Azure Security and hosting for The Portal Connector (TPC).

This document describes Azure Security information as it pertains to hosting The Portal Connector as an App Service and detail options for supporting High Availability and Multi-region App Service configurations available in Azure. Also includes a link to Sitefinity's security and best practices whitepaper.

1. Azure Infrastructure and App Services

1.1. Introduction to Azure Security: https://learn.microsoft.com/en-us/azure/security/fundamentals/overview

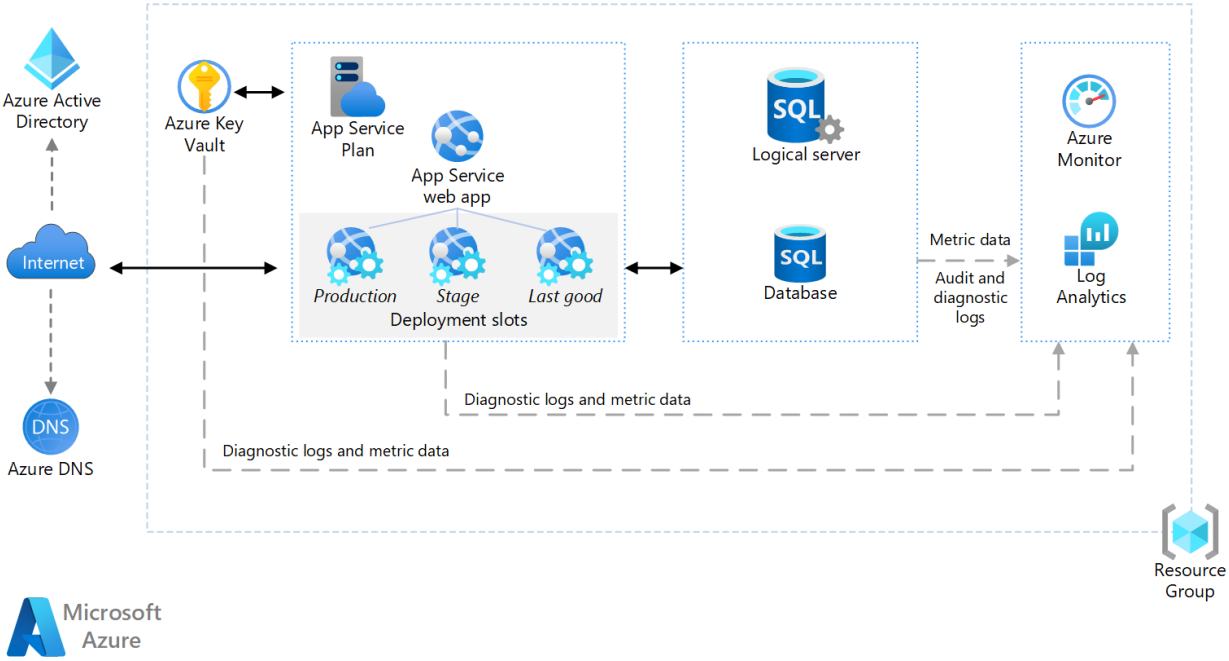


Figure 1: Azure Infrastructure

Microsoft Azure runs in datacenters managed and operated by Microsoft and comply with key industry standards, such as **ISO/IEC 27001:2013** and **NIST SP 800-53** for security and reliability.

- **ISO/IEC 27001:2013** specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization (https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en)

- **NIST SP 800-53** is a publication that recommends security controls for federal information systems and organizations and documents security controls for all federal information systems, except those designed for national security. (https://www.techopedia.com/definition/28830/nist-800-53)

1.2 Azure Infrastructure Security

The Microsoft Cloud Infrastructure and Operations team designs, builds, operates, and improves the security of the cloud infrastructure. This team ensures that the Azure infrastructure is delivering high availability and reliability, high efficiency, and smart scalability. The team provides a more secure, private, and trusted cloud.

Uninterruptible power supplies and vast banks of batteries ensure that electricity remains continuous if a short-term power disruption occurs. Emergency generators provide backup power for extended outages and planned maintenance. If a natural disaster occurs, the datacenter can use onsite fuel reserves.

a. Fundamentals: https://learn.microsoft.com/en-us/azure/security/fundamentals/infrastructure
b. Availability: https://learn.microsoft.com/en-us/azure/security/fundamentals/infrastructure-availability
c. Physical security: https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security

1.2.1 Azure Infrastructure Monitoring

https://learn.microsoft.com/en-us/azure/security/fundamentals/infrastructure-monitoring

Azure security has defined requirements for active monitoring. Service teams configure active monitoring tools in accordance with these requirements. Active monitoring tools include the Microsoft Monitoring Agent (MMA) and System Center Operations Manager. These tools are configured to provide time alerts to Azure security personnel in situations that require immediate action.

1.2.2 Azure Infrastructure Integrity

https://learn.microsoft.com/en-us/azure/security/fundamentals/infrastructure-integrity

All components in the software stack that are installed in the Azure environment are custom built following the Microsoft Security Development Lifecycle (SDL) process. All software components, including operating system (OS) images and SQL Database, are deployed as part of the change management and release management process. The OS that runs on all nodes is a customized version. The exact version is chosen by the fabric controller (FC) according to the role it intends for the OS to play. In addition, the host OS doesn't allow installation of any unauthorized software components.

1.2.3 Azure Data Protection

https://learn.microsoft.com/en-us/azure/security/fundamentals/protection-customer-data

Azure provides customers with strong data security, both by default and as customer options.
Data segregation: Azure is a multi-tenant service, which means that multiple customer deployments and VMs are stored on the same physical hardware. Azure uses logical isolation to segregate each customer's data from the data of others. Segregation provides the scale and economic benefits of multi-tenant services while rigorously preventing customers from accessing one another's data.
At-rest data protection: Customers are responsible for ensuring that data stored in Azure is encrypted in accordance with their standards. Azure offers a wide range of encryption capabilities, giving customers the flexibility to choose the solution that best meets their needs. Azure Key Vault helps customers easily maintain control of keys that are used by cloud applications and services to encrypt data. Azure Disk Encryption enables customers to encrypt VMs. Azure Storage Service Encryption makes it possible to encrypt all data placed into a customer's storage account.
In-transit data protection: Microsoft provides a number of options that can be utilized by customers for securing data in transit internally within the Azure network and externally across the Internet to the end user. These include communication through Virtual Private Networks (utilizing IPsec/IKE encryption), Transport Layer Security (TLS) 1.2 or later (via Azure components such as Application Gateway or Azure Front Door), protocols directly on the Azure virtual machines (such as Windows IPsec or SMB), and more.
Additionally, "encryption by default" using MACsec (an IEEE standard at the data-link layer) is enabled for all Azure traffic travelling between Azure datacenters to ensure confidentiality and integrity of customer data.

Data redundancy: Microsoft helps ensure that data is protected if there is a cyberattack or physical damage to a datacenter. Customers may opt for:

- In-country/in-region storage for compliance or latency considerations.
- Out-of-country/out-of-region storage for security or disaster recovery purposes.
  Data can be replicated within a selected geographic area for redundancy but cannot be transmitted outside it. Customers have multiple options for replicating data, including the number of copies and the number and location of replication datacenters.
  When you create your storage account, select one of the following replication options:
- **Locally redundant storage (LRS)**: Locally redundant storage maintains three copies of your data. LRS is replicated three times within a single facility in a single region. LRS protects your data from normal hardware failures, but not from a failure of a single facility.
- **Zone-redundant storage (ZRS)**: Zone-redundant storage maintains three copies of your data. ZRS is replicated three times across two to three facilities to provide higher durability than LRS. Replication occurs within a single region or across two regions. ZRS helps ensure that your data is durable within a single region.
- **Geo-redundant storage (GRS)**: Geo-redundant storage is enabled for your storage account by default when you create it. GRS maintains six copies of your data. With GRS, your data is replicated three times within the primary region. Your data is also replicated three times in a secondary region hundreds of miles away from the primary region, providing the highest level of durability. In the event of a failure at the primary region, Azure Storage fails over to the secondary region. GRS helps ensure that your data is durable in two separate regions.

Data destruction: When customers delete data or leave Azure, Microsoft follows strict standards for deleting data, as well as the physical destruction of decommissioned hardware. Microsoft executes a complete deletion of data on customer request and on contract termination. For more information, see Data management at Microsoft.

1.2.4 Azure information system components and boundaries

https://learn.microsoft.com/en-us/azure/security/fundamentals/infrastructure-components

Azure is a cloud computing platform and infrastructure for building, deploying, and managing applications and services through a network of datacenters. Microsoft manages these datacenters.

Based on the number of resources you specify, Azure creates virtual machines (VMs) based on resource need. These VMs run on an Azure hypervisor, which is designed for use in the cloud and isn't accessible to the public.
On each Azure physical server node, there's a hypervisor that runs directly over the hardware. The hypervisor divides a node into a variable number of guest VMs. Each node also has one root VM, which runs the host operating system. Windows Firewall is enabled on each VM. You define which ports are addressable by configuring the service definition file. These ports are the only ones open and addressable, internally or externally. All traffic and access to the disk and network is mediated by the hypervisor and root operating system.
At the host layer, Azure VMs run a customized and hardened version of the latest Windows Server. Azure uses a version of Windows Server that includes only those components necessary to host VMs. This improves performance and reduces attack surface. Machine boundaries are enforced by the hypervisor, which doesn't depend on the operating system security.

1.2.5 Azure Network Architecture

https://learn.microsoft.com/en-us/azure/security/fundamentals/infrastructure-network

The Azure network architecture provides connectivity from the Internet to the Azure datacenters. Any workload deployed (IaaS, PaaS, and SaaS) on Azure is leveraging the Azure datacenter network.

1.2.6 Azure SQL Database security features

https://learn.microsoft.com/en-us/azure/security/fundamentals/infrastructure-sql

Azure SQL Database provides a relational database service in 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. These capabilities build upon the controls that are inherited from Azure.

2. Azure App Services

2.1. **Security in Azure App Service**: https://learn.microsoft.com/en-us/azure/app-service/overview-security

The Portal Connector (TPC) is utilizing Azure App Service platform for hosting. The platform components of App Service, including Azure VMs, storage, network connections, web frameworks, management, and integration features, are actively secured and hardened. App Service goes through vigorous compliance checks on a continuous basis to make sure that:

- Your app resources are secured from the other customers' Azure resources.
- VM instances and runtime software are regularly updated to address newly discovered vulnerabilities.
- Communication of secrets (such as connection strings) between your app and other Azure resources (such as SQL Database) stays within Azure and doesn't cross any network boundaries. Secrets are always encrypted when stored.
- All communication over the App Service connectivity features, such as hybrid connection, is encrypted.
- Connections with remote management tools like Azure PowerShell, Azure CLI, Azure SDKs, REST APIs, are all encrypted.
- 24-hour threat management protects the infrastructure and platform against malware, distributed denial-of-service (DDoS), man-in-the-middle (MITM), and other threats.

3. Azure High availability zones and highly available multi-region architecture for App service deployments for TPC.

3.1. High availability zones:

3.1.1. Azure App Service can be deployed into availability zones (AZ) to help you achieve resiliency and reliability for your business-critical workloads. This architecture is also known as zone redundancy. Azure regions and availability zones are designed to help you achieve reliability for your business-critical workloads. Azure maintains multiple geographies. These discrete demarcations define disaster recovery and data residency boundaries across one or multiple Azure regions. Maintaining many regions ensures customers are supported across the world.

3.1.2. For App Services that are configured to be zone redundant, the platform automatically spreads the VM instances in the App Service plan across three zones in the selected region. If a VM instance capacity larger than three is specified and the number of instances is a multiple of three (3 * N), the instances will be spread evenly. However, if the number of instances is not a multiple of three, the remainder of the instances will get spread across the remaining one or two zones. Note: Additional hosting costs for additional App Services

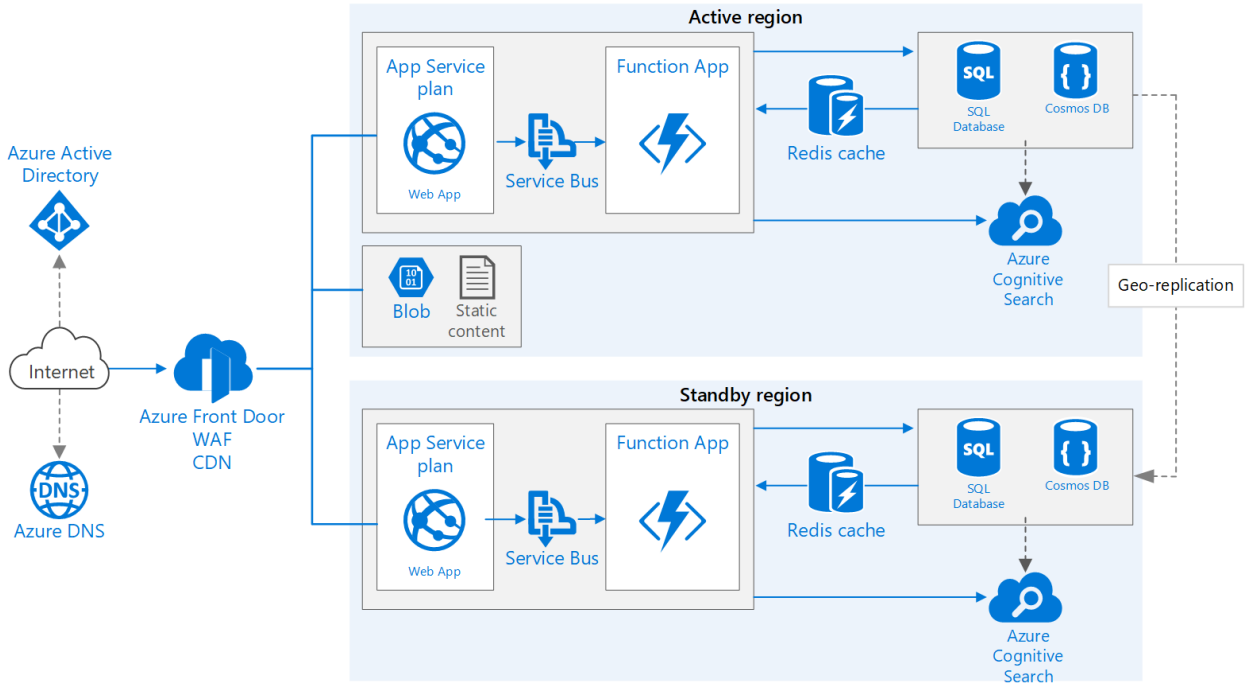
3.1.3. Can be enabled in any of the following regions:

- Australia East
- Brazil South
- Canada Central
- Central India
- Central US
- East Asia
- East US
- East US 2
- France Central
- Germany West Central
- Japan East
- North Europe
- Norway East
- Qatar Central
- South Africa North
- South Central US
- Southeast Asia
- Sweden Central
- Switzerland North
- UAE North
- UK South
- West Europe
- West US 2
- West US 3

3.2. Highly available multi-region App service:

This example architecture is based on the Scalable web application example architecture and extends it to show how to run an Azure App Service application in multiple regions to achieve high availability.

1.1 Architecture



High availability when configuring redundancy zones. 3 instances are balanced across zones.

https://learn.microsoft.com/en-us/azure/reliability/migrate-app-service

Note: Additional hosting costs for this configuration

4. **Sitefinity Security and their white paper:** https://www.progress.com/sitefinity-cms/platform/security