HITRUST

6175 Main Street
Suite 420
Frisco, TX 75034

855.HITRUST
(855-448-7878)
www.HITRUSTAlliance.net

July 8, 2019

Microsoft Azure
1 Microsoft Way
Redmond, WA 98052

Based upon representation from management as to the accuracy and completeness of information provided, the procedures performed by an Authorized External Assessor to validate such information, and HITRUST's independent confirmation that the work was performed in accordance with the HITRUST® CSF Assurance Program, the following systems and infrastructure of the Organization ("Scope") meet the HITRUST CSF® v9.2 certification criteria:

> Microsoft Azure: AI + Machine Learning (Azure Public Cloud); Azure Compute (Azure Public Cloud, Azure Government, Azure Germany); Azure Containers (Azure Public Cloud); Analytics (Azure Public Cloud, Azure Government);Azure Databases (Azure Public Cloud, Azure Government, Azure Germany); Azure Developer Tools (Azure Public Cloud); Azure Integration (Azure Public Cloud); Azure Internet of Things (Azure Public Cloud, Azure Government, Azure Germany); Azure Management Tools (Azure Public Cloud, Azure Government, Azure Germany); Azure Networking (Azure Public Cloud, Azure Government, Azure Germany); Azure Security + Identity (Azure Public Cloud, Azure Government, Azure Germany); Azure Storage (Azure Public Cloud, Azure Government, Azure Germany); Azure Web + Mobile (Azure Public Cloud, Azure Government, Azure Germany); Microsoft Online Services (Azure Public Cloud, Azure Government, Azure Germany); Internal Supporting Infrastructure (Azure Public Cloud, Azure Government, Azure Germany); and Azure Datacenters (Azure Public Cloud, Azure Government, Azure Germany)

The certification is valid for a period of two years assuming the following occurs:

- A monitoring program is in place to determine if the controls continue to operate effectively over time,
- Annual progress is being made on areas identified in the Corrective Action Plan(s) (CAPs),
- No data security breach reportable to a federal or state agency by law or regulation has occurred,
- No significant changes in the business or security policies, practices, controls, and processes have occurred that might impact its ability to meet the HITRUST CSF certification criteria, and
- Timely completion of the interim assessment as defined in the HITRUST CSF Assurance Program Requirements.

HITRUST

6175 Main Street
Suite 420
Frisco, TX 75034

855.HITRUST
(855-448-7878)
www.HITRUSTAlliance.net

HITRUST has developed the HITRUST CSF, a certifiable framework that provides organizations with the needed structure, detail and clarity relating to information protection. With input from leading organizations within the industry, HITRUST identified a subset of the HITRUST CSF control requirements that an organization must meet to be HITRUST CSF Certified. For those HITRUST CSF control requirements that are not currently being met, the Organization must have a CAP that outlines its plans for meeting such requirements.

HITRUST performs a quality assurance review consistent with the HITRUST CSF Assurance Program requirements to ensure that the scores are consistent with the testing performed by the Authorized External Assessor. In addition to the full report that follows, users of the report can refer to the document Leveraging HITRUST CSF Assessment Reports: A Guide for New Users for questions on interpreting the results contained herein or contact HITRUST customer support at support@hitrustalliance.net. A full copy of the HITRUST CSF Certification Report has also been issued to the organization listed above; if interested in obtaining a copy of the full report, you will need to contact the organization directly. Users of this report are also assumed to be familiar with and understand the services provided by the Organization listed above, and what specific services are being used by the user organization.

Additional information on the HITRUST CSF Certification program can be found at the HITRUST website at https://hitrustalliance.net.

HITRUST

Assessment Context

Prepared for	Microsoft Azure One Microsoft Way Redmond, WA 98052
Contact	Alan Luk Principal PM alanluk@microsoft.com
Date of Report	July 8, 2019
Period of Assessment	April 3, 2019 – July 3, 2019
Period of HITRUST QA	October - November, 2019
Assessment Option	HITRUST CSF Security Assessment
Procedures Performed by Assessor	On-site 3rd party testing included: • Interviews • Review of documents • Review and testing of technical settings
Company Background	Microsoft Azure is a cloud computing platform for building, deploying, and managing applications through a global network of Microsoft and third-party managed datacenters. It supports both Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) cloud service models and enables hybrid solutions that enable cloud services with customers' on-premises resources. Microsoft Azure supports many customers, partners, and government organizations that span across a broad range of products and services, geographies, and industries. Microsoft Azure is designed to meet their security, confidentiality and compliance requirements. Microsoft datacenters support Microsoft Azure and many other Microsoft Online Services ("Online Services"). Online Services such as Graph, Power BI and others are Software as a Service (SaaS) services that leverage the underlying Microsoft Azure platform and datacenter infrastructure.
Number of Employees	20000
Geographic Scope of Operations Considered for the Assessment	Off-shore (outside U.S.)
Organizational Risk Factors	
Number of Records that are currently held:	More than 60 Million Records
Systematic Risk Factors	
Does the system(s) store, process, or transmit PHI?	No
Is the system(s) accessible from the Internet?	Yes
Is the system(s) accessible by a Third Party?	No

Does the system(s) transmit or receive data with a third party/business partner?	No
Is the system(s) accessible from a public location?	No
Are Mobile devices used in the environment?	No
Number of interfaces to other systems:	Greater than 75
Number of users of the system(s):	Greater than 5,500
Number of transactions per day:	Greater than 85,000

Regulatory Risk Factors

None selected

Scope of Systems in the Assessment

Organization and Industry Segment Overview

Microsoft Azure is a cloud service provider, offering hardware, infrastructure, and computing platforms for building, deploying, and managing applications and services. Azure supports many customers, partners, and government organizations that span a broad range of products and services, geographies, and industries. Microsoft Azure does this through a global network of Microsoft Corporation and third-party managed datacenters. Microsoft Azure includes Azure Public Cloud, Azure Government, and Azure Germany. Microsoft Azure supports both Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) offerings. Microsoft Azure product offerings are designed to meet their customers' security, privacy, and compliance requirements. Microsoft Azure physical infrastructure is owned and managed by Microsoft Cloud Infrastructure and Operations (MCIO).

Service(s) / Product(s) Provided

Microsoft Azure offers their customers IaaS and PaaS solutions, which their customers may use to store, process, or transmit electronic protected health information (ePHI) and other protected information. The scope of this HITRUST engagement is restricted to the management layer of the Azure infrastructure, and no customer deployments within the Azure IaaS and PaaS environments. As a business, Microsoft Azure does not store, process, or transmit patient health data (ePHI). Microsoft Azure customers are responsible for the security of the ePHI they store, process, or transmit. In order to provide the highest level of assurance to its customers, the Microsoft Azure environment was assessed with the assumption all IaaS and PaaS deployments could contain ePHI. Azure does not have access to their customers' data, including ePHI.

Primary System(s)

The types of systems used to provide the IaaS and PaaS services are listed below in the Scope Overview section of this document. These systems incorporate and interact with various information security components including the following:

Components	Description
Operating Systems	Windows Server and Client versions; multiple Linux variants
Virtualization Platforms	Custom hypervisors to manage resources, enhance isolation of multitenant client environments, and realize efficiencies
Database Platforms	Multiple platforms and versions, supporting service implementations and functioning as services themselves
Web Portals	Custom interfaces to support client and service management

Components	Description
Encryption Mechanisms	Custom implementations including Hardware Security Modules (HSMs)
Virtual Private Networks	Remote access methods for system administration and client access
Jumpboxes	Server-based logical isolation of sensitive data environments
Routers and Switches	Network devices architected in a tiered design to enhance management and isolation of sensitive data transmissions
Firewall	Network devices to filter traffic to/from sensitive environments, and between the client and management networks
Antimalware Mechanisms	Both industry and custom endpoint protection solutions for service and client virtual machines
Vulnerability Scanner	Mechanisms for internal and external scanning of both service and client resources
Change Management	Software tools to track and record approval of infrastructure and application change
Secret Store	Secure encrypted storage of Microsoft Azure and customer secrets and keys

Datacenter Facilities:

Microsoft Azure also uses facilities located around the world. The codes listed after each location represent the facilities in that location.

North America	Europe	Asia	South America	Australia
Santa Clara, CA (BY1/2/3/4/21 /22)	Vienna, Austria (VIE)	Hong Kong (HK1/2, HKG20)	Campinas, Brazil (CPQ01/02)	Macquarie Park (SYD03)
Phoenix, AZ (PHX20)	Helsinki, Finland (HEL01)	Mumbai, India (BOM01)	Fortaleza, Brazil (FOR01)	Melbourne (MEL01)
Des Moines, IA (DM1/2/3, DSM05)	Amsterdam, Netherlands (AM1/2/3, AMS04/05/06/20)	Dighi, India (PNQ01)	Rio de Janeiro, Brazil (RIO01)	
Chicago, IL (CH1/3, CHI20)	Durham, United Kingdom (MME20)	Ambattur, India (MAA01)	Sao Paulo, Brazil (GRU)	
San Antonio, TX (SN1/2/3/4/5/6)	Chessington, United Kingdom	Osaka, Japan (OSA01/02/20)	Santiago, Chile (SCL01)	

North America	Europe	Asia	South America	Australia
	(LON20)			
Ashburn, VA (BL2/3/5/7)	London, United Kingdom (LON21)	Tokyo, Japan (KAW, TYO01/21/22)	Humacao, Puerto Rico (PR1)	
Boydton, VA (BN1/3/4/6)	Cardiff, United Kingdom (CWL20)	Cyberjaya, Malaysia (KUL01)		
Bristow, VA (BLU)	Dublin, Ireland (DB3/4/5, DUB06/07/20)	Singapore (SG1/2/3, SIN20)		
Reston, VA (BL4/6/30)	Paris, France (PAR02/20/21/22)	Busan, South Korea (PUS01, PUS20)		
Tukwila, WA (TK5)	Marseille, France (MRS20)	Seoul, South Korea (SEL20)		
Quincy, WA (CO1/2, MWH01)	Frankfurt, Germany (FRA20)			
Cheyenne, WY (CYS01/04)				
San Jose, CA (SJC31)				
Sterling, VA (BL20)				
Toronto, Canada (YTO20)				
Quebec City, Canada (YQB20)				

Service(s) Outsourced

Microsoft Azure has outsourced a very small number of services. Specifically, some data centers are outsourced to third-party datacenter hosting providers.

Scope Overview

Microsoft Azure offers three distinct environments for its customers: Azure Public Cloud, Azure Germany, and Azure Government. The following chart depicts the service offerings and environment.

System Name	Components	Service Offering	Full	Partial	With Exclusions	Description of Exclusions
AI + Machine Learning (Azure Public Cloud)	Microsoft Windows Server 2012 Ubuntu Linux	Azure Bot Service	X			
		Azure Machine Learning Service				

System Name	Components	Service Offering	Full	Partial	With Exclusions	Description of Exclusions
	Microsoft SQL Server 2012	Cognitive Services				
		Cognitive Services Computer Vision				
		Cognitive Services Content Moderator				
		Cognitive Services Custom Vision				
		Cognitive Services Face				
		Cognitive Services Language Understanding				
		Cognitive Services QnA Maker				
		Cognitive Services Speech Services				
		Cognitive Services Text Analytics				
		Cognitive Services Translator Speech				
		Cognitive Services Translator Text				
		Cognitive Services Video Indexer				
		Machine Learning Studio				
		Microsoft Genomics				
		Microsoft Healthcare Bot				
Azure Compute (Azure Public Cloud, Azure Government, Azure Germany)	Microsoft Windows Server 2012 Ubuntu Linux Custom Hardware	Azure Functions		X	X	The following environments do not offer the listed services: **Azure Germany** • Azure Functions
		Azure Migrate				
		Azure Red Hat OpenShift				
		Batch				
		Cloud Services				
		Service Fabric				

System Name	Components	Service Offering	Full	Partial	With Exclusions	Description of Exclusions
		Virtual Machines (including SQL VM) Virtual Machine Scale Sets				• Azure Migrate • Azure Red Hat OpenShift **Azure Government** • Azure Red Hat OpenShift
Azure Containers (Azure Public Cloud)	Microsoft Windows Server 2012 Ubuntu Linux Custom Hardware	Azure Container Service Azure Kubernetes Service (AKS) Container Instances Container Registry	X			
Analytics (Azure Public Cloud, Azure Government,	Microsoft Windows Server 2012 Ubuntu Linux Microsoft SQL Server 2012 Custom Hardware	Azure Analysis Services Azure Data Explorer Azure Stream Analytics Azure Time Series Insights Data Lake Analytics HDInsight		X	X	The following environments do not offer the listed services: **Azure Germany** • Azure Data Explorer • Azure Time Series Insights • Data Lake Analytics **Azure Government** • Azure Stream Analytics • Azure Time Series Insights • Data Lake Analytics
Azure Databases (Azure Public Cloud, Azure Government, Azure Germany)	Microsoft Windows Server 2012 Ubuntu Linux Microsoft SQL Server 2012 Custom Hardware	Azure Cosmos DB Azure Database for MariaDB Azure Database for MySQL Azure Database for PostgreSQL Azure Database Migration Service Azure SQL Database		X	X	The following environments do not offer the listed services: **Azure Germany** • Azure Database for MariaDB • Azure Database for MySQL

System Name	Components	Service Offering	Full	Partial	With Exclusions	Description of Exclusions
		Redis Cache SQL Data Warehouse SQL Server Stretch Database				• Azure Database for PostgreSQL • Azure Database Migration Service **Azure Government** • Azure Database Migration Service
Azure Developer Tools (Azure Public Cloud)	Microsoft Windows Server 2012 Ubuntu Linux Custom Hardware	Application Insights Azure Lab Services	X			
Azure Integration (Azure Public Cloud)	Microsoft Windows Server 2012 Ubuntu Linux Custom Hardware	API Management Azure API for FHIR Data Catalog Logic Apps Service Bus	X			
Azure Internet of Things (Azure Public Cloud, Azure Government, Azure Germany)	Microsoft Windows Server 2012 Ubuntu Linux Custom Hardware	Azure IoT Central Azure IoT Hub Event Grid Event Hubs Notification Hubs		X	X	The following environments do not offer the listed services: **Azure Germany** • Azure IoT Central • Event Grid **Azure Government** • Azure IoT Central
Azure Management Tools (Azure Public Cloud, Azure Government, Azure Germany)	Microsoft Windows Server 2012 Ubuntu Linux Custom Hardware	Automation Azure Advisor Azure Monitor Azure Policy Azure Resource Manager Cloud Shell Log Analytics Microsoft Azure Portal		X	X	The following environments do not offer the listed services: **Azure Germany** • Automation • Azure Advisor • Azure Policy • Cloud Shell • Log Analytics

System Name	Components	Service Offering	Full	Partial	With Exclusions	Description of Exclusions
		Scheduler				
Azure Networking (Azure Public Cloud, Azure Government, Azure Germany)	Microsoft Windows Server 2012 Ubuntu Linux Custom Hardware (Cisco, Juniper)	Application Gateway Azure Bastion Azure DDoS Protection Azure DNS Azure Firewall Azure Front Door Service Content Delivery Network (including Microsoft CDN) ExpressRoute Load Balancer Network Watcher Traffic Manager Virtual Network VPN Gateway		X	X	The following environments do not offer the listed services: **Azure Germany** • Azure Bastion • Azure DDoS Protection • Azure Firewall • Azure Front Door Service • Content Delivery Network (including Microsoft CDN) **Azure Government** • Azure Bastion • Azure Front Door Service • Content Delivery Network (Including Microsoft CDN)
Azure Security + Identity (Azure Public Cloud, Azure Government, Azure Germany)	Microsoft Windows Server 2012 Ubuntu Linux Custom Hardware	Azure Active Directory (Free, Basic) Azure Active Directory (Premium) Azure Active Directory B2C Azure Active Directory Domain Services Azure Advanced Threat Protection Azure Dedicated HSM Azure Information Protection Key Vault		X	X	The following environments do not offer the listed services: **Azure Germany** • Azure Active Directory (Premium) • Azure Active Directory (B2C) • Azure Active Directory Domain Services • Azure Advanced Threat Protection

System Name	Components	Service Offering	Full	Partial	With Exclusions	Description of Exclusions
		Multi-Factor Authentication (MFA) Security Center				• Azure Dedicated HSM • Azure Information Protection • Security Center **Azure Government** • Azure Active Directory B2C • Azure Active Directory Domain Services • Azure Advanced Threat Protection • Azure Dedicated HSM
Azure Storage (Azure Public Cloud, Azure Government, Azure Germany)	Microsoft Windows Server 2012 Ubuntu Linux Custom Hardware	Azure Archive Storage Azure Data Lake Storage Gen 1 Backup Import/Export Site Recovery Storage (Blobs (including Azure Data Lake Storage Generation 2), Disks, Files, Queues, Tables, Cool and Premium) StorSimple		X	X	The following environments do not offer the listed services: **Azure Germany** • Azure Archive Storage • Azure Data Lake Storage Gen1 • Import/Export • StorSimple **Azure Government** • Azure Data Lake Storage Gen1
Azure Web + Mobile (Azure Public Cloud, Azure Government, Azure Germany)	Microsoft Windows Server 2012 Ubuntu Linux Custom Hardware	App Service Azure Search Azure SignalR Service Media Services		X	X	The Following environments do not offer the listed services: **Azure Germany** • Azure Search • Azure SignalR Service

System Name	Components	Service Offering	Full	Partial	With Exclusions	Description of Exclusions
						Azure Government • Azure Search • Azure SignalR Service
Microsoft Online Services (Azure Public Cloud, Azure Government, Azure Germany)	Microsoft Windows Server 2012 Ubuntu Linux Custom Hardware	Dynamics 365 AI for Customer Insights Dynamics 365 Customer Engagement Dynamics 365 for Marketing Dynamics 365 Fraud Protection Microsoft Cloud App Security Microsoft Flow Microsoft Graph Microsoft Intune Microsoft PowerApps Microsoft Stream Power BI Power BI Embedded		X	X	The Following environments do not offer the listed services: **Azure Germany** • Dynamics 365 AI for Customer Insights • Dynamics 365 Customer Engagement • Dynamics 365 for Marketing • Dynamics 365 Fraud Protection • Microsoft Cloud App Security • Microsoft Flow • Microsoft Intune • Microsoft PowerApps • Microsoft Stream **Azure Government** • Dynamics 365 AI for Customer Insights • Dynamics 365 Customer Engagement • Dynamics 365 for Marketing • Dynamics 365 Fraud Protection • Microsoft Cloud App Security

System Name	Components	Service Offering	Full	Partial	With Exclusions	Description of Exclusions
Internal Supporting Infrastructure (Azure Public Cloud, Azure Government, Azure Germany)	Microsoft Windows Server 2012 Ubuntu Linux Custom Hardware	AAD Gateway	X			
		AAD SyncFabric				
		ACIS - Live Site Management				
		Active Directory Ibiza UX - RBAC				
		Azure Device Registration Service (ADRS)				
		AAD Application Proxy				
		Secret Store Service				
		Azure Watson				
		DNS Service (AzDNS, IDNS, Recursive Resolvers)				
		CEDIS - Active Directory Federation Services				
		CEDIS-Active Directory Domain Services				
		Compute Manager				
		AAD Connect Health				
		Datacenter Secrets Management Service (dSMS)				
		Datacenter Security Token Service (dSTS)				
		Evolved Security Token Service (eSTS)				
		Fabric Network Devices				
		FrontDoor				
		Geneva Warm Path				
		Hybrid Identity Service				
		Hybrid Networking Services				

System Name	Components	Service Offering	Full	Partial	With Exclusions	Description of Exclusions
		(including Phynet)				
		IAM - Management UX				
		IAM - Data Insights and Reporting Service				
		IAM - Information Worker UX				
		IAM - Management Admin UX				
		IAM - Self Service Credentials Management Service				
		IAM - Shared Backend Services				
		SQL IaaS				
		Windows Azure Jumpbox				
		Just In Time (JIT)				
		Kusto				
		Microsoft Online Directory Services (MSODS)				
		Organizational ID (OrgID)				
		PilotFish				
		Policy Administration Service (PAS)				
		Red Dog Front End (RDFE)				
		Service Fabric				
		SonarDaas				
		ICM Incident Management Service				
		Azure Security Monitoring (ASM SLAM)				
		Storage Resource Provider (SRP)				

System Name	Components	Service Offering	Full	Partial	With Exclusions	Description of Exclusions
		WANetMon				
		Windows Azure Release Manager (WARM)				
		Workflow				
Azure Datacenters (Azure Public Cloud, Azure Government, Azure Germany)	Microsoft Windows Server 2012 Ubuntu Linux Custom Hardware	Microsoft Datacenter and Operations Services	X			

Scope Description

The following sections describe the Microsoft Azure boundary for the purposes of this Validated Assessment, encompassing all public-facing services and supporting infrastructure described in the Scope Overview above. Note that the description applies to all three Azure clouds -- Azure Public Cloud, Azure Government, and Azure Germany –through one or more of which a given service is made available for customer use.

Internet Routing and Fault Tolerance:

A globally redundant internal and external Microsoft Azure Domain Name Service (MADNS) infrastructure along with multiple primary and secondary Domain Name Service (DNS) server clusters provide for fault tolerance while additional Microsoft Azure network security controls such as NetScaler are used to prevent Distributed Denial of Service (DDoS) attacks and protect the integrity of Microsoft Azure DNS services.

The MADNS servers are located at multiple datacenter facilities. The MADNS implementation incorporates a hierarchy of secondary/primary DNS servers to publicly resolve Microsoft Azure customer domain names. These domain names typically resolve to a CloudApp.net address which wraps the Virtual IP (VIP) address for the customer's service. Unique to Microsoft Azure, the VIP corresponding to internal Dedicated IP (DIP) address of the tenant translation is done by the Microsoft Azure load balancers responsible for that VIP.

Microsoft Azure is hosted in geographically distributed Microsoft Azure datacenters and is built on state-of-the-art routing platforms implementing robust and scalable architectural standards. Some of the notable features are:

- Multiprotocol Label Switching (MPLS) based traffic engineering providing efficient link utilization and graceful degradation of service in case of outage
- Networks implemented with "need plus one" (N+1) redundancy architectures or better.

- Externally, datacenters served by dedicated, high-bandwidth network circuits that redundantly connect properties with over 1,200 Internet service providers globally at multiple peering points providing in excess of 2,000 gigabytes per second (Gbps) of edge capacity.

As Microsoft owns its own network circuits between datacenters, these attributes help the Microsoft Azure offering achieve 99.9+% network availability without the need for traditional third-party Internet service providers.

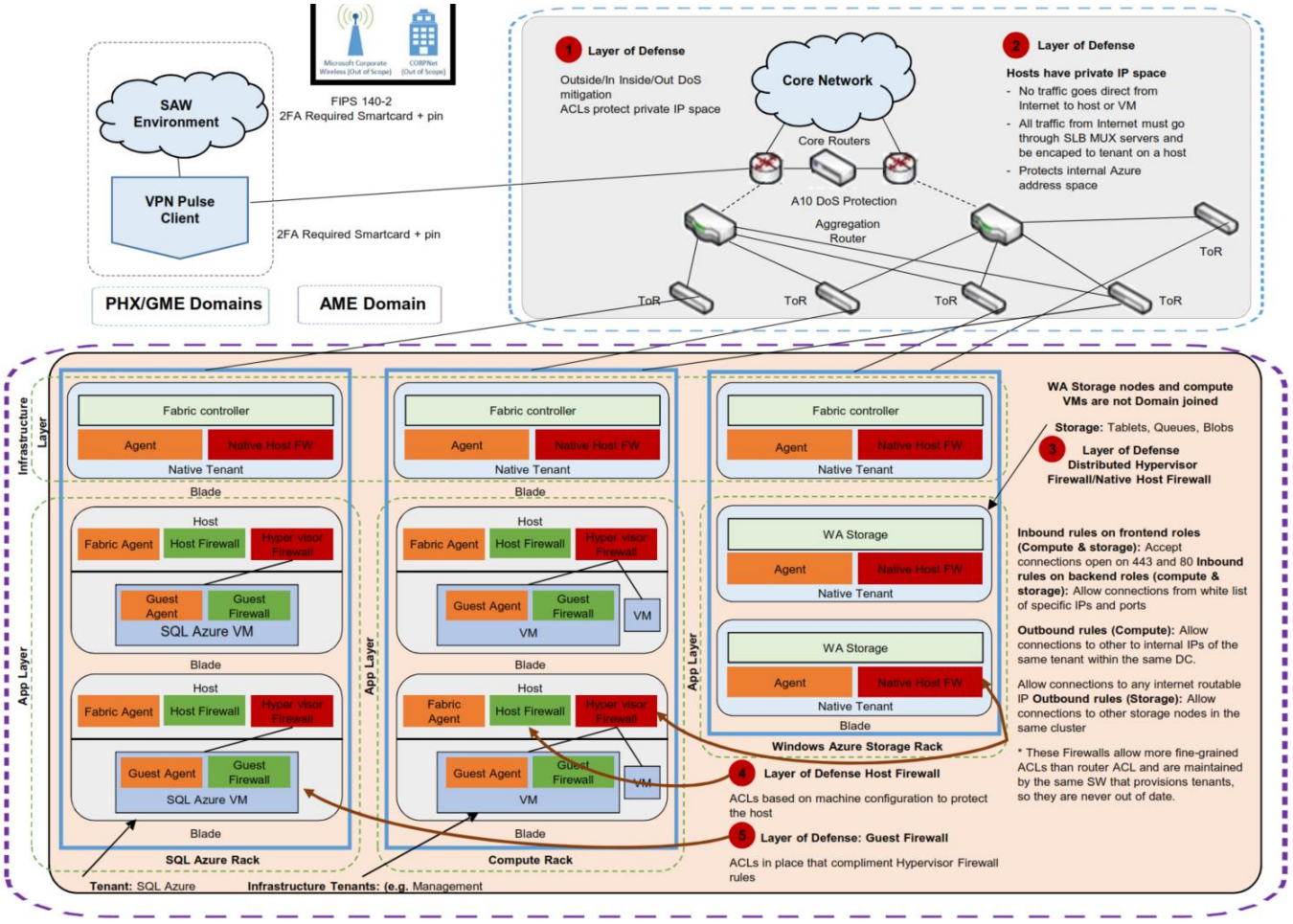
Connection to Production Network and Associated Firewalls:
The Microsoft Azure network Internet traffic flow policy directs traffic to the Azure Production network located in the nearest regional datacenter. Since the Azure Production datacenters maintain consistent network architecture and hardware, the below traffic flow description applies consistently to all datacenters.
Once Internet traffic for Microsoft Azure is routed to the nearest datacenter, a connection is established to the access routers. These access routers serve to isolate traffic between Azure nodes and customer-instantiated virtual machines (VMs). Network infrastructure devices at the access and edge locations are the boundary points where ingress and/or egress filters are applied. These routers are configured through a tiered Access Control List (ACL) to filter unwanted network traffic and apply traffic rate limits, if necessary. Traffic that is allowed by ACL is routed to the load balancers. Distribution routers are designed to allow only Microsoft-approved IP addresses, provide anti-spoofing, and established Transmission Control Protocol (TCP) connections using ACLs.

External Load Balancing devices are located behind the access routers to perform Network Address Translation (NAT) from Internet-routable IPs to Azure internal IPs. They also route packets to valid Production internal IPs and ports, and act as a protection mechanism to limit exposing internal Production Network address space.

By default, Microsoft enforces Hypertext Transfer Protocol Secure (HTTPS) for all traffic being transmitted to the customer's web browsers, including login and all traffic thereafter. The use of TLS v1.2 enables a secure tunnel for traffic to flow through. ACLs on access and core routers ensure the source of the traffic is consistent with what is expected.

An important distinction in this architecture compared to traditional security architecture is that there are no dedicated hardware firewalls, specialized intrusion detection/prevention devices, or other security appliances normally expected before connections are made to the Azure Production environment. Customers typically expect these hardware firewall devices in the Microsoft Azure network; however, there are none employed within Microsoft Azure. Almost exclusively, those security features are built into the software running the Microsoft Azure environment to provide robust multi-layered security mechanisms including firewall capabilities. Additionally, the scope of the boundary and associated sprawl of critical security devices is significantly easier to manage and inventory because it is managed by the software running

Microsoft Azure. Microsoft Azure implements host-based software firewalls inside the Production network as shown in the diagram below:



As shown in the diagram above, several core security and firewall features reside within the core Microsoft Azure environment. These security features reflect a defense-in-depth strategy within the Microsoft Azure environment. Customer's data in Microsoft Azure is protected by the following firewalls:

- Hypervisor Firewall (Packet Filter): This firewall is implemented in the Hypervisor and configured by the Fabric Controller (FC) agent. This firewall protects the tenant running inside the VM from unauthorized access. By default, when a VM is created all traffic is blocked and then the FC agent adds rules/exceptions in the filter to allow authorized traffic. There are two categories of rules that are programmed here:
    - Machine Config or Infrastructure Rules: By default all communication is blocked. There are exceptions to allow a VM to send and receive Dynamic Host Configuration Protocol (DHCP) communications, DNS information, send traffic to the "public" Internet, outbound to other VMs within the FC cluster and Operating System (OS) Activation server. Since the VMs' allowed list of outgoing destinations does not include Microsoft Azure router

subnets and other Microsoft properties, this acts a one layer of defense for them.

  - Role Configuration File: This defines the inbound ACLs based on the tenants' service model. For example, if a tenant has a web front on port 80 on a certain VM, then port 80 is opened to all IP addresses. If the VM has a worker role running, then the worker role is opened only to the VM within the same tenant.

- Native Host Firewall: Microsoft Azure Fabric and Storage run on a Native OS which has no Hypervisor and hence the Windows Firewall is configured with the above two sets of rules.
- Host Firewall: The host firewall protects the Host partition which runs the Hypervisor. The rules are programmed to allow only the FC and jumpboxes to talk to the host partition on a specific port. The other exceptions are to allow DHCP response and DNS Replies. Microsoft Azure uses a Machine Configuration file which has the template of firewall rules for the host partition. There is also a host firewall exception that allows VMs to communicate to Host components (wireserver & metadata server) through specific protocol/ports.
- Guest Firewall: This is the Windows Firewall piece of the Guest OS (which is configurable by the customer on customer VMs and storage).

Types of Rules on Firewalls:
A rule is defined as {Security Response Center (Src) IP, Src Port, Destination IP, Destination Port, Destination Protocol, In/Out, Stateful/Stateless, Stateful Flow Timeout}. SYN packets are allowed in or out only if any one of the rules permits. For TCP, Microsoft Azure uses stateless rules where the principle is that it only allows all non-SYN packets into or out of the VM. The security premise is that any host stack is resilient of ignoring a non-SYN if it has not seen a SYN packet previously. The TCP protocol itself is stateful, and in combination with the stateless SYN-based rule achieves an overall behavior of a stateful implementation.

For User Datagram Protocol (UDP), Microsoft Azure uses a stateful rule. Every time a UDP packet matches a rule, a reverse flow is created in the other direction. This flow has a built-in timeout.

Customers are responsible for setting up their own firewalls on top of what Microsoft Azure provides. Here customers are able to define the rules for inbound and outbound traffic.

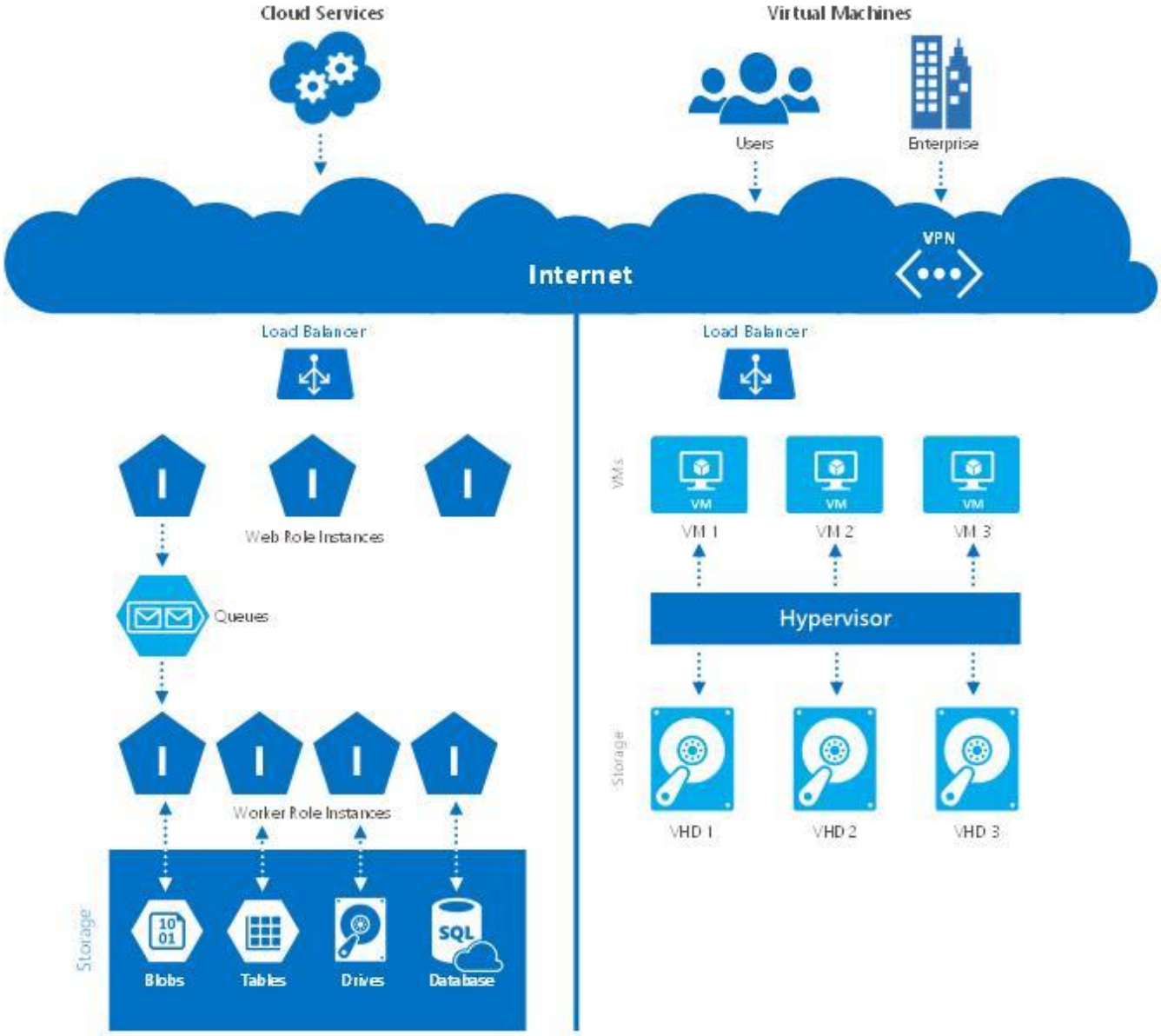
Additional Azure Network Security Features:
Infrastructure components are assigned IP addresses that are from Dedicated IPs (DIPs). An attacker on the Internet cannot address traffic to those addresses because they would not reach Microsoft. Internet Gateway routers filter packets addressed solely to internal addresses so they would not enter the Production network. The only components that accept traffic directed to VIPs are load balancers.

The firewalls implemented on all internal nodes have three primary security architecture considerations for any given scenario:

- They are placed behind the Load Balancer (LB) and accept packets from anywhere. These are intended to be externally exposed and would correspond to the open ports in a traditional perimeter firewall.
- Only accept packets from a limited set of addresses. This is part of the defense-in-depth strategy against denial of service attacks. Such connections are cryptographically authenticated.
- Firewalls can only be accessed from select internal nodes, in which case they accept packets only from an enumerated list of source IP addresses, all of which are DIPs within the Azure network. For example, an attack on the Corporate network could direct requests to these addresses, but they would be blocked unless the source address of the packet was one in the enumerated list within the Azure network.
- The access router at the perimeter blocks outbound packets addressed to an address that is inside the Azure network because of its configured static routes.

Data Flow:

The figure below illustrates customer data flow through Microsoft Azure based on user subscription. Microsoft Azure customers can use any of the web roles or worker roles based on the subscription. Based on the number of role instances specified by customers, Microsoft Azure creates a Persistent Virtual Machine (VM) for each role instance, and then runs the role in those VMs. There are several storage options that can be used by a Microsoft Azure-hosted application or by a set of desktop applications accessing the storage in the cloud such as Tables, Blobs, Queues, Drives or SQL Database.



Data Segregation and Customer Isolation:

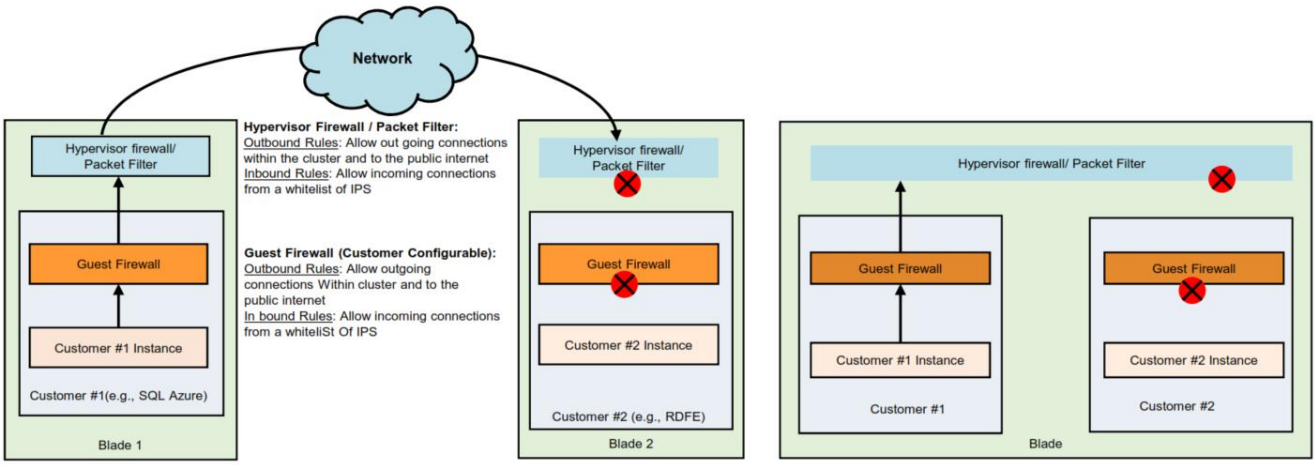
The Microsoft Azure Production network is structured such that publicly accessible system components are segregated from internal resources. Physical and logical boundaries exist between web servers providing access to the public-facing Microsoft Azure Management Portal and the underlying Microsoft Azure virtual infrastructure. The Microsoft Azure virtual infrastructure is where customer application instances and customer data reside. All publicly accessible information is managed within the Azure Production network. This network is subject to two-factor authentication and boundary protection mechanisms, as well as the firewall and security feature set described in the previous section and data isolation functions as noted below.

- Unauthorized Systems and Isolation of the Fabric Controller (FC):

    - Since the FC is the central orchestrator of the Microsoft Azure Fabric, significant controls are in place to mitigate threats to it, especially from potentially compromised FAs within customer applications. FC does not recognize any hardware whose device information (e.g. MAC address) is not pre-loaded within the FC. The DHCP servers on the FC have configured lists of MAC addresses of the nodes they are willing to boot. Even if unauthorized systems are connected, they would not be incorporated into Fabric inventory, and therefore not connected or authorized to communicate with any system within the Fabric inventory. This reduces the risk of unauthorized systems communicating with the FC and gaining access to the VLAN and Microsoft Azure.
- Virtual Local Area Network (VLAN) Isolation:
    - Main (interconnects untrusted customer nodes)
    - FC VLAN (contains trusted FCs and supporting systems)
    - Device VLAN (contains trusted network and other infrastructure devices)
- Packet Filtering:
    - The IPFilter and the software firewalls implemented on the Root OS and Guest OS of the nodes enforce connectivity restrictions and prevent unauthorized traffic between VMs.
- Hypervisor, Root OS, and Guest VMs
    - The isolation of the Root OS from the Guest VMs, and the Guest VMs from one another, is managed by the Hypervisor and the Root OS.

The diagram below illustrates how customer isolation is implemented within Microsoft Azure using two scenarios as examples:

Microsoft Azure Customer Isolation



Scenario 1: Communication between two customer VMS instantiated on different blades

Scenario 1: Role instance of one customer trying to access a VM of another customer in the same cluster

Flow:
1) Request originates at customer #1 role instance.
2) The out going connection request is not blocked by guest firewall and Hypervisor Firewall.
3)The request is routed through the network to the appropriate TOR
4) The incoming request is blocked by the packet Filter on the destination node if it is from a different tenant.

Scenario 2: Communication between two customer VMS instantiated on the same blade

Scenario 2: Role instance of one customer trying to access a VM of another customer in the same blade/Node

Flow:
1) Request originates at customer #1 role instance.
2) The connection request is not blocked by guest firewall.
3)The request is blocked by the packet filter on the Hypervisor.
4) As a defense in depth strategy, the guest firewall on the destination customer #2 role also blocks the request..

Firewall Definitions

Hypervisor Firewall (packet Filter): This is implemented in the hypervisor and configured by fabric controller agent. This protects the tenant running inside the VM from unauthorized access. By default when the VM is created all traffic is blocked and then fabric controller agent updates the packet filter to add rules\exceptions to allow authorized traffic. There are two categories of rules that are programmed here:

Machine config or infrastructure Rules: By default all communication is blocked. There are exceptions to allow a VM to send and receive DHCP, DNS, send traffic to the "public" interest, outbound to other VMs within the fabric controller cluster and OS Activation server. Since the VMs allowed list of outgoing destination does not include WA router subnets, GFS BE and other Microsoft properties, this acts as one layer of defense for them. They may have additional layers of defense on their side. The template of the rules is in the attached Machine Config File.
-Role configuration File: This defines the inbound ACLs based on the tenants service model. For example if a tenant has a web frontend on port 80 on a certain VM, then we open port 80 to all IPS. If the VM has a backend or worker role running then we open the worker role only to the VMs within the same tenant.

Native Host firewall: WA Fabric and storage run on a native OS which has no hypervisor and hence the Windows firewall is configured with the above two sets of rule. Storage runs native to optimize performance

Host firewall: The host firewall is to protect the Host partition which manages the hypervisor. The rules are programmed to allow only the fabric controller and jump boxes to talk to the host partition on specific ports. The other exceptions are to allow DHCP response and DNS Replies. We have attached a Machine configuration file which has the template of firewall rules for the host partition.

Customer Guest Firewall: This is the replication of the rules in the VM Switch packet filter but programmed in a different software layer, i.e., the Windows Firewall of the guest OS.

End-to-End Customer Authentication Scenario for Microsoft Azure:

There are three conceptual steps that customers are required to perform to gain access to Microsoft Azure:

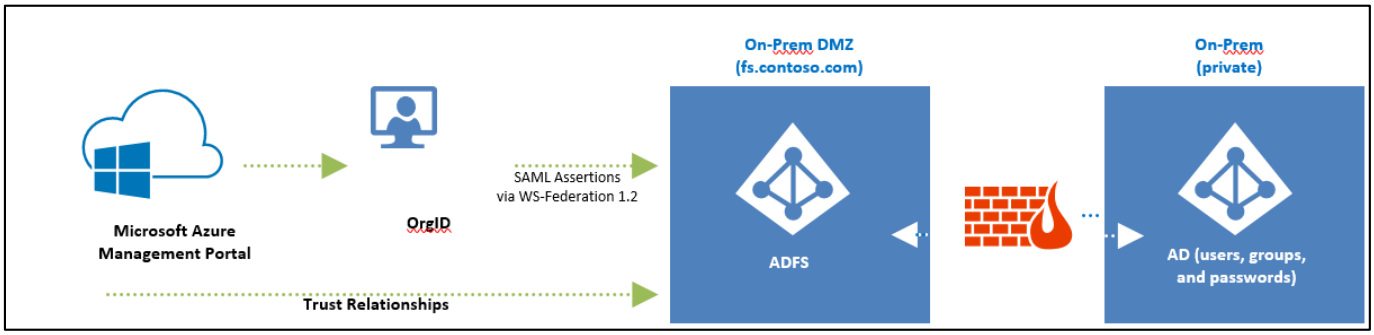
1. Customer purchases a new Azure subscription using a federated identity issued by the governmental or corporate authority. This identity is governed by two-factor authentication for every access to the Azure purchasing or billing workflows.
2. Customer logs into the Microsoft Azure Management Portal using the same federated identity used to purchase the new subscription. The Microsoft Azure Management Portal provides the basis for all management functions to computational assets in the Azure cloud, including programmatic access to any other Azure feature. As in the first step, every access to the Microsoft Azure Management Portal is governed by two-factor authentication.
3. Customer obtains an access token from the Microsoft Azure Management Portal which provides programmatic API access to Azure services. These tokens can take several different forms, such as X.509 certificates for access to the Microsoft Azure Management APIs, a Base64-encoded Storage key (512-bit), or a Microsoft Azure SQL DB

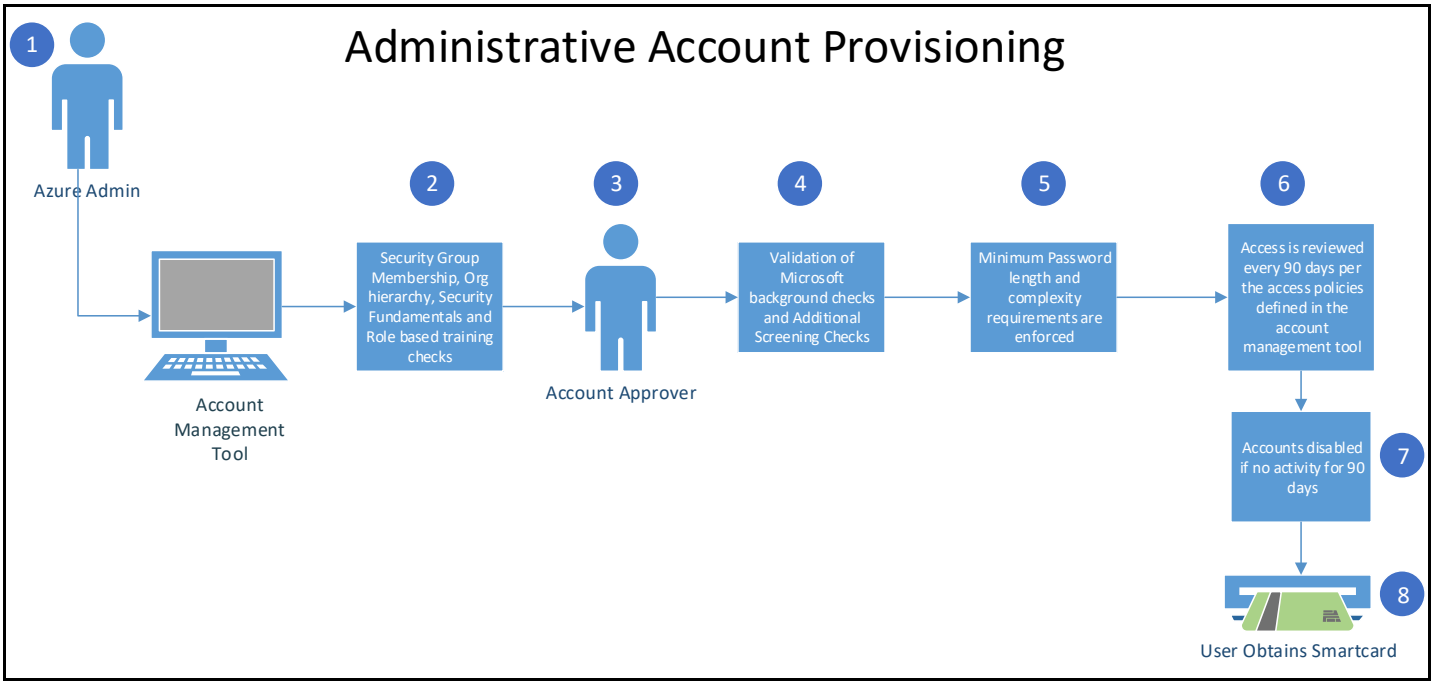
administrator login and password. The only method to obtain these tokens is via two-factor authentication to the Microsoft Azure Management Portal. Programmatic access to Azure is governed by a revocable token obtained via two-factor authentication into the Microsoft Azure Management Portal.

Federated Identities:

Federated identities are stored entirely within an on-premises identity store such as Active Directory. External services such as Azure never touch the passwords directly. Instead a set of trusted claims are issued by the on-premise Active Directory Federation Services (ADFS) gateway which attest to the correct authentication status of the user.

In this model all user password scenarios (validate password, set/reset password, forgot password, etc.) are handled entirely by the on-premises IT department of the external company. However, the one-time set up of federation is lengthy and performed at an overall corporate level with the assistance of the central IT department. It requires, among other things, proof of control of the company's DNS name (e.g. contoso.com) before federation can commence. Federated identities with the Azure public cloud result in the following trust topology:

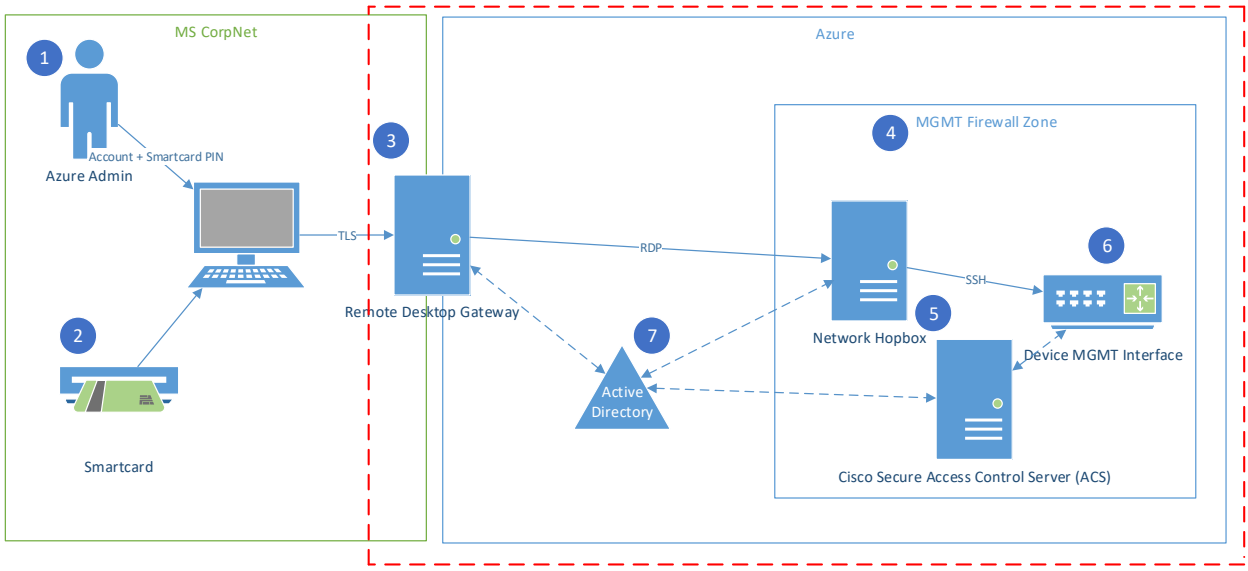




Requirements for Obtaining a Microsoft Azure Administrative Account:

1) User access requests are managed through the Account Management tool, which has built in automated workflows for the end to end account provisioning and deletion processes
2) Upon receiving a request, Account Management tool checks for training requirements, access to the appropriate Security Groups (SGs) and routes the request for approval
3) Manager Approval is required for all account requests to justify business need
4) Background Checks and Screening – access requires users undergo screening. In this step, completion of required screenings are validated
5) Password Security Requirements - The user must establish a password that meets the minimum complexity requirements
6) Accounts that have access to Microsoft Azure systems must be reviewed every 90 days by Microsoft Azure group owners
7) AD accounts that have been disabled for 15 days after 90 days of inactivity are deleted. Azure will automatically disable any user accounts within Azure Infrastructure managed domains on a daily basis if no HR record exists (e.g., after termination), or have been inactive over 90 days
8) 2FA – Users are authenticated using two-factor authentication for production access.

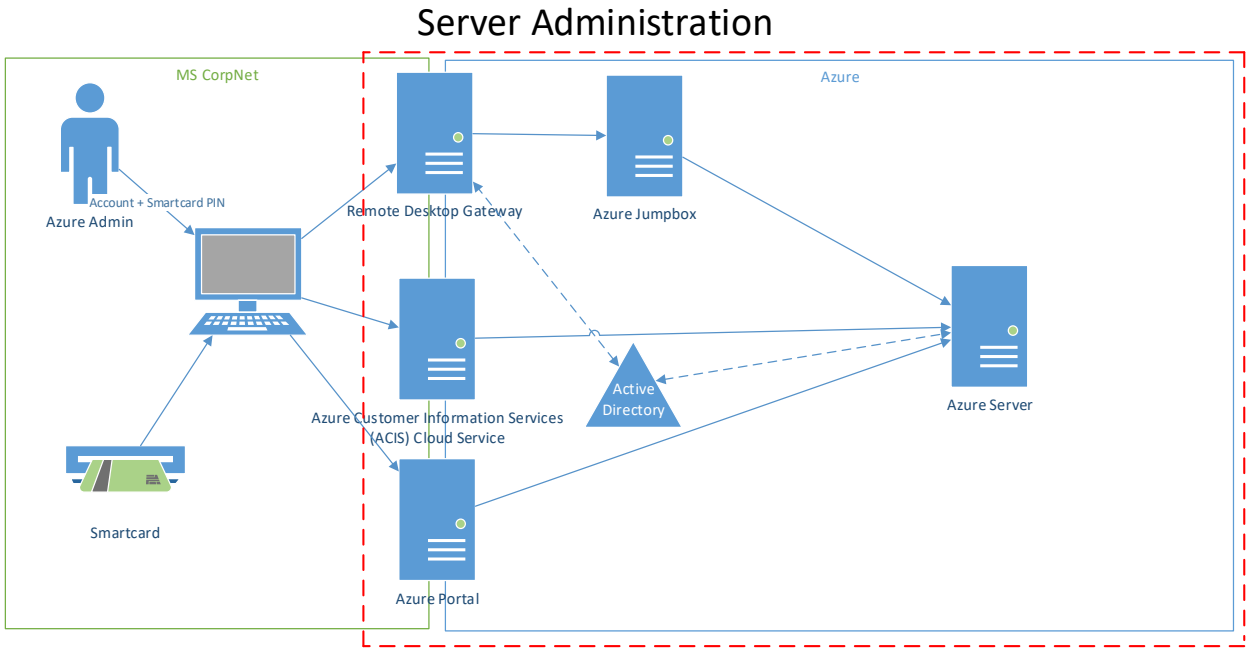
Network Device Administration



Requirements for Network Device Administration (NDA) within Microsoft Azure:

1) Requirements for obtaining a production network account (cf. *Requirements for obtaining a Microsoft Azure Administrative Account*)
2) Smartcard token
3) Remote Desktop Gateway (i.e., Remote Desktop Protocol (RDP) connectivity)
4) Network resources in a separate LAN
5) Network Hop box access needed for device administration (via Secure Shell connectivity)
6) Device MGMT interface access
7) Active Directory (AD) role-based access control (RBAC) to network resources (via the Cisco Secure Access Control Server (ACS))

8) Broken Line (Red): Boundary encompasses in-scope NDA components



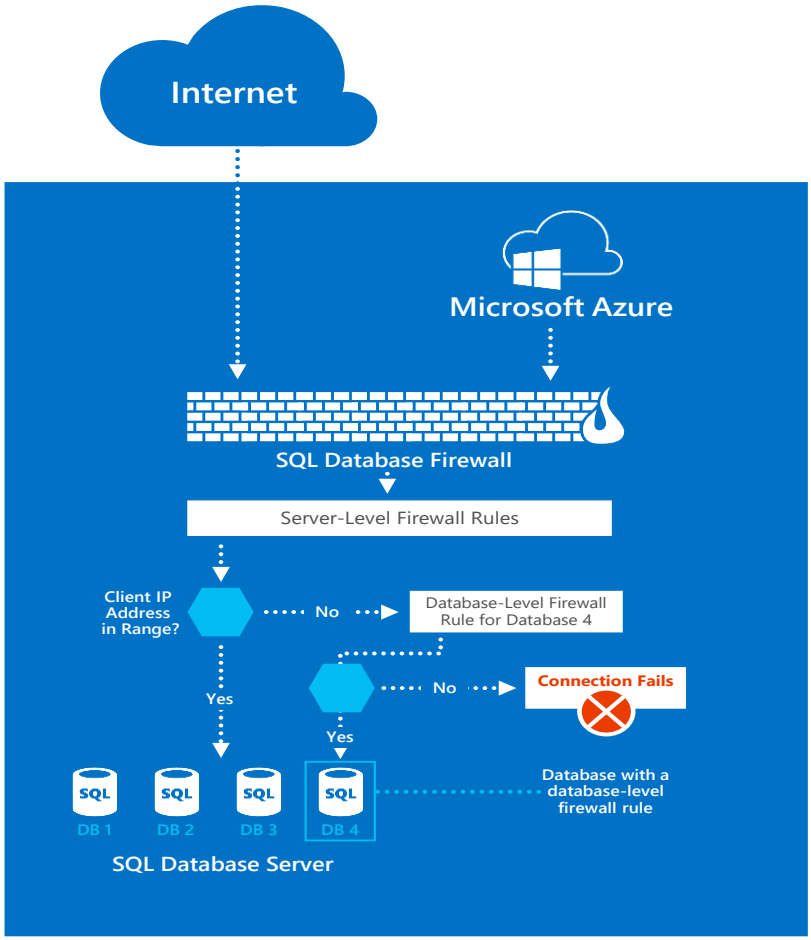
Requirements for Server Administration (SA) within Microsoft Azure:

1) Requirements for obtaining a production network account (cf. *Requirements for obtaining a Microsoft Azure Administrative Account*)
2) Smartcard token
3) Remote Desktop Gateway (interactive access via RDP)
4) Azure Jumpbox access for server administration (via RDP connectivity)
5) Active Directory (AD) role-based access control (RBAC) to server resources
6) Azure Customer Information Services (ACIS) cloud service (non-interactive access)
7) Azure Portal (non-interactive access)
8) Broken Line (Red): Boundary encompasses in-scope SA components

Microsoft Azure SQL Database Security Features:

Microsoft Azure SQL Database provides a relational database service in Microsoft Azure. To protect customer data and provide strong security features that customers expect from a relational database service, SQL Database has its own sets of security capabilities which build upon the controls inherited from Microsoft Azure:

- Usage of Tabular Data Stream (TDS) protocol:
  - Microsoft Azure SQL Database only supports the TDS protocol, which requires the database to be accessible only over the default port of TCP/1433.
- Microsoft Azure SQL Database Firewall:
  - To help protect customers' data, Microsoft Azure SQL Database includes a firewall functionality which by default prevents all access to the SQL Database server, as shown in the figure below.



Microsoft Azure

- The gateway firewall provides the capability to limit addresses allowing for granular control to customers to specify ranges of acceptable IP addresses. The firewall grants access based on the originating IP address of each request. Firewall configuration can be accomplished using a Management Portal or programmatically using the Microsoft Azure SQL Database Management Representational State Transfer (REST) Application Programming Interface (API). The Microsoft Azure SQL Database Gateway firewall by default prevents all customer TDS access to Microsoft Azure SQL Databases and such access must be configured using ACLs to permit Microsoft Azure SQL Database connections by source and destination Internet addresses, protocols, and port numbers.

- DoSGuard:
  - Denial-of-service (DoS) attacks are further reduced by a SQL Database Gateway service called DoSGuard that actively tracks failed logins from IP addresses, and in the event of multiple failed logins from a specific IP address within a period of time, the IP address is blocked from accessing any resources in the service for a pre-defined time period. In addition to the above, the Microsoft Azure SQL Database gateway also performs:

- Secure channel capability negotiations to implement TDS FIPS 140-2 validated encrypted connections when connecting to the database servers.
- Stateful TDS packet inspection while accepting connections from clients in order to validate the connection information and pass on the TDS packets to the appropriate physical server based on the database name specified in the connection string.

The overarching principle for network security of the Microsoft Azure SQL Database offering is to only allow connection and communication that is necessary to allow the service to operate, blocking all other ports, protocols, and connections by default. VLANs and ACLs are used to restrict network communications by source and destination networks, protocols, and port numbers. Approved mechanisms to implement network-based ACLs include ACLs on routers and load balancers managed by Azure Networking, Guest VM firewall and Microsoft Azure SQL Database gateway firewall rules (configured by the customer).

Microsoft Azure Encryption:

Microsoft Azure implements the transmission confidentiality control by ensuring that the cryptography complies with the Microsoft Cryptographic Standards for the SDL-covered products through a hybrid model using both symmetric and asymmetric keys for encrypting and protecting confidentiality of data, which at a high-level are:

- Advanced Encryption Standard (AES) 128 or 256 for symmetric encryption/decryption
- Rivest Shamir Adelman (RSA) 2048 or 4096 for asymmetric encryption/decryption and digital signatures
- Secure Hash Algorithm (SHA) 256, 384, or 512 for cryptographic hash operations

In addition, Microsoft Azure follows measures to protect the confidentiality/integrity of transmitted information in accordance with FIPS 140-2 by meeting or exceeding requirements as outlined:

- FIPS 140-2 Secure Sockets Layer TLS encryption is automatically handled & established by Microsoft Azure for all TDS connections.
- Communications between the Microsoft Azure service offerings and the Microsoft Azure Management Portal are configured to require FIPS 140-2 validated encryption (via Transport Layer Security (TLS) 1.2)
- The Microsoft Azure virtual environment enforces key communications between Microsoft Azure internal components to be protected with self-signed SSL certificates.

Certificate and Private Key Management:

Certificates and private keys are uploaded via Service Management API (SMAPI) or the Microsoft Azure Management Portal as PKCS12 (PFX) files protected in transit by TLS. Those PKCS12 files may be password protected, but if so, the password must be included in the same message. SMAPI removes the password protection (if necessary) and encrypts the entire PKCS12 blob using SMAPI's public key and stores it in a secret store on the FC, along with a short certificate name, and the public key as metadata.

Microsoft Azure provides a secure certificate store which enables automatic deployment of service-specific certificates. Each Microsoft Azure subscription has an associated certificate store to which customers can upload certificates. The certificate store is independent of any hosted service, so it can store certificates whether or not they are currently being used by any of the services.

Certificates can therefore be managed separately from services, and may be managed by different individuals. For example, a developer may upload a service package that refers to certificates that an IT manager has previously uploaded to Microsoft Azure. An IT manager can manage and renew those certificates without stopping the service or uploading a new service package.

Encryption key management is left to the implementation of the end-user, so that end customers can develop a secure architecture that works for their particular solutions and architectures. Customers have full control for data encryption both at rest and in transit. Microsoft Azure provides the ability to use secure certificates to secure data and the .NET 3.5/4.0 Cryptography API.