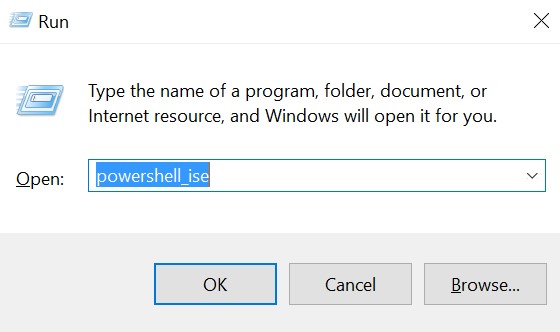
## Controlling Access with ARM Policies

### 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

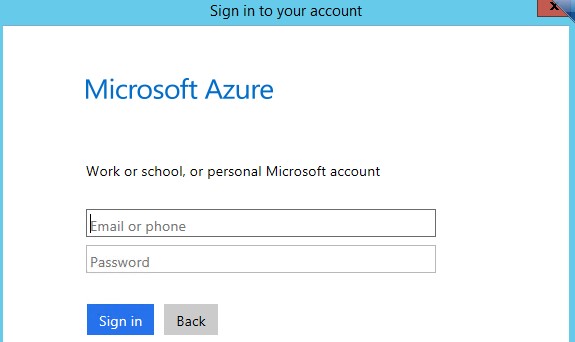
1. Launch the PowerShell Integrated System Environment (ISE) by typing in PowerShell\_ISE in the Windows run prompt.



1. 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

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

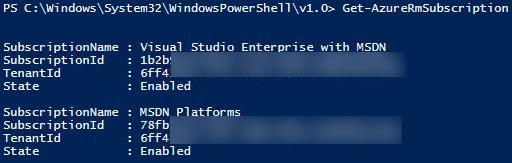


1. In the **PowerShell ISE Console Pane** run the following command to list the subscriptions that are attached to your account.

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.



1. 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. |

1. 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"

1. 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"

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

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

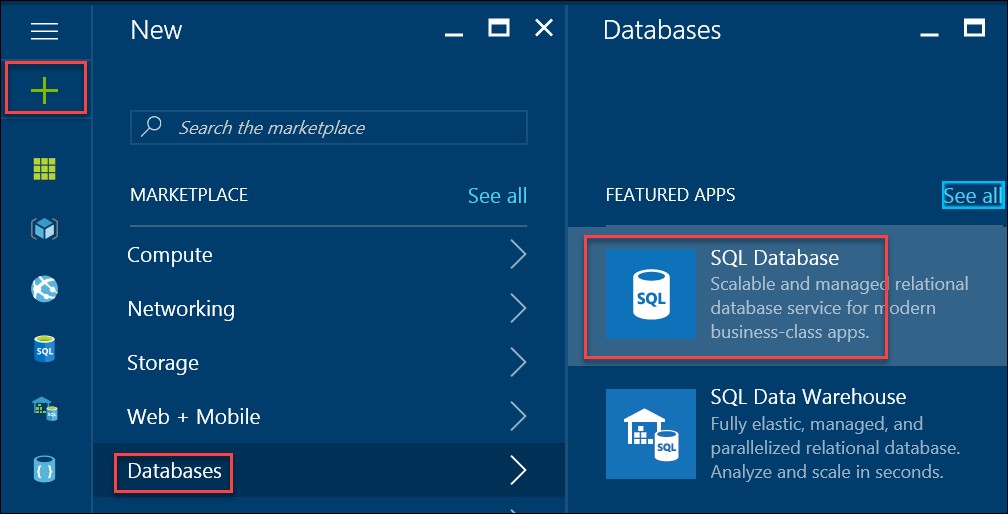
1. Now we will assign the newly created policy to our resource group by executing the following PowerShell command.

New-AzureRmPolicyAssignment -Name "ServiceCatalogPolicyAssignment" -

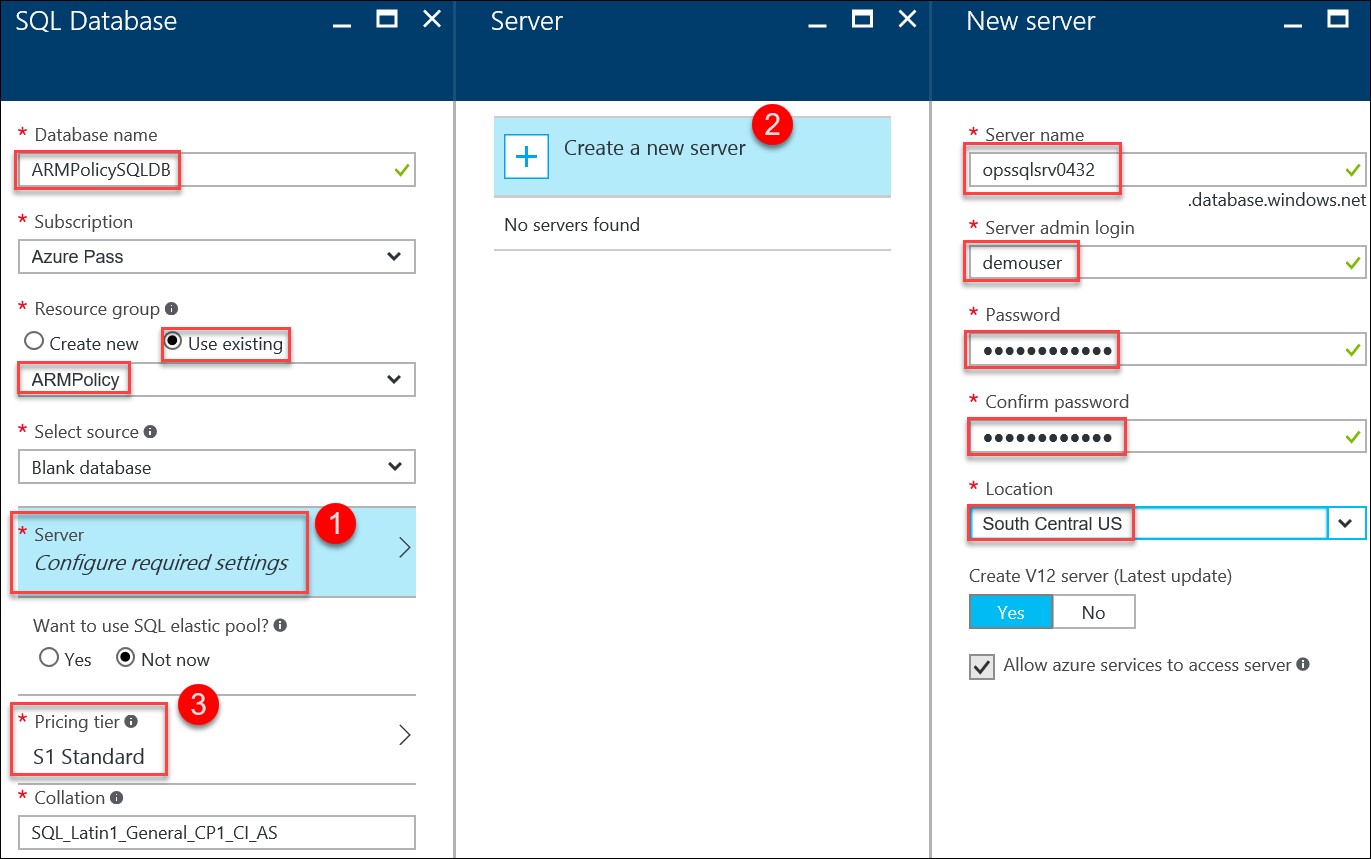
PolicyDefinition $Policy -Scope $ResourceGroup.ResourceId

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

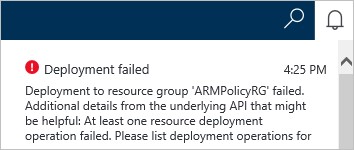
1. In the Azure Portal, click **New**, **Databases**, **SQL Database**.



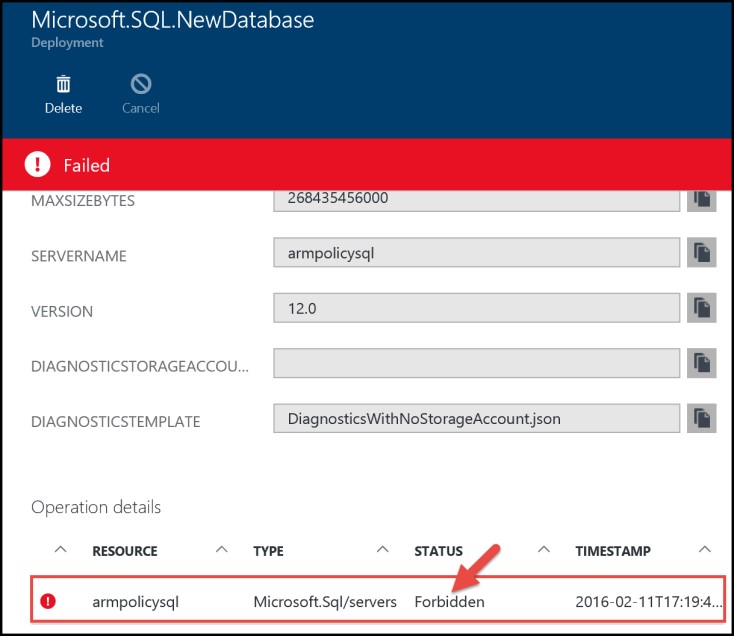
1. On the SQL Database blade, specify the settings below and click **Server**, to **Create a new server**. Click **Select** on the New server blade and **Create** on the SQL Database blade.



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



1. 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.



1. 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.



### 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.