Lenovo Engineered Solution for Microsoft Edge Cloud

Windows Azure Pack with System Center 2016 on Windows Server 2016

Deployment Guide

First Edition (June 2017)

Table of Contents

Introduction

Microsoft™ Edge Cloud is an on-premise, remotely managed, cloud-based solution designed for companies with multiple sites. It includes an edge server that is managed by Microsoft's private cloud solution. This edge server runs on converged infrastructure and can remain independently operational, thus keeping the remote site running even if it loses a connection to the main data center or the Internet. Local applications, file and print, point of sale, and domain services remain available and synch with the data center servers when connections are back online.

The edge server takes advantage of existing Azure™ connected services (such as Office 365 for email and Office applications), while using Azure cloud backup for disaster recovery scenarios. The solution at the remote edge locations can start small as a single server, and scale to more servers as a business grows.

At the data center side, the solution is hosted on Microsoft's System Center™ Virtual Machine Manager (VMM) providing infrastructure as a service (IaaS). The management of the solution is provided by Windows™ Azure Pack which provides a management portal and tenant portal that seamlessly integrates with System Center. The management portal is intended for overall environment administration by a centralized IT team. The tenant portal enables each customer or division to manage their own servers and sites.

Windows Azure Pack overview

Windows Azure Pack is Microsoft's on-premise cloud solution, that runs on standard server hardware, and is ideal for small to midsize businesses. The solution is highly scalable, up to enterprise levels, thanks to the underlying System Center resources. Azure Pack provides a set of Azure technologies for private cloud environments, all provided with Windows Server™ without additional costs. The solution can also expand and integrate with Azure public cloud components, to create hybrid cloud environments as your business demands.

For the purpose of this document, the following roles are used to clarify use of the two different Azure Pack portals.

- IT Administrators
  This refers to the central IT administration team that manages the entire infrastructure that supports Azure Pack. They use the Azure Pack admin portal, to manage the environment and tenant capabilities and resources
- Tenant Administrators
  This refers to the customer, self-service portal users. They use the Azure Pack tenant portal to manage virtual machine environments allocated to them, whether hosted in the data center or at remote sites.

Simplified management is provided by two portals: an administrative portal for IT administrators and a tenant self-service portal for tenant administrators. Both run on the same centralized infrastructure as services provided by Microsoft System Center components.

One of the huge benefits of Azure Pack is the ability to easily deploy and manage virtual machines, both locally in the data center and at remote sites. Azure Pack also supports SQL™ databases as a service (DBaaS) and web application hosting or platform as a service (PaaS)

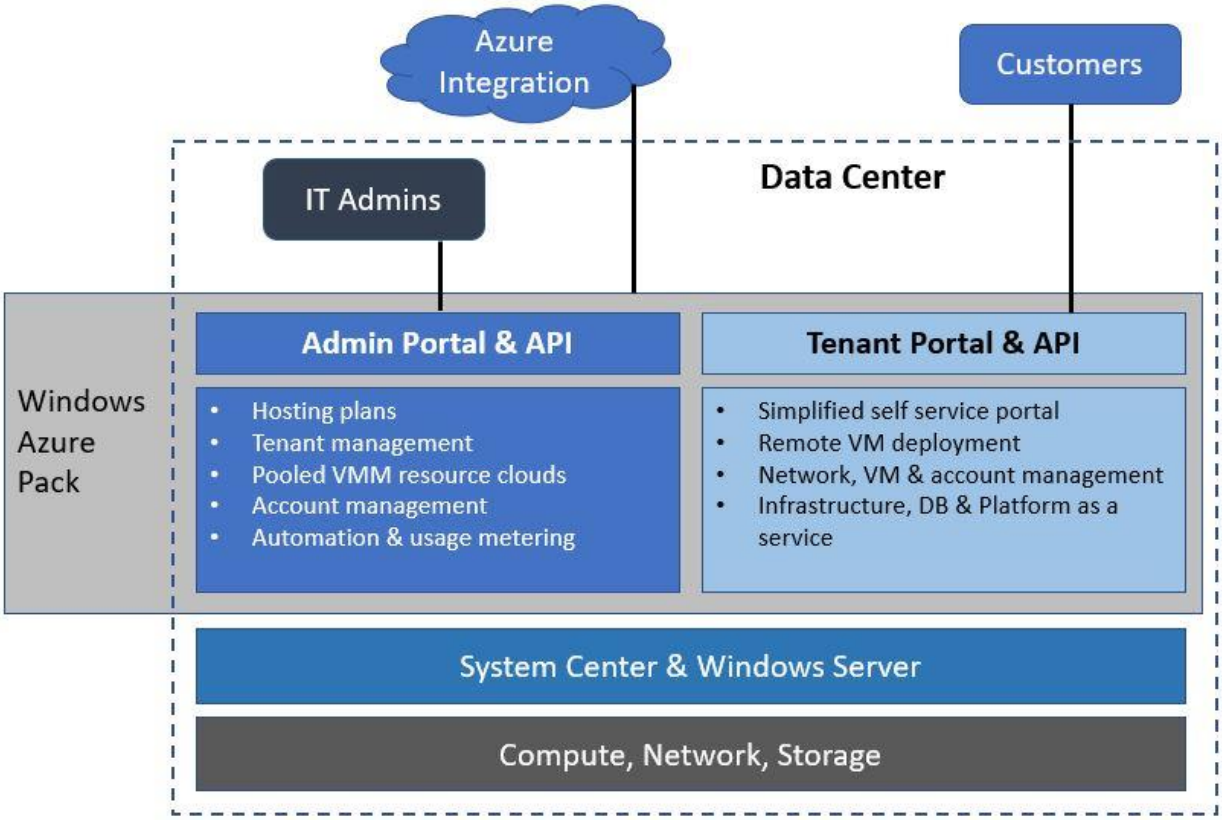

Figure 1 Windows Azure Pack features overview

For the test configuration, some of the components are combined to keep the number of VMs low and to validate a minimum configuration. The VMs and roles are as follows:

- VM1: System Center 2016 Virtual Machine Manager (SCVMM)
- VM2: SQL Server 2016 & Service Provider Foundation (SPF) 2016
- VM3: Windows Azure Pack – IIS based IT admin portal
- VM4: Windows Azure Pack – IIS based tenant self-service portal
- VM5: Windows RAS VPN and routing

Edge Cloud has most of its components at the data center or MSP/CSP location, while maintaining the ability to manage remote sites via the tenant portal running at the data center.

Supporting components

Edge Cloud requires the following components as foundations for the installation of Windows Azure Pack. Below is a summary of each component. The System Center components listed are the minimal required for Azure Pack, however they could be expanded upon where additional features are needed.

- **System Center 2016 VMM (SCVMM)**

  Should be installed on a dedicated VM with adequate processing and RAM resources.

- **Service Provider Foundation 2016 (SPF)**

  This is a sub-component of System Center Orchestrator, and is installed by running the System Center Orchestrator installation package and selecting the Service Provider Foundation install option only. No other Orchestrator components are needed.

- **SQL Server 2016**

  This solution uses SQL 2016, which is fully compatible with all the components needed for Azure Pack integration and System Center 2016.

  Note: SQL needs to be in mixed mode, as some components require the SQL SA account. It also needs to have a domain-level SQL service account created with SQL admin level credentials; this is requested by the various components during the installations.

- **Azure Cloud subscription**

  An Azure subscription is required to create a backup vault, which is a backup-specific storage pool. The cloud-based storage is more cost effective in hardware and operational expenses, when compared to on-premise solutions. Azure backup uses a lightweight agent on each remote server for file-level backups.

- **Storage**

  The recommended storage for the Hyper-V cluster at the data center is Storage Spaces Direct (S2D). However, any other supported storage in a customer's data center could also be leveraged. A Storage Spaces pool is also recommended for the edge server, which utilizes the System x3650 M5 internal storage capability.

- **Windows Patches**

  Ensure that all security and fix patches are installed, and recheck for updates after Azure Pack is installed, in order to pick up any Azure Pack update rollups. In addition to security patches, the rollups include fixes and important Azure Pack versioning updates that resolve issues or provide improved or additional functionality.

- **Office 365**

  Office 365 provides a hybrid Office software solution that can be installed on the local PC or laptop, or accessed fully online within the Office 365 portal. It provides access for multiple device types, from any location. For edge cloud remote sites, Office 365 is the recommended method for providing email and Office applications for remote workers.

- **Domain services**

  Each tenant will have a resource Domain Controller(DC) deployed as a VM in the data center. This DC will synch with the one installed at each remote site, for redundancy.

- **Solution Monitoring**

  Additional System Center solutions such as Operations Manager might be needed to provide monitoring capabilities. However, the assumption is most customers have adequate infrastructure monitoring in place that the solution can leverage.

Solution architecture

The overall design includes both data center and remote site components. At the data center, the core components of Windows Azure Pack are hosted on virtual infrastructure, which is all managed by System Center VMM. The Azure Pack admin and tenant portals are hosted at the data center; tenant administrators can remotely manage their servers and remote sites by logging into their own tenant portal.

The Azure Pack admin portal is where IT administrators control what each tenant can do within their tenant portals. Some of the actions available in the tenant portal includes VM deployment to remote sites or the datacenter, managing the VMs, remotely connecting to the server consoles, and performing backups. There is flexibility in the design, and existing SQL or System Center environments can be leveraged for this solution.

There are some complex dependencies between SQL Server, System Center, IIS web services, and Azure Pack components. These are addressed in the detailed installation steps. Attention to detail during the installation is important for a successful deployment.

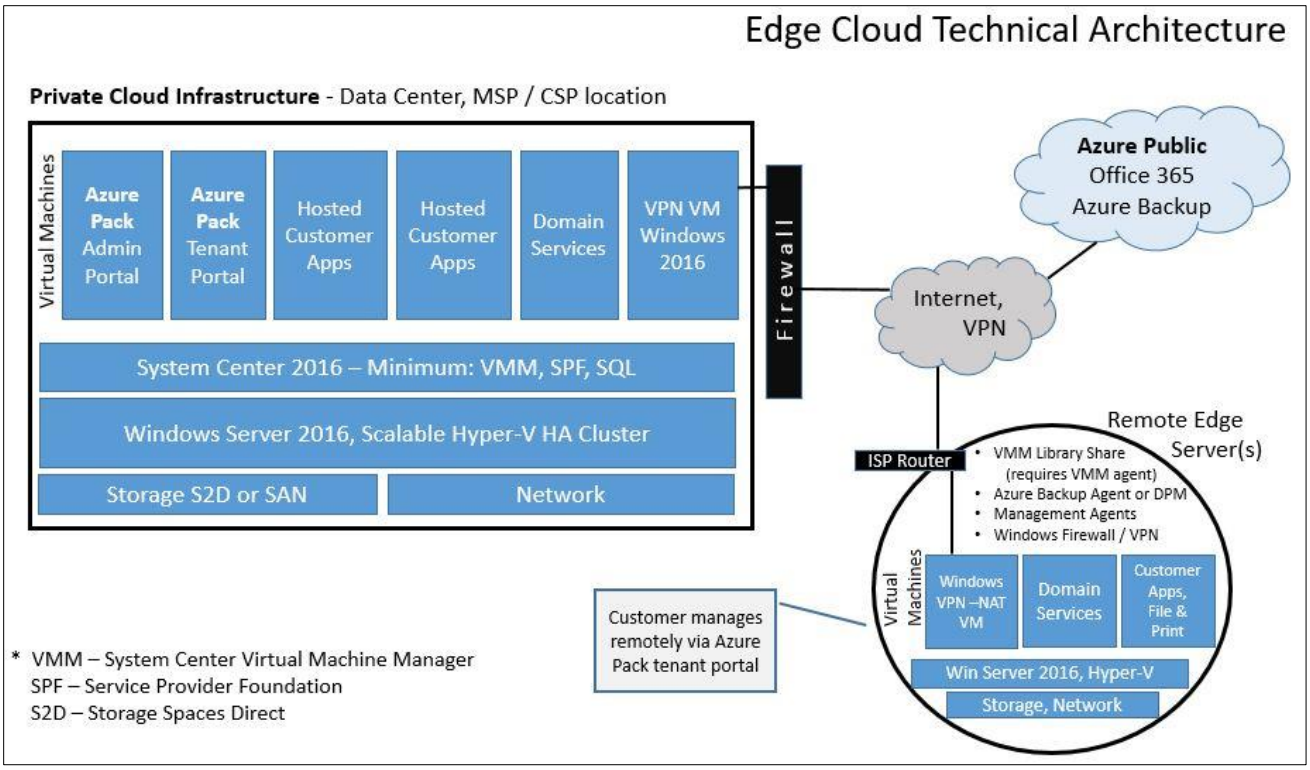

Figure 2 Edge Cloud Architecture drawing

As shown in the figure 2 above, the minimum components at the data center side include System Center VMM manager (VMM), System Center Service Provider Foundation (SPF) and SQL Server to host the configuration databases. These components can all run on VMs. Additionally, a customer can host application VMs in the data center environment, and manage them from within the Azure Pack tenant portal.

Office 365 is the recommended approach to providing customers with email and office tools. The solution also makes use of Azure Backup capabilities, to minimize the need for on-site backup storage.

At the edge server, the infrastructure is Hyper-converged, with compute, network and storage resources all running on one system. The edge server can of course be clustered as well, in larger remote sites or where high availability is required. The edge server utilizes Windows built-in components for virtualization, storage, VPN, and security. The server is configured as a VMM library server, which means it has the VMM agent installed and a network share setup, so that OS deployment images can be stored locally. A read-only Active Directory domain controller and DNS runs on a dedicated VM, in order to provide local login and name resolution in the event of a network outage.

Network design

The solution uses combined physical and virtual networking to create a secure IPsec VPN tunnel between the data center and remote sites. There must be flexibility in the design so that the

configuration can be altered to fit the various existing network topologies at either the data center or remote sites. The deployment will require network review and planning to determine the best overall design. The decision to use the built-in Windows VPN solution for the test configuration and this document is intended to keep the configuration straightforward and the costs lower. It is also possible to use a customer's existing VPN hardware or solution.

With the introduction of Windows Server 2016 Software Defined Networking (SDN) there are several options available for VPN and virtual networking. The solution defined in this document uses the simplest approach that is included with Windows Server, which is a Routing and Remote Access persistent site-to-site VPN. If a customer has the full Windows 2016 SDN network stack in place, then the solution could be configured to take advantage of this level of virtual infrastructure. The full deployment of Windows 2016 and System Center SDN is well beyond the scope of this solution, as it involves major decisions on how a customer's network is designed and managed.

Note: During the testing, we discovered that internal mode Hyper-V virtual switches are not supported with VMM. This is because VMM requires an associated physical NIC to manage, which internal virtual switches do not have. The work-around is to use an external mode virtual switch, but leave it un-cabled. This is what is meant by internal switch in figure 3. For the clustered nodes, these NICs are cabled directly to each other functioning as a direct connected heartbeat and live migration link. The design goal is to keep the VMs on their own virtual switch, without exposing them to the Internet directly. All traffic goes through the VPN/NAT/Firewall VM for site-to-site or Internet access.

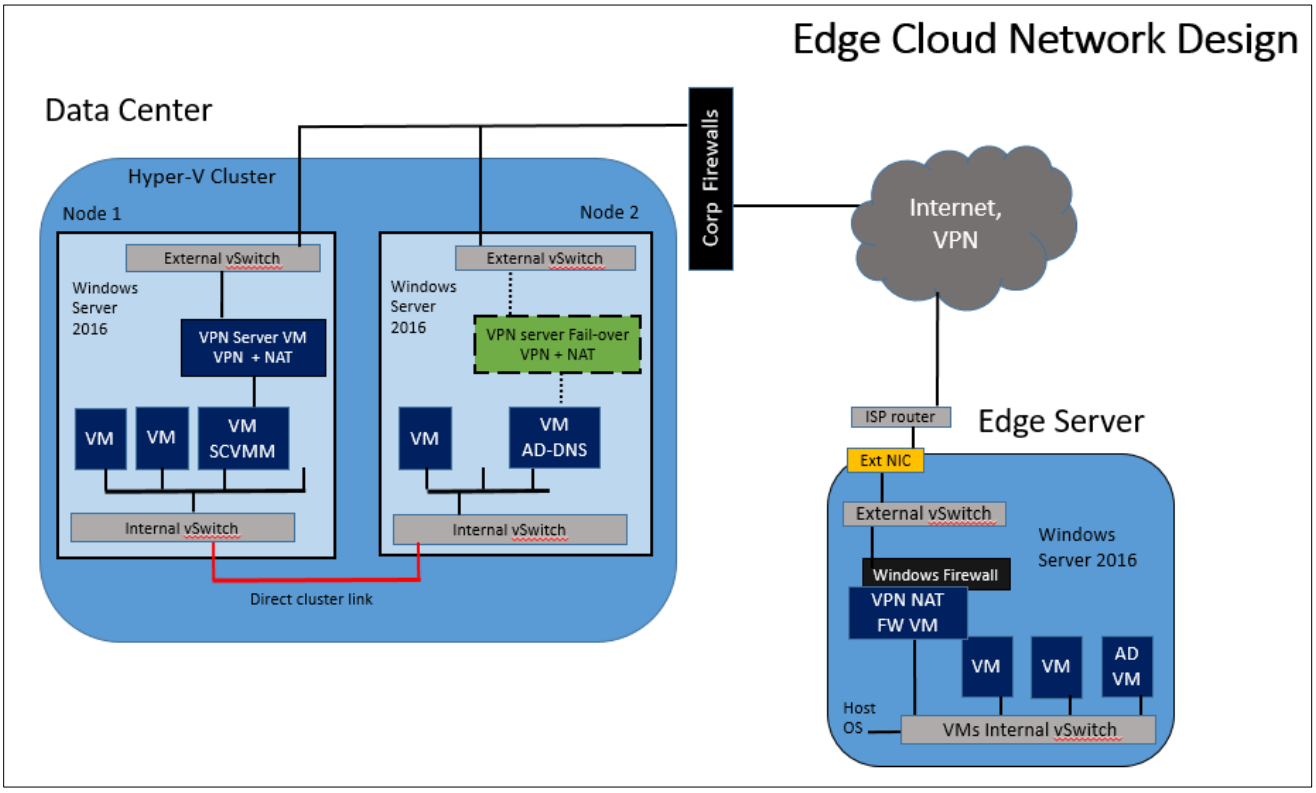

Figure 3 Edge Cloud high-level network design

Remote site network

The remote site design assumes there might only be an ISP router connection to the internet. The internet connection at the server's physical port is protected by the Windows firewall running on a dedicated VM. The internal VMs and the edge server OS accesses the network though an internal Hyper-V virtual switch that is routed through the dedicated VPN/NAT Firewall VM.

Data Center network

The data center side of the solution is running on highly-available VMs hosted on scalable Lenovo™ x3650 multi-node Hyper-V clusters. All customer environments will vary; however, the solution assumes there is an existing firewall in place, protecting the data center. As a result, the Windows firewall is turned off on all systems within the data center.

In a typical data center, there are several ways to implement VPNs with firewalls. The VPN server can be outside the firewall, between two firewalls in a DMZ or inside the firewall. Since this solution takes advantage of Windows networking features, the VPN termination point is inside the corporate firewall.

VPN connectivity is handled by the Windows 2016 RAS VPN and routing feature., running on a dedicated and highly available VM. This provides an easily managed graphical interface, making VPN management more straight forward. Using the Windows VPN components simplifies ongoing administration by keeping all VPN configuration changes at the Windows VPN server. Corporate firewall changes would only need to be made once, which allows VPN traffic through to the VPN server. Afterwards, all VPN administration is done on the Windows VPN server.

Installation

The components and installation order are indicated below. You must ensure the right components are installed on the specified VM, as some of the components look and sound very similar. Some components can be combined on one VM: however, the following is recommended based on Microsoft's documentation and best practices for a distributed but minimal installation. Larger installations can scale further with a more distributed architecture, and load balancing the Azure Pack roles by following the Microsoft design documentation.

The installation steps that follow are based on the test configuration. A customer can scale out and provide additional redundancy where needed or expected. For example, during testing we used a single SQL server for the tests, but a production environment would normally use a high availability SQL configuration. It is also possible to use existing infrastructure in a customer's environment such as Hyper-V hosts, SQL server and System Center components.

Detailed steps on the installation and setup of common Microsoft products (such as Windows Server, SQL server and System Center) are beyond the scope of this document. Refer to the widely available Microsoft documentation for installing these infrastructure pieces.

In general, throughout the document, the installation order should be the same order as it is presented Here is a summary of the following installation steps and the order.

1. Set up service accounts
2. Deploy Hyper-V and System Center infrastructure
    a. Set up the cluster and storage
    b. System Center components
    c. Detailed guidance for Service Provider Foundation
3. Configure Azure Pack security pre-requisites
4. Deploy Azure Pack components
    a. Install the Azure Pack Admin Portal
    b. Install the Azure Pack Tenant Portal
    c. Azure Pack post installation tasks
5. Configure the VMM fabric
6. Register SPF and VMM with Azure Pack
7. Azure Pack Plan creation
8. Create user accounts
9. Identity Management

Set up service accounts

Due to the distributed nature of the solution, domain level service accounts are required or recommended for many of the components. Before starting the installation, create the following domain service accounts. All installation tasks should be performed while logged in with a domain admin level account.

- SQL Server
- Service Provider Foundation
- System Center VMM

Deploy Hyper-V and System Center infrastructure

The recommendations below are just a starting point, and sized for smaller environments. This is what was used for the test configuration. As always, scale the environment out as needed. Although we cover Microsoft's Storage Spaces Direct (S2D) in this guide, existing SAN-based shared storage can be used for the cluster, if that is preferred.

The next task is to set up the cluster and storage, which will host the Hyper-V environment. In the example below, we use the built-in disks in the two System x3650 M5s to leverage Microsoft's Storage

Spaces Direct (S2D) as the cluster storage. Since this is a new technology, the detailed steps are included here. We are using the available network cards (NICs) in the server, faster cards provide better performance since the cluster uses the local network in a fabric configuration.

Note: The drives to be used for S2D cannot be connected to any type of RAID controller. They must use a SAS HBA such as the N2215 that is specified in the Bill of Materials. The drives used for the OS mirror in the back of the server are connected to the internal Server RAID controller.

Set up the cluster and storage

It is recommended that PowerShell be used to configure the storage and cluster, due to the specific configuration requirements of S2D clustered storage. The two Windows servers should be domain-joined, and logged in with a domain administrator-level account.

1. Verify the internal drives are connected to the SAS HBA. S2D doesn't allow any type of RAID controller for the drives, even in JBOD or pass-through mode.
2. Install the required server roles if they are not installed, by running the script below.

```
Install-WindowsFeature -Name File-Services
Install-WindowsFeature -Name Failover-Clustering -IncludeManagementTools
Install-WindowsFeature -Name Hyper-V -IncludeManagementTools -Restart
```

3. In the Windows network properties, disable any NICs that won't be used in the configuration, such as the USB Remote NDIS device.
4. Check that the internal drives to be used are online in Windows Disk Manager. An identical number of drives must be available on each node.
5. Run the following PowerShell commands to verify that the nodes are ready for the S2D and cluster deployment.

```
Test-Cluster -Node Srvr01,Srvr02 -Include "Storage Spaces
Direct",Inventory,Network,"System Configuration"
```

6. Resolve any configuration issues that are flagged during the test. Once all issues are resolved and retested, run the following command to create the cluster. Specific storage will be added in a later step, so this command includes the -NoStorage switch.

```
New-Cluster -Name MyCluster -Node Srvr01,Srvr02 -NoStorage
```

7. After the cluster creation is complete, configure a file share witness. First, create a network share on another server. Then use Cluster Manager to specify the file share witness.
8. The next step is to enable S2D for the cluster. Run the following command to configure it:

```
Enable-ClusterStorageSpacesDirect –CimSession MyCluster -PoolFriendlyName
MyS2DPool
```

Give this command adequate time to finish. It may appear to hang for extended periods of time. This is considered normal, and a known Microsoft issue that may be resolved soon.

After it completes, a single storage pool exists, which is available to both nodes as shared storage. It also creates two storage tiers, one called Performance the other Capacity. This is setup automatically, as the PowerShell commands configure the SSDs for performance caching.

At this point, virtual disks and volumes can be configured and mapped to the cluster as Cluster Shared Volumes (CSV).

System Center components

1. Deploy 5 VMs running **Windows Server 2016**. If a System Center environment is not available at this point for VM creation, then create a single VM and then save it off as a template. Run Sysprep after the base OS configuration is done. This VHDX image will also be used later to populate the VMM library server with OS template files.

2. Install **SQL Server 2016** on one of the VMs.
   Important: Ensure that SQL authentication is set to Mixed mode. Some of the configurations require domain accounts, and others require the local SQL SA account.

3. Install **System Center Virtual Machine Manager 2016** on one of the VMs.

4. Install **Service Provider Foundation 2016**, this is also installed on the SQL Server VM. Due to the critical role SPF plays, use the detailed installation steps provided in the next section.

   One VM will be used as a dedicated VPN and NAT server. The other two VMs will host the Azure Pack tenant and admin portals. These are installed later and covered in the sections titled Site to site VPN configuration and Deploy Azure Pack components.

   After installing the above SQL and System Center components, check windows update for important updates.

Detailed Installation steps for Service Provider Foundation

SPF facilitates communication between Azure Pack and System Center. Detailed installation steps are provided here to help ensure that this important part of the solution is installed and configured correctly. Pay special attention to the assignment of accounts and permissions, as SPF requires credentials on both System Center and Azure Pack components.

The following are necessary prerequisites before installing SPF.

1. Use Server Manager to install these features on the SPF server:

- Add Role: Web Server (IIS) server. Include the following additional services:
    - Basic Authentication
    - Windows Authentication
    - Application Deployment ASP.NET 4.5
    - Application Development ISAPI Extensions
    - Application Deployment ISAPI Filters
    - IIS Management Scripts and Tools Role Service
- Add Feature: Management OData IIS Extension
- Add Feature: .NET Framework 4.5 features, WCF Services, HTTP Activation

2. Install the following web services, by downloading from the links below:

    - WCF Data Services 5.0 for OData V3
    - ASP.NET MVC 4

3. SPF requires the VMM console (only) to be installed locally. There are several prerequisites for the VMM console first:
    a. MSODBsql (a prerequisite for SQL cmdline tools) Download from Microsoft's site.
    b. SQL cmd line tools, available from Microsoft site
    c. Download and run ADK win 8 kit to install Windows deployment tools and Win PE environment

4. After the above VMM pre-requisites are all installed, then the VMM console can be installed.

After all the above SPF prerequisites are completed, reboot the server and then proceed with the SPF installation as follows.

Note: Regarding the next section, only one SPF service account should have been created in the earlier steps. Assign it as the service account for each of the 4 web services that will need to be configured. Be aware that each of the 4 web service configuration pages look nearly identical during installation, except for the name of the web service – e.g. Admin, Provider, Usage and VMM. Enter this same account information on each of the 4 repeating configuration pages that appear.

1. Launch the System Center Orchestrator 2016 installer.
2. On the start page, select **Service Management** - **Standalone installations** > **Service Provider Foundation.**

Figure 4 Location of SPF installation link in System Center Orchestrator Installer

3. Click **Install** after the SPF screen appears, to start the installation.
4. Accept the license agreement to continue.
5. Ensure that the installer passes the check for pre-requisites indicated earlier.
6. Enter the SQL server name, using the default port of 1433.
7. Accept the defaults for the web service paths, and select which certificate type to use.
8. Configure the 4 web services. A separate configuration page will appear for each one, prompting for account information. **Important:** As stated previously, use the same SPF domain account for all 4 services.
    - Admin web service
    - Provider web service
    - Usage web service
    - VMM web service

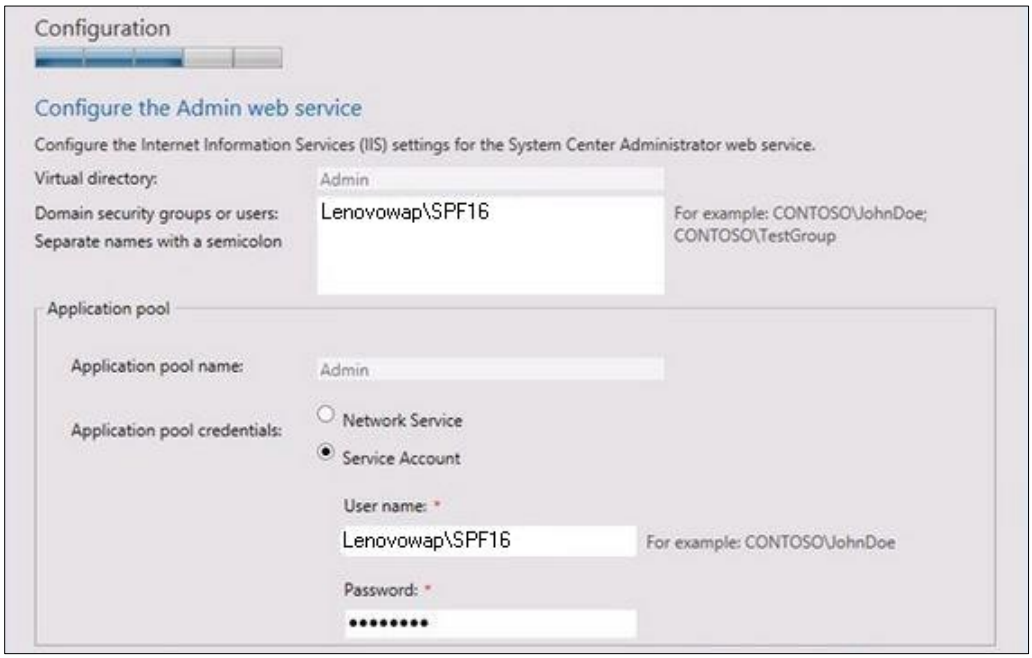

Figure 5 Configuring the 4 web services in Service Provider Foundation install screen

Note: SPF will create 4 local Windows security groups with the same names.

9. Specify Customer Experience Improvement Program participation.
10. Enable Microsoft update for SPF components.
11. Click **Install** to proceed.
12. Confirm the installation finished successfully and click **Close** to finish.

Configure Azure Pack security pre-requisites

After the above components are installed, configure the following accounts and additional security. **These settings are critical** for a successful installation of the Azure Pack components that follows.

1. SPF service account added as VMM admin role; this is set in the VMM console.

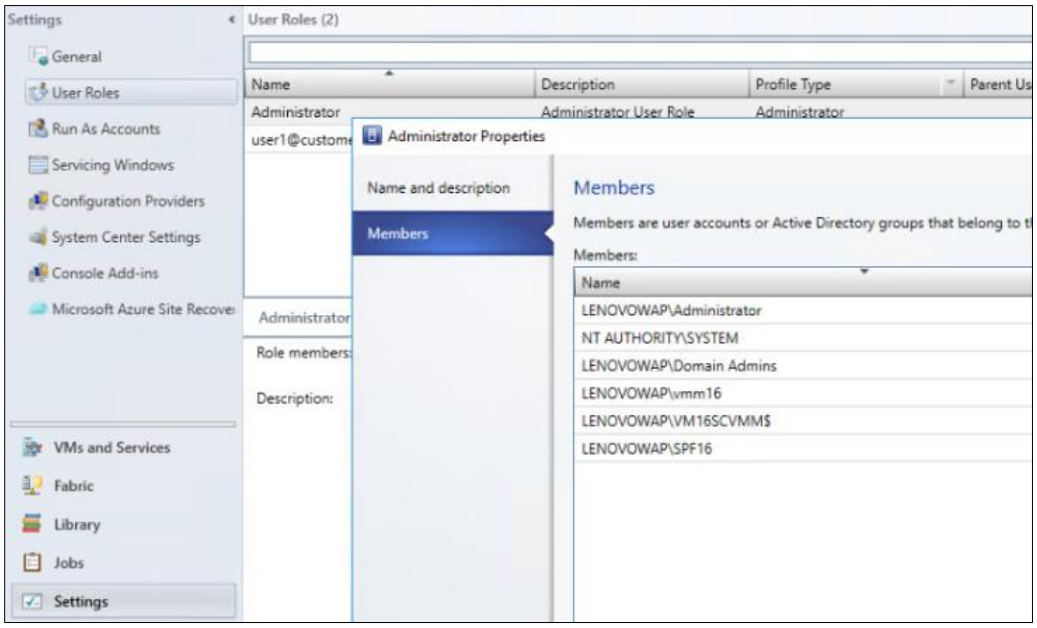

Figure 6 Adding the SPF domain level account to the VMM Administrator role in the VMM console

2. SPF and VMM service account added to local administrator group on VMM server.
3. VMM machine account added to local admin group on any VMM library servers. This is the VMM server computer account, not a service account.
4. SPF service account added to local admin group on the SPF server.

   Note: The SPF service account is the account specified during SPF setup and is the credential used for the 4 SPF IIS application pools.

5. Add SPF service account as member of SA role on SQL server. This is not done during setup.

6. Verify the VMM console that was installed on the SPF server can connect to the VMM server.
7. Log in to the SPF server locally at least once with the SPF service account.
8. SPF service account must be added to each of the 4 SPF web service local groups that were created during the SPF install, as shown in figure 7:

SPF_Admin	Admin Web Service Users
SPF_Provider	Provider Web Service Users
SPF_Usage	Usage Web Service Users
SPF_VMM	VMM Web Service Users

Figure 7 The four local Windows security groups created by the SPF install

9. Create a **local** user account on the SPF server (not a domain account). This account must also be added to the 4 local groups that the SPF install created, and be a member of the local administrator group. It is unclear from the Microsoft documentation what this account is for, or how it is used, but we are following Microsoft guidance on it.

Deploy Azure Pack components

After the above prerequisites are configured, the Azure Pack components can be installed. Due to the complex nature of the product and installation, there is not an Azure Pack installation file to download. The distributed components are installed from the Microsoft **Web Platform Installer 5.0**, which must be downloaded from the following Microsoft site.

https://www.microsoft.com/web/downloads/platform.aspx

After downloading the installer, launch it to install it on the server. It must be installed on both the tenant and admin Azure Pack portal VMs.

Install Azure Pack Admin Portal

Use the following procedure to install the Azure Pack admin portal on the Admin VM.

1. Install the Web Platform Installer 5.0 on the server.
2. Launch the Web Platform Installer on the Azure Pack admin VM.
3. Select **Products** at the top, then **Windows Azure** from the left pane.

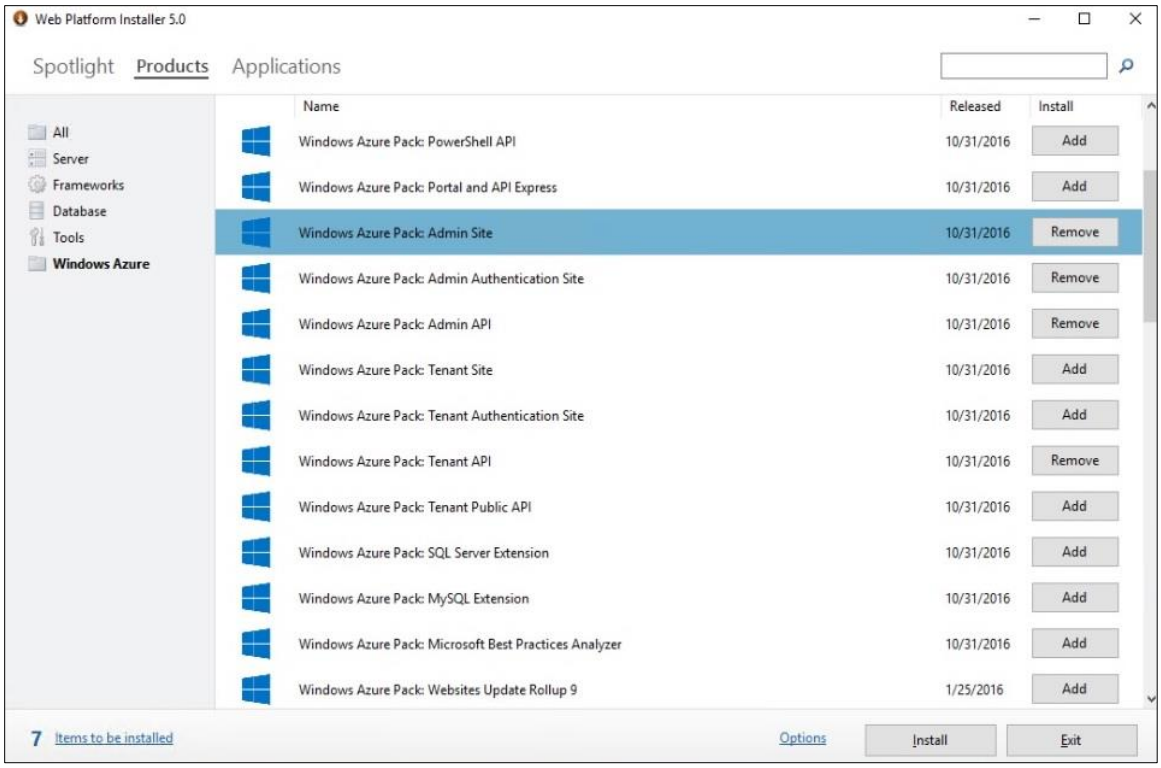

Figure 8 List of Windows Azure products to install on admin portal

4. From the list, select the following 4 components as shown above by clicking **Add** for each:

   - **Windows Azure Pack Admin Site**
   - **Windows Azure Pack Admin Authentication Site**
   - **Windows Azure Pack Admin API**
   - **Windows Azure Pack Tenant API**

5. Click **Install** to continue
6. Click **I Accept** to continue, if you agree to the licensing terms for the products

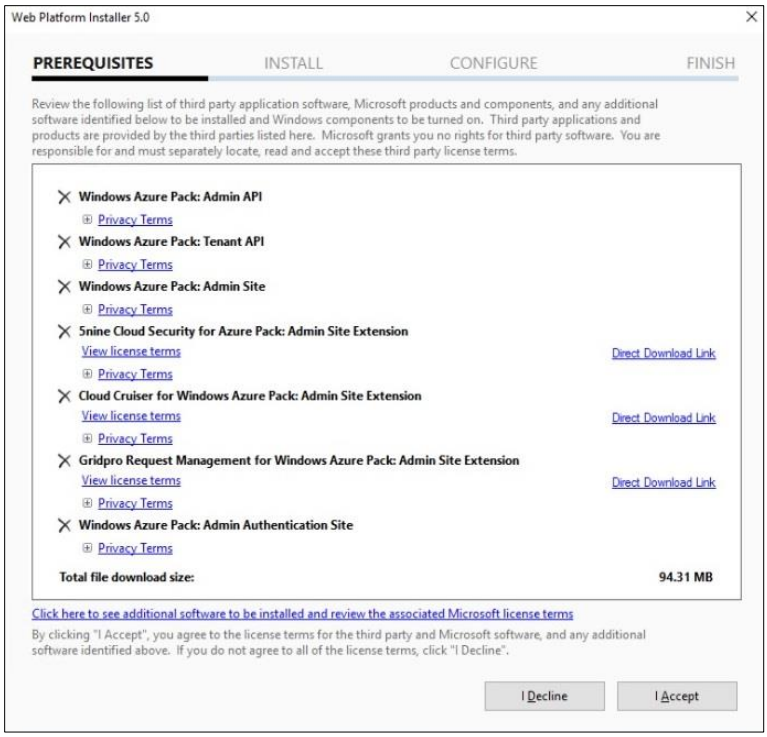

Figure 9 List of Azure Pack prerequisites

7. Click on **Continue** to proceed with the configuration phase.

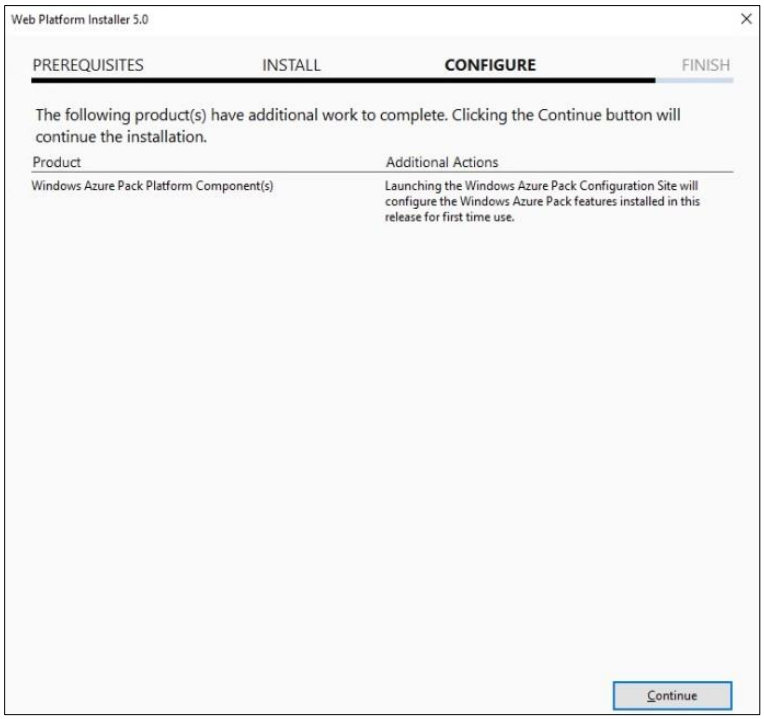

Figure 10 Configuration phase of Azure Pack installation

8. The web based configuration wizard appears. Click **configure now** to continue.

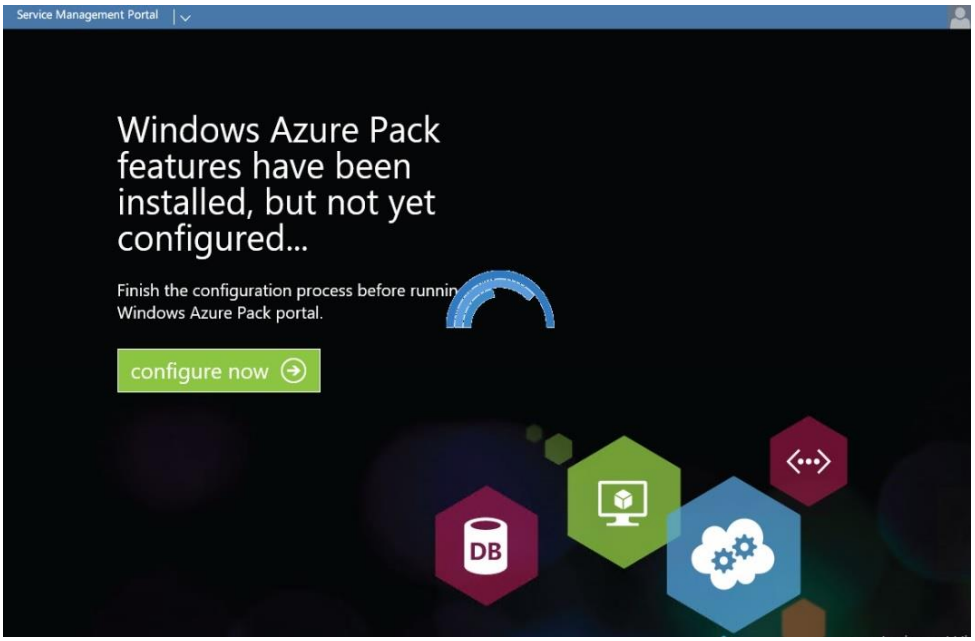

Figure 11 Azure Pack configuration web site welcome screen

9. The Database configuration screen appears, as shown in figure 12.

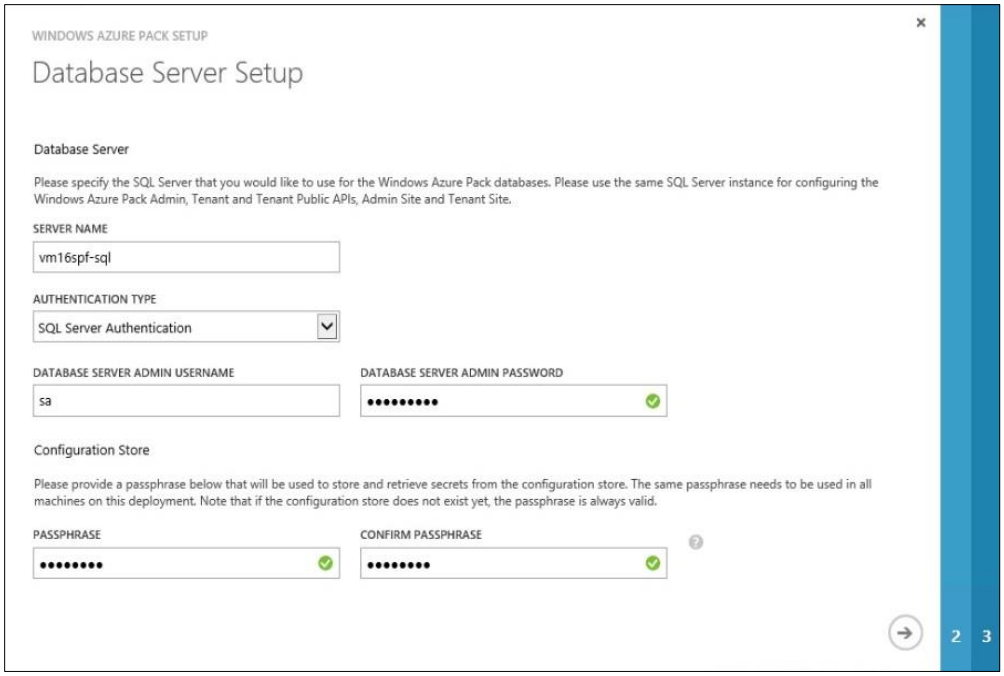

Figure 12 Azure Pack SQL database setup page

10. Enter the SQL server name and instance. If using the default SQL server instance, then just enter the SQL server name.

11. For Authentication Type, select **SQL Server Authentication** and enter the **SA** account and password. Use of domain or Windows accounts is not supported here.

12. Enter the configuration store passphrase. **Note:** The same passphrase MUST be used on each Azure Pack server in the installation, so make sure its recorded for use later.

13. Verify all the sections have green check marks, and click the lower **right arrow** to proceed.

14. Select whether to be involved in the Customer Experience Improvement program, and then click the lower **right arrow** to continue.

15. Confirm the components to be installed. Some of the items listed are pre-requisites or additional Windows components needed by the Azure Pack.

Figure 13 Summary of features to be installed

16. After the configuration finishes, verify all components are green

Figure 14 Summary and status of all features installed

The following is the summary after the installation, showing all the pre-requisites and additional software components that were needed. Note that even though we selected only 4 items, there are many additional supporting backend components that are installed.

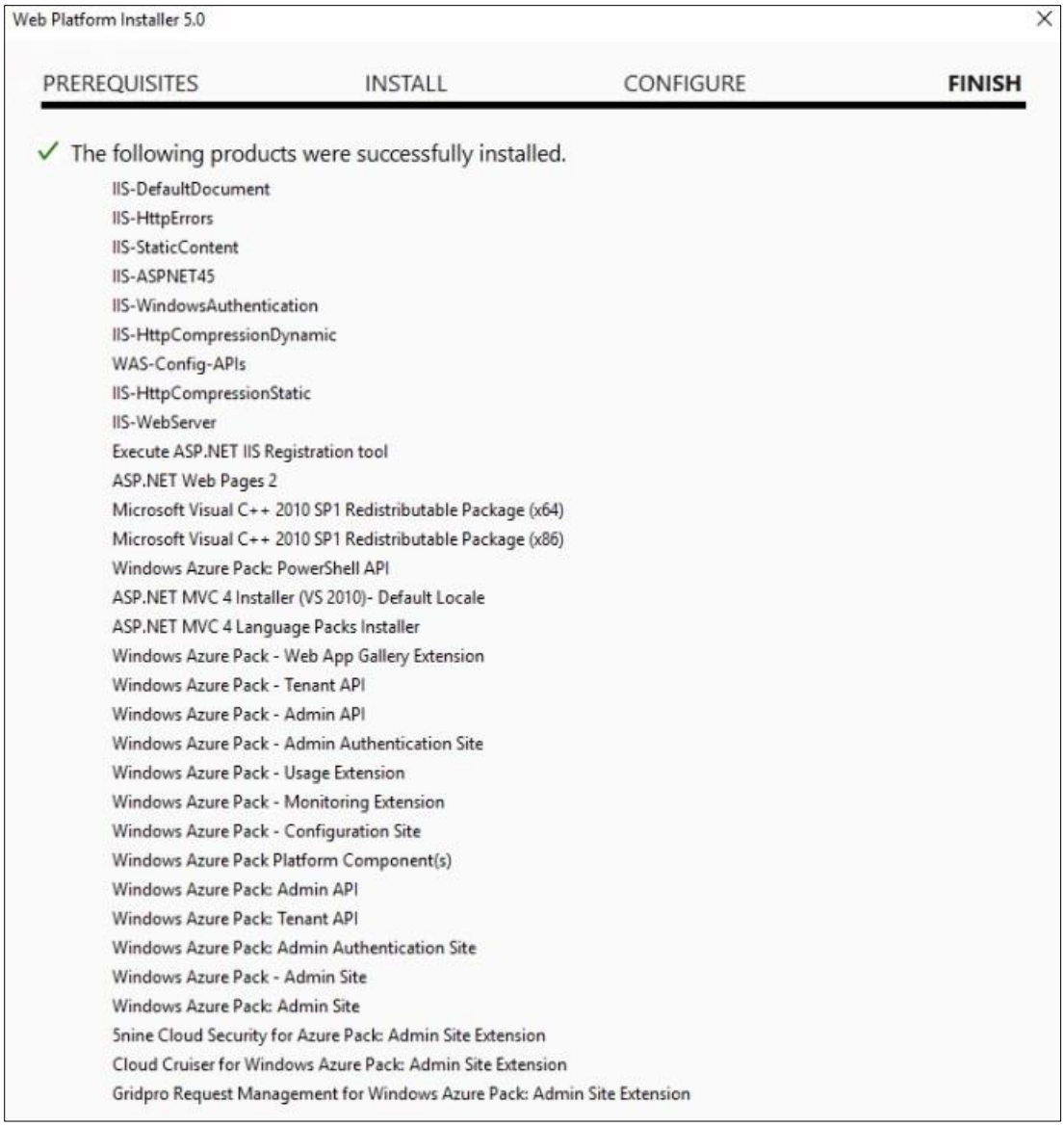

Figure 15 Summary of Azure Pack and all prerequisite and supporting products installed

Install Azure Pack Tenant Portal

Follow the steps below to install the Azure Pack tenant portal on the tenant VM. The steps and screens for installing the tenant portal components are the same as for installing the admin portal, except for the list of components that is selected. Thus, the full set of screen shots are not duplicated in this section.

1. Install the Web Platform Installer on the tenant VM.
2. Launch the Web Platform Installer on the Azure Pack tenant VM.
3. Select **Products** at the top, then **Windows Azure** from the left pane.

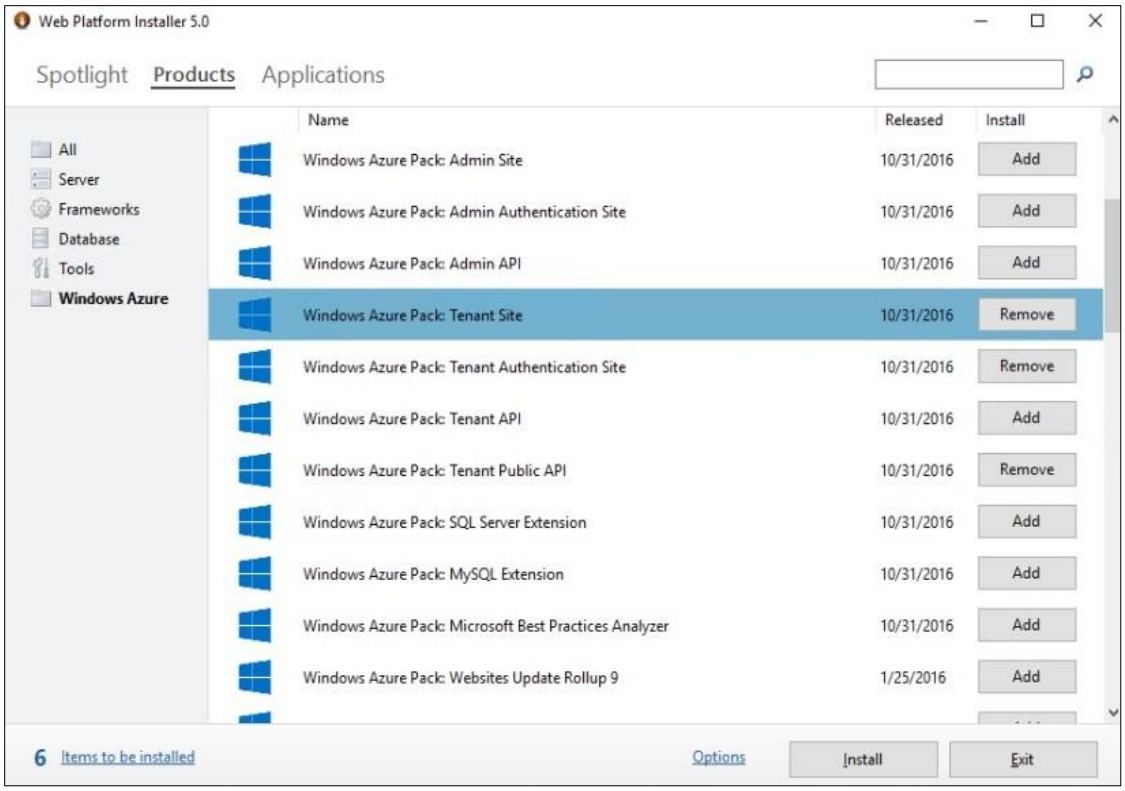

Figure 16 List of Azure Pack products to be installed

4. From the Products list, select the following 3 components as shown above by clicking **Add**:

   - Install **Windows Azure Pack Tenant Site** management portal
   - Install **Windows Azure Pack Tenant Authentication Site**
   - Install **Windows Azure Pack Tenant Public API**

5. Click Install to proceed.
6. Follow the same process as the prior admin portal installation.
   When it completes, the following summary of installed components is shown.

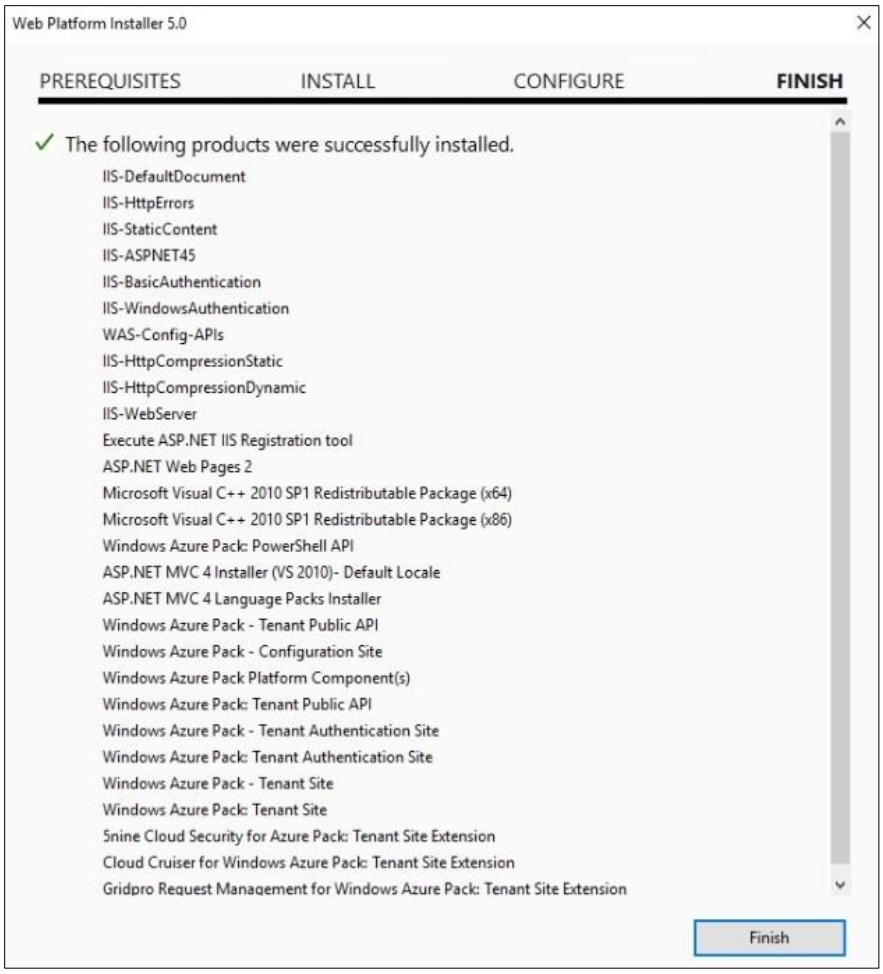

Figure 17 List of all Azure Pack and prerequisite products installed

Azure Pack post install tasks

After the admin and tenant portals are successfully installed, complete the following steps to ensure the systems are ready for integration with System Center VMM.

1. Check Windows update for important updates to the Azure components. Azure Pack was initially released around the Windows 2012 timeframe. Since then, there have been several important update rollups that provide additional stability and integration with Windows 2016 and System Center 2016 products.

2. Verify both the Azure tenant and admin portal web sites load without any errors. You can access the sites from the admin and tenant portal servers via the start menu -> Management **Service** -> **Windows Azure Pack Administration Site** or **The Windows Azure Pack Tenant site.**

3. Validate the installation with Azure Pack Configuration Analyzer. The download and instructions can be found at the following Microsoft site: https://technet.microsoft.com/en-us/library/dn469327.aspx

   Note: The Analyzer will mention some services should be distributed more for redundancy: these warnings can be ignored as we are purposely trying to consolidate roles for smaller deployments. The combinations outlined here are derived from Microsoft's deployment guidance for a minimal distributed install. The main purpose of running the analyzer is to discover any major configuration issues and correct them before proceeding.

Configure the VMM fabric

The following VMM fabric configurations are foundational to support the VM clouds and infrastructure as a service (IaaS) that is managed by Azure Pack. Several of these steps assume the remote edge server is online; thus, the section on Edge server deployment needs to be followed first. Be aware that many of the configurations in this section are site specific. As a result, each tenant remote site needs to have individual objects that control how that site is managed by VMM. These include:

- Host sub-groups
- Sub-clouds
- VMM agent, library and share
- Logical networks
- IP pools
- Local storage for VM files
- Hardware profiles
- VM templates

1. Create a VMM **run as account** and assign to VMM administrator role. In the VMM console, select **Settings -> Run As Accounts**.

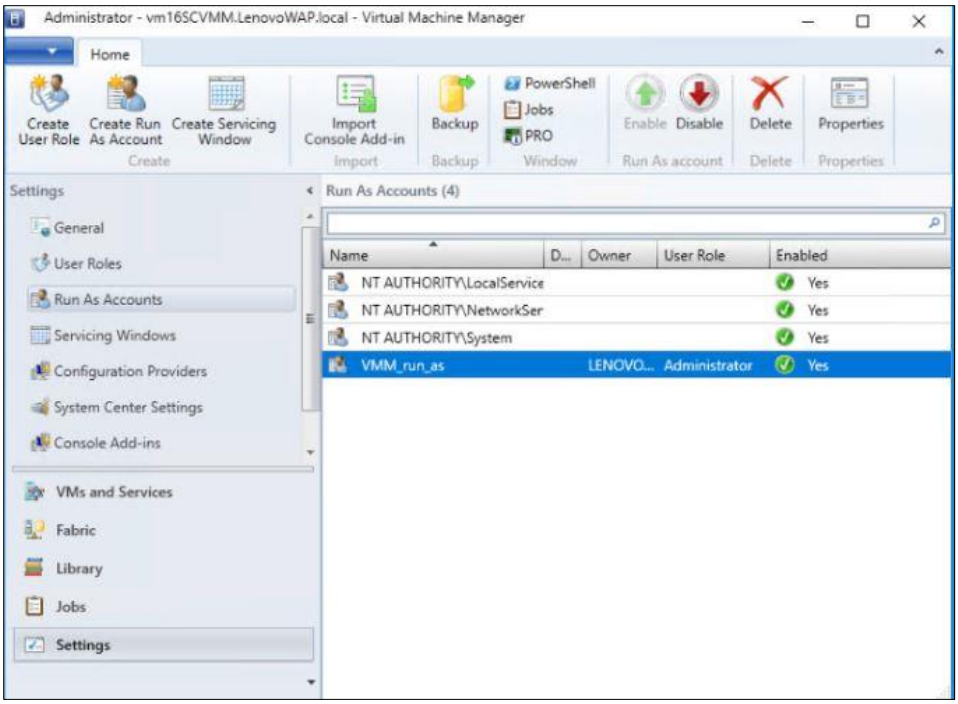

Figure 18 Creating Run As Accounts in VMM

2. Create a **Host Group** representing the tenant in the Fabric workspace of VMM, under Servers in the left pane. Then create sub-groups for each remote site.

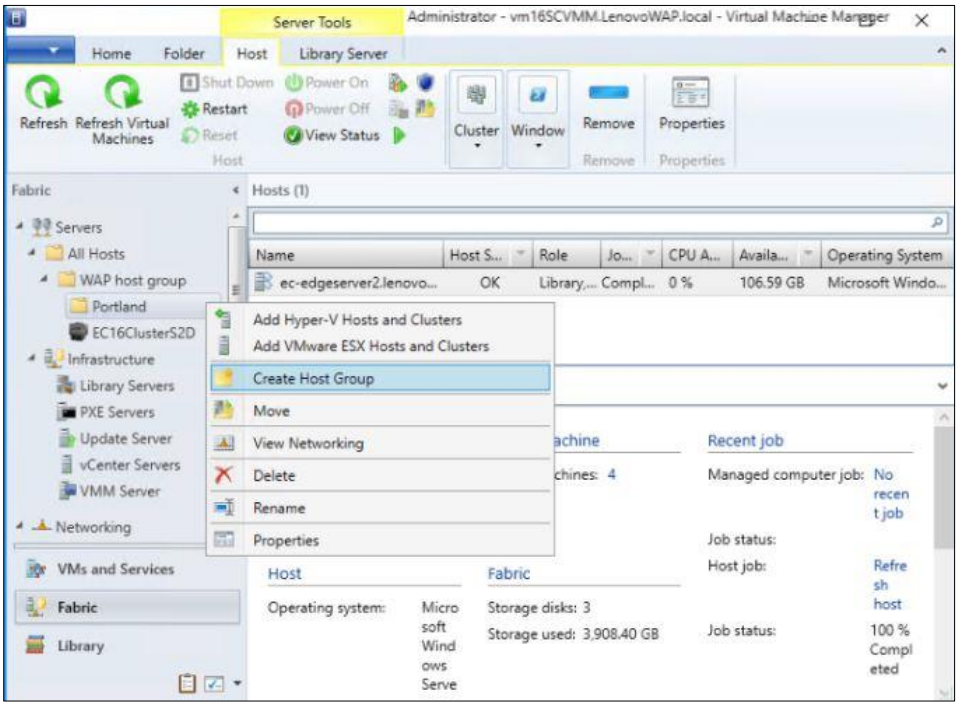

Figure 19 Creating a host group or sub-groups in VMM Fabric view

Note: Host groups are later mapped to VM Clouds. Each tenant must be grouped in their own Host groups, with sub groups for each remote site. These are used for directing site VM deployments

3. Add the remote host(s) to the sub-group and set the default VM storage path during the Add Host wizard process.

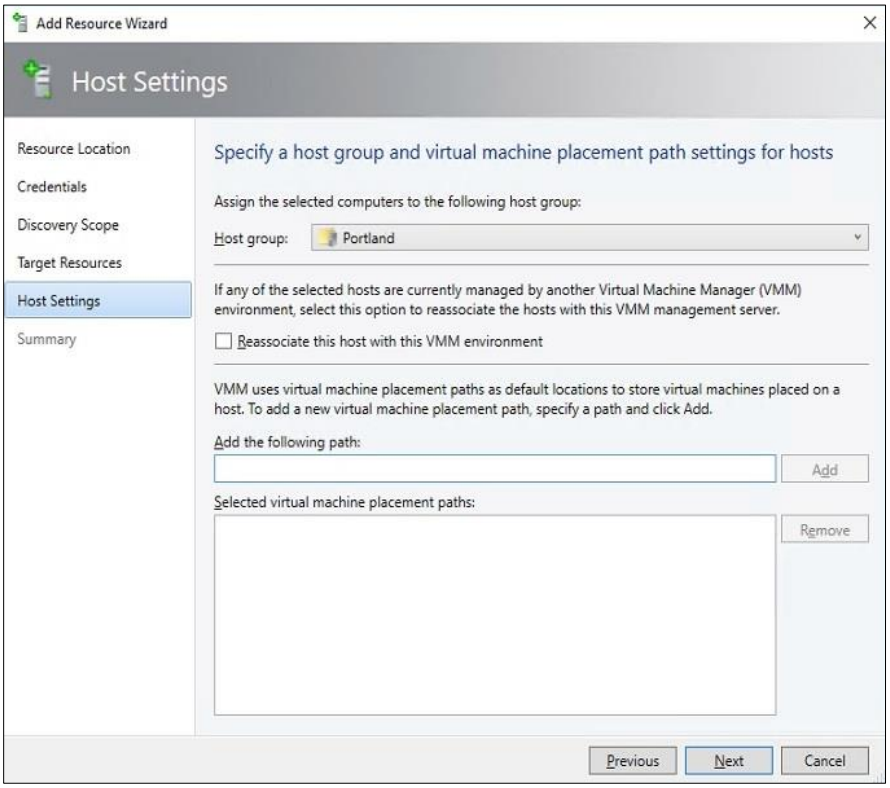

Figure 20 Specifying default location of deployed VMs when adding them to the sub-group

4. Configure a VMM library server for each remote site. This is usually the edge server itself, so it does not need to be a dedicated VM. Before proceeding, create a share on the remote server. Then from the VMM Library work space, right click **Library Servers**, and select **Add Library Server**. VMM will remotely install the VMM agent on the server and map to the share.

5. Associate the **VMM library** with the host group, from the library server Properties page.

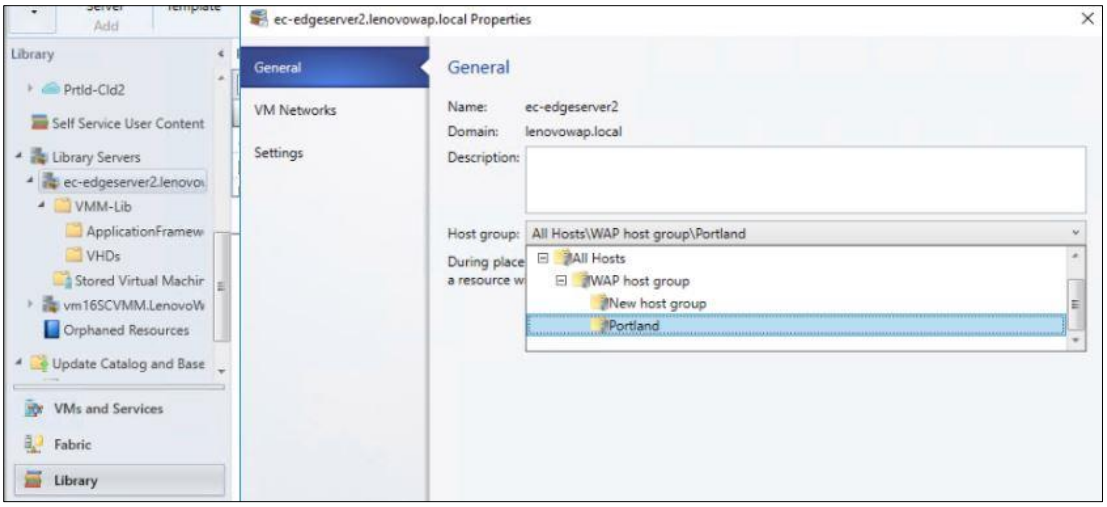

Figure 21 Mapping a remote site's VMM library server to a Host Group

6. After adding Hyper-V hosts, VMM will add a logical and VM network based on the virtual switch it discovers on the host(s) and will name it after the virtual switch name on the host. You should ensure that the created network is associated with the correct host group and cloud. This automatic network creation can also be turned off in VMM settings. Some administrators find it useful to identify which networks are associated with which each host.

7. Create any additional **logical networks** and corresponding **VM networks** that map to subnets and remote sites. During the network creation, select the **One connected network** option, and create a **network site**. Each network site should be a separate subnet.

   Note: For the test configuration, we did not utilize Hyper-V VLANs. When creating a network site within the logical network wizard, **leave the VLAN number set to 0,** which disables VLAN use.

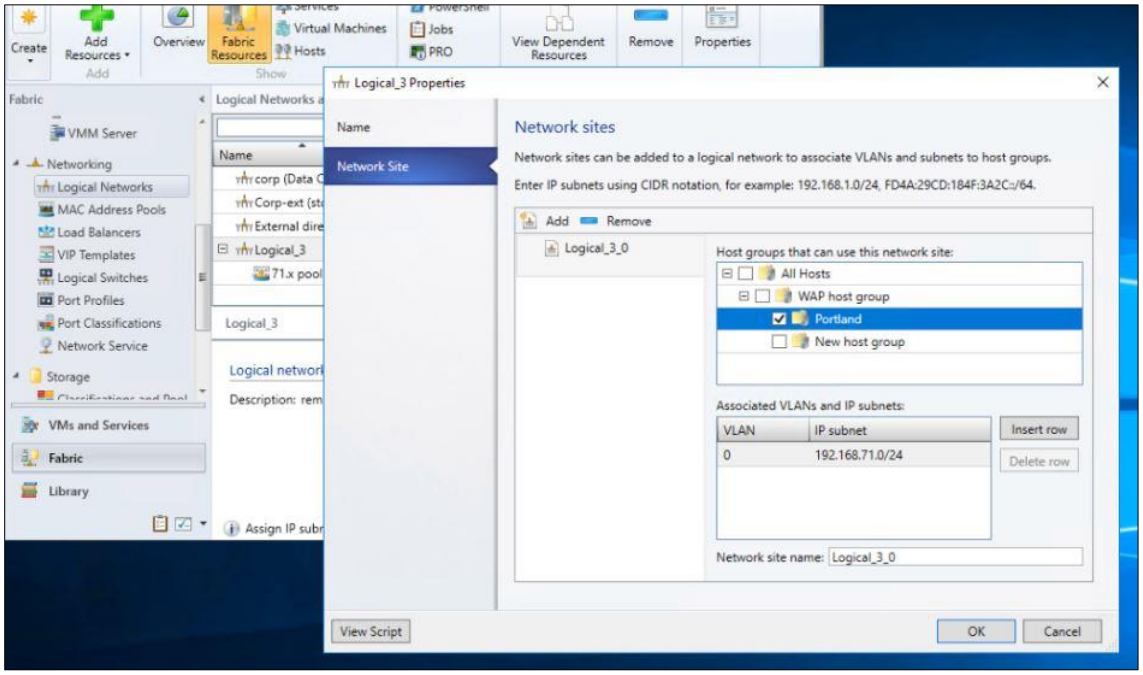

Figure 22 Create a new logical network and assign subnet

8. Create static IP pools for each VM network /subnet. Right click on the logical network and select **Create IP Pool.** These will be used by the VM deployment templates for IP assignment at remote sites.

9. Logical networks for each site need to be assigned within VMM to several resources for full connectivity within the solution. Check the network sections of each of the following, and assign the correct logical network to it:
    a. From the Library workspace, assign it at the VMM library server for the site.

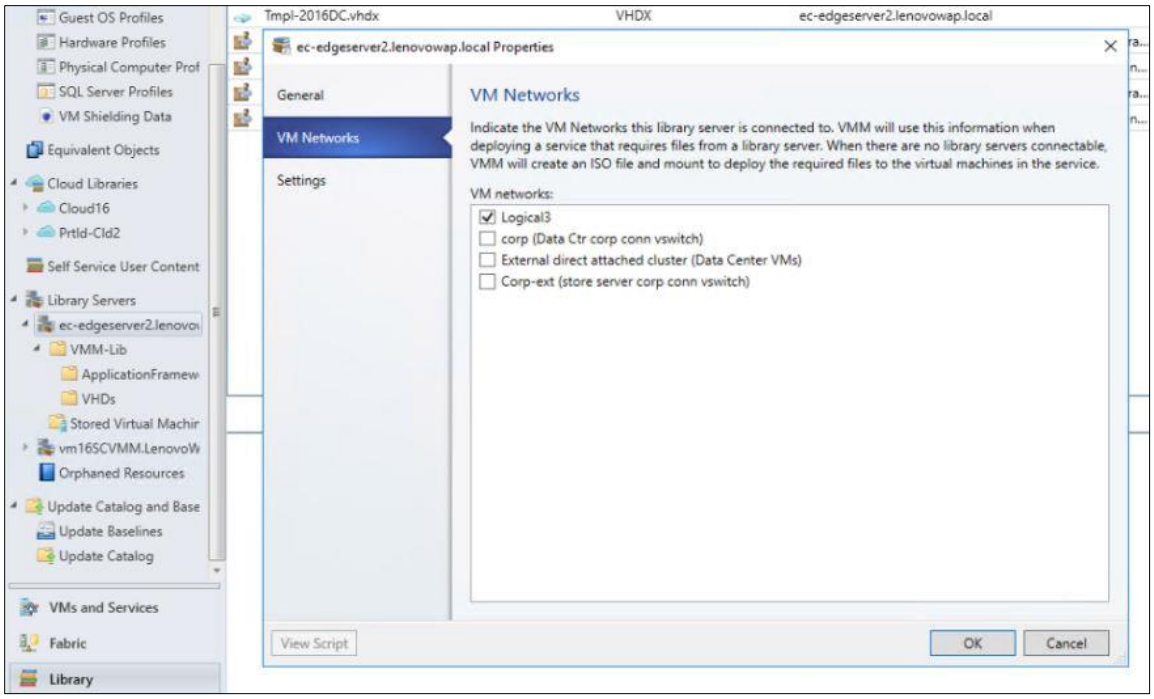

Figure 23 Assign logical network to site library server

b. From the Fabric workspace, assign it at the host server, in the site host group. Right click the host server, select **Properties** -> **Hardware** -> **Network Adapters** and click on the logical network section for the physical NIC being used at the site for the virtual switch being used by the VMs. Check the box for the site's network/subnet.

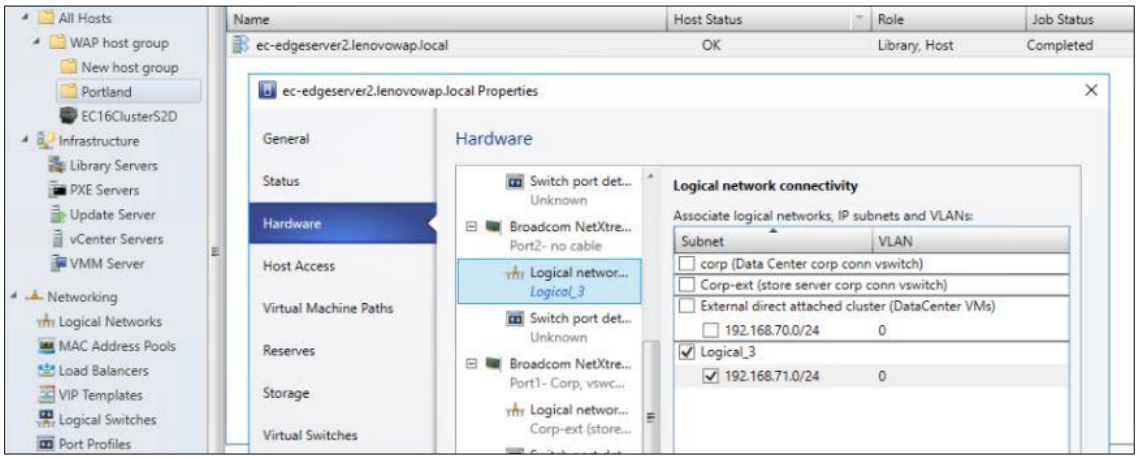

Figure 24 Assign virtual network connections for the Hyper-V host

c. From the VMs and Services workspace, Clouds, open properties on the cloud for the site. Go to **Logical Networks** and check the box for the correct network.

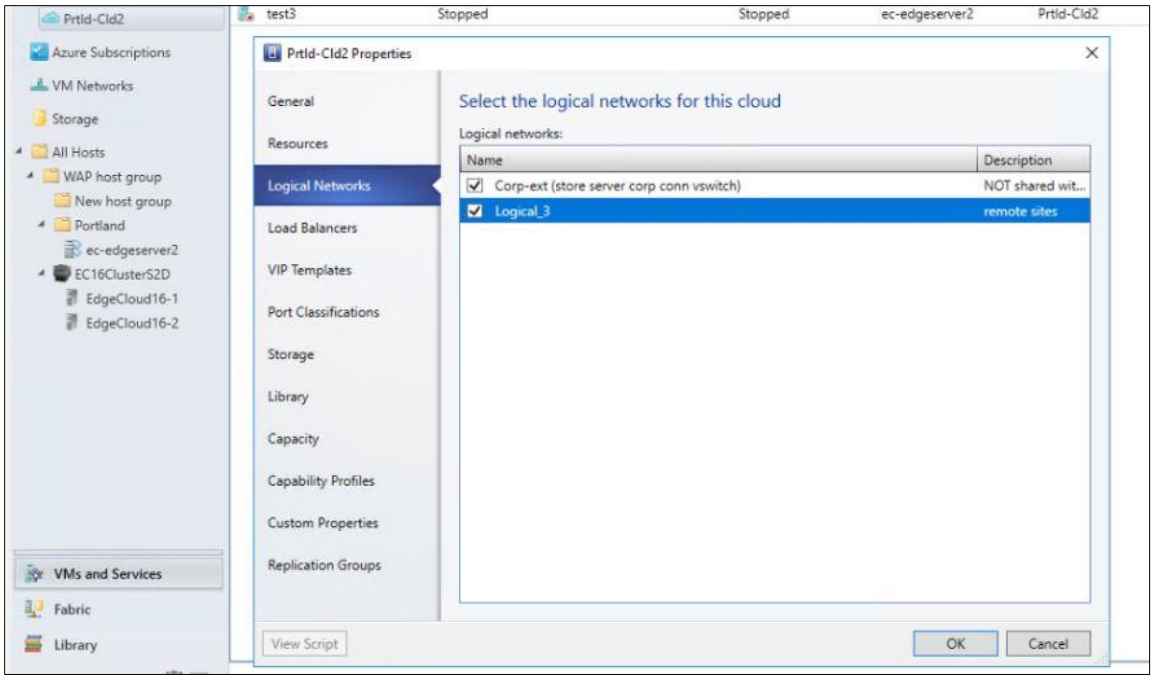

Figure 25 Assigning logical networks to the VM Clouds representing remote sites

10. Add storage capacity to VMM. If you are using Windows Storage Spaces or Spaces Direct, use the **File share option.** Otherwise, configure a supported SAN device. Note that this storage is for VMs that are hosted at the data center, either for infrastructure use or hosting customer application VMs. VMM does not control storage at the remote site, other than specifying where the VM files are stored and the location of the VMM library share.

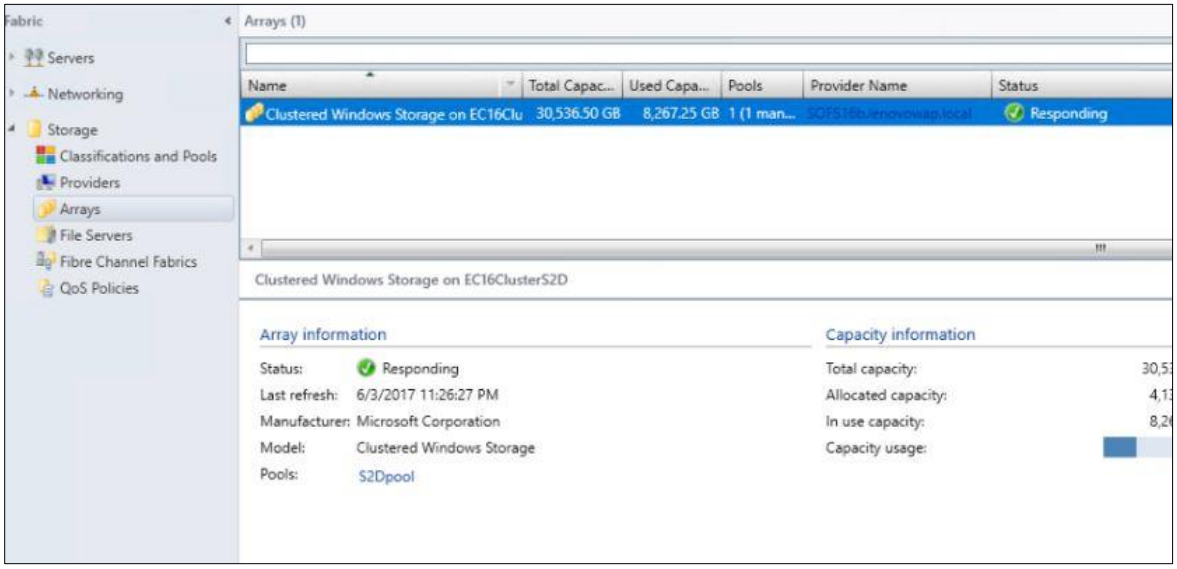

Figure 26 View of configured VMM storage arrays

The example above shows what was used for the test configuration, which was a Scale-out File Server (SOFS) setup on the existing Storage Spaces Direct cluster. The following PowerShell command creates the file server on the existing cluster storage:

```
New-StorageFileServer -StorageSubSystemName clustername.your.com -
FriendlyName SOFS1 -HostName SOFS1 -Protocols SMB
```

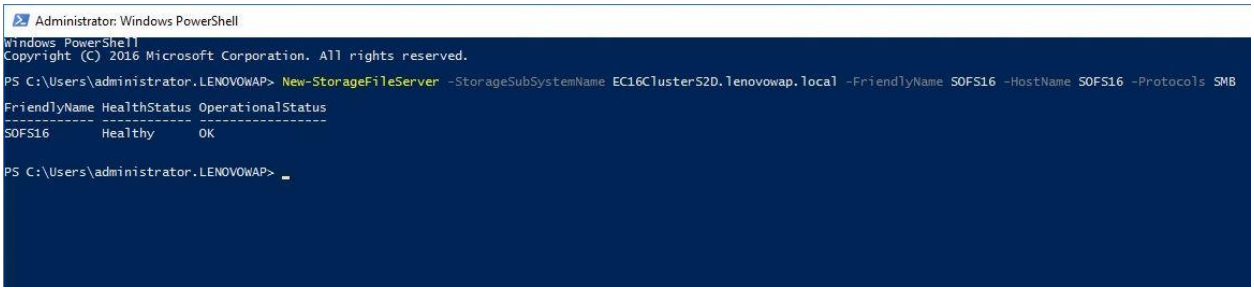

Figure 27 PowerShell command to create clustered file server role for VMM storage

After the above command completes, create the file share hosted on an available Cluster Shared Volume (CSV).

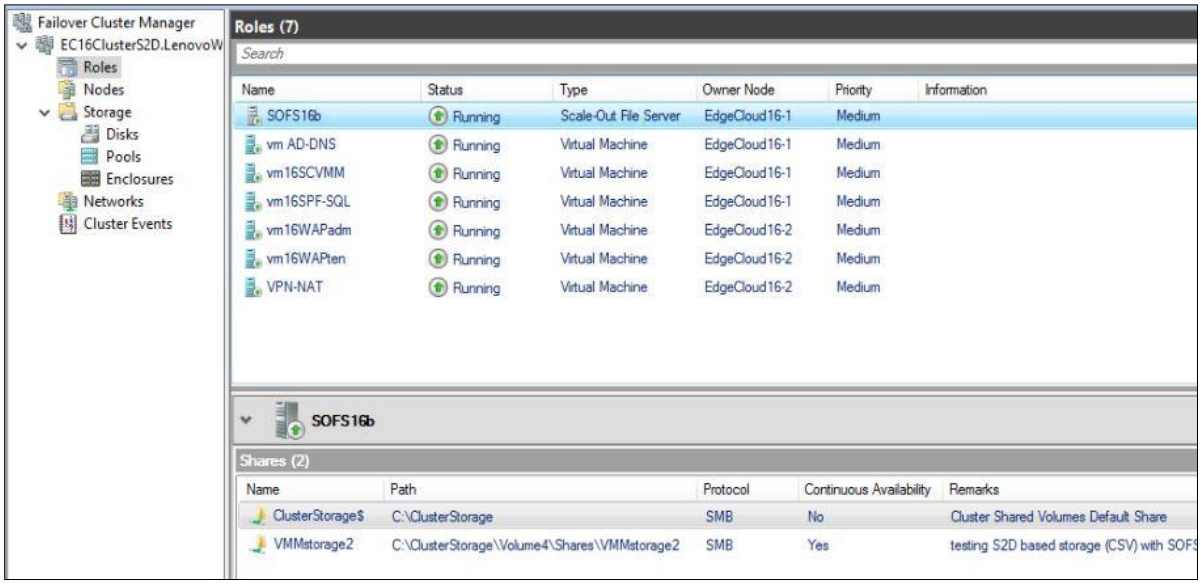

Figure 28 View of SMB file shares added to the clustered file server role

11. Copy one or more sysprepped VHD files to the VMM library, by using the **Import Physical Resource** option, shown in figure 29. These are OS images which will be used by the VMM templates. Each site will only need to have the VHD files copied out to its VMM library share

once, after which VMs are deployed using the local VHD image file. This saves on network utilization and makes the VM deployment faster.

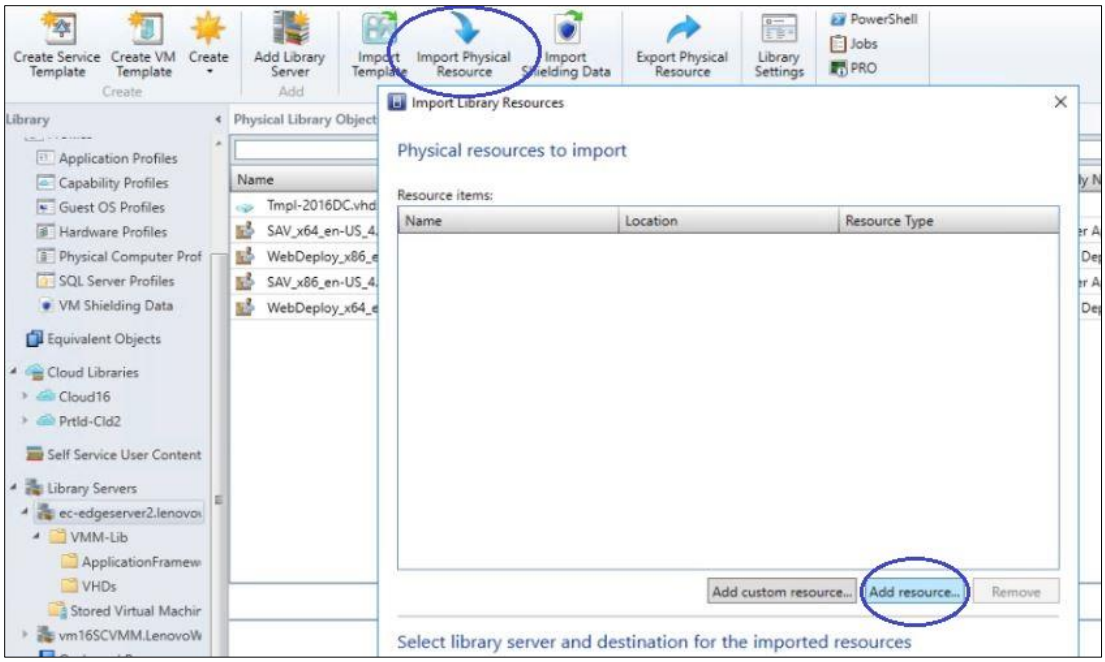

Figure 29 Adding VHDX OS image files to the VMM library server

12. Create a new cloud from the VMM **VMs and Services** view. Right click **Clouds**, and select **Create Cloud**.

    Important: Keep in mind, a separate cloud is created for each tenant, which maps to the host group created previously for the tenant. The cloud topology maps exactly to the underlying host group topology. Each tenant remote site must be a sub-host group with a corresponding sub-cloud created. This is the method VMM uses to assign resources to specific locations, and the concept is especially critical for the correct deployment of VMs to the edge servers at remote sites.

    For the cloud creation wizard, follow the prompts to assign resources that were created earlier. During this task the host group is assigned to the cloud. The wizard then specifies resources from the host group such as logical networks, storage, library server, and capacity limits. Azure Pack will use all the resources in this cloud configuration to present resources to tenants.

    Important: Do not enable any Capability Profiles in the clouds or host groups. These are not compatible or supported with Azure Pack.

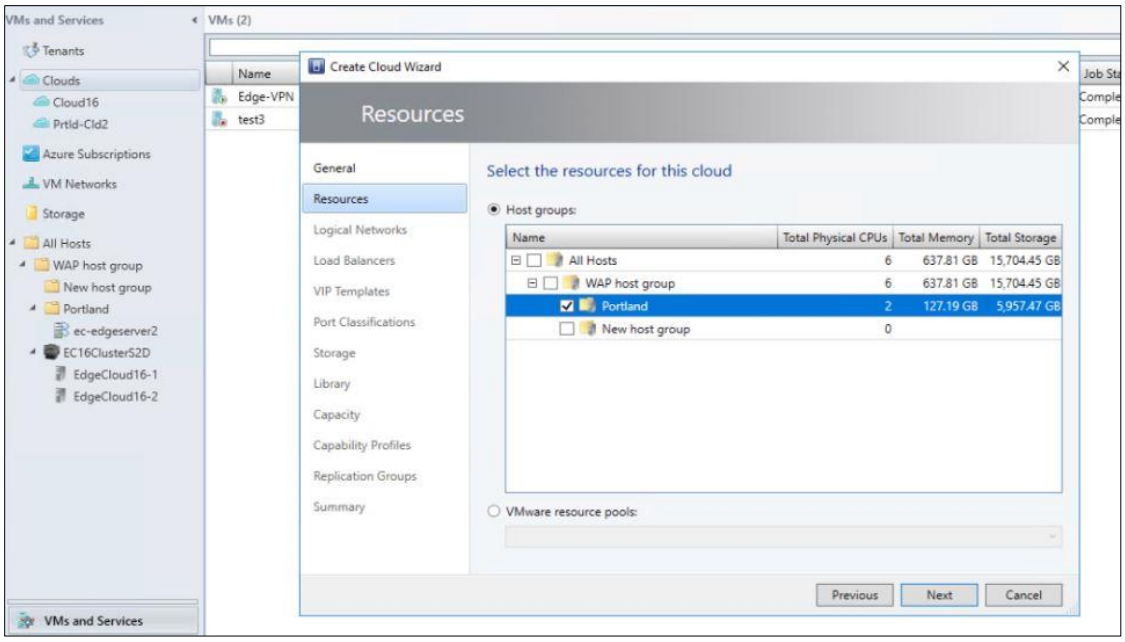

Figure 30 Assigning the host group to the cloud during the cloud creation wizard

13. Each remote site must have one or more hardware profiles created. These are required by Azure Pack plans, which are used to assign resources to tenants and deploy VMs. Create the Hardware Profile from the Library view, **Profiles** section. Right click **Hardware** and select **Create Hardware Profile,** and follow the wizard prompts. This is primarily used to pre-set sizing of compute, memory and network resources. Ensure the correct virtual network and IP pool is selected for the site, as shown in figure 31.

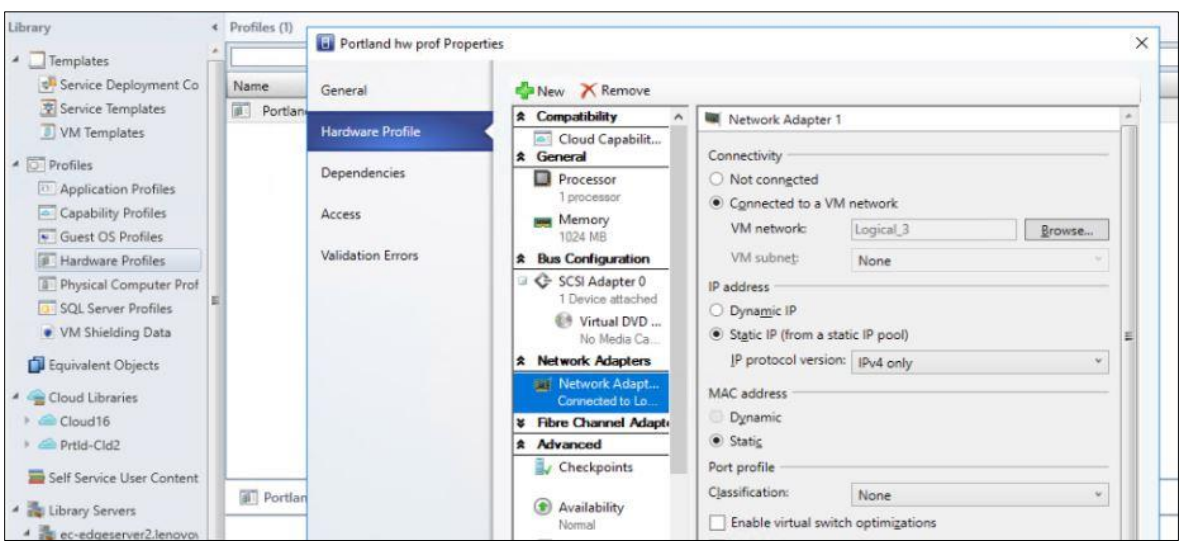

Figure 31 Setting compute, memory and network resources in the hardware profiles

14. Each remote site must also have one or more VM templates created. These are required by Azure Pack plans and are site specific. The templates specify OS settings, product ID, VMM library location of OS image, storage location of VM files, and pull information from the associated hardware profile created previously. Create a VM template from the VMM Library view, VM Templates. Right click **VM Templates,** and select **Create VM Template.**

    As shown in figure 32, the important template settings are the source VHDX OS image file, which should pull from the sites local VMM library share location, and not over the network from another server. Also, ensure the network section specifies the correct virtual network, which should already be correct if it is pulling from the right hardware profile for the site.

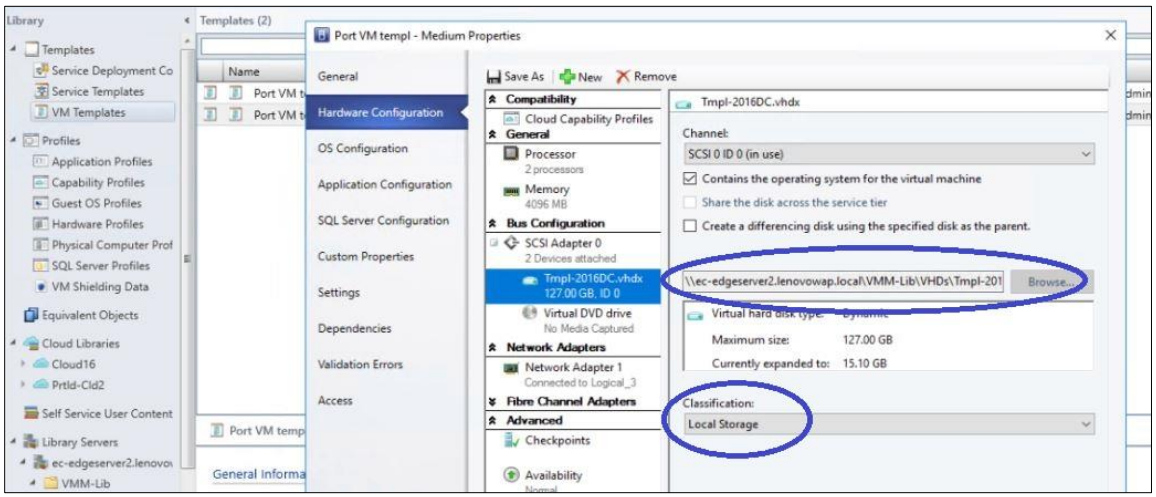

Figure 32 Configuring source VHDX file and VM file storage locations in the VM templates wizard

Important: As already mentioned, do not use any of the Capability Profiles in VMM such as ESX, XenServer, or Hyper-V. These are not compatible with Azure Pack and will break the VM deployments.

Note: To use the admin or tenant portal you must login using a Windows 8.1 or newer client machine.

Register SPF with Azure Pack

This section covers connecting SPF and VMM to the Azure Pack admin portal, which allows Azure Pack to communicate with VMM.

1. Logon to the Azure Pack admin VM, and launch the Azure Pack admin portal from the start menu -> Management **Service** -> **Windows Azure Pack Administration Site**.

2. After logging into the website, click on **VM Clouds** and select **Register System Center Service Provider Foundation.**

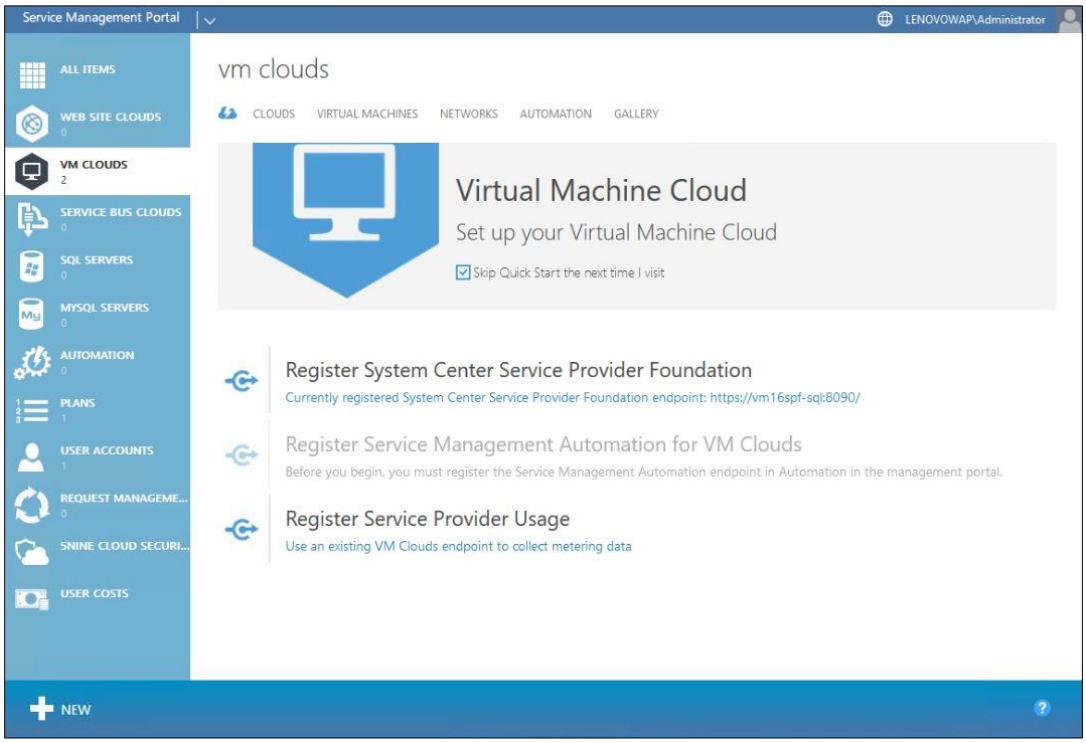

Figure 33 Initial configuration of Azure Pack, registering the Service Provider Foundation (SPF)

3. In the web form that opens, type the FQDN **URL of the SPF server** and port in this format: https://server.domain.com:8090 If the right format isn't used, it will not connect.

4. Enter the **User Name** in this format: Domain\user account. Note that this account **must** be the SPF admin account that was specified during SPF setup, and is the same domain level account that runs the four SPF web services on the SPF server.

5. Enter the **User account password** and click the **arrow** to continue.

6. Wait a few minutes, and then the status should show the registered SPF server.

Register VMM with Azure Pack

The next step is to register the VMM server with Azure Pack, so that it can see and manage cloud resources.

1. From the Azure Pack admin portal, click on **Clouds.**

2. It will state that no virtual machine cloud provider was found, this is normal because it has not been configured yet.

3. Click on **Use an existing virtual machine cloud provider to provision virtual machines.**

4. Enter the FQDN of the VMM server in this format: **VMMservername.domain.com.**

5. Click the **Register arrow** to register the VMM server.

6. After a few minutes, the VMM server should appear in the cloud list with a status of Ready.

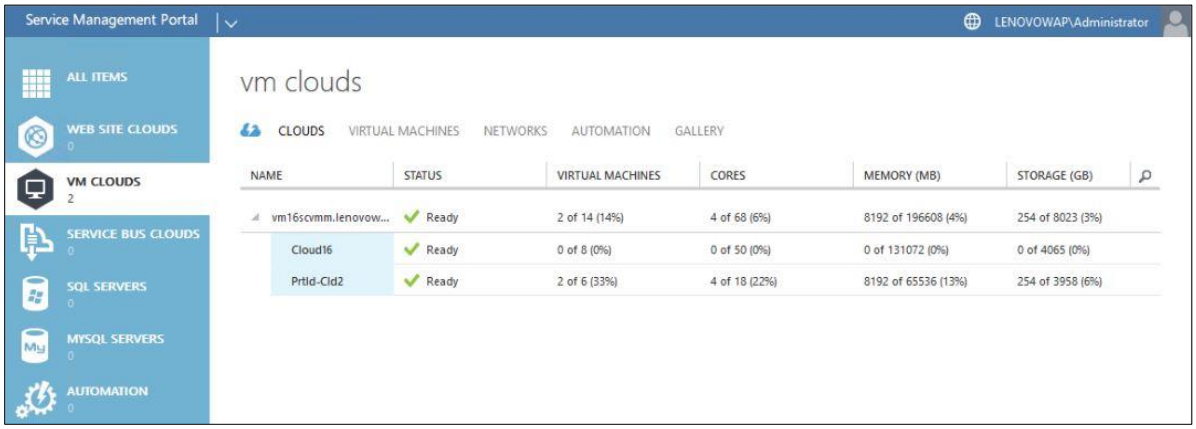

Figure 34 View of currently configured VM Clouds after registering the VMM server

Azure Pack plan creation

Before creating user accounts, one or more plans must be created. User accounts are assigned to plans, which controls what options and resources are available when the tenant administrator logs in to the tenant portal.

Important: Until the plans are made public, they are not available to tenants.

1. In the admin portal, Click **Plans** in the left pane, click **New +** at the lower left, then **Create Plan**.

2. Specify the name and what services to include, then click the **check mark** to finish.

3. After the plan creation finishes, click on it in the list. It will say that it's not configured, which is normal.

4. Click on the desired service to configure it.

5. Configure specifics in the plan, including which cloud it applies to, usage limits, networks, hardware profiles, VM templates, and any additional settings that apply to your environment. All of these options will be available in drop-down lists because they have been created within VMM already and are available for use. After all fields are completed, click **Save**.

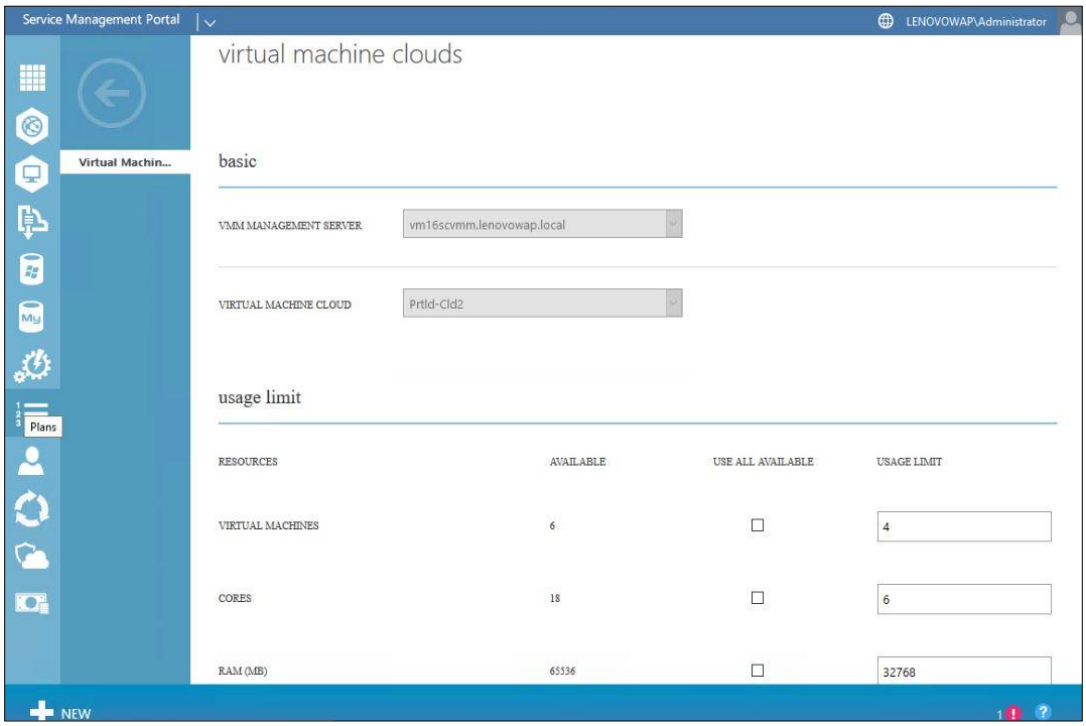

Figure 35 View of plan configuration in the Azure Pack admin portal

6. At the lower left on the task bar, make the plan public so it can be assigned to tenants.

To test the plan, proceed to the next section for account creation. Afterwards you can login to the tenant portal and verify the plan functions as expected.

Create user accounts

Tenant accounts are created in the Azure Pack admin portal. These are tenant administrator level accounts that will have rights and resources for managing their own Azure tenant environment and remote sites.

To create users:

1. Click on **User Account** in the left pane, then select **Quick Create**.
2. Fill in the **email account** and **password** fields.
3. Choose a plan from the available ones in the drop-down list.
4. Click **Create** to finish.

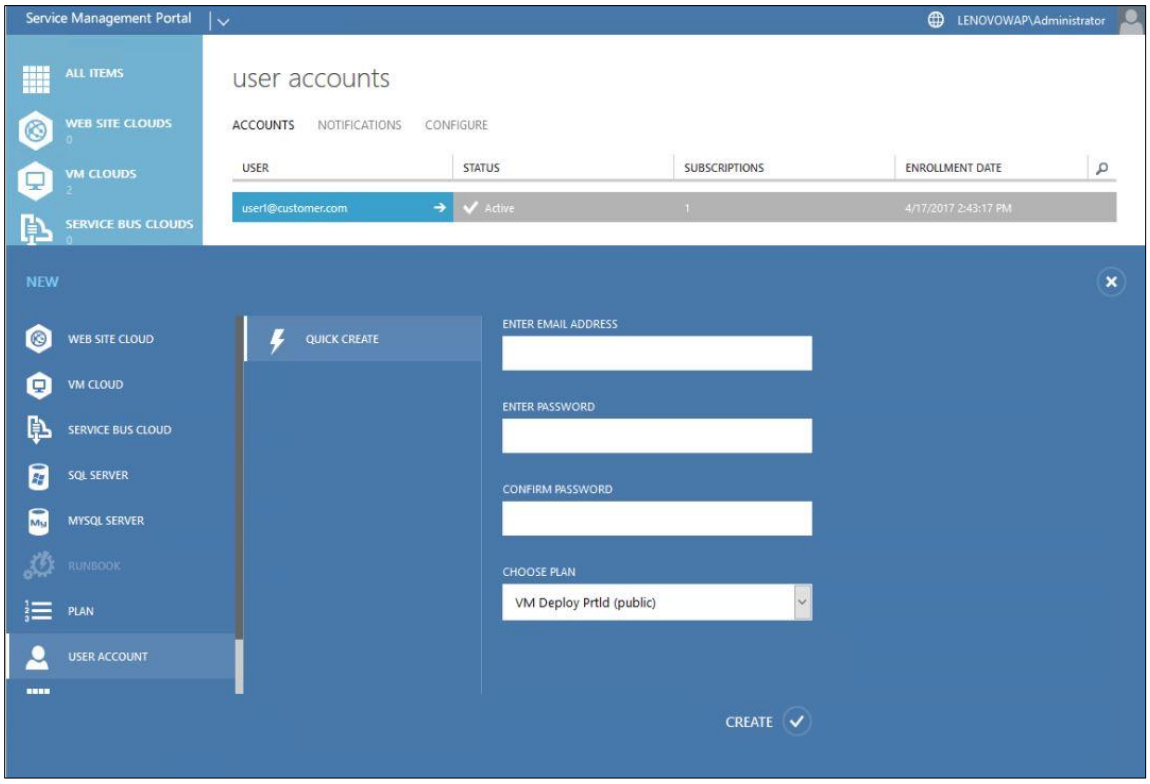

Figure 36 Creating user accounts in the Azure Pack admin portal

5. Go to the Azure Pack tenant server, and test the login. The portal link is on the start menu, under **Management Service** -> **Windows Azure Pack Tenant Site**
6. After logging in, verify the expected plan has been assigned and is available for use.

Identity Management

The included Azure Pack authentication methods are based on Windows authentication for the admin portal, and local asp.net accounts for the tenant portal. The main reason to use the built-in authentication is simplicity. Not all customers will have the infrastructure or expertise to support complicated authentication models. The authentication that is included with Azure Pack works well, and since the number of accounts will be limited to the IT personnel each tenant has, the authentication method doesn't need to be highly scalable.

Optionally more robust authentication models for Azure Pack in production environments include Active Directory Federation Services (ADFS) or Azure Active Directory. Both methods scale well and are ideal for high volume multi-tenant environments and web services. ADFS uses claims-based authentication with trusts created for each tenant. It can also be integrated with Office 365 accounts. The down side to these methods is that they are more complex to implement and administer.

Edge server deployment

The edge server uses several Windows Server roles and features to accomplish the goal of being outside the cloud but connected and managed by it. As a remote server, it lives on the edge of the Microsoft cloud, taking advantage of both on-premise private and Azure public cloud benefits.

Figure 37 Lenovo system x3650 M5 server

The edge server is a **Lenovo system x3650 M5**. Some of the key features of the x3650 M5 include:

- Designed for enterprise workloads with power, efficiency and reliability
- Flexible storage configurations for workload-optimized performance
- Up to 120TB of local storage for enterprise applications and data intensive workloads
- Simplified server management with Lenovo XClarity
- Built-in Lenovo Trusted Platform Assurance, and optional self-encrypting drives
- Intel Xeon E5-2600 v4 processors (up to 44 cores per server)
- 12Gbps RAID support—devices and infrastructure—up to four RAID adapters, up to eight front-mounted NVMe PCIe SSDs and up to four GPUs
- Smart energy-efficient features such as extended operating temperature, 80 PLUS® Titanium power supplies (up to 96 percent efficiency), active/standby power supply modes, dual fan zone design, and TruDDR4 Memory (up to 45 percent lower energy use over DDR3), and optional Lenovo XClarity Energy Manager
- Run more virtual machines and workloads with up to 22 percent more cores than previous generation

Detailed information on the x3650 M5 can be found here:

https://lenovopress.com/lp0068-lenovo-system-x3650-m5-machine-type-8871

Configuring the edge server

This section covers the installation of each edge server component and provides guidance on configuration. A basic level of Windows server setup and administration is assumed, and many of the steps below are standard server setup tasks. If the action is a well-known Windows procedure, then detailed steps are not included.

Below is a summary of components and services to configure on the edge server. Each one is a separate section, and should be followed in the order presented unless otherwise noted.

1. Base OS configuration
2. Hyper-V and VM setup
3. VPN and domain services
4. VMM configurations
5. Azure Backup
6. Windows firewall

Base OS configuration

1. Install the OS. The solution is based on Windows Server 2016, and the Data Center edition media is included with the edge server. Use the two drives at the back of the x3650 M5 for the mirrored OS volume. This frees up the remaining drives for data storage.
2. Set IP addresses on 2 of the NICs. One will be internet facing, the other a private network.
3. Turn off the Windows Firewall as we will be using a separate firewall VM, which is covered later.
4. Enable remote desktop and patch the OS.
5. Configure the local storage pool, this is using the server's internal disks and Windows Storage Spaces. Provision enough large RAID protected volumes to support VM files storage.

Hyper-V and VM setup

1. Add the Hyper-V role
2. Configure Hyper-V virtual switches
    - Configure an external mode virtual switch using the internet facing NIC, and un-check **Allow management operating system to share this network adapter**. This should result in a dedicated and isolated connection into the firewall VM. Keep in mind it will no longer show up in Ipconfig, Network adapter list or be visible in general to the host OS. It can be un-hidden later if configuration changes are needed, by temporarily sharing it with the OS.

- Configure a second external mode virtual switch using another NIC port, for VM internal use as a private network.
  Note: This second virtual switch uses a physical NIC port, but is not cabled.

3. Create a network share to be used by VMM as a Library Server later. Copy one or more sysprepped OS images (VHDX files) to this share.
4. Provision 2 VMs, one will be for Active Directory, the other as a VPN-NAT server. Use the VHDX file copied to the server to create the VMs.
5. Connect the VPN VM to both virtual switches by adding 2 virtual NICs to the VM and setting IP addresses. This will prepare the VM to function as a router for VPN and NAT purposes.
6. Patch the VPN VM, enable remote desktop, turn off the Windows firewall for now.

VPN and Domain services

Before continuing with this section, the VPN connections to the data center need to be configured, which could not be done until the base OS and networking was setup on the edge server.

1. Install the VPN role on the VPN VM and configure a VPN connection to the data center VPN server. Follow the **Site to site VPN configuration** on page 52, then return here to continue.
2. **After there is a VPN connection to the data center**, join the edge server to the domain.
3. On the AD VM, set the private IP address and the default gateway to the internal IP of the VPN VM. The AD VM should now have access to both the internet and the data center.
4. Patch the AD VM, enable remote desktop and turn off the Windows firewall.
5. Join the AD VM to the domain.
6. Install Active Directory services on the AD VM.
   - Promote the AD VM to a domain controller.
   - Be careful to select the Read-Only domain controller check box. This is a standard best practice for remote servers.
   - In the VM properties, configure the VM to save at shut down, and auto-start. This will ensure the VM starts whenever the server restarts, providing local authentication.

VMM configurations

1. From the VMM console, add the edge server to the corresponding Host sub-group for the site. VMM will automatically install the VMM agent on the server at this point.
2. Configure site logical and virtual networks in VMM. Refer to the earlier section on Configuring the VMM fabric for more details.
3. Configure a VMM sub-cloud for the site, from the VMM console.
4. Add the VMM server's machine account (computer account) to the Local Admin group on the edge server to provide the needed VMM library permissions.
5. Add the edge server as a VMM library server, from the VMM console Library view.

The edge server will have the VMM agent installed on it, which enables the VMM server to deploy and manage VMs remotely, while using the local VMM library for OS images or any other files needed. This

reduces the network bandwidth usage for VM deployment to the initial copying of the files to the VMM library.

Azure Backup

Azure Backup is a cloud integrated data protection solution for backing up on-premises data to Microsoft Azure. The configuration includes creating a backup vault to store the data in Azure, setting up credentials, installing the agent, and scheduling the backups.

Note: Perform all the following steps directly from the edge server, or the registration and authentication process will fail.

1. Login to the Azure portal at https://portal.microsoft.com
2. A subscription is required to setup a backup vault within Azure and download the agent software. Trial versions can be used temporarily for testing out Azure features.
3. In the Azure portal, type "recovery" in the search box at the top, and select **Recovery Services vaults**.

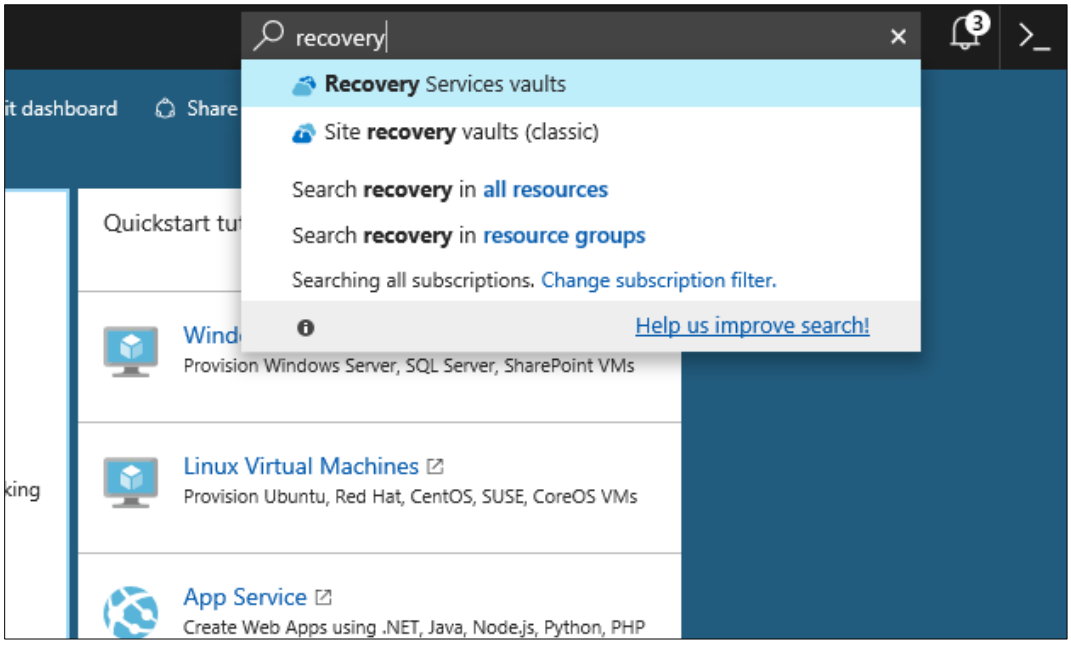

Figure 38 Opening Recovery Services Vaults in Azure

4. On the Recovery Services vaults page, click on **Create Recovery Services vaults**.
5. Give the vault a name and select an existing or create a new resource group, and click **Create.** The vault is created within a couple minutes, if it doesn't appear then click **Refresh**.

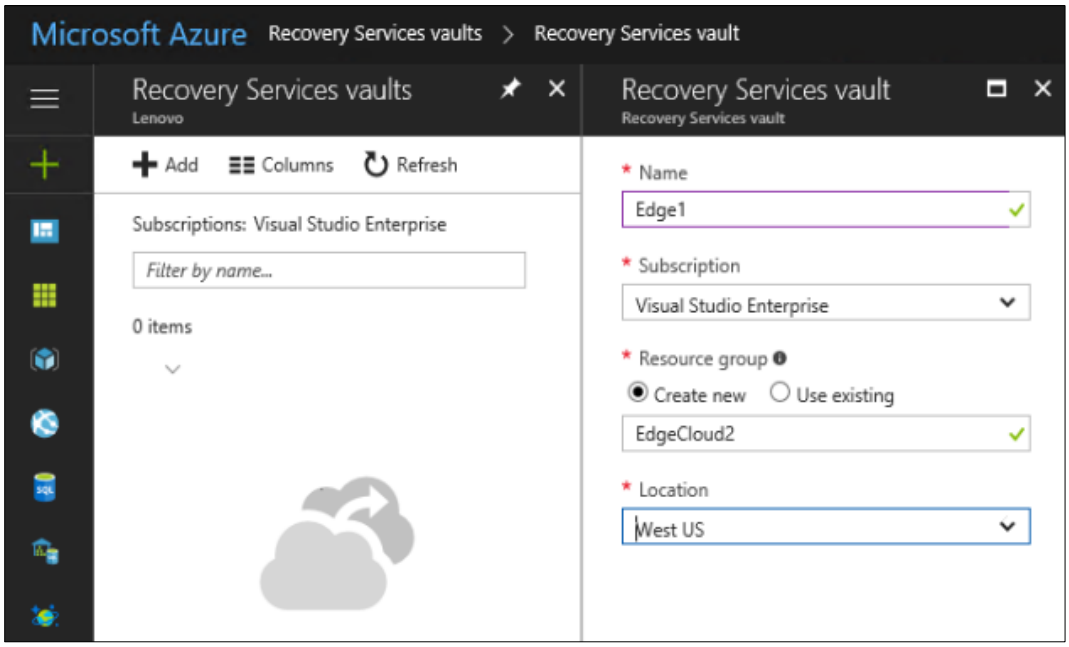

Figure 39 Creating a Recovery Services vault in Azure

6. Click on the vault just created. Under **Getting Started** in the left pane, click **Backup**
7. The Backup goal page opens. Enter **On-premises** and **Files and folders,** click **OK**

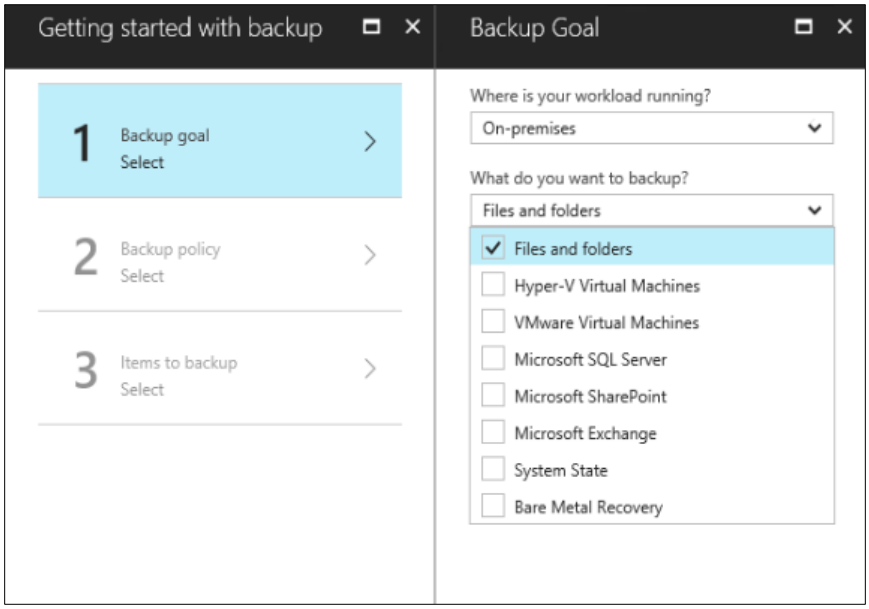

Figure 40 Setting options in the Backup Goal wizard

8. Azure provides a list of steps to follow, to configure your environment to meet the backup goals specified.
   Note: These steps are being done on the edge server, so the download is local, and the credentials download applies only to the computer connected to the Azure portal website.

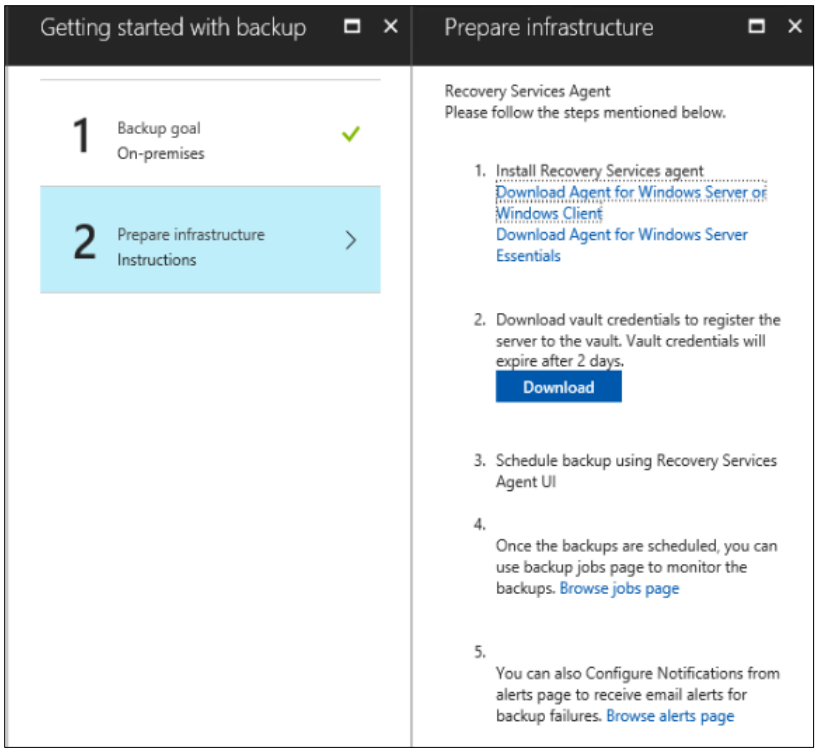

Figure 41 Guidance from the Azure wizard on preparing the backup environment

9. Follow the guidance provided above by Azure.
    a. Click on the link to download the Azure Backup agent.
    b. Install it on the edge server.
    c. Select the defaults on the agent install wizard.
    d. Leave the agent installer final screen open when it completes. Do not click on Proceed to Registration yet.
10. Download the vault credentials. The credentials provide 2 days to complete registration.
11. Go back to the agent installer final screen, and click on **Proceed to Registration.**
12. The registration wizard will prompt for the location of the downloaded credentials.
13. The registration information is extracted and displayed, as shown in figure 41.
14. Click **Next** to continue.

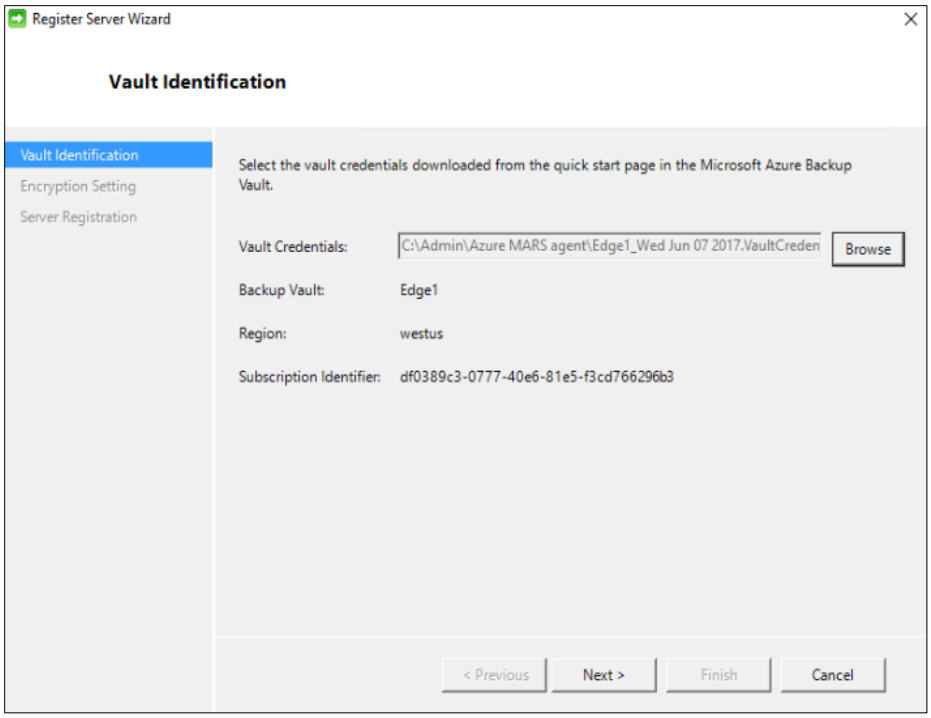

Figure 42 Register Server Wizard successfully loaded registration details

15. Enter the encryption pass phrase and the location to save it.

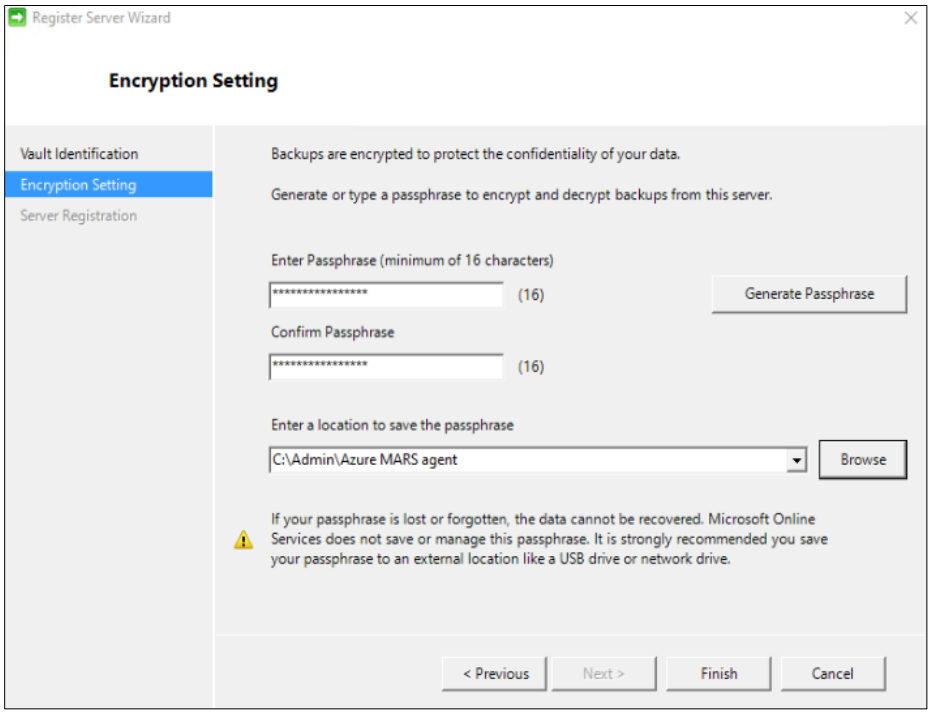

Figure 43 Setting the backup passphrase and save location

16. Click **Finish** to register the server.

17. After a few minutes, the server shows as successfully registered.

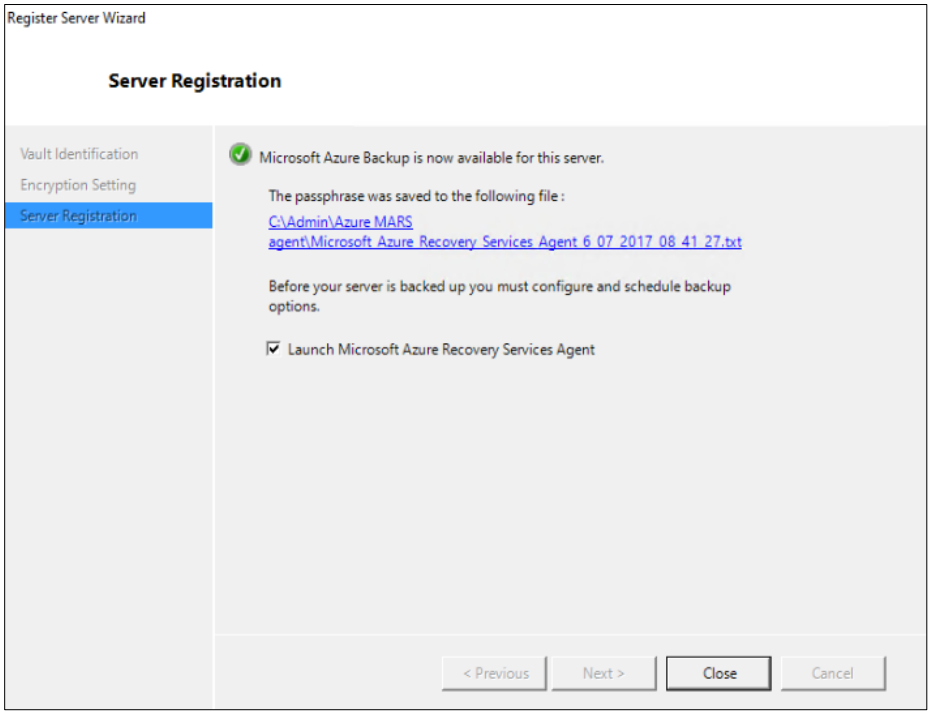

Figure 44 Successfully registered server with Azure Backup

18. Launch Azure Backup from the Start menu.

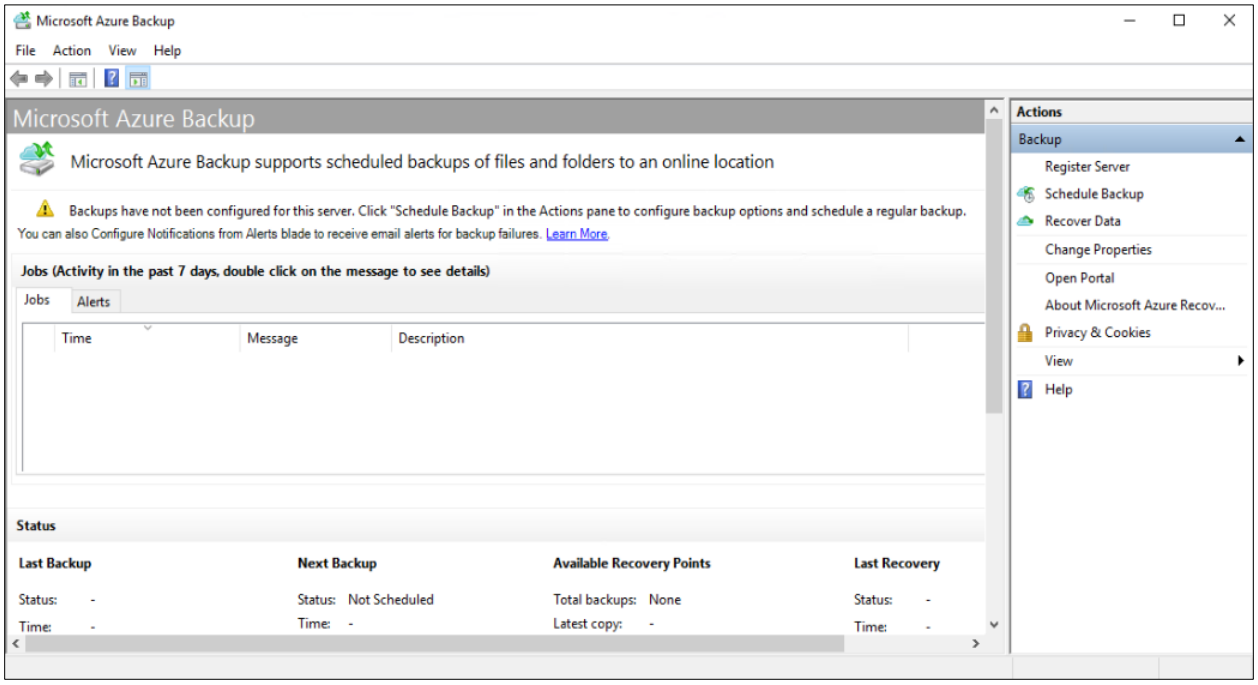

Figure 45 Azure Backup console

19. In the backup console, from the right pane, select **Schedule Backup** to launch the wizard.
20. Follow the Schedule wizard to select files for backup, the schedule, retention settings, and online or offline type.
21. After the wizard completes, click on **Backup Now** from the right pane of the backup console to test the backups.

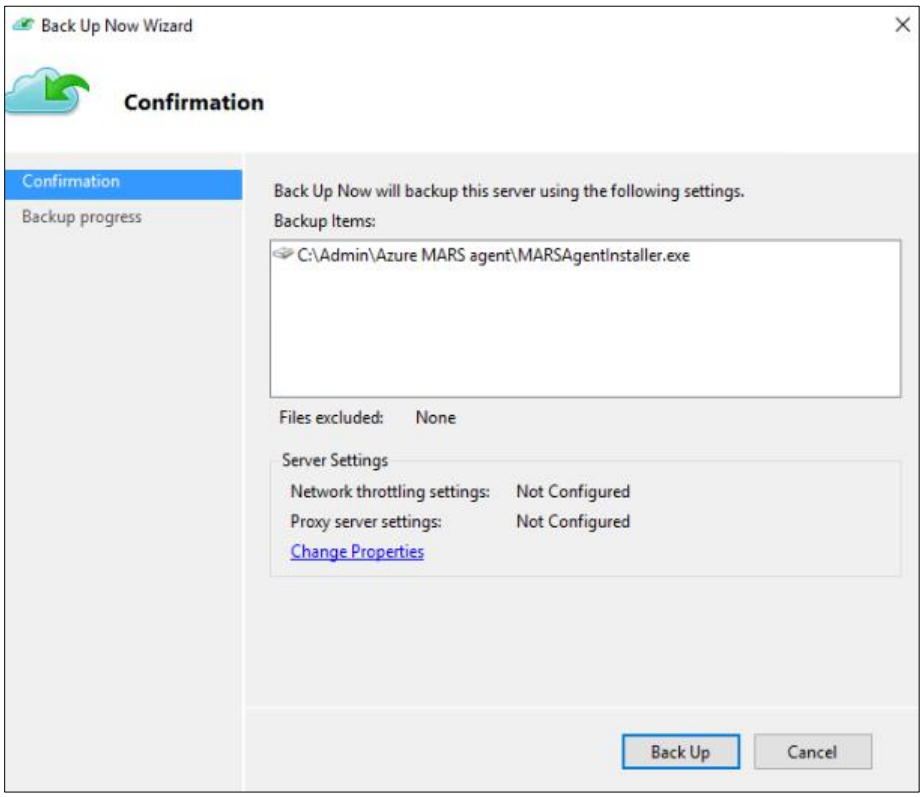

Figure 46 Confirmation of backup job

22. After the backup finishes, the job and status is logged in the backup console. The status of the backups can also be viewed within the Azure Portal.

Be aware that the first backup will take longer, since it is a full backup of the data. Subsequent backups will be incremental, and finish much faster.

Windows Firewall

The firewall solution is the Windows 2016 Firewall with Advanced Security. We are running it on a dedicated VM functioning as a combined VPN / NAT / Firewall server. All traffic, for both the VMs and the host OS should go through this VM. All VMs and the edge server host OS are using the internal IP of the VPN VM as their default gateway, to direct traffic through it.

The physical NIC from the Internet is mapped directly to the external mode virtual switch, and the connection is not shared with the OS. This isolates internet traffic and sends it directly to the firewall VM. With this approach, there is only one firewall to manage.

The Windows firewall automatically enables rules for VPN and NAT when those services are installed to allow their traffic through. However, the steps below should be done to confirm the rules are set, and that the correct interface is protected.

Follow the steps below to check the firewall configuration on the VPN VM.

1. First, make sure the firewalls on the other VMs and host OS are all off.
2. Logon to the Firewall VM, and from the start menu, search option, type "firewall". Select the **Windows Firewall with Advanced Security**.
3. In the Firewall console, verify the private and domain are off, and only public is enabled. This is protecting the internet facing connection.

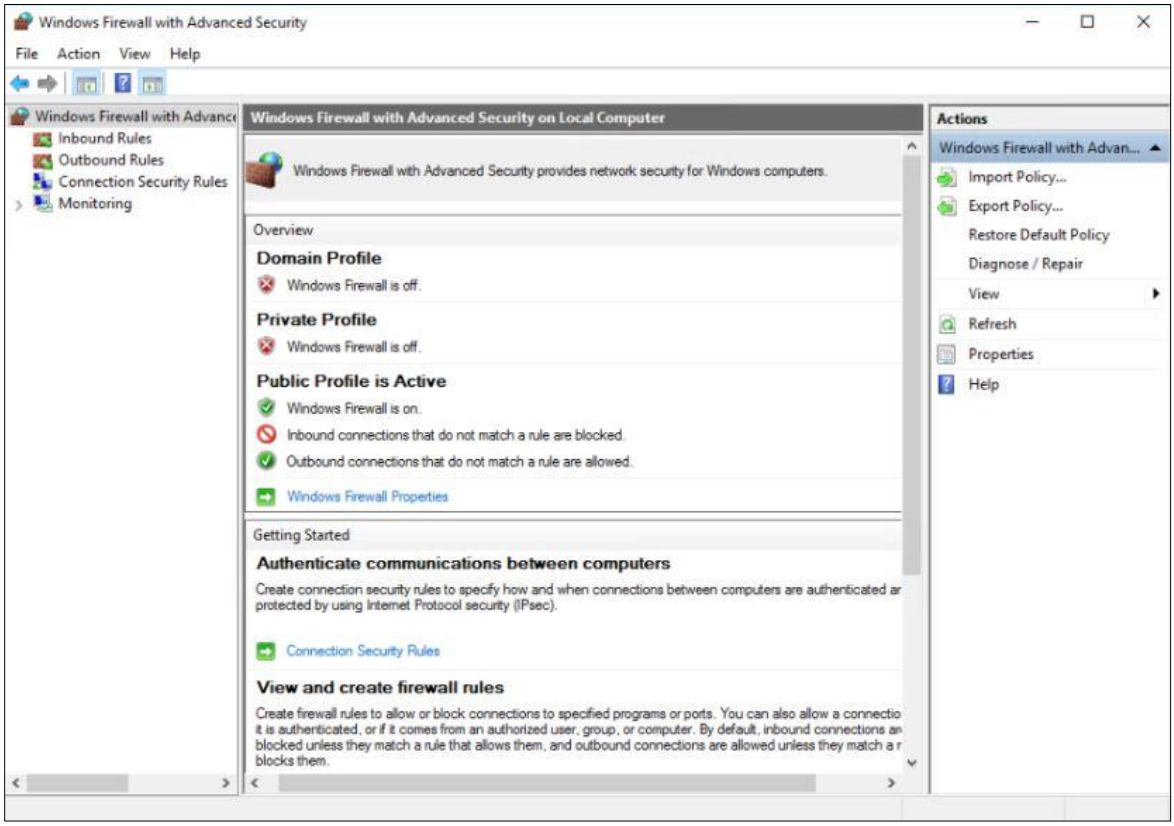

Figure 47 View of firewall profiles and status

4. Click on Inbound rules in the left pane. Scroll down and verify the Routing and Remote Access rules are enabled. This is allowing VPN and routing traffic through the internet facing connection.

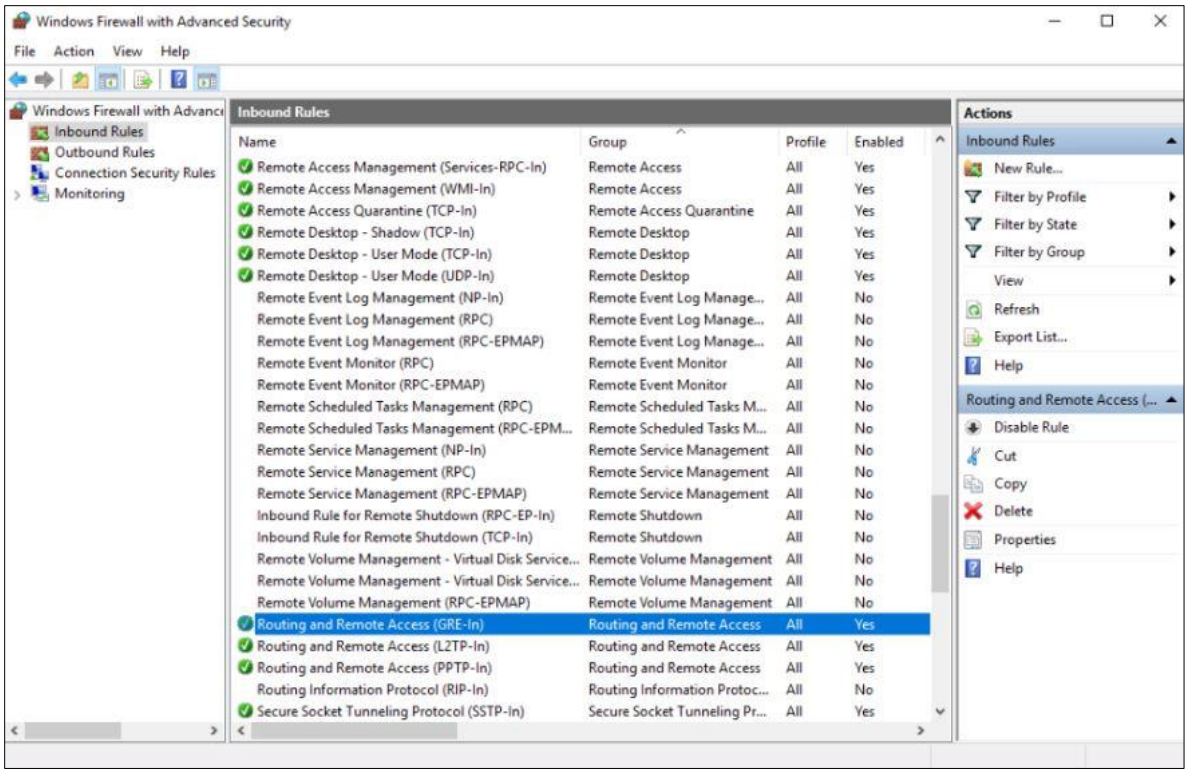

Figure 48 List of firewall rules, showing RAS protocols allowed

Site-to-site VPN configuration

The VPN setup is dependent on having the edge server VPN VM configured and online, which was covered in the earlier section.

The VPN server is running as a dedicated VM on both the edge server and in the data center location. It is a dual-homed VM, since it performs routing, NAT and firewall services. One virtual NIC is connected to the internal virtual switch and the other is connected to the internet facing virtual switch. The connection between sites is created by specifying the target external IP address of each VPN VM. It is secured by the IKEv2 protocol and pre-shared key.

Complete the steps below to configure the VPN connection. The steps will cover setting up one side of the connection. After one side is complete, repeat the same steps to create the other side.

1. Provision a VM at the data center environment and prepare the OS as usual. It will need two virtual NICs added, and IP addresses assigned. One on the private network, one on the internet facing.
2. The VPN VMs do not need to be joined to the domain.
3. During setup of the VPN, turn off the Windows firewall on both VMs. It will be enabled again later.

4. Create a local user account on each VPN VM with a descriptive name such as DCTR-VPN or EDGE-VPN. These will be used for VPN authentication. Open the properties of the accounts, go to the **Dial-in** tab, **Network Access Permissions**, and choose **Allow Access.**
5. Add the Remote Access role, from Server Manager, Add Roles and Features.

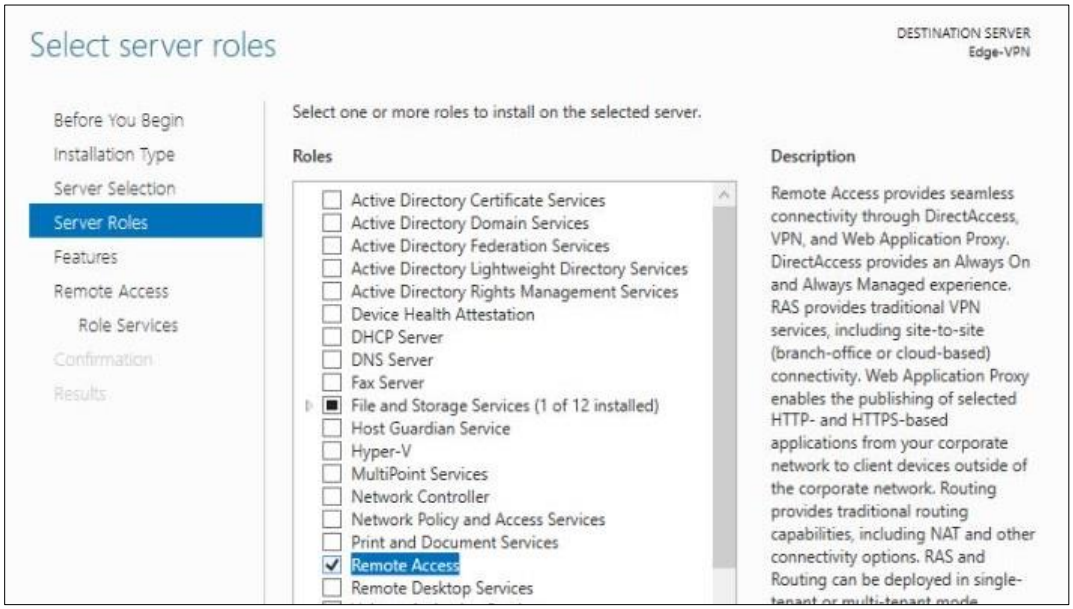

Figure 49 Adding the Remote Access role

6. Check the **DirectAccess and VPN (RAS)** and **Routing** check boxes. The solution does not use DirectAccess, however Microsoft groups both features together so both are installed.

Figure 50 Selecting role services to install for VPN support

7. After the role installation finishes, click on the link **Open the Getting Started Wizard.**

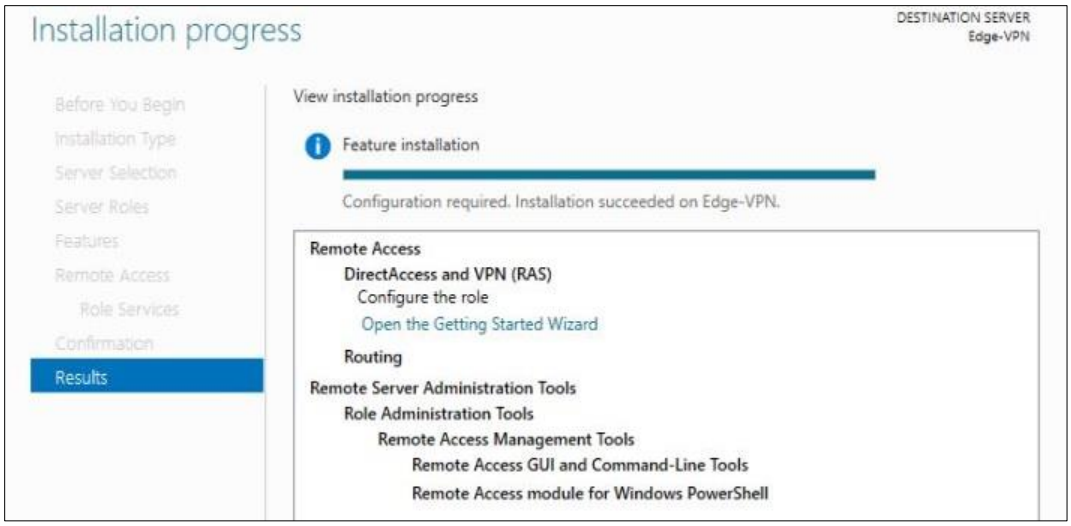

Figure 51 Installation complete, ready to start the configuration wizard

8. In the getting started wizard, select **Deploy VPN only.**

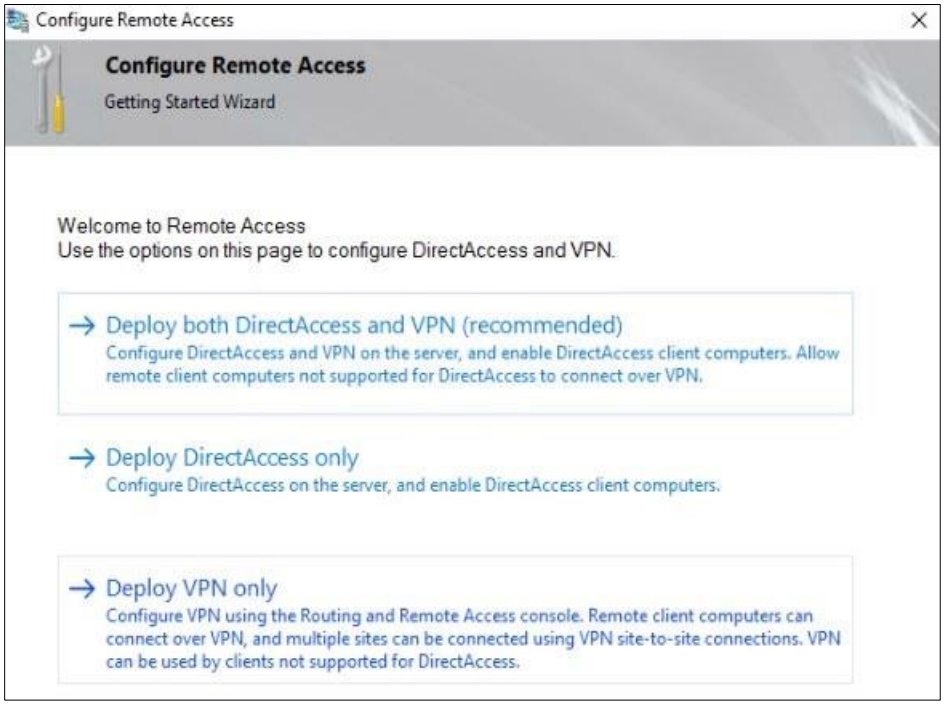

Figure 52 View of getting started wizard, configuration options

9. After selecting VPN only, the **Routing and Remote Access** console opens.
10. Right click the server name, and select **Configure and Enable Routing and Remote Access.**

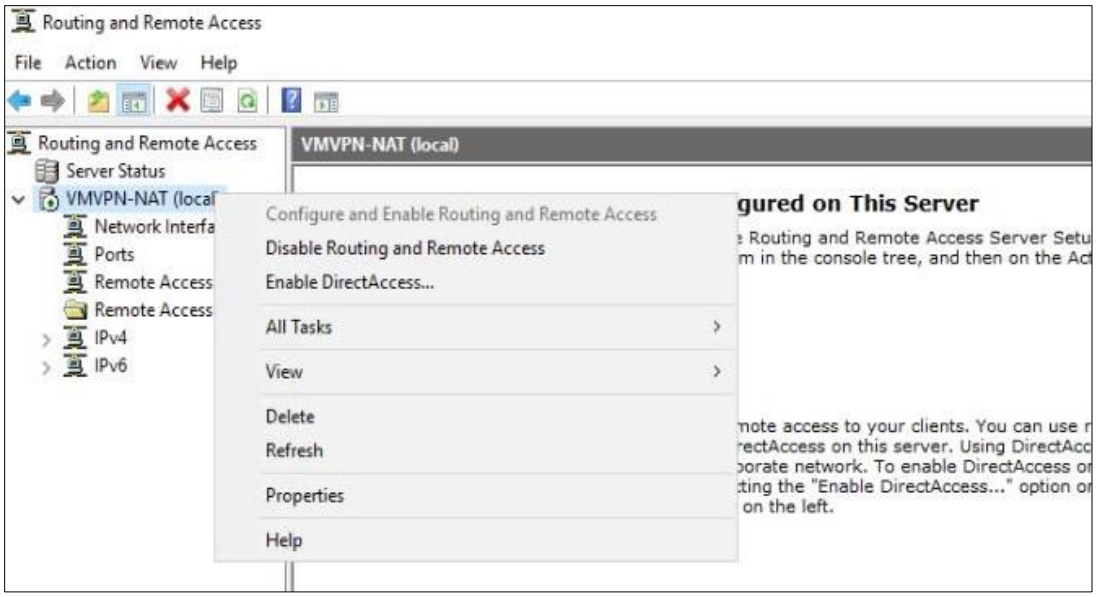

Figure 53 Start configuring routing and VPN services

11. Select **Custom Configuration** on the next screen.
12. On the next screen select **VPN access, Demand-dial connections** and **NAT.**
13. Click **Finish** and then **Start Service.**

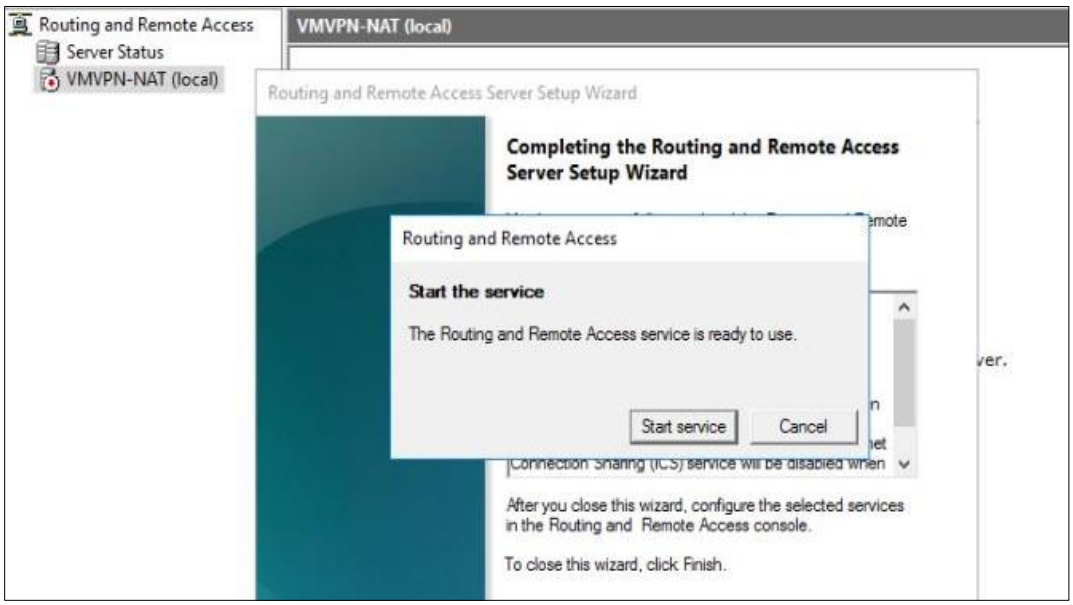

Figure 54 Complete the setup wizard and start the services

14. Right click **Network Interfaces**, and select **New Demand-dial interface.**
15. Enter the interface name. Use the same name as the account that was created earlier, such as DCTR-VPN.
16. On the connection type screen, choose **Connect using virtual private networking (VPN).**
17. At the VPN type screen, choose **IKEv2.**

18. On the destination address screen, enter the **external IP address** of the VPN VM at the **other site.**
19. Select **Route IP packets on this interface** and **Add a user account so a remote router can dial in.**

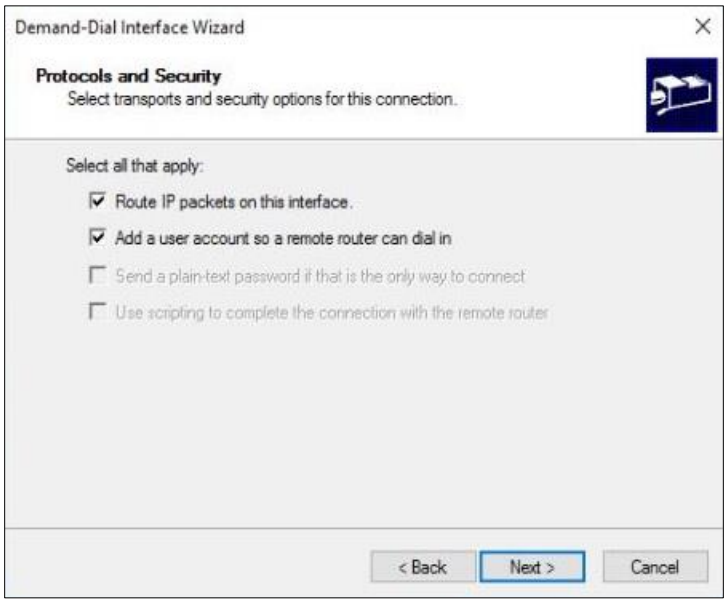

Figure 55 Selecting transport and security options for the connection

20. Add a static route. This is the network ID of the target private subnet at the other site. It allows routing of packets to that subnet. Be sure to use the correct format, as shown in figure 55. The metric value is not critical; 10 to 20 range is fine.

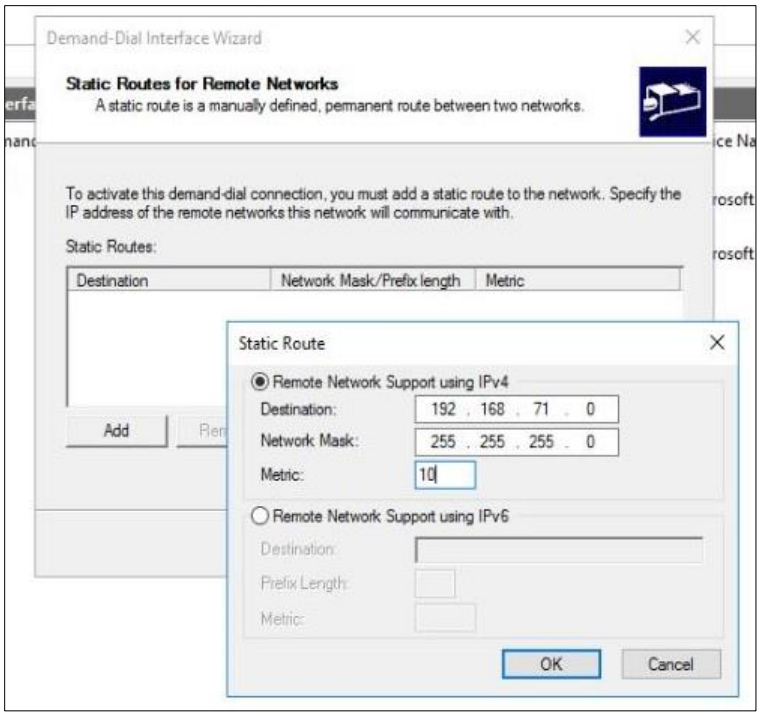

Figure 56 Setting static routes to the target site's subnet

21. Enter the **Dial in** credentials, which is the local Windows account created earlier.
22. Enter the **Dial out** credential, this is the account on the target, remote site VPN VM created earlier.
23. The following message may appear regarding the account, click yes to use the account.

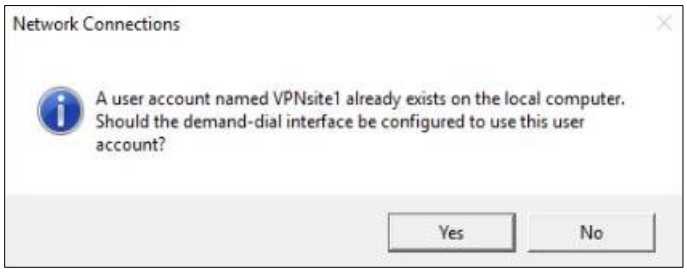

Figure 57 Confirm use of existing account created previously

24. Right click the Demand dial interface just created and select properties, the following screen opens. Set the IKEv2 **preshared key**. This is just a string of characters, similar to a password. Write it down, it will be needed to configure the other side later.

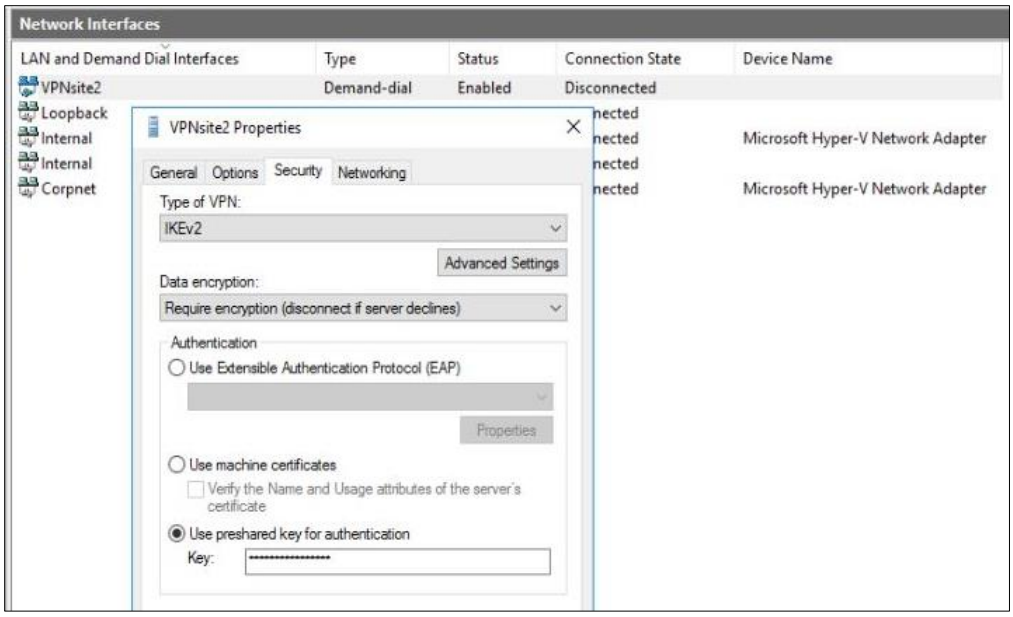

Figure 58 Configuring the IKE v2 preshared key on the Security tab of interface properties

25. Go to the Options tab, and set the connection to **Persistent**. Click **OK** to save.

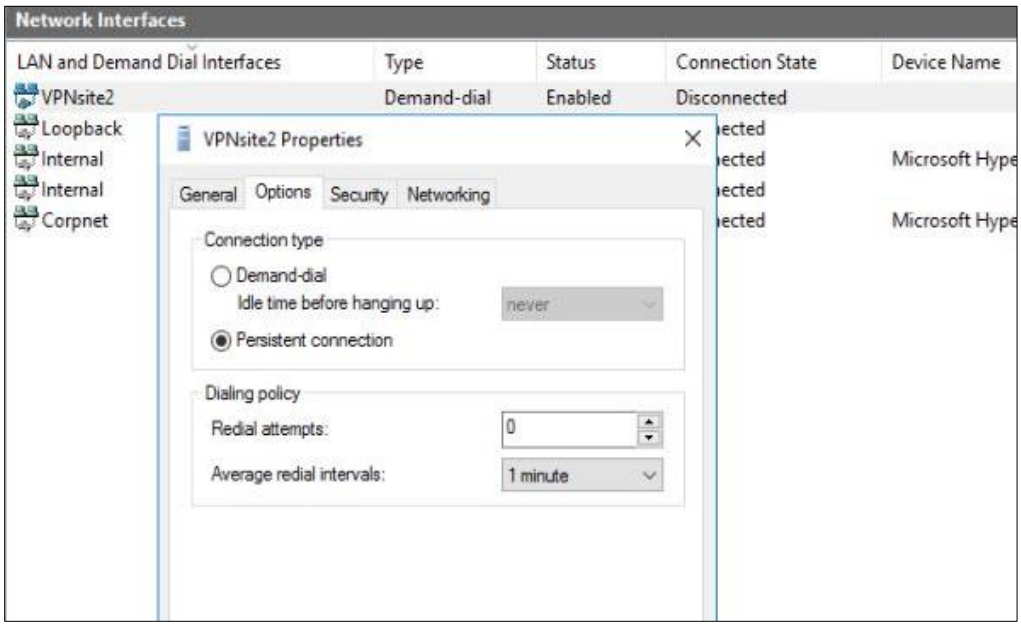

Figure 59 Set the connection to persistent from the Options tab

26. Repeat the above steps to configure the other side of the VPN connection.
27. After the configuration is complete on both sides, right click the connection in the list of interfaces, and select **Connect**. This can be done from either side. The connection should show connected and remain connected since it is set to persistent.

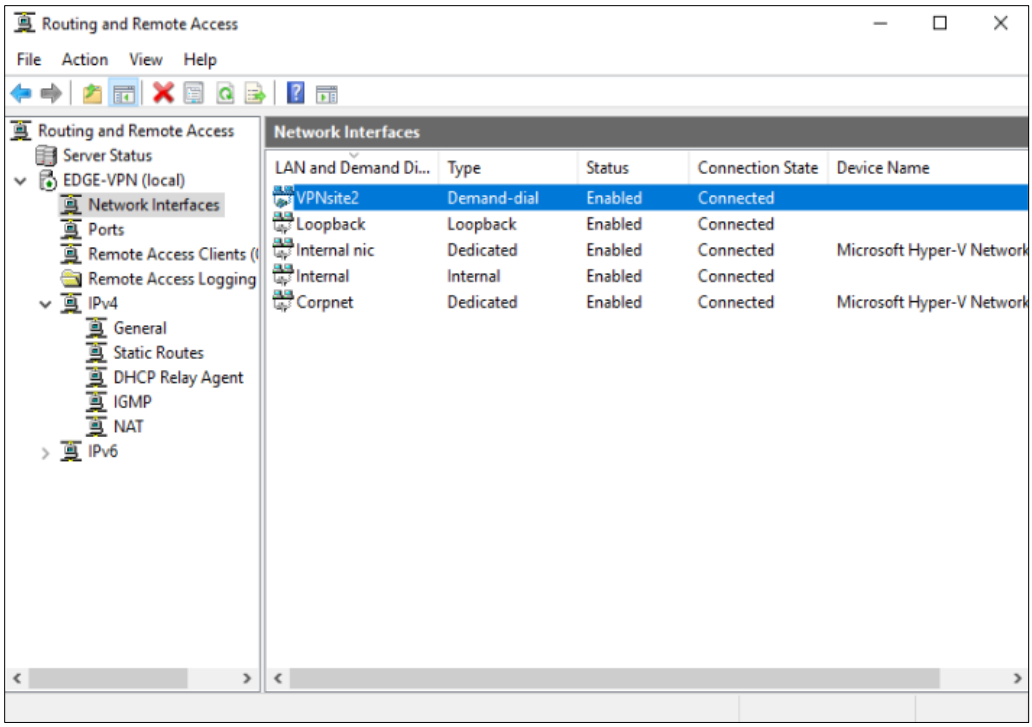

Figure 60 View of successfully connected VPN connection

Configure NAT

This section continues within the Routing and Remote Access management console. Follow the steps below to configure network address translation (NAT) to allow the internal VMs to access the internet through the VPN routing VM.

1. Check the list of Network interfaces in the console, and confirm which one is internal and which is external. See figure 59 above.
2. Right click on **NAT** in the left panel under **IPv4**, and choose **New Interface.**
3. Select the **internal** interface from the list and click **Ok.**
4. Select **Private interface connected to private network**, click **OK.**
5. Right click again on NAT, and select **New Interface.**
6. This time select the **external** interface, click **OK.**
7. Select **Public interface connected to internet**, and check the box **Enable NAT on this interface.** NAT is now configured. Internet requests from clients on the internal network will be sent out through the external interface.
8. On both the edge server and data center, set the default gateway on the VMs and host OS to the internal IP address of the VPN VM. This will route all site-to-site and internet traffic out through the VPN VM.
9. Enable the Windows Firewall on the VPN VM for the public interface only, and only on the edge server. The data center side uses the corporate firewall not the Windows firewall.

As new sites are added, additional VPN connections will need to be configured in the same manner.

Overview of Azure Pack portals

Admin portal

The admin portal is designed for the IT Administrators to manage the entire Azure Pack environment and integration with the underlying System Center resources. This portal is where user accounts are created, and resources are assigned to tenants. Plans are created and assigned to tenants, which control what the tenants have access to. Overall resources for the environment are managed and capacity can be monitored and controlled.

The following screens provide an overview of the admin portal.

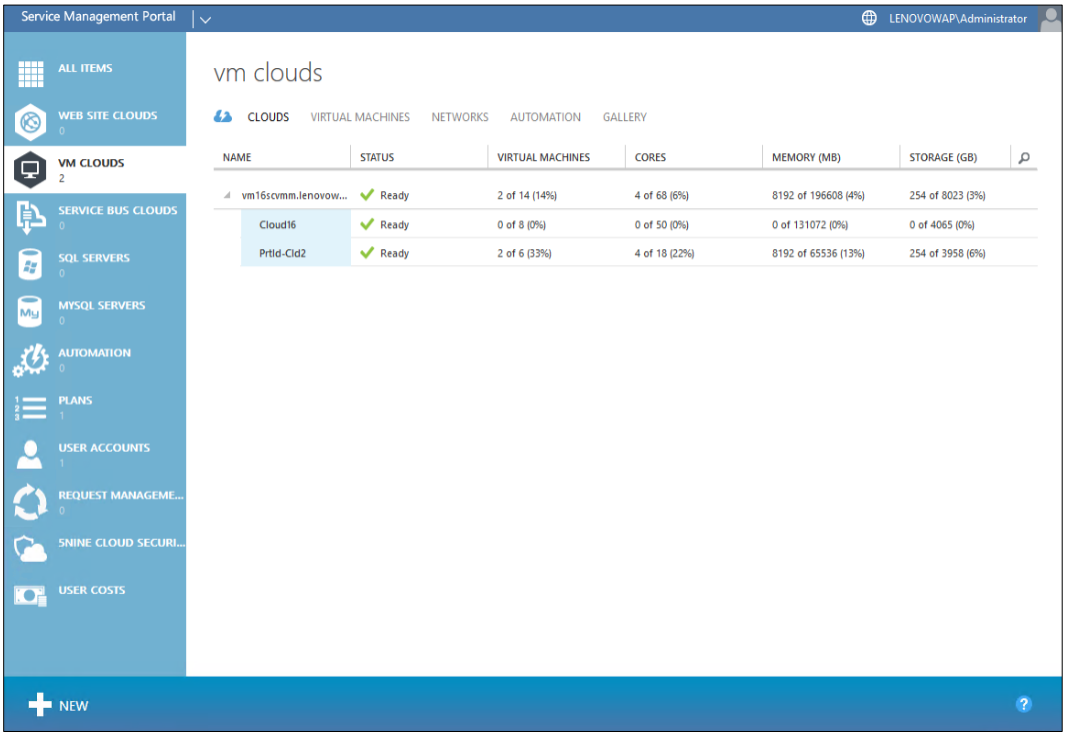

Figure 61 View of VM Clouds configured and their status

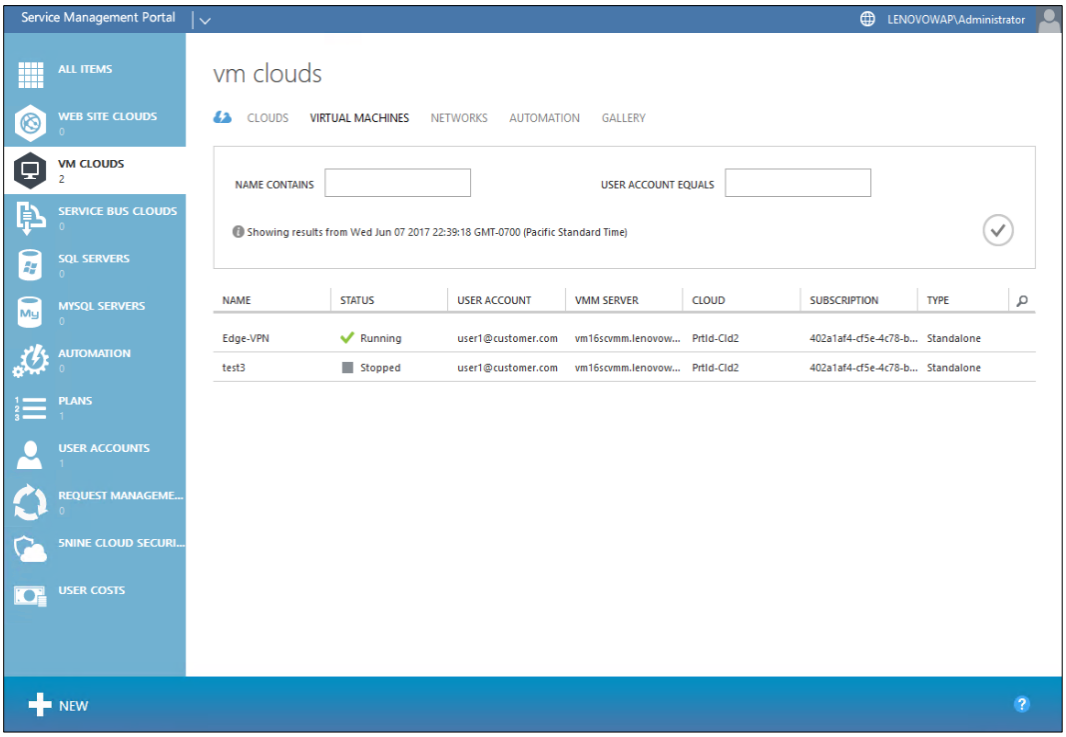

Figure 62 View of VMs deployed at a remote site. Click on one to administer or connect to it

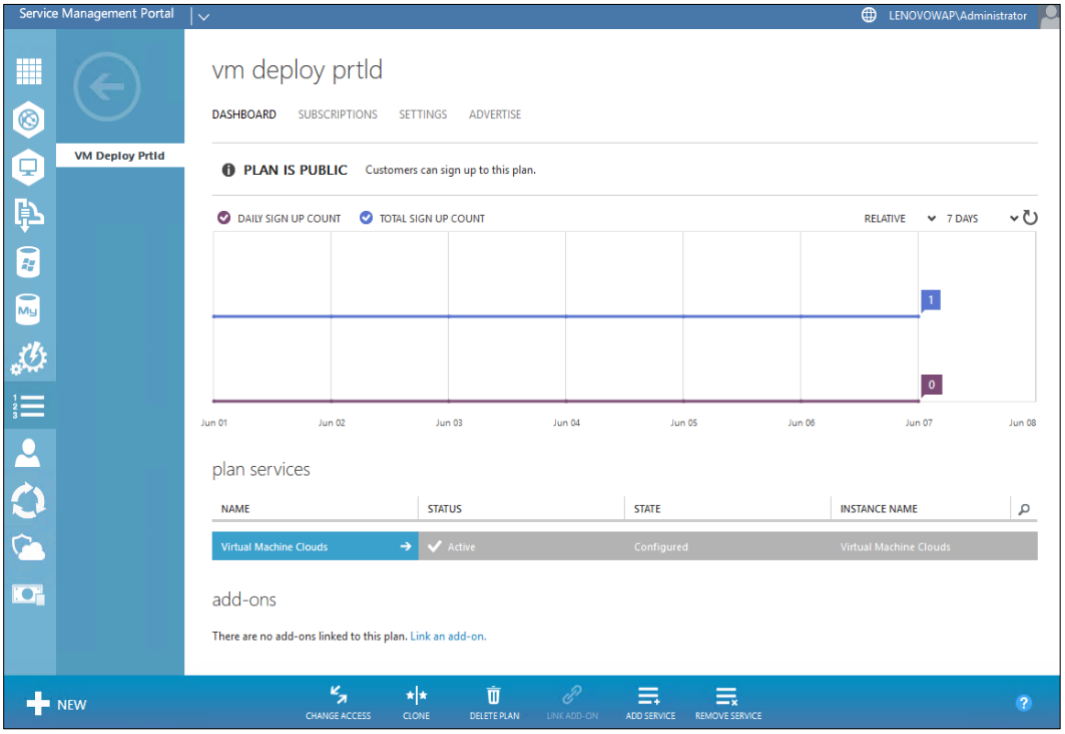

Figure 63 View of a sample plan, usage statistics and management options along the lower pane

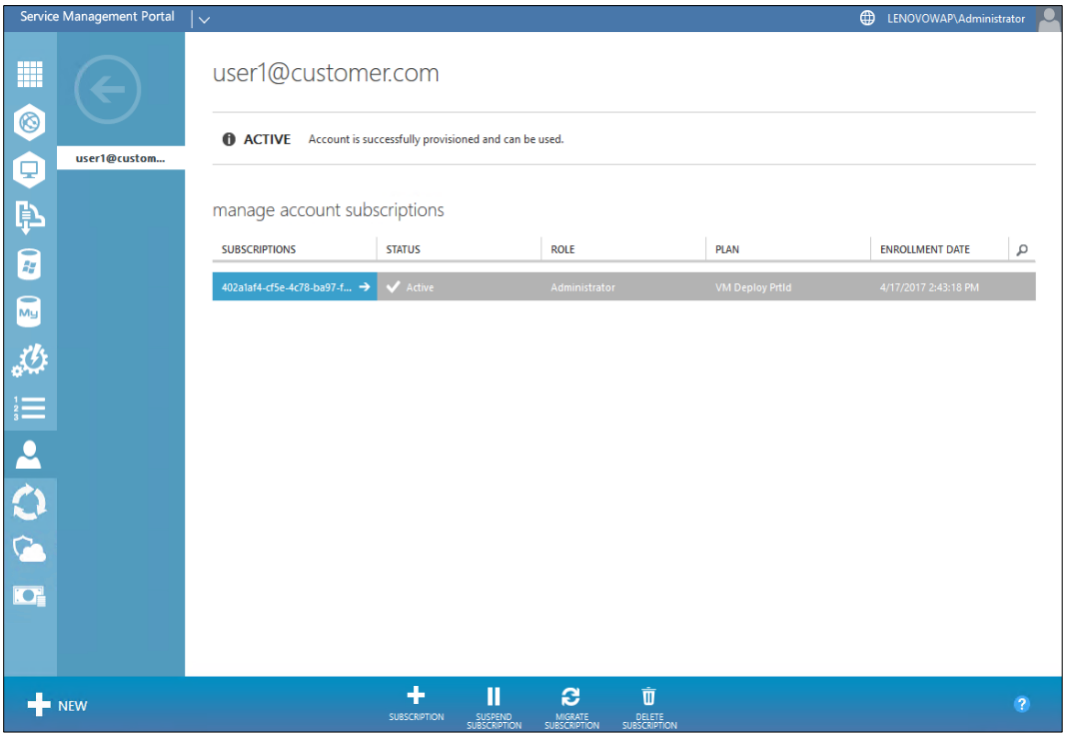

Figure 64 User management page, with management options along lower pane

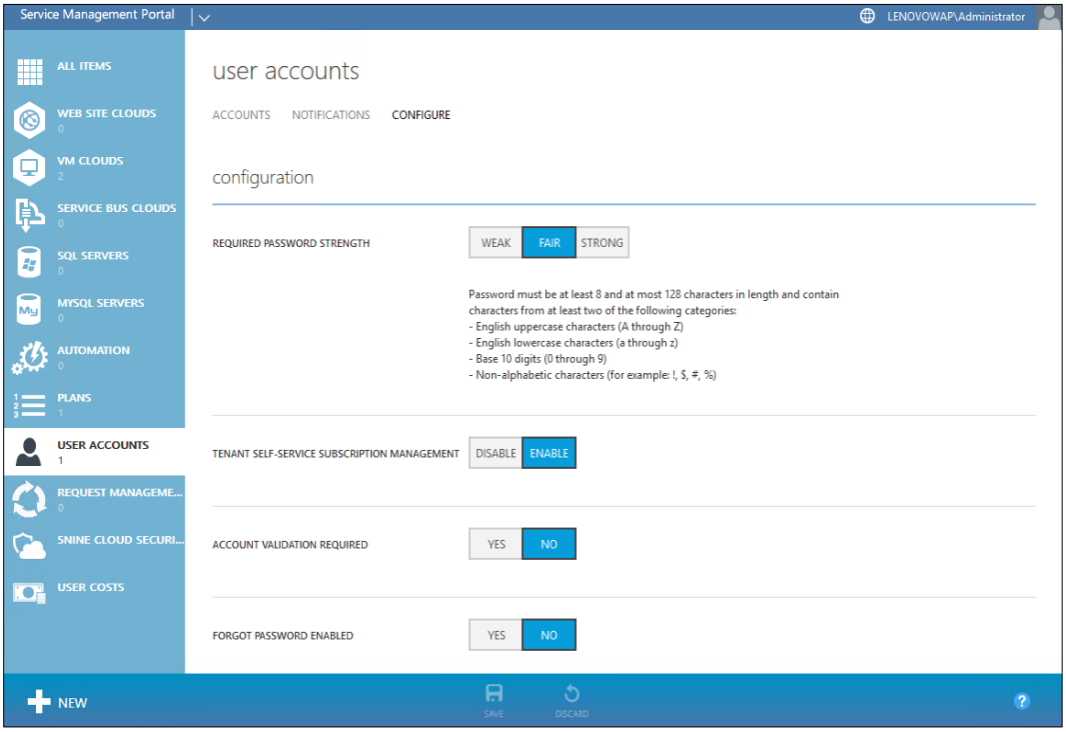

Figure 65 User account and security policy configuration options

Tenant Portal

The tenant portal is designed for use by the tenant administrators. The tenant administrators are expected to be system administrator level staff. The intuitive interface and controlled resources also help make the solution easily manageable by less experienced IT staff.

After a tenant administrator logs in to the tenant portal they can view the services available to them. They have several options to configure their own environment, such as deploying and managing VMs, creating logical networks, taking checkpoints, etc.

What is available within the tenant portal depends on what has been provisioned for each tenant from the Azure Pack admin portal. This could include SQL databases, other applications or web site creation options.

The following screens provide an overview of the tenant portal.

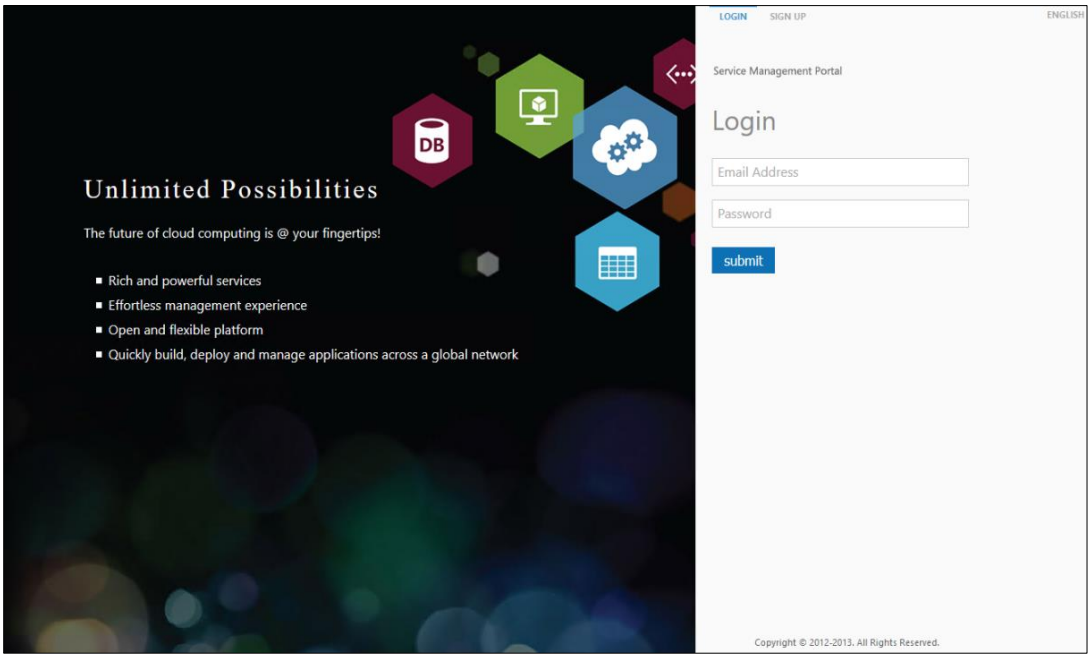

Figure 66 Azure Pack Tenant Portal login screen. Page can be customized with tenant logo or graphics

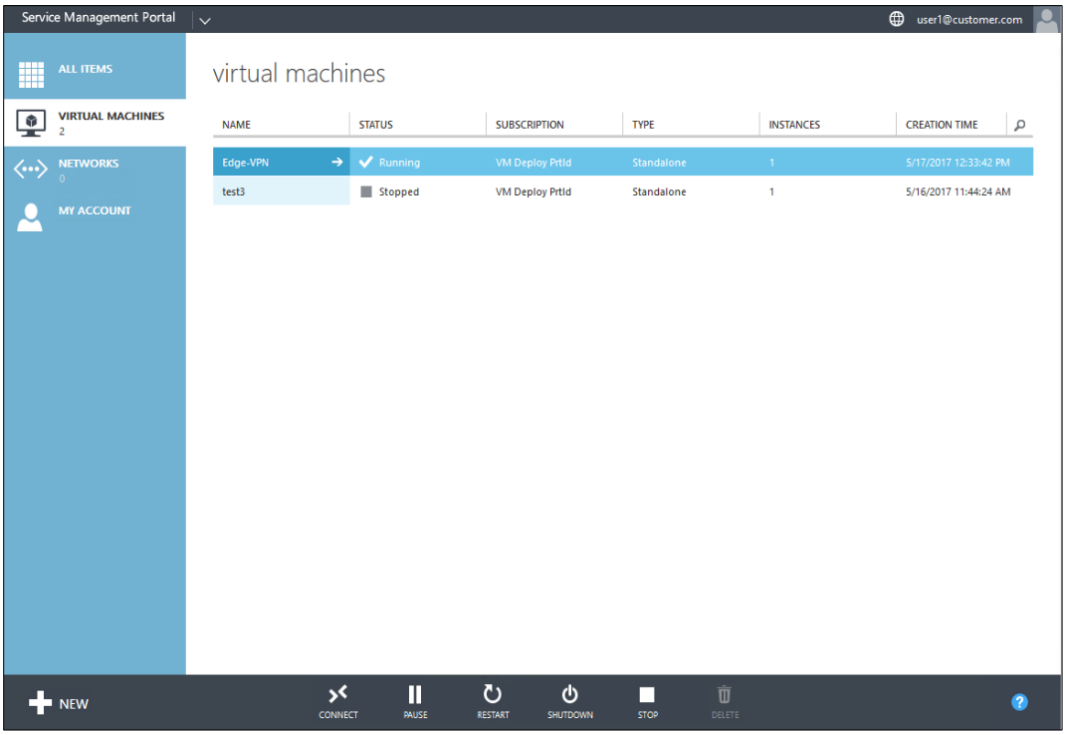

Figure 67 VMs deployed at remote site, with the administration options along the lower pane

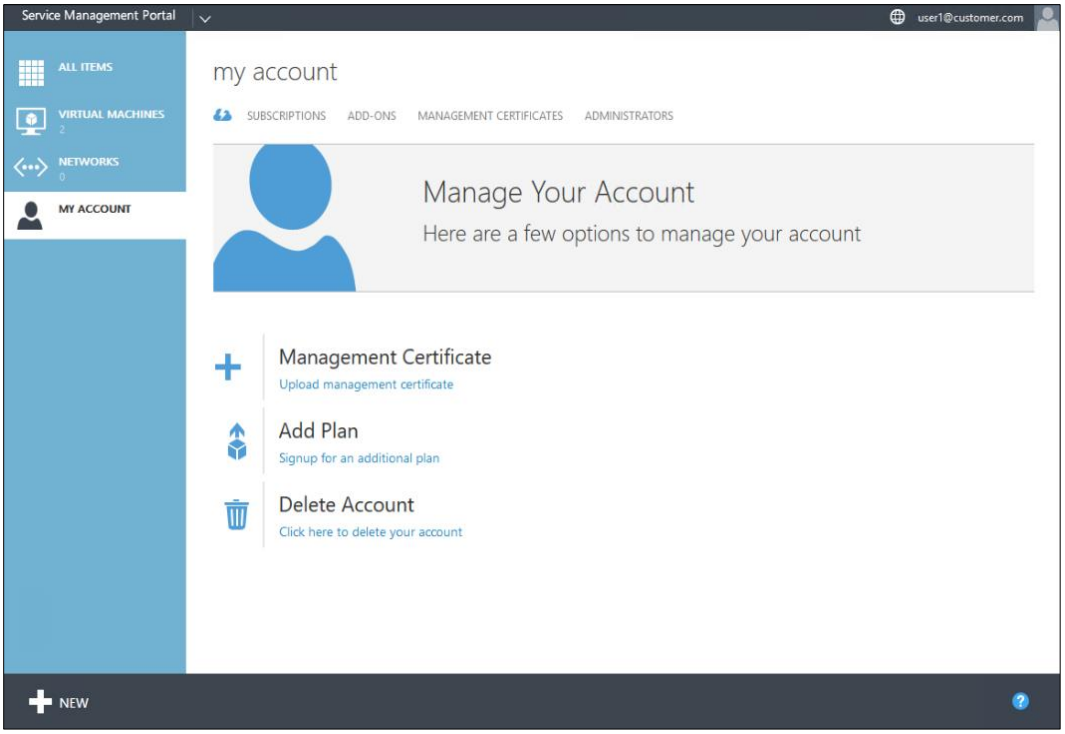

Figure 68 User options for managing their account

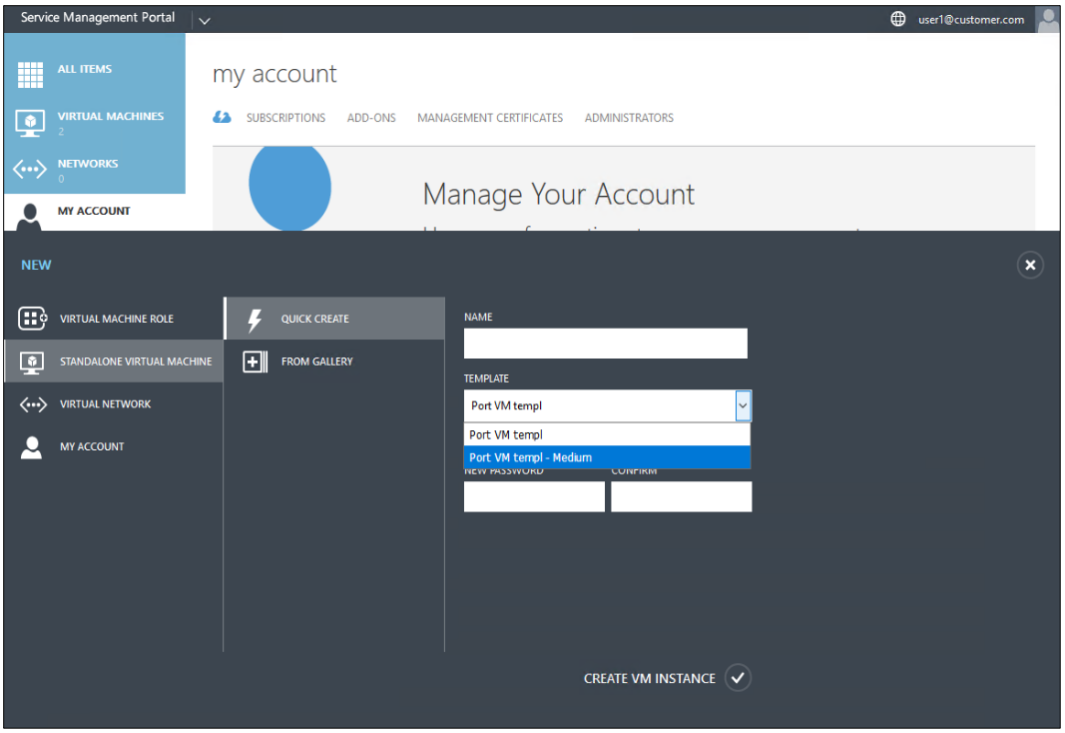

Figure 69 Deploying a new VM, selecting a size and location

Appendix A. Bill of Materials

There are two configurations for the Lenovo System x3650 M5, a medium and a large, depending on the system resources required. The data center side of the solution requires a minimum of two systems for the Microsoft Failover Cluster. The remote sites each have a single system. Below are the Bill of Materials for both sizings.

Edge Cloud Medium Configuration

Qty	**Part number**	**Product Description**		
1	8871AC1	EdgeCloud_medium_WS16 : Lenovo System x3650 M5		
1	ATDY	2.5" Flexible Base (up to 24x 2.5") w/o Power Supply		
1	ATFC	Addl Intel Xeon Processor E5-2609 v4 8C 1.7GHz 20MB 1866MHz 85W		
1	ATEM	Intel Xeon Processor E5-2609 v4 8C 1.7GHz 20MB Cache 1866MHz 85W		
8	ATC8	8GB TruDDR4 Memory (1Rx4, 1.2V) PC4-19200 CL17 2400MHz LP RDIMM		
1	A5GH	System x3650 M5 Rear 2x 2.5" HDD Kit (Independent RAID)		
1	A5G6	x3650 M5 8x 2.5" HS HDD Assembly Kit (Single RAID)		
1	A3YY	N2215 SAS/SATA HBA		
1	A45W	ServeRAID M1215 SAS/SATA Controller		
5	A4TX	1TB 7.2K 6Gbps NL SATA 2.5" G3HS HDD		
2	AT89	300GB 10K 12Gbps SAS 2.5" G3HS HDD		
2	A578	240GB SATA 2.5" MLC G3HS Enterprise Value SSD		
1	A5GZ	Broadcom NetXtreme 2x10GbE BaseT Adapter		
1	A1ML	Integrated Management Module Advanced Upgrade		
1	A5FV	System x Enterprise Slides Kit		
1	ATE4	System x3650 M5 Planar BDW		

1	ATE6	x3650 M5 Front IO Cage Std. (3x USB, Optional LCD/Optical drive)		
1	ATE7	System x3650 M5 2.5" Bezel without LCD Light Path		
1	ATEA	System x3650 M5 EIA L - Blank		
1	A5KG	9.5mm Ultra-Slim SATA DVD-ROM		
1	3797	1.5m Green Cat5e Cable		
1	A5EU	System x 750W High Efficiency Platinum AC Power Supply		
1	6311	2.8m, 10A/100-250V, C13 to IEC 320-C14 Rack Power Cable		
1	A5V7	System x3650 M5 ODD Cable for 2.5" Model		
4	ATEC	System x3650 M5 Single Rotor Fan		
1	A5FT	System x3650 M5 Power Paddle Card		
1	A5G1	System x3650 M5 EIA Plate		
1	A5V4	System x3650 M5 Right EIA		
1	AUK7	Enable TPM 2.0 and Secure Boot		
1	5977	Select Storage devices - no configured RAID required		
1	A5FZ	System x3650 M5 Riser Filler		
1	ATG2	System Documentation and Software-US English		
1	A483	Populate and Boot From Rear Drives		
1	ATGF	System x3650 M5 WW Packaging		
1	9206	No Generic Preload Specify		
1	A4C2	HDD Filler ASM GEN 3 Single Filler		
1	9205	Drop-in-the-Box Specify		
1	ATE3	System x3650 M5 System Level Code		
1	ATE1	System x3650 M5 Single Rotor Fan Cage		
1	ATE2	System x3650 M5 System Agency Label		
1	ASQA	System x3650 M5 Rear 2x 2.5" HDD Label (Independent RAID-Riser1)		
1	ATRG	System X M5 rear USB Port Cover		
2	A2HP	Configuration ID 01		
2	A4EL	HDD Filler ASM GEN 3 Quad Filler		
1	A1L7	CFF Power Supply Filler		
1	A5H0	2U Bracket for Broadcom NetXtreme 2x10GbE BaseT Adapter		
1	9201	Windows Specify		
1	5374CM1	5374CM1 : Configuration Instruction		
1	A5M2	ServeRAID M1215 SAS/SATA Controller Upgrade Placement		
1	A2HP	Configuration ID 01		

1	A2JX	Controller 01		
1	5374CM1	5374CM1 : Configuration Instruction		
1	A2HP	Configuration ID 01		
1	A46U	N2215 SAS/SATA HBA Placement		
1	A2JY	Controller 02		
1	5372SWX	HIPO : xSeries HIPO		
1	AXUG	Windows Svr 2016 Datacenter (16 core)-MultiLang (not preinstalled)		
1	A86Y	8871-AC1 Routing Code		
1	01GX546	Lenovo services1 : 3Y Tech Install Parts 24x7x4 Response		
1	5731W16	Operating system : Windows Server 2016		
1	V2MUBG	Per 16 Cores W2016 Dtc 16C ML NoPreinstal		
1	3523	Drop-in-the-Box		
1	3444	Serial Number Only		

Edge Cloud Large Configuration

Qty	Part number	Product Description		
1	8871AC1	EdgeCloud_large_WS16 : Lenovo System x3650 M5		
1	ATDY	2.5" Flexible Base (up to 24x 2.5") w/o Power Supply		
1	A5EE	Intel Xeon Processor E5-2630 v3 8C 2.4GHz 20MB Cache 1866MHz 85W		
1	A5EK	Addl Intel Xeon Processor E5-2630 v3 8C 2.4GHz 20MB 1866MHz 85W		
16	ATC8	8GB TruDDR4 Memory (1Rx4, 1.2V) PC4-19200 CL17 2400MHz LP RDIMM		
1	A5GH	System x3650 M5 Rear 2x 2.5" HDD Kit (Independent RAID)		
1	A5G6	x3650 M5 8x 2.5" HS HDD Assembly Kit (Single RAID)		
1	A3YY	N2215 SAS/SATA HBA		
1	A45W	ServeRAID M1215 SAS/SATA Controller		
2	AT89	300GB 10K 12Gbps SAS 2.5" G3HS HDD		
4	AT80	2TB 7.2K 12Gbps NL SAS 2.5" G3HS HDD		
2	AT9M	400GB Enterprise Mainstream 12Gb SAS G3HS 2.5" SSD		
1	A5GZ	Broadcom NetXtreme 2x10GbE BaseT Adapter		
1	A1ML	Integrated Management Module Advanced Upgrade		
1	A5FV	System x Enterprise Slides Kit		
1	ATE4	System x3650 M5 Planar BDW		
1	ATE6	x3650 M5 Front IO Cage Std. (3x USB, Optional LCD/Optical drive)		
1	ATE7	System x3650 M5 2.5" Bezel without LCD Light Path		
1	ATEA	System x3650 M5 EIA L - Blank		

1	A5KG	9.5mm Ultra-Slim SATA DVD-ROM		
1	3797	1.5m Green Cat5e Cable		
1	A5EU	System x 750W High Efficiency Platinum AC Power Supply		
2	6311	2.8m, 10A/100-250V, C13 to IEC 320-C14 Rack Power Cable		
1	A5V7	System x3650 M5 ODD Cable for 2.5" Model		
1	ATEE	System x3650 M5 Dual Rotor Fan Cage		
4	ATEB	System x3650 M5 Dual Rotor Fan		
1	A5FT	System x3650 M5 Power Paddle Card		
1	A5G1	System x3650 M5 EIA Plate		
1	A5V4	System x3650 M5 Right EIA		
1	AUK7	Enable TPM 2.0 and Secure Boot		
1	5977	Select Storage devices - no configured RAID required		
1	A5FZ	System x3650 M5 Riser Filler		
1	ATG2	System Documentation and Software-US English		
1	A483	Populate and Boot From Rear Drives		
1	ATGF	System x3650 M5 WW Packaging		
1	9206	No Generic Preload Specify		
2	A4C2	HDD Filler ASM GEN 3 Single Filler		
1	9205	Drop-in-the-Box Specify		
1	ATE3	System x3650 M5 System Level Code		
1	ATE2	System x3650 M5 System Agency Label		
1	ASQA	System x3650 M5 Rear 2x 2.5" HDD Label (Independent RAID-Riser1)		
1	ATRG	System X M5 rear USB Port Cover		
2	A2HP	Configuration ID 01		
2	A4EL	HDD Filler ASM GEN 3 Quad Filler		
1	A1L7	CFF Power Supply Filler		
1	A5H0	2U Bracket for Broadcom NetXtreme 2x10GbE BaseT Adapter		
1	9201	Windows Specify		
1	5374CM1	5374CM1 : Configuration Instruction		
1	A5M2	ServeRAID M1215 SAS/SATA Controller Upgrade Placement		
1	A2HP	Configuration ID 01		
1	A2JX	Controller 01		
1	5374CM1	5374CM1 : Configuration Instruction		

1	A2HP	Configuration ID 01		
1	A46U	N2215 SAS/SATA HBA Placement		
1	A2JY	Controller 02		
1	5372SWX	HIPO : xSeries HIPO		
1	AXUG	Windows Svr 2016 Datacenter (16 core)-MultiLang (not preinstalled)		
1	A86Y	8871-AC1 Routing Code		
1	01GX546	Lenovo services1 : 3Y Tech Install Parts 24x7x4 Response		
1	5731W16	Operating system : Windows Server 2016		
1	V2MUBG	Per 16 Cores W2016 Dtc 16C ML NoPreinstal		
1	3523	Drop-in-the-Box		
1	3444	Serial Number Only		