Contents

[Multiple Site-2-Site VPN Tunnel Walkthrough 1](#_Toc21701100)

[Scenario 1](#_Toc21701101)

[The Process 1](#_Toc21701102)

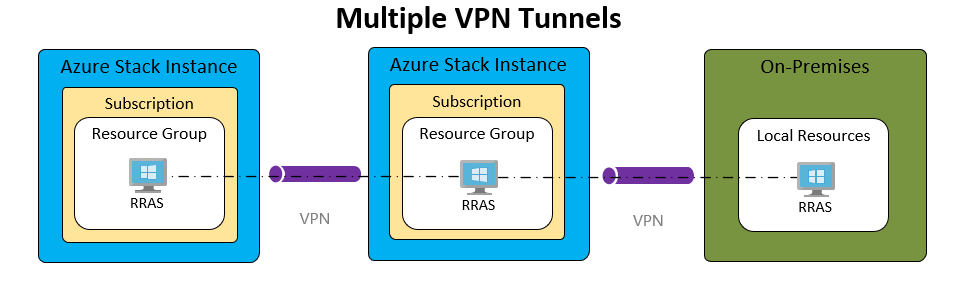
[Walkthrough 1](#_Toc21701103)

[Deploy ‘WebTier’ to Azure Stack Instances PPE1 1](#_Toc21701104)

# Multiple Site-2-Site VPN Tunnel Walkthrough

This guide will walk through using the template to create multiple resource groups with associated Virtual Networks and how to connect these systems

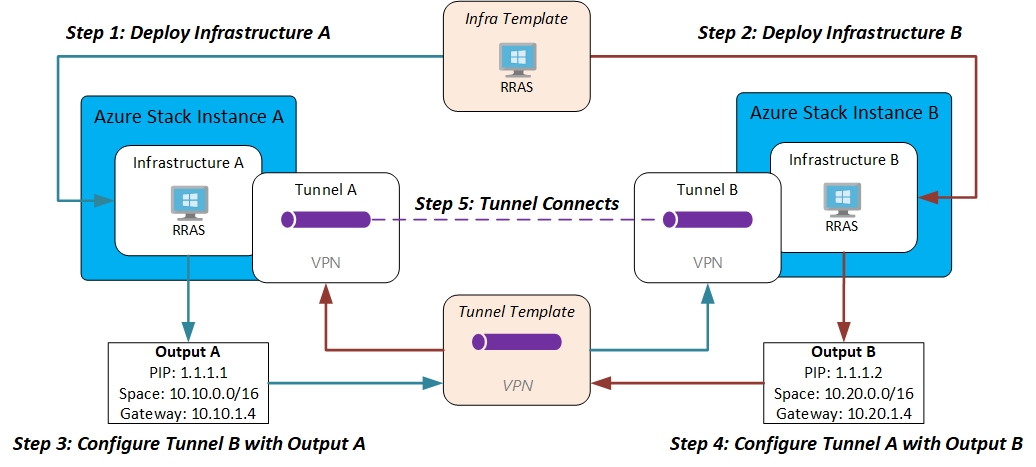
## Scenario



* We will deploy a 3 tier application, Web, App and DB.
* Will will be deploy the first two template on separate Azure Stack instances
* ‘WebTier’ will be deployed on PPE1 and ‘AppTier’ will be deployed on PPE2
* We will connected the WebTier and AppTier with an IKE tunnel
* We will then connect the AppTier to an onpremise system that we will call the DBTier

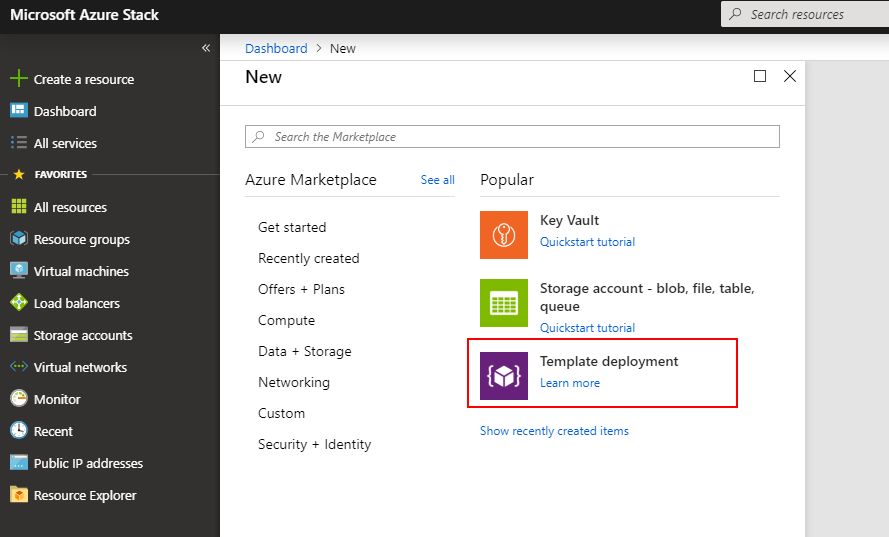
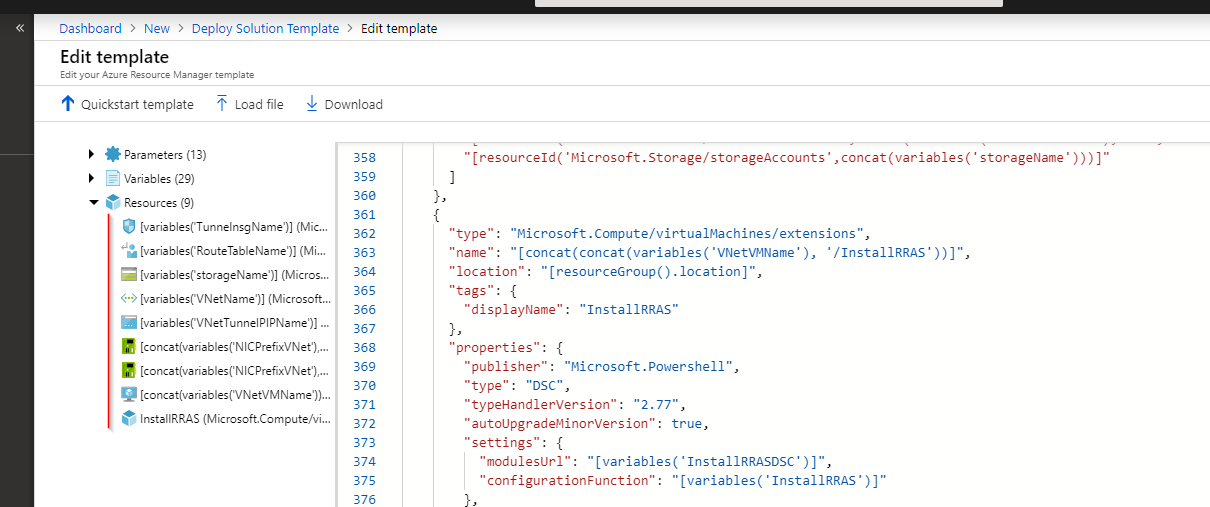
## The Process

This is a multi-step process illustrated below. For this scenario we are going to be using the Azure Stack Portal UI. However, you can use PowerShell or Azure CLI or other CI/CD tool chains capture the outputs and use then as inputs.

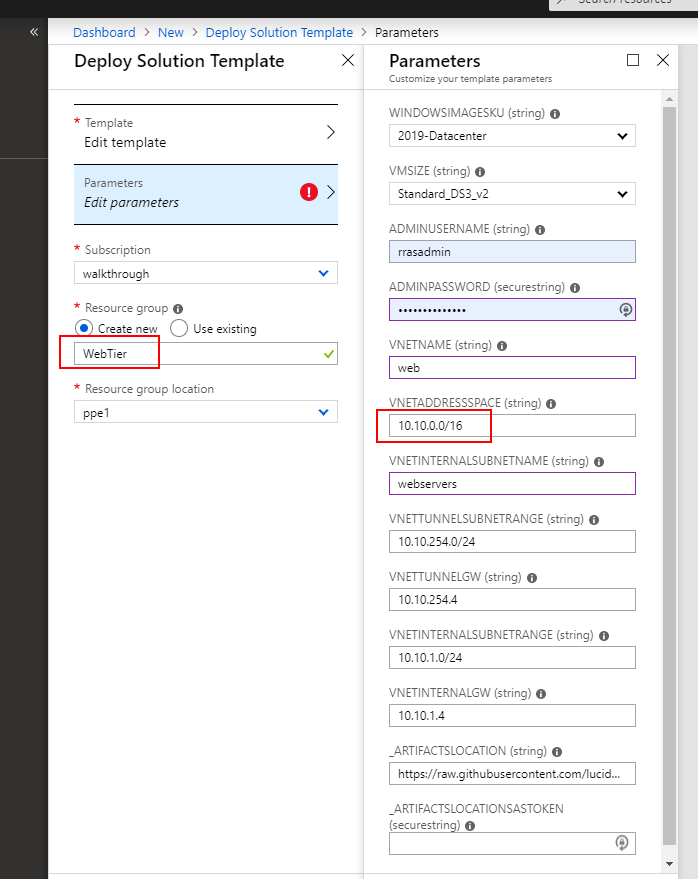


## Walkthrough

### Deploy ‘WebTier’ to Azure Stack Instances PPE1

1. Open the portal and create a resource
2. Select Template Deployment
3. 
4. Copy and paste the content of the azuredeploy.json into the template window. You will see the resources contained within the template, click save
5. 
6. Enter a Resource Group name and ensure the parameters are correct.

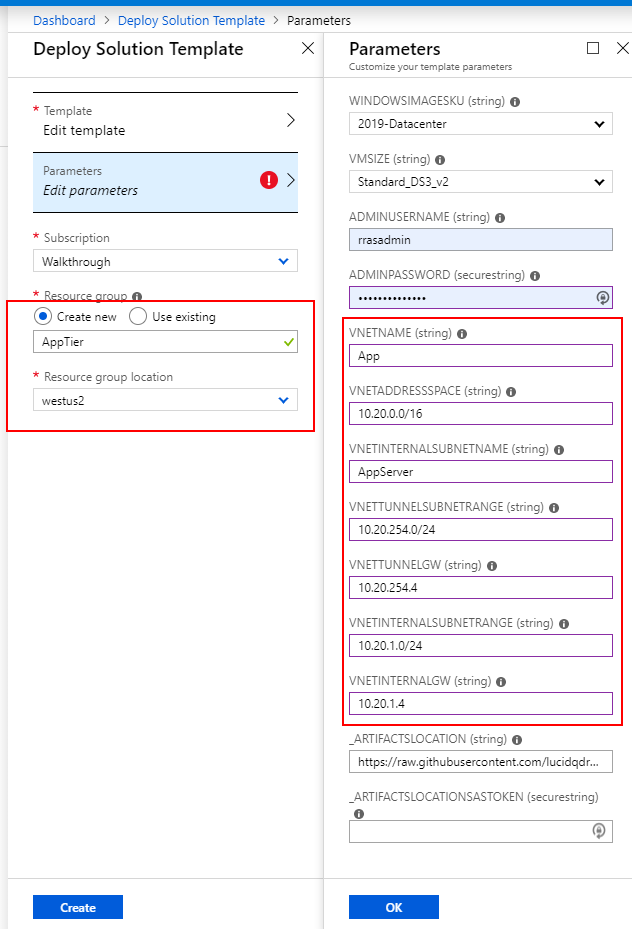
**Note:** the WebTier address space will be **10.10.0.0/16** and you can see resource group location is **PPE1**

1. 

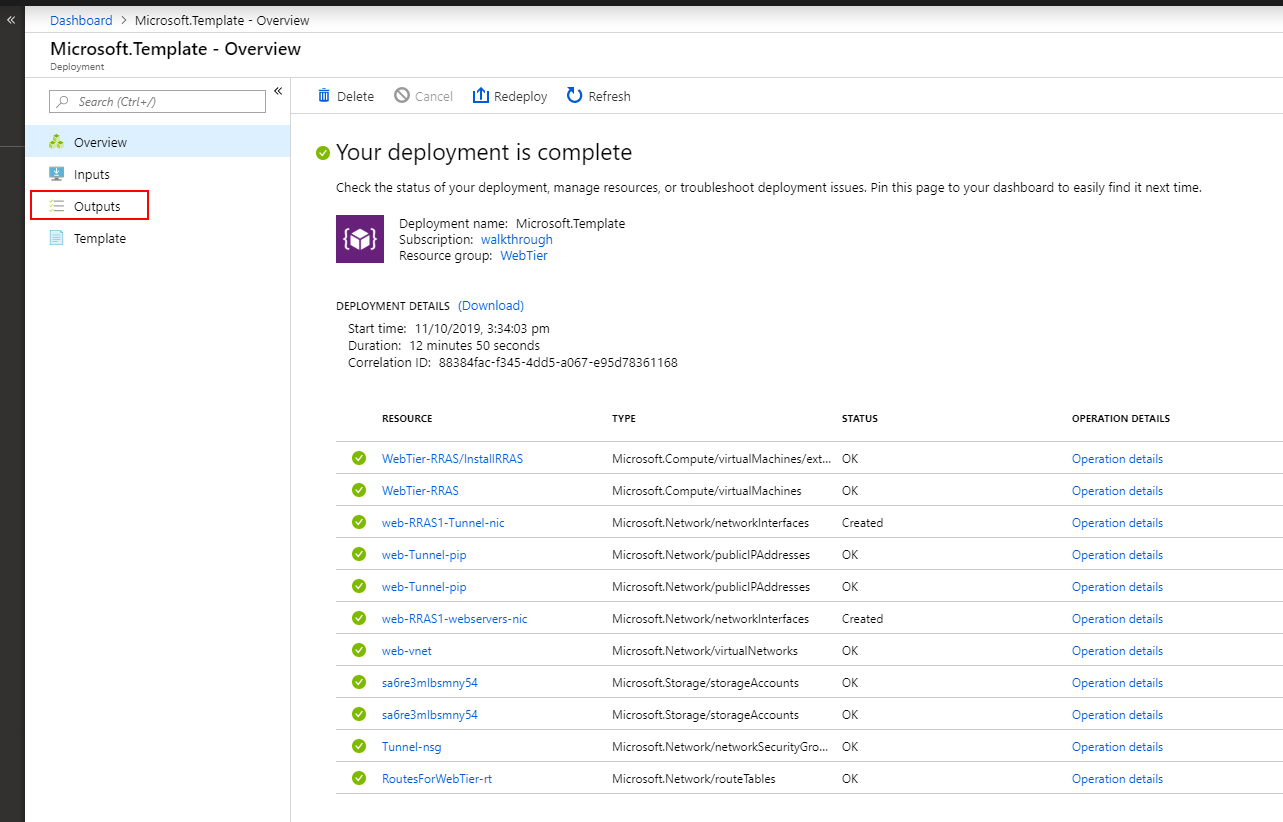
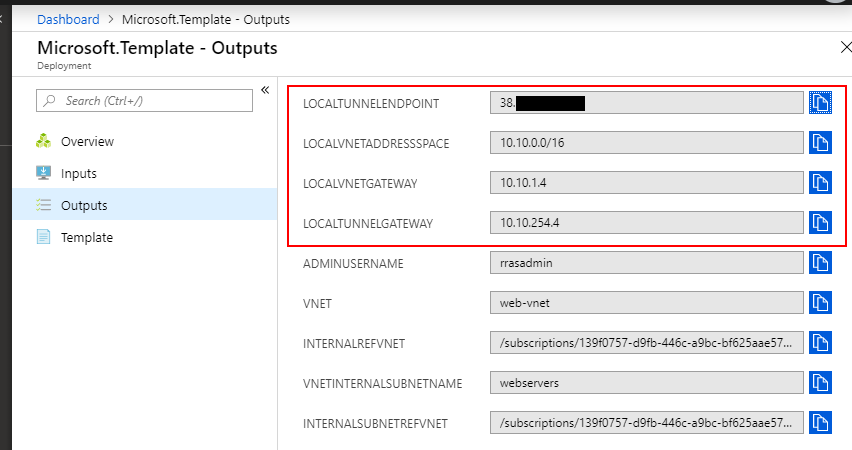
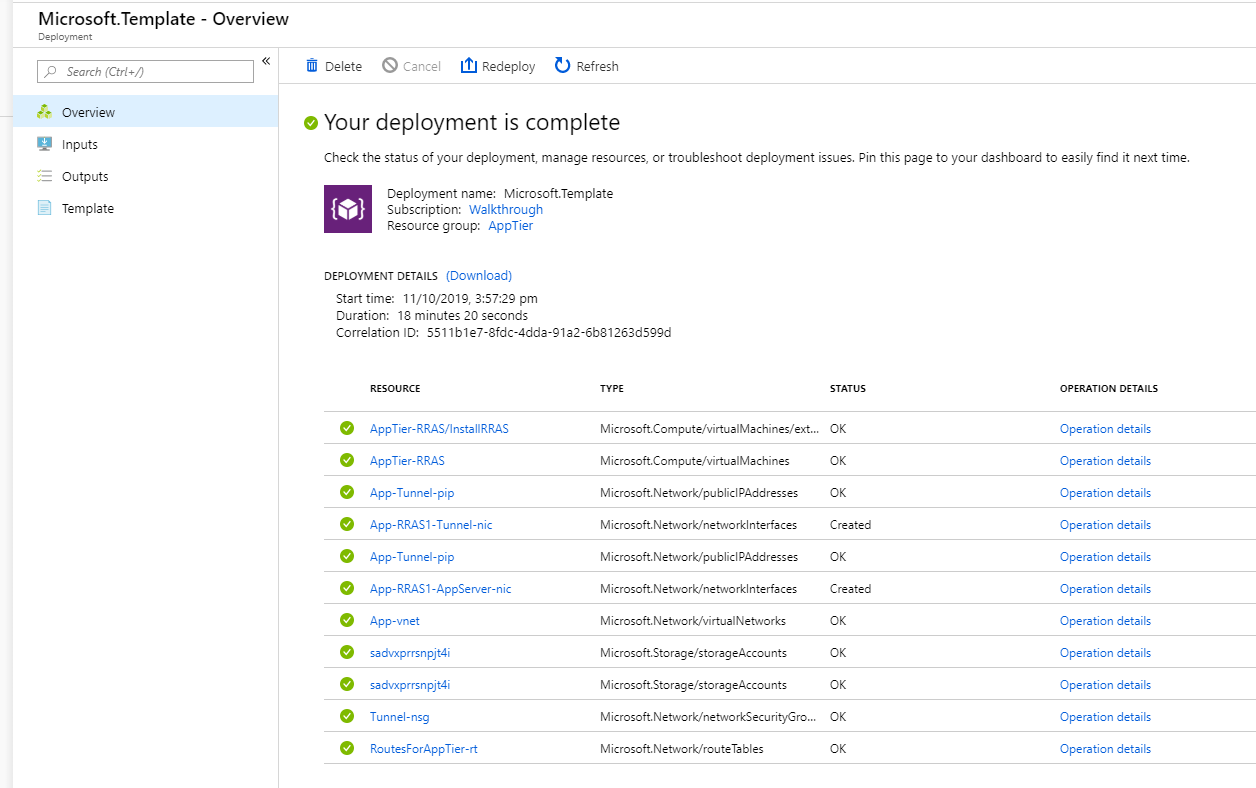
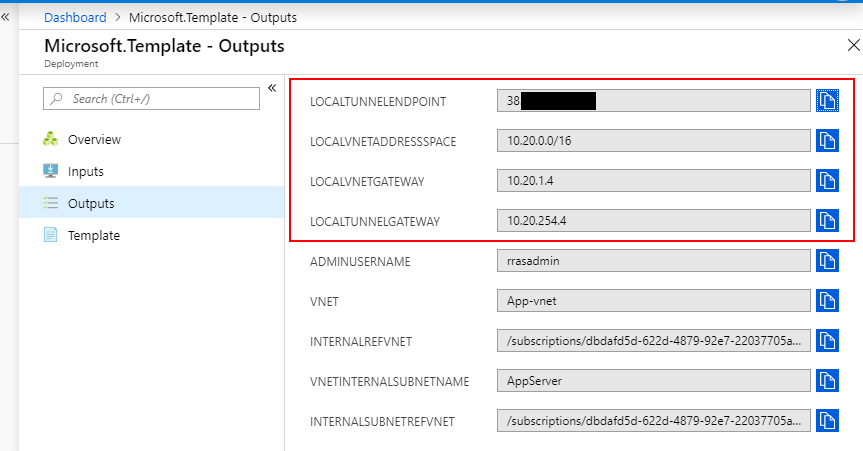
### Deploy ‘AppTier’ to Azure Stack Instances WestUS2

1. Same process as the ‘WebTier’ but different parameters as shown here

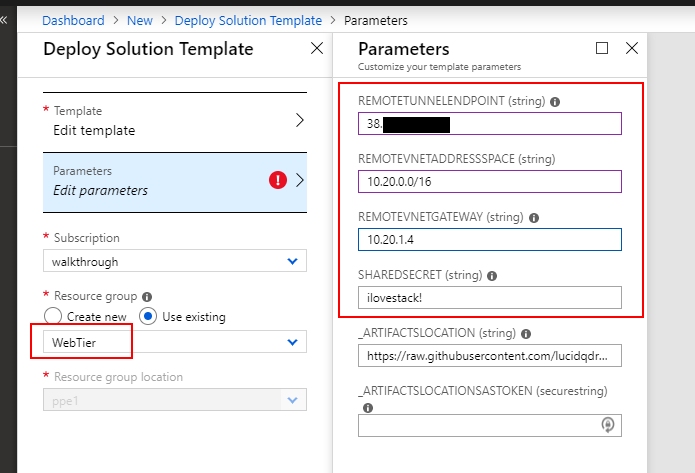
**Note:** the AppTier address space will be **10.20.0.0/16** and you can see resource group location is **WestUS2**

1. 

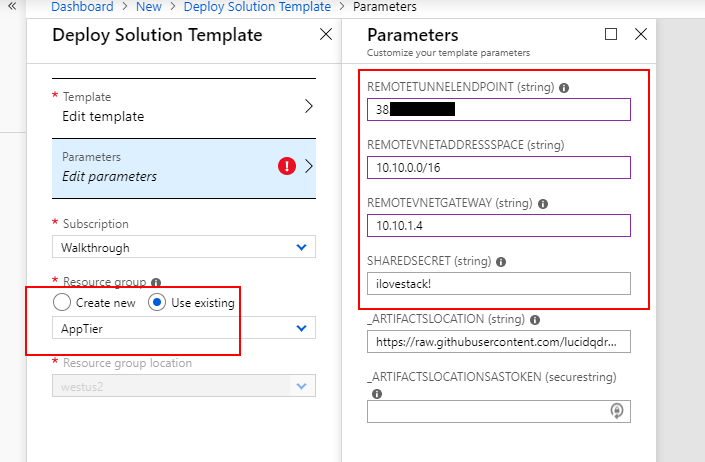
### Review the deployments for ‘WebTier’ and ‘Apptier’ and capture Outputs

1. Review the deployment completed successfully. Click Outputs
2. 
3. I would suggest copying these first 4 values into notepad
4. 
5. Repeat for ‘AppTier’ deployment
6. 
7. 

### Create Tunnel from ‘WebTier’ to ‘AppTier’

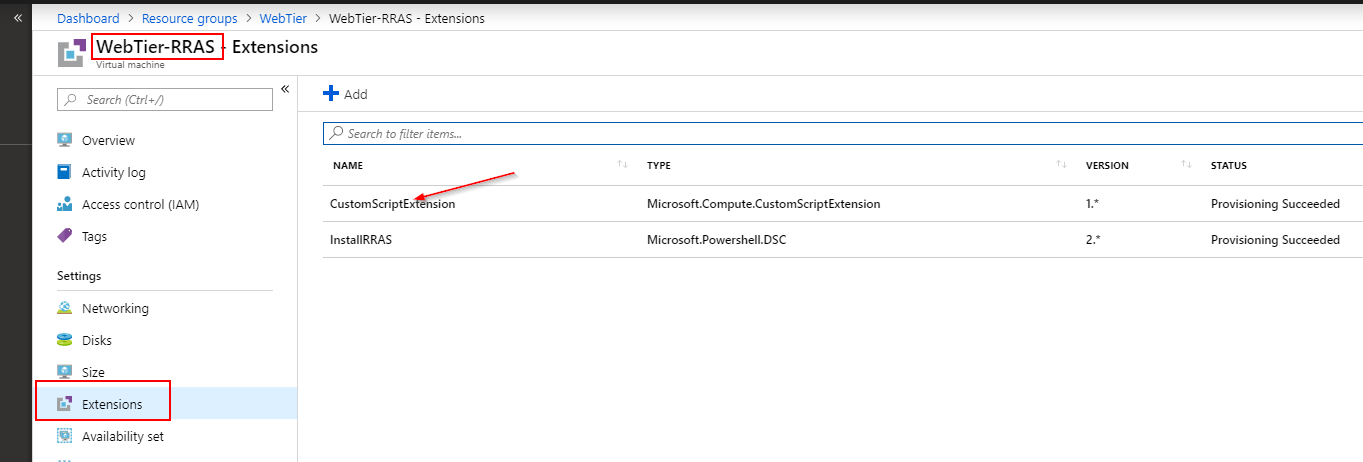
1. Create a resource
2. Select template deployment
3. Paste the contents from **azuredeploy.tunnel.ike.json**
4. Select edit parameters
5. 

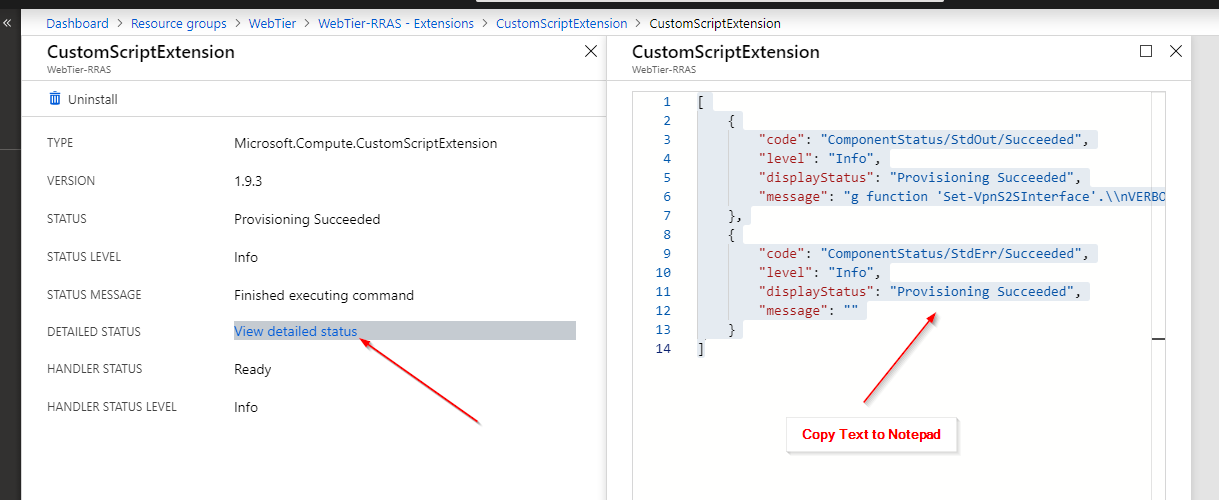
### Create Tunnel from ‘AppTier’ to ‘WebTier’

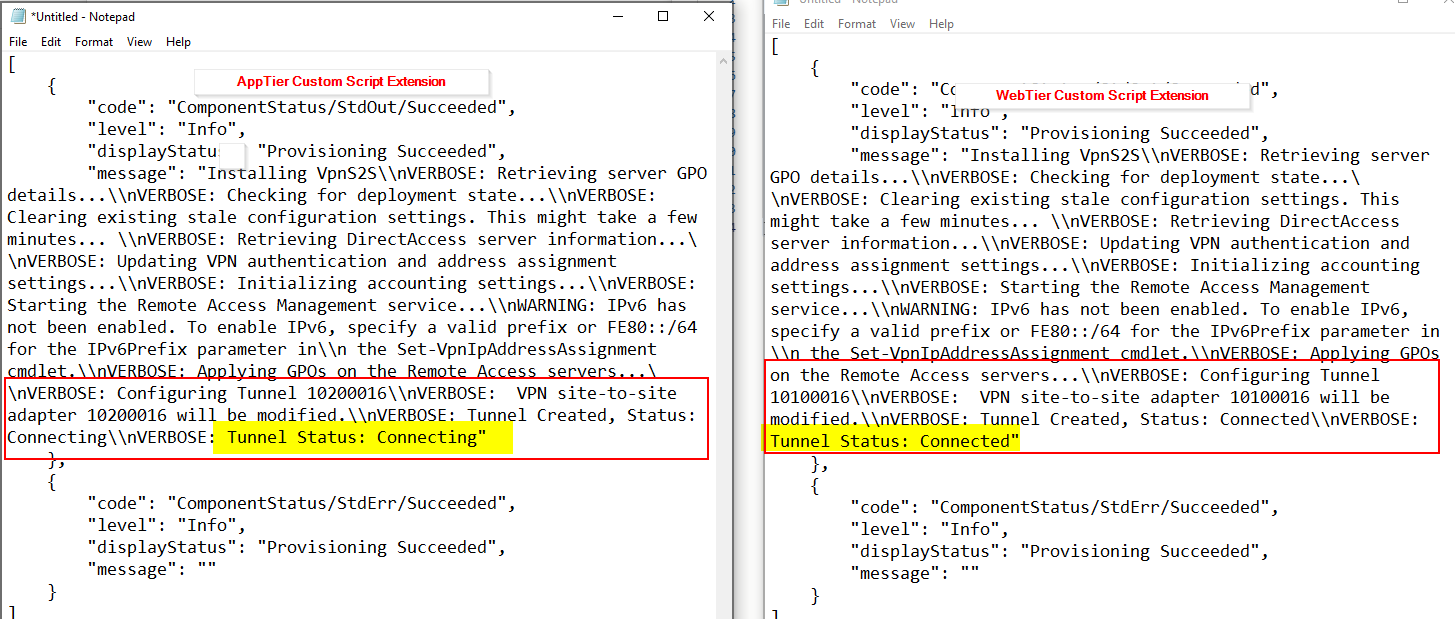
1. Create a resource
2. Select template deployment
3. Paste the contents from **azuredeploy.tunnel.ike.json**
4. Select edit parameters
5. 

### Viewing Tunnel Deployment

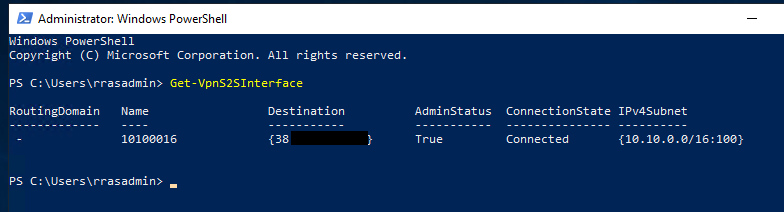
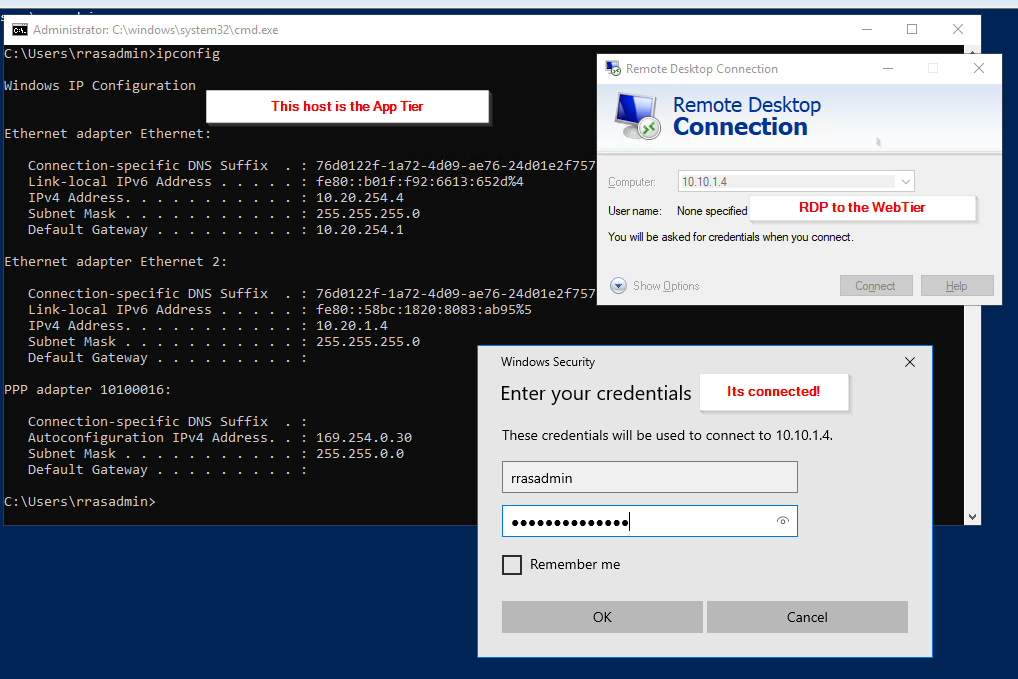
If you view the output from the custom script extension you can see the tunnel being created and it should show the status. Unless you run both very quickly you will generally see one showing ‘connecting’ wating for the other side to be ready and the other side will show ‘connected’ once it is deployed.







### Trouble shooting on the RRAS vm

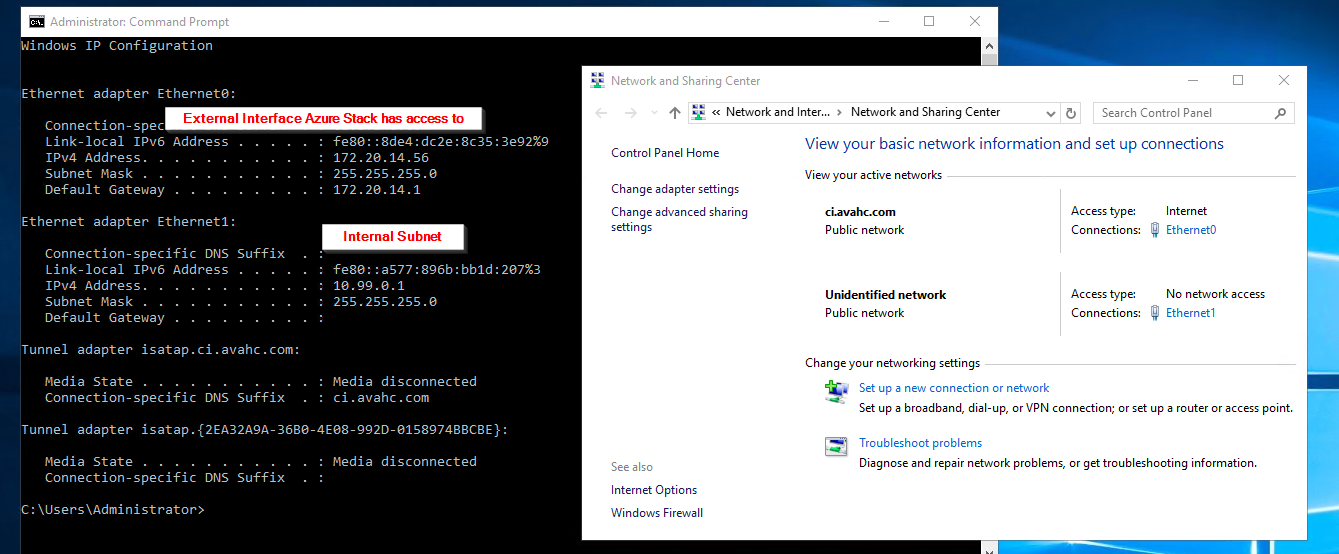
1. Change the RDP rule from Deny to Allow.
2. RDP to the system with your username and password specified during deployment
3. Open a PowerShell window and run get-VPNS2SInterface
4. 
5. From here you can use the RemoteAccess cmdlets to manage the system
6. 

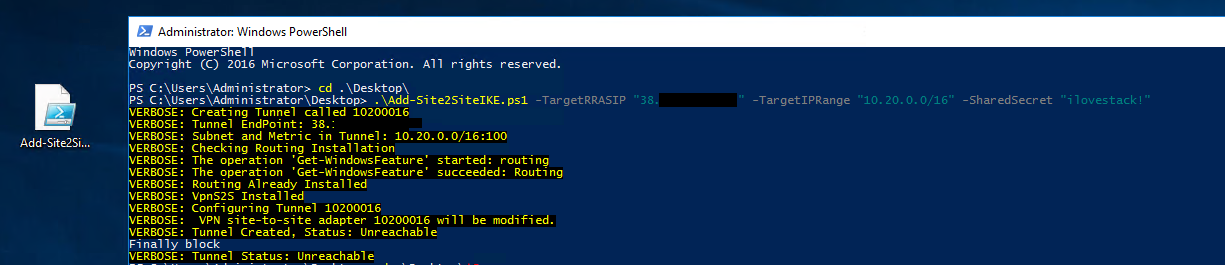
### Install RRAS on a on-premises VM ‘DBTier’

1. This is a Windows 2016 image
2. If you copy the Add-Site2SiteIKE.ps1 script and run it locally it will install the WindowsFeature and RemoteAccess

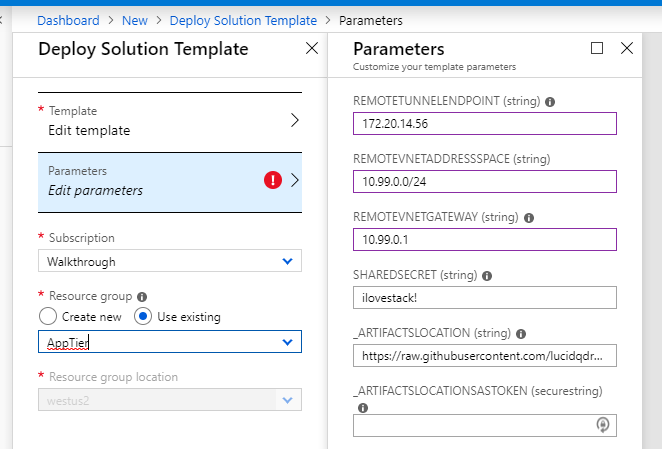
**Note:** Depending on your environment you may need to reboot your system

For reference here is the on-premise machine network configuration

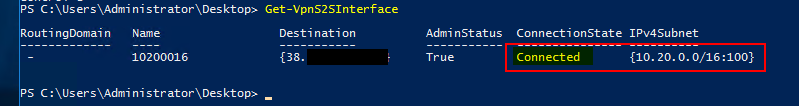
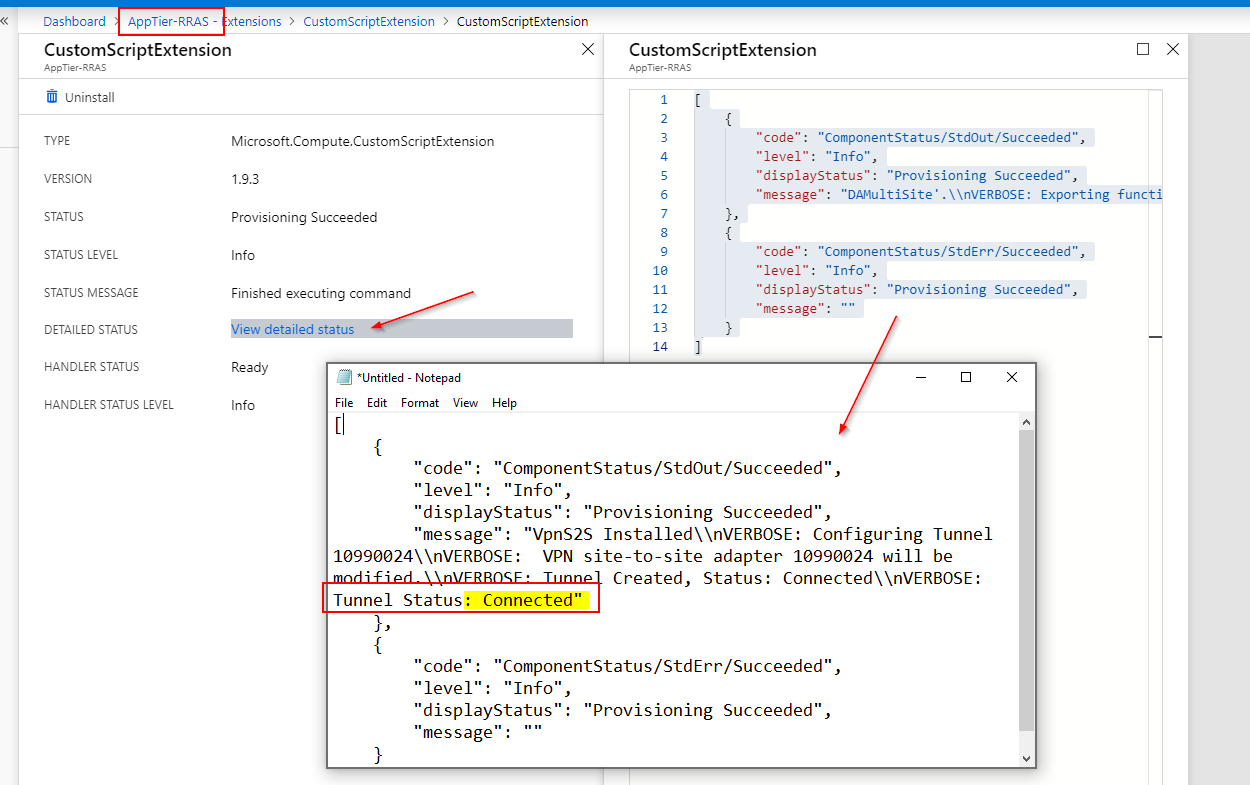


1. Run the script adding the Output parameters we captured from the AppTier template deployment
2. 
3. The tunnel is now configured and waiting for the AppTier connection

### Configure ‘AppTier to DBTier’

1. Create a resource
2. Select template deployment
3. Paste the contents from **azuredeploy.tunnel.ike.json**
4. Select edit parameters
5. 
6. We can see we have the AppTier Selected and the remote internal network 10.99.0.1

### Confirm Tunnel between ‘AppTier’ and ‘DBtier’

1. From the on-premise system we can see the tunnel is connected
2. 
3. From the AppTier custom script extension it shows connected
4. 

**Note:** You can test RDP both ways

**Important Note:** To implement this solution on-premises you will most likely need to deploy routes to the Azure Stack remote network into you switching infrastructure or at a minimum on specific VMs