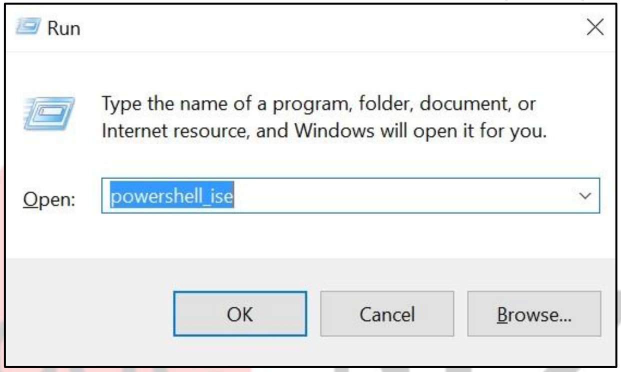
Controlling Access with ARM Policies

Lab Overview

In this lab, you will deploy an Azure Resource Manager Policy that restricts access to a resource provider and apply it to a new custom resource group.

Exercise 1: Configure the Azure PowerShell cmdlets for your Subscription

1. Launch the PowerShell Integrated System Environment (ISE) by typing in PowerShell_ISE in the Windows run prompt.



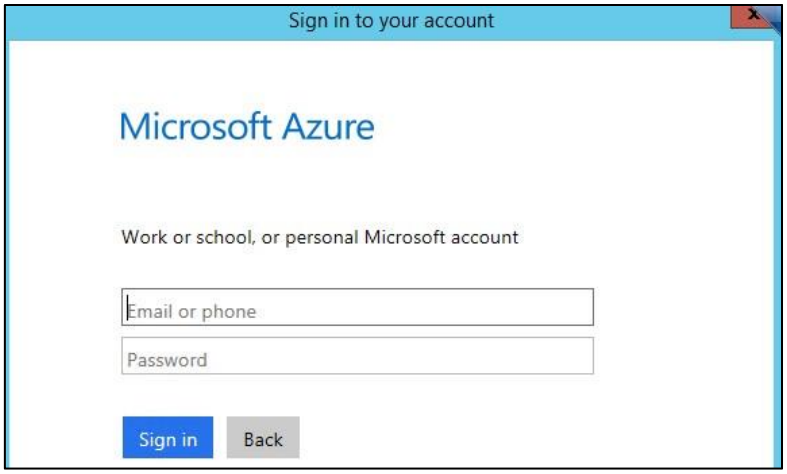
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: powershell_ise

2. In the **PowerShell ISE Console Pane** run the **Login-AzureRmAccount** cmdlet by typing the cmdlet name in and pressing **Enter**. This cmdlet will launch a dialog that will allow you to login with your Azure subscription credentials. The session is valid for 12 hours as long as you do not close and re-open the PowerShell ISE.

```
Login-AzureRmAccount
```

3. Enter the credentials for your Azure subscription when prompted.



Sign in to your account

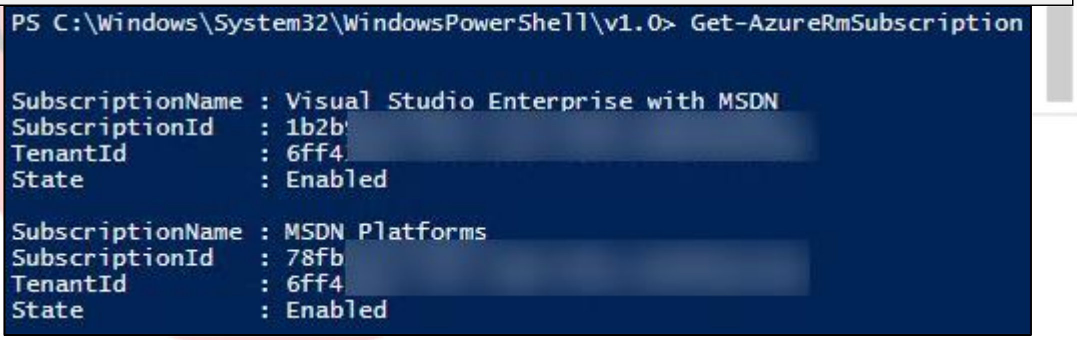
Microsoft Azure

Work or school, or personal Microsoft account

4. In the **PowerShell ISE Console Pane** run the following command to list the subscriptions that are attached to your account.

```
Get-AzureRMSubscription
```

```
The return from Azure will look like the follow. Make note of
the
SubscriptionID that matches the subscription you used earlier in
                        the lab.
```



```
PS C:\Windows\System32\WindowsPowerShell\v1.0> Get-AzureRmSubscription


SubscriptionName : Visual Studio Enterprise with MSDN
SubscriptionId   : 1b2b[redacted]
TenantId         : 6ff4[redacted]
State            : Enabled

SubscriptionName : MSDN Platforms
SubscriptionId   : 78fb[redacted]
TenantId         : 6ff4[redacted]
State            : Enabled
```

5. In the **PowerShell ISE Console Pane** run the following command to Select the subscription that will be used for the reminder of the course. Replace [subscription id] leaving the quotes.

```
Select-AzureRmSubscription -SubscriptionId
"[subscription id]"
```

Exercise 2: Create and Assign a new ARM Policy to a Resource Group

1. Open File Explorer and navigate to C:\OpsgilityTraining. Right-click the ServiceCatalogPolicy.json file and select **Open with** and then choose **Notepad**.

```
The ServiceCatalogPolicy.json file is broken into two major parts.

The first part consists of conditions and logical operators which define
the actions of the policy.

The second part defines the effect when the conditions are fulfilled.

This file shows that only actions on services of type
Microsoft.Resources/*, Microsoft.Compute/*, Microsoft.Storage/*, and
Microsoft.Network/* are allowed. Anything else will be denied. After
examining the file, close the file.
```

2. Create a new resource group by running the following command and pressing **Enter**. Replace the value of the **Location** parameter with the location nearest to you.

```
New-AzureRMResourceGroup -Name ARMPolicyRG -Location "South
Central US"
```

3. Create a new policy definition using the ServiceCatalogPolicy.json file by executing the following PowerShell command.

```
New-AzureRmPolicyDefinition -Name ServiceCatalogPolicy -
Description "Policy to allow only certain resource types" -
Policy "C:\OpsgilityTraining\ServiceCatalogPolicy.json"
```

4. Create a $ResourceGroup variable and a $Policy variable by executing the following PowerShell commands.

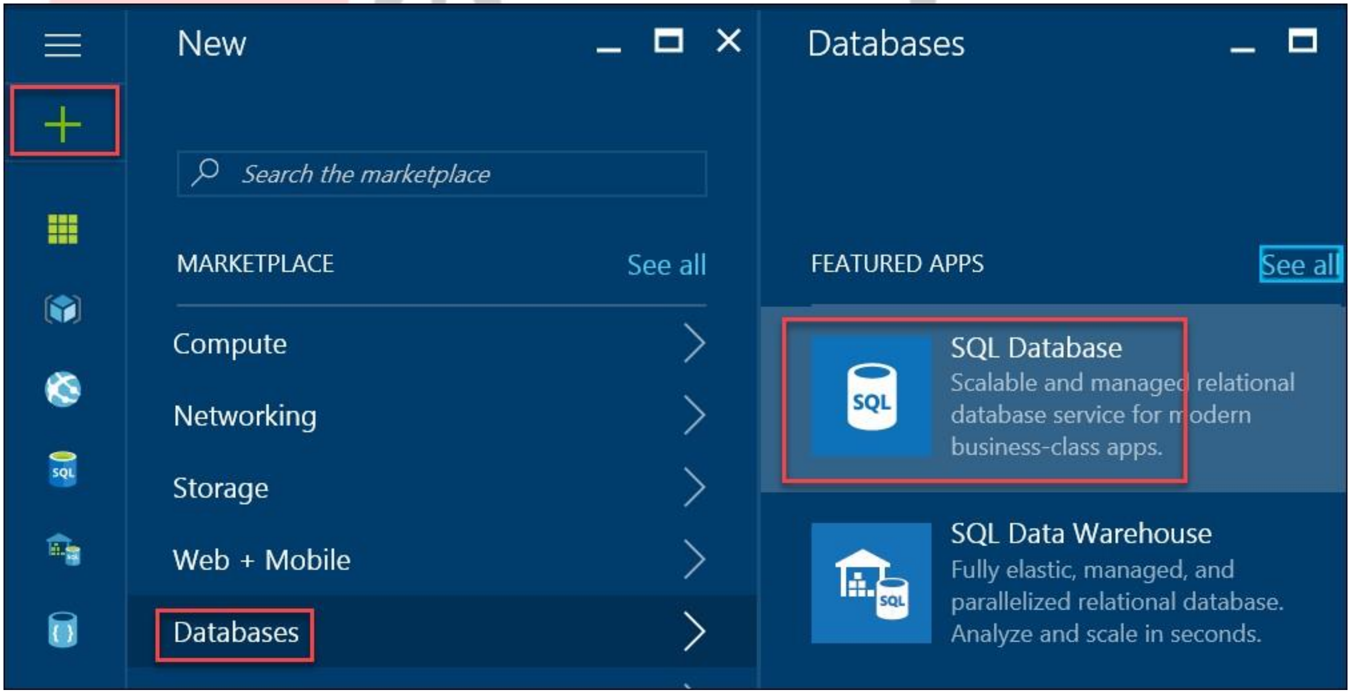
```
$ResourceGroup = Get-AzureRmResourceGroup -Name "ARMPolicyRG"
$Policy = Get-AzureRmPolicyDefinition -Name "ServiceCatalogPolicy"
```

5. Now we will assign the newly created policy to our resource group by executing the following PowerShell command.

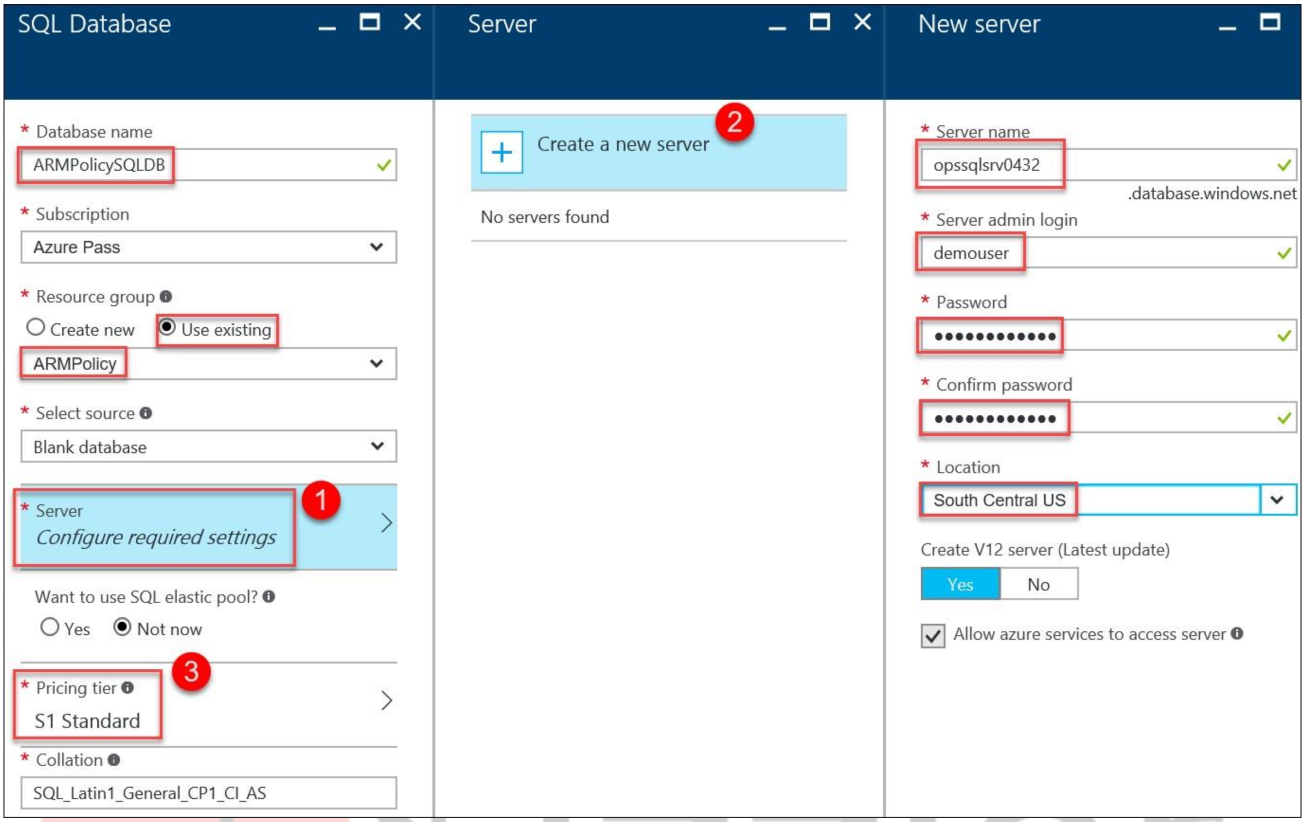
```
New-AzureRmPolicyAssignment -Name
"ServiceCatalogPolicyAssignment" -
PolicyDefinition $Policy -Scope $ResourceGroup.ResourceId
```

Exercise 3: Deploy a SQL VM to the newly created Policy Restricted Resource Group

1. In the Azure Portal, click **New**, **Databases**, **SQL Database**.


New
Search the marketplace
MARKETPLACE
See all
Compute
Networking
Storage
Web + Mobile
Databases
Databases
FEATURED APPS
See all
SQL Database
Scalable and managed relational database service for modern business-class apps.
SQL Data Warehouse
Fully elastic, managed, and parallelized relational database. Analyze and scale in seconds.

2. On the SQL Database blade, specify the settings below and click **Server**, to **Create a new server**. Click **Select** on the New server blade and **Create** on the SQL Database blade.



SQL Database

* Database name: ARMPolicySQLDB ✓

* Subscription: Azure Pass

* Resource group: ○ Create new ● Use existing

ARMPolicy

* Select source: Blank database

* Server: *Configure required settings*

Want to use SQL elastic pool? ○ Yes ● Not now

* Pricing tier: S1 Standard

* Collation: SQL_Latin1_General_CP1_CI_AS

Server

＋ Create a new server

No servers found

New server

* Server name: opssqlsrv0432 ✓ .database.windows.net

* Server admin login: demouser ✓

* Password: •••••••••••• ✓

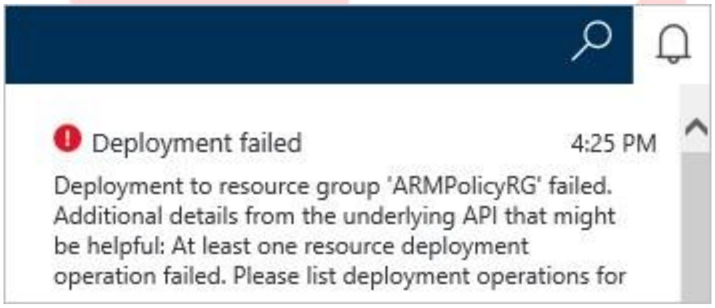
* Confirm password: •••••••••••• ✓

* Location: South Central US

Create V12 server (Latest update): Yes No

☑ Allow azure services to access server

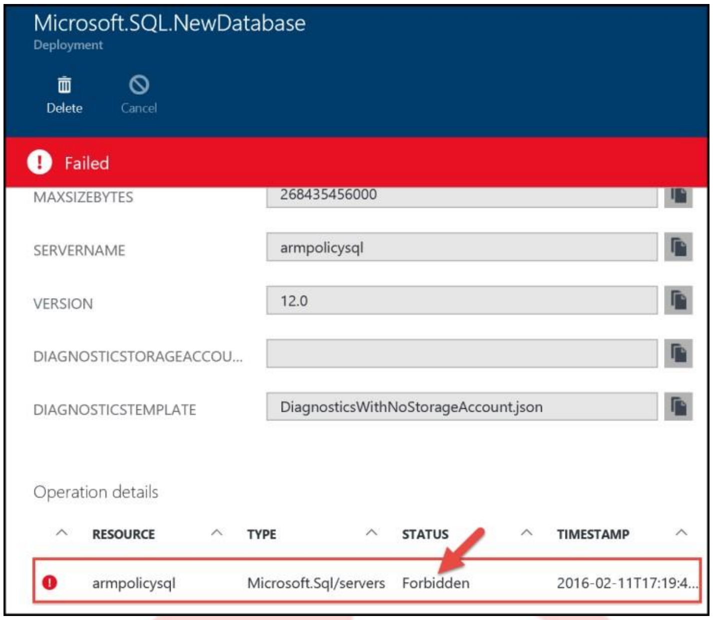
3. In the Azure Portal you will get an error alert. Click on the alert to drill into the details of the alert.



Deployment failed 4:25 PM

Deployment to resource group 'ARMPolicyRG' failed. Additional details from the underlying API that might be helpful: At least one resource deployment operation failed. Please list deployment operations for

4. On the Microsoft.SQL.NewDatabase blade you will see the status is **Failed**. Scroll to the Operation details at the bottom of the summary output. Notice that the status is Forbidden. Click on this entry to view the details of the operation.



Microsoft.SQL.NewDatabase
Deployment

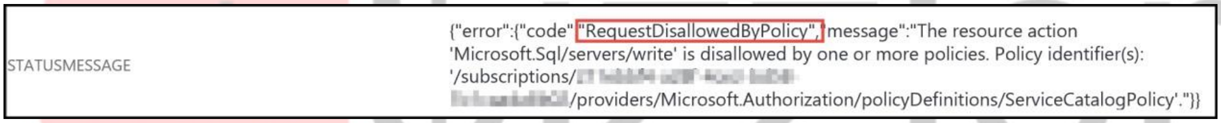
Failed

MAXSIZEBYTES	268435456000
SERVERNAME	armpolicysql
VERSION	12.0
DIAGNOSTICSTORAGEACCOU...	
DIAGNOSTICSTEMPLATE	DiagnosticsWithNoStorageAccount.json

Operation details

RESOURCE	TYPE	STATUS	TIMESTAMP
armpolicysql	Microsoft.Sql/servers	Forbidden	2016-02-11T17:19:4...

5. In the **Operation details** blade, review the Status Message. Note the underlying reason for the failure is RequestDisallowedByPolicy. The status message also has an explanation of the error and contains the policy identifier.



STATUSMESSAGE	{"error":{"code":"RequestDisallowedByPolicy","message":"The resource action 'Microsoft.Sql/servers/write' is disallowed by one or more policies. Policy identifier(s): '/subscriptions/[redacted]/providers/Microsoft.Authorization/policyDefinitions/ServiceCatalogPolicy'."}}

Lab Summary

In this lab, you deployed an Azure Resource Manager Policy that restricted access to a resource provider and applied it to a new custom resource group.