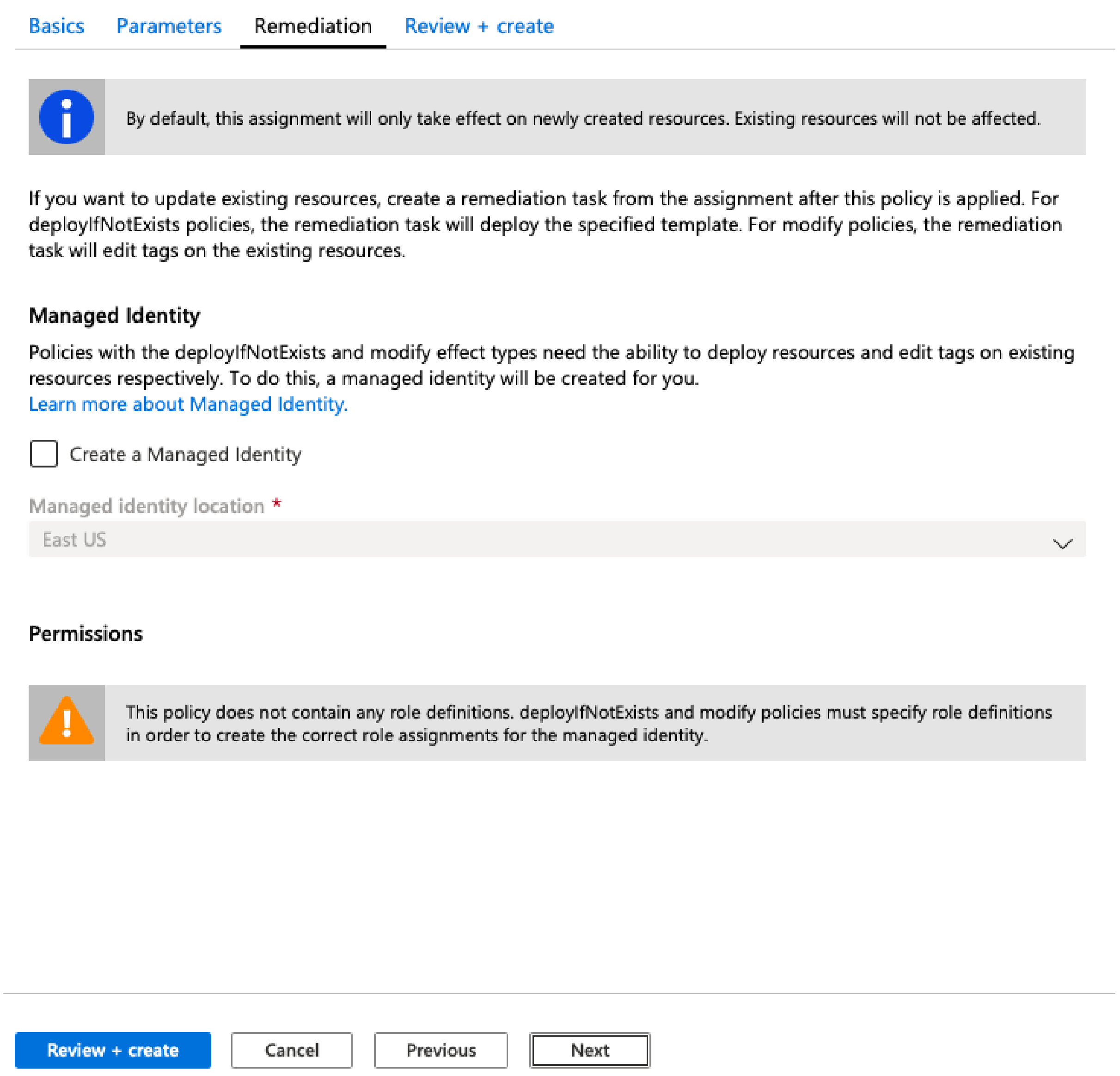
7. In the **Assign policy** pane, in the **PARAMETERS** section, click on the arrow at the end of the **Allowed locations** box and from the subsequent list choose **Japan West**. Leave all other values as they are and Click **Assign**.

Note: The **Assignment name** is automatically populated with the policy name you selected, but you can change it if you wish. You can also add an optional **Description** and **Assigned by** will automatically fill based on whoever is logged in. This field is optional, so custom values can be entered. Leave the **Create a Managed Identity** option unchecked. However, this box **must** be checked when the policy or initiative includes a policy with the **deployIfNotExists** effect.



This policy has no parameters.

8. The **Allowed locations** policy assignment is now listed on the **Policy - Assignments** pane and it is now in place and available to enforce at the scope level we specified i.e. at subscription level.



By default, this assignment will only take effect on newly created resources. Existing resources will not be affected.

If you want to update existing resources, create a remediation task from the assignment after this policy is applied. For deployIfNotExists policies, the remediation task will deploy the specified template. For modify policies, the remediation task will edit tags on the existing resources.

Managed Identity

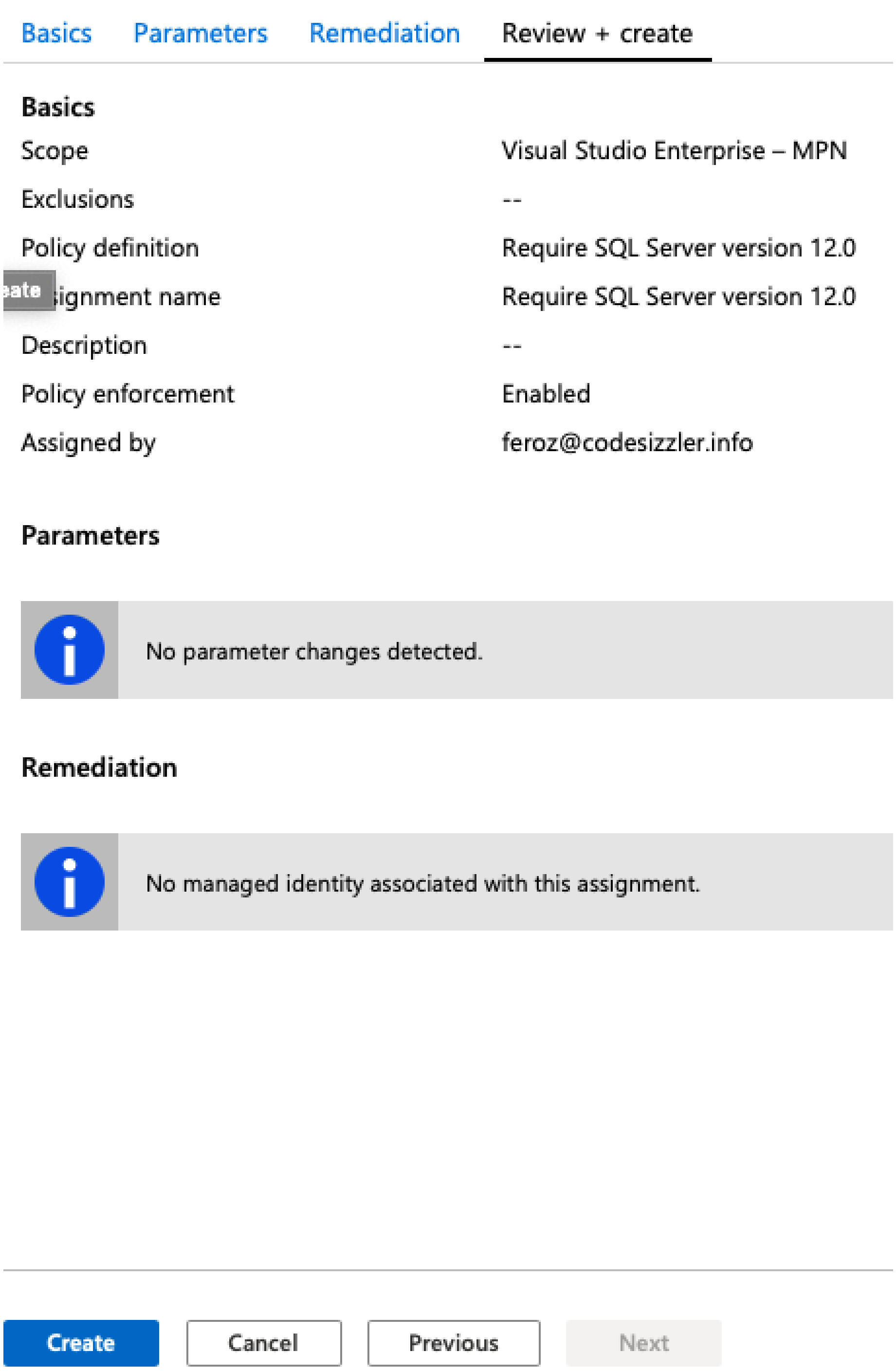
Policies with the deployIfNotExists and modify effect types need the ability to deploy resources and edit tags on existing resources respectively. To do this, a managed identity will be created for you.
Learn more about Managed Identity.

□ Create a Managed Identity

Managed identity location *
East US

Permissions

This policy does not contain any role definitions. deployIfNotExists and modify policies must specify role definitions in order to create the correct role assignments for the managed identity.



Basics

Scope	Visual Studio Enterprise – MPN
Exclusions	--
Policy definition	Require SQL Server version 12.0
ignment name	Require SQL Server version 12.0
Description	--
Policy enforcement	Enabled
Assigned by	feroz@codesizzler.info

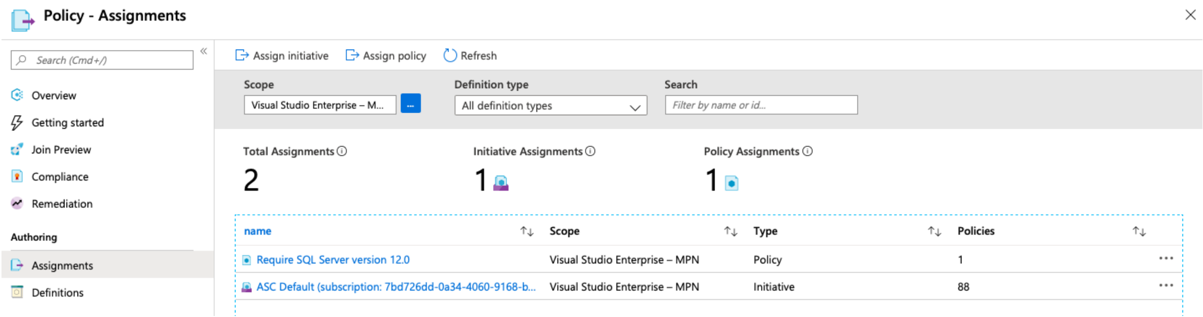
Parameters

No parameter changes detected.

Remediation

No managed identity associated with this assignment.

\



Scope: Visual Studio Enterprise – M...

Definition type: All definition types

Search: Filter by name or id...

Total Assignments: 2

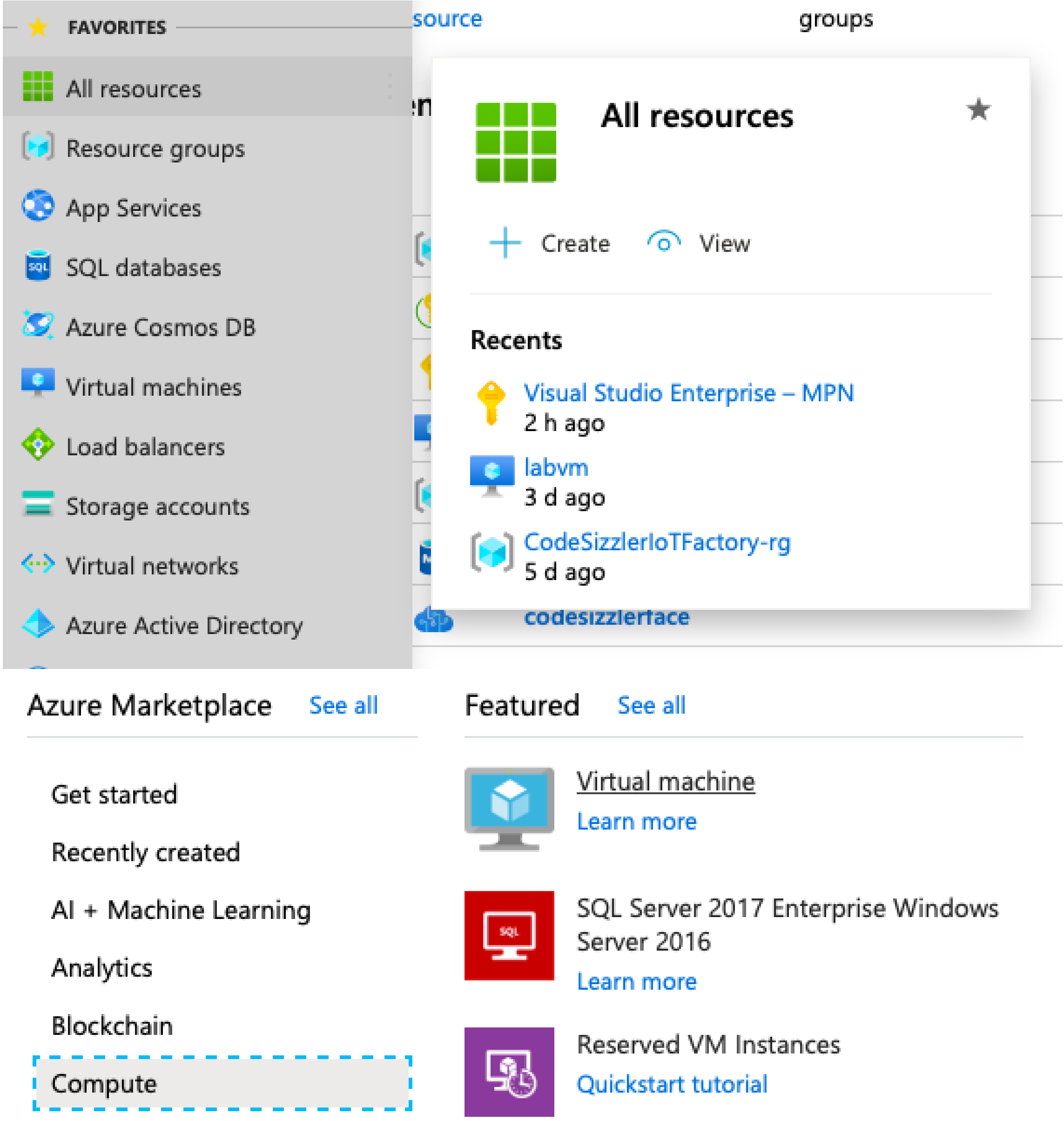
Initiative Assignments: 1

Policy Assignments: 1

name	Scope	Type	Policies
Require SQL Server version 12.0	Visual Studio Enterprise – MPN	Policy	1
ASC Default (subscription: 7bd726dd-0a34-4060-9168-b...	Visual Studio Enterprise – MPN	Initiative	88

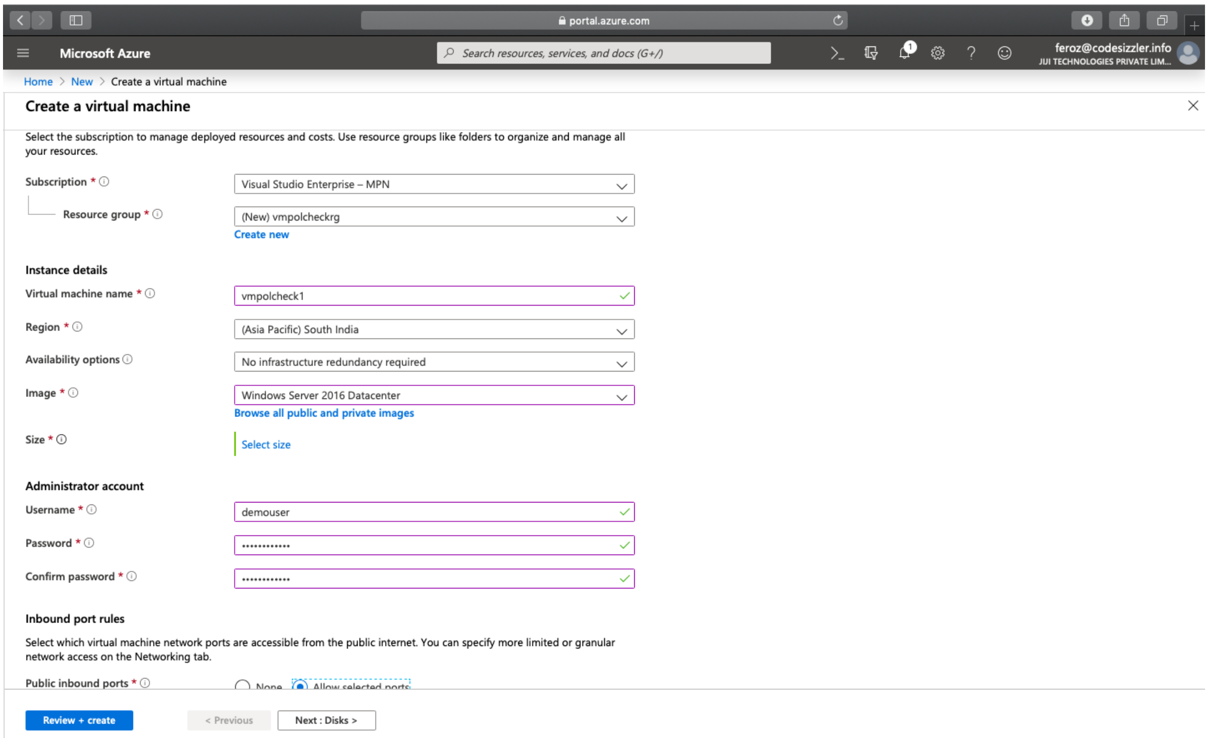
Test Allowed location policy

1. In the Azure Portal, in the **FAVORITES** list on the left hand side, then click **Create virtual machine**



2. In the **Create a virtual machine** pane on the **Basics** tab fill in the fields with the following values, leaving all other values as default, and Click **Review + create**
   - **Subscription**: < select your own subscription. Ensure it is the same subscription you assigned the allowed locations policy to earlier >
   - **Resource group**: < click **Create new** and enter a value i.e. **vmpolcheckrg**
   - **Virtual machine name**: vmpolcheck1
   - **Region**: < select any Datacenter location other than the one that you used as a parameter value earlier in the policy assignment i.e. we assigned **Japan West** earlier as the allowed Datacenter location, so use **(Europe) North Europe** now >
   - **Authentication type**: Password
   - **Username**: azureuser

- **Password**: Password0134!



Home > New > Create a virtual machine

Create a virtual machine

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *: Visual Studio Enterprise – MPN

Resource group *: (New) vmpolcheckrg

Create new

Instance details

Virtual machine name *: vmpolcheck1

Region *: (Asia Pacific) South India

Availability options: No infrastructure redundancy required

Image *: Windows Server 2016 Datacenter

Browse all public and private images

Size *: Select size

Administrator account

Username *: demouser

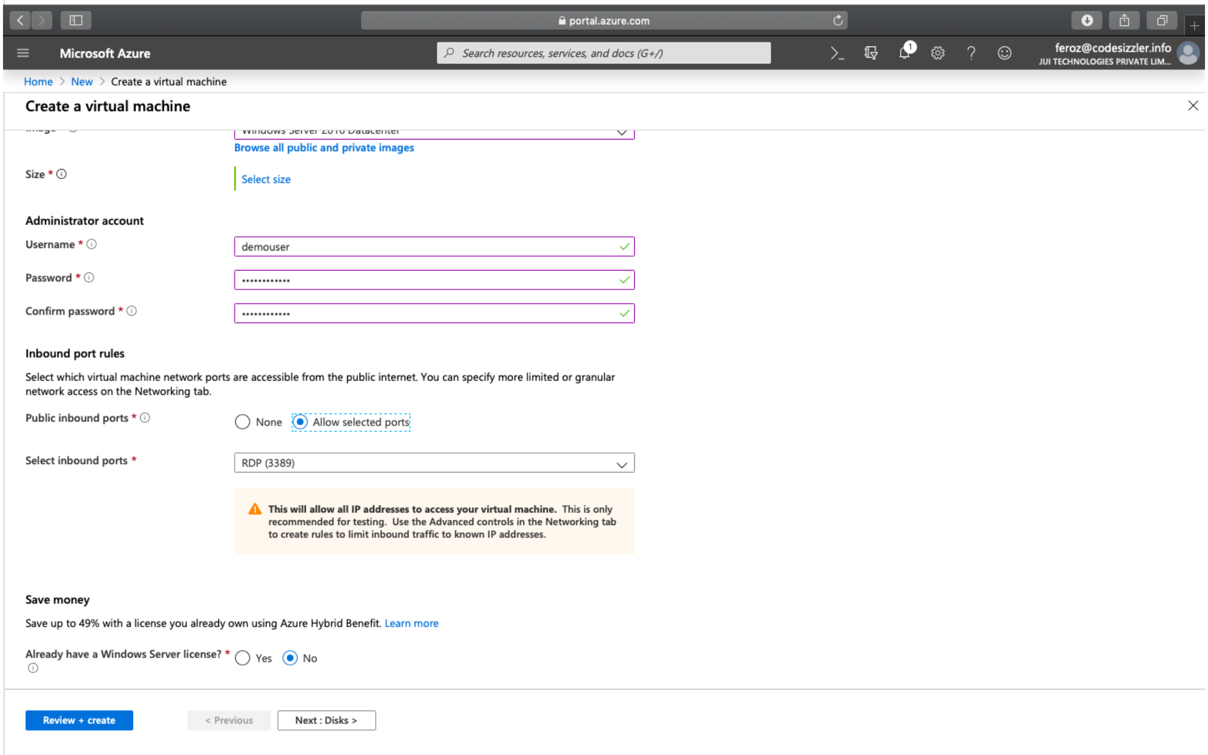
Password *: ••••••••••••

Confirm password *: ••••••••••••

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports *: ○ None ● Allow selected ports



Home > New > Create a virtual machine

Create a virtual machine

Browse all public and private images

Size *: Select size

Administrator account

Username *: demouser

Password *: ••••••••••••

Confirm password *: ••••••••••••

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports *: ○ None ● Allow selected ports

Select inbound ports *: RDP (3389)

⚠ **This will allow all IP addresses to access your virtual machine.** This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

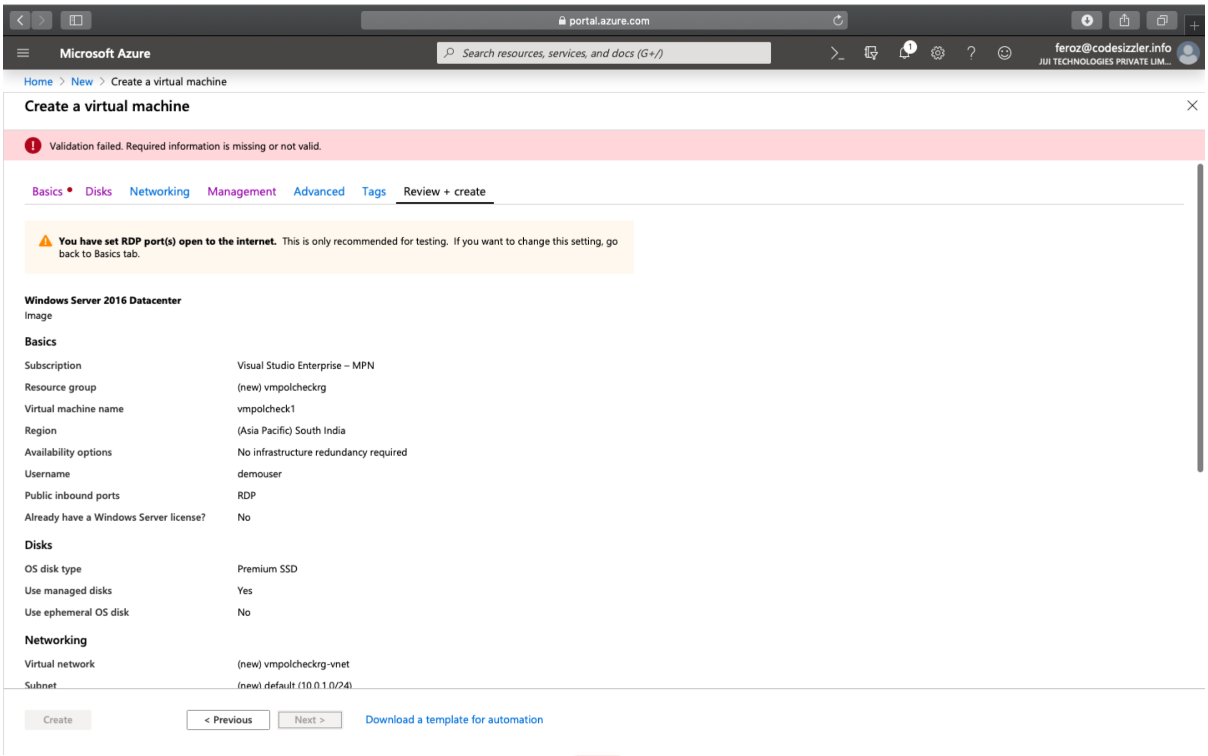
Save money

Save up to 49% with a license you already own using Azure Hybrid Benefit. Learn more

Already have a Windows Server license? *: ○ Yes ● No

3. You will receive a Validation failed message, and click on the **Click here to view details** message the resultant **Errors** blade, on the **Summary** tab note the error message, **Resource xyz was disallowed by Policy** and the policy name listed as **Allowed locations**

Note: You can dig in further for specifics, by clicking on the **Raw Error** tab and viewing the output and also by clicking on the Allowed locations policy, to view the policy that blocked the deployment.



portal.azure.com
Microsoft Azure
Search resources, services, and docs (G+/)
feroz@codesizzler.info
JUI TECHNOLOGIES PRIVATE LIM...
Home > New > Create a virtual machine

Create a virtual machine

Validation failed. Required information is missing or not valid.

Basics • Disks Networking Management Advanced Tags Review + create

You have set RDP port(s) open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.

Windows Server 2016 Datacenter
Image

Basics

Subscription	Visual Studio Enterprise – MPN
Resource group	(new) vmpolcheckrg
Virtual machine name	vmpolcheck1
Region	(Asia Pacific) South India
Availability options	No infrastructure redundancy required
Username	demouser
Public inbound ports	RDP
Already have a Windows Server license?	No

Disks

OS disk type	Premium SSD
Use managed disks	Yes
Use ephemeral OS disk	No

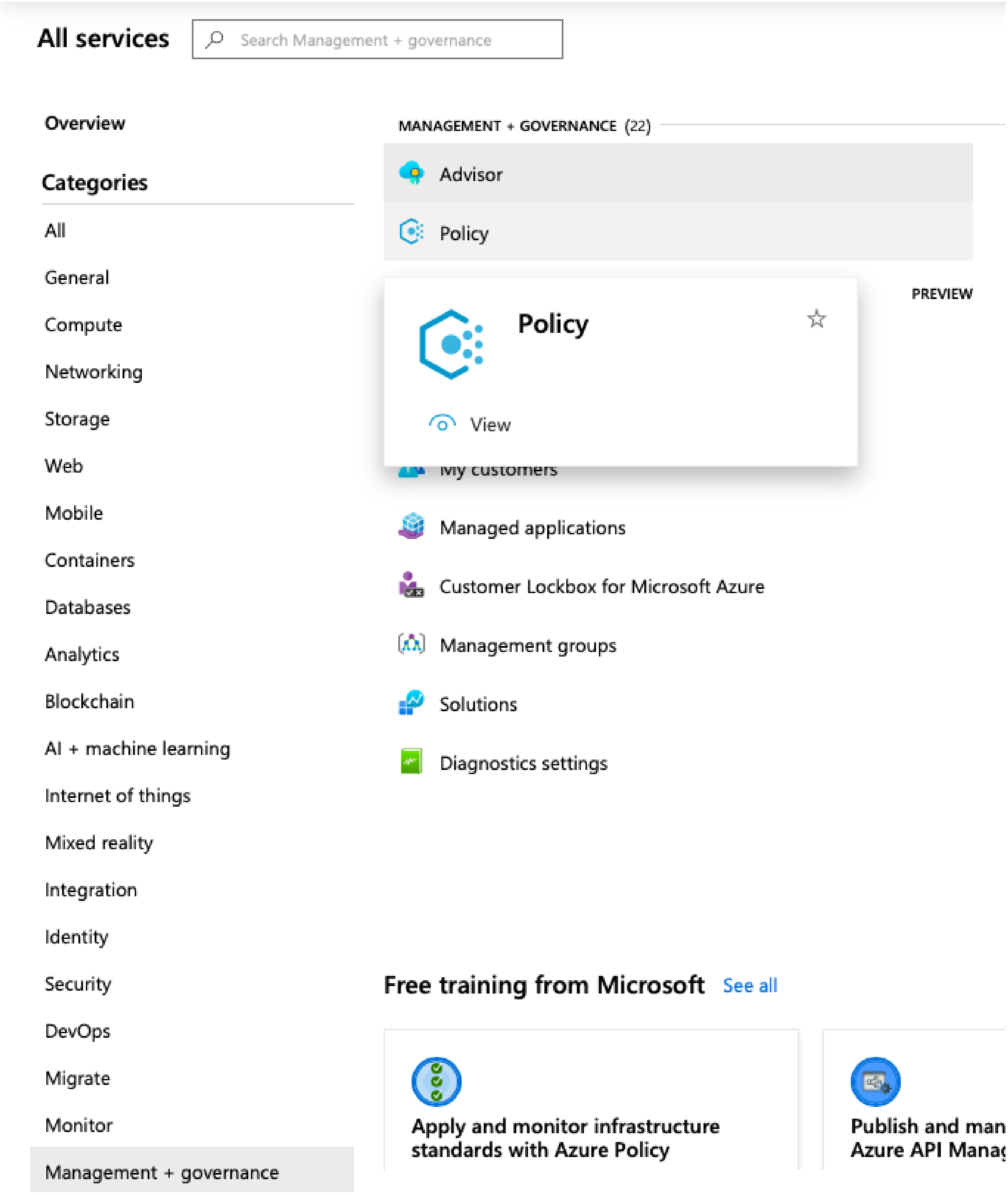
Networking

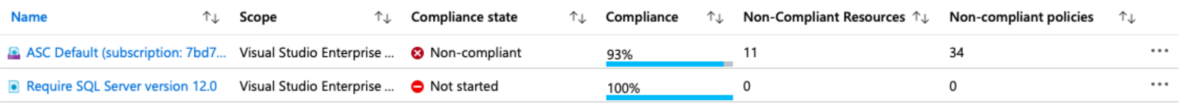
Virtual network	(new) vmpolcheckrg-vnet
Subnet	(new) default (10.0.1.0/24)

Delete the policy assignment

1. In the Azure Portal click **All Services** > **Management + governance** then **Policy** and on the **Policy** pane select **Compliance** in the left side of the page. Within this pane you can view the compliance state of the various policies you have assigned.

Note: The Allowed location policy is listed as non-compliant in the screenshot, as there are pre-existing resources deployed outside of **Japan West**, which were created prior to the policy assignment, when using Azure Cloud Shell and other Azure resources.

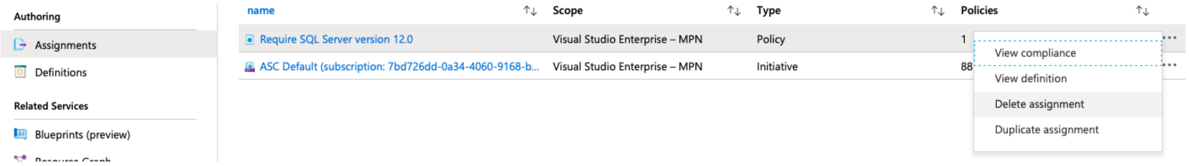




Name ↑↓	Scope ↑↓	Compliance state ↑↓	Compliance ↑↓	Non-Compliant Resources ↑↓	Non-compliant policies ↑↓	
ASC Default (subscription: 7bd7...	Visual Studio Enterprise ...	☒ Non-compliant	93%	11	34	···
Require SQL Server version 12.0	Visual Studio Enterprise ...	⊖ Not started	100%	0	0	···

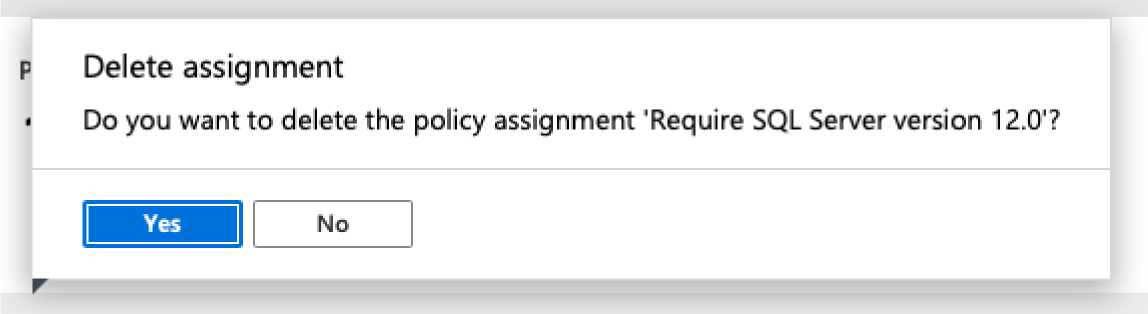
2. Go to **Assignments** and click on the ellipsis at the end of the **Allowed locations** policy assignment. Then select **Delete Assignment** from the

resultant menu.



name	Scope	Type	Policies
Require SQL Server version 12.0	Visual Studio Enterprise – MPN	Policy	1
ASC Default (subscription: 7bd726dd-0a34-4060-9168-b...	Visual Studio Enterprise – MPN	Initiative	88

3. Confirm you wish to delete the policy assignment in the **Delete assignment** dialogue by clicking **Yes**



Delete assignment

Do you want to delete the policy assignment 'Require SQL Server version 12.0'?

odeSizzler