**Gassco Azure Landing Zone   
High Level document**

**Prepared by –**

**Contributors –**

**Document Information**

|  |  |  |  |
| --- | --- | --- | --- |
| **Project Name** |  | **Version No** | **1.0** |
| **Date** |  |
| **Project Owner:** |  | **Telephone No:** |  |
| **Executive Sponsor** |  | **Telephone No:** |  |
| **Program Manager** |  | **Telephone No:** |  |
| **Target Implementation date** |  |  |  |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Revision Date** | **Summary of Changes** | **Changes marked** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Document Contributors**

|  |  |  |  |
| --- | --- | --- | --- |
| **Cloud Solution Architect** |  | Contact Info: |  |
| **Platform Architect** |  | Contact Info: |  |
| **Security Architect** |  | Contact Info: |  |
| **Identity Architect** |  | Contact Info: |  |
| **Network Architect** |  | Contact Info: |  |

**Solution Quality Check**

**Document Reviewers**

|  |  |  |  |
| --- | --- | --- | --- |
| **Role / Title** | **Name** | **Date** | **Comments / Attachments** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Document Approvers**

|  |  |  |  |
| --- | --- | --- | --- |
| **Role / Title** | **Name** | **Date** | **Comments / Attachments** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**CONTENTS**

[1 GLOSSARY OF TERMS 7](#_Toc41584746)

[2 EXECUTIVE SUMMARY 7](#_Toc41584747)

[3 SCOPE 7](#_Toc41584748)

[4 AUDIENCE & STAKEHOLDERS 8](#_Toc41584749)

[5 AZURE GOVERNANCE 8](#_Toc41584750)

[5.1 ENTERPRISE ENROLLMENTS, DEPARTMENTS & ACCOUNTS 9](#_Toc41584751)

[5.1.1 TRANSFER BILLING OWNERSHIP OF AN AZURE SUBSCRITION 10](#_Toc41584752)

[5.2 MANAGEMENT GROUPS 11](#_Toc41584753)

[5.3 SUBSCRIPTIONS 12](#_Toc41584754)

[5.4 RESOURCE GROUPS 12](#_Toc41584755)

[5.5 NAMING CONVENTIONS 12](#_Toc41584756)

[5.6 RESOURCE TAGS 13](#_Toc41584757)

[5.7 RESOURCE LOCKS 14](#_Toc41584758)

[5.8 AZURE POLICIES 15](#_Toc41584759)

[5.9 ROLE-BASED ACCESS CONTROLS (RBAC) 15](#_Toc41584760)

[5.10 COST MANAGEMENT 16](#_Toc41584761)

[5.10.1 COST ANALYSIS 17](#_Toc41584762)

[5.10.2 BUDGETS 17](#_Toc41584763)

[5.10.3 AZURE ADVISOR 18](#_Toc41584764)

[5.10.4 HYBRID BENEFIT 18](#_Toc41584765)

[5.10.5 RESERVED INSTANCES & AZURE DISK RESERVATION DISCOUNTS 18](#_Toc41584766)

[5.10.6 DEV/TEST SUBSCRIPTIONS 19](#_Toc41584767)

[6 NETWORK 19](#_Toc41584768)

[6.1 AZURE REGIONS & LOCATIONS 19](#_Toc41584769)

[6.2 HUB & SPOKE TOPOLOGY 19](#_Toc41584770)

[6.2.1 VNET PEERING 20](#_Toc41584771)

[6.3 EXPRESS ROUTE 23](#_Toc41584772)

[6.3.1 AZURE PRIVATE PEERING 24](#_Toc41584773)

[6.3.2 MICROSOFT PEERING 24](#_Toc41584774)

[6.4 SITE TO SITE VPN 24](#_Toc41584775)

[6.5 AZURE BASTION 24](#_Toc41584776)

[6.6 AZURE VNET & SUBNETS 26](#_Toc41584777)

[6.7 IP ADRESS MANAGEMENT 26](#_Toc41584778)

[6.8 ROUTING 26](#_Toc41584779)

[6.9 LOAD BALANCERS 27](#_Toc41584780)

[6.9.1 EXTERNAL & INTERNAL LOAD BALANCERS 27](#_Toc41584781)

[6.9.2 APPLICATION GATEWAY 27](#_Toc41584782)

[6.9.3 TRAFFIC MANAGER 28](#_Toc41584783)

[7 SECURITY 28](#_Toc41584784)

[7.1 KEY DESIGN COSIDERATIONS – NETWORK SECURITY 29](#_Toc41584785)

[7.2 SECURED SUBSCRIPTIONS 29](#_Toc41584786)

[7.3 OUTBOUND TRAFFIC SECURITY (“xxxxx”) 30](#_Toc41584787)

[7.4 INBOUND TRAFFIC SECURITY (“xxxxx”) 30](#_Toc41584788)

[7.5 NETWORK SECURITY GROUPS 31](#_Toc41584789)

[7.6 KEY DESIGN CONSIDERATIONS – DATA SECURITY 32](#_Toc41584790)

[7.7 CLOUD ACCESS SECURITY BROKER 33](#_Toc41584791)

[7.8 KEY DESIGN CONSIDERATIONS – VM SECURITY 34](#_Toc41584792)

[7.9 AZURE SECURITY CENTER 34](#_Toc41584793)

[7.10 SIEM integration 34](#_Toc41584794)

[8 COMPUTE & STORAGE 36](#_Toc41584795)

[8.1 VIRTUAL MACHINES 36](#_Toc41584796)

[8.1.1 AVAILABILITY ZONES/SETS 36](#_Toc41584797)

[8.1.2 CUSTOM (GOLD) IMAGES 37](#_Toc41584798)

[8.1.3 OS HARDENING STANDARDS 37](#_Toc41584799)

[8.1.4 VM AUTOMATION 37](#_Toc41584800)

[8.2 STORAGE 38](#_Toc41584801)

[8.2.1 STORAGE ACCOUNTS 38](#_Toc41584802)

[8.2.2 DISK STORAGE 38](#_Toc41584803)

[8.2.3 DISK TYPES 39](#_Toc41584804)

[8.2.4 FILE STORAGE 39](#_Toc41584805)

[8.2.5 AZURE FILES AUTHENTICATION 41](#_Toc41584806)

[8.2.6 ENCRYPTION 41](#_Toc41584807)

[8.3 KEY DESIGN CONSIDERATIONS 41](#_Toc41584808)

[9 AZURE ACTIVE DIRECTORY 42](#_Toc41584809)

[9.1 ON-PREMISES WINDOWS SERVERS AD ACCOUNTS INTEGRATION WITH AZURE AD 43](#_Toc41584810)

[9.1.1 HYBRID IDENTITY 43](#_Toc41584811)

[9.1.2 DIRECTORY & PASSWORD SYNCRONIZATION 44](#_Toc41584812)

[9.1.3 FEDERATION 45](#_Toc41584813)

[9.2 ACTIVE DIRECTORY DOMAIN SERVICES FOR AZURE 46](#_Toc41584814)

[9.2.1 AZURE AD DOMAIN SERVICES 46](#_Toc41584815)

[9.2.2 EXTENDING WINDOWS SERVER AD TO AZURE VM 47](#_Toc41584816)

[9.3 KEY DESIGN CONSIDERATIONS 49](#_Toc41584817)

[10 BACKUP & DR 49](#_Toc41584818)

[10.1 RECOVERY SERVICES VAULT 50](#_Toc41584819)

[10.2 AZURE IaaS VM BACKUP 50](#_Toc41584820)

[10.2.1 SNAPSHOT CONSISTENCY 51](#_Toc41584821)

[10.3 FILES & FOLDERS BACKUP 51](#_Toc41584822)

[10.3.1 BACKUP TYPES 52](#_Toc41584823)

[10.4 AZURE SQL BACKUP 52](#_Toc41584824)

[10.5 EMC AVAMAR 54](#_Toc41584825)

[10.6 KEY DESIGN CONSIDERATIONS 54](#_Toc41584826)

[10.7 AZURE SITE RECOVERY 55](#_Toc41584827)

[11 MONITORING 56](#_Toc41584828)

[11.1 AZURE MONITOR 56](#_Toc41584829)

[11.2 SCOM (WINDOWS/SQL MONITORING) 57](#_Toc41584830)

[11.3 OEM(LINUX/ORACLE MONITORING) 58](#_Toc41584831)

[12 ATTACHMENT CHECK LIST 58](#_Toc41584832)

[13 REFERENCES 58](#_Toc41584833)

# GLOSSARY OF TERMS

|  |  |
| --- | --- |
| **Term** | **Description** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# EXECUTIVE SUMMARY

his Azure Foundation Design describes the cloud platform for Gassco [West Europe] and is based on Azure Infrastructure-as-a-Service (IaaS) & Platform-as-a-Service(PaaS).

The primary purpose of this Foundation Design document is to provide foundation for a scalable, resilient architecture for consuming Azure services for GASSCO . The main goal is to utilize Azure to prepare for new technical capabilities, scale to meet geographic or market demands, modernize Application, decoupling complex application, modernize identity & security posture and controls, if needed facilitate datacenter exit future by migrating on-premise workloads to Azure. The implementation of Azure will to optimize internal operations and increase business agility.

This document is a high-level design and best-practices guide for deploying the workloads on Microsoft Azure cloud infrastructure. It describes Microsoft Azure capabilities and deployment architecture recommendations with respect to GASSCO Standards.

# SCOPE

The scope of the document is to define how Azure IaaS features and capabilities will be utilized at “xxxxx”and include

* Azure Regions & Subscriptions
* Resource Hierarchy
* Governance
* Naming & Tagging standards
* Network Design
* Security Design
* Compute & Storage
* Backup
* Operations Management –
* Monitoring
* Security Patching & Configuration Management

The scope is limited to Azure native capabilities and will not extend to third-party applications. PaaS, DevOps & Automation are out of scope in the initial design of the foundation. The proposed design does not put any restriction through Azure Policies that would limit application team(s) ability to deploy PaaS features.

# AUDIENCE & STAKEHOLDERS

This document has been prepared for

* Strategic Leadership
* Architecture Team
* Technical SME's

Following are the key stakeholders.

|  |  |  |
| --- | --- | --- |
| **Name** | **Role** | **Email** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# AZURE GOVERNANCE

The concept of an enterprise scaffold allows to balance the need of governance with the need of agility.

An enterprise scaffold for Azure is a set of flexible controls and Azure capabilities that provide structure to the environment, and anchors for services built on the public cloud. The enterprise scaffold is "purpose-built" to be flexible to support both traditional IT workloads and agile workloads. The enterprise scaffold is intended to be the foundation of each new subscription within Azure. It enables administrators to ensure workloads meet the minimum governance requirements of an organization without preventing business groups and developers from quickly meeting their own goals.

This section provides design for each of the azure capabilities and features that make up the azure scaffold.

A screen shot of a computer

Description automatically generated

## ENTERPRISE ENROLLMENTS, DEPARTMENTS & ACCOUNTS

The Azure Hierarchy is the relationship of the Azure Enterprise Enrollment through to subscriptions and resource groups. The enterprise enrollment defines the shape and use of Azure services from a contractual point of view.

Within the Enterprise Agreement, you can further subdivide into departments, accounts, subscriptions, and resource groups to match the organization structure.

A diagram of a account

Description automatically generated

The hierarchy in the above image allows for significant flexibility in how Azure is organized. Hierarchy should reflect billing, resource management, and resource access.

There are three common patterns for Azure Enrollments - Functional, Business Unit and Geographic as depicted in the below image.

A diagram of a company

Description automatically generatedA diagram of a business division

Description automatically generatedA diagram of a company

Description automatically generated

“XXXXX” recommends adoption of business unit pattern for its flexibility in modeling an organization's cost model as well as reflecting span of control and achieves the strategic goals of “xxxxx”.

The following image depicts the proposed hierarchy.

<Diagram>

### **TRANSFER BILLING OWNERSHIP OF AN AZURE SUBSCRITION**

Microsoft allows transfer of Azure subscription's billing ownership to another account. Transferring billing ownership to another account provides the administrators in the new account permission to perform billing tasks such as change payment method, view charges, and cancel the subscription.

Enterprise administrators can transfer billing ownership of subscriptions between accounts within an enrollment. However, self-service subscription transfer through Azure portal is not supported and will need to Microsoft support

Following are some of the key points to consider -

* All resources in a subscription like Resource Groups, VM, Disks, etc. transfer to the new account. However, if you transfer subscription to an account in another Azure AD tenant, any administrator roles and Role-based Access Control (RBAC) assignments on the subscription do not transfer. Also, app registrations and other tenant-specific services don't transfer along with the subscription.
* Usage and billing history do not transfer with the subscription.
* Resources (those supported by azure) can also be moved to new resource groups or subscription.

## MANAGEMENT GROUPS

Management groups allow us to create a hierarchy that is separate from your billing hierarchy, solely for efficient management of resources and are much more flexible than departments and accounts. Azure management groups provide a level of scope above subscriptions. We can organize subscriptions into containers called "management groups" and apply your governance conditions to the management groups. All subscriptions within a management group automatically inherit the conditions applied to the management group. Management groups give you enterprise-grade management at a large scale. All subscriptions within a single management group must trust the same Azure Active Directory tenant.

Each directory is given a single top-level management group called the "Root" management group. This root management group is built into the hierarchy to have all management groups and subscriptions fold up to it. Anything assigned on the root will apply across all management groups, subscriptions, resource groups, and resources within the directory by having one hierarchy within the directory.

Key points to consider

* A management group tree can support up to six levels of depth (excluding Root)
* Each management group and subscription can only support one parent.
* Each management group can have many children.

A root management group will be created, and 3 child MG will be created for Prod, Non-Prod and Hub respectively.

A diagram of a group

Description automatically generated

## SUBSCRIPTIONS

A subscription refers to the logical entity that provides entitlement to deploy and consume Azure resources. Following are the three common patterns for creating subscriptions.

**Application/service:** Subscriptions represent an application or a service (portfolio of applications)

**Lifecycle:** Subscriptions represent a lifecycle of a service, such as Production or Development.

**Department:** Subscriptions represent departments in the organization.

“XXXXX” recommends using the lifecycle pattern and creating subscriptions for hub (network), inf (security, active directory, monitoring), production, non-production and dev/test (if required). We also suggest creating dedicated subscriptions for specific applications and then use resource groups to separate the environments further.

4 Subscriptions are to be created for <X Company>.

## RESOURCE GROUPS

The concept of Resource Group was introduced in Azure Resource Manager. It is a container that holds related resources for an Azure solution and should include only those resources that you want to manage as a group

Following are key factors to consider while defining resource groups -

* Resource Group is the main components used to perform charge back using tags. All the resources located in RG are charge back to the same line of business. All Tags are applied at RG levels are inherited by the below resources.
* All the resources in the resource group should share the same lifecycle and should be deployed, updated, and deleted together.

## NAMING CONVENTIONS

Applying a well-defined naming and metadata tagging conventions to cloud-hosted resources helps IT staff to quickly find and manage resources. Well-defined names and tags also help to align cloud usage costs with business teams by using chargeback and show back accounting mechanisms.

A naming and tagging strategy include business and operational details as components of resource names and metadata tags:

* The business side of this strategy ensures that resource names and tags include the organizational information that's needed to identify the teams.
* The operational side ensures that names and tags include information that IT teams use to identify the workload, application, environment, criticality, and other information useful for managing resources.

Following template has Microsoft Cloud Adoption Framework recommendations which needs to be further updated and aligned with “xxxxx” business needs.



## RESOURCE TAGS

Resource Tags are metadata which are applied to Azure resources and provide additional information about the resource and associated application and line of business. Azure provides the ability to assign up to fifteen tags to each resource, each tag can contain up to 512 case sensitive characters.

Each tag consists of a name and a value pair and will be used for

* Chargeback billing process, it uses the Business Service Id and Business Service Name tags
* Define the environment
* Define who manages the workload.
* Define the type of platform and data classification

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tag Name** | **Description** | **Key** | **Example Value** | **Required?** |
| Application Name | Name of the application, service, or workload the resource is associated with. | *ApplicationName* | *{app name}* | *Yes* |
| Approver Name | Person responsible for approving costs related to this resource. | *Approver* | *{email}* | *Yes* |
| Budget required/approved | Money allocated for this application, service or workload. | *BudgetAmount* | *{$}* | *No* |
| Business Unit | Top-level division of your company that owns the subscription or workload the resource belongs to. In smaller organizations, this may represent a single corporate or shared top-level organizational element. | *BusinessUnit* | *FINANCE, MARKETING,{Product Name},CORP,SHARED* | *Yes* |
| Cost Center | Accounting cost center associated with this resource. | *CostCenter* | *{number}* | *Yes* |
| Disaster Recovery | Business criticality of this application, workload, or service. | *DR* | *Mission Critical, Critical, Essential* | *Yes* |
| End Date of the Project | Date when this application, workload, or service is planned to be retired. | *EndDate* | *{date}* | *No* |
| Environment | Deployment environment of this application, workload, or service. | *Env* | *Prod, Dev, QA, Stage, Test* | *Yes* |
| Owner Name | Owner of the application, workload, or service. | *Owner* | *{email}* | *Yes* |
| Requester Name | User that requested the creation of this application. | *Requestor* | *{email}* | *No* |
| Service Class | Service Level Agreement level of this application, workload, or service. | *ServiceClass* | *Dev, Bronze, Silver, Gold* | *Yes* |
| Start Date of the project | Date when this application, workload, or service was first deployed. | *StartDate* | *{date}* | *No* |
| Service Now Request No # | SNOW Change or Service Request # created for the request | *Change Number* | *CHGxxxxx* | *Yes* |

## RESOURCE LOCKS

Resource Locks provide a way for administrators to lock down Azure resources to prevent deletion or changing of a resource. These locks sit outside of the Role Based Access Controls (RBAC) hierarchy and when applied will place the restriction on the resource for all users.

**CanNotDelete** means authorized users can still read and modify a resource, but they can't delete the resource.

**ReadOnly** means authorized users can read a resource, but they can't delete or update the resource. Applying this lock is like restricting all authorized users to the permissions granted by the Reader role.

By default, resource locks can be applied by only users belonging to **Owner and User Access Administrator built-in RBAC Roles**

Resource locks can be applied to subscriptions, resource groups or individual resources as required. When you lock Subscription, all resources in that subscription (including ones added later) inherit the same lock. Once applied, these locks impact all users regardless of their roles, if it becomes necessary to delete or change a resource with a lock in place then the lock will need to be removed before this can occur.

## AZURE POLICIES

Azure Policy is a compliance management service in Azure that is used to create, assign and, manage policies. These policies enforce different rules and effects over your resources, so those resources stay compliant with your corporate standards and service level agreements.

While RBAC focuses on user action on the resources, Azure policies help to control resource properties of both existing resources and new deployments.

Besides **Owner and Contributor built in roles**, The **Resource Policy Contributor role** includes the most policy operations.

Following is a brief synopsis of the different terms used in Azure policy -

* Policy definitions describe resource compliance and the remediation measures to take when a resource in non-compliant. Azure has 100+ built-in policies that are available and it also supports creation of custom policies if needed.
* Policy parameters are values which are defined during a policy creation.
* Policy assignment defines the scope of the policy definitions. The scope could be management groups, subscriptions or resource groups to which the policy definitions are assigned. Policy assignments are inherited by the child resources, but it allows to exclude a sub scope.
* Initiative is a collection of policy definition which are tailored towards a single goal.

“XXXXX” to recommend must have policies that should be implemented in the landing zone across the various IaaS components. “xxxxx”to adopt CIS benchmarks for Azure which include policy recommendations.

## ROLE-BASED ACCESS CONTROLS (RBAC)

Role-based access control (RBAC) is an authorization system built on Azure Resource Manager that provides fine-grained access management of Azure resources. It's a best practice to follow the principle of least privilege while granting access to users.

The following diagram shows a suggested pattern for using RBAC.

A screenshot of a diagram

Description automatically generated

Access is controlled using role assignments. A role assignment consists of three elements: **security principal, role definition, and scope.**

A security principal is an object that represents a user, group, service principal, or managed identity that is requesting access to Azure resources.

A role definition is a collection of permissions. It's typically just called a role. A role definition lists the operations that can be performed, such as read, write, and delete.

Azure includes several built-in roles that you can use. The following three built-in roles apply to all resources.

* Owner - Has full access to all resources including the right to delegate access to others.
* Contributor - Can create and manage all types of Azure resources but can’t grant access to others.
* Reader - Can view existing Azure resources.

There are 72+ built-in which allow management of specific Azure resources. For example, the Virtual Machine Contributor role allows a user to create and manage virtual machines.

If a built-in role doesn’t meet the specific needs, we can create custom roles for Azure resources. However, this is not a best practice

## COST MANAGEMENT

Cost Management requires participation of finance, accounts and business stakeholders. This section outlines the cost management capabilities of Azure and needs to be fine-tuned based on “xxxxx”requirements.

Azure Cost Management is an azure native solution to analyze costs, create and manage budgets, export data, and review and act on optimization recommendations to save money.

### **COST ANALYSIS**

Cost analysis help to explore and analyze organizational costs. You can view aggregated costs by organization to understand where costs occur over time and identify spending trends. You can view accumulated costs over time to estimate monthly, quarterly, or even yearly cost trends against a budget.

You must have at least read access to one or more of the following scopes to view cost data.

* Billing account
* Department
* Enrollment account
* Management group
* Subscription
* Resource group

Initial cost analysis view includes Total costs, Budgeted costs (if available), Accumulated cost and Pivot charts. Customization of cost views is supported.

Grouping (Group by) lets you quickly see how your spending is categorized by common resource and usage properties, like resource group or resource tags. To group by tags, select the tag key you want to group by. You'll see costs broken down by each value for that tag, with an extra segment for resources that don't have that tag applied.

Cost Management only supports resource tags from the date the tags are applied directly to the resource.

You can Download information from cost analysis to generate a CSV file for all data currently shown in the Azure portal. Any filters or grouping that you apply are included in the file.

### **BUDGETS**

Budgets help you plan for and drive organizational accountability. With budgets, you can account for the Azure services you consume or subscribe to during a specific period - Monthly, Quarterly or Yearly.

Alerts can be configured to warn about impending budget overages. When the budget thresholds are exceeded, only notifications are triggered, resources are not affected, and consumption isn't stopped. You can use budgets to compare and track spending as you analyze costs.

Budgets reset automatically at the end of a period (monthly, quarterly, or annually) for the same budget amount when you select an expiration date in the future.

The following Azure permissions are supported per subscription for budgets by user and group:

**Owner** – Can create, modify, or delete budgets for a subscription.

**Contributor and Cost Management contributor** – Can create, modify, or delete their own budgets. Can modify the budget amount for budgets created by others.

**Reader and Cost Management reader** – Can view budgets that they have permission to.

### **AZURE ADVISOR**

Azure Cost Management works with Azure Advisor to provide cost optimization recommendations. Azure Advisor helps you optimize and improve efficiency by identifying idle and underutilized resources.

Azure Advisor monitors your virtual machine usage for 14 days and then identifies underutilized virtual machines. Virtual machines whose CPU utilization is five percent or less and network usage is seven MB or less for four or more days are considered low-utilization virtual machines. (The 5% or less CPU utilization setting is the default, but you can adjust the settings)

The list of recommendations identifies usage inefficiencies or shows purchase recommendations that can help you save additional money. The totaled potential yearly savings shows the total amount that you can save if you shut down or deallocate all your VMs that meet recommendation rules. If you don't want to shut them down, you should consider resizing them to a less expensive VM SKU.

The Impact category, along with the Potential yearly savings, are designed to help identify recommendations that have the potential to save as much as possible. The high impact recommendations are Buy reserved virtual machine instances to save money over pay-as-you-go costs and Optimize virtual machine spend by resizing or shutting down underutilized instances. Medium impact recommendations are Reduce costs by eliminating un-provisioned ExpressRoute circuits and Reduce costs by deleting or reconfiguring idle virtual network gateways.

Besides Cost, Azure Advisor provides recommendation on following categories which will be covered in later sections of this document.

* High Availability: To ensure and improve the continuity of your business-critical applications.
* Security: To detect threats and vulnerabilities that might lead to security breaches.
* Performance: To improve the speed of your applications.

While, budgets, cost analysis and advisor are tools for cost management, “XXXXX” recommends Reserved VM instances and Hybrid Benefit which potentially save up to 80% costs when compared to pay-as-you-go.

### **HYBRID BENEFIT**

As per Azure pricing documentation, The Azure Hybrid Benefit helps you get more value from your Windows Server licenses and save up to 40 percent\* on virtual machines. You can use the benefit with Windows Server Datacentre and Standard edition licences covered with Software Assurance or Windows Server Subscriptions. Depending on the edition, you can convert or re-use your licences to run Windows Server virtual machines in Azure and pay a lower base compute rate (Linux virtual machine rates).

### **RESERVED INSTANCES & AZURE DISK RESERVATION DISCOUNTS**

Azure Reservations helps you save money by pre-paying for one-year or three-years of virtual machine, SQL Database compute capacity, Azure Cosmos DB throughput, or other Azure resources. Pre-paying allows you to get a discount on the resources you use. Reservations can significantly reduce your virtual machine, SQL database compute, Azure Cosmos DB, or other resource costs up to 72% on pay-as-you-go prices. Reservations provide a billing discount and don't affect the runtime state of your resources.

Combined with Reserved Virtual Machine Instances you can decrease your total VM costs. The reservation discount is applied automatically to the matching disks in the selected reservation scope, you don't need to assign a reservation to a Managed disk to get the discounts. Discounts are applied hourly on the disk usage and any unused reserved capacity does not carry over.

### **DEV/TEST SUBSCRIPTIONS**

Enterprise Dev/Test subscriptions are available for EA customers and offer special lower Dev/Test rates on Windows Virtual Machines, Cloud Services, SQL Database, HDInsight, App Service and Logic Apps.

Enterprise Dev/Test is exclusively for development and testing your applications. Usage within the subscription does not carry a financially backed SLA.

“XXXXX” recommends use of Dev/Test subscriptions for sandbox environments.

# NETWORK

The networking services in Azure provide a variety of networking capabilities for connectivity, application protection, application delivery and network monitoring. In this section, we will elaborate on the network design for “xxxxx”.

## AZURE REGIONS & LOCATIONS

An Azure region is an area within a geography, containing one or more datacenters. Each Azure region is paired with another region within the same geography, together making a regional pair (except for Brazil South which is paired with US South Central). It is recommended to configure business continuity disaster recovery (BCDR) across regional pairs to benefit from Azure’s isolation and availability policies. For applications which support multiple active regions, using both regions in a region pair where possible is ideal to ensure optimal availability for applications and minimized recovery time in the event of a disaster.

Following are the proposed regions for “xxxxx”.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **“xxxxx”Data Center /Branch Offices** | **Peering Location Express Route Only)** | **Azure Region** | **Azure Location** | **Paired Region** |
|  |  |  |  |  |
|  |  |  |  |  |

## HUB & SPOKE TOPOLOGY

This reference architecture shows how to extend Active Directory services from your on-premises datacenter to Azure, and how to add a network virtual appliance (NVA/ Azure Firewall) that can act as a firewall.

A diagram of a computer network

Description automatically generated

A Hub is defined as a network and security shared service architecture deployment model which achieves “xxxxx”'s security and compliance requirements, principles of least privilege and separation of duties, while enabling architecture principles of cost-effectiveness and elasticity. It enhances performance across diverse geographic service boundaries and ensures network isolation, segmentation and inspection across north-south and east-west traffic flows.

The Hub is the primary integration point for datacenter connectivity in a region and is the central hosting location for network and security services, domain and federation services, remote access solutions, internet proxy services, secure file transfer, web service exposure, external load balancing and centralized operations, log management and reporting.

A Spoke is an autonomous or an application-centric subscription which provides for a granular isolation between functional service tiers and drives the accountability of consumed cloud resources to a “xxxxx” business IT application owner. It can be considered an "enforcement" point of granular application and data access management control.

The Spoke can be a complete datacenter hosting Environment or an application-centric Subscription. A Spoke could also represent an opportunity to overcome subscription limitations such as enabling greater flexibility to achieve business changes across IT such as DevOps or Infrastructure-as-Code

### **VNET PEERING**

Virtual network peering enables to seamlessly connect networks in Azure Virtual Network which appear as one for connectivity purposes. The traffic between virtual machines is routed through Microsoft's private network only.

Azure supports the following types of peering:

* Virtual network peering: Connect virtual networks within the same Azure region.
* 1 VNET will be created in each subscription – hub, inf, prd and npe, as both the datacenters (OnPrem DCs) and branch offices are located within the same geographic region.
* VNET in inf, prd, and npe subscriptions will be peered with hub subscription VNET

* Global virtual network peering: Connecting virtual networks across Azure regions.

Following diagram depicts the proposed design for “xxxxx”

<DIAGRAM>

* Azure East US and West US region have been selected as the Primary and DR regions respectively.
* Wilson DC will use an ExpressRoute Circuit to connect to East US and West US region
* Stamford DC will use an S2S VPN to connect to East US and West US region

## EXPRESS ROUTE

ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a Layer 3 private connection facilitated by a connectivity provider. With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure and Office 365. ExpressRoute connections do not go over the public Internet and offer more reliability, faster speeds, consistent latencies, and higher security than typical connections over the Internet. ExpessRoute circuits support bandwidth of 10 Gbps.

Connectivity can be from an any-to-any (IP VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a co-location facility.

The following figure shows a logical representation of connectivity between your WAN and Microsoft.

A diagram of a computer network

Description automatically generated

Following are the key benefits of Express Route Circuits

* Connectivity to Microsoft cloud services across all regions in the geopolitical region.
* Global connectivity to Microsoft services across all regions with the ExpressRoute premium add-on.
* Dynamic routing between your network and Microsoft via BGP.
* Built-in redundancy in every peering location for higher reliability.
* Connection uptime SLA.
* QoS support for Skype for Business.

### **AZURE PRIVATE PEERING**

Azure VM's (IaaS) that are deployed within a virtual network can be connected through the private peering domain. The private peering domain is a trusted extension of organizations core network into Microsoft Azure. We can set up bi-directional connectivity between the core network and Azure virtual networks (VNets). This peering allows to connect to VM's and cloud services directly on their private IP addresses.

### **MICROSOFT PEERING**

Connectivity to Microsoft online services like Office 365 and Azure PaaS services occurs through Microsoft peering. Microsoft enable bi-directional connectivity between your WAN and Microsoft cloud services through the Microsoft peering routing domain.

## SITE TO SITE VPN

A Site-to-Site VPN gateway connection is used to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. This type of connection requires a VPN device located on-premises that has an externally facing public IP address assigned to it.

A close-up of a tube

Description automatically generated

A VPN gateway is a specific type of virtual network gateway that is used to send encrypted traffic between an Azure virtual network and an on-premises location over the public Internet. You can also use a VPN gateway to send encrypted traffic between Azure virtual networks over the Microsoft network. Each virtual network can have only one VPN gateway. However, you can create multiple connections to the same VPN gateway (a maximum of 30).

VPN gateways should be deployed in Azure Availability Zones. This brings resiliency, scalability, and higher availability to virtual network gateways and protects on-premises network connectivity to Azure from zone-level failures.

A virtual network can have two virtual network gateways; one VPN gateway and one ExpressRoute gateway

## AZURE BASTION

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

Following are the key features of Azure Bastion

* RDP and SSH directly in Azure portal
* Remote Session over SSL and firewall traversal for RDP/SSH
* No Public IP required on the Azure VM
* No hassle of managing NSGs
* Protection against port scanning
* Protect against zero-day exploits. Hardening in one place only

A diagram of a network

Description automatically generated

The above figure shows the architecture of an Azure Bastion deployment. In this diagram:

* The Bastion host is deployed in the virtual network.
* The user connects to the Azure portal using any HTML5 browser.
* The user selects the virtual machine to connect to.
* With a single click, the RDP/SSH session opens in the browser.
* No public IP is required on the Azure VM.

Azure Bastion deployment is per virtual network, not per subscription/account or virtual machine. Once you provision an Azure Bastion service in your virtual network, the RDP/SSH experience is available to all your VMs in the same virtual network.

A jumpbox VM will be deployed in Management Subnet to support SQL Management Studio and other features not supported by Azure Bastion.

## AZURE VNET & SUBNETS

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.

VNET's and Subnets for “xxxxx”were designed based on the following best practices

* Ensure non-overlapping address spaces. Make sure VNet address space (CIDR block) does not overlap with your organization's other network ranges.
* Subnets should not cover the entire address space of the VNet. Plan and reserve some address space for the future.
* It is recommended to have fewer large VNets than multiple small VNets. This will prevent management overhead.
* Securing VNet using Network Security Groups (NSGs).

## IP ADRESS MANAGEMENT

## ROUTING

Azure automatically creates system routes and assigns the routes to each subnet in a virtual network. System routes can't be created or removed but some system routes can be overridden with custom (user-defined) routes. Azure creates default system routes for each subnet. Each default route contains an address prefix and next hop type. When traffic leaving a subnet is sent to an IP address within the address prefix of a route, the route that contains the prefix is the route Azure uses.

Azure adds additional optional default routes to specific subnets, or every subnet, when you use specific Azure capabilities like VNET peering, Virtual Network Gateway and VirtualNetworkServiceEndpoint.

Custom routes can be created by explicitly creating user-defined routes or by exchanging border gateway protocol (BGP) routes between your on-premises network gateway and an Azure virtual network gateway. Virtual appliance (Firewall), Virtual network gateway, Virtual network and Internet can be configured as next hops

If multiple routes contain the same address prefix, Azure selects the route type, based on the following priority:

1. User-defined route
2. BGP route
3. System route

Note:

System routes for traffic related to virtual network, virtual network peerings, or virtual network service endpoints, are preferred routes, even if BGP routes are more specific.

## LOAD BALANCERS

Azure Load Balancer operates at layer four of the OSI model. It's the single point of contact for clients. Load Balancer distributes inbound flows that arrive at the load balancer's front end to backend pool instances. These flows are according to configured load balancing rules and health probes. The backend pool instances can be Azure Virtual Machines or instances in a virtual machine scale set.

### **EXTERNAL & INTERNAL LOAD BALANCERS**

A diagram of a computer network

Description automatically generated

A public (external) load balancer can provide outbound connections for virtual machines (VMs) inside VNET. These connections are accomplished by translating their private IP addresses to public IP addresses. Public Load Balancers are used to load balance internet traffic to VMs.

A private (internal) load balancer is used where private IPs are needed at the frontend only. Internal load balancers are used to load balance traffic inside a virtual network. A load balancer frontend can be accessed from an on-premises network in a hybrid scenario.

### **APPLICATION GATEWAY**

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications. Application Gateway works at Layer 7 of OSI model and can make routing decisions based on additional attributes of an HTTP request, such as URI path or host headers.

A diagram of a computer network

Description automatically generated

Besides application layer load balancing, application gateway offers

* Secure Sockets Layer (SSL/TLS) termination
* Sizing & Autoscaling
* Zone redundancy
* Static VIP
* Web application firewall
* Ingress Controller for AKS
* URL-based routing
* Multiple-site hosting
* Redirection
* Session affinity
* Websocket and HTTP/2 traffic
* Connection draining
* Custom error pages
* Rewrite HTTP headers

### **TRAFFIC MANAGER**

Azure Traffic Manager is a DNS-based traffic load balancer that enables you 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.

# SECURITY

## KEY DESIGN COSIDERATIONS – NETWORK SECURITY

* Traffic between on premise and cloud needs to be encrypted. For site to site VPN’s, IPSEC will be used to encrypt traffic.
* ExpressRoute is used to connect the primary datacenter to cloud. Microsoft peering needs to be established so that all traffic between on premise and IaaS, PaaS and SaaS instances are confined to Microsoft backbone. A site to site IPSEC VPN can be established over Microsoft peering for encryption of traffic.
* Azure subscriptions are designed such that a whitelisted set of services can be consumed by application teams. Over a period, new services can be incorporated within the shared application subscription based on security profile of the shared service. For any service consumed within the shared subscription, the service needs to limit public entry points and can be tied to a V-Net.
* For “xxxxx”, the subscriptions are in a hub-spoke model.
  + The hub will host shared infrastructure services, gateway subnet and a DMZ zone.
  + The gateway subnet will connect on premise to cloud. The shared infrastructure services will host domain controllers, DNS servers, configuration management and orchestrators. The DMZ zone will host the firewalls.
  + The spokes will be connected to the hub using V-Net peering. Traffic between virtual networks is limited to Microsoft backbone and is private.
  + User defined routes will be enabled on the subnets for the spokes such that all outbound traffic is diverted to the private load balancer IP for FortiGate. The firewall will perform a source NAT on traffic.
  + For inbound traffic, FortiGate will inspect traffic and perform source and destination NAT. In addition, for external applications the traffic post inspection will be forwarded to an application gateway enabled with WAF.
* Applications hosted on the spoke needs to have necessary network segmentation. Flat networks provide an easy terrain for malicious actors to maneuver through and make detection a challenge. The primary outcome of having multiple zones and segments is to minimize the opportunity for lateral movement once a network is compromised. Network security groups must be enabled at a subnet level, which will define ports and protocols enabled for east west communication between application components like web, middleware and database. Security teams need to perform risk assessments on applications and provide recommendations accordingly. External applications with high risk profile need to undergo a penetration test at a minimum.
* SaaS based applications need to go through a third-party risk assessment. The third-party risk assessment teams need to go through SOC type 2 reports and look at the overall security posture of the application before consumption. This will include checking authentication, authorization, transport and data security controls prior to consumption.

## SECURED SUBSCRIPTIONS

**HUB Subscription –** This subscription will host networking components like vpnGateway and Express Route Gateway.

**INF Subscription** – This subscription will house the shared infrastructure services on the cloud, like domain controllers, DNS, orchestrators, configuration management servers etc.

**NPE Subscription** – The NPE subscription will help application teams consume services, whitelisted by the cloud architecture and security team to develop and test applications, as they move to cloud.

**PROD Subscription** – The shared PROD subscription will help application teams consume services, again whitelisted by cloud architecture and security team to move applications to cloud production environment.

**Dedicated NPE Subscription** – In cases when the application team needs services not available in the shared model can opt for a dedicated subscription to host the application environment.

**Dedicated PROD Subscription** – In cases when the application team needs services not available in the shared model can opt for a dedicated subscription to host the application environment in Production.

## OUTBOUND TRAFFIC SECURITY

FortiGate will be leveraged to control outbound traffic flow. User-defined routes on the private subnets direct traffic to the load balancer’s private IP address, which shares a subnet with the firewall private interfaces.

The firewall applies source NAT to outbound internet traffic. The firewall translates the source address to its public interface. The firewall security policy allows appropriate application traffic from the resources in the spoke subscriptions to the internet. This would include opening traffic for Windows Updates, Git hub repositories etc.

The same internal load balancer that distributes outbound traffic to the firewalls also distributes the spoke-to-spoke east-west traffic.

## INBOUND TRAFFIC SECURITY

FortiGate will be used as an NVA for inbound traffic filtering. For inbound traffic, a public load balancer distributes traffic to the inbound active –active nodes of the FortiGate firewalls. Load-balancer rules forward inbound TCP/80 (HTTP) and TCP/443 (HTTPS) traffic to the firewalls. User-defined routes defined in the public interface will ensure that the firewall only receives traffic from the public load balancer. The firewall applies both destination and source NAT to inbound traffic. Destination NAT will translate the FQDN address object associated with the load-balancer public DNS name to the application hosted behind a WAF gateway. The source NAT translates the source to be the IP address of the private interface of the firewall, ensuring return traffic flows symmetrically. The firewall security policy allows appropriate application traffic to the resources in the private network while firewall security profiles prevent known malware and vulnerabilities from entering the network.

A diagram of a computer

Description automatically generated

The above architecture is based on hub-spoke model. Each region will have a dedicated hub – for “xxxxx”, one hub will be located at Wilson and another at Stamford.

## NETWORK SECURITY GROUPS

Network security groups will provide control on east-west traffic between applications. As best practice, recommended by Microsoft, network security groups will be attached to subnets. Network security groups can be tied to network interfaces. In order to keep the environment uniform and provide easier management, allow only network security groups to be attached to a subnet. As part of design, create a default network security group, which will be attached every time a subnet is created.

For inbound access, create allow rule for specific CIDR ranges (specific V-net’s) and deny rule from virtual network any any. These default rules will be created with higher priority numbers so that application teams can create rules which override them, if required.

For outbound access, create allow rules to allow traffic to specific on premise CIDR ranges, deny traffic to Internet. In addition, based on vulnerability solutions used you may require allowing traffic to specific CIDR ranges.

Application teams can make changes to the network security rules attached but will not be able to open ports for specific protocols which sends traffic in clear text, ex: Telnet, SMTP, FTP etc. Application teams can only open well-known ports to trusted CIDR ranges.

Below is a table for well-known ports:

|  |  |
| --- | --- |
| **Protocol** | **Port** |
| RDP | 3389 |
| SSH | 22 |
| MS SQL | 1433 |
| MySQL | 3306 |
| PostgreSQL | 5432 |
| Oracle | 1521 |
| PSQL | 1583, 3351 |
| Redshift | 5439 |
| Firebird | 3050 |
| Docker | 2735, 2736 |
| SMB | 445 |

It is advised that application teams configure applications with well-known ports and not use custom ports as security by obfuscation is not a good practice.

## KEY DESIGN CONSIDERATIONS – DATA SECURITY

* “xxxxx”should define data classification policies for the cloud. Data classification policies will govern data that can be classified as restricted, internal, confidential and public.
* Access control on resource groups will be based on least privilege and custom roles can be created for users/groups based on “need to know”. Resource group tagging can be very useful for organizing resources and can also drive compliance.
* Storage accounts used for storing data should not be opened for anonymous access. Storage account secrets needs to be rotated as per policy. When accessing storage blobs user delegated signed URL’s should be a preferred mechanism instead of embedding secrets within the code. Azure automation or serverless functions can be leveraged to detect storage accounts which are opened for anonymous access.
* Storage accounts support encryption at rest. As best practice, “xxxxx”need to manage the encryption keys that are used to encrypt data on Azure storage. If the data is extremely critical use of client-side encryption is the preferred approach where data is encrypted using asymmetric encryption algorithms before it is transferred to Azure storage.
* Shadow IT is a grey area and often security is not aware of the SaaS services that users or teams are consuming in the cloud. Microsoft CASB solutions can be leveraged to inject logs from on premise devices as a continuous stream or as a snapshot. This will give a complete picture of the unsanctioned applications in use within the environment.
* Sanctioned applications commonly SaaS platforms pose a risk on what data are stored and shared by the users. Microsoft CASB can integrate with SaaS based services over API and can scan data based on policies configured in offline mode.
* Inline data protection can be achieved with Microsoft CASB as it can integrate with Azure conditional forwarding for managed and unmanaged devices. Intune can be used additionally for mobile device management and can have policies which may further improve the security profile. For Office 365 and mobile based access it can encrypt data on devices and mandate the use of biometric authentication.
* In addition to SaaS based applications, Microsoft CASB can help protect IaaS services and custom applications.

## CLOUD ACCESS SECURITY BROKER

Microsoft CASB solutions span across Identity and Access Management, Threat Protection, Information Protection and Security Management.

The design needs to enable CASB in multi-mode so that API and inline introspection of traffic can be enabled. The API will provide offline scan of data across multiple SaaS services and integration with Azure conditional forwarding will scan data in real time.

Microsoft CASB can identity Shadow IT. For primary datacenters connected to Azure we will leverage loggers which will send data to CASB over syslog. For remote sites we will upload the data to CASB for parsing. Another mechanism is using Microsoft Defender ATP which can send Shadow IT information. But this approach is not selected as Microsoft Defender ATP is not the default EDR solution for clients. The traffic sent from logger to CASB needs to be sent over an HTTPS channel.

Intune is an MDM solution – an optional component in the architecture. Intune policies for managed and unmanaged devices can drive up the value of a CASB solution. The customer can fine tune policies on Intune which can block access to SaaS based applications or certain activities like downloads of files on unmanaged devices.

Another optional component is Azure Information Protection. Azure Information protection can help you classify data. CASB solution can look at the metadata information of files and can take actions based on classification.

The logs from CASB needs to be integrated with Azure Sentinel SIEM solution for “xxxxx”.

A diagram of a cloud

Description automatically generated

## KEY DESIGN CONSIDERATIONS – VM SECURITY

* Users logging onto Azure need to provide a second factor of authentication especially if the connection is not initiated from trusted IP ranges. Privileged accounts (co-admins, owners) will always need to provide MFA for logging into Azure.
* Azure VM’s should be organized in resource groups and RBAC access will be provided to the application teams for the resource group.
* Create Azure templates within a resource group and provide access to all application teams so that they can provision the IaaS resources into specific resource groups. The Azure templates will be based on golden images created from Azure ami’s. The images used needs to be updated over a period with latest patches.
* Ani-virus agent (Symantec), Vulnerability agents will be pushed to the IaaS instances using GPO. It’s important to note that agents cannot be installed as part of the golden image as this might have issues with GUID’s and the agents will not report back to the management console properly.
* In addition, Microsoft monitoring agent can be pushed to Azure VM’s for logging into Log Analytics workspace.
* Vulnerability scans will scan all VM’s every week and will create a report, based on which patching needs to be scheduled either using GPO/SCCM.
* There should be no assignment of public IP addresses to network interfaces for VM’s. This can be monitored through Azure Policy/automation/serverless functions.
* Tags needs to be allocated to all Azure VM’s. Tags play an important role and can be used to implement RBAC policies. Tags can be monitored using Azure Policies/Automation/serverless monitoring.
* Just in time access can be enabled on Azure VM’s for RDP and SSH. RBAC policies are checked for a user before access is granted for the session.

## AZURE SECURITY CENTER

Azure Security Center is a native unified infrastructure security management system that strengthens the security posture and provides advanced threat protection. Security Center protects both Windows and Linux servers, by installing the Microsoft Monitoring Agent on them.

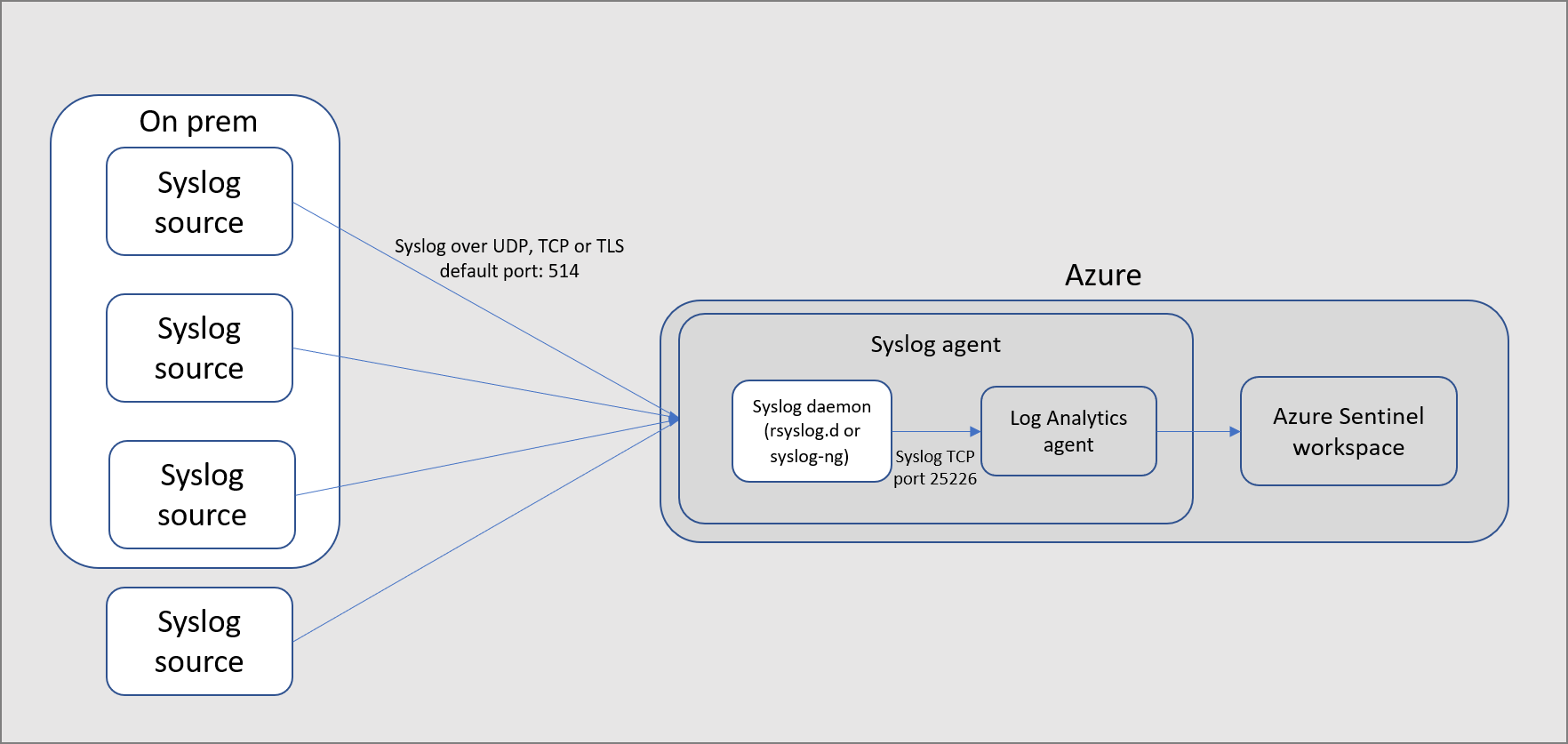
Security Center has two tiers - Free and Standard

* Free tier offers only continuous assessment and security recommendations and secure score
* Standard Tier offers premium features like threat detection alerts, JIT VM Access, adaptive application controls and regulatory compliance dashboards & reports and threat protection for Azure VMs and PaaS services

“XXXXX” recommends adopting a standard tier and adopting CIS benchmarks to strengthen security posture.

## SIEM integration

Azure Sentinel will be used as a managed SIEM solution. It operates on top of Log Analytics and can integrate with Azure AD, Azure Security Center, Microsoft CASB, Microsoft Defender ATP etc. Additionally, it provides API based integration with products like Barracuda, F5, Forcepoint DLP etc. Azure Sentinel can also be connected to data sources which uses syslog to send data – it can provide agents that can be installed on servers, which will do the necessary conversion of data so that it can be fed to Log Analytics.



The above diagram shows how syslog data is consumed by Azure Sentinel.

By default, Azure Sentinel supports data storage for 31 days, but the retention period can be increased up to 730 days.

Default RBAC roles are provided as below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Role** | **Create and run playbooks** | **Create and edit dashboards, analytic rules, and other Azure Sentinel resources** | **Manage incidents (dismiss, assign, etc.)** | **View data, incidents, dashboards and other Azure Sentinel resources** |
| Azure Sentinel reader | -- | -- | -- | X |
| Azure Sentinel responder | -- | -- | X | X |
| Azure Sentinel contributor | -- | X | X | X |
| Azure Sentinel contributor + Logic App contributor | X | X | X | X |

In addition, custom roles can be created for Azure Sentinel.

For visualization, Grafana can be used with Sentinel as it offers easy integration.

# COMPUTE & STORAGE

Compute refers to the hosting model for the computing resources that application runs on. Azure Hosting model consists of Virtual Machines, App Service, Service Fabric, Azure Functions, Azure Kubernetes Service, Container Instances and Azure Batch accounts.

This document and section scope is limited to Virtual Machines

## VIRTUAL MACHINES

Azure Virtual Machines are image service instances that provide on-demand and scalable computing resources with usage-based pricing. Azure offers a range of virtual machines for both Linux and Windows.

### **AVAILABILITY ZONES/SETS**

Availability Zones is a high-availability offering that protects your applications and data from datacenter failures. Availability Zones are unique physical locations within an Azure region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking. To ensure resiliency, there’s a minimum of three separate zones in all enabled regions. The physical separation of Availability Zones within a region protects applications and data from datacenter failures. Zone-redundant services replicate your applications and data across Availability Zones to protect from single-points-of-failure. With Availability Zones, Azure offers industry best 99.99% VM uptime SLA.

A diagram of a server

Description automatically generated

An Availability Zone in an Azure region is a combination of a fault domain and an update domain. For example, if you create three or more VMs across three zones in an Azure region, your VMs are effectively distributed across three fault domains and three update domains.

**Availability sets** are another datacenter configuration to provide VM redundancy and availability. This configuration within a datacenter ensures that during either a planned or unplanned maintenance event, at least one virtual machine is available and meets the 99.95% Azure SLA

Note: A single instance virtual machine in an availability set by itself should use Premium SSD or Ultra Disk for all operating system disks and data disks in order to qualify for the SLA for Virtual Machine connectivity of at least 99.9%.

### **CUSTOM (GOLD) IMAGES**

Following are VM provisioning recommendations which should be considered as a target state.

* VMs to be created using Azure market place image
* Automate installation of required agents via scripts or SCCM deployments
* OS Hardening policies to be applied via scripts (linux) and AD group policy (windows).

While these are target state objectives, in the interim “xxxxx”will need to leverage custom (gold) images which are hardened and have all the required agents (Antivirus, backup, monitoring etc) installed.

### **OS HARDENING STANDARDS**

“xxxxx”to follow CIS Benchmarks and Microsoft best practices and apply OS hardening standards via AD group policy

### **VM AUTOMATION**

DRYiCE MyCloud is a proactive hybrid cloud lifecycle management product and empowers organizations to govern, provision, monitor and manage infrastructure. It helps combining data exploration and data visualization in an easy-to-use application that enables effective analysis and actionable insights for IaaS/PaaS/SaaS.

KEY BENEFITS

* DRYiCE MyCloud automates the management of the hybrid cloud environment while ensuring agility, flexibility and scalability.
* Improved SLAs & reduction in cost of operations
* High visibility on infrastructure usage and capacity trending
* ITIL framework based Standardization & Alignment of processes
* Unified reporting
* Effective utilization of existing tools and platforms
* Business objectives aligned IT Metrics
* Over 40% increase in virtual asset utilization
* 100% reduction in manual effort for provisioning

## STORAGE

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables.

### **STORAGE ACCOUNTS**

An Azure storage account contains all Azure Storage data objects: blobs, files, queues, tables, and disks. The storage account provides a unique namespace for your Azure Storage data that is accessible from anywhere in the world over HTTP or HTTPS. Data in Azure storage account is durable and highly available, secure, and massively scalable.

Following are the types of storage accounts -

* General-purpose v2 accounts: Basic storage account type for blobs, files, queues, and tables. Recommended for most scenarios using Azure Storage.
* General-purpose v1 accounts: Legacy account type for blobs, files, queues, and tables. Use general-purpose v2 accounts instead when possible.
* BlockBlobStorage accounts: Storage accounts with premium performance characteristics for block blobs and append blobs. Recommended for scenarios with high transactions rates, or scenarios that use smaller objects or require consistently low storage latency.
* FileStorage accounts: Files-only storage accounts with premium performance characteristics. Recommended for enterprise or high performance scale applications.
* BlobStorage accounts: Legacy Blob-only storage accounts. Use general-purpose v2 accounts instead when possible.

Microsoft recommends using a general-purpose v2 storage account for most scenarios. General-purpose v2 storage accounts offer multiple access tiers for storing data based on your usage patterns.

### **DISK STORAGE**

Azure managed disks are block-level storage volumes that are managed by Azure and used with Azure Virtual Machines. The available types of disks are ultra-disks, premium solid-state drives (SSD), standard SSDs, and standard hard disk drives (HDD).

There are three main disk roles in Azure which map to the disks that are attached to the virtual machine - **the data disk, the OS disk, and the temporary disk**.

* A data disk is used to store application data. Each data disk has a maximum capacity of 32,767 gibibytes (GiB). The size of the virtual machine determines how many data disks you can attach to it and the type of storage you can use to host the disks.
* Every virtual machine has one attached operating system disk. That OS disk has a pre-installed OS, which was selected when the VM was created. This disk contains the boot volume. This disk has a maximum capacity of 2,048 GiB.
* Every VM contains a temporary disk, which is not a managed disk. The temporary disk provides short-term storage for applications and processes and is intended to only store data such as page or swap files. Data on the temporary disk may be lost during a maintenance event event or when you redeploy a VM. On Azure Linux VMs, the temporary disk is /dev/sdb by default and on Windows VMs the temporary disk is D: by default.

### **DISK TYPES**

The following table provides a comparison of ultra-disks, premium solid-state drives (SSD), standard SSD, and standard hard disk drives (HDD) .

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Ultra-disk** | **Premium SSD** | **Standard SSD** | **Standard HDD** |
| Disk type | SSD | SSD | SSD | HDD |
| Scenario | IO-intensive workloads such as  SAP HANA, top tier databases (for example, SQL, Oracle), and other transaction-heavy workloads. | Production and performance sensitive workloads | Web servers, lightly used enterprise applications and dev/test | Backup, non-critical, infrequent access |
| Max disk size | 65,536 gibibyte (GiB) | 32,767 GiB | 32,767 GiB | 32,767 GiB |
| Max throughput | 2,000 MiB/s | 900 MiB/s | 750 MiB/s | 500 MiB/s |
| Max IOPS | 160,000 | 20,000 | 6,000 | 2,000 |

### **FILE STORAGE**

Azure Files offers fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) protocol. Azure file shares can be mounted concurrently by cloud or on-premises deployments of Windows, Linux, and macOS. Additionally, Azure file shares can be cached on Windows Servers with Azure File Sync for fast access near where the data is being used.

The following diagram illustrates the Azure Files management constructs:

A diagram of a file sharing

Description automatically generated

Azure Files offers two, built-in, convenient data access methods

**Direct cloud access:** Any Azure file share can be mounted by Windows, macOS, and/or Linux with the industry standard Server Message Block (SMB) protocol or via the File REST API. With SMB, reads and writes to files on the share are made directly on the file share in Azure.

**Azure File Sync:** With Azure File Sync, shares can be replicated to Windows Servers on-premises or in Azure. Your users would access the file share through the Windows Server, such as through an SMB or NFS share. This is useful for scenarios in which data will be accessed and modified far away from an Azure datacenter, such as in a branch office scenario.

The following table illustrates how your users and applications can access your Azure file share:

|  |  |  |
| --- | --- | --- |
|  | **Direct cloud access** | **Azure File Sync** |
| What protocols do you need to use? | Azure Files supports SMB 2.1, SMB 3.0, and File REST API. | Access your Azure file share via any supported protocol on Windows Server (SMB, NFS, FTPS, etc.) |
| Where are you running your workload? | **In Azure**: Azure Files offers direct access to your data. | **On-premises with slow network**: Windows, Linux, and macOS clients can mount a local on-premises Windows File share as a fast cache of your Azure file share. |
| What level of ACLs do you need? | Share and file level. | Share, file, and user level. |

Azure Files offers two performance tiers: standard and premium.

**Standard file shares** are backed by hard disk drives (HDDs) but are available in a pay-as-you-go billing model.

**Premium file shares** are backed by solid-state drives (SSDs). Azure Backup is available for premium file shares and Azure Kubernetes Service supports premium file shares in version 1.13 and above. Premium file shares are available with LRS in most regions that offer storage accounts and with ZRS in a smaller subset of regions.

To perform a bulk data transfer from an existing file share, such as an on-premises file share, into Azure Files, we can use Azure File Sync, Azure Import/Export, Robocopy and AzCopy.

### **AZURE FILES AUTHENTICATION**

Until recently, Azure Files supported identity based authentication over SMB through Azure Active Directory Domain Services (Azure AD DS) only. The Windows ACLs (NTFS DACLs) configured in on-premises AD would not be applied to Azure Files.

However, Azure announced the preview of Azure Files Active Directory (AD) authentication (<https://azure.microsoft.com/en-us/blog/preview-of-active-directory-for-authentication-on-azure-file/> ) which allows to mount Azure Files using AD credentials with the exact same access control experience as on-premises.

“XXXXX” recommends deploying a file server in Azure Virtual Machines till the AD authentication feature is generally available. This should be an interim solution till the AD authentication is generally available.

### **ENCRYPTION**

Managed disks offer two different kinds of encryption -

* Server-Side Encryption (SSE) -

Azure Storage automatically encrypts data at rest. Data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption.

* Azure Disk Encryption (ADE) –

It allows to encrypt the OS and Data disks used by an IaaS Virtual Machine. The encryption process is integrated with Azure Key Vault to allow you to control and manage the disk encryption keys.

For Windows, the drives are encrypted using industry-standard BitLocker encryption technology.

For Linux, the disks are encrypted using the DM-Crypt technology.

## KEY DESIGN CONSIDERATIONS

|  |  |
| --- | --- |
| S.No | Design Principle |
| 1 | All applications and databases will be created in an Availability Zone for high availability. |
| 2 | GenV2 storage accounts will be created and used when such a requirement arises. |
| 3 | Only Managed Disk will be used as data disks |
| 4 | Premium SSD will be used for Production workloads and Standard SSD will be used for non- prod workloads. |
| 5 | Data disk encryption to be enabled using Keyvaults to comply with CIS benchmarks |

# AZURE ACTIVE DIRECTORY

Azure Active Directory (Azure AD) is Microsoft’s cloud-based identity and access management service and provides -

* Identity management for applications across all categories of Microsoft s cloud (SaaS, PaaS, IaaS).
* Consolidated identity management for third-party cloud applications
* in your portfolio.
* Collaboration with partners.
* Management of customer identities.
* Integration with web-based applications located on-premises.
* For line of business (LOB) applications hosted on virtual machines in Azure IaaS, you can use Domain Services in Azure AD. Or, you can extend your on-premises Windows Server Active Directory (AD) environment.

A diagram of a service

Description automatically generated

With an Office 365 or an Azure subscription, you automatically get Azure AD with access to all features. Azure AD can be further upgraded to Premium P1 and Premium P2 licenses which provide self-service, enhanced monitoring, security reporting, and secure access for your mobile users.

“xxxxx”will opt for a Premium P1 plan and in future may opt for Premium P2 plan to leverage native Privileged Identity Management and Identity Protection features.

## ON-PREMISES WINDOWS SERVERS AD ACCOUNTS INTEGRATION WITH AZURE AD

Using cloud-only accounts is not recommended for enterprise-scale organizations unless Windows Server AD is not already used on premises.

Integration of on-premises Windows Server AD accounts with Azure AD provides access to both Microsoft SaaS services and cloud-based identity options for Azure PaaS and IaaS applications.

Following are the two recommended approaches -

* Directory and password synchronization
* Federation

### **HYBRID IDENTITY**

Azure AD Connect is the Microsoft tool designed to meet and accomplish hybrid identity goals.

It provides the following features:

* Password hash synchronization - A sign-in method that synchronizes a hash of a users on-premises AD password with Azure AD.
* Pass-through authentication - A sign-in method that allows users to use the same password on-premises and in the cloud but doesn't require the additional infrastructure of a federated environment.
* Federation integration - Federation is an optional part of Azure AD Connect and can be used to configure a hybrid environment using an on-premises AD FS infrastructure. It also provides AD FS management capabilities such as certificate renewal and additional AD FS server deployments.
* Synchronization - Responsible for creating users, groups, and other objects. As well as, making sure identity information for your on-premises users and groups is matching the cloud. This synchronization also includes password hashes.
* Health Monitoring - Azure AD Connect Health can provide robust monitoring and provide a central location in the Azure portal to view this activity. However, Azure AD Connect Health Monitoring requires an Premium P1 license.

A diagram of a cloud

Description automatically generated

### **DIRECTORY & PASSWORD SYNCRONIZATION**

A diagram of a cloud datacenter

Description automatically generated

This is the simplest option and the recommended option for most enterprise organizations.

* User accounts are synchronized from your on-premises directory to your Azure AD tenant. The on-premises directory remains the authoritative source for accounts.
* Azure AD performs all authentication for cloud-based services and applications.
* Supports multi-forest synchronization.

**Password synchronization**

* Users enter the same password for cloud services as they do on-premises.
* User passwords are never sent to Azure AD. Instead a hash of each password is synchronized. It is not possible to decrypt or reverse-engineer a hash of a password or to obtain the password itself.

**Multi-factor authentication (MFA)**

* You can take advantage of basic MFA features offered with Office 365.
* Applications in Azure can take advantage of the Azure Multi-Factor Authentication service.
* Directory synchronization does not provide integration with on-premises MFA solutions.

### **FEDERATION**

A diagram of a cloud datacenter

Description automatically generated

Federation provides additional enterprise capabilities. It is also more complex and introduces more dependencies for access to cloud services.

* All authentication to Azure AD is performed against the on-premises directory via Active Directory Federation Services (AD FS) or another federated identity provider.
* Works with non-Microsoft identity providers.
* Password hash sync adds the capability to act as a sign-in backup for federated sign-in (if the federation solution fails).

It is advised to use federation only if AD FS, third party identity provider, integrated smart card/MFA solution is already deployed

Federated authentication requires a greater investment in infrastructure on-premises as

* The on-premises servers must be Internet-accessible through a corporate firewall. Microsoft recommends the use of Federation Proxy servers deployed in a perimeter network, screened subnet, or DMZ.
* Requires hardware, licenses, and operations for AD FS servers, AD FS proxy or Web Application Proxy servers, firewalls, and load balancers.
* Availability and performance are important to ensure users can access Office 365 and other cloud applications.

## ACTIVE DIRECTORY DOMAIN SERVICES FOR AZURE

Many LOB solutions that run on virtual machines require Windows Server AD for the following functionality:

* Support for NTLM, Kerberos, or LDAP-based authentication
* Domain-joined virtual machines
* Group Policy

There are two recommended solutions available to achieve this -

* Azure AD Domain Services
* Extending Windows Server AD to Azure VM

### **AZURE AD DOMAIN SERVICES**

A screenshot of a computer

Description automatically generated

AD Domain Services can be enabled in the existing Azure AD tenant. There is no need to deploy and manage domain controllers. This managed domain is a standalone domain and is not an extension of an organizations on-premises domain/forest infrastructure. However, all user accounts, group memberships and credentials from the on-premises directory are available in this managed domain. Users login using the same corporate credentials they use for Azure AD.

* Domain Services is connected to a virtual network in Azure IaaS.
* This instance of Domain Services can be used by other virtual networks that are connected to the virtual network configured with Domain Services

AD Domain Services is an ideal solution when applications require domain services support for:

* Server application management.
* Server login.
* User authentication over Kerberos, NTLM, or LDAP.
* Directory lookup over LDAP/LDAPS.

### **EXTENDING WINDOWS SERVER AD TO AZURE VM**

A screenshot of a computer

Description automatically generated

* This configuration is a hybrid deployment of Windows Server AD on premises and in Azure. It requires:
* A virtual network in Azure IaaS.
* A site-to-site VPN connection or ExpressRoute connection.
* Extending your on-premises, private IP address range to virtual machines in the virtual network.
* Deploying one or more domain controllers in the Azure virtual network designated as a global catalog server (reduces egress traffic across the VPN connection).

Extending on-premises Windows Server AD domain to Azure is ideal when the requirement is

* Schema extensibility.
* Ability to write to existing directory identities.
* Support for applications in Azure virtual networks where network
* isolation is a requirement.
* Support across multiple Azure subscriptions.
* Certificate or smartcard-based authentication for applications.

Following is a reference architecture for

A diagram of a computer application

Description automatically generated

This architecture is commonly used when the on-premises network and the Azure virtual network are connected by a VPN or ExpressRoute connection and supports bidirectional replication. This architecture is recommended for hybrid applications in which functionality is distributed between on-premises and Azure, and applications and services that perform authentication using Active Directory.

A separate ADDS and Management Subnet have been provisioned in the VNETs of EMEA, APAC and LATAM region to support this architecture

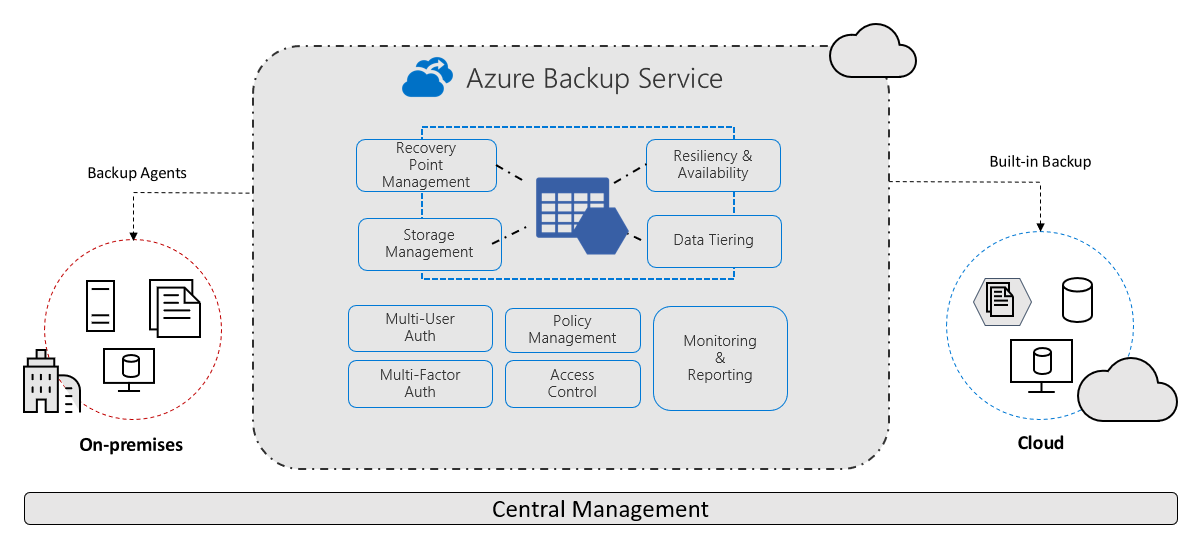
* It is recommended to create an AD DS site including the subnets defined for application in Azure. Then, configure a site link between your on-premises AD DS sites, and AD DS will automatically perform the most efficient database replication possible. This database replication requires little beyond the initial configuration.
* It is not recommended to assign operations masters roles to the domain controllers deployed in Azure.

## KEY DESIGN CONSIDERATIONS

|  |  |
| --- | --- |
| S.No | Design Principle |
| 1 | “xxxxx”to opt for a Premium P1 plan |
| 2 | 6 Domain Controllers will be created, a pair in an availability zone per region - EMEA, APAC and LATAM |
| 3 | For Hybrid Identity, Azure AD connect to be configured for integrating Windows AD |
| 4 | Passthrough authentication to be configured in AAD Connect |
| 5 | AAD Connect Health Monitor to be configured. |

# BACKUP & DR

Azure Backup service provides simple, secure, and cost-effective solutions to back up your data, both in Azure as well as on on-premises, and recover it from the Microsoft Azure cloud.



Azure Backup can backup the following workloads.

* On-premises - Back up files, folders, system state using the Microsoft Azure Recovery Services (MARS) agent. Or use the DPM or Azure Backup Server (MABS) agent to protect on-premises VMs (Hyper-V and VMWare) and other on-premises workloads
* Azure VMs - Back up entire Windows/Linux VMs (using backup extensions) or back up files, folders, and system state using the MARS agent.
* Azure Files shares - Backup Azure File shares to a storage account
* SQL Server in Azure VMs - Back up SQL Server databases running on Azure VMs
* SAP HANA databases in Azure VMs - Backup SAP HANA databases running on Azure VMs

## RECOVERY SERVICES VAULT

Azure Backup stores backed-up data in a Recovery Services vault. A Recovery Services Vault is an online-storage entity in Azure that's used to hold data, such as backup copies, recovery points, and backup policies.

Azure Backup offers two types of replication to keep your storage/data highly available.

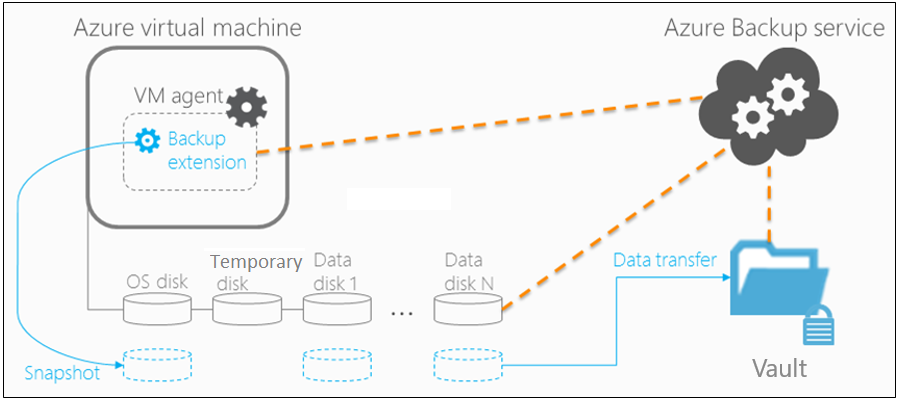
**Locally redundant storage (LRS)** replicates your data three times (it creates three copies of your data) in a storage scale unit in a datacenter. All copies of the data exist within the same region. LRS is a low-cost option for protecting your data from local hardware failures.

**Geo-redundant storage (GRS)** is the default and recommended replication option. GRS replicates your data to a secondary region (hundreds of miles away from the primary location of the source data). GRS costs more than LRS, but GRS provides a higher level of durability for your data, even if there's a regional outage.

## AZURE IaaS VM BACKUP

Azure Virtual Machine Backup is an integrated backup solution that protects your virtual machines and applications deployed in Microsoft Azure. Azure Virtual Machine Backup provides application-consistent protection for cloud-based workloads with all VSS aware workloads supported.

Following image depicts the workflow of an Azure VM Backup



### **SNAPSHOT CONSISTENCY**

The following table explains the different types of snapshot consistency –

| **Snapshot** | **Details** | **Recovery** | **Consideration** |
| --- | --- | --- | --- |
| Application-consistent | App-consistent backups capture memory content and pending I/O operations. App-consistent snapshots use a VSS writer (or pre/post scripts for Linux) to ensure the consistency of the app data before a backup occurs. | When you're recovering a VM with an app-consistent snapshot, the VM boots up. There's no data corruption or loss. The apps start in a consistent state. | Windows: All VSS writers succeeded  Linux: Pre/post scripts are configured and succeeded |
| File-system consistent | File-system consistent backups provide consistency by taking a snapshot of all files at the same time. | When you're recovering a VM with a file-system consistent snapshot, the VM boots up. There's no data corruption or loss. Apps need to implement their own "fix-up" mechanism to make sure that restored data is consistent. | Windows: Some VSS writers failed  Linux: Default (if pre/post scripts aren't configured or failed) |
| Crash-consistent | Crash-consistent snapshots typically occur if an Azure VM shuts down at the time of backup. Only the data that already exists on the disk at the time of backup is captured and backed up. | Starts with the VM boot process followed by a disk check to fix corruption errors. Any in-memory data or write operations that weren't transferred to disk before the crash are lost. Apps implement their own data verification. For example, a database app can use its transaction log for verification. If the transaction log has entries that aren't in the database, the database software rolls transactions back until the data is consistent. | VM is in shutdown (stopped/ deallocated) state. |

## FILES & FOLDERS BACKUP

Azure Backup uses the MARS agent to back up data from on-premises machines and Azure VMs to a backup Recovery Services vault in Azure. The MARS agent can:

* Run on on-premises Windows machines so that they can back up directly to a backup Recovery Services vault in Azure.
* Run on Windows VMs so that they can back up directly to a vault.
* Run on Microsoft Azure Backup Server (MABS) or a System Center Data Protection Manager (DPM) server. In this scenario, machines and workloads back up to MABS or to the DPM server. The MARS agent then backs up this server to a vault in Azure.
* By installing a MARS Agent, we can enable backup of files, folders, and the system state.

### **BACKUP TYPES**

The following table explains the different types of backups and when they're used:

| **Backup type** | **Details** | **Usage** |
| --- | --- | --- |
| **Full** | A full backup contains the entire data source. Takes more network bandwidth than differential or incremental backups. | Used for initial backup. |
| **Differential** | A differential backup stores the blocks that changed since the initial full backup. Uses a smaller amount of network and storage, and doesn't keep redundant copies of unchanged data.  Inefficient because data blocks that are unchanged between later backups are transferred and stored. | Not used by Azure Backup. |
| **Incremental** | An incremental backup stores only the blocks of data that changed since the previous backup. High storage and network efficiency.  With incremental backup, there's no need to supplement with full backups. | Used by DPM/MABS for disk backups, and used in all backups to Azure. Not used for SQL Server backup. |

## AZURE SQL BACKUP

Azure Backup can back up SQL Server databases running on Azure VMs. SQL Server databases are critical workloads that require a low recovery point objective (RPO) and long-term retention.

A diagram of a computer system

Description automatically generated

This solution leverages the SQL native APIs to take backups of your SQL databases.

Azure supports Full, Differential and Log backup types on Azure.

|  |  |  |
| --- | --- | --- |
| **Backup type** | **Details** | **Usage** |
| **Full backup** | A full database backup backs up the entire database. It contains all the data in a specific database or in a set of filegroups or files. A full backup also contains enough logs to recover that data. | At most, you can trigger one full backup per day. You can choose to make a full backup on a daily or weekly interval. |
| **Differential backup** | A differential backup is based on the most recent, previous full-data backup.  It captures only the data that's changed since the full backup | At most, you can trigger one differential backup per day.  You can't configure a full backup and a differential backup on the same day. |
| **Transaction log backup** | A log backup enables point-in-time restoration up to a specific second. | At most, you can configure transactional log backups every 15 minutes. |

Following are limitations of SQL backup which need to be considered

* SQL Server backup can be configured in the Azure portal or **PowerShell**, CLI is not supported.
* VM running SQL Server requires internet connectivity to access Azure public IP addresses.
* SQL Server **Failover Cluster Instance (FCI)** is not supported.
* Back up and restore operations for mirror databases and database snapshots aren't supported.
* Using more than one backup solutions to back up standalone SQL Server instance or SQL Always on availability group may lead to backup failure; refrain from doing so.
* Backing up two nodes of an availability group individually with same or different solutions, may also lead to backup failure.
* Azure Backup supports only Full and Copy-only Full backup types for **Read-only** databases
* Databases with large number of files can't be protected. The maximum number of files that is supported is **~1000**.
* You can back up to **~2000** SQL Server databases in a vault. You can create multiple vaults in case you have a greater number of databases.
* You can configure backup for up to **50** databases in one go; this restriction helps optimize backup loads.
* Azure support databases up to **2 TB** in size; for sizes greater than that performance issues may come up.
* It is recommended that the backup is configured on only one node of an AG. Backup should always be configured in the same region as the primary node. Cross-region backups are not supported

## KEY DESIGN CONSIDERATIONS

|  |  |
| --- | --- |
| S.No | Design Prinicple |
| 1 | All Production VMs will be backed up using Azure IaaS VM backup |
| 2 | Dev/Test, UAT VMs will be backed up using Azure IaaS VM backup |
| 3 | MARS agent may be used for Files/Folder level backup if required |
| 4 | Azure SQL Backups maybe used for production SQL workloads to reduce license cost of EMC Avamar. |
| 5 | Azure MAB server will not be used to backup on-premises workloads |

## AZURE SITE RECOVERY

Along with Azure Backup, Site recovery service aids business continuity and disaster recovery (BCDR) strategy that keeps your data safe, and apps and workloads up and running, when planned and unplanned outages occur. Site Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location. When an outage occurs at your primary site, you fail over to secondary location, and access apps from there. After the primary location is running again, you can fail back to it.

Site Recovery can manage replication for:

* Azure VMs replicating between Azure regions.
* On-premises VMs, Azure Stack VMs and physical servers.

Following are the features of ASR.

|  |  |
| --- | --- |
| **Feature** | **Details** |
| **Simple BCDR solution** | Using Site Recovery, you can set up and manage replication, failover, and failback from a single location in the Azure portal. |
| **Azure VM replication** | You can set up disaster recovery of Azure VMs from a primary region to a secondary region. |
| **On-premises VM replication** | You can replicate on-premises VMs and physical servers to Azure, or to a secondary on-premises datacenter. Replication to Azure eliminates the cost and complexity of maintaining a secondary datacenter. |
| **Workload replication** | Replicate any workload running on supported Azure VMs, on-premises Hyper-V and VMware VMs, and Windows/Linux physical servers. |
| **Data resilience** | Site Recovery orchestrates replication without intercepting application data. When you replicate to Azure, data is stored in Azure storage, with the resilience that provides. When failover occurs, Azure VMs are created, based on the replicated data. |
| **RTO and RPO targets** | Keep recovery time objectives (RTO) and recovery point objectives (RPO) within  organizational limits. Site Recovery provides continuous replication for Azure VMs and VMware VMs, and replication frequency as low as 30 seconds for Hyper-V. You can reduce RTO further by integrating with Azure Traffic Manager. |
| **Keep apps consistent over failover** | You can replicate using recovery points with application-consistent snapshots. These snapshots capture disk data, all data in memory, and all transactions in process. |
| **Testing without disruption** | You can easily run disaster recovery drills, without affecting ongoing replication. |
| **Flexible failovers** | You can run planned failovers for expected outages with zero-data loss, or unplanned failovers with minimal data loss (depending on replication frequency) for unexpected disasters. You can easily fail back to your primary site when it's available again. |
| **Customized recovery plans** | Using recovery plans, can customize and sequence the failover and recovery of multi-tier applications running on multiple VMs. You group machines together in a recovery plan, and optionally add scripts and manual actions. Recovery plans can be integrated with Azure automation runbooks. |
| **BCDR integration** | Site Recovery integrates with other BCDR technologies. For example, you can use Site Recovery to protect the SQL Server backend of corporate workloads, with native support for SQL Server AlwaysOn, to manage the failover of availability groups. |
| **Azure automation integration** | A rich Azure Automation library provides production-ready, application-specific scripts that can be downloaded and integrated with Site Recovery. |
| **Network integration** | Site Recovery integrates with Azure for simple application network management, including reserving IP addresses, configuring load-balancers, and integrating Azure Traffic Manager for efficient network switchovers. |

Applications which will leverage Azure Site Recovery as a DRaaS need to be identified along with RPO/RTO SLA requirements for the same. Based on the requirement, a Hot, Warm or Cold Strategy needs to be designed specific to the application.

# MONITORING

Azure Monitor is a native monitoring solution and provides monitoring capabilities for Azure VMs, Containers, PaaS Applications, Log Analytics and allow to create customized dashboards, smart alerts and reports (workbooks).

Network Watcher provides packet capture, traffic flow and diagnosis of VPN connectivity issues.

Network Performance Monitoring (NPM) provides Express Route Circuit Monitoring

## AZURE MONITOR

The following diagram gives a high-level view of Azure Monitor

A screenshot of a computer

Description automatically generated

Azure monitor collects two types of data **- metrics and logs**

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.

Azure Monitor Logs is a log data platform that collects activity logs and resource logs along with other monitoring data to provide deep analysis across your entire set of resources.

* Resource Logs provide insight into operations that were performed within an Azure resource
* Activity logs provides insight into the operations on each Azure resource in the subscription,
* Azure Active Directory logs contains the history of sign-in activity and audit trail of changes made in the Azure Active Directory for a tenant

Data collected by Azure Monitor Logs is stored in a Log Analytics workspace. Data in Azure Monitor Logs is retrieved using a log query written with the Kusto query language.

Moogsoft, an AI based event correlation engine can be integrated to Azure Monitor by using webhooks to aid command center operations.

## SCOM (WINDOWS/SQL MONITORING)

Microsoft SCOM will be used to monitor SQL DB on Azure IaaS VMs and VM (OS) monitoring. SCOM configuration and management is supported by “XXXXX” Monitoring operations team. To know more about SCOM architecture and deployed solution, please refer the runbook

## OEM(LINUX/ORACLE MONITORING)

Oracle Enterprise Manager will be used to monitor Oracle and Linux workloads. Link to existing OEM runbook to be added. Link to OEM runbook

# ATTACHMENT CHECK LIST

# REFERENCES