Azure Cloud Governance Design Document Version 0.1 Intact US CCoE

Table of Contents

[Introduction 4](#_Toc83898826)

[Definition of Scope 4](#_Toc83898827)

[Abbreviation 5](#_Toc83898828)

[Governance Foundation 5](#_Toc83898829)

[Azure Design 5](#_Toc83898830)

[Organization Structure 8](#_Toc83898831)

[Overview 8](#_Toc83898832)

[Tenant Management 8](#_Toc83898833)

[Management Groups 8](#_Toc83898834)

[Subscriptions 9](#_Toc83898835)

[Dev/Test Subscriptions 9](#_Toc83898836)

[Network & Connectivity 10](#_Toc83898837)

[Virtual Network (Vnet) 10](#_Toc83898838)

[CIDR Creation Process 10](#_Toc83898839)

[Network Interface 10](#_Toc83898840)

[Bastion 11](#_Toc83898841)

[Azure Firewall 11](#_Toc83898842)

[Azure Firewall Rules 12](#_Toc83898843)

[Traffic Manager 12](#_Toc83898844)

[Application Gateway 12](#_Toc83898845)

[NSG Flow 13](#_Toc83898846)

[Site-to-Site VPN 13](#_Toc83898847)

[Express Route Circuit 13](#_Toc83898848)

[Internal Load Balancer 13](#_Toc83898849)

[Compute & Storage 14](#_Toc83898850)

[Virtual Machines 14](#_Toc83898851)

[Storage Accounts 15](#_Toc83898852)

[Lifecycle management feature 15](#_Toc83898853)

[Azure Disks 15](#_Toc83898854)

[Snapshot 16](#_Toc83898855)

[Key Vault 16](#_Toc83898856)

[Key Vault Access Policy 16](#_Toc83898857)

[Management & Operations 16](#_Toc83898858)

[Azure Monitor 16](#_Toc83898859)

[Monitoring 16](#_Toc83898860)

[Metrics 17](#_Toc83898861)

[Logs 17](#_Toc83898862)

[Threshold Level 17](#_Toc83898863)

[Enable Azure Monitor and Alerts 17](#_Toc83898864)

[Enable Recommended Metric and Azure Alerts 18](#_Toc83898865)

[Log Analytics Workspace 18](#_Toc83898866)

[Activity Logs 19](#_Toc83898867)

[Azure Backup & Restore 19](#_Toc83898868)

[Backup – Virtual Machine 19](#_Toc83898869)

[Backup – SQL PaaS Databases 20](#_Toc83898870)

[SQL Databases Backup Policy 20](#_Toc83898871)

[Backup – Collect IaC Templates 21](#_Toc83898872)

[Security & Compliance 21](#_Toc83898873)

[Policy Standards 21](#_Toc83898874)

[Azure Policy Exceptions 22](#_Toc83898875)

[Azure Policy Exemptions 22](#_Toc83898876)

[Azure Policy Effects 22](#_Toc83898877)

[Configuration Policies to be Applied 22](#_Toc83898878)

[Configuration Policies with Resource Exclusions 25](#_Toc83898879)

[Configuration Policies Requires approval 26](#_Toc83898880)

[Building Blocks 27](#_Toc83898881)

[Naming Standards 27](#_Toc83898882)

[Tagging 28](#_Toc83898883)

[Azure Blueprints for IaC 28](#_Toc83898884)

[ARM Templates 29](#_Toc83898885)

[CCoE US Process 29](#_Toc83898886)

[Azure Advisor 30](#_Toc83898887)

[Appendix 30](#_Toc83898888)

# Introduction

INTACT US is looking to secure and govern their Azure cloud with best policies for engineering & operations, optimum cost, and top-notch security. To help attain the above task, the activities are divided into three sections.

This document provides technical design for activities that are to be performed in only *Cloud Engineering*.

The purpose of this document is to define the Azure governance- Cloud Operations INTACT US. It refers to Policies, Standards, design decisions, and constraints that INTACT US should be aware of and sign-off of the Technical Design architecture.

This document is based on the Intact US and Microsoft Cloud Adoption Framework for Azure and will be leveraged to adopt best practices, tools and guidance prescribed by Intact US to help achieve desired business outcomes. This guidance aligns to the following phases of the cloud adoption lifecycle, ensuring easy access to the right guidance at the right time.

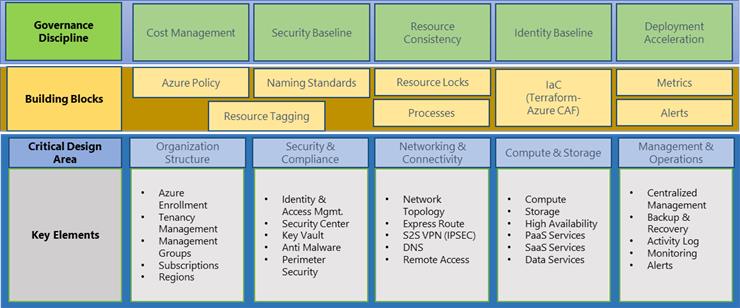
## Definition of Scope

Now Word knows that paragraph is a heading and includes it in the TOC.

## Abbreviation

|  |  |
| --- | --- |
| **Abbreviation** | **Description** |
| IaC | Infrastructure as Code |
| VPN | Virtual Private Network |
| Vnet | Virtual Network |
| RBAC | Role Based Access Control |
| IDAM | Identity and Access Management |
|  |  |

# Governance Foundation



TOC.

# Azure Design

Intact US’s design topology within Azure is a Hub and Spoke model. The hub is a virtual networks (VNet) in Azure that acts as a central point of connectivity and shared services. The Hub connects to the on-premises network. The spokes are VNets that peer with the Hub and used to isolate workloads, departments, subscriptions, etc. while sharing the common services. Traffic flows between the on-premises data-center and the hub through an ExpressRoute or VPN gateway connection. The spokes are infrastructure logical level subscriptions with High Availability in the Azure region.

At present, the majority of the resources in Azure are not exposed to the public network. All the traffic is routed through Palo Alto via UDR from Azure.



**Components used in Architecture**

* **Hub VNet**. The hub is the central point of connectivity to host services and the internet. Services deployed in Hub VNet can be consumed by the different workloads hosted in the spoke VNets.
* **Workload subnet**. The subnets are defined in the Spoke VNets.
* **Spoke VNets**. Spokes are used to isolate workloads in their VNets, managed separately from other spokes. Each workload includes multiple tiers, with multiple subnets connected through Azure load balancers.
* **VNet peering**. To establish communication between two VNets, the VNets must peer to each other. Peering connections are non-transitive, low latency connections between VNets. VNet peering is used to connect the hub to each spoke.
* **UDR**User Defined Routing or UDR to control the routing tables between subnets within a subnet as well as between VNets thereby allowing for greater control over network traffic flow.
* **Azure Firewall**Azure Firewall is deployed in the hub, which provides an additional layer of security.
* **Network Security Groups (NSG), Application Security Groups (ASG) and Azure DNS**- Private DNS for private endpoints which is automatically created and removed by azure.
* **Azure Storage Accounts** – Secure transfer is enabled to allow blob public access is disabled. No anonymous access to the blobs within the storage account is permitted.
* **Azure Virtual Machine sizes** – VM sizes are fixed based on use cases and types (General, Memory, and Compute-optimized)
* **Managed Disks and Encryption.** – Azure managed disk default encryption is enabled
* **Azure Recovery Vault (Backup)** – Azure site recovery for production workloads in the East US2 region with 24-hour-retention-policy.
* Managed Identities, Azure MFA, RBAC, ADFS
* **Azure Monitor and Event Hub** – Logs are fetched from the resources and using the consumer group the logs are being monitored.
* **Azure Naming Convention** – Azure standard naming convention is being followed  <https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/resource-naming>
* **Azure Terraform** Deployment template (for New requests)

# Organization Structure

## Overview

## Tenant Management

Azure provides four levels of management scope: management groups, subscriptions, resource groups, and resources. The following image shows the relationship of these levels.

* **Management groups:** These groups are containers that help you manage access, policy, and compliance for multiple subscriptions. All subscriptions in a management group automatically inherit the conditions applied to the management group.
* **Subscriptions**: A subscription logically associates user accounts and the resources that were created by those user accounts. Each subscription has limits or quotas on the amount of resources you can create and use. Organizations can use subscriptions to manage costs and the resources that are created by users, teams, or projects.
* **Resource groups**: A resource group is a logical container into which Azure resources like web apps, databases, and storage accounts are deployed and managed.
* **Resources:** Resources are instances of services that you create, like virtual machines, storage, or SQL databases.

## Management Groups

An Azure Management group is logical containers that allow Azure Administrators to manage access, policy, and compliance across multiple Azure Subscriptions. Management groups allows administrator to build an Azure Subscription tree that can be used with several other Azure service, including **Azure Policy** and **Azure Role Based Access Control**. Azure Management Groups provide flexibility for organizing policy, access control, and compliance across multiple subscriptions.

Intact US CCoE has to define the Management group hierarchy based on cloud departments accessing azure subscriptions. The best way to utilize Management groups, hierarchy as shown below

## 

## Subscriptions

A Subscription in Azure is a logical container into which Azure resources (Virtual Machines, Virtual Networks, Storage Accounts, etc.) can be deployed. It can also be used for coarse-grained access control to these resources, by leveraging [Role Based Access Control (RBAC)](https://docs.microsoft.com/en-us/azure/role-based-access-control/overview) or [Management Groups](https://docs.microsoft.com/en-us/azure/azure-resource-manager/management-groups-overview). Subscriptions are not tied to an Azure Region and as a result can contain resources from any number of Regions.

Effective subscription design helps organizations establish a structure to organize and manage assets in Azure.  As accounts provide segregation at a high level, we need to define the number of accounts that need to be created. Base the creation of accounts online of businesses, compliance, and environment within the organization. There are seven main types of subscriptions available,

* Management Subscription
* Connectivity Subscription
* Identity Subscription
* Dev / Non-Prod Subscriptions
* Prod Subscription
* Sandbox Subscription
* Decommission Subscription

### Dev/Non-Prod Subscriptions

Intact US to utilize Azure Dev/Non-Prod service provided by Microsoft Azure which provides functionality for managing environments that contain Azure Virtual Machines.

It helps developers and testers to quickly create environments in Azure whilst minimizing waste and controlling cost. Developers can also use artifacts to quickly deploy and configure applications. By using custom images and formulas, developers can save virtual machines (VMs) as templates, and easily reproduce them across the team. Dev/Non-Prod Labs also offers several configurable policies that lab administrators can use to reduce waste and manage a team’s environments. **The benefit of no additional Microsoft software charges on Azure Virtual Machines and exclusive dev/test rates on other Azure services.**

**Key Features: -**

* Quickly provision development and test environments
* Minimize waste with quotas and policies.
* Works with your CI/CD tools
* Special lower Dev/Test rates on Windows Virtual Machines, Cloud Services, SQL Database, HDInsight, App Service and Logic Apps
* Additional savings with Reservations for one-year or three-year commitment on VMs and Azure SQL Database
* Same great EA rates on other Azure services
* Centralized management via the Azure Enterprise Portal
* No separate payment - just use the funds already on your Enterprise Agreement.

# Network & Connectivity

## Virtual Network (Vnet)

Intact US has divided their network infrastructure at the subscription level like DEV, PROD.  Additionally, maintains two separate virtual network in each subscription.

* Vnet with separate subnets for App, Web, DB and Integration (Shared Services) Tier

Add Security team recommendations if any.

## CIDR Creation Process

Intact maintains unique IP ranges across Azure region and environments and stores the data in the standard document. “”

Virtual network created IP address range that has been used will be marked as assigned in CIDR inventory and will not be used for other environments.

* Intact Us to perform the cleanup activity on regular interval.
  + Frequency – Bi-Weekly

## Network Interface

Azure network security group will be used to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, source and destination, port, and protocol can be specified.

Refer below table with approved list of inbound and outbound ports for each application.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Category** | **Best Practices** | **Impacted Resource count** | **Action Plan** | **Intact US Feedback** |
| Network & Security | Network Security Groups Inbound Rules with Potentially Dangerous Ports Exposed | ?? | Checks each Network Security Group to ensure it does not allow traffic from potentially dangerous ports. | Need to review the open ports considered dangerous |
| Network Security Groups Outbound Rules Set To All Ports | >> | Checks each Network Security Group to see if it allows outbound traffic from all ports. | Since all traffic goes through Firewall we determined not to configure outbound ports. |
| Network Security Groups Outbound Rules with Dangerous Ports Exposed | !! | Checks each Network Security Group to see if it allows outbound traffic to a dangerous port. | Since all traffic goes through Firewall we determined not to configure outbound ports. |
| Network Security Groups Outbound Rules with Potentially Dangerous Ports Exposed | !! | Checks each Network Security Group to see if it allows outbound traffic to a potentially dangerous port. | Since all traffic goes through Firewall we determined not to configure outbound ports. |

## Bastion

Azure Bastion is a fully managed PaaS service that provides secure and seamless RDP and SSH access to virtual machines directly through the Azure Portal. Azure Bastion is provisioned directly in Virtual Network (VNet) and supports all VMs in your Virtual Network (VNet) using SSL without any exposure through public IP addresses.

Bastion provides secure RDP and SSH connectivity to all the VMs in the virtual network in which it is provisioned. Using Azure Bastion protects virtual machines from exposing RDP/SSH ports to the outside world, while still providing secure access using RDP/SSH. With Azure Bastion, you connect to the virtual machine directly from the Azure portal without additional agent installed on virtual machines or creating a jump host.

* we suggest to utilize Bastion service for secure RDP and SSH connectivity.
* Azure currently support Azure Bastion and VNet peering can be used together. When VNet peering is configured, you don't have to deploy Azure Bastion in each peered VNet.

## Azure Firewall

Azure Firewall is managed cloud-based network security service that protects your Azure Virtual Network resource, It’s a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.

Azure Firewall supports inbound and outbound filtering. Inbound protection is typically used for non-HTTP/S protocols. For example, RDP, SSH, and FTP protocols. For best inbound HTTP/S protection, use a web application firewall such as Azure Web Application Firewall (WAF).

### Azure Firewall Rules

*Application Rule Collection:*

Limiting outbound HTTP/S traffic to a specified list of fully qualified domain names (FQDN) including wild cards.  An FQDN tag represents a group of fully qualified domain names (FQDNs) associated with well-known Microsoft services. What are the Microsoft services to tagged and allowed to be determined (Based on requirements).Custom FQDN rules (specific traffic to be allow) creating Target FQDN.

*Network rule Collection:*

Network traffic rules allow or deny network traffics by source and destination IP address, port, and protocol. Azure Firewall is fully stateful, so it can distinguish legitimate packets for different types of connections. Rules are enforced and logged across multiple subscriptions and virtual networks.

* Intact US to document all Firewalls rules in a centralized repository.
* Intact US can use Azure firewall manager as centralized configuration and management of multiple Azure Firewall instances, across Azure regions and subscriptions.
* Intact US to review below list of Virtual Networks does not have Firewall configured and also maintain exclusion list.

|  |  |  |  |
| --- | --- | --- | --- |
| **Virtual Networks** | **Azure Firewall Policy** | **Resource Group** | **Location** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Traffic Manager or cloudflare

Azure Traffic Manager is a DNS-based traffic load balancer that helps to distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness.

Traffic Manager uses DNS to direct client requests to the most appropriate service endpoint based on a traffic-routing method and the health of the endpoints. An endpoint is any Internet-facing service hosted inside or outside of Azure. Traffic Manager provides a range of traffic-routing methods and endpoint monitoring options to suit different application needs and automatic failover models. Traffic Manager is resilient to failure, including the failure of an entire Azure region though Traffic manager has feature automatic failure.

* Intact US currently not using Traffic manager. Use this service for future requirement to separate the traffic between application in different Azure regions.

## Application Gateway or cloudflare

Application Gateway is L7 load balancer from Azure service. Proposing to enable Web Application Firewall on Application gateway.  Application Gateway can make routing decisions based on additional attributes of an HTTP request, unlike traditional load balancer.

Azure Web Application Firewall (WAF) on Azure Application Gateway provides centralized protection of your web applications from common exploits and vulnerabilities. Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. SQL injection and cross-site scripting are among the most common attacks.

WAF on Application Gateway is based on Core Rule Set Addressed Web Application Security Project (OWASP) vulnerabilities. The WAF automatically updates to include protection against new vulnerabilities, with no additional configuration needed.

Application Gateway is L7 load balancer from Azure service. Proposing to enable Web Application Firewall on Application gateway.  Application Gateway can make routing decisions based on  
Implement Azure policy for Web Application Firewall (WAF) should use the detection mode for Application Gateway. Also add exceptions for to WAF that can only be in detection due to SLA.

## NSG Flow

**Flow** logs are the source of truth for all network activity in your cloud environment. Whether you're trying to optimize resources or large enterprise trying to detect intrusion, Flow logs are your best bet. You can use it for optimizing network flows, monitoring throughput, verifying compliance, detecting intrusions and more.

* Currently, we propose Intact US to maintain flow log retention for 3 days. Implement Azure policy for Flow log should be configured for every network security group.

## Express Route Circuit

ExpressRoute extend your on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider. With ExpressRoute, we can establish connections to Microsoft cloud services, such as Microsoft Azure and Office 365.

ExpressRoute connections do not go over the public Internet. This allows ExpressRoute connections to offer more reliability, faster speeds, consistent latencies, and higher security than typical connections over the Internet.

Based on Intact US existing architecture, Express route Circuits are currently in two regions (East US2 & West US2), two peering locations (Washington DC & Chicago) and Seven Subscriptions.

## Internal Load Balancer

Application Gateway will be used as Internal load balancer. Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications. Traditional load balancers operate at the transport layer (OSI layer 4 – TCP and UDP) and route traffic based on source IP address and port, to a destination IP address and port.  Intact Us has Application gateway load balancer with WAF (Web Application Firewall)

# Compute & Storage

## Virtual Machines

Azure Virtual Machine is one of several types of on-demand, scalable computing resources that Azure offers. Typically, it is advised to choose a virtual machine if need is for more control over the computing environment than the other choices offer.

Virtual Machines are critical Azure services in Intact US Infra environment.  Decision on Azure virtual machine sizing should be based on determining factors like such as processing power, memory, and storage capacity. VM sizes will be different for different workloads such as Web server machines does not require compute power while database servers require more compute power than web and application server. Below are preferred VM sizes

|  |  |
| --- | --- |
| **General Purpose**: Balanced CPU-to-memory ratio. Ideal for testing and development, small to medium databases, and low to medium traffic web servers. | B2ms (2vCPU, 8 GiB Mem, up to 4 data disk, 1920 max IOPS) |
| B4ms (4vCPU, 16 GiB Mem, up to 8 data disk, 2880 max IOPS) |
| B8ms (8vCPU, 32 GiB Mem, up to 16 data disk, 4320 max IOPS) |
| D2s\_v3 (2vCPU, 8 GiB Mem, up to 4 data disk, 3200 max IOPS) |
| D4s\_v3 (4vCPU, 16 GiB Mem, up to 8 data disk, 6400 max IOPS) |
| D8s\_v3 (8vCPU, 32 GiB Mem, up to 16 data disk, 12800 max IOPS) |
| DS1\_v2 (1vCPU, 3.5 GiB Mem, up to 4 data disk, 3200 max IOPS) |
| DS2\_v2 (2vCPU, 7 GiB Mem, up to 8 data disk, 6400 max IOPS) |
| DS3\_v2 (4vCPU, 14 GiB Mem, up to 16 data disk, 12800 max IOPS) |
| DS4\_v2 (8vCPU, 28 GiB Mem, up to 32 data disk, 25600 max IOPS) |
| DS5\_v2 (16vCPU, 56 GiB Mem, up to 64 data disk, 51200 max IOPS) |
| **Memory Optimized**: High memory-to-CPU ratio. Great for relational database servers, medium to large caches, and in-memory analytics. | E2s\_v3 (2vCPU, 16 GiB Mem, up to 4 data disk, 3200 max IOPS) |
| E4s\_v3 (4vCPU, 32 GiB Mem, up to 8 data disk, 6400 max IOPS) |
| E8s\_v3 (8vCPU, 64 GiB Mem, up to 16 data disk, 12800 max IOPS) |
| **Compute Optimized**: High CPU-to-memory ratio. Good for medium traffic web servers, network appliances, batch processes, and application servers. | F2s\_v2 (2vCPU, 4 GiB Mem, up to 4 data disk, 3200 max IOPS) |
| F4s\_v2 (4vCPU, 8 GiB Mem, up to 8 data disk, 6400 max IOPS) |
| F8s\_v2 (8vCPU, 16 GiB Mem, up to 16 data disk, 12800 max IOPS) |

## Storage Accounts

Azure Storage platform is Microsoft's cloud storage solution for modern data storage scenarios. Core storage services offer a massively scalable object store for data objects, disk storage for Azure virtual machines (VMs), a file system service for the cloud, a messaging store for reliable messaging, and a NoSQL store.

Azure Storage accounts will be leveraged to store the Virtual Machines boot diagnostic logs. Diagnostic logs will be to check the boot logs in case of Virtual Machine booting issues and to check the Virtual Machine status under Boot Diagnostics section.

### Lifecycle management feature

Intact US recommend utilizing the Storage “*Lifecycle management*” feature to auto manage Storage tiers to optimize performance and cost.

Azure Blob Storage lifecycle management offers a rich, rule-based policy which you can use to transition your data to the best access tier and to expire data at the end of its lifecycle.

Lifecycle management policy helps you:

* Transition blobs to a cooler storage tier such as hot to cool, hot to archive, or cool to archive in order to optimize for performance and cost.
* Delete blobs at the end of their lifecycles.
* Define up to 100 rules.
* Run rules automatically once a day.
* Apply rules to containers or specific subset of blobs, up to 10 prefixes per rule.

## Azure Disks

Disks used in Azure virtual machines as a place to store an operating system, applications, and data. Page Blobs are used to store the disks. Azure Disks are designed for 99.999% availability.

* *Unmanaged disks* - Unmanaged disks are the traditional type of disks that have been used by VMs. With these, you create your own storage account and specify that storage account when create the disk. We have to make sure don't put too many disks in the same storage account to overcome the 20,000 IOPS per Storage limitation.
* *Managed Disks* - Handles the storage account creation/management in the background for us and ensures that do not have to worry about the scalability limits of the storage account. We need to simply specify the disk size and the performance tier (Standard/Premium).
  + Standard Disk - Standard Disk is backed by HDDs and delivers cost-effective storage.
  + Premium Disk - Premium Disk is backed by SSDs, and delivers high-performance, low-latency disk support for VMs running I/O-intensive workloads. We can use Premium Disks with DS, DSv2, GS, Ls, or FS series Azure VMs.

Intact US to audit and clean the unattached disks from all Azure subscriptions.

Intact US to perform the cleanup activity on regular interval.

* Frequency – Bi-Weekly

## Snapshot

Intact US uses snapshot feature to create image of existing virtual machines prior to making any changes to environment. Azure snapshots and images are charged at $0.05/GB per month for both Standard LRS and ZRS options based on the used portion of the disk.

For example, if you create a snapshot of a managed disk with provisioned capacity of 128 GB and actual used data size of 10 GB, snapshot will be billed only for the used data size of 10 GB. If you choose to store them on SSD storage, you will be charged at $0.132/GB per month.

* Intact US to audit the existing snapshot and delete the unwanted snapshots.
* Avoid taking snapshots in premium SSD.
* Intact US to perform the cleanup activity on regular interval.
  + Frequency – Bi-Weekly

## Key Vault

Azure Key Vault is a tool for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, or certificates. A vault is a logical group of secrets.

Azure Key vault will be used to store local account passwords, SSL certificates required for Web servers and SQL encryptions keys. One Azure key vault will be created for each customer and it will be mapped to customer Azure Active Directory in customer service platform.

* Intact US to create access policy definitions for Azure Key vault management.
* Implement below list of Azure policies to maintain the configuration standards
  + Certificates should have the specified maximum validity period.
  + Key vaults should have soft delete enabled.
  + Keys should have expiration dates set.
  + Secrets should have expiration dates set.
  + Secrets should have the specified maximum validity period.

### Key Vault Access Policy

Access to Azure Key vault will be managed using Built in roles and Key vault access policy through Azure Active Directory Security groups. Key Vault Contributor is a built-in role available which will provide contributor access to Azure Key vault. Access Policy is a setting available within Azure Key Vault to define the access for secrets, keys, and certificates. Access policy can be created for users, security groups, managed identities, Azure applications.

# Management & Operations

## Azure Monitor

### Monitoring

Intact US will use Azure Monitor to monitor all Azure service and integrate with ELK or command center. Azure Monitor is a full stack monitoring service in Azure that provides a complete set of features to monitor Azure resources in addition to resources in other clouds and on-premises. The Azure Monitor data platform collects data into logs and metrics where they can be analyzed together using a complete set of monitoring tools. All data collected by Azure Monitor fits into one of two fundamental types, **metrics and logs.**

### Metrics

Metrics are numerical values that describe some aspect of a system at a particular point in time. They are lightweight and capable of supporting near real-time scenarios. Metrics are collected at regular intervals and are useful for alerting because they can be sampled frequently, and an alert can be fired quickly with relatively simple logic. Metrics are retrieved from Virtual Machine host level.

Intact US has shared the recommended services for Azure services and divided metrics into three categories.

* Availability and Outage
* Proactive Monitoring
* Trend analysis

### Logs

Logs in Azure Monitor contain different kinds of data organized into records with different sets of properties for each type. Logs can contain numeric values like Azure Monitor Metrics but typically contain text data with detailed descriptions. They further differ from metric data in that they vary in their structure and are often not collected at regular intervals. Telemetry such as events and traces are stored Azure Monitor Logs in addition to performance data so that it can all be combined for analysis.

A common type of log entry is an event, which is collected sporadically. Events are created by an application or service and typically include enough information to provide complete context on their own. For example, an event can indicate that a particular resource was created or modified, a new host started in response to increased traffic, or an error was detected in an application. Logs are retrieved from Virtual Machines Guest level.

Log rhythm and Sentinel

### Threshold Level

* To enable monitoring for all Azure services.
* Analyze the trend for each metric with at least 2 weeks of data.
* Identify the threshold value based on trend/usage analysis and enable Azure alerts.

### Enable Azure Monitor and Alerts

* Intact US to enable Azure monitor for below Azure Services with recommended metrics and alerts.
* Required to enable diagnostic setting for few services to capture the specific logs.
* Trustmark should have process in place to review whether all Azure services are being monitored.

|  |  |  |
| --- | --- | --- |
| **S. No** | **Resources** | **Recommended Metrics** |
| 1 | Express Route circuit | BitsInPerSecond, BitsOutPerSecond, Arp Availability, Bgp Availability |
| 2 | Firewall | Application rules hit count, Firewall health state, Network rules hit count |
| 3 | Load balancer | Data Path Availability, Health Probe Status |
| 4 | Public Ips | Inbound bytes DDoS, Under DDoS attack or not, Inbound packets DDoS, Byte Count, Data Path Availability |
| 5 | Traffic Manager | Endpoint Status by Endpoint, Queries by Endpoint Returned |
| 6 | Storage Accounts | Availability, Egress, Ingress, Used capacity. |
| 7 | Virtual Network Gateway | P2S Connection Count, Gateway S2S Bandwidth, Gateway P2S Bandwidth, Tunnel Bandwidth, Tunnel Egress Bytes, Tunnel Ingress Bytes |
| 8 | Application Gateway | Application Gateway Total Time, Web Application Firewall Blocked Requests Count, Current Capacity Units, Current Compute Units, CPU Utilization, Current Connections, Failed Requests, Total Requests, Unhealthy Host Count, Backend Connect Time, Backend Response Status, Client RTT |

### Enable Recommended Metric and Azure Alerts

Resources which are partially being monitored using Azure monitor or using log analytics from Azure Monitor.  Intact US to enable missing metric and alerts for below Azure services.

|  |  |  |
| --- | --- | --- |
| **S. No** | **Resources** | **Recommended Metrics** |
| 1 | Key Vault | Overall Vault Availability, Overall Vault Saturation |
| 2 | Virtual machines | Disk Read Bytes, Disk Write Bytes, Network In Total, Network Out Total, Percentage CPU |
| 3 | Azure SQL | Blocked by Firewall, CPU percentage, Data space allocated, Data space used percent, Deadlocks, DTU percentage, Failed Connections, Data space allocated, CPU percentage, DTU percentage, eDTU used, SQL Server process core percent, SQL Server process memory percent, Data space used percent, Workers percentage |
| 4 | Azure Cosmos DB | Account Network Settings Updated, Account Replication Settings Updated, Region Failed Over, Region Removed, Service Availability, Total Requests |
| 5 | Azure Backup or Recovery Vault | Send email alerts for both Azure backup and Site Recovery Failures.  Hence, no action is required |

## Log Analytics Workspace

Azure Monitor stores log data in a Log Analytics workspace, which is an Azure resource and a container where data is collected, aggregated, and serves as an administrative boundary. Data in a workspace is organized into tables, each of which stores different kinds of data and has its own unique set of properties based on the resource generating the data. Most data sources will write to their own tables in a Log Analytics workspace.

Log analytics workspace will be created in each subscription and corresponding virtual machines in that subscription will be connected to the workspace. Microsoft monitoring agent will be installed automatically on Virtual machine after the log analytics is connected and using Microsoft monitoring agent, logs will be captured. Logs will be further filtered using KQL (Kusto Query Language) and an Azure alert will be triggered automatically based on the threshold that has been set for monitoring.

* Set daily cap and data retention to control the usage cost [Link](https://docs.microsoft.com/en-us/azure/azure-monitor/platform/manage-cost-storage#default-retention)
* Create or use as few Log Analytics workspaces as possible, consolidate as much as you can into a “central” workspace.
* To avoid bandwidth costs by creating “regional” workspaces so that the sending Azure resource is in the same Azure region as your workspace.
* Be selective in installing Azure monitoring solutions to control ingestion costs.

## Activity Logs

Intact US uses activity logs with default retention of 90 days.

* Enable diagnostics setting for Azure Activity log to send and store logs for more than 90 days in a Storage account or Log analytics workspace.
* Enable activity log alert for Azure policy operations like write and delete operations to monitor policy changes. *Azure Monitor - Alerts New alert Rule - Select resource - Select type Policy Assignment - Conditions  - Select create/Delete/Exempt policy assignment.*
* Define and enable activity log alerts for critical administrative operations like resource deletion, etc.

## Azure Backup & Restore

Azure Backup is the Azure-based service use to back up and restore data in the Microsoft cloud.  Azure Backup is a cloud-based solution that is reliable, secure, and cost-competitive. Azure Backup offers multiple options to backup multiple type of data.  Azure backup provides multiple benefits like Unlimited scaling, Multiple storage options (LRS/GRS), Data encryption, Application-consistent backup, Long-term retention etc.

Azure Backup has been chosen as backup tool for customers' service platform since it is Azure cloud native tool, and it provides backup feature for all both Virtual machines and SQL database backup. Intact US to create process document for Backup, restore, retention policy for Virtual machines and Databases.

### Backup – Virtual Machine

Windows Virtual Machines in Azure environment will be added to Azure VM Backup. Azure VM Backup installs VM backup extension on target machines and use **VSS (Volume Shadow Copy)** to take full backups during the first backup and incremental backups after first backup is finished.

Features includes:

1. **Disk exclusion:** Disks from Virtual machines can be excluded to reduce backup cost.
2. **Incremental backup**: Incremental backup for Azure VM’s ensures that backups are using less storage and time efficient, by transferring only those changes made since the last backup.
3. **Compression:** Backups are compressed to reduce the required storage space
4. **Security:** All backup traffic from your servers to the Backup vault is encrypted by using Advanced Encryption Standard 256. The data is sent over a secure HTTPS link. The backup data is also stored in the Backup vault in encrypted form. Only the customer holds the passphrase to unlock this data. Microsoft cannot decrypt the backup data at any point.
5. **Maximum retention policy:** Daily backups can have maximum retention up to ?? days and yearly retention up to ?? years.

* CCoE team is working to enable backup for Virtual machines.
* CCoE team to identify the Virtual Machines and disk which can be excluded from complete VM Backup.  E.g., You have a critical data to be backed up in only one disk, or a subset of the disks and don’t want to back up the rest of the disks attached to a VM.
* CCoE team to maintain document for resource exclusions from Azure backup. E.g., Backed up by Commvault, Azure unsupported VMs.
* CCoE team to review the Azure Advisor report to know the Virtual machines are missing from Azure Backup.  *Azure Portal - Advisor - Recommendations - Security - Azure Backup* should be enabled for virtual machines.
* For any exclusion, Click the above Advisor rule, select the list of resources, click on Exempt, and select the exemption category.
  + - Mitigated (resolved through a third-party service)
    - Waiver (risk accepted)

**BreakUp list:**

|  |
| --- |
| Backup Needs to be enabled |
| Backup needs to be enabled after review |
| Backed up by Commvault |
| Backup not required (Domain Controllers, SCCM, Sandbox Servers) |
| Azure Backup Unsupported (OpenShift VMs) |

### Backup – SQL PaaS Databases

Azure Backup offers a stream-based, specialized solution to back up SQL Server running in Azure VMs. This solution aligns with Azure Backup's benefits of zero-infrastructure backup, long-term retention, and central management. SQL Databases are critical in application which needs to be taken backup for various reasons like server failures, corrupt DB or in case of restoration after failure of version upgrade.

Azure Backup uses a backup extension that will be installed on SQL server and extension consists of SQL plugin with a coordinator which does orchestration of streaming backup data to recovery service vault. To discover the SQL databases on server, Azure backup creates virtual service account **NT SERVICE\AzureWLBackupPluginSvc and it will require sysadmin access to databases**.

Features include:

* Workload aware backups that support all backup types - full, differential, and log
* 15-min RPO (recovery point objective) with frequent log backups
* Point-in-time recovery up to a second
* Individual database level backup and restore.

### SQL Databases Backup Policy

SQL Database backup policy will be created based on customer defined retention polices requirement and data changes in the environment.

* Create process document for SQL Databases backup and retention for each environment.

### Backup – Collect IaC Templates

|  |  |  |
| --- | --- | --- |
| **S. No** | **Product** | **Action Plan** |
| 1 | Express Route circuit |  |
| 2 | Firewall |  |
| 3 | Load balancer |  |
| 4 | Public Ips |  |
| 5 | Traffic Manager |  |
| 6 | Storage Accounts |  |
| 7 | Virtual Network Gateway |  |
| 8 | Application Gateway |  |

# Security & Compliance

## Policy Standards

Azure Policy is a service in Azure that you use to define, assign, and, manage standards for resources in your environment. It can prevent the creation of disallowed resources, ensure new resources have specific settings applied, and run evaluations of your existing resources to scan for non-compliance.

Planning out a consistent Azure cloud infrastructure starts by setting Azure Policy. It is an important **security** and compliance factor in Hexaware’s' service platform to maintain consistency in each customer environments. Based on requirement and best practices, Azure policies will be categorized and applied to customer environment.

Intact US to check the Azure Policy dashboard for non-compliance data periodically and apply remediation or add exemption.

* Review frequency – First week of every month

Security team to add their recommendations.

## Azure Policy Exceptions

Compliance with this Policy is required unless a formal policy exception is granted. Policy exception requests will be formally documented, reviewed, and approved or denied in accordance with the Risk Exception Procedure.

## Azure Policy Exemptions

The Azure Policy exemptions is used to *exempt* a resource hierarchy or an individual resource from evaluation of initiatives or definitions. Resources that are *exempt* count toward overall compliance but can't be evaluated or have a temporary waiver.

Below are the two-exemption category.

*Mitigated:* The exemption is granted because the policy intent is met through another method.

*Waiver:* The exemption is granted because the non-compliance state of the resource is temporarily accepted. Another reason to use this category is for a resource or resource hierarchy that should be excluded from one or more definitions in an initiative but shouldn't be excluded from the entire initiative.

## Azure Policy Effects

Below are the standard process for Azure Policy assignment based on policy effects.

*Please note, all remediation or changes should test and validate in non-production environment.*

**Audit effect - Audit** is used to create a warning event in the activity log when evaluating a non-compliant resource, but it doesn't stop the request. There is no direct risk in audit policy assignment. Create a single blueprint or policy initiative and apply to all subscription.   However, policy remediation changes should test and validate in non-production environment first.

**Deny effect -** Deny is used to prevent a resource request that doesn't match defined standards through a policy definitiCompliance with this Policy is required unless a formal policy exception is granted. Policy exception requests will be formally documented, reviewed, and approved or denied in accordance with the Risk Exception Procedure.on and fails the request.  Direct risk in applying deny policy.   To overcome this, create a separate policy initiative and use policy enforcement mode (enable or disable).  When enforcement mode is disabled, the policy effect isn't enforced (i.e., deny policy won't deny resources). Compliance assessment results are still available.  Review the compliance report, enforce, and test the policy impact in non-production environment first.

**Deploy effect -** It will deploy or enable the specific feature.  E.g., enable Advanced Threat Protection on Storage Accounts.  In most cases, deploy policy remediation will have additional cost as well.   Test the policy in non-production environment first.

**Disabled effect -** It will be useful to disable/stop single assignment instead of disabling all that policy's assignments.  Disable effect will stop the policy from evaluation.  It is useful to temporarily disable the specific policy for testing situations.

## Configuration Policies to be Applied

We are proposing below policies in Intact US Subscriptions and can be further reviewed.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **S. No** | **Policy** | **Action Plan** | **Policy Effect during implementation** | **Policy Effect after resource exclusion or  Remediation** | **Comments and exceptions** |
| 1 | Custom subscription owner roles should not exist | Implement the Policy | Audit | NA |  |
| 2 | RDP access from the Internet should be blocked | Implement the Policy | Audit | NA |  |
| 3 | SSH access from the Internet should be blocked | Implement the Policy | Audit | NA |  |
| 4 | Audit VMs that do not use managed disks | Implement the Policy | audit | NA |  |
| 5 | Storage account public access should be disallowed | Implement the Policy | audit | Deny | Proceed with Audit initially unless Security thinks we should deny. |
| 6 | Azure Cosmos DB allowed locations | Implement the Policy | audit | Deny | Proceed with Audit initially |
| 7 | Public network access on Azure SQL Database should be disabled | Implement the Policy | audit | NA |  |
| 8 | Certificates should have the specified maximum validity period | Implement the Policy | audit | Deny |  |
| 9 | Key vaults should have soft delete enabled | Implement the Policy | audit | Deny |  |
| 10 | Keys should have expiration dates set | Implement the Policy | audit | Deny |  |
| 11 | Secrets should have expiration dates set | Implement the Policy | audit | Deny |  |
| 12 | Secrets should have the specified maximum validity period | Implement the Policy | audit | Deny |  |
| 13 | Flow log should be configured for every network security group | Implement the Policy | Audit | NA | Proceed. NSG Flow logs is already enabled for 3-day retention. Follow Trustmark retention as like our other network service logs.  At minimal, greater than or equal to 90 day, configured for reliability and compliance purposes |
| 14 | Azure VPN gateways should not use 'basic' SKU | Implement the Policy | Audit | NA |  |
| 15 | Azure Cosmos DB accounts should have firewall rules | Implement the Policy | Audit | Deny and Enable Policy Enforcement | App team to review.  This will affect users working from home that go through Direct Access or VPN. If Cosmos DB can be configured with Private Endpoint then we will need that or a Jump server for those that need access.. |
| 16 | Network Watcher should be enabled | Implement the Policy | AuditIfNotExists | NA |  |
| 17 | SQL servers should be configured with 90 days auditing retention or higher. | Implement the Policy | AuditIfNotExists | NA |  |
| 18 | An activity log alert should exist for specific Policy operations | Implement the Policy | AuditIfNotExists | NA |  |
| 19 | An Azure Active Directory administrator should be provisioned for SQL servers | Implement the Policy | AuditIfNotExists | NA | Proceed. Need to determine who needs to have the access and apply group to admin. |
| 20 | Gateway subnets should not be configured with a network security group | Implement the Policy | Deny and Enable Policy Enforcement | NA | Proceed. We do not have NSG rules on Gateway Subnets. |
| 21 | Add or replace a tag on resources | Implement the policy for any new tags | Modify | NA |  |
|  |  |  |  |  |  |

## Configuration Policies with Resource Exclusions

* Collect resource exclusion list and get approval from Intact US leads.
* Create and apply below policies in audit mode or Deny mode (Disable enforcement).
* For existing policies, edit and update the parameters and enable the enforcement mode for deny action.
* For any cleanup activities, add resource exclusion into deny policy and enable enforcement and proceed with resource deletion.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S.No** | **Policy** | **Action Plan** | **Policy Effect during implementation** | **Policy Effect after resource exclusion or  Remediation** |
| 1 | Append a tag and its value from the resource group | Edit the existing Policy and add Resource exclusion | Append | NA |
| 2 | Append a tag and its value to resource groups | Edit the existing Policy and add Resource exclusion | Append | NA |
| 3 | Audit resource location matches resource group location | Implement the Policy and add Resource exclusion | Audit | NA |
| 4 | Web Application Firewall (WAF) should use the specified mode for Application Gateway | Implement the Policy and add Resource exclusion | Audit | Deny |
| 5 | Geo-redundant storage should be enabled for Storage Accounts | Implement the Policy and add Resource exclusions | Audit | NA |
| 6 | All Internet traffic should be routed via your deployed Azure Firewall | Implement the Policy and add Resource exclusion | AuditIfNotExists | NA |
| 7 | Allowed locations | Edit the existing Policy and add Resource exclusion | Deny and Disable Policy Enforcement | Deny and Enable Policy Enforcement |
| 8 | Allowed locations for resource groups | Edit the existing Policy and add Resource exclusion | Deny and Disable Policy Enforcement | Deny and Enable Policy Enforcement |
| 9 | Network interfaces should not have public Ips | Implement the Policy and add Resource exclusion | Deny and Disable Policy Enforcement | Deny and Enable Policy Enforcement |
|  |  |  |  |  |

## Configuration Policies Requires approval

* Collect the required details before  policy deployment like VM extension types, allowed SKU and get approval from Intact Us leads.
* Create and apply below policies in audit mode or Deny mode (Disable enforcement).
* For any cleanup activities, add resource exclusion into deny policy and enable enforcement and proceed with resource deletion.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **S. No** | **Policy** | **Action Plan** | **Policy Effect during implementation** | **Policy Effect after resource exclusion or  Remediation** | **Comments and exceptions** |
| 1 | Only approved VM extensions should be installed | Implement the policy after approval for VM extension types | Audit | Deny and Enable Policy Enforcement | Get the list of  VM extensions  in each region by using PowerShell query and get approval |
| 2 | Not allowed resource types | Implement the policy after approval for resource types | Deny and Disable Policy Enforcement | Deny and Enable Policy Enforcement | Find and add not allowed resources |
| 3 | Allowed virtual machine size SKUs | Implement the policy after approval for SKU Types | Deny and Disable Policy Enforcement | Deny and Enable Policy Enforcement | Get the approved SKU list before implementation |
| 4 | Allowed storage account SKUs | Implement the policy after approval for SKU Types | Deny and Disable Policy Enforcement | Deny and Enable Policy Enforcement | Get the approved SKU list before implementation |
| 5 | Deploy Advanced Threat Protection on Storage Accounts | Implement the Policy after approval for additional cost | DeployIfNotExists | NA |  |

# Building Blocks

## Naming Standards

An effective naming convention assembles resource names by using important resource information as parts of a resource's name. Naming convention should be in the way that from name, anyone can identify the resource's type, its associated workload, its deployment environment, and additionally Azure region hosting it.

* Define the naming standards for below missing resources and document it
* Create a ITSM process to define naming standards for future resources types and document it.

|  |  |
| --- | --- |
| **Resources Type** | **Action** |
| Bastion | Document the Naming standard for this resource type |
| ExpressRoute circuit |  |
| Firewall |  |
| Local network gateway |  |
| Log Analytics workspace |  |
| Recovery Services vault |  |
| Snapshot |  |
| Virtual network gateway |  |
| Application Gateway |  |
| Log Analytics workspace | Define and document the Naming standard for this resource type |
| Resources Type | Action |

## Tagging

Intact US to have basic tags like Business unit, environment in the IaC Terraform templates.

## Azure CAF for IaC

Azure CAF enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements. Azure Blueprints makes it possible for development teams to rapidly build and stand-up new environments with trust they're building within organizational compliance with a set of built-in components, such as networking, to speed up development and delivery.

Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:

* Role Assignments
* Policy Assignments
* Terraform IaC Templates
* Resource Groups

IaC Templates are documents that don’t exist natively within Azure – these templates are normally stored locally or in a central code repository such as Github or Gitlab. Once these templates are deployed, there is no connection between the template and the resources that have been deployed. This can lead to issues such as templates not being updated in a timely manner for any changes that are required for the resource (and future resources) or templates being updated without proper documentation as to what might have changed.

## Terraform Templates

Terraform Templates are a way to declare the objects you want, the types, names and properties in a tf file which can be checked into source control and managed like any other code file. Terraform Templates are what really gives us the ability to roll out Azure “Infrastructure as code”

Terrafrom Azure Resource Manager Template defines the resources you need to deploy for your solution.

## CCoE US Process

We have reviewed Intact US maintains Enterprise Design document and Virtual machine build checklist

We could see Intact US is following some process for Access and Resource management.  Therefore, we recommend to create and document them for below processes.

* Azure Access Management
* Account Credential Management
* Azure Custom Image Creation
* Hardening and Patch Management
* Backup management for Virtual machine, SQL PAAS Databases, Network configurations and any exclusions from backup
* High Availability and Disaster recovery
* Azure policy Management with implementation, changes, and exclusions.

# Azure Advisor

The Advisor is focusing on best practices and recommendations that work for most organizations.  Microsoft calls Azure Advisor as your personalized cloud consultant to help you optimize your Azure environment.

Intact US CCoE Governance team to review the Azure Advisor report on periodically and apply the recommendations or add exemption.

* + Review Frequency – First week of every month
  + Review the Azure Advisor Score report and try to achieve 100 Percent.
  + Create Advisor alerts for High and Medium impact Recommendations.
  + Create Exemptions for resources based on mitigation. Mitigation can be set with or without an expiration date.  Expiration date option will be useful for temporary exemptions.  Mitigation types as follows.
    - Mitigated (resolved through a third-party service)
    - Waiver (risk accepted)

The Advisor dashboard displays personalized recommendations for all your subscriptions. You can apply filters to display recommendations for specific subscriptions and resource types.

Azure recommendations are divided into five categories:

**Reliability** (formerly called High Availability): To ensure and improve the continuity of your business-critical applications. For more information, see Advisor Reliability recommendations.

**Security**: To detect threats and vulnerabilities that might lead to security breaches.

**Performance**: To improve the speed of your applications.

**Cost**: To optimize and reduce your overall Azure spending.

**Operational Excellence**: To help you achieve process and workflow efficiency, resource manageability and deployment best practices.

# Appendix

|  |  |  |
| --- | --- | --- |
| Documents | Description | Link/Path |
|  |  |  |
|  |  |  |