


Deploy a migration infrastructure

10/01/2018 • 37 minutes to read • Contributors 

In this article

[Overview](#)

[Before you start](#)

[On-premises architecture](#)

[Step 1: Buy and subscribe to Azure](#)

[Step 2: Manage hybrid identity](#)

[Step 3: Design for resiliency](#)

[Step 4: Design a network infrastructure](#)

[Step 5: Plan for governance](#)

[Step 6: Consider security](#)

[Conclusion](#)

[Next steps](#)

This article shows how the fictional company Contoso prepares its on-premises infrastructure for migration, sets up an Azure infrastructure in preparation for migration, and runs the business in a hybrid environment. When you use this example to help plan your own infrastructure migration efforts, keep the following in mind:

- The provided sample architecture is specific to Contoso. Review your own organization's business needs, structure, and technical requirements when making important infrastructure decisions about subscription design or networking architecture.
- Whether you need all the elements described in this article depends on your migration strategy. For example, if you're building only cloud-native apps in Azure, you might need a less complex networking structure.

Overview

Before Contoso can migrate to Azure, it's critical to prepare an Azure infrastructure. Generally, there are six broad areas Contoso needs to think about:

- ✓ **Step 1: Azure subscriptions.** How will Contoso purchase Azure, and interact with the Azure platform and services?
- ✓ **Step 2: Hybrid identity.** How will it manage and control access to on-premises and Azure resources after migration? How does Contoso extend or move identity management to the cloud?
- ✓ **Step 3: Disaster recovery and resilience.** How will Contoso ensure that its apps and infrastructure are resilient if outages and disasters occur?
- ✓ **Step 4: Networking.** How should Contoso design a networking infrastructure, and establish connectivity between its on-premises datacenter and Azure?
- ✓ **Step 5: Security.** How will it secure the hybrid/Azure deployment?
- ✓ **Step 6: Governance.** How will Contoso keep the deployment aligned with security and governance requirements?

Before you start

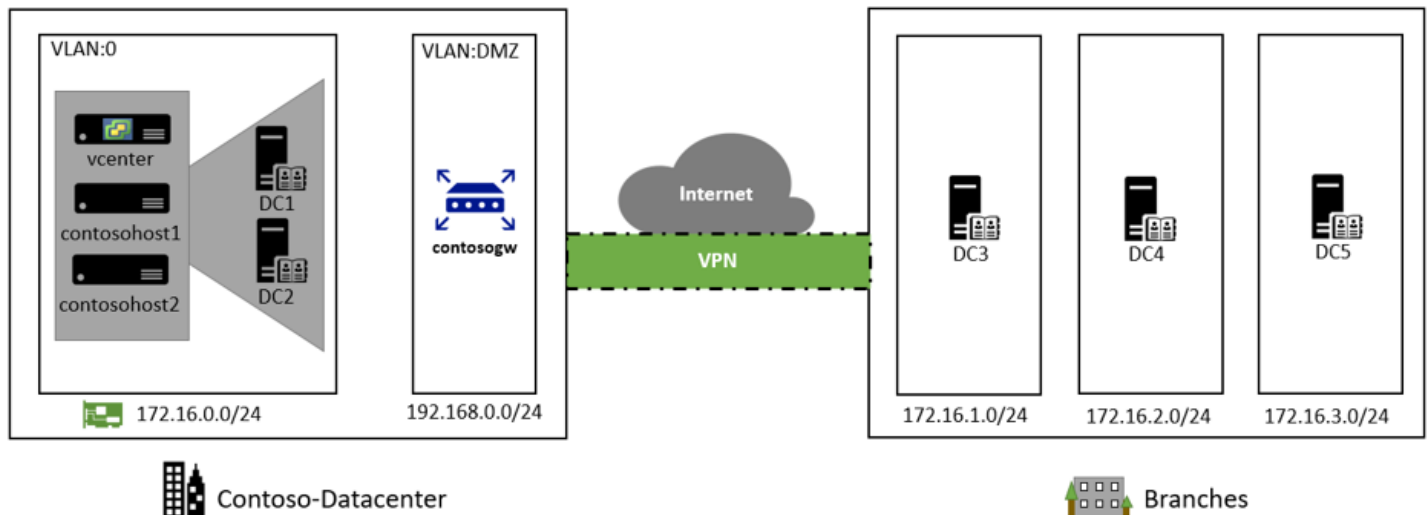
Before we start looking at the infrastructure, you might want to read some background information about the Azure capabilities we discuss in this article:

- Several options are available for purchasing Azure access, including Pay-As-You-Go, Enterprise Agreements (EA), Open Licensing from Microsoft resellers, or from Microsoft Partners known as Cloud Solution Providers (CSPs). Learn about [purchase options](#), and read about how [Azure subscriptions are organized](#).

- Get an overview of Azure [identity and access management](#). In particular, learn about [Azure AD and extending on-premises Active Directory to the cloud](#). There's a useful downloadable e-book about [identity and access management \(IAM\) in a hybrid environment](#).
- Azure provides a robust networking infrastructure with options for hybrid connectivity. Get an overview of [networking and network access control](#).
- Get an introduction to [Azure Security](#), and read about creating a plan for [governance](#).

On-premises architecture

Here's a diagram showing the current Contoso on-premises infrastructure.



- Contoso has one main datacenter located in the city of New York in the Eastern United States.
- There are three additional local branches across the United States.
- The main datacenter is connected to the internet with a fiber metro ethernet connection (500 mbps).
- Each branch is connected locally to the internet using business class connections, with IPSec VPN tunnels back to the main datacenter. This allows the entire network to be permanently connected, and optimizes internet connectivity.
- The main datacenter is fully virtualized with VMware. Contoso has two ESXi 6.5 virtualization hosts, managed by vCenter Server 6.5.
- Contoso uses Active Directory for identity management, and DNS servers on the internal network.
- The domain controllers in the datacenter run on VMware VMs. The domain controllers at local branches run on physical servers.

Step 1: Buy and subscribe to Azure

Contoso needs to figure out how to buy Azure, how to architect subscriptions, and how to license services and resources.

Buy Azure

Contoso is going with an [Enterprise Agreement \(EA\)](#). This entails an upfront monetary commitment to Azure, entitling Contoso to earn great benefits, including flexible billing options and optimized pricing.

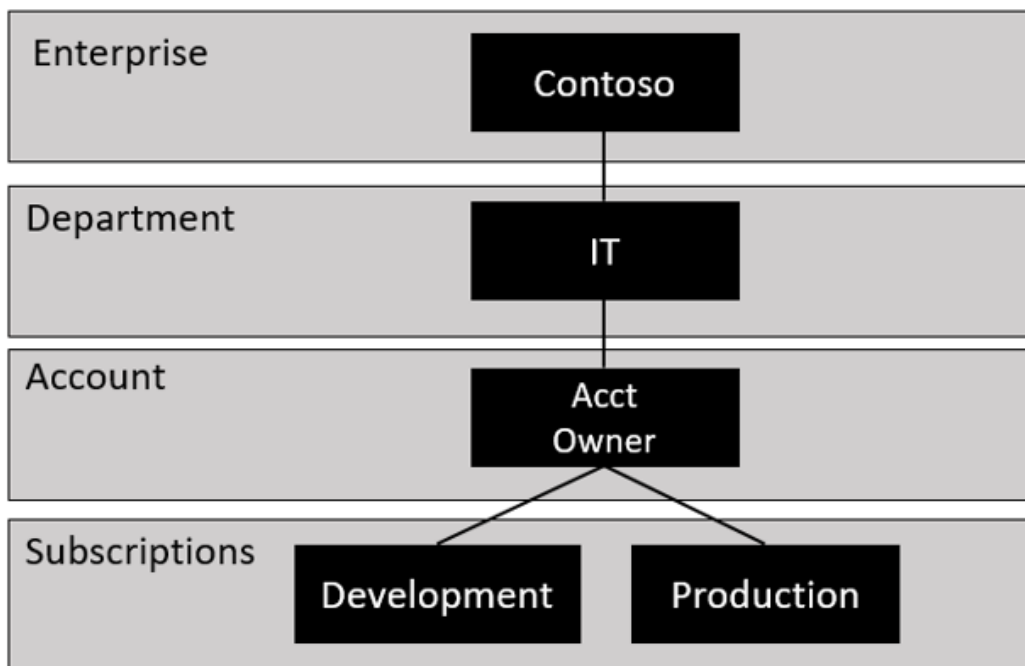
- Contoso estimated what its yearly Azure spend will be. When it signed the agreement, Contoso paid for the first year in full.
- Contoso needs to use all commitments before the year is over, or lose the value for those dollars.
- If for some reason Contoso exceeds its commitment and spends more, Microsoft will invoice them for the difference.

- Any cost incurred above the commitment will be at the same rates as those in the Contoso contract. There are no penalties for going over.

Manage subscriptions

After paying for Azure, Contoso needs to figure out how to manage Azure subscriptions. Contoso has an EA, and thus no limit on the number of Azure subscriptions it can set up.

- An Azure Enterprise Enrollment defines how a company shapes and uses Azure services, and defines a core governance structure.
- As a first step, Contoso has defined a structure known as an enterprise scaffold for Enterprise Enrollment. Contoso used [this article](#) to help understand and design a scaffold.
- For now, Contoso has decided to use a functional approach to manage subscriptions.
 - Inside the enterprise it will use a single IT department that controls the Azure budget. This will be the only group with subscriptions.
 - Contoso will extend this model in the future, so that other corporate groups can join as departments in the Enterprise Enrollment.
 - Inside the IT department Contoso has structured two subscriptions, Production and Development.
 - If Contoso requires additional subscriptions in the future, it needs to manage access, policies and compliance for those subscriptions. Contoso will do that by introducing [Azure management groups](#), as an additional layer above subscriptions.



Examine licensing

With subscriptions configured, Contoso can look at Microsoft licensing. The licensing strategy will depend on the resources that Contoso wants to migrate into Azure and how Azure VMs and services are selected and deployed.

Azure Hybrid Benefit

When deploying VMs in Azure, standard images include a license that will charge Contoso by the minute for the software being used. However, Contoso has been a long-term Microsoft customer, and has maintained EAs and open licenses with Software Assurance (SA).

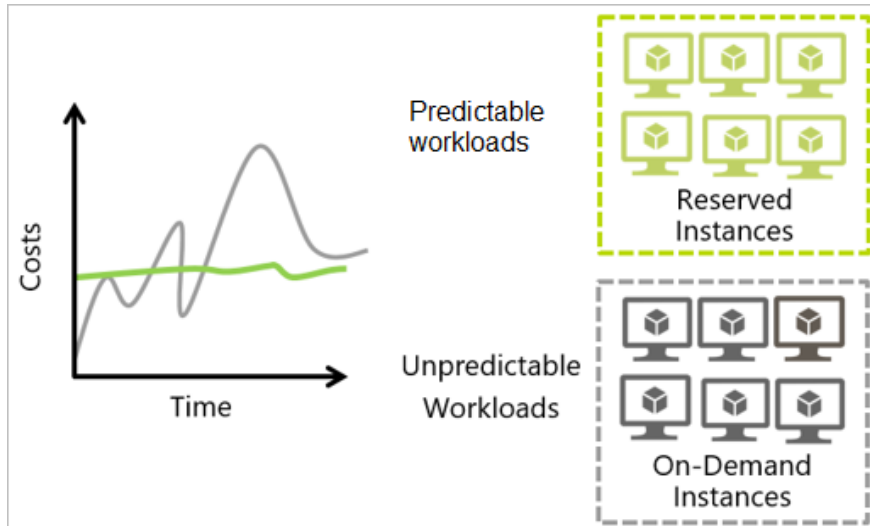
Azure Hybrid Benefit provides a cost-effective method for Contoso migration, by allowing it to save on Azure VMs and SQL Server workloads by converting or reusing Windows Server Datacenter and Standard edition licenses covered with Software Assurance. This will enable Contoso to pay a lower based compute rate for VMs and SQL Server. [Learn more.](#)

License Mobility

License Mobility through SA gives Microsoft Volume Licensing customers like Contoso the flexibility to deploy eligible server apps with active SA on Azure. This eliminates the need to purchase new licenses. With no associated mobility fees, existing licenses can easily be deployed in Azure. [Learn more](#).

Reserve instances for predictable workloads

Predictable workloads are those that always need to be available with VMs running. For example, line-of-business apps such as a SAP ERP system. On the other hand, unpredictable workloads are those that are variable, such as VMs that are on during high demand and off when demand is low.



In exchange for using reserved instances for specific VM instances must be maintained for large durations of time, Contoso can get both a discount, and prioritized capacity. Using [Azure Reserved Instances](#), together with Azure Hybrid Benefit, Contoso can save up to 82% off regular pay-as-you-go pricing (April 2018).

Step 2: Manage hybrid identity

Giving and controlling user access to Azure resources with identity and access management (IAM) is an important step in pulling together an Azure infrastructure.

- Contoso decides to extend its on-premises Active Directory into the cloud, rather than build a new separate system in Azure.
- It creates an Azure-based Active Directory to do this.
- Contoso doesn't have Office 365 in place, so it needs to provision a new Azure AD.
- Office 365 uses Azure AD for user management. If Contoso was using Office 365, it would already have an Azure AD tenant, and can use that as the primary directory.
- [Learn more](#) about Azure AD for Office 365, and learn [how to add a subscription](#) to an existing Azure AD tenant.

Create an Azure AD

Contoso is using the Azure AD Free edition that's included with an Azure subscription. Contoso admins set up a directory as follows:

1. In the [Azure portal](#), they navigate to **Create a resource > Identity > Azure Active Directory**.
2. In **Create directory**, they specify a name for the directory, an initial domain name, and region in which the Azure AD directory should be created.

ⓘ **Note**

The directory that's created has an initial domain name in the form **domainname.onmicrosoft.com**. The name can't be changed or deleted. Instead, they need to add its registered domain name to Azure AD.

Add the domain name

To use its standard domain name, Contoso admins need to add it as a custom domain name to Azure AD. This option allows them to assign familiar user names. For example, a user can log in with the email address billg@contoso.com, rather than needing billg@contosomigration.microsoft.com.

To set up a custom domain name they add it to the directory, add a DNS entry, and then verify the name in Azure AD.

1. In **Custom domain names > Add custom domain**, they add the domain.
2. To use a DNS entry in Azure they need to register it with their domain registrar.
 - In the **Custom domain names** list, they note the DNS information for the name. It's using an MX entry.
 - They need access to the name server to do this. They log into the Contoso.com domain, and create a new MX record for the DNS entry provided by Azure AD, using the details noted.
3. After the DNS records propagate, in the details name for the domain, they select **Verify** to check the custom domain name.

contoso.com

Domain name

Delete

To use contoso.com with your Azure AD, create a new TXT record with your domain name registrar using the info below.

[\(Use MX record instead\)](#)

ALIAS OR HOST NAME

@

DESTINATION OR POINTS TO ADDRESS

MS=ms85139411

TTL

3600

[Share these settings via email](#)

Verify domain

Verification will not succeed until you have configured your domain with your registrar as described above.

Verify

Set up on-premises and Azure groups and users

Now that the Azure AD is up and running, Contoso admins need to add employees to on-premises Active Directory groups that will synchronize to Azure Active Directory. They should use on-premises group names that match the names of resource groups in Azure. This makes it easier to identify matches for synchronization purposes.

Create resource groups in Azure

Azure resource groups gather Azure resources together. Using a resource group ID allows Azure to perform operations on the resources within the group.

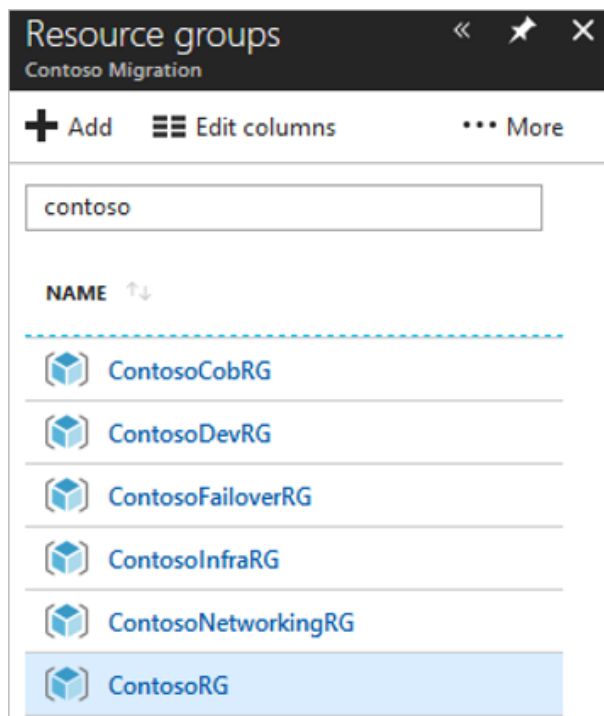
- An Azure subscription can have multiple resource groups, but a resource group can only exist within a single subscription.
- In addition, a single resource group can have multiple resources, but a resource can only belong to a single resource group.

Contoso admins set up Azure resource groups as summarized in the following table.

Resource group	Details
ContosoCobRG	<p>This group contains all resources related to continuity of business (COB). It includes vaults that Contoso will use for the Azure Site Recovery service, and the Azure Backup service.</p> <p>It will also include resources used for migration, including Azure Migrate and Azure Database Migration Service.</p>
ContosoDevRG	This group contains development and test resources.
ContosoFailoverRG	This group serves as a landing zone for failed over resources.
ContosoNetworkingRG	This group contains all networking resources.
ContosoRG	This group contains resources related to production apps and databases.

They create resource groups as follows:

1. In the Azure portal > **Resource groups**, they add a group.
2. For each group they specify a name, the subscription to which the group belongs, and the region.
3. Resource groups appear in the **Resource groups** list.

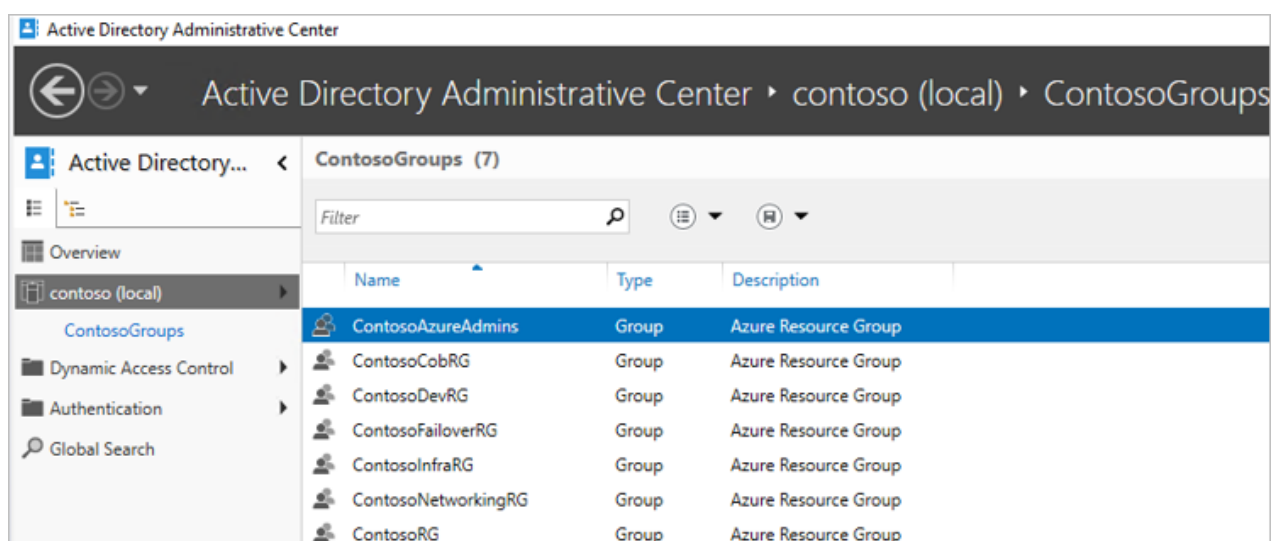


Scaling resource groups

In future, Contoso will add other resource groups based on needs. For example, they could define a resource group for each app or service, so that they can be managed and secured independently.

Create matching security groups on-premises

1. In the on-premises Active Directory, Contoso admins set up security groups with names that match the names of the Azure resource groups.



2. For management purposes, they create an additional group that will be added to all of the other groups. This group will have rights to all resource groups in Azure. A limited number of Global Admins will be added to this group.

Synchronize Active Directory

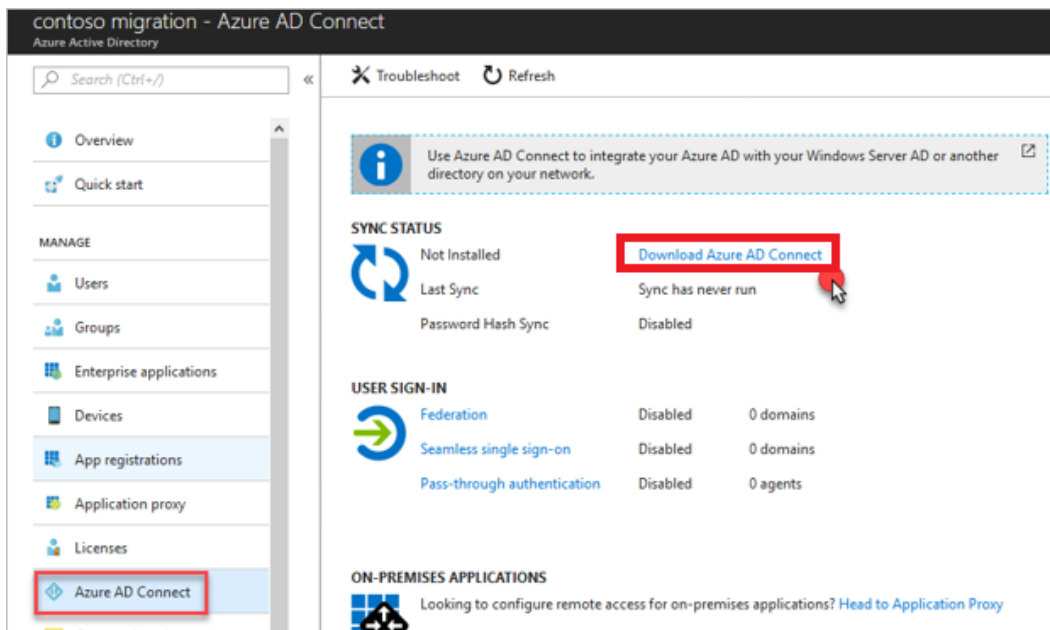
Contoso wants to provide a common identity for accessing resources on-premises and in the cloud. To do this, it will integrate the on-premises Active Directory with Azure AD. With this model:

- Users and organizations can take advantage of a single identity to access on-premises applications and cloud services such as Office 365, or thousands of other sites on the internet.
- Admins can use the groups in Active Directory to implement [Role Based Access Control \(RBAC\)](#) in Azure.

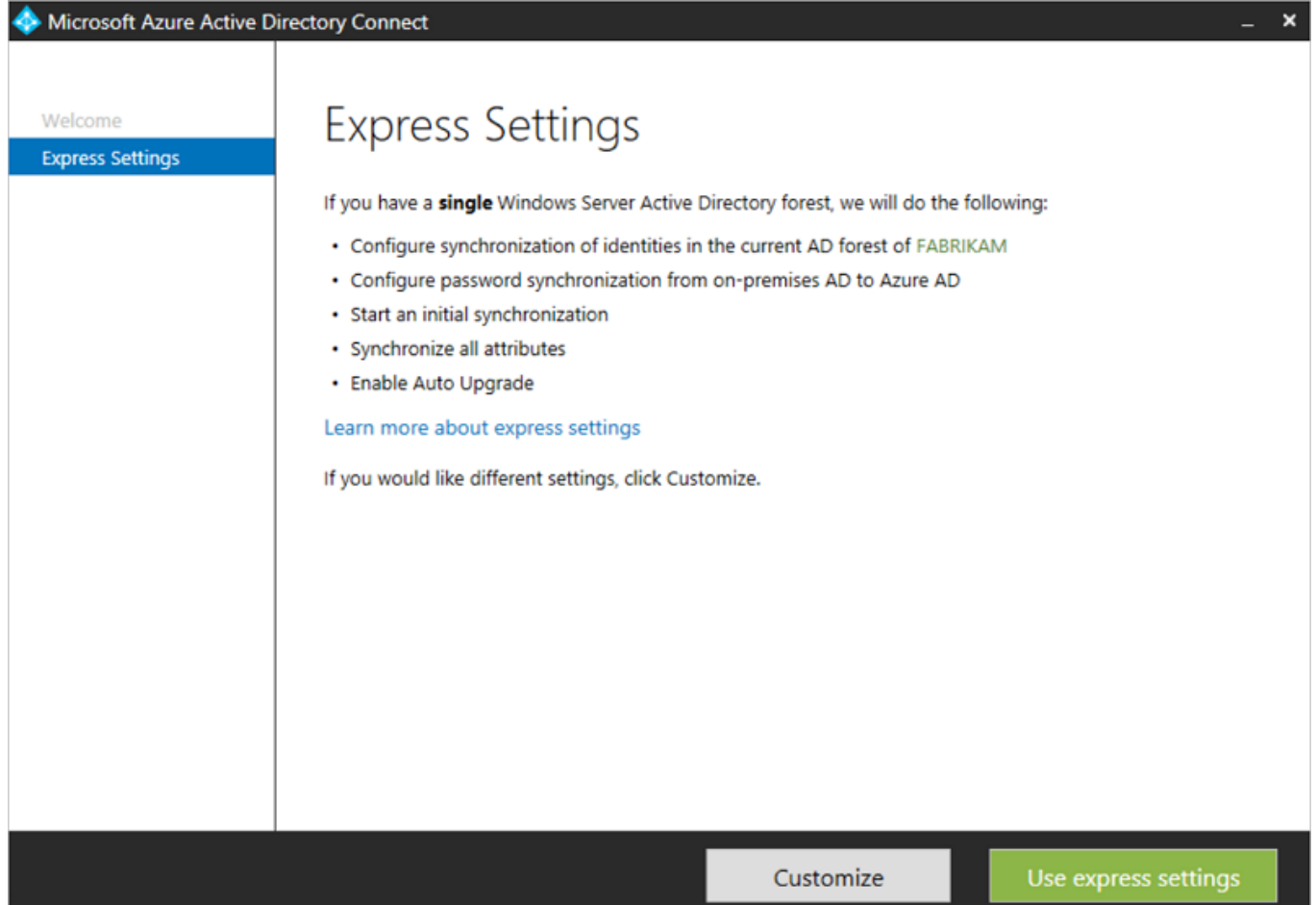
To facilitate integration, Contoso uses the [Azure AD Connect tool](#). When you install and configure the tool on a domain controller, it synchronizes the local on-premises Active Directory identities to Azure AD.

Download the tool

1. In the Azure portal, Contoso admins go to **Azure Active Directory** > **Azure AD Connect**, and download the latest version of the tool to the server they're using for synchronization.



2. They start the **AzureADConnect.msi** installation, with **Use express settings**. This is the most common installation, and can be used for a single-forest topology, with password hash synchronization for authentication.



3. In **Connect to Azure AD**, they specify the credentials for connecting to the Azure AD (in the form CONTOSO\admin or contoso.com\admin).

The screenshot shows the 'Connect to Azure AD' form. It has a title 'Connect to Azure AD' and a subtitle 'Enter your Azure AD global administrator credentials. ?'. There are two input fields: 'USERNAME' with the value 'contosoadmin@contosomigration.onmicrosoft.com' and 'PASSWORD' with a masked password represented by dots.

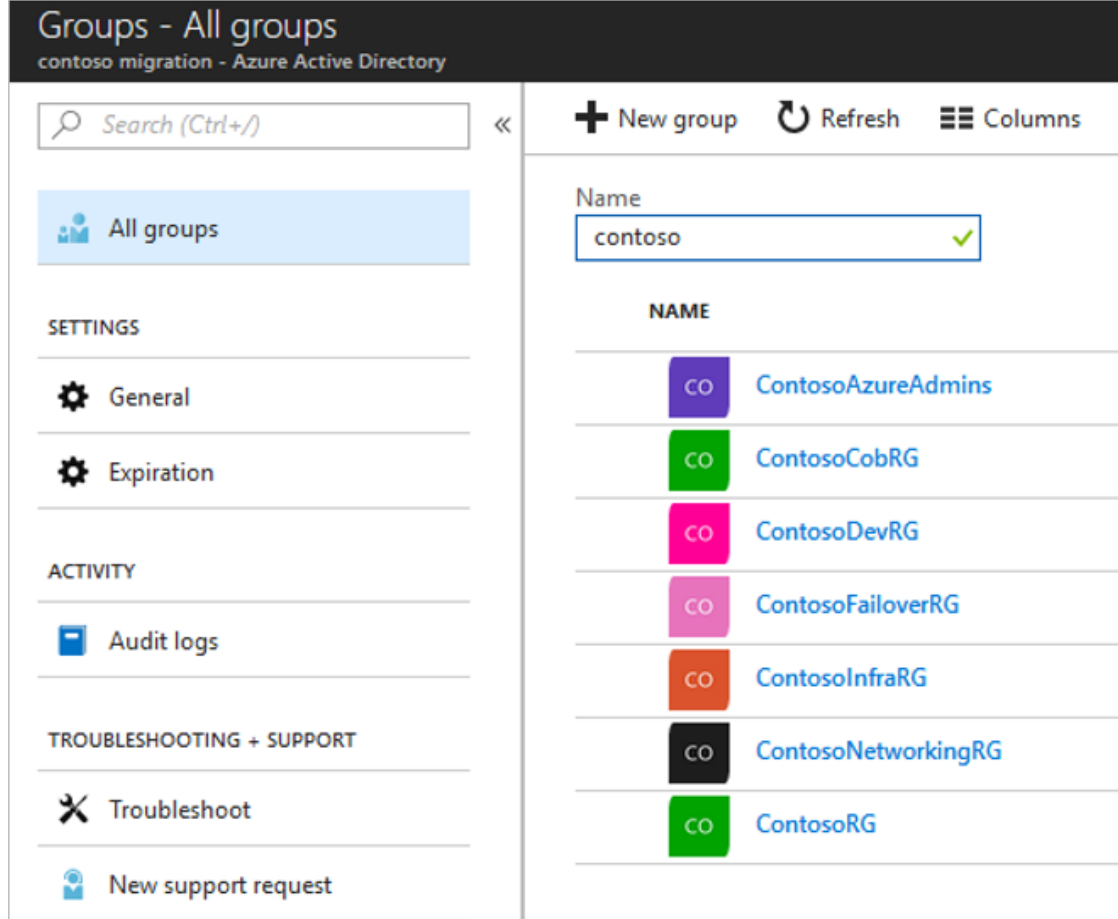
4. In **Connect to AD DS**, they specify credentials for the on-premises Active Directory.

The screenshot shows the 'Connect to AD DS' form. It has a title 'Connect to AD DS' and a subtitle 'Enter the Active Directory Domain Services enterprise administrator credentials: ?'. There are two input fields: 'USERNAME' with the value 'CONTOSO.COM\administrator' and 'PASSWORD' with a masked password represented by dots.

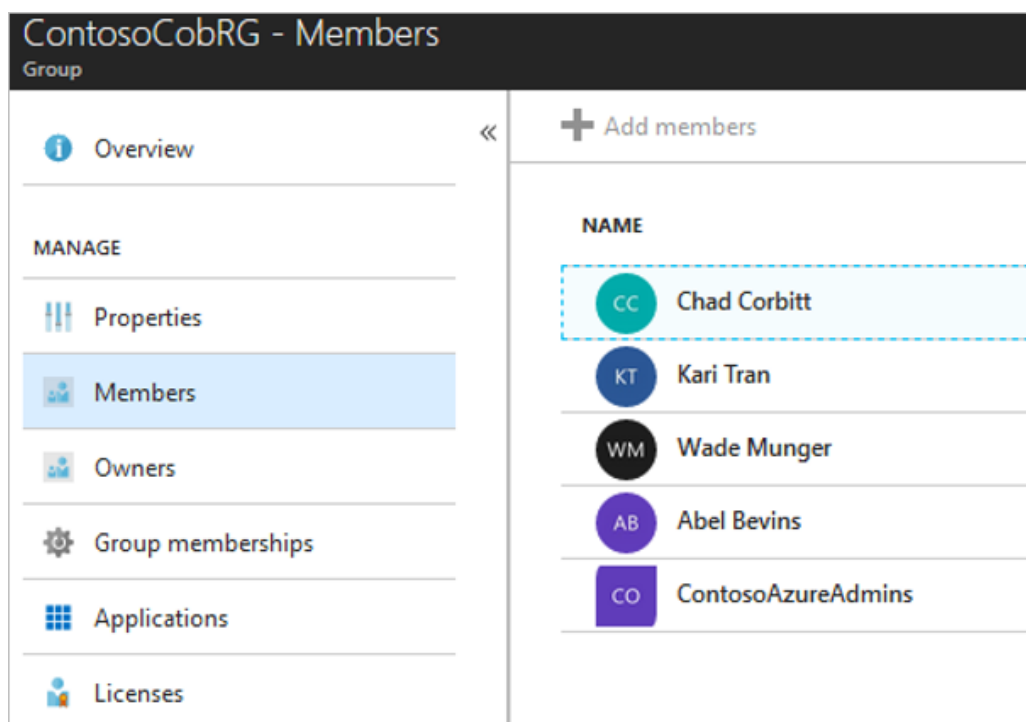
5. In **Ready to configure**, they select **Start the synchronization process when configuration completes** to start the sync immediately. Then they install.

Note that:

- Contoso has a direct connection to Azure. If your on-premises Active Directory is behind a proxy, read this [article](#).
- After the first synchronization, on-premises Active Directory objects are visible in the Azure AD directory.



- The Contoso IT team is represented in each group, based on its role.



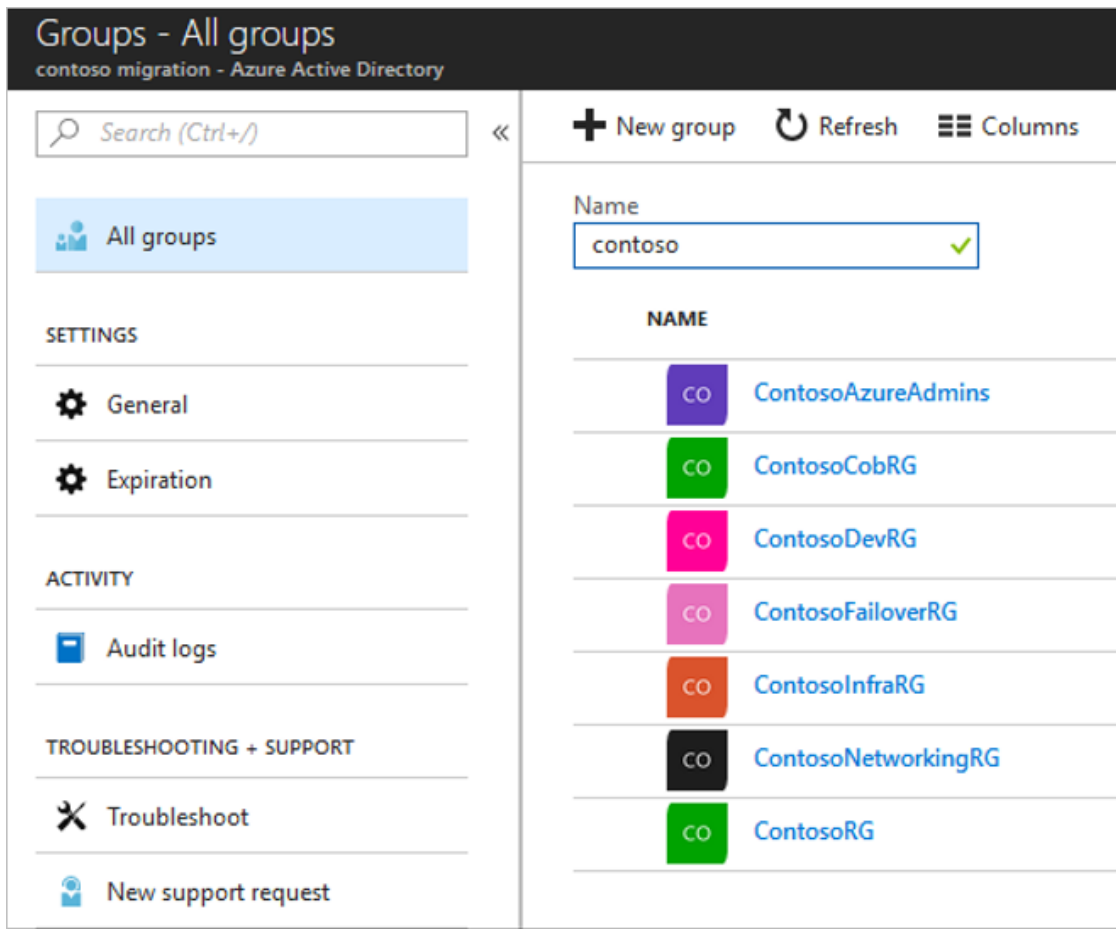
Set up RBAC

Azure [role-based access control \(RBAC\)](#) enables fine-grained access management for Azure. Using RBAC, you can grant only the amount of access that users need to perform tasks. You assign the appropriate RBAC role to users, groups, and applications at a scope level. The scope of a role assignment can be a subscription, a resource group, or a single resource.

Contoso admins now assigns roles to the Active Directory groups that they synchronized from on-premises.

1. In the **ControlCobRG** resource group, they select **Access control (IAM) > Add role assignment**.

2. In **Add role assignment** > **Role**, > **Contributor**, they select the **ContosoCobRG** group from the list. The group then appears in the **Selected members** list.
3. They repeat this with the same permissions for the other resource groups (except for **ContosoAzureAdmins**), by adding the Contributor permissions to the account that matches the resource group.
4. For the **ContosoAzureAdmins** group, they assign the **Owner** role.



Step 3: Design for resiliency

Set up regions

Azure resources are deployed within regions.

- Regions are organized into geographies, and data residency, sovereignty, compliance and resiliency requirements are honored within geographical boundaries.
- A region is composed of a set of datacenters. These datacenters are deployed within a latency-defined perimeter, and connected through a dedicated regional low-latency network.
- Each Azure region is paired with a different region for resiliency.
- Read about [Azure regions](#), and understand [how regions are paired](#).

Contoso has decided to go with the East US 2 (located in Virginia) as the primary region, and Central US (located in Iowa) as the secondary region. There are a couple of reasons for this:

- The Contoso datacenter is located in New York, and Contoso considered latency to the closest datacenter.
- The East US 2 region has all the service and products that Contoso needs to use. Not all Azure regions are the same in terms of the products and services available. You can review [Azure products by region](#).
- Central US is the Azure paired region for East US 2.

As it thinks about the hybrid environment, Contoso needs to consider how to build resilience and a disaster recovery strategy into the region design. Broadly, strategies range from a single-region deployment, which relies on Azure

platform features such as fault domains and regional pairing for resilience, through to a full Active-Active model in which cloud services and database are deployed and servicing users from two regions.

Contoso has decided to take a middle road. It will deploy apps and resources in a primary region, and keep a full copy of the infrastructure in the secondary region, so that it's ready to act as a full backup in case of complete app disaster, or regional failure.

Set up availability

Availability sets:

Availability sets help protect apps and data from a local hardware and networking outage within a datacenter.

- Availability sets distribute Azure VMs across different physical hardware within a datacenter.
- Fault domains represent underlying hardware with a common power source and network switch within the datacenter. VMs in an availability set are distributed across different fault domains to minimize outages caused by a single hardware or networking failure.
- Update domains represent underlying hardware that can undergo maintenance or be rebooted at the same time. Availability sets also distribute VMs across multiple update domains to ensure at least one instance will be running at all times.

Contoso will implement availability sets whenever VM workloads require high availability. [Learn more.](#)

Availability zones:

Availability zones help protect apps and data from failures affecting an entire datacenter within a region.

- Each availability zone represents a unique physical location within an Azure region.
- Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking.
- There's a minimum of three separate zones in all enabled regions.
- The physical separation of zones within a region protects applications and data from datacenter failures.

Contoso will deploy availability zones as apps call for scalability, high-availability, and resiliency. [Learn more.](#)

Set up backup

Azure Backup:

Azure Backup allows you to back up and restore Azure VM disks.

- Azure backup allows automated backups of VM disk images, stored in Azure storage.
- Backups are application consistent, ensuring backed up data is transactionally consistent and that applications will boot up post-restore.
- Azure Backup supports locally redundant storage (LRS) to replicate multiple copies of your backup data within a datacenter, in case of a local hardware failure.
- In the event of a regional outage, Azure Backup also supports geo-redundant storage (GRS), replicating your backup data to a secondary paired region.
- Azure Backup encrypts data in-transit using AES 256. Backed-up data at-rest is encrypted using [Storage Service Encryption \(SSE\)](#).

Contoso will use Azure Backup with GRS on all production VMs to ensure workload data is backed up and can be quickly restored in case of outage or other disruption. [Learn more.](#)

Set up disaster recovery

Azure Site Recovery:

Azure Site Recovery helps ensure business continuity by keeping business apps and workloads running during regional outages.

- Azure Site Recovery continually replicates Azure VMs from a primary to a secondary region, ensuring functional copies in both locations.
- In the event of an outage in the primary region, your application or service fails over to using VMs instances replicated in the secondary region, minimizing potential disruption.
- When operations return to normal, your applications or services can fail back to VMs in the primary region.

Contoso will implement Azure Site Recovery for all production VMs used in mission-critical workloads, ensuring minimal disruption during an outage in the primary region. [Learn more](#)

Step 4: Design a network infrastructure

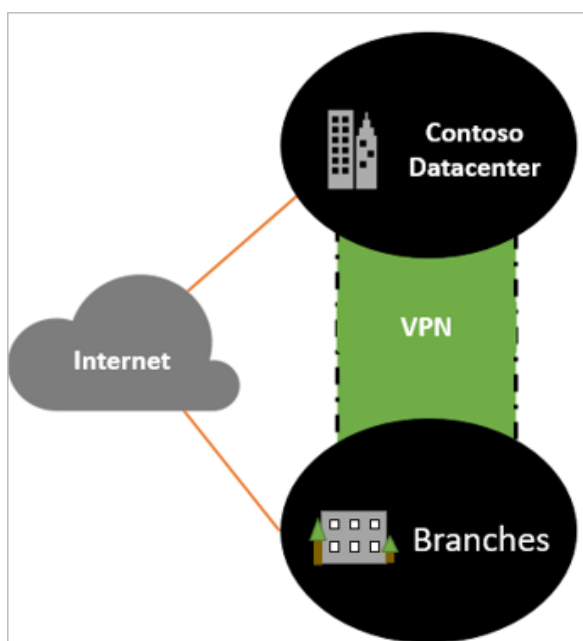
With the regional design in place, Contoso is ready to consider a networking strategy. It needs to think about how the on-premises datacenter and Azure connect and communicate with each other, and how to design the network infrastructure in Azure. Specifically Contoso needs to:

- **Plan hybrid network connectivity.** Figure out how it's going to connect networks across on-premises and Azure.
- **Design an Azure network infrastructure.** Decide how it will deploy networks over regions. How will networks communicate within the same region, and across regions?
- **Design and set up Azure networks.** Set up Azure networks and subnets, and decide what will reside in them.

Plan hybrid network connectivity

Contoso considered a [number of architectures](#) for hybrid networking between Azure and the on-premises datacenter. [Read more](#) about comparing options.

As a reminder, the Contoso on-premises network infrastructure currently consists of the datacenter in New York, and local branches in the eastern portion of the US. All locations have a business class connection to the internet. Each of the branches is then connected to the datacenter via an IPsec VPN tunnel over the internet.



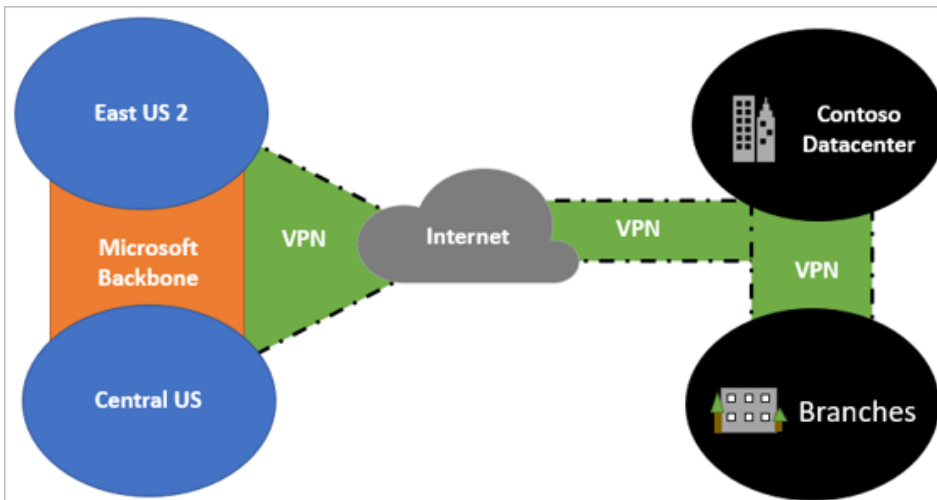
Here's how Contoso decided to implement hybrid connectivity:

1. Set up a new site-to-site VPN connection between the Contoso datacenter in New York and the two Azure regions in East US 2 and Central US.
2. Branch office traffic bound for Azure virtual networks will route through the main Contoso datacenter.

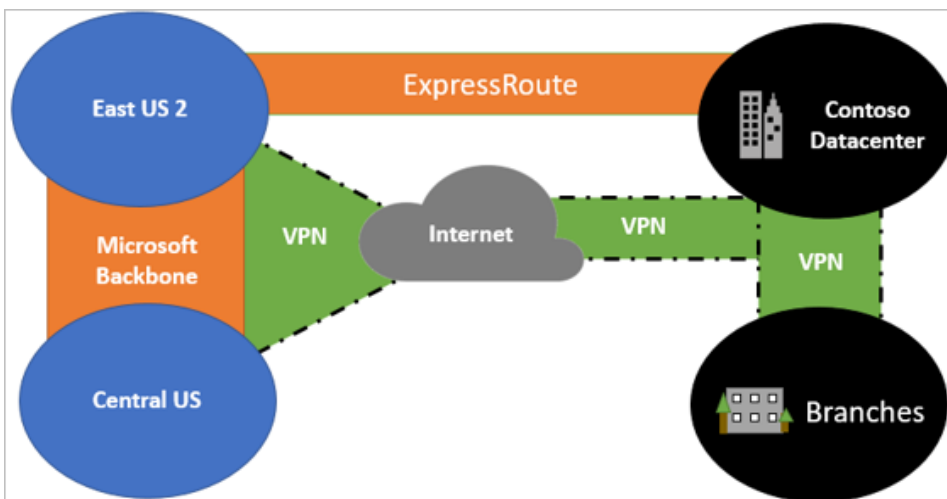
3. As Contoso scales up Azure deployment, it will establish an ExpressRoute connection between the datacenter and the Azure regions. When this happens, Contoso will retain the VPN site-to-site connection for failover purposes only.

- [Learn more](#) about choosing between a VPN and ExpressRoute hybrid solution.
- Verify [ExpressRoute locations and support](#).

VPN only:



VPN and ExpressRoute:



Design the Azure network infrastructure

It's critical that Contoso puts networks in place in a way that makes the hybrid deployment secure and scalable. To do this, Contoso are taking a long-term approach, and are designing virtual networks (VNets) to be resilient and enterprise ready. [Learn more](#) about planning VNets.

To connect the two regions, Contoso has decided to implement a hub-to-hub network model:

- Within each region, Contoso will use a hub and spoke model.
- To connect networks and hubs, Contoso will use Azure network peering.

Network peering

Azure provides network peering to connect VNets and hubs. Global peering allows connections between VNets/hubs in different regions. Local peering connects VNets in the same region. VNet peering provides several advantages:

- Network traffic between peered VNets is private.
- Traffic between the VNets is kept on the Microsoft backbone network. No public internet, gateways, or encryption is required in the communication between the VNets.

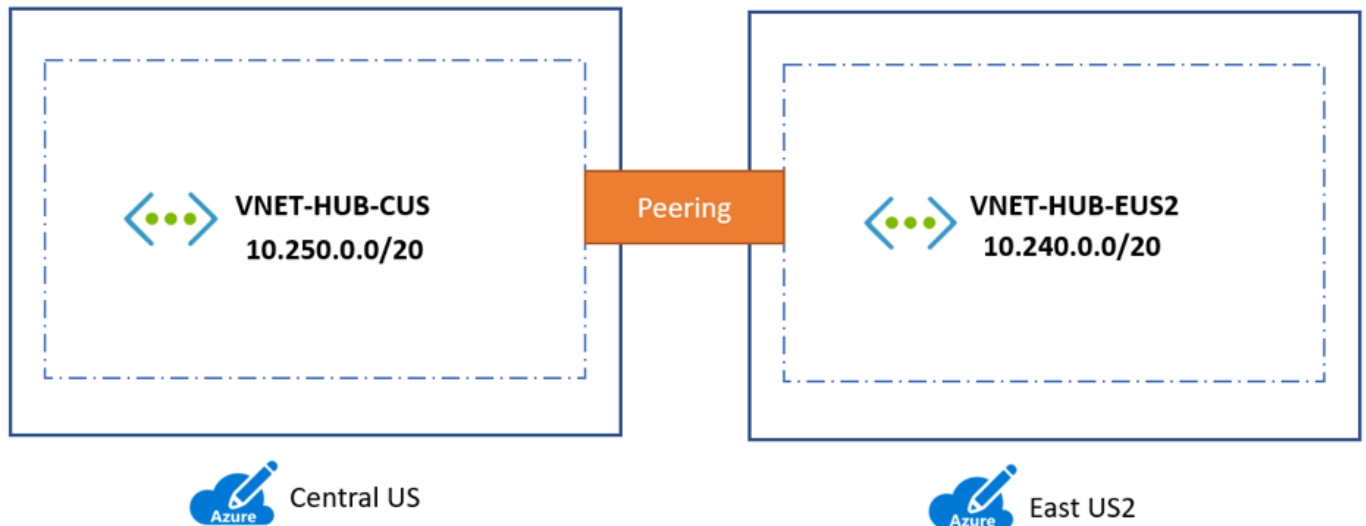
- Peering provides a default, low-latency, high-bandwidth connection between resources in different VNets.

[Learn more](#) about network peering.

Hub-to-hub across regions

Contoso will deploy a hub in each region. A hub is a virtual network (VNet) in Azure that acts as a central point of connectivity to your on-premises network. The hub VNets will connect to each other using global VNet peering. Global VNet peering connects VNets across Azure regions.

- The hub in each region is peered to its partner hub in the other region.
- The hub is peered to every network in its region, and can connect to all network resources.



Hub and spoke model within a region

Within each region, Contoso will deploy VNets for different purposes, as spoke networks from the region hub. VNets within a region use peering to connect to their hub, and to each other.

Design the hub network

Within the hub and spoke model that Contoso has chosen, it needs to think about how traffic from the on-premises datacenter, and from the internet, will be routed. Here's how Contoso has decided to handle routing for both the East US 2 and Central US hubs:

- Contoso is designing a network known as "reverse c", as this is the path that the packets follow from the inbound to outbound network.
- The network architecture has two boundaries, an untrusted front-end perimeter zone and a back-end trusted zone.
- A firewall will have a network adapter in each zone, controlling access to trusted zones.
- From the internet:
 - Internet traffic will hit a load-balanced public IP address on the perimeter network.
 - This traffic is routed through the firewall, and subject to firewall rules.
 - After network access controls are implemented, traffic will be forwarded to the appropriate location in the trusted zone.
 - Outbound traffic from the VNet will be routed to the internet using user-defined routes. The traffic is forced through the firewall, and inspected in line with Contoso policies.
- From the Contoso datacenter:
 - Incoming traffic over VPN site-to-site (or ExpressRoute) hits the public IP address of the Azure VPN gateway.
 - Traffic is routed through the firewall and subject to firewall rules.

- After applying firewall rules, traffic is forwarded to an internal load balancer (Standard SKU) on the trusted internal zone subnet.
- Outbound traffic from the trusted subnet to the on-premises datacenter over VPN is routed through the firewall, and rules applied, before going over the VPN site-to-site connection.

Design and set up Azure networks

With a network and routing topology in place, Contoso is ready to set up Azure networks and subnets.

- Contoso will implement a Class A private network in Azure (0.0.0.0 to 127.255.255.255). This works, since on-premises it currently has a Class B private address space 172.160.0/16 so Contoso can be sure there won't be any overlap between address ranges.
- It's going to deploy VNets in the primary and secondary regions.
- Contoso will use a naming convention that includes the prefix **VNET** and the region abbreviation **EUS2** or **CUS**. Using this standard, the hub networks will be named **VNET-HUB-EUS2** (East US 2), and **VNET-HUB-CUS** (Central US).
- Contoso doesn't have an [IPAM solution](#), so it needs to plan for network routing without NAT.

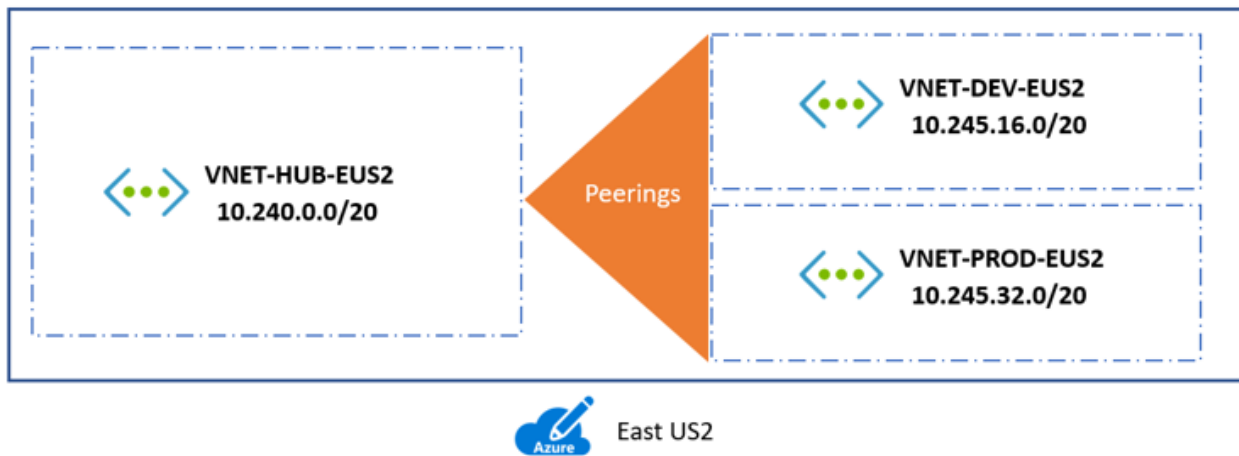
Virtual networks in East US 2

East US 2 is the primary region that Contoso will use to deploy resources and services. Here's how Contoso will architect networks within it:

- **Hub:** The hub VNet in East US 2 is the central point of primary connectivity to the on-premises datacenter.
- **VNets:** Spoke VNets in East US 2 can be used to isolate workloads if required. In addition to the Hub VNet, Contoso will have two spoke VNets in East US 2:
 - **VNET-DEV-EUS2.** This VNet will provide the development and test team with a fully functional network for dev projects. It will act as a production pilot area, and will rely on the production infrastructure to function.
 - **VNET-PROD-EUS2.** Azure IaaS production components will be located in this network.
 - Each VNet will have its own unique address space, with no overlap. Contoso intend to configure routing without requiring NAT.
- **Subnets:**
 - There will be a subnet in each network for each app tier
 - Each subnet in the Production network will have a matching subnet in the Development VNet.
 - In addition, the Production network has a subnet for domain controllers.

VNets in East US 2 are summarized in the following table.

VNet	Range	Peer
VNET-HUB-EUS2	10.240.0.0/20	VNET-HUB-CUS2, VNET-DEV-EUS2, VNET-PROD-EUS2
VNET-DEV-EUS2	10.245.16.0/20	VNET-HUB-EUS2
VNET-PROD-EUS2	10.245.32.0/20	VNET-HUB-EUS2, VNET-PROD-CUS



Subnets in the East US 2 Hub network (VNET-HUB-EUS2)

Subnet/zone	CIDR	**Usable IP addresses
IB-UntrustZone	10.240.0.0/24	251
IB-TrustZone	10.240.1.0/24	251
OB-UntrustZone	10.240.2.0/24	251
OB-TrustZone	10.240.3.0/24	251
GatewaySubnets	10.240.10.0/24	251

Subnets in the East US 2 Dev network (VNET-DEV-EUS2)

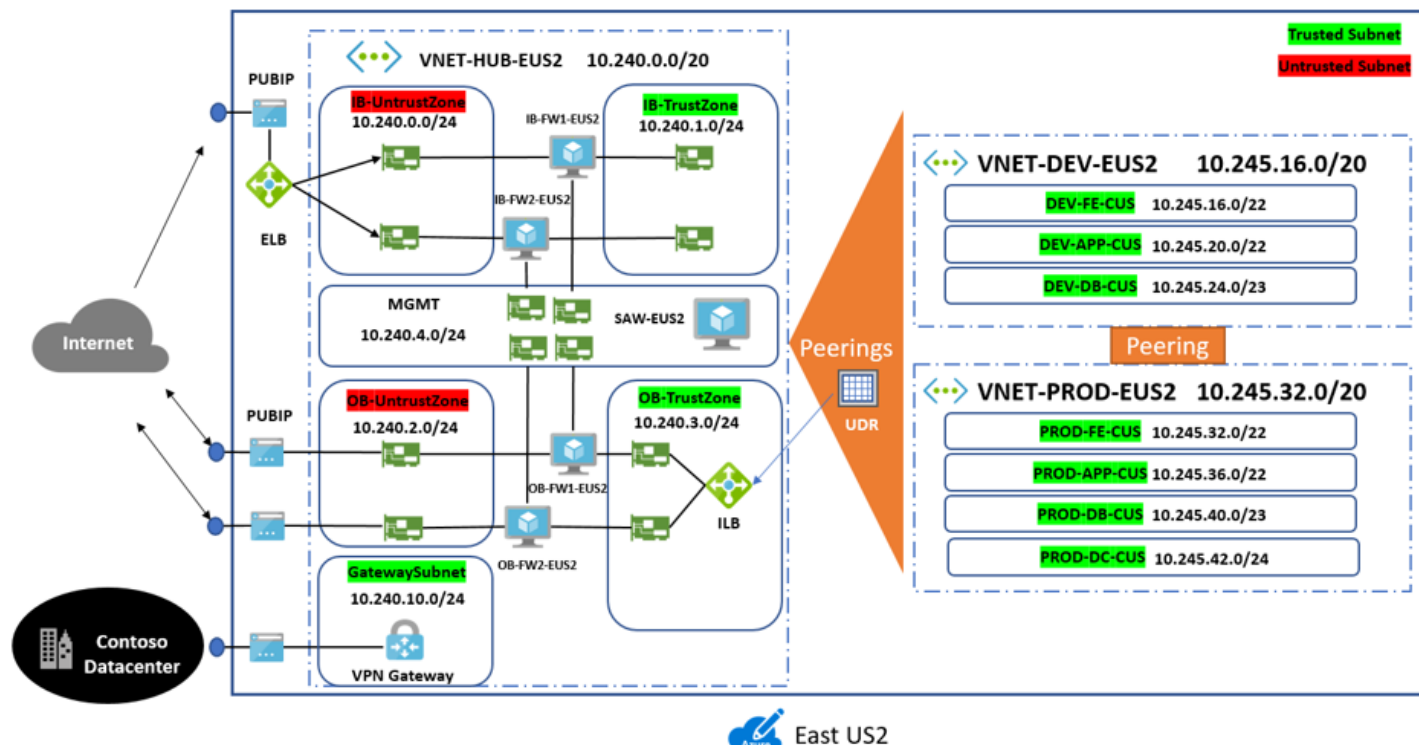
The Development VNet is used by the development team as a production pilot area. It has three subnets.

Subnet	CIDR	Addresses	In subnet
DEV-FE-EUS2	10.245.16.0/22	1019	Front-ends/web tier VMs
DEV-APP-EUS2	10.245.20.0/22	1019	App-tier VMs
DEV-DB-EUS2	10.245.24.0/23	507	Database VMs

Subnets in the East US 2 Production network (VNET-PROD-EUS2)

Azure IaaS components are located in the Production network. Each app tier has its own subnet. Subnets match those in the Development network, with the addition of a subnet for domain controllers.

Subnet	CIDR	Addresses	In subnet
PROD-FE-EUS2	10.245.32.0/22	1019	Front-ends/web tier VMs
PROD-APP-EUS2	10.245.36.0/22	1019	App-tier VMs
PROD-DB-EUS2	10.245.40.0/23	507	Database VMs
PROD-DC-EUS2	10.245.42.0/24	251	Domain controller VMs



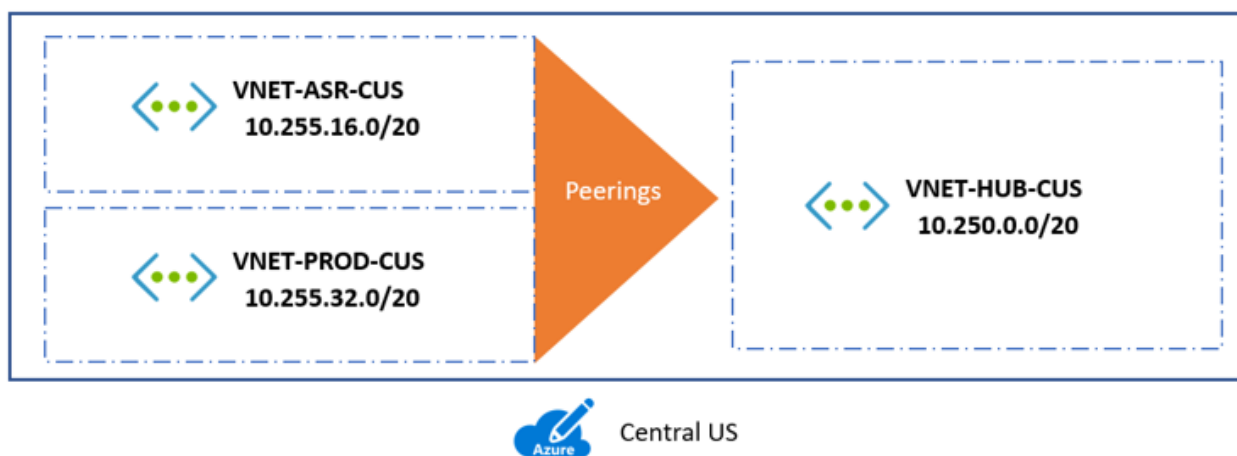
Virtual networks in Central US (secondary region)

Central US is Contoso's secondary region. Here's how Contoso will architect networks within it:

- **Hub:** The hub VNet in East US 2 is the central point of connectivity to the on-premises datacenter, and the spoke VNets in East US 2 can be used to isolate workloads if required, managed separately from other spokes.
- **VNets:** Contoso will have two VNets in Central US:
 - VNET-PROD-CUS. This VNet is a production network, similar to VNET-PROD_EUS2.
 - VNET-ASR-CUS. This VNet will act as a location in which VMs are created after failover from on-premises, or as a location for Azure VMs that are failed over from the primary to the secondary region. This network is similar to the production networks, but without any domain controllers on it.
 - Each VNet in the region will have its own address space, with no overlap. Contoso will configure routing without NAT.
- **Subnets:** The subnets will be architected in a similar way to those in East US 2. The exception is that Contoso doesn't need a subnet for domain controllers.

The VNets in Central US are summarized in the following table.

VNet	Range	Peer
VNET-HUB-CUS	10.250.0.0/20	VNET-HUB-EUS2, VNET-ASR-CUS, VNET-PROD-CUS
VNET-ASR-CUS	10.255.16.0/20	VNET-HUB-CUS, VNET-PROD-CUS
VNET-PROD-CUS	10.255.32.0/20	VNET-HUB-CUS, VNET-ASR-CUS, VNET-PROD-EUS2



Subnets in the Central US Hub network (VNET-HUB-CUS)

Subnet	CIDR	Usable IP addresses
IB-UntrustZone	10.250.0.0/24	251
IB-TrustZone	10.250.1.0/24	251
OB-UntrustZone	10.250.2.0/24	251
OB-TrustZone	10.250.3.0/24	251
GatewaySubnet	10.250.2.0/24	251

Subnets in the Central US Production network (VNET-PROD-CUS)

In parallel to the production network in the primary East US 2 region, there's a production network in the secondary Central US region.

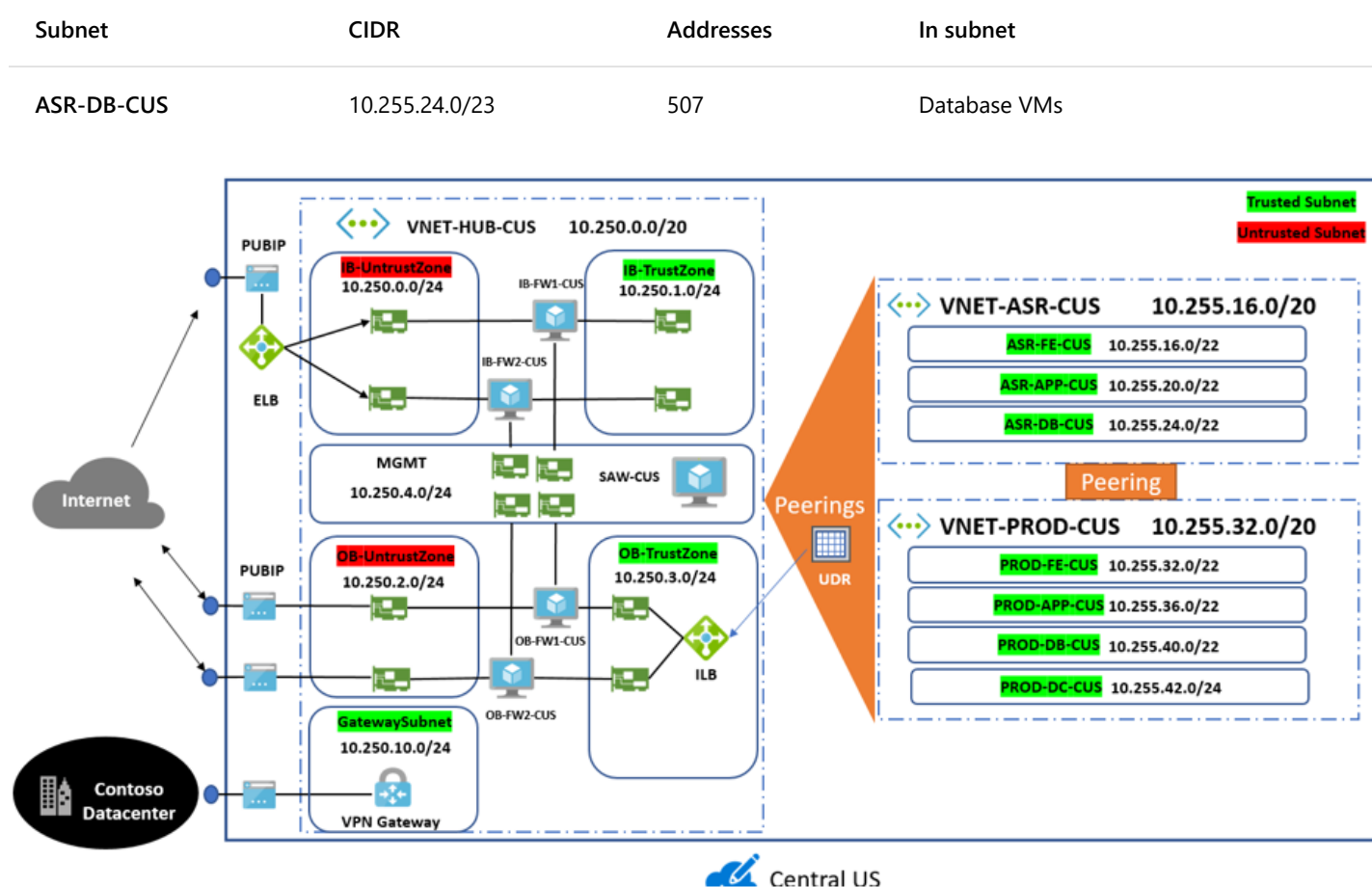
Subnet	CIDR	Addresses	In subnet
PROD-FE-CUS	10.255.32.0/22	1019	Front-ends/web-tier VMs
PROD-APP-CUS	10.255.36.0/22	1019	App-tier VMs
PROD-DB-CUS	10.255.40.0/23	507	Database VMs
PROD-DC-CUS	10.255.42.0/24	251	Domain controller VMs

Subnets in the Central US failover/recovery network in Central US (VNET-ASR-CUS)

The VNET-ASR-CUS network is used for purposes of failover between regions. Site Recovery will be used to replicate and fail over Azure VMs between the regions. It also functions as a Contoso datacenter to Azure network for protected workloads that remain on-premises, but fail over to Azure for disaster recovery.

VNET-ASR-CUS is the same basic subnet as the production VNet in East US 2, but without the need for a domain controller subnet.

Subnet	CIDR	Addresses	In subnet
ASR-FE-CUS	10.255.16.0/22	1019	Front-ends/web-tier VMs
ASR-APP-CUS	10.255.20.0/22	1019	App-tier VMs



Configure peered connections

The hub in each region will be peered to the hub in the other region, and to all VNets within the hub region. This allows for hubs to communicate, and to view all VNets within a region. Note that:

- Peering creates a two-sided connection. One from the initiating peer on the first VNet, and another one on the second VNet.
- In a hybrid deployment, traffic that passes between peers needs to be visible from the VPN connection between the on-premises datacenter and Azure. To enable this, there are some specific settings that must be set on peered connections.

For any connections from spoke VNets through the hub to the on-premises datacenter, Contoso needs to allow traffic to be forwarded, and transverse the VPN gateways.

Domain controller

For the domain controllers in the VNET-PROD-EUS2 network, Contoso wants traffic to flow both between the EUS2 hub/production network, and over the VPN connection to on-premises. To do this it Contoso admins must allow the following:

1. **Allow forwarded traffic** and **Allow gateway transit configurations** on the peered connection. In our example this would be the VNET-HUB-EUS2 to VNET-PROD-EUS2 connection.

VNET-HUB-EUS2-to-VNET-PROD-EUS2
VNET-HUB-EUS2

Save Discard Delete

Name
VNET-HUB-EUS2-to-VNET-PROD-EUS2

Peering status
Connected

Provisioning state
Succeeded

Peer details

Address space
10.245.32.0/20

Virtual network
VNET-PROD-EUS2

Configuration

Allow virtual network access

Disabled Enabled

☒ Allow forwarded traffic

☒ Allow gateway transit

☐ Use remote gateways

2. **Allow forwarded traffic** and **Use remote gateways** on the other side of the peering, on the VNET-PROD-EUS2 to VNET-HUB-EUS2 connection.

VNET-PROD-EUS2-to-VNET-HUB-EUS2
VNET-PROD-EUS2

Save Discard Delete

Name
VNET-PROD-EUS2-to-VNET-HUB-EUS2

Peering status
Connected

Provisioning state
Succeeded

Peer details

Address space
10.240.0.0/20

Virtual network
VNET-HUB-EUS2

Configuration

Allow virtual network access

Disabled Enabled

☒ Allow forwarded traffic

☐ Allow gateway transit

☒ Use remote gateways

3. On-premises they'll set up a static route that directs the local traffic to route across the VPN tunnel to the VNet. The configuration would be completed on the gateway that provides the VPN tunnel from Contoso to Azure. They use RRAS for this.

IPv4 Static Route ? X

Interface: VNET-HUB-EUS2

Destination: 10 . 245 . 0 . 0

Network mask: 255 . 255 . 0 . 0

Gateway: . . .

Metric: 30

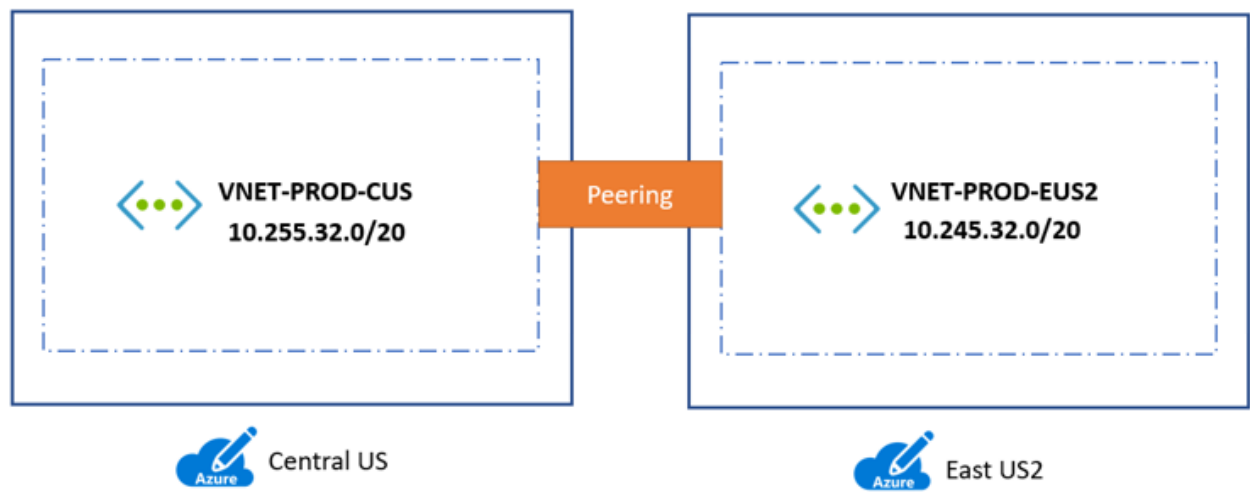
☐ Use this route to initiate demand-dial connections

OK Cancel

Production networks

A spoked peer network can't see a spoked peer network in another region via a hub.

For Contoso's production networks in both regions to see each other, Contoso admins need to create a direct peered connection for VNET-PROD-EUS2 and VENT-PROD-CUS.

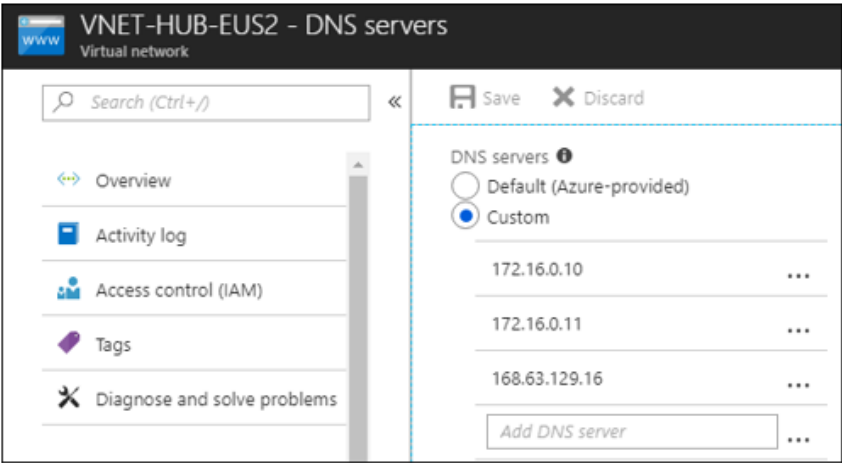


Set up DNS

When you deploy resources in virtual networks, you have a couple of choices for domain name resolution. You can use name resolution provided by Azure, or provide DNS servers for resolution. The type of name resolution you use depends on how your resources need to communicate with each other. Get [more information](#) about the Azure DNS service.

Contoso admins have decided that the Azure DNS service isn't a good choice in the hybrid environment. Instead, they will use the on-premises DNS servers.

- Since this is a hybrid network all the VMs on-premises and in Azure need to be able to resolve names to function properly. This means that custom DNS settings must be applied to all the VNETs.
- Contoso currently has DCs deployed in the Contoso datacenter and at the branch offices. The primary DNS servers are CONTOSODC1(172.16.0.10) and CONTOSODC2(172.16.0.1)
- When the VNETs are deployed, the on-premises domain controllers will be set to be used as DNS servers in the networks.
- To configure this, when using custom DNS on the VNet, Azure's recursive resolvers IP address (such as 168.63.129.16) must be added to the DNS list. To do this, Contoso configures DNS server settings on each VNet. For example, the custom DNS settings for the VNET-HUB-EUS2 network would be as follows:



In addition to the on-premises domain controllers, Contoso are going to implement four more to support the Azure networks, two for each region. Here's what Contoso will deploy in Azure.

Region	DC	VNet	Subnet	IP address
--------	----	------	--------	------------

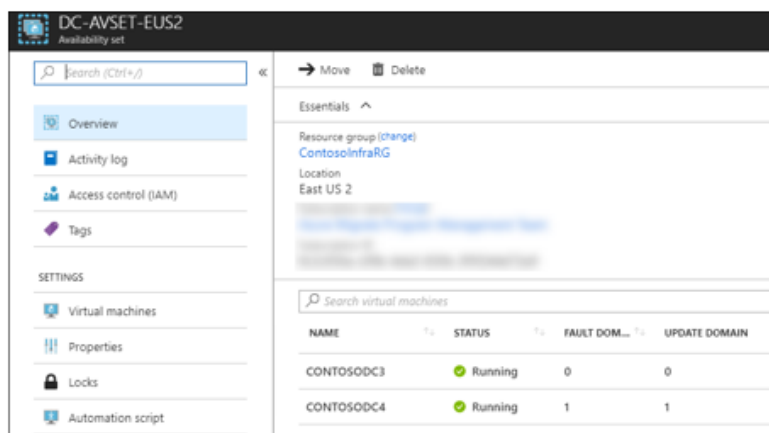
Region	DC	VNet	Subnet	IP address
EUS2	CONTOSODC3	VNET-PROD-EUS2	PROD-DC-EUS2	10.245.42.4
EUS2	CONTOSODC4	VNET-PROD-EUS2	PROD-DC-EUS2	10.245.42.5
CUS	CONTOSODC5	VNET-PROD-CUS	PROD-DC-CUS	10.255.42.4
CUS	CONTOSODC6	VNET-PROD-CUS	PROD-DC-CUS	10.255.42.4

After deploying the on-premises domain controllers, Contoso needs to update the DNS settings on networks on either region to include the new domain controllers in the DNS server list.

Set up domain controllers in Azure

After updating network settings, Contoso admins are ready to build out the domain controllers in Azure.

1. In the Azure portal, they deploy a new Windows Server VM to the appropriate VNet.
2. They create availability sets in each location for the VM. Availability sets do the following:
 - Ensure that the Azure fabric separates the VMs into different infrastructures in the Azure Region.
 - Allows Contoso to be eligible for the 99.95% SLA for VMs in Azure. [Learn more.](#)



3. After the VM is deployed, they open the network interface for the VM. They set the private IP address to static, and specify a valid address.

ipconfig1
contosodc3633

Save Discard

Public IP address settings

Public IP address

Disabled Enabled

Private IP address settings

Virtual network/subnet

VNET-PROD-EUS2/PROD-DC-EUS2

Assignment




Dynamic Static

* IP address

10.245.42.4

4. Now, they attach a new data disk to the VM. This disk contains the Active Directory database, and the sysvol share.

- The size of the disk will determine the number of IOPS that it supports.
- Over time the disk size might need to increase as the environment grows.
- The drive shouldn't be set to Read/Write for host caching. Active Directory databases don't support this.

<input type="checkbox"/>		CONTOSODC3	Virtual machine
<input type="checkbox"/>		CONTOSODC3_OsDisk_...	Disk
<input type="checkbox"/>		CONTOSODC3-Data-Disk	Disk

5. After the disk is added, they connect to the VM over Remote Desktop, and open Server Manager.

6. Then in **File and Storage Services**, they run the New Volume Wizard, ensuring that the drive is given the letter F: or above on the local VM.

New Volume Wizard

Confirm selections

Before You Begin
Server and Disk
Size
Drive Letter or Folder
File System Settings
Confirmation
Results

Confirm that the following are the correct settings, and then click Create.

VOLUME LOCATION

Server: CONTOSODC3
Disk: Disk 2
Free space: 64.0 GB

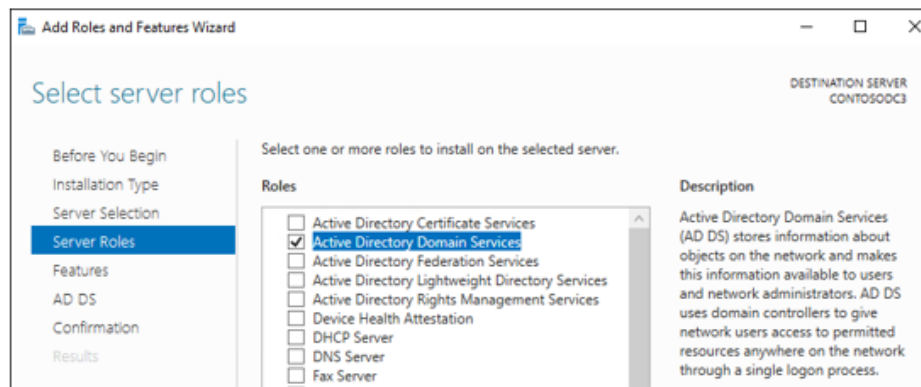
VOLUME PROPERTIES

Volume size: 64.0 GB
Drive letter or folder: F:\
Volume label: Data

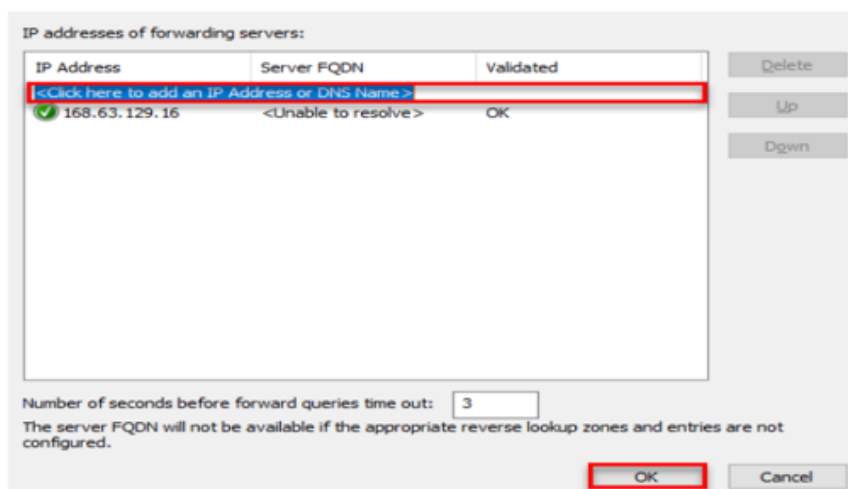
FILE SYSTEM SETTINGS

File system: NTFS
Short file name creation: Disabled
Allocation unit size: Default

7. In Server Manager, they add the **Active Directory Domain Services** role. Then, they configure the VM as a domain controller.



8. After the VM is configured as a DC and rebooted, they open DNS Manager and configure the Azure DNS resolver as a forwarder. This allows the DC to forward DNS queries it can't resolve in the Azure DNS.

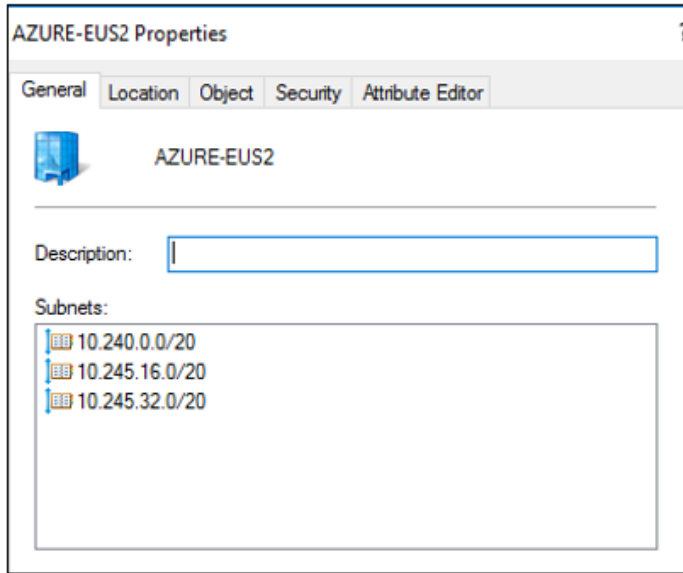


9. Now, they update the custom DNS settings for each VNet with the appropriate domain controller for the VNet region. They include on-premises DCs in the list.

Set up Active Directory

Active Directory is a critical service in networking, and must be configured correctly. Contoso admins will build Active Directory sites for the Contoso datacenter, and for the EUS2 and CUS regions.

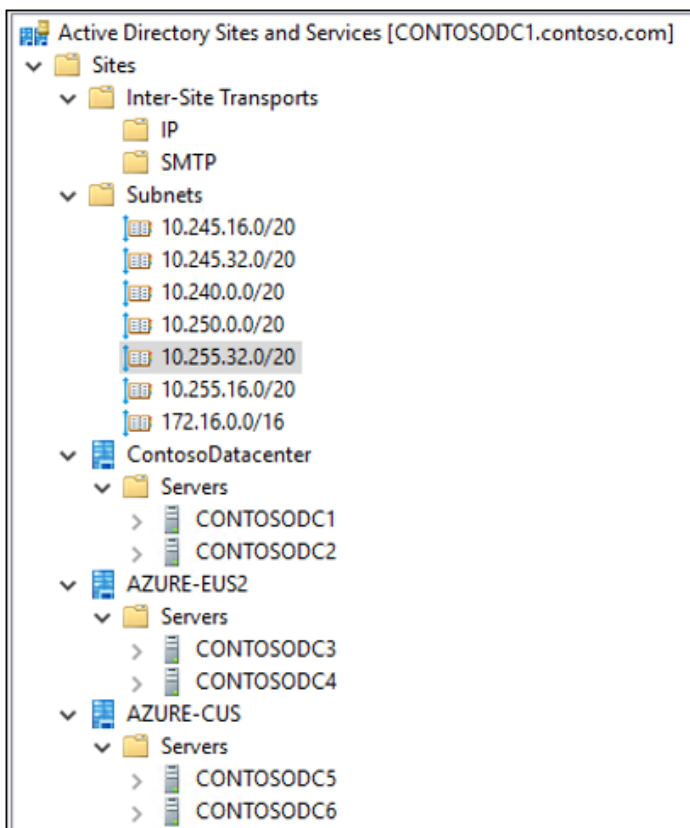
1. They create two new sites (AZURE-EUS2, and AZURE-CUS) along with the datacenter site (ContosoDatacenter).
2. After creating the sites, they create subnets in the sites, to match the VNets and datacenter.



3. Then, they create two site links to connect everything. The domain controllers should then be moved to their location.

Name	Type
ContosoDatacenter-To-Azure-CUS	Site Link
ContosoDatacenter-To-Azure-EUS2	Site Link

4. After everything is configured, the Active Directory replication topology is in place.



5. With everything complete, a list of the domain controllers and sites are shown in the on-premises Active Directory Administrative Center.

Active Directory Administrative Center ▸ contoso (local) ▸ Domain Controllers					
Active Directory...		Domain Controllers (6)			
Filter					
	Name	Site	Type	Domain Controller...	Description
CONTOSODC1	ContosoDatacenter	Domain Controller	Global Catalog		
CONTOSODC2	ContosoDatacenter	Domain Controller	Global Catalog		
CONTOSODC3	AZURE-EUS2	Domain Controller	Global Catalog		
CONTOSODC4	AZURE-EUS2	Domain Controller	Global Catalog		
CONTOSODC5	AZURE-CUS	Domain Controller	Global Catalog		
CONTOSODC6	AZURE-CUS	Domain Controller	Global Catalog		

Step 5: Plan for governance

Azure provides a range of governance controls across services and the Azure platform. [Read more](#) for a basic understanding of options.

As they configure identity and access control, Contoso has already begun to put some aspects of governance and security in place. Broadly, there are three areas it needs to consider:

- **Policy:** Azure Policy applies and enforces rules and effects over your resources, so that resources stay compliant with corporate requirements and SLAs.
- **Locks:** Azure allows you to lock subscriptions, resource groups, and other resources, so that they can only be modified by those with authority to do so.
- **Tags:** Resources can be controlled, audited, and managed with tags. Tags attach metadata to resources, providing information about resources or owners.

Set up policies

The Azure Policy service evaluates your resources, scanning for those not compliant with the policy definitions you have in place. For example, you might have a policy that only allows certain types of VMs, or requires resources to have a specific tag.

Policies specify a policy definition, and a policy assignment specifies the scope in which a policy should be applied. The scope can range from a management group to a resource group. [Learn](#) about creating and managing policies.

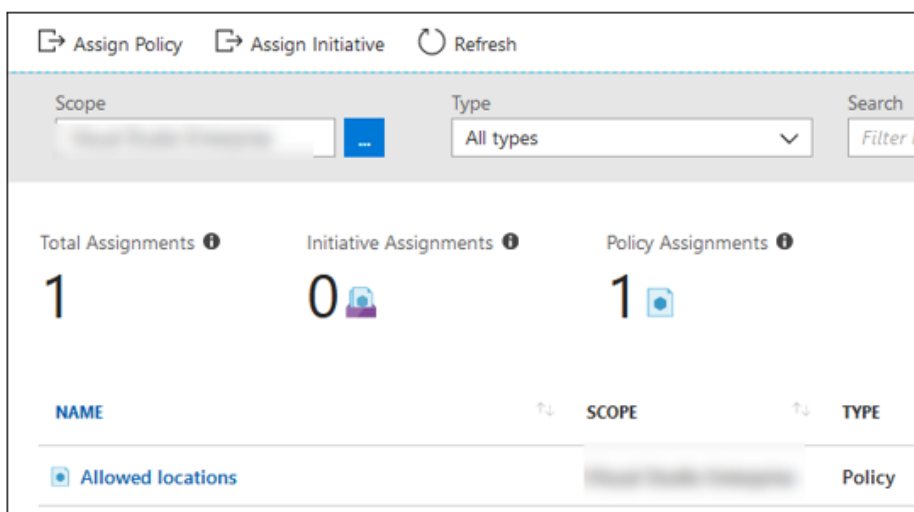
Contoso wants to get started with a couple of policies:

- It wants a policy to ensure that resources can only be deployed in the EUS2 and CUS regions.
- It wants to limit VM SKUs to approved SKUs only. The intention is to ensure that expensive VM SKUs aren't used.

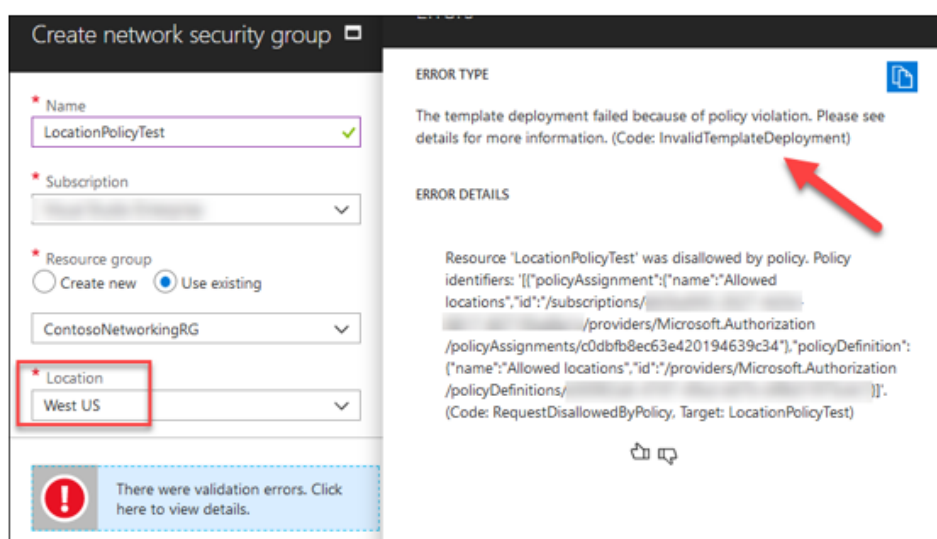
Limit resources to regions

Contoso uses the built-in policy definition **Allowed locations** to limit resource regions.

1. In the Azure portal, select **All services**, and search for **Policy**.
2. Select **Assignments** > **Assign policy**.
3. In the policy list, select **Allowed locations**.
4. Set **Scope** to the name of the Azure subscription, and select the two regions in the allowed list.

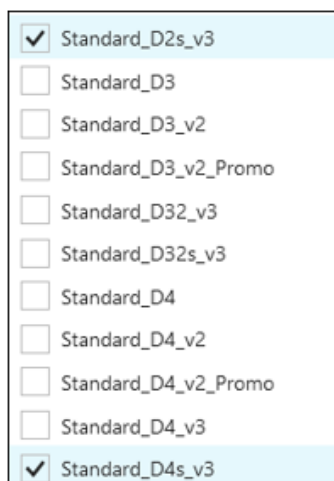


5. By default the policy is set with **Deny**, meaning that if someone starts a deployment in the subscription that isn't in EUS2 or CUS, the deployment will fail. Here's what happens if someone in the Contoso subscription tries to set up a deployment in West US.



Allow specific VM SKUs

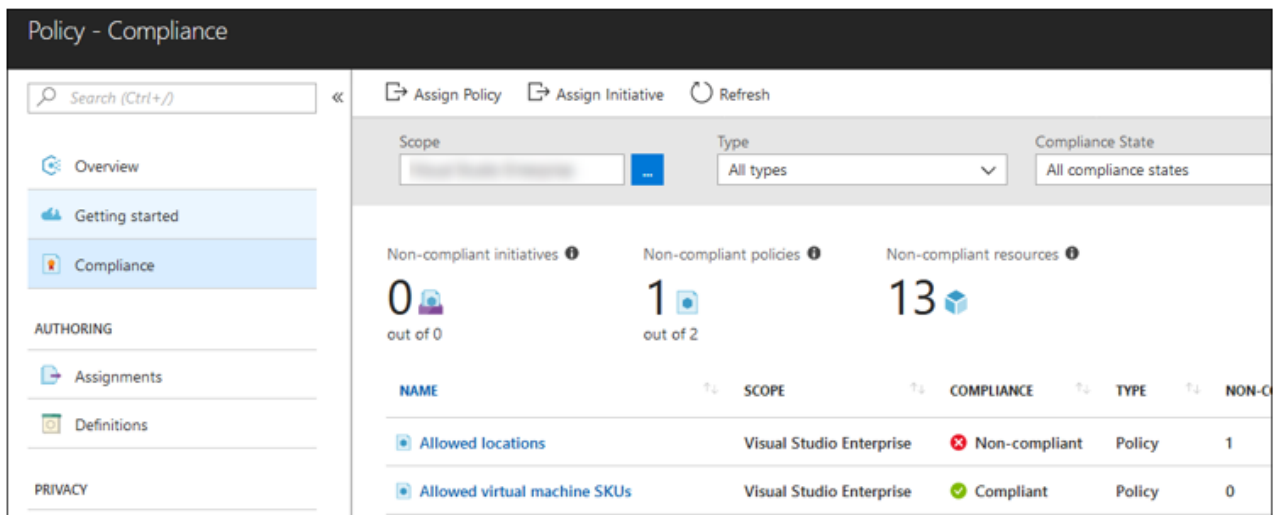
Contoso will use the built-in policy definition **Allow virtual machines SKUs** to limit the type of VMs that can be created in the subscription.



Check policy compliance

Policies go into effect immediately, and Contoso can check resources for compliance.

1. In the Azure portal, select the **Compliance** link.
2. The compliance dashboard appears. You can drill down for further details.



Set up locks

Contoso has long been using the ITIL framework for the management of its systems. One of the most important aspects of the framework is change control, and Contoso wants to make sure that change control is implemented in the Azure deployment.

Contoso is going to implement locks as follows:

- Any production or failover component must be in a resource group that has a ReadOnly lock. This means that to modify or delete production items, the lock must be removed.
- Nonproduction resource groups will have CanNotDelete locks. This means that authorized users can read or modify a resource, but can't delete it.

[Learn more](#) about locks.

Set up tagging

To track resources as they're added, it will be increasingly important for Contoso to associate resources with an appropriate department, customer, and environment.

In addition to providing information about resources and owners, tags will enable Contoso to aggregate and group resources, and to use that data for chargeback purposes.

Contoso needs to visualize its Azure assets in a way that makes sense for the business. For example by role or department. Note that resources don't need to reside in the same resource group to share a tag. Contoso will create a simple tag taxonomy so that everyone uses the same tags.

Tag name	Value
CostCenter	12345: It must be a valid cost center from SAP.
BusinessUnit	Name of business unit (from SAP). Matches CostCenter.
ApplicationTeam	Email alias of the team that owns support for the app.
CatalogName	Name of the app or ShareServices, per the service catalog that the resource supports.
ServiceManager	Email alias of the ITIL Service Manager for the resource.

Tag name	Value
COBPriority	Priority set by the business for BCDR. Values of 1-5.
ENV	DEV, STG, PROD are the possible values. Representing developing, staging, and production.

For example:

CostCenter : 12345
BusinessUnit : IT
ApplicationTeam : IT-Networking@contoso.com
CatalogName : SharedServices
COBPriority : 1
ENV : PROD
ServiceManager : chad@contoso.com

After creating the tag, Contoso will go back and create new policy definitions and assignments, to enforce the use of the required tags across the organization.

Step 6: Consider security

Security is crucial in the cloud, and Azure provides a wide array of security tools and capabilities. These help you to create secure solutions, on the secure Azure platform. Read [Confidence in the trusted cloud](#) to learn more about Azure security.

There are a few aspects for Contoso to consider:

- **Azure Security Center:** Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads. With Security Center, you can apply security policies across your workloads, limit your exposure to threats, and detect and respond to attacks. [Learn more](#).
- **Network security groups (NSGs):** An NSG is a filter (firewall) that contains a list of security rules which, when applied, allow or deny network traffic to resources connected to Azure VNets. [Learn more](#).
- **Data encryption:** Azure Disk Encryption is a capability that helps you encrypt your Windows and Linux IaaS virtual machine disks. [Learn more](#).

Work with the Azure Security Center

Contoso is looking for a quick view into the security posture of its new hybrid cloud, and specifically its Azure workloads. As a result, Contoso has decided to implement Azure Security Center starting with the following features:

- Centralized policy management
- Continuous assessment
- Actionable recommendations

Centralize policy management

With centralized policy management, Contoso will ensure compliance with security requirements by centrally managing security policies across the entire environment. It can simply and quickly implement a policy which applies to all of its Azure resources.

Security policy - Security policy

Search (Ctrl+J)

POLICY COMPONENTS

Data Collection

Security policy

Email notifications

Pricing tier

Save

Show recommendations for

System updates ⓘ	On	Off	
Security configurations ⓘ	On	Off	
Endpoint protection ⓘ	On	Off	
Disk encryption	On	Off	
Network security groups	On	Off	
Web application firewall	On	Off	
Next generation firewall	On	Off	
Vulnerability Assessment	On	Off	
Storage Encryption	On	Off	
JIT Network Access	On	Off	UPGRADE
Adaptive Application Controls	On	Off	UPGRADE
SQL auditing & Threat detection	On	Off	
SQL Encryption	On	Off	

Assess and action

Contoso will take advantage of the continuous security assessment which monitors the security of machines, networks, storage, data, and applications; to discover potential security issues.

- Security Center will analyze the security state of Contoso's compute, infrastructure, and data resources, and of Azure apps and services.
- Continuous assessment helps the Contoso operations team to discover potential security issues, such as systems with missing security updates or exposed network ports.
- In particular Contoso wants to make sure all of the VMs are protected. Security Center helps with this, verifying VM health, and making prioritized and actionable recommendations to remediate security vulnerabilities before they're exploited.

Endpoint Protection not installed on Azure VMs



Filter

Install on 6 VMs

VIRTUAL MACHINE		STATE	SEVERITY	
<input checked="" type="checkbox"/>	CONTOSODC3	Open	High	...
<input checked="" type="checkbox"/>	CONTOSODC4	Open	High	...
<input checked="" type="checkbox"/>	CONTOSODC5	Open	High	...
<input checked="" type="checkbox"/>	CONTOSODC6	Open	High	...

Work with NSGs

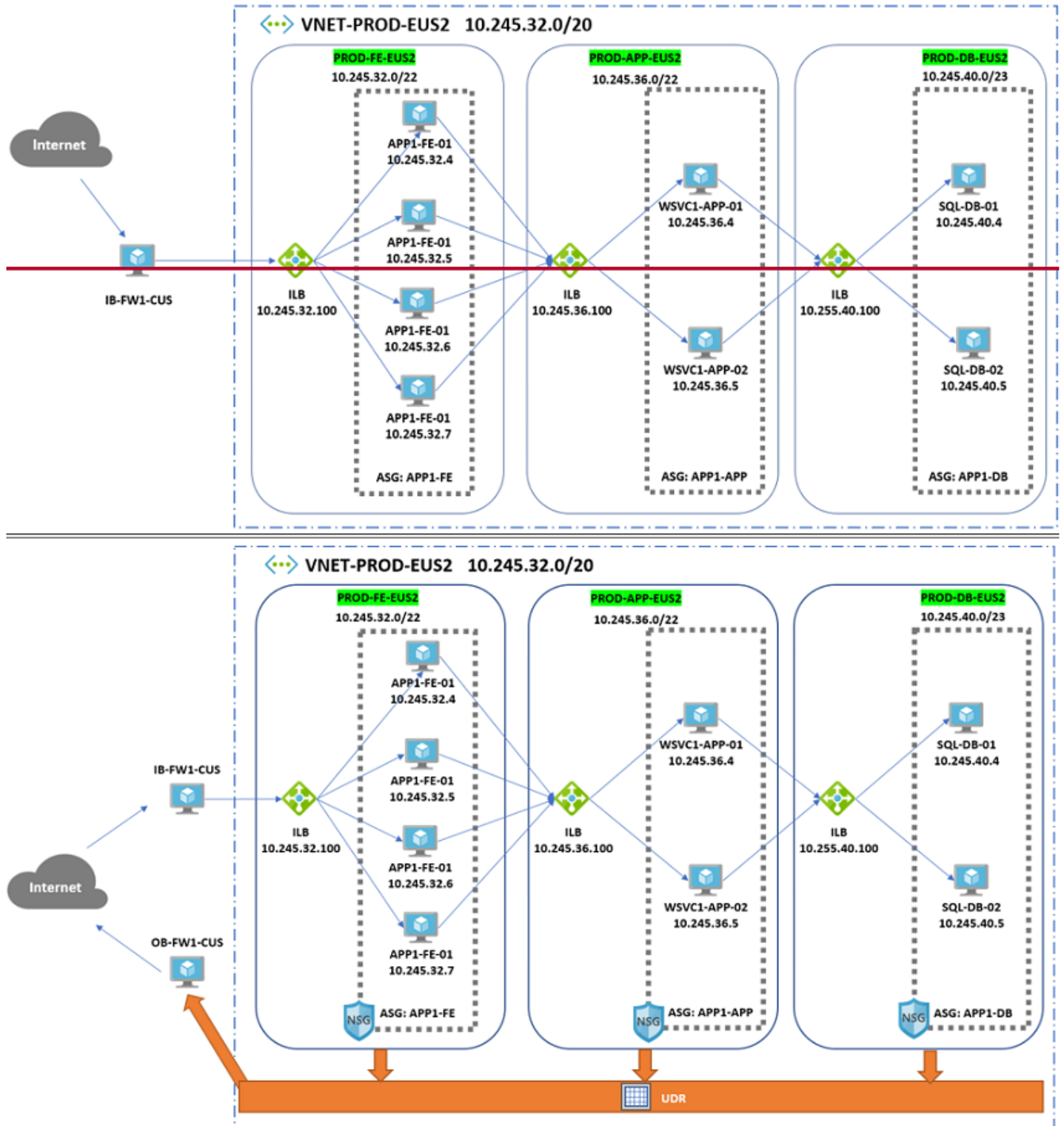
Contoso can limit network traffic to resources in a virtual network using network security groups.

- A network security group contains a list of security rules that allow or deny inbound or outbound network traffic based on source or destination IP address, port, and protocol.
- When applied to a subnet, rules are applied to all resources in the subnet. In addition to network interfaces, this includes instances of Azure services deployed in the subnet.
- Application security groups (ASGs) enable you to configure network security as a natural extension of an app structure, allowing you to group VMs and define network security policies based on those groups.
 - Application security groups mean that Contoso can reuse the security policy at scale, without manual maintenance of explicit IP addresses. The platform handles the complexity of explicit IP addresses and multiple rule sets, allowing you to focus on your business logic.
 - Contoso can specify an application security group as the source and destination in a security rule. After a security policy is defined, Contoso can create VMs, and assign the VM NICs to a group.

Contoso will implement a mix of NSGs and ASGs. Contoso is concerned about NSG management. It's also worried about the overuse of NSGs, and the added complexity for operations staff. Here's what Contoso will do:

- All traffic into and out of all subnets (north-south), will be subject to an NSG rule, except for the GatewaySubnets in the Hub networks.
- Any firewalls or domain controller will be protected by both subnet NSGs and NIC NSGs.
- All production applications will have ASGs applied.

Contoso has built a model of how this will look for its applications.



The NSGs associated with the ASGs will be configured with least privilege to ensure that only allowed packets can flow from one part of the network to its destination.

Action	Name	Source	Target	Port
Allow	AllowInternetToFE	VNET-HUB-EUS1/IB-TrustZone	APP1-FE 80, 443	
Allow	AllowWebToApp	APP1-FE	APP1-DB	1433
Allow	AllowAppToDB	APP1-APP	Any	Any
Deny	DenyAllInbound	Any	Any	Any

Encrypt data

Azure Disk Encryption integrates with Azure Key Vault to help control and manage the disk-encryption keys and secrets in a Key Vault subscription. It ensures that all data on VM disks are encrypted at rest in Azure storage.

- Contoso has determined that specific VMs require encryption.
- Contoso will apply encryption to VMs with customer, confidential, or PPI data.

Conclusion

In this article, Contoso set up an Azure infrastructure and policy for Azure subscription, hybrid identify, disaster recovery, networking, governance, and security.

Not all of the steps that Contoso completed here are required for a migration to the cloud. In this case, it wanted to plan a network infrastructure that can be used for all types of migrations, and is secure, resilient, and scalable.

With this infrastructure in place, Contoso is ready to move on and try out migration.

Next steps

After setting up their Azure infrastructure, Contoso is ready to begin migrating workloads to the cloud. See the [migration patterns and examples overview](#) section for a selection of scenarios using this sample infrastructure as a migration target.