Microsoft

Independent Service Auditor’s Report

Microsoft Corporation - Microsoft Azure and Microsoft Datacenters

Table of Contents

I. Independent Service Auditor's Report 3

II. Management's Assertion 4

III. Description of Microsoft Azure System and Microsoft Datacenters 5

Deloitte & Touche LLP
925 Fourth Avenue, Suite 3300,
Seattle, WA 98104-1126
Tel: +1 206 716 7000
Fax: 206 965-7000
www.deloitte.com

I. Independent Service Auditor's Report

To: Microsoft Azure and Microsoft Datacenters

We have examined the effectiveness of Microsoft Azure ("Azure") and Microsoft Cloud Infrastructure and Operations' (MCIO) controls related to the in-scope Azure features / services and the Microsoft datacenters managed by MCIO, to meet the criteria for the security, availability, processing integrity and confidentiality principles ("applicable trust services criteria")[1], during the period January 1, 2016 to June 30, 2016[2], based on the American Institute of Certified Public Accountants (AICPA) and Chartered Professional Accountants of Canada (CPA Canada) trust services principles and criteria. Azure and MCIO's ("Service Organizations") management is responsible for maintaining the effectiveness of these controls. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA, and accordingly, included (1) obtaining an understanding of the controls related to the in-scope Azure features / services and the Microsoft datacenters managed by MCIO, to meet the applicable trust services criteria (2) testing and evaluating the operating effectiveness of the Service Organizations' controls, and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of the nature and inherent limitations of controls, the Service Organizations' ability to meet the aforementioned criteria may be affected. For example, controls may not prevent or detect and correct error or fraud, unauthorized access to systems and information, and failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion, the Service Organizations maintained, in all material respects, effective controls to meet the applicable trust services criteria during the period January 1, 2016 to June 30, 2016 to provide reasonable assurance that:

- the system was protected against unauthorized access, use or modification,
- the system was available for operation and use as committed or agreed,
- information within the system, designated as "confidential", was protected as committed or agreed, and
- the system processing was complete, valid, accurate, timely, and authorized

based on the AICPA and CPA Canada trust services principles and criteria for security, availability, processing integrity and confidentiality.

Deloitte & Touche LLP

October 28, 2016
Seattle, WA

---

[1] Applicable Trust Services Principles for Microsoft datacenters - Security and Availability.

[2] Controls were placed into operation from April 1, 2016 for the following Microsoft Azure features / services – Application Gateway, IoT Hub, Key Vault, Machine Learning, Ibiza, Site Recovery, Stream Analytics, Device Registration Service, IaaS Experience, StorSimple, VPN Gateway, Backup, Compute Platform, Network Resource Provider, Storage Resource Provider, Active Directory Portal Extension for Ibiza Portal (ADIUX), Policy Administration Service, Service Fabric - RP Clusters, Network Manager Agent, Network Service Manager, Regional Network Manager, Datacenter Secrets Management Service, OneDDoS, OneDeploy Express v2, WANetMon. Additionally, controls were placed into operation from May 1, 2016 for Cool Storage service.

II. Management's Assertion

Assertion by Management of Microsoft Azure and Microsoft Cloud Infrastructure and Operations for the period from January 1, 2016 through June 30, 2016

Management Assertion Regarding the Effectiveness of its Controls

Microsoft Azure ("Azure") and Microsoft Cloud Infrastructure and Operations (MCIO) maintained effective controls over the security, availability, processing integrity, and confidentiality of the system relating to the in-scope Azure features / services and Microsoft datacenters[3] managed by MCIO that support Azure and other Microsoft Online Services, throughout the period January 1, 2016 to June 30, 2016[4], to provide reasonable assurance that:

- the system was protected against unauthorized access, use or modification,
- the system was available for operation and use as committed or agreed,
- information within the system, designated as "confidential", was protected as committed or agreed, and
- the system processing was complete, valid, accurate, timely, and authorized

based on the AICPA and CPA Canada trust services principles and criteria for security, availability, processing integrity and confidentiality.

The following description of the system identifies the aspects of Azure features / services and Microsoft datacenters covered by this assertion.

Microsoft Azure and Microsoft Datacenters

[3] Applicable Trust Services Principles for Microsoft datacenters - Security and Availability.

[4] Controls were placed into operation from April 1, 2016 for the following Microsoft Azure features / services - Application Gateway, IoT Hub, Key Vault, Machine Learning, Ibiza, Site Recovery, Stream Analytics, Device Registration Service, IaaS Experience, StorSimple, VPN Gateway, Backup, Compute Platform, Network Resource Provider, Storage Resource Provider, Active Directory Portal Extension for Ibiza Portal (ADIUX), Policy Administration Service, Service Fabric - RP Clusters, Network Manager Agent, Network Service Manager, Regional Network Manager, Datacenter Secrets Management Service, OneDDoS, OneDeploy Express v2, WANetMon. Additionally, controls were placed into operation from May 1, 2016 for Cool Storage service.

III. Description of Microsoft Azure System and Microsoft Datacenters

Overview of Operations

Business Description

Microsoft Azure ("Azure") is a cloud computing platform and infrastructure for building, deploying and managing applications and features / services 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) and enables hybrid solutions that integrate cloud services with customers' on-premises resources. Azure supports many customers, partners, and government organizations that span across a broad range of products and services, geographies and industries. Azure is designed to meet their security, privacy, and compliance requirements.

Microsoft Cloud Infrastructure and Operations (MCIO) manages the security and compliance of the Microsoft datacenters that support Azure and other Microsoft Online Services (i.e., Office 365, Visual Studio Team Services and CRM Online). These datacenters operate internally under the MCIO team. MCIO delivers the core physical infrastructure and foundational technologies that support operations, physical security, and compliance of the datacenters.

Report Scope Boundary

This report covers the following Azure features / services[5,6], including infrastructure, development, operations, and support for Cloud Services, as well as infrastructure for Microsoft Online Services:

1. **Compute Services**
   - Batch
   - Cloud Services (includes stateless Web and Worker roles)
   - Fabric (also known as Compute Manager)[7]
   - Red Dog Front End[7,8]
   - Service Management Application Programming Interface
   - Virtual Machines (including those with SQL Server)

---

[5] Controls were placed into operation from April 1, 2016 for the following Microsoft Azure features / services - Application Gateway, IoT Hub, Key Vault, Machine Learning, Ibiza, Site Recovery, Stream Analytics, Device Registration Service, IaaS Experience, StorSimple, VPN Gateway, Backup, Compute Platform, Network Resource Provider, Storage Resource Provider, Active Directory Portal Extension for Ibiza Portal (ADIUX), Policy Administration Service, Service Fabric - RP Clusters, Network Manager Agent, Network Service Manager, Regional Network Manager, Datacenter Secrets Management Service, OneDDoS, OneDeploy Express v2, WANetMon.

[6] Controls were placed into operation from May 1, 2016 for Cool Storage service.

[7] Services which are accessible internally only and not available externally for customers.

[8] Services for which American Institute of Certified Public Accountants (AICPA) Processing Integrity trust principle was examined.

2. **Web & Mobile**
    - App Service
        i. Mobile Apps (formerly known as Mobile Services)
        ii. Web Apps
    - API Management
    - Notification Hubs
    - Workflow
3. **Data & Storage**
    - Cool Storage[6]
    - Redis Cache
    - SQL Database
    - Storage (includes blobs, queues, tables, files, and disks)
    - Premium Storage
    - StorSimple[5]
4. **Analytics**
    - HDInsight
    - Machine Learning[5]
    - Stream Analytics[5]
5. **Internet of Things**
    - Event Hubs
    - IoT Hub[5]
    - Machine Learning[5]
    - Notification Hubs
    - Stream Analytics[5]
6. **Networking**
    - Application Gateway[5]
    - ExpressRoute
    - Load Balancer
    - Traffic Manager
    - Virtual Network
    - VPN Gateway[5]
7. **Media**
    - Media Services
8. **Enterprise Integration**
    - Backup[5]
    - Service Bus
    - Site Recovery[5]

9. Identity & Access Management

- Azure Active Directory
  - i. Microsoft Online Directory Services and Organizational Identity[7]
  - ii. Access Control Service
  - iii. Evolved Secure Token Service[7]
  - iv. Device Registration Service[5]
  - v. Identity and Access Management - Self-Service Password Reset
  - vi. Identity and Access Management - Cloud Password Single Sign-On
  - vii. Identity and Access Management - Self-Service Group Management
  - viii. Identity and Access Management - Sync Fabric
- Rights Management Service
- Multi-Factor Authentication

10. Management & Security

- Microsoft Azure Portal (Current[8], Ibiza[5,8], IaaS Experience[5])
- Scheduler
- Automation
- Key Vault[5]
- Log Analytics (formerly known as Operational Insights)
- Intune

Locations Covered by this Report

Azure production infrastructure is located in globally distributed datacenters managed by MCIO. These datacenters deliver the core physical infrastructure that includes physical security, data protection, and physical hardware asset management and network services. These datacenters are managed, monitored, and operated by Microsoft operations staff delivering online services with 24x7x365 continuity. These purpose-built facilities are part of a network of datacenters that provide mission critical services to Azure and other Microsoft Online Services (i.e., Office 365 and CRM Online). The datacenters in scope for the purposes of this report are:

Domestic	
Santa Clara, CA (BY1/2/3/4)	Bristow, VA (BLU)
Des Moines, IA (DM1/2/3, DSM05)	Reston, VA (BL4)
Chicago, IL (CH1/3)	Tukwila, WA (TK5)[9]
San Antonio, TX (SN1/2/3/4)	Quincy, WA (CO1/2, MWH01)
Ashburn, VA (BL2/3/5)	Cheyenne, WY (CYS01/04)
Boydton, VA (BN1/3/4/6)	

[9] Microsoft Azure did not operate out of these regions during the examination period - January 1, 2016 to June 30, 2016.

International	
North America • Toronto, Canada (YTO20)[10] • Quebec City, Canada (YQB20)[10] Australia • Macquarie Park, Australia (SYD03) • Melbourne, Australia (MEL01)	South America • Campinas, Brazil (CPQ01/02) • Fortaleza, Brazil (FOR01)[9] • Rio de Janeiro, Brazil (RIO01)[9] • Sao Paulo, Brazil (GRU)[9] • Santiago, Chile (SCL01)[9] • Humacao, Puerto Rico (PR1)[9]
Europe • Vienna, Austria (VIE01)[9] • Vantaa, Finland (HEL01)[9] • Biere, Germany (LEJ20) • Frankfurt, Germany (FRA20) • Amsterdam, Netherlands (AM1/2/3, AMS04/05) • Billingham, United Kingdom (MME20) • Chessington, United Kingdom (LON20) • Dublin, Ireland (DB3/4/5, DUB06)	Asia • Hong Kong (HK1/2) • Mumbai, India (BOM01) • Dighi, India (PNQ01) • Ambattur, India (MAA01) • Osaka, Japan (OSA1/2) • Tokyo, Japan (KAW, TYO01) • Cyberjaya, Malaysia (KUL01)[9] • Singapore (SG1/2/3) • Busan, South Korea (PUS01)[9]

In addition to datacenter, network and personnel security practices, Azure also incorporates security practices at the application and platform layers to enhance security for application development and service administration.

People

Azure is comprised and supported by the following groups who are responsible for the delivery and management of Azure's cloud-based features / services:

Datacenters - Microsoft Cloud and Infrastructure Operations

MCIO provides the core physical infrastructure that Azure and other Microsoft Online Services (i.e., Office 365 and CRM Online) are built on. MCIO is part of Microsoft's Cloud and Enterprise group and delivers the foundational technologies that support operations, physical security, and compliance of the datacenters.

Cloud and Enterprise Security

The Cloud and Enterprise Security team works to make Azure a secure and compliant cloud platform by building common security technologies, tools, processes and best practices across. The Cloud and Enterprise Security team is involved in the review of deployments and enhancements of Azure features / services to facilitate security considerations at every level of the Secure Development Lifecycle (SDL). They also perform security reviews and provide security guidance for the MCIO datacenters.

[10] Datacenters that were placed into operation from May 5, 2016.

Azure Production Support

The Azure Production Support team is responsible for build out, deployment and management of Azure features / services. This team consists of Live Site monitoring, Deployment Engineering, and Customer Support.

Azure Engineering Feature Teams

The Azure Engineering Feature teams manage the component lifecycle including development of new features / services, escalation point for support and operational support for existing features / services (DevOps model).

Global Ecosystem and Compliance Team

The Global Ecosystem and Compliance team is responsible for developing, maintaining and monitoring the Information Security (IS) program including the ongoing Risk Assessment process.

As part of managing compliance adherence, the team drives related features within the Azure product families. This team consists of personnel responsible for training, privacy, risk assessment and internal and external audit coordination.

Networking

The Networking team is responsible for implementing, monitoring and maintaining the Microsoft network. This team consists of personnel responsible for network configuration, network problem management, and network capacity management.

Azure Environment

Azure is developed and managed by the Azure team, and provides the virtual environment and platform where customers host their applications and data. MCIO provides the underlying physical infrastructure on which the Azure platform runs and data is stored.

Services and Features Overview

Azure provides a platform where customers, users, and applications can interact. Below is an overview of the Azure services, their key features and the interrelationships with customers and end-users.

Azure Management Portal

Azure Management Portal ("Azure Portal") is an administrative portal for managing customer accounts and deploying, managing, and monitoring their hosted features / services.

Azure Portal and Service Management Application Programming Interfaces

Azure is designed to abstract much of the infrastructure and complexity that typically underlies applications (i.e., servers, operating systems and network) so that developers can focus on building and deploying applications.

Customers manage these Azure applications through the Azure Portal and Service Management Application Programming Interfaces (SMAPI) and are authenticated by their Microsoft Accounts or Organizational Accounts.

Red Dog Front End

Red Dog Front End (RDFE) is the communication path from the user to the Fabric. RDFE is the publicly exposed API which is the front end to the Azure Management Portal and the SMAPI (i.e., APIs used to manage Azure features / services).

Microsoft Online Services Customer Portal and Microsoft Accounts / Organizational Accounts

Users who have access to Azure customer applications have established authentication and authorization privileges based on their Microsoft Accounts (MSA) and / or Organizational Accounts. Azure customer billing is handled by Microsoft Online Services Customer Portal (MOCP).

Azure Infrastructure

Azure Core Infrastructure Details

Azure Node Detail

The collection of Azure Hypervisor, Root Operating Systems, Fabric Agent, Customer Virtual Machines (VMs), and Guest Agents make up the Azure Node.

Fabric Controller Lifecycle Management

In Azure, VMs (nodes) run on groups of physical servers known as "clusters", of approximately 1,000 machines. Each cluster is independently managed by a scaled-out and redundant platform Fabric Controller (FC) software component.

FC Managed Operating Systems

An Azure OS base image Virtual Hard Disk (VHD) is deployed on all Host, Native, and Guest VMs in the Azure production environment. The three types of FC managed OS images are:

1. **Host OS:** Host OS is a customized version of the Windows OS that runs on Host Machine Root VMs

2. **Native OS:** Native OS runs on Azure native tenants such as the FC itself, Azure Storage and Load Balancer that do not have any hypervisor

3. **Guest OS:** Guest OS runs on Guest VMs (for IaaS, FC will run customer provided images on a VHD)

Software Development Kits

Azure is a Windows Server-based environment that allows customers to create applications in many development languages. Microsoft provides language-specific Software Development Kits (SDKs) for .NET, Java, PHP, Ruby and Node.js. In addition, there is a general Azure SDK that provides basic support for any language, such as C++ or Python.

Compute Services

Azure Virtual Machines

Azure VMs is an IaaS feature that provides customers with the ability to deploy and run VMs with Windows Server and Linux operating systems. This enables customers to migrate their workloads to the Azure cloud without a need to change existing code.

SQL Virtual Machines

A SQL VM enables customers to create a SQL Server in the cloud that they control and manage. SQL VMs offer a robust infrastructure for SQL Server by using Azure as a hosting environment of enterprise database applications.

Cloud Services

Azure Cloud Services provide a PaaS environment that customers can use to create highly available and scalable applications and services. Customers upload applications and Azure manages the deployment details - from provisioning to load balancing and health monitoring for continuous availability.

Batch

Azure Batch provides a foundational platform service for application developers where their application needs to perform large-scale compute; it manages the large number of VMs on which the workloads are executed and provides the job scheduling capabilities which allocate workload tasks to the VMs for execution.

Web & Mobile

App Service - Mobile Apps

App Service - Mobile Apps allows customers to 1) accelerate mobile application development by providing a turnkey way to structure storage, authenticate users, and send push notifications, 2) build connected applications for any platform and deliver a consistent experience across devices, and 3) accelerate getting started with data, authentication, push notifications and custom business logic for apps on Windows, iOS, Android and more.

App Service - Web Apps

Azure App Service - Web Apps is a highly scalable web hosting service for public and private clouds that is optimized for cloud hosting economics and is integrated with the Operations Support System (OSS) Web Apps, frameworks, and tools. App Service - Web Apps offers secure and flexible development, deployment and scaling options for any sized web application.

API Management

API Management is a turnkey solution for publishing APIs to external and internal consumers. API publishers can use the service to quickly create consistent and modern API gateways for existing backend services hosted anywhere. The publisher defines an API surface area and the policies needed to transform this façade for their backend using the Publisher Portal, PowerShell or administration APIs.

Notification Hubs

Azure Notification Hubs provide an easy-to-use, multiplatform, scaled-out push infrastructure that enables customers to send mobile push notifications from any backend (in the cloud or on-premises) to any mobile platform.

Workflow

The Azure Workflow service provides a high-scale, high-density environment where workflows authored by customers in the Office 365 platform can execute. SharePoint Online allows workflows to be created that are attached to SharePoint sites or lists. Using this, customers can automate numerous human and document management processes.

Data & Storage

SQL Database

SQL Database is a relational database service in Azure that is based on the market-leading Microsoft SQL Server database engine. Azure SQL Database delivers mission-critical capabilities including predictable performance, scalability with no downtime, business continuity and data protection-all with near-zero administration.

Redis Cache

Redis Cache is an open source implementation of an in-memory cache server. A cache service allows quick access to frequently requested data. Redis Cache handles the management aspects of the cache instances, providing customers with replication of data, fail-over, and connecting to the cache using Secure Sockets Layer (SSL) support, etc.

Storage

The Storage service for Azure provides distributed persistent storage and five different data storage types: blobs, queues, tables, files and disks. The Storage access control model allows each subscription to create one or more Storage accounts. Each Storage account has a primary and secondary secret key that is used to control access to the data within the Storage account. Every Storage service account has redundant data copies for fault tolerance.

Premium Storage

Premium Storage delivers high-performance, low-latency disk support for I/O intensive workloads running on Azure VMs. With Premium Storage, applications can have up to 32 TB of storage per VM and achieve 64,000 IOPS (input / output operations per second) per VM with extremely low latencies for read operations.

Cool Storage

Cool Storage is a low cost Blob Storage for cool object data, where the data is not accessed often. Example use cases for Cool Storage include backups, media content, scientific data, compliance and archival data. Customers can use Cool Storage to retain data that is seldom accessed.

StorSimple

StorSimple is a hybrid cloud storage solution which integrates Cloud Services with hybrid storage technologies. It arranges data in logical tiers based on current usage, age, and relationship to other data. Data that is most active is stored locally, while less active and inactive data is automatically migrated to the cloud.

Analytics

HDInsight

Azure HDInsight is a managed Apache Hadoop ecosystem offering in the cloud. It handles various amounts of data, scaling from terabytes to petabytes on demand, and can process unstructured or semi-structured data from web clickstreams, social media, server logs, devices and sensors, and more.

Stream Analytics

Azure Stream Analytics is a fully managed real-time stream computation service providing low latency, highly resilient, scalable processing of streaming data.

Machine Learning

Azure Machine Learning is a service that enables users to experiment with their data, develop and train a model using training data and operationalize the trained model as a web service that can be called for predictive analytics.

Internet of Things

IoT Hub

Azure IoT Hub is a fully managed service that enables reliable and secure bi-directional communications between millions of IoT devices and a solution back-end.

Event Hubs

Event Hubs is a feature of Service Bus. It is an event and telemetry ingress service that can be used for common application and user workflow monitoring. Event Hubs provide provisioning of capacity to process events from millions of event publishers while preserving event order on a per-device basis.

Notification Hubs

Please see above under Web & Mobile section.

Machine Learning

Please see above under Analytics section.

Stream Analytics

Please see above under Analytics section.

Networking

Virtual Network

Azure Virtual Network (VNet) enables customers to create a logically isolated section in Azure and securely connect it to their on-premises datacenter or a single client machine using an IPsec connection.

Azure Virtual Network encompasses the following:

- **VNet Directory Service** - Virtual Network Directory Service is a lightweight, reliable and high performance service that maintains the mappings from customer IP address space to physical IP address space.

- **Network Manager Agent** - Node Network Manager Agent (NM Agent) is a plugin that has the physical address, customer address and MAC address of the Node and interacts with the Visual FoxPro (VFP) driver.

- **Network Service Manager** - Network Service Manager (NSM) is a cluster level network controller which manages network resources and network state provisioning.

- **Regional Network Manager** - Regional Network Manager (RNM) is the service responsible for managing network resources on a regional basis for the virtual network.

ExpressRoute

Azure ExpressRoute enables customers to extend their on-premises networks into Azure over a dedicated private connection facilitated by a connectivity partner. Connectivity can be from any-to-any (IP Virtual Private Network (VPN)) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a co-location facility.

Traffic Manager

Azure Traffic Manager allows customers to control distribution of user traffic to their specified endpoints, which can include Azure Cloud services, websites and other endpoints. Traffic Manager applies an intelligent policy engine to Domain Name Service (DNS) queries for the domain names of their Internet resources.

Load Balancer

Azure Load Balancer is an infrastructure component that provides load balancing capabilities to internal components as well as to external customers who want to add high availability and capacity to their applications. Load Balancer distributes incoming traffic load among healthy service instances in Cloud Services or VMs defined in a load balancer set. Azure Load Balancer can be used for TCP / UDP-based protocols such as HTTP, HTTPS, SMTP, as well as other protocols used for real-time voice and video messaging applications.

Application Gateway

Application Gateway is a virtual appliance that offers HTTP-based application delivery services through HTTP round-robin load balancing, session affinity via cookies, and SSL offload.

VPN Gateway

VPN Gateway is used to send network traffic between virtual networks and on-premises locations. It is also used to send traffic between multiple virtual networks within Azure (VNet-to-VNet).

Media

Media Services

Azure Media Services provides customers a PaaS layer for managing media workflows in Azure. The two services in production today are Media Encoding and Media Streaming. Media Encoding enables customers to upload their raw mezzanine content to Azure Storage and trigger media processing jobs. Media Streaming enables customers to deliver media for consumption by end-users.

Enterprise Integration

Service Bus

Service Bus provides a multi-tenant service for connecting applications through the cloud. It provides a hosted, secure, and widely available infrastructure for widespread communication, large-scale event distribution, naming, and service publishing.

Backup

Microsoft Azure Backup enables customers to protect important server data off-site with automated backup to Microsoft Azure. Customers can manage their cloud backups from the tools in Windows Server, Windows Server Essentials, or System Center Data Protection Manager.

Site Recovery

Microsoft Azure Site Recovery contributes to a customer's Business Continuity and Disaster Recovery (BCDR) strategy by orchestrating replication of on-premises physical servers and virtual machine servers to the cloud (Azure) or to a secondary datacenter.

Identity & Access Management

Azure Active Directory

Microsoft Online Directory Services

Azure Active Directory is a comprehensive identity and access management cloud solution that provides a robust set of capabilities to manage users and groups. It helps secure access to on-premises and cloud applications, including Microsoft Online Services like Office 365 and many non-Microsoft SaaS applications.

Federated Sync - The Federated Service Synchronization web service enables federated services to synchronize identity, address book, and licensed capability assignments from the Microsoft Online Directory Services (MSODS) or simply Directory Services (DS) and to publish provisioning-related state back to the DS.

Directory Synchronization - Directory Synchronization (DirSync) is a foundational and critical scenario of the identity and access management solution used for integrating with Azure AD. With

Directory Synchronization, customers can manage the entire lifecycle of their cloud user and group accounts using their on-premises AD management tools.

Organizational Identity

Organizational Identity (OrgID) is the identity provider for Azure Active Directory. It provides authentication services for identities owned by enterprise customers of Microsoft's Cloud Services, including Azure and Office 365.

Evolved Secure Token Service

Evolved Secure Token Service (evoSTS) is an Azure web service role built for identity and federation, providing a stateless service that accesses multiple principal and key stores. evoSTS absorbs the roles of multiple STSs, so that partners see one Azure AD STS.

Access Control Service

Access Control Service (ACS) is a cloud-based service that provides an easy way of authenticating and authorizing users to gain access to web applications and services while allowing the features of authentication and authorization to be factored out of the code.

Device Registration Service

Azure Device Registration Service (ADRS) enables customers' employees' devices to be provisioned with an identity.

Identity and Access Management

Identity and Access Management - Self Service Password Reset

The Identity and Access Management - Self Service Password Reset (IAM - SSPR) service is a cloud-based service that allows Azure AD tenant administrators to register for and subsequently reset their passwords without needing to contact Microsoft support.

Identity and Access Management - Cloud Password Single Sign On

IAM - Cloud Password Single Sign On (SSO) provides customers the ability to use a single set of credentials to access both on-premises and online resources.

Identity and Access Management - Self Service Group Management

The IAM - Self Service Group Management (SSGM) service supports group object Create, Read, Update, and Delete (CRUD) operations through Graph API. The Azure Active Directory Graph API provides programmatic access to Azure AD through Representational State Transfer (REST) API endpoints. Applications can use the Graph API to perform CRUD operations on directory data and objects.

Identity and Access Management - Sync Fabric

IAM - Sync Fabric (SF) enables the automatic creation, management and removal of user identities in SaaS applications by connecting to provisioning endpoints provided by application vendors.

Rights Management Service

Azure Rights Management Service (RMS) helps protect organization's sensitive information from unauthorized access, and controls how this information is used. Rights Management uses encryption, identity, and authorization policies to help protect files and email.

Multi-Factor Authentication

Multi-Factor Authentication (MFA) is a method of authentication that requires the use of more than one verification method and adds a critical second layer of security to user sign-ins and transactions to cloud-based and on-premises applications.

Management & Security

Scheduler

Scheduler is a high availability service that enables customers to create jobs that can invoke an HTTP / HTTPS endpoint, and post a message to an Azure Storage queue, Azure Service Bus queue, or Azure Service Bus topic on a regular interval or prescribed schedule.

Automation

Azure Automation service provides customers a fully managed, multi-tenant, PaaS layer for automating daily processes, and reducing error-prone manual activities. Customers can orchestrate their end-to-end workflows, as well as integrate with many systems within Azure.

Key Vault

Key Vault helps safeguard cryptographic keys and secrets used by cloud applications and services. It streamlines the key management process and enables customers to maintain control of keys that access and encrypt their data.

Log Analytics

Log Analytics service enables customer's IT operations teams to gain deep insights from Windows Servers and Linux source, and from any datacenter and cloud environments. It enables transformation of machine data into near real-time operational intelligence and provides Microsoft and community-developed patterns for analyzing data and better decision making.

Intune

Intune is a cloud-based service that helps customers manage Windows PCs, and iOS, Mac OS X, Android, and Windows mobile devices. Customers can use Intune alone or integrate it with System Center 2012 R2 Configuration Manager to extend their management capabilities.

Azure Services Supporting Infrastructure

Physical Network

The Azure Physical Network (PhyNet) infrastructure is used to provide all datacenter connectivity for all Azure capacity - Compute, Storage, etc. The physical network infrastructure is completely transparent to all Azure customers.

Active Directory Gateway

Active Directory Gateway (ADGateway) is an Azure web service which acts as a stateless front door / reverse proxy for all requests to other services in Azure AD.

Active Directory Portal Extension for Ibiza Portal

Active Directory Portal Extension for Ibiza Portal (ADIUX) is a stateless UI service built on top of Ibiza SDK to be used in the Azure Management Portal to allow Role Based Access Control (RBAC) scenarios, such as enumerating roles, assigning and removing users and groups from roles and vice versa, inviting MSA users into directory in order to assign them to roles etc.

Identity and Access Management - User Interface

The IAM – User Interface (ADUXP) service acts as the core data layer that serves the Azure Portal Administrator UX, as well as portions of the Information Worker UX.

Identity and Access Management - User Experience

IAM - User Experience (IAMUX) is a simple web service that hosts various pages that information workers interact with to perform daily tasks like managing their profile, changing their passwords, and the like.

Policy Administration Service

Policy Administration Service (PAS) is responsible for providing RBAC capability to an application.

Red Dog Operating System

The Red Dog Operating System (RDOS) team provides all Guest and Host Operating Systems for the virtual environment and the services hosted on Azure.

Secret Store

Secret Store is an encrypted storage solution for securely managing secrets of the Microsoft Azure platform.

Datacenter Secrets Management Service

Datacenter Secrets Management Service (dSMS) is a Microsoft Azure service which automates secrets generation, their delivery to the consumer services and periodic rollover at runtime.

Azure Resource Manager

Azure Resource Manager (ARM) is a collection of capabilities that enables the deployment and management of resources in Azure.

Service Fabric - Resource Provider Clusters

Service Fabric - Resource Provider (RP) Clusters provide the runtime and VM hosting capabilities for the Azure core resource providers which include Compute Platform and Network Resource Provider.

Compute Platform

Compute Platform (CP) offers the regional Control Plane for all IaaS-related services for Azure Compute Manager.

Network Resource Provider

Network Resource Provider (NRP) is the frontend service for Microsoft Azure Networking.

Storage Resource Provider

Storage Resource Provider (SRP) enables customers to manage storage accounts and keys programmatically.

Datacenter Security Token Service

Datacenter Security Token Service (dSTS) provides a highly available and scalable security token service for authenticating and authorizing clients (users and services) of Azure Foundation and Essential services.

Jumpboxes

Jumpboxes are used by Azure service teams to operate Azure services. Jumpbox servers allow access to and from datacenters.

DNS

AzDNS

AzDNS is the Domain Name System (DNS) service that hosts critical domains belonging to the Azure platform, as opposed to the customers' domains.

IDNS

The IDNS service offers hostname to Dedicated Internet Protocol (DIP) resolution within the customers' VNet. This allows different VMs / roles in the VNet to refer to each other by a friendly name rather than an IP.

Recursive Resolvers

Recursive Resolvers provide DNS resolution capabilities to Azure VMs and infrastructure.

OneDDoS

OneDDoS is a fully automated solution aimed primarily at protecting the underlying infrastructure from Distributed Denial of Service (DDoS) attacks.

Backend Health Management

Backend Health Management is available to first-party customers for management of hyper-scale services used in high-availability scenarios.

OneDeploy Express v2

OneDeploy Express v2 offers a safe and secure method to rollout services to multiple regions across Azure.

Windows Azure Network Monitoring

Windows Azure Network Monitoring (WANetMon) is a network monitoring tool used to monitor and troubleshoot issues within the Azure network.

Data

Customers upload data for storage or processing within the features / services or applications that are hosted on the cloud services platform. In addition, certain types of data are provided by the customers or generated on the customer's behalf to enable the usage of the Cloud Services. Microsoft only uses customer data in order to support the provisioning of the features / services subscribed to by the customers in accordance with the Service Level Agreements (SLAs).

Data Ownership

Microsoft does not inspect, approve, or monitor applications that customers deploy to Azure. Moreover, Microsoft does not know what kind of data customers choose to store in Azure. Microsoft does not claim data ownership over the customer information entered into Azure. Azure's Agreement states, "Except for Software we license to you, as between the parties, you retain all right, title and interest in and to Customer Data. We acquire no rights in Customer Data, other than the right to host Customer Data on Microsoft systems, including the right to use and reproduce Customer Data within Microsoft systems solely for such hosting purposes."