Microsoft

Azure Virtual Datacenter

An approach to isolation, security, and trust in the Microsoft cloud

By Mark Ozur
Hatay Tuna
Callum Coffin
Telmo Sampaio

Azure Engineering

October 2017

Contents

List of figures

Overview

Azure Virtual Datacenter is an approach to making the most of the Azure cloud platform's capabilities while respecting your existing security and networking policies. When deploying enterprise workloads to the cloud, IT organizations and business units must balance governance with developer agility. Azure Virtual Datacenter provides models to achieve this balance with an emphasis on governance.

Deploying workloads to the cloud introduces the need to develop and maintain trust in the cloud to the same degree you trust your existing datacenters. The first model of Azure Virtual Datacenter guidance is designed to bridge that need through a locked-down approach to virtual infrastructures. This approach isn't for everyone. It's specifically designed to guide enterprise IT groups in extending their on-premises infrastructure to the Azure public cloud. We call this approach the trusted datacenter extension model. Over time, several other models will be offered, including those that allow secure Internet access directly from a virtual datacenter.

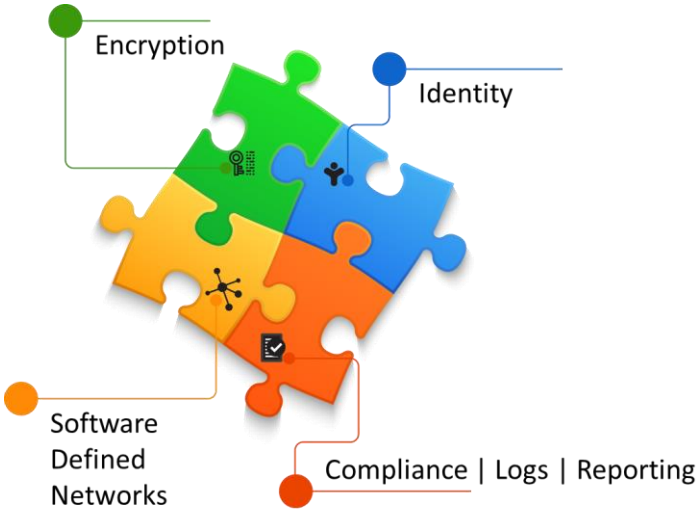

Figure 1. The four components that make the Azure Virtual Datacenter possible: identity, encryption, software-defined networking, and compliance.

In the Azure Virtual Datacenter model, you can apply isolation policies, make the cloud more like the physical datacenters you know, and achieve the levels of security and trust you need. Four components any enterprise IT team would recognize make it possible: software-defined networking, encryption, identity management, and the Azure platform's underlying compliance standards and certifications. These four are key to making a virtual datacenter a trusted extension of your existing infrastructure investment.

Central to this model is the idea that your cloud infrastructure has isolation boundaries that can be thought of as your corporate *namespace*. Think of it as your isolated cloud within Azure. Within this virtual boundary, security controls, network policies, and compliance come together, providing you with an IT infrastructure on Azure capable of securely integrating cloud resources with your existing on-premises datacenter.

You can deploy new virtual *workspaces* in the virtual datacenter much as you would deploy additional capacity to your physical datacenter. These virtual workspaces are self-contained

environments where workloads can run independently, and workload teams can get workspace-specific access. Workspaces enable teams to build solutions and manage workloads with great freedom while adhering to the overall access and security policies defined in the central IT infrastructure.

This guide is intended for enterprise IT architects and executives. Using the lens of the physical datacenter, the guide discusses an approach to designing secure, trusted virtual datacenters on the Azure platform. Azure Virtual Datacenter is not a specific product or service but rather a way to think about cloud infrastructures. It offers proven practices and guidance to help smooth your migration to the cloud.

At the end of this guide, you can learn about the upcoming Azure Virtual Datacenter Automation guidance. This guidance includes a collection of scripts and Azure Resource Manager templates that will help you build an Azure Virtual Datacenter using the trusted extension model.

PART 1
WHAT IS AZURE VIRTUAL DATACENTER?

Azure Virtual Datacenter is a way to think about deploying your application estate in a cloud-based architecture while preserving key aspects of your current IT governance and taking advantage of cloud computing's agility.

There are very real, underlying differences between hosting in the cloud and running in a traditional datacenter. Achieving the level of governance in the cloud environment that you experience in a traditional datacenter requires a sound understanding of why you do what you do today, and how that is achieved in Azure.

Unlike your existing on-premises datacenter environment, the Azure public cloud operates using shared physical infrastructure and a software-defined environment abstraction. The Azure Virtual Datacenter model allows you to structure isolated workloads in the Azure multitenant environment that meet your governance policies.

Governing your workloads requires integrating management processes, regulatory requirements, and security processes within a cloud environment. The Azure Virtual Datacenter model provides basic guidance for creating an organization's separation of roles, responsibilities, and policies in the cloud.

Introduction: the essential components

A virtual datacenter is an isolated environment (like a building with walls) for cloud-hosted resources (like servers and networks) that supports the application of organizational policies (like security and compliance). It starts with an Azure subscription, the doorway to the environment for deploying Azure resources and services.

A key tenet of the Azure Virtual Datacenter model is to place as little trust as possible in the surrounding hosting environment. Therefore, the virtual datacenter must impose isolation, security, and compliance measures within its environment just as a physical datacenter would. The main difference is how these measures are implemented. Azure Virtual Datacenter relies on the following essential components:

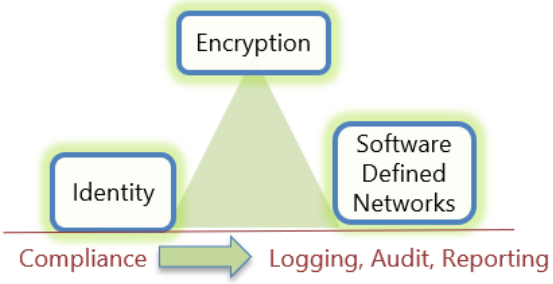

Figure 2. Compliance with security and policy is the foundation of the Azure Virtual Datacenter approach to trust, where automated auditing capabilities uncover potential issues.

- **Software-defined networking** provides virtual abstractions for your physical network elements, such as network topologies, firewalls, intrusion detection mechanisms, load balancers, and routing policy. You can create, configure, and manage network topologies, support isolation, and provision perimeter networks.
- **Identity management and role-based access control (RBAC)** govern access to the computing, networking, data, and applications in a virtual datacenter. Based on the least privilege model of access control, the virtual datacenter denies access to resources by default. Access must be explicitly granted to specific users, groups, or applications performing particular roles.
- **Encryption**. Data in transit, at rest, and in process is encrypted. This Encryption isolates confidential information from the rest of the environment, including the underlying platform. Even virtual machines are booted with encryption. This conservative approach may not be needed for all Azure hosting scenarios but is a foundation of the virtual datacenter's intentionally strict trust model.
- **Compliance.** Azure infrastructure and services meet a broad set of international, industry-specific, and country-specific compliance standards. To help ensure the safety of your data, Microsoft also verifies how compliance is achieved through rigorous third-party audits that validate Azure's adherence to standards-mandated security controls. In addition, virtual datacenters make extensive use of automated compliance monitoring, logging, and reporting

systems, operational rigor, transparency through audit reports, and aggressive testing methods such as red teaming.

A logical isolation for multiple workspaces

The virtual datacenter exists as a conceptual namespace grouping together all the resources you use within the virtual datacenter. This namespace serves as the virtual walls isolating your resources from other tenants on the platform and from the external Internet.

Workloads such as line-of business applications are hosted in separate, isolated workspaces. These workspaces provide the required infrastructure and management services to securely deploy workload resources and are quickly and easily instantiated to preserve developer agility. Workspaces adhere to the virtual datacenter's access control and policy standards, which can be augmented with additional workspace-specific rules. Workspaces are configured by policy to route all external traffic through the central IT infrastructure, where organizational policies can be applied. Multiple workloads can be deployed to a single workspace, or in separate, isolated workspaces.

A shared infrastructure of trust

To use a virtual datacenter as a trusted datacenter extension, you need to know the level of control you have over your resources and the degree of trust you place in specific elements of the platform. The underlying Azure platform takes on all the responsibilities for physical infrastructure maintenance and security. In a traditional on-premises datacenter, your organization would assume these responsibilities. In addition to handing off responsibility for the physical assets involved in a running a datacenter, you also need to be sure that you can trust the Azure platform to provide you with the controls and management tools to build secure solutions in the multitenant cloud.

When it comes to compliance, Microsoft is building products to make customers' lives easier. The Azure platform has the largest compliance portfolio in the industry and continues to grow every year. However, while Microsoft implements compliance measures at the platform level, you must also do your part within the applications you create on the platform.

The Microsoft Compliance Manager tool provides transparency into the controls managed by the platform and the controls you are responsible for managing. The tool also helps you understand compliance for those controls. Whether that involves a configuration on the platform such as encryption or multi-factor authentication or a knowledgebase article on a process like role assignments, the goal is the same.

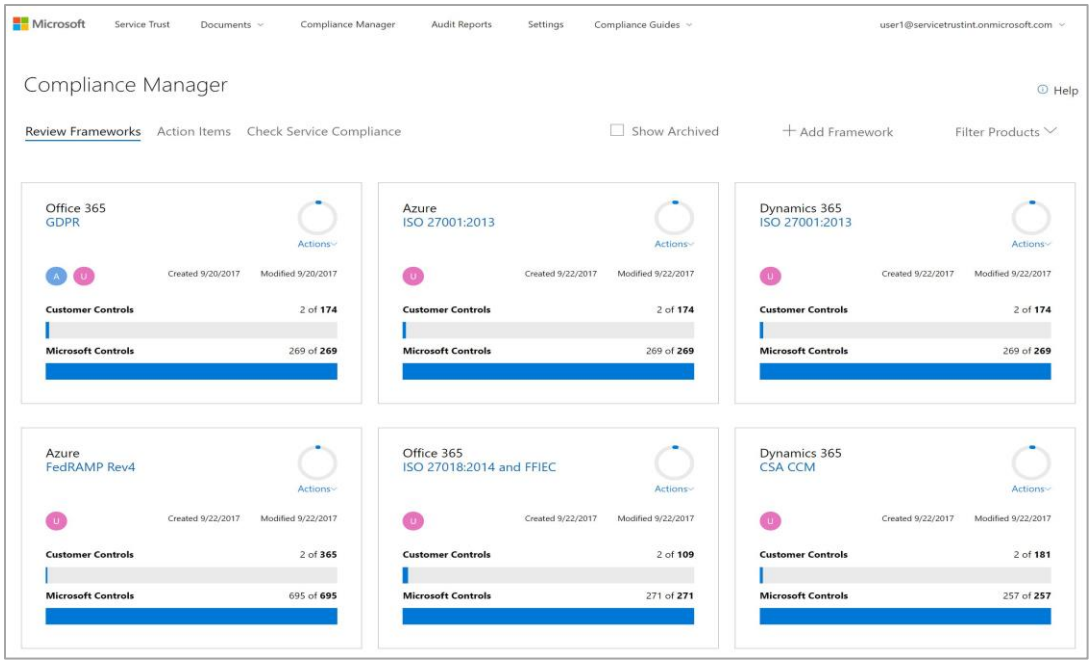

Figure 3. The Microsoft Compliance Manager dashboard.

A global platform

Azure organizes its platform capabilities into geographic regions. Each contains one or more datacenters located in relative proximity to each other to support robust high availability and disaster recovery scenarios. A world map shows Azure datacenters (as of October 2017) on most every continent. This reach enables you to deliver your solutions close to your customers and employees and compete in even more geographic markets.

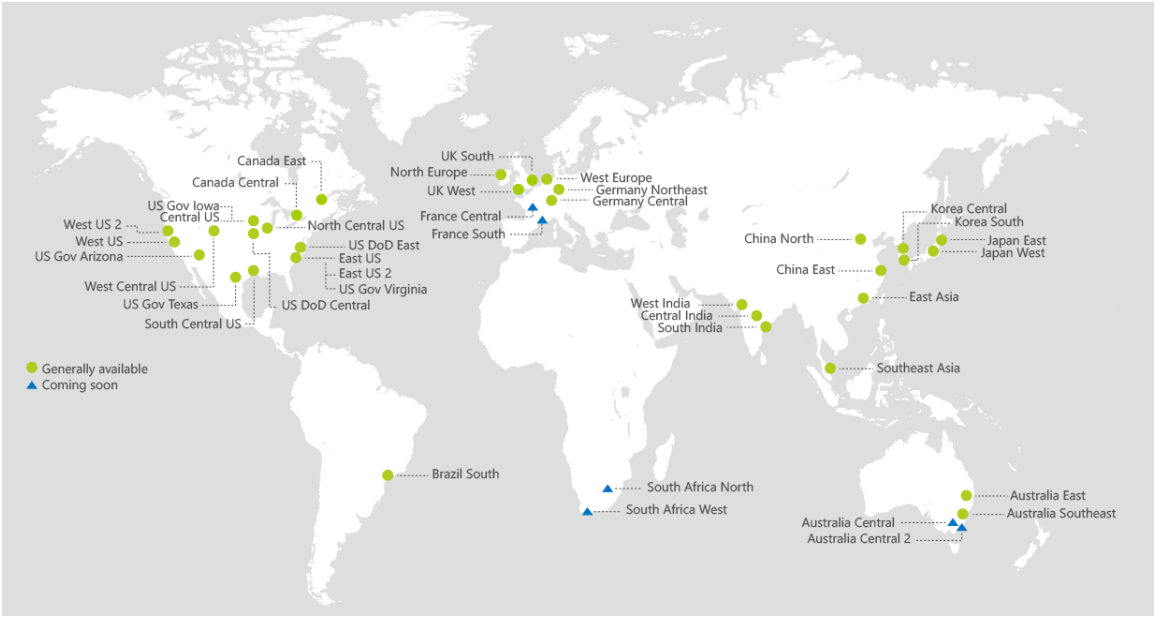

Figure 4. The Azure platform is supported by a growing network of Azure-managed datacenters around the world.

Azure datacenters contain physical network, compute, and storage devices like any traditional physical datacenter, just at hyper-scale. So at some level, the same facility maintenance, security, and access control requirements you already apply in your physical datacenter also apply to Azure datacenters. The main difference is that those requirements are managed by the Azure datacenter staff, rather than your own teams.

Because of Azure's global reach, data sovereignty can be an important concern that you didn't have to deal with when only maintining your on-premises infrastructure. Governance policies can be applied to your Azure subscriptions to ensure that resources are deployed only to regions that meet your data residency requirements. To see which Azure region is right for you, see the Azure datacenters website.

A regional infrastructure

For business continuity and disaster recovery scenarios, each Azure region is paired with complementary geo-political regions (for example, North Europe and West Europe regions). Regional pairs (with the exception of Brazil South and Southeast Asia/East Asia) offer the same data-residency and sovereignity for both members of the pair. Replicating resources across paired regions reduces the likelihood of natural disasters, civil unrest, power outages, or physical network outages affecting both regions at once.

Azure further breaks down regions into multiple availability zones—low-latency, connected environments supporting highly available applications. Availability zones help protect against any potential outage within a specific datacenter in a region.

By default, resources in a virtual datacenter exist within a single Azure region, allowing components to connect with greater security and with minimum network latency. Just as you might replicate your physical datacenter to provide a high-availability infrastructure, instances of a virtual datacenter can be created in multiple regions. Applications executing within a workspace can take advantage of all Azure high-availability features within a region and across regions. For example, using Global VNet Peering, it is possible to extend the virtual datacenter across regions. Features such as SQL Database geo-replication also help to keep multiple instances of workloads in sync and available.

Trust through isolation

In the multitenant cloud environment, a subscription provides the first layer of isolation through its association with Azure Active Directory (Azure AD). Azure AD isolates identity information and provides authentication for accessing a subscription and its resources. Azure AD can also support Azure Multi-Factor Authentication (MFA), which provides a highly recommended second layer of authentication security.

Azure AD roles are essential for a virtual datacenter using Role-Based Access Control (RBAC). RBAC is used for controlling management access to resources such as services, virtual machines, storage, and databases. RBAC can enable access to a resource for an individual Azure AD user or group, or an Azure AD role. However, the settings within a resource are often governed by that resource's internal configuration, not RBAC. For example, access to the guest operating system of a virtual machine is configured within the operating system.

In addition to locking down access control and permissions, read-only or delete locks can be

placed on individual resources and collections called resource groups. For example, central IT administrators might apply a read-only lock to a virtual network, allowing users and other resources to use but not modify the network. Or a workspace owner could apply a delete lock to a virtual machine in the workspace to allow DevOps teams to configure the resource but not delete it.

Regardless of the level of isolation and security applied to a resource group or resource, any attempt to access, modify, or delete a resource leaves an audit trail. Azure Activity Log records all resource activity, including actions, actors, and if an action was successful.

Another way to isolate resources is to enable just in time access control of virtual machines. This recommended feature limits the amount of time a management endpoint attached to a virtual machine remains open. Locking down inbound traffic in this way is particularly important for any virtual machines used to perform broad management functions within the virtual datacenter.

As with an on-premises datacenter, regular security tests should be run against Azure–hosted resources, using both automated processes and manual review. These tests should always include port scanning, penetration testing, and fuzz testing. Azure Security Center provides threat prevention, detection, and response capabilities that are built in to Azure, including and includes risk-mitigation tools such as endpoint protection for virtual machine anti-malware protection.

▸ See also

Introduction to Azure Security

Isolation in the Public Cloud

Azure network security

Azure Virtual Machine security overview

Azure Storage security guide

Microsoft Trust Center: Design and operational security

Trust through encryption

The Azure Virtual Datacenter model makes global encryption a critical priority. All data must be encrypted at all times—while in transit and at rest.

Azure Key Vault is the primary mechanism for storing and managing the keys, secrets, and certificates associated with encryption, authentication, and cryptographic non-repudiation processes within a virtual datacenter.

All cryptographic keys, connection strings, certificates, and other secrets used by applications or resources in a virtual datacenter must be stored and managed as well. Key Vault supports a FIPS 140-2 Level 2-validated hardware security model (HSM), and allows you to generate keys using your on-premises HSM and securely transfer them to Key Vault.

Keys stored in Key Vault can also be used to encrypt storage assets, and to help secure PaaS services or individual applications. For example, a database connection string can be stored in Key Vault instead of an application's configuration files or environment variables. Authorized applications and services within Azure Virtual Datacenter can use, but not modify, keys stored in

Key Vault. Only key owners can make changes to keys stored in Key Vault.

Data in transit

The Azure Virtual Datacenter model uses encryption to enforce isolation of data as it moves between:

- On-premises networks and the virtual datacenter. Data passes through either an encrypted site-to-site virtual private network (VPN) connection or an isolated, private ExpressRoute.
- Applications running in a different virtual datacenter (that is, from one virtual datacenter to another).
- Applications running in the same Azure virtual datacenter.
- Platform services, including both internal and external endpoints—storage accounts, databases, and management APIs.

In these scenarios, the Azure Virtual Datacenter approach is to use the SSL/TLS protocols to exchange data between both the virtual datacenter and application components. All network traffic has some degree of encryption applied at all times. In addition, all communication between internal Azure components within the virtual datacenter are protected using SSL/TLS, enforced by a firewall in the central IT infrastructure.

Data at rest

Data at rest is also encrypted, including data stored on Azure Storage and in relational databases, which may offer additional encryption. For example, Azure SQL Database includes Transparent Data Encryption (TDE).

The central IT infrastructure uses Azure Storage for several tasks, such as storing logs. Azure Storage Service Encryption (SSE) provides encryption at rest for all Azure Storage services by encrypting data before writing it to storage. SSE decrypts the data immediately prior to retrieval. SSE-enabled Azure Storage accounts can handle encryption, decryption, and key management in a totally transparent fashion. All data is encrypted using 256-bit AES encryption, and both Microsoft-managed and customer-managed encryption keys are supported.

Virtual machine disk image encryption is also a critical part of ensuring isolation and virtual machine security within a shared tenant environment. The Azure Virtual Datacenter model depends on the platform's ability to securely create, host, and access virtual machines with encrypted disks. Azure supports two models for encrypting virtual machines:

- For virtual machines created in Azure, you can use Azure Disk Encryption. The BitLocker feature of Windows and the DM-Crypt feature of Linux provide volume encryption for the operating system and data disks. The Azure Marketplace contains hundreds of preconfigured virtual machine images that you can quickly deploy and encrypt.
- You can also use pre-encrypted virtual machines created using your on-premises Hyper-V hosts, using DM-Crypt or BitLocker with your internal policies and configuration. After validating an image on-premises, you can then upload the relevant internally managed keys to your Key Vault instance, then deploy the pre-encrypted VHD disk images as Azure virtual machines.

Data in process

Another near-term addition to the Azure platform is support for Confidential Computing through Trusted Execution Environments (TEE) using technologies such as enclaves. Intel Secure Guard Extensions (SGX) and other enclave technologies allow developers to create secure, trusted execution environments. Enclaves provide an encrypted area for data and code that can only be processed by CPU-based security mechanisms in the process-embedded TEE.

Microsoft is also investing in cryptographic research. For example, homomorphic encryption (HE) can be used to encrypt stored data so that storage can be outsourced to an untrusted cloud. Applications can make use of HE data as is without first decrypting it. For more information about using HE in a bioinformatics context, see the paper from Microsoft Research, Manual for Using Homomorphic Encryption for Bioinformatics.

Upcoming virtual machine security capabilities

The Azure platform is continuously adding services and features designed to make your virtual machines and environments more secure. Upcoming versions of Windows Server will add Azure support for numerous features currently available today in on-premises versions of Windows Server 2016 Hyper-V, including two key capabilities:

- Secure Boot: Ensures that each component loaded during the boot process is digitally signed and validated.
- Shielded virtual machines: Provides protection from compromised or malicious administrators. The disk and state of the virtual machine are encrypted, so only the virtual machine or tenant administrators can access it. Shielded virtual machines use a virtual Trusted Platform Module (TPM), are encrypted using BitLocker, and only run on approved hosts.

See also

Encryption in the Microsoft Cloud

What is Azure Key Vault?

Azure Storage Service Encryption for Data at Rest

Azure Disk Encryption for Windows and Linux IaaS VMs

PART 2
HOW CONTOSO COMPOSES A TRUSTWORTHY DATACENTER

In general, virtual datacenters introduce new challenges to the service management landscape. Together with Azure Virtual Datacenter principles, good IT management processes help enterprises realize the benefits of public cloud computing such as self-service, scalability, and elasticity.

This section describes a reference implementation for Contoso, a fictional financial services enterprise. It is based on real-life engagements with global organizations that have successfully made the transition to the cloud with the requisite regulatory approval.

Centralize access control and connect workspaces

Contoso's virtual datacenter design specifies a centralized set of IT security and management capabilities. They want business units to be able to deploy individual workloads with the agility and flexibility common to Azure solutions, while adhering to central IT policies. The basic infrastructure is supported by a hub-and-spoke network architecture connecting the central IT infrastructure with workloads.

They plan to set up a fast, private connection between the virtual datacenter and their network on-premises. They don't want to allow direct access to the Internet or external networks other than their own. All Internet-bound traffic must pass through the on-premises network—where it is subject to any security restrictions and policy managed there.

Figure 5 shows their initial proposal. For the final Contoso architecture, see Figure 11 at the end of this section.

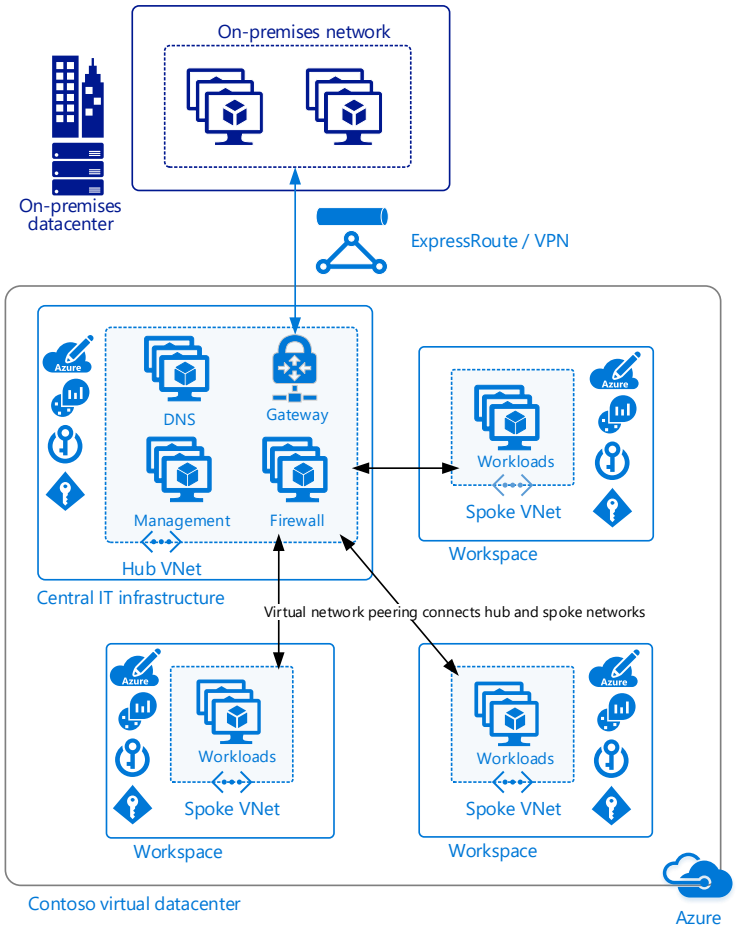

Figure 5. Proposed high-level architecture for Contoso virtual datacenter.

On-premises connectivity

To avoid sending traffic over the public Internet, Contoso wants to use a dedicated, private connection between their on-premises network and the virtual datacenter. The Azure Virtual Datacenter model supports two methods of connecting a virtual datacenter center to on-premises networks:

- ExpressRoute uses a dedicated, private connection facilitated by a connectivity provider.
- Azure VPN gateways create a site-to-site connection that passes encrypted traffic over the public Internet.

Contoso plans to set up an ExpressRoute connection, which offers more reliability, faster speeds, and lower latencies than typical connections over the Internet. ExpressRoute creates a direct link between the on-premises network and Azure. However, ExpressRoute connections take time to acquire and deploy. While they wait for ExpressRoute, Contoso can immediately set up a site-to-site VPN gateway, a common tactic used by many organizations to quickly get started using Azure resources.

After the ExpressRoute connection is in place, they can convert the VPN gateway to a failover connection in case the ExpressRoute goes down. They could also use it as a secondary connection for workloads that don't require the increased speed and lower latency of ExpressRoute.

Separation of responsibility in the datacenter

Contoso wants the separation of responsibilities found in their on-premises operations to be reflected in their virtual datacenter. To organize jobs and responsibilities within the IT infrastructure, Contoso manages roles and assigns users to those roles using their on-premises directory service. Azure AD surfaces these roles in Azure, where they can be applied to access rules for the virtual datacenter's resources.

RBAC gives Contoso a way to assign different teams to various management tasks within the virtual datacenter. They give Central IT control over core access and security features, but also use a distributed approach to access that gives software developers and other teams large amounts of control over specific workloads.

Any significant change to resources or infrastructure involves multiple roles—that is, more than one person must review and approve a change. This separation of responsibilities limits the ability of a single person to access sensitive data or introduce vulnerabilities without the knowledge of other team members.

For example, the Network Operations person responsible for the central network infrastructure must approve certain infrastructure requests from the Network Operations person who oversees a specific application's virtual network. Contoso decided that these two similar roles should be split between the central team overseeing the common components of the infrastructure (Corporate NetOps) and the many people who oversee the individual application deployments (Application NetOps). Likewise, they take the same approach to Security Operations and other roles. Contoso can centrally manage policy for the organization as well as unleash application teams to innovate within those policies.

Management roles

Contoso's current IT service management organization revolves around the activities that occur throughout the entire IT lifecycle: managing compliance, configurations, and audits. To handle these activities for the new virtual datacenter, Contoso organizes IT users from both the central and application teams into the following roles:

Group	Common role name	Responsibilities
Security Operations	SecOps	Provide general security oversight. Establish and enforce security policy such as encryption at rest. Manage encryption keys. Manage firewall rules.
Network Operations	NetOps	Manage network configuration and operations within virtual networks of the virtual datacenter such as routes and peerings.
Systems Operations	SysOps	Specify compute and storage infrastructure options and maintain resources that have been deployed.
Development, Test and Operations	DevOps	Build workload features and applications. Operate features and applications to meet service-level agreements (SLAs) and other quality standards. DevOps roles are generally not used in the central IT infrastructure.

Following Azure Virtual Datacenter principles, access and security for resources within each workspace should be handled through workspace-specific groups independent of the central IT groups. Workload teams can then maintain their own resources, deploy solutions, and create access policies, while the central IT teams retain overall control of the virtual datacenter and communication into and out of it.

Each group should have a unique and easily identifiable name that indicates the section of the datacenter they are responsible for. Contoso creates a nomenclature to differentiate the roles associated with managing the central virtual datacenter services from the roles associated with managing the workspaces and workloads.

Common IT infrastructure groups	Workspace-specific groups
CorpSecOps	*App*SecOps
CorpNetOps	*App*NetOps
CorpSysOps	*App*SysOps
CorpDevOps	*App*DevOps

Where "*App*" is a descriptive prefix for a workload's primary function, for instance, "*LOBService1*NetOps" for a workspace hosting a specific line-of-business application.

Identity management with Azure AD

Contoso wants to provide a common identity for managing resources on their virtual datacenter. To do this, they plan to integrate their on-premises directory services with Azure AD. Azure AD Connect is used to provide synchronization of users and roles between Contoso's on-premises Active Directory service and the Azure AD tenant associated with the virtual datacenter.

Individual workloads and applications hosted in virtual datacenter workspaces may or may not make use of the shared identity services, but all management of Azure resources will use Azure AD for access control.

▸ See also

Microsoft hybrid identity solutions

Azure AD Connect and federation

Compose in layers driven by policy

Policy is built in layers using the components discussed in Part 1—software-defined networking, encryption, identity management, and compliance.

Proposed Contoso architecture

The core of Contoso's virtual datacenter is a central IT infrastructure through which all network traffic flows, policies are set, and core monitoring occurs. This infrastructure is segmented in its own environment, providing central security and networking services, including a hub virtual network that connects to other parts of the datacenter. It also manages any external connections used by resources hosted outside the virtual datacenter.

The design calls for isolated workspaces that support Contoso's various workload deployments such as Microsoft SharePoint or SAP services. Each workspace has its own management resources and spoke virtual networking infrastructure. Teams can add other policies to control access and resource usage within their workspace while adhering to central policies.

The central IT infrastructure environment and each workspace are created as separate Azure subscriptions. This policy decision is designed to increase workload flexibility and avoid subscription-related limits. Each central IT and workspace subscription is associated with the main organizational Azure AD tenant, but teams can also set up additional workspace-specific access controls and policies. For example, workspace-level RBAC enables teams to deploy resources for specific workloads or projects. If some teams want to run more than one workload in their workspace, they can do so without needing another subscription. Enforcement of global organizational policies is maintained on all subscriptions.

The Contoso virtual datacenter's central IT infrastructure includes the following:

- Subscription level security policy and monitoring settings.
- Subscription level, networking-specific policy and monitoring settings.
- Any connections to on-premises networks or the Internet.
- The central hub virtual network, through which all traffic between cloud workloads and the on-premises network must pass.
- The central firewall that, in line with the trusted extension model, inspects and redirects traffic passing through the virtual datacenter to an on-premises network.
- Operational tools and shared management services used by the virtual datacenter.

Workspaces include the following:

- Resource Manager policy settings that prevent direct access to external networks and route traffic through the central IT infrastructure.
- The workspace spoke virtual network.
- Workload-specific operational tools, such as log and key management.
- Workload resources.

Initial environment setup

Before any workspace subscriptions are created, Contoso configures their Azure AD tenant. This tenant was created when Contoso's Azure Enterprise Agreement was established and will be used for authentication and access control across the entire virtual datacenter. They integrate identity management between their on-premises Active Directory and Azure AD, using Azure AD Connect to synchronize credentials and accounts between the two environments.

Central IT and workspace subscriptions are created separately by Contoso's Azure Account Administrator, who ensures all subscriptions created for the virtual datacenter are associated with the organization's Azure AD tenant.

After a subscription is created, the standard SecOps, NetOps, SysOps, and DevOps roles for that subscription are added to Azure AD and given appropriate permissions.

Central IT infrastructure and workspace layout

Contoso organizes the central IT infrastructure and workspace subscriptions into functional resource groups. They use Resource Manager policies to establish rules about what and how resources can be deployed through Resource Manager. These policies can also be applied at the resource group level. For instance, they can apply policies to a resource group created for developers that allows the creation of virtual machines and prevents the creation of networking resources or storage accounts. Resource groups are also used for access control. Contoso assigns specific roles to certain resource groups, while denying them access to the wider subscription.

Contoso will create the following resource groups in the central IT subscription:

Resource group	Description
Networking	Contains the virtual network and related policy mechanisms such as the custom user-defined routes (UDRs) and network

	security groups (NSGs) used by the central IT infrastructure.
Operations	Hosts management services for central IT such as Microsoft Operations Management Suite (OMS) workspaces and network monitoring services.
Key vault	Provides access to the central IT Key Vault.
Shared services	Contains virtual machines providing DNS and domain services to the virtual datacenter.
Central firewall	Contains the central firewall providing layer 7 and potentially layer 4 outbound filters.
Management	Contains the virtual machines providing management jumpbox capabilities.

The breakdown of resource groups within workspaces depends on the needs of individual workloads, but Contoso will provide each workspace with the following groups on creation:

Resource group	Description
Networking	Contains the virtual network, related NSGs, and custom routing policies used by the workspace.
Operations	Hosts workspace-specific management services such as OMS workspaces and network monitoring services.
Key vault	Provides access to workspace-specific Key Vault.

Resource Manager policies

The base Resource Manager policies defined for a subscription and for resource groups are inherited by all resources within them. The Contoso virtual datacenter implements the following policies on both the central IT infrastructure and all workspaces:

Policies	Description
Deny public IP	Prevents the creation of any new public IP endpoints. For workspaces, this policy applies at the subscription level. The central IT infrastructure applies this policy on all resource groups, allowing the subscription owner to add a public IP for a VPN connection if necessary.
Enforce storage encryption	Forces any storage accounts created to use encryption. This policy is applied at the subscription level for central IT and all workspaces.
Restrict allowed regions	Restricts the creation of any resources within the subscription to specific Azure regions. Contoso restricts the deployment of resources to regions

	within the United States. This policy is applied at the subscription level for central IT and all workspaces.

Key Vault setup

With the *enforce storage encryption* policy in place on all subscriptions, Contoso needs to securely host and store encryption keys before any storage or virtual machines can be deployed.

After creating resource groups, Contoso provisions Key Vault for each environment—central IT and all workspace subscriptions. When the provisioning is complete, a cryptographic key is created and stored in Key Vault, which is then used to perform storage encryption tasks. An encrypted storage account is created in the Key Vault resource group for storing audit log information related to the vault.

Edit access to secrets and keys within the vault is restricted to the CorpSecOps or workload-specific SecOps role. Other roles can use secrets and keys to encrypt and decrypt storage and access encrypted virtual machines, but they cannot modify or otherwise access any keys.

Hub virtual network setup

Contoso implements the central IT infrastructure hub and multiple workspace spokes of their virtual datacenter as separate virtual networks, residing in their respective subscriptions. They base the design of their a virtual network on the hub-spoke topology proposed in the Azure network virtual datacenter paper. Contoso's CorpNetOps group configures virtual network peering to provide basic connectivity between the central IT infrastructure hub and the workspace spoke virtual networks. If a workload goes out of compliance, central IT can immediately sever the peering connection, effectively cutting off all resources in the affected workspace from the wider virtual datacenter.

Contoso's infrastructure policy requires a consistent IP address schema across all virtual networks within the virtual datacenter. This schema makes sure addresses do not overlap with on-premises networks, allowing the virtual datacenter to coexist with those networks when the two are connected over VPN or ExpressRoute. In addition, within the virtual datacenter, IP address ranges for any of the central IT and workspace virtual networks must not overlap for peering links between spokes and hub to work.

Central firewall

Data exfiltration is a major concern to Contoso, so they want to implement a layer-7 whitelisting mechanism to control data leaving the virtual datacenter. They set up a firewall using one or more network virtual appliances (NVAs) in the central IT infrastructure, and all traffic from a workspace to the outside world must pass through it. These virtual devices are designed to handle the networking and security functionality traditionally handled by physical firewall devices.

Through the central firewall, the central IT infrastructure controls the traffic allowed to pass in and out of the virtual datacenter and determines how that traffic is directed. The central firewall manages network flow within the virtual datacenter and between resources hosted in the virtual datacenter and those in external environments, including the on-premises datacenter.

UDRs on the workspace subnets route outbound traffic to the central firewall.

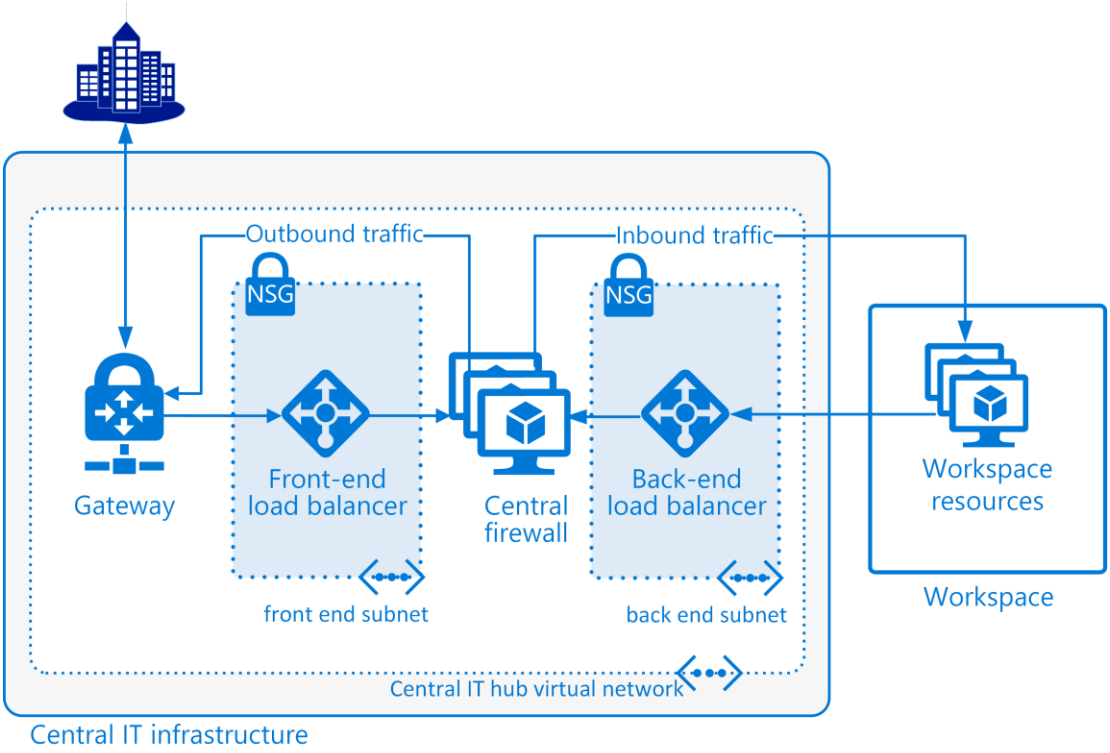

Figure 6. How the central firewall uses load balancers and traffic routing.

Contoso is expecting a large amount of traffic between their on-premises network and workloads hosted on the virtual datacenter. To handle the load and provide redundancy, the central firewall will consist of multiple NVAs. Two load balancers, using the High Availability Ports feature, will distribute traffic: A front-end load balancer handles traffic going to the workspaces from the network on-premises, and a back-end load balancer handles traffic going from workloads to the network on-premises.

▸ See also

Secure networks with virtual appliances

User-defined routes and IP forwarding

Gateways and perimeter networks

Contoso needs to set up a perimeter network to provide network connectivity with their on-premises datacenter networks. Perimeter networks in a virtual datacenter are usually handled as subnets of the central IT infrastructure's hub virtual network. When both this hub network and the remote network are fully trusted, the perimeter network can be implemented simply using a gateway to ensure traffic is routed properly to and from the central firewall.

In Contoso's implementation of the trusted extension model, a DMZ is not required, because all traffic flows only between the on-premises network and the virtual datacenter. This traffic passes through either an isolated ExpressRoute connection or a secure site-to-site VPN, and subscription policy prevents any public access to the virtual datacenter itself.

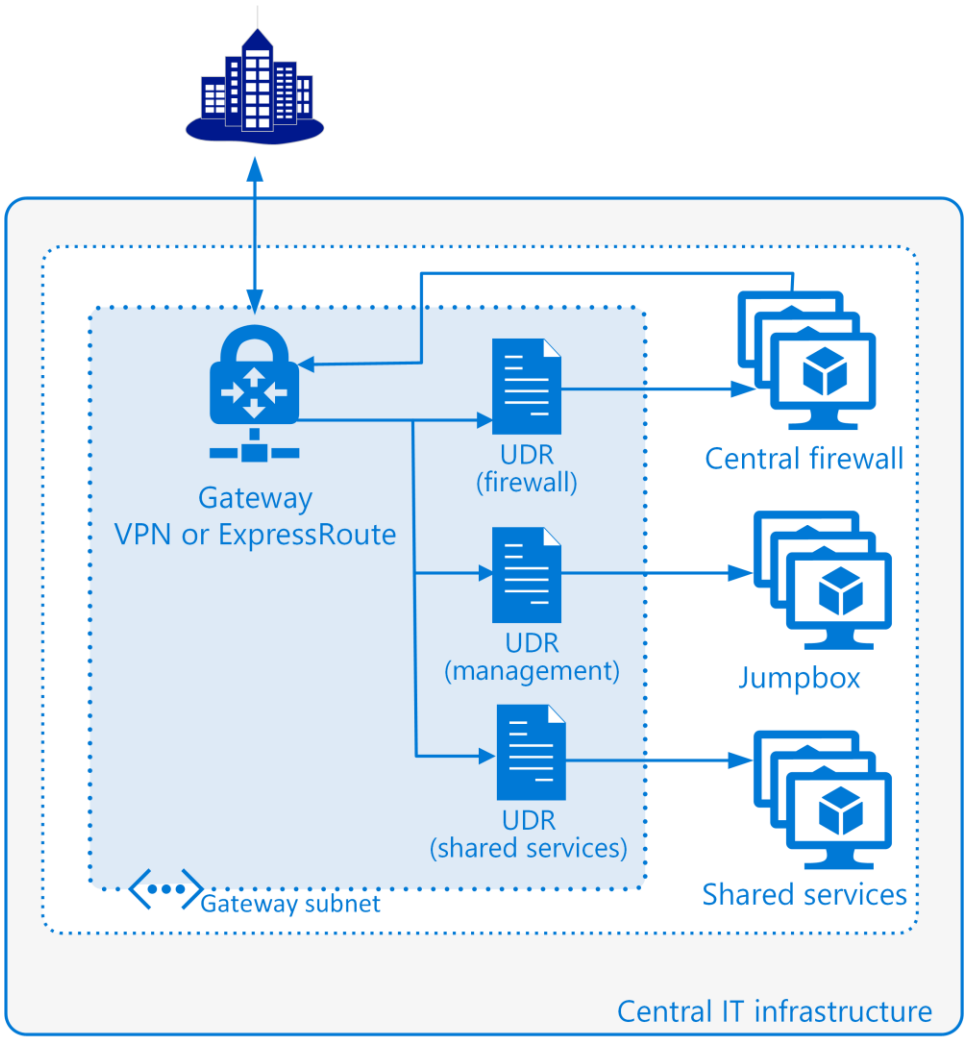

Figure 7. The gateway subnet routes traffic to the appropriate part of the central IT infrastructure.

This gateway is configured in a subnet of the central IT infrastructure's hub virtual network. The subnet implements UDRs to send incoming traffic to one of three destinations. Requests for workspace resources are processed through the central firewall. Administrator requests for remote access to configure network resources are sent to the management jumpboxes. Requests for tasks such as name resolution are routed to the shared services subnet.

In any case where the perimeter borders an untrusted source such as a public Internet connection, the Azure Virtual Datacenter model requires a full DMZ. To use this option, Contoso's perimeter network would include UDRs to send traffic to NVAs hosted on a DMZ subnet. This traffic gets processed, and only approved requests make it through either to the outside world or into the secured central IT hub virtual network, where it can be forwarded to the appropriate workspace spoke network.

▸ See also

[Azure Reference Architectures: Connect an On-premises Network to Azure]

[Azure Reference Architectures: DMZ between Azure and the Internet]

Administration and management

By default, Contoso's on-premises network lacks direct access to the virtual datacenter's virtual networks or connected resources. CorpSecOps needs to configure the central firewall and oversee other management tasks in the central IT infrastructure that are not available through the Azure portal or management APIs. To support this capability, Contoso will create a set of secured jumpbox virtual machines connected to the central IT hub network. They will configure UDR rules to allow administrators to connect to these virtual machines from the on-premises network, and directly access virtual machines and NVAs hosted in the virtual datacenter.

Jumpboxes are created inside a management subnet, and NSG rules applied to this subnet restrict access to specific IPs on the on-premises network. Contoso will be deploying two jumpboxes to the central IT infrastructure as an availability set. To gain access to these virtual machines, administrators must be authorized through the just in time access control mechanism.

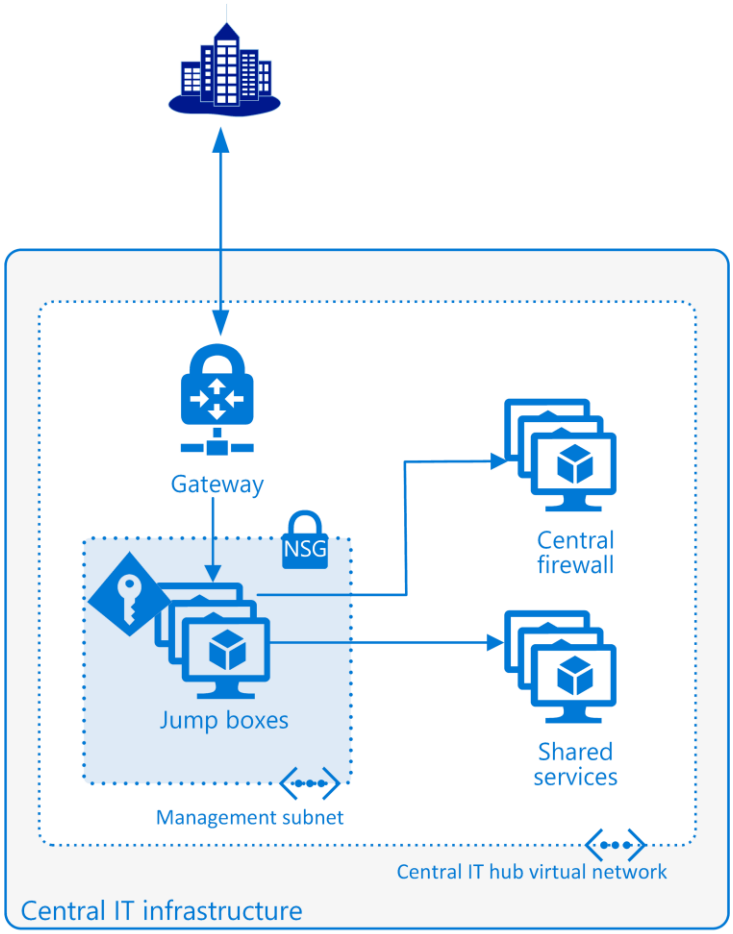

Figure 8. Administrators on-premises use hardened jumpboxes (bastion hosts) to remotely configure the central firewall and manage virtual machines and NVAs over the virtual network. NSGs restrict access to specific ports and IP addresses.

See also

Implementing Secure Administrative Hosts

Filter network traffic with network security groups

Shared services

The shared services subnet provides a central place to deploy core functionality used by workspaces. For example, workloads in the virtual datacenter need to resolve names for on-premises resources, and the on-premises network needs to resolve names for virtual datacenter resources, so Contoso deploys DNS as the first shared service. Contoso also wants to integrate their DNS infrastructure, so they can use consistent name resolution across virtual and on-premises environments.

Contoso will provide DNS services by creating a primary and secondary domain controller running Azure Active Directory Domain Services in the central IT infrastructure environment, configured to handle DNS resolution for the virtual datacenter. These servers are configured to forward DNS requests from the virtual datacenter to the on-premises environment, and the on-premises DNS servers are likewise configured to forward DNS requests for names of workspace resources to the shared services DNS servers.

See also

[Name Resolution for VMs and Role Instances]

Deploy workloads within workspaces

In their virtual datacenter implementation, Contoso considers DevOps at every layer, so teams stay productive and processes can be automated. Development teams need continuous integration and deployment pipelines, and all teams need to be able to monitor their workloads and resources.

Contoso's virtual datacenter policy manages workspaces as separate subscriptions, giving workload teams considerable control over their deployment environments. Developers get the agility Azure provides while remaining in compliance with the broader Contoso security and isolation policies enforced through the central IT infrastructure.

Workspace management roles

Earlier, Contoso defined workspace-specific SecOps, NetOps, SysOps and DevOps roles. These workspace management roles have control over the workspace subscription and any resources they deploy into it—within the confines of the central IT policy restrictions. When the workspace subscription is created, Resource Manager policies are set up to restrict external access and route all outbound traffic through the central IT infrastructure.

The workspace SecOps and NetOps roles have the responsibility to lock down the workspace virtual networks based on Contoso policy for each specific workload. DevOps teams can have considerable flexibility in deploying any operating resources they need to support a workload. If DevOps activities require Internet or ExpressRoute access, the traffic goes through the central IT hub virtual network controlled by the central IT CorpSecOps team. Central firewall rules must be implemented for this traffic to make it through to the on-premises network, and the CorpSecOps team will be responsible for reviewing and implementing any requested updates to the firewall.

Choosing the right service model for a workload

When planning workload deployments, Contoso DevOps teams can decide for themselves how much trust to hand over to the platform. Azure services offer a tradeoff between control and platform trust. Generalized cloud workloads fall into three broad categories, which represent a spectrum of control and trust on one end (IaaS) vs. the ease of management coupled with platform trust on the other (SaaS), with platform as a service (PaaS) in the middle.

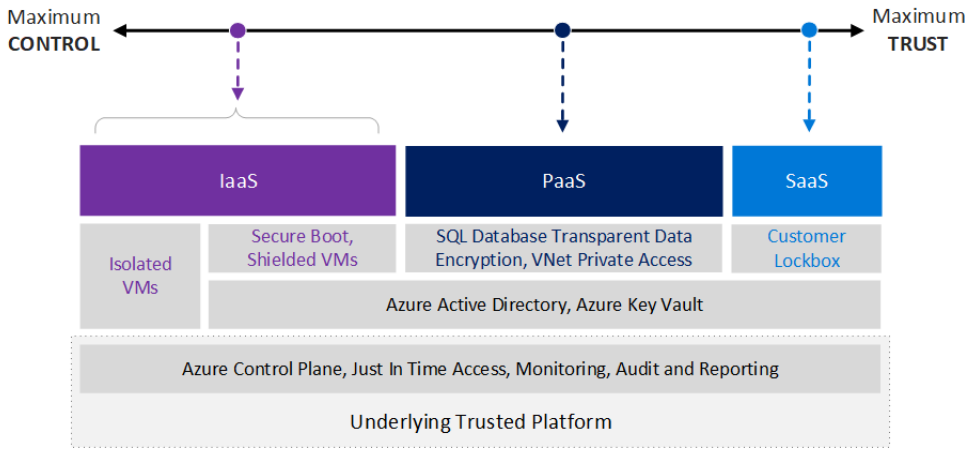

Figure 9. The Azure platform offers a range of options to suit the level of control DevOps needs for workloads deployed to the virtual datacenter.

Virtual network integration with PaaS

Some Contoso business units would like to use Azure PaaS offerings, such as Azure Batch, Azure SQL Database, and Azure Storage. Although these services provide security and encryption capabilities, by default most of them use a public endpoint for access. Contoso's security and network teams prefer to avoid any services that rely on public endpoints for access. Instead, they want services to be accessible only from inside workspace virtual networks.

They can integrate Azure services in a virtual network, which enables private, secured access for services such as HDInsight, Azure Batch, and Azure Storage. Two patterns are supported. In the first pattern, the service deploys dedicated instances into the virtual network, where they can only be used by resources with access to that network. Azure Batch and HDInsight follow this pattern.

The second pattern, virtual network service endpoints, is an Azure feature that extends a virtual network's private address space and identity to Azure services over a direct connection. This option helps secure service resources by allowing access only from the virtual network, providing private connectivity to these resources and preventing access from external networks. Service endpoints use the Microsoft backbone network and allow PaaS resources to be restricted to a single virtual network, or inside a single subnet capable of using NSGs to further secure network access.

Azure Storage and SQL Database follow this pattern. Additional Azure services are planning to support this feature in the future.

▸ See also

Virtual network integration for Azure services

Announcing Virtual Network integration for Azure Storage and Azure SQL

Virtual Network Service Endpoints

Auditing and logging

Governance and control of workloads begins with collecting log data, but Contoso also needs to trigger actions based on specific, reported events. Within the virtual datacenter, Azure resources

have logging policies enabled by default.

Different types of logging and monitoring services can be used to track the behavior of virtual datacenter resources. The Contoso SysOps team uses the two main types of logs offered by Azure:

- **Audit logs** (also called operational logs) provide insight into the operations performed on resources in an Azure subscription. Every Azure resource within a virtual datacenter produces audit logs.
- **Azure diagnostic logs** are generated by a resource and provide rich, frequent data about the operation of that resource. The content of these logs varies by resource type.

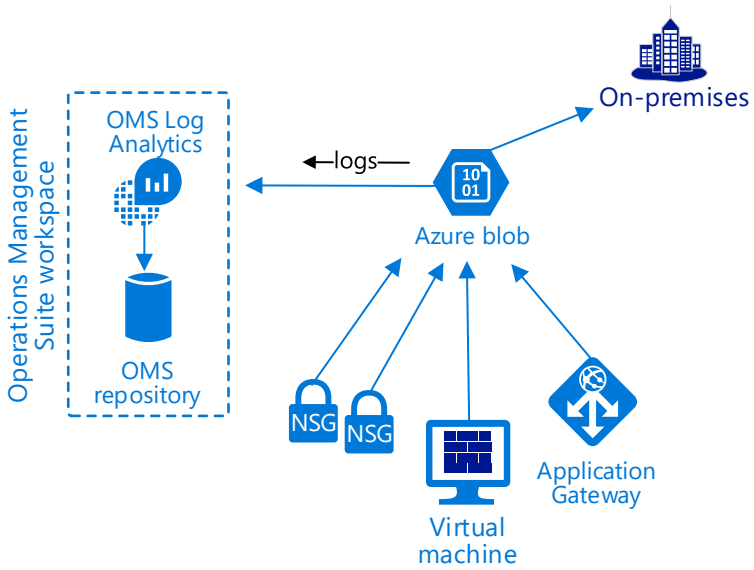

Figure 10. Virtual datacenter activities are continuously logged and monitored. Logging data is imported into OMS and is also available for use in on-premises log analytics.

Contoso wants to extend the standard monitoring framework already used for their on-premises systems and integrate the logs generated by virtual datacenter resources. If they want to keep logging activities in the cloud, they can use OMS. Its log analyzer helps to collect, correlate, search, and act on log and performance data generated by operating systems, applications, and infrastructure cloud components.

▸ See also

Azure Logging and Auditing

Use Azure security and monitoring tools

Continuous monitoring, auditing, and reporting are critical to proper governance. Azure provides Contoso an extensive set of management capabilities to help authorized individuals oversee the security configuration baselines and policy drift, network traffic, intrusion detection, and many other IT service management tasks. Most of these tasks can be handled by OMS, Azure Security Center, Azure Network Watcher, and Azure AD reporting.

Tool	Description
OMS	• Gives teams visibility and control across hybrid cloud implementations with simplified operations management and security. • Offers real-time operational insights through integrated search and custom dashboards that analyze all the records across all workloads in a virtual datacenter.
Azure Monitor	• Monitors across Azure resources. • Supports performance metrics and diagnostic logging. • Provides integration with SQL Database, NSGs, and Azure Blog Storage. • Supports custom alert rules that can notify teams of performance issues and trigger automated actions.
Azure AD	• Helps secure virtual datacenter resources by providing diagnostic reports. • Provides reports on sign-on anomalies, the use of integrated applications, errors, and even specific users. Offers activity logs of all audited events, group activities, password resets, and registration activities.
Azure Security Center	• Detects security threats or breaches within a virtual datacenter and helps to detect, prevent, and respond to threats to hosted resources. • Provides security monitoring and centralized policy management across Azure subscriptions used in a virtual datacenter. • Supports definition of security policies for resources within a specified subscription or resource group, alerts the appropriate security teams of any policy violations, and offers recommendations for remediation.

	• Collects, analyzes, and fuses log data from compute services, network resources, and partner solutions such as firewalls. • Supports Microsoft Digital Crimes Unit, the Microsoft Security Response Center (MSRC), and other resources designed to stop attacks and prevent future attacks.
Azure Network Watcher	• Provides network monitoring capabilities so you can visualize network topologies and identify unhealthy connections and resources. • Includes diagnostics for connectivity, latency, DNS check, trace route, IP flow verification, security group views, next hop, and packet capture. • Reveals performance and health through flow analysis, security analysis, bandwidth usage, protocol analyzer, and network subscription limits. • Shows configurations and views of all network logs and alerts.

▸ See also

Azure Operational Security best practices

Best practices for creating management solutions in Operations Management Suite (OMS)

Azure Architecture Center - Best Practices: Monitoring and diagnostics

Final Contoso architecture

The finished Contoso architecture lays out a complete trusted datacenter extension to their existing on-premises IT infrastructure. The following table summarizes the decisions they made, shown in Figure 11.

Area	Decisions
Identity management	• Roles in place • RBAC rules configured for central IT infrastructure • RBAC rules configured for workspaces • Azure AD Connect set up to synchronize users and roles with on-premises Active Directory
Subscription	• Separate subscriptions for central IT infrastructure and each workspace • Subscription-level access control and policy
Network	• No public Internet access allowed from within the virtual

	datacenter • DNS services configured and integrated with the on-premises network • ExpressRoute connection between the virtual datacenter and on-premises network • Central IT hub network • Central firewall to inspect traffic between the on-premises network and workspace networks • Connectivity between central IT and workspace virtual networks via virtual network peering • Workspace subscription policies, NSGs, and UDRs
Management	• Management jumpboxes accessible only from on-premises network when authorized through the just in time access authorization mechanism

When complete, the Contoso virtual datacenter is ready to deploy workloads accessible only through the central IT infrastructure, and subject to the access controls, policy, and networking configuration enforced by Contoso's central IT management team.

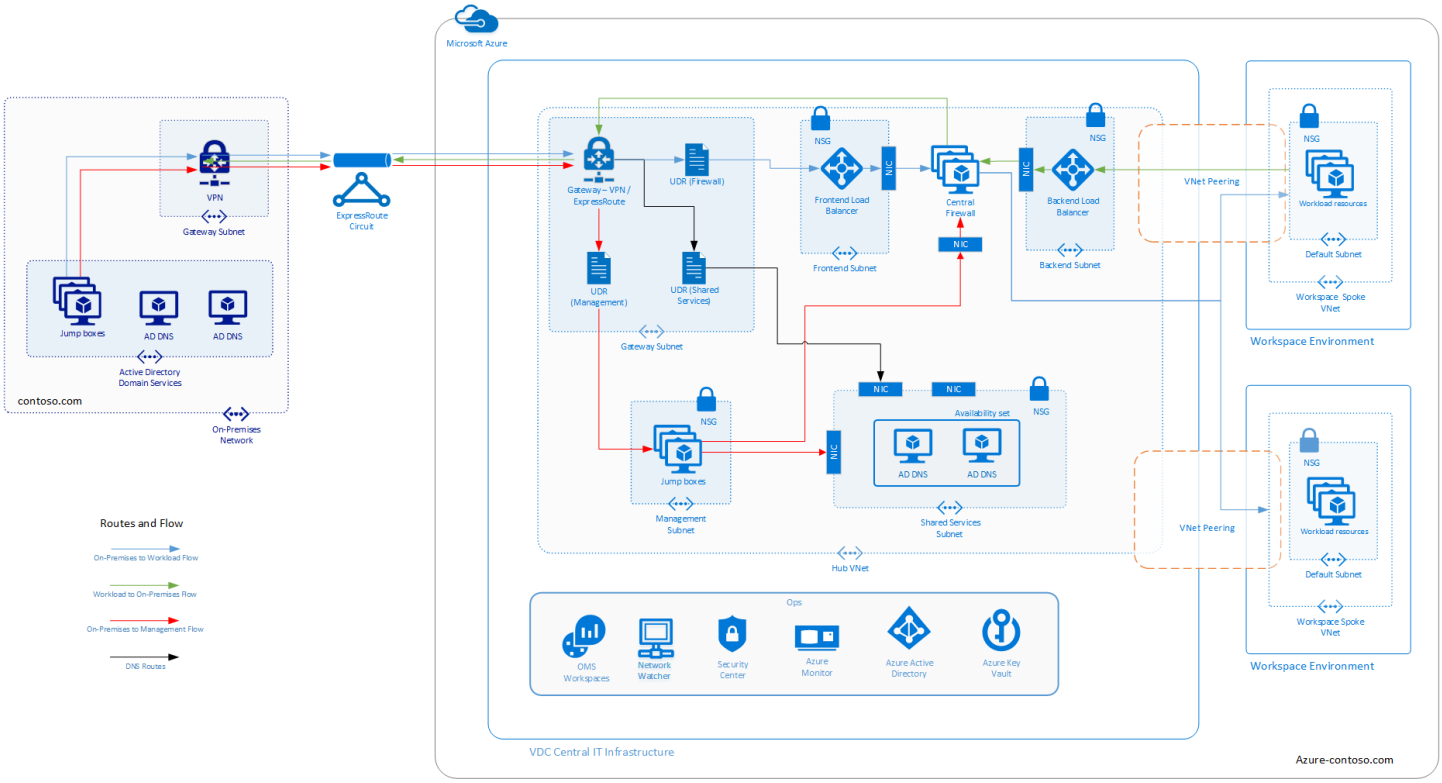

Figure 11. Final Contoso architecture with major components and traffic flows (on-premises to workload, workload to on-premises, on-premises to management, and DNS).

PART 3
The cloud datacenter transformation

Cloud datacenter transformation is an ongoing process to modernize your IT infrastructure and take advantage of the cloud. As part of this process, your organization needs to plan how to make use of the Azure cloud, and how to best structure workloads to most efficiently use your existing on-premises assets in combination with cloud resources. The Azure Virtual Datacenter model offers a starting point on this journey.

Balancing governance and agility

As part of any cloud datacenter transformation, enterprise IT and governance teams have two high-level goals: the ability to create isolation boundaries around applications, and the ability to enforce those boundaries with policy. Developers and their line-of-business (LOB) sponsors have goals, too: to make the most of the agility cloud platforms offer to drive competitive advantages. Striking a balance between these two factors is the objective of the Azure Virtual Datacenter model.

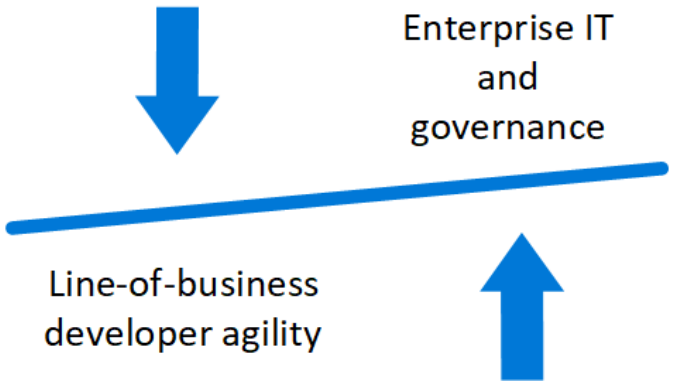

Figure 12: Enterprise IT and governance should be balanced against developer agility in a successful cloud datacenter transformation.

Enterprise IT wants their cloud-based applications to be governed by many of the same policies as their on-premises implementations. Even born-in-the-cloud applications, especially multitenant PaaS offerings and SaaS application such as Office 365, need to have well defined isolation boundaries and role-based policy enforcement. The Azure Virtual Datacenter model begins to give enterprise IT the controls they need to enforce governance.

Virtual datacenter patterns

In the datacenter and application transformation journey, three distinct workload patterns emerge:

- IaaS compute resources with data remaining in the on-premises datacenter.
- IaaS with data using cloud-based storage, but with minimal use of other PaaS (besides storage).
- Cloud applications composed entirely of multiple platform services.

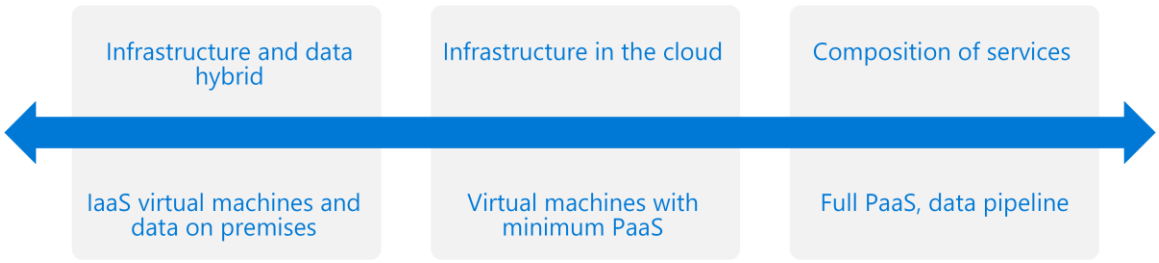

Figure 13: Virtual datacenter patterns showing the range of platform services used. On one end, IaaS virtual machines use only on-premises data; on the other, the full use of cloud-based PaaS services.

The first pattern is usually called a partial lift and shift, or strictly IaaS, where no multitenant platform services are consumed. In this pattern, the virtual machines processing data are hosted in the cloud, but all data is stored on-premises and accessed over ExpressRoute. Even Active Directory services are located on-premises. This pattern includes scenarios where the data can flow to the cloud in an anonymized or tokenized fashion. Such scenarios remove much of the data sensitivity but severely limit what types of processing that can be done with that data.

The second pattern involves a limited integration of IaaS resources to build a basic cloud infrastructure. For example, virtual machines may make use of essential PaaS services such as Storage or Key Vault. Some additional services such as Azure SQL Database may also be consumed to provide cost and management savings.

The third pattern fully uses PaaS services to construct a complete solution such as an Azure data analytics pipeline (IoT Hub, Azure Machine Learning, HDInsight, Azure Data Lake).

Moving forward with Azure Virtual Datacenter

The Azure Virtual Datacenter model provides guidance for a coherent and consistent deployment model of workloads in the Azure cloud. The first edition of this model focuses on creating a trusted datacenter extension for virtual machine-based workloads hosted on the public cloud.

Future editions of this model will show how additional elements can be used to achieve isolation of more complex scenarios, such as orchestrator based workloads, or workloads composed of platform services. Future models will also support secure Internet access directly from the virtual datacenter.

Virtual Datacenter Automation

The Virtual Datacenter Automation guidance (currently being used in select initial deployments) is a set of Python and Azure CLI V2 scripts, Resource Manager templates, and documentation. The goal of this guidance is to provide everything necessary to create a working example of a virtual datacenter on Azure.

The first version of the automation guidance focuses on creating a trusted datacenter extension like the Contoso example described in this document. This involves creating an isolated virtual

datacenter connected to your on-premises networks through ExpressRoute or a VPN connection. It includes instructions for configuring the parameters needed to create a virtual datacenter that can connect to your existing network resources.

To learn more about Virtual Datacenter Automation, contact your Microsoft Account Team and visit the Azure Architecture reference site.

Glossary of key features and services

The following technologies, features, and concepts are key to composing a trusted datacenter extension based on the Azure Virtual Datacenter model.

Azure Active Directory Provides authentication and access control capabilities for Azure-based resources. Azure AD is a cloud-based, multitenant directory and identity service. Azure AD supports integration with on-premises identity providers and supports RBAC and just in time access controls. Azure AD supports MFA using phone, text, mobile app, or custom authentication methods using an oAuth token. A good practice is to enable MFA for your various IT roles and application users.

Azure Key Vault The primary mechanism for storing, managing, and accessing cryptographic keys on the Azure platform. Key Vault is a centralized service that provides management for certificates, connection strings, secrets, and cryptographic keys used to encrypt storage assets and secure PaaS services or individual applications. With Key Vault, you can use cryptographic keys generated and managed by Microsoft, or custom keys managed by your organization and uploaded to Key Vault. It supports a virtual HSM container service that provides access to physical HSMs.

Azure Resource Manager Provides the mechanism for provisioning and managing resources within a virtual datacenter. Resource Manager and related APIs allow you to implement policies enforcing data residency when creating resources.

Disaster recovery A process used to help recover data and ensure business continuity in the case of a major technology infrastructure and systems failure.

ExpressRoute Supports private connections between Azure datacenters and infrastructure on your premises or in a colocation environment. ExpressRoute connections don't go over the public Internet, and they offer more reliability, faster speeds, and lower latencies than typical Internet connections.

FIPS Federal Information Processing Standard.

Homomorphic Encryption (HE) Refers to a special type of encryption technique that allows for computations to be done on encrypted data, without requiring access to a secret (decryption) key. The results of the computations remain encrypted and can be revealed only by the owner of the secret key.

HSM Hardware security module.

IaaS Infrastructure as a service.

Just in time VM access Just in time virtual machine (VM) access can be used to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.

Load balancer In Azure, a Layer 4 (TCP, UDP) load balancer that distributes incoming traffic among resources in your virtual network.

MFA Multi-Factor Authentication.

Network security group (NSG) Simple, stateful packet inspection devices that allow the creation of allow/deny rules for network traffic. An NSG can allow or deny traffic to and from a single IP address, to and from multiple IP addresses, or even to and from entire subnets. When an NSG is associated with a subnet, the rules apply to all resources connected to the subnet. Traffic can further be restricted by also associating additional NSGs to individual virtual machines.

Network virtual appliance (NVA) A dedicated and preconfigured virtual machine image designed to handle the type of networking and security functionality traditionally handled by gateways, routers, and firewall devices.

NVA Network virtual appliance.

PaaS Platform as a service.

RBAC Role-based access control.

Resource group A collection of Azure resources, such as virtual machines, services, and networking devices within a subscription. You can apply access control and security policies at the resource group level, rather than managing individual resources.

Secure Boot An upcoming feature in Azure. Secure Boot will make sure each component loaded during the boot process is digitally signed and validated.

Shielded virtual machine An upcoming feature in Azure designed to protect virtual machines from compromised or malicious administrators. Shielded virtual machines encrypt the disk and state of virtual machines so only the virtual machine or tenant administrators can access it. Shielded virtual machines use a virtual TPM module, are encrypted using BitLocker, and only run on approved hosts.

SSE Storage Service Encryption.

SSL Secure Sockets Layer.

Subscription The outermost Azure environment holding all the virtualized resources, applications, and other constructs used for billing and management. Each subscription has a trust relationship with a single Azure AD directory.

TLS Transport Layer Security.

User-defined route (UDR) Custom route tables you create within your virtual network. UDRs are attached to subnets within your virtual networks and establish next-hop and IP forwarding rules for any traffic leaving that subnet.

Virtual machine (VM) An on-demand, scalable Azure compute resource. A virtual machine can run Windows or Linux based workloads in the Azure virtual environment.

Virtual network A logical representation of your network in the cloud. On the Azure platform, virtual networks act as a cloud analog to physical networks on-premises. Virtual networks also provide the default isolation boundary between resources on the platform. Sometimes called a VNet.

VM Virtual machine.

VPN Virtual private network.

VPN gateway A type of network connection that sends encrypted traffic across a shared or public network. The Azure VPN Gateway service connects your on-premises networks to Azure through site-to-site VPNs, similar to the way you set up and connect to a remote branch office. Connectivity uses the industry-standard protocols, Internet Protocol Security (IPsec) and Internet Key Exchange (IKE).

For more information

Azure Platform

- Azure datacenters: https://azure.microsoft.com/en-us/overview/datacenters/
- Overview of Availability Zones in Azure: https://docs.microsoft.com/en-us/azure/availability-zones/az-overview
- High availability for applications built on Microsoft Azure https://docs.microsoft.com/en-us/azure/architecture/resiliency/high-availability-azure-applications
- Azure subscription and service limits, quotas, and constraints: https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits
- Azure Security Center: https://azure.microsoft.com/en-us/services/security-center/
- Microsoft Trust Center—Compliance: https://www.microsoft.com/en-us/TrustCenter/Compliance/default.aspx
- Microsoft Trust Center—Design and operational security: https://www.microsoft.com/en-us/trustcenter/security/designopsecurity
- Microsoft Trust Center—Transparency: https://www.microsoft.com/en-us/trustcenter/about/transparency
- Red Teaming: Using Cutting-Edge Threat Simulation to Harden the Microsoft Enterprise Cloud: https://azure.microsoft.com/en-us/blog/red-teaming-using-cutting-edge-threat-simulation-to-harden-the-microsoft-enterprise-cloud/

Identity and Azure Active Directory

- Azure Active Directory Documentation: https://docs.microsoft.com/en-us/azure/active-directory/
- What is Azure Multi-Factor Authentication? https://docs.microsoft.com/en-us/azure/multi-factor-authentication/multi-factor-authentication
- Microsoft hybrid identity solutions: https://docs.microsoft.com/en-us/azure/active-directory/choose-hybrid-identity-solution

- Integrate your on-premises directories with Azure Active Directory: https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect
- Azure AD Connect and federation: https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnectfed-whatis

Isolation and security

- Microsoft Service Trust documents: https://servicetrust.microsoft.com/Documents/TrustDocuments
- Introduction to Azure Security: https://docs.microsoft.com/en-us/azure/security/azure-security
- Isolation in the Azure Public Cloud: https://docs.microsoft.com/en-us/azure/security/azure-isolation
- Microsoft Cloud Security for Enterprise Architects: https://www.microsoft.com/en-us/download/48121
- Azure network security: https://docs.microsoft.com/en-us/azure/security/azure-network-security
- Azure Virtual Machines security overview: https://docs.microsoft.com/en-us/azure/security/security-virtual-machines-overview
- Manage virtual machine access using just in time (Preview): https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time
- Azure Storage security guide: https://docs.microsoft.com/en-us/azure/storage/common/storage-security-guide

Encryption

- Encryption in the Microsoft Cloud: https://www.microsoft.com/en-us/download/details.aspx?id=55848
- What is Azure Key Vault? https://docs.microsoft.com/en-us/azure/key-vault/key-vault-whatis
- Azure Storage Service Encryption for Data at Rest: https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption
- Azure Disk Encryption for Windows and Linux IaaS VMs: https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption
- How to generate and transfer HSM-protected keys for Azure Key Vault: https://docs.microsoft.com/en-us/azure/key-vault/key-vault-hsm-protected-keys
- Introducing Azure confidential computing: https://azure.microsoft.com/en-us/blog/introducing-azure-confidential-computing/
- Homomorphic Encryption: https://www.microsoft.com/en-us/research/project/homomorphic-encryption/

- Manual for Using Homomorphic Encryption for Bioinformatics: https://www.microsoft.com/en-us/research/publication/manual-for-using-homomorphic-encryption-for-bioinformatics/
- Dubai Security Blog—Diving into Secure Boot: https://blogs.technet.microsoft.com/dubaisec/2016/03/14/diving-into-secure-boot/
- A closer look at shielded VMs in Windows Server 2016: https://blogs.technet.microsoft.com/windowsserver/2016/05/10/a-closer-look-at-shielded-vms-in-windows-server-2016/

Virtual networking

- Microsoft Azure Virtual Data Center (VNet-focused): https://docs.microsoft.com/en-us/azure/networking/networking-virtual-datacenter
- Network security groups in Azure: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg
- User-defined routes and IP forwarding in Azure: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview
- Network Virtual Appliances: https://azure.microsoft.com/en-us/solutions/network-appliances/
- Virtual appliance scenario: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-scenario-udr-gw-nva
- Connect an on-premises network to Azure: https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/
- Implementing a DMZ between Azure and the Internet: https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/dmz/secure-vnet-dmz
- Implementing Secure Administrative Hosts: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-secure-administrative-hosts
- Resolution for VMs and Role Instances: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-name-resolution-for-vms-and-role-instances
- Virtual network for Azure services: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure-services
- Announcing Virtual Network integration for Azure Storage and Azure SQL: https://azure.microsoft.com/en-us/blog/announcing-virtual-network-integration-for-azure-storage-and-azure-sql/
- Azure virtual network service endpoints: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview
- High Availability Ports overview: https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-ha-ports-overview

Operations

- Azure Operational Security best practices: https://docs.microsoft.com/en-us/azure/security/azure-operational-security-best-practices
- OMS Management solution best practices: https://docs.microsoft.com/en-us/azure/operations-management-suite/operations-management-suite-solutions-best-practices
- Monitoring and diagnostics guidance: https://docs.microsoft.com/en-us/azure/architecture/best-practices/monitoring