**C:\Users\Charles\Desktop\Dropbox (10th Magnitude)\Marketing\Images\Brand Artwork\Logo 3.0\Standard_RGB\10thmagnitude-logo-rgb.tif**

**Azure Cloud Architecture Design**

**Presented to:**

**Helmerich & Payne**

8/27/2019

10th Magnitude, LLC

20 North Wacker Drive #530

Chicago, IL 60606

Notice of Confidentiality © 2017 10th Magnitude, LLC All rights reserved

THIS DOCUMENT IS 10TH MAGNITUDE PROPRIETARY AND CONFIDENTIAL INFORMATION AND IS SUBJECT TO THE TERMS OF THE 10TH MAGNITUDE NON-DISCLOSURE AGREEMENT. NEITHER THIS DOCUMENT NOR ITS CONTENTS MAY BE REVEALED OR DISCLOSED TO UNAUTHORIZED PERSONS OR SENT OUTSIDE THE AFOREMENTIONED COMPANY WITHOUT PRIOR PERMISSION FROM 10TH MAGNITUDE.

Table of Contents

[1 The Beginning 3](#_Toc17743596)

[Why the cloud? 3](#_Toc17743597)

[The Journey 4](#_Toc17743598)

[Experimentation and Innovation 4](#_Toc17743599)

[2 Strategy & Goals 6](#_Toc17743600)

[Business Strategy & Cloud Strategy 6](#_Toc17743601)

[Cloud Team 6](#_Toc17743602)

[Adoption Framework 7](#_Toc17743603)

[Principles 11](#_Toc17743604)

[Building and Executing the Plan 11](#_Toc17743605)

[Shared Services (HUB) design 12](#_Toc17743606)

[Enterprise HUB and Shared Services 13](#_Toc17743607)

[Shared services to be offered (examples) 14](#_Toc17743608)

[Azure Policy - Description 21](#_Toc17743609)

[Azure Policy Composition 21](#_Toc17743610)

[Azure Policy Initiatives 21](#_Toc17743611)

[Initiative Definition 21](#_Toc17743612)

[Initiative assignment 22](#_Toc17743613)

[Recommendations 22](#_Toc17743614)

[Suggested Initiatives: 22](#_Toc17743615)

[1. Security Center 22](#_Toc17743616)

[2. Diagnostic Logging 22](#_Toc17743617)

[3. Governance 23](#_Toc17743618)

[4. Network 23](#_Toc17743619)

[Consumption and Financials 25](#_Toc17743620)

[Cloud Consumers 26](#_Toc17743621)

[Networking within the Shared Service (HUB) model 27](#_Toc17743622)

[HUB/Spoke subscription topology 34](#_Toc17743623)

[Azure Paired regions 35](#_Toc17743624)

[Dealing with legacy workloads within Azure 36](#_Toc17743625)

[Monitoring and Logging 37](#_Toc17743626)

# The Beginning

## Why the cloud?

The public cloud has become a core element of any enterprise technology strategy. The success of that strategy and key to enterprise adoption can be tied to effective implementation and integration, governance, development, and operations of the underlying cloud framework and how an organization utilizes it daily. This cloud strategy is not impacted by a single department or team and knows no boundaries. Each organization also takes somewhat of a different path along the journey based on their culture, history, and immediate priorities. The strategy and maturity progression will also impact all portions of an organization, and all parties will have to adapt and iterate to find the right fit for the enterprise.

A key aspect and beginning of an organizations public cloud strategy is to answer *WHY the public cloud*. Establishing this up front can assist with defining the enterprise strategic objectives of why this journey to the public cloud is so important. Usually this can be seen by reviewing the trend of financial growth in an organizations private cloud. Operations staff, capital equipment management, software/operating system/platform maintenance, speed of infrastructure delivery, etc. could easily start to consumer large portions of an IT organizations budget, with only a small focus on innovation and business value. In almost all cases, these are not core components to the business either. Other “Why’s” can also be found within the application development practices. Application lifecycle activities, development practices, tooling, and ultimately the architecture and approach for application development are extremely integrated with the public cloud. It is natural for the why of public cloud to have a lot of input and impact from application development use cases.

Beyond modifying technical financials, quenching the thirst for innovation, and understanding application lifecycle, efficiency and speed or time to market are also key factors for the motivation and integration of the public cloud. In today’s challenging global marketplace all organizations are finding that inefficiency will have an immense effect on the quality and perception of their products and services. Further, the speed of delivery, the agility of your technology, and how you outpace your competitors will allow for organizations to keep the competitive edge and maintain leadership in the marketplace.

Establishing your organizations Cloud Strategy and aligning it to your adoption lifecycle of these activities should be evangelized across the organization and those teams and departments that are being affected by the cloud adoption. Your cloud lifecycle should support continual improvement through periodic realignment with your organizational strategy and evaluation of optimization and innovation opportunities.

|  |  |
| --- | --- |
|  | Cloud Adoption Lifecycle |

## The Journey

The journey thru the Cloud Lifecycle becomes one of continuous improvement. This goes beyond just simple TCO and ROI of the cloud platform and addresses the why aspects we mention above. Migration to the cloud and optimization of workloads is only half the story. The cloud opens all sorts of possibilities for innovation, which makes not only IT better, but provides direct benefit to the business, making the IT not just a cost center, but a real partner in driving value and growth for the business.

This partnership will drive the goal of any enterprise strategy: to create competitive differentiation and advantage. Technology will now drive transformative innovation thru the enablement of a global cloud platform and the services it contains, dwarfing what is capable within the private cloud. This transformational innovation will drive a different culture and approach that most organizations have today. It will influence IT, leadership of the enterprise, and any custodian or consumer that leverages the cloud.

The first part of this journey is to establish your strategy and goals you expect to achieve through the cloud and relate them to a lifecycle roadmap. This roadmap then defines the execution of the first iteration thru the buildup of your cloud lifecycle.

The last 2 key items of the lifecycle are to measure and improve. The journey to the cloud must be measured and continually improved, and at a much greater pace and scale than the traditional private cloud.

## Experimentation and Innovation

Competing agendas is the basis for cloud experimentation and innovation. On one side are the expectations as stewards and custodians of enterprise IT systems to maintain what has always been done, “keep the lights on.” On the other we are being driven to innovate, seize new opportunities, support evolving business needs, and better serve customers.

With the cloud, the balance between maintenance and innovation shifts. The reduction of effort around keeping the lights on allows for the focus on innovation.

Regardless of the risk-adverse nature of an organization, one that is moving to the cloud will find that the approach to support this innovation will be met if you adopt some specific Innovation Principles:

1. Go fast: The cloud enables projects to be deployed quickly, which enables a “try many, use best” to learn quickly.
2. Push the boundaries: IT needs to adapt to the cloud, embrace new architectures and processes, test limits, and support redesign and refactoring approaches
3. Data Driven: Use the monitoring and analytics capabilities of the cloud to find efficiencies and to assist with making decisions.
4. Keep it simple: Consolidate, centralize where possible, right size, and do not overcomplicate
5. Communicate: Success and driving cloud adoption will be met by ongoing and clear communication with stakeholders

There is no doubt that the public cloud has become a real differentiator and main driver for digital transformation, however cloud success will be established thru continuous improvement, innovation, and healthy conversation. Any great technological change involves much more than pure technology. It also requires a shift in culture, enterprise IT and application development processes, roles, governance, and engineering.

# Strategy & Goals

## Business Strategy & Cloud Strategy

Today, most organizations are utilizing the cloud to some extent, but many still rely upon legacy and outdated approaches to technology that they have been leveraged for many years. To achieve further adoption and drive an organizational change, enterprises need to develop a comprehensive plan for making the transition to a cloud-first way of working (public or hybrid). The cloud should become the preferred and prioritized model to be agile and flexible, improve business and IT performance, disrupt business processes, and adapt to the changing digital landscape. Evangelizing and supporting this approach with senior leadership, key application platforms, and core infrastructure teams will be vital to the cloud adoption lifecycle.

## Cloud Team

A key component to promote long-term commitment to the cloud journey is the creation and establishment of a Cloud Team within the organization. The cloud teams focus is to facilitate the enterprise adoption of the cloud thru analysis and experimentation. It supports the architectures that the business requires, design pattern construction, guidance for deployment, and to support the evangelizing and communication of the business and cloud strategies. The figure below is a recommended approach and charter areas of the cloud team to support.



The following Charter definitions describe the responsibilities of the Cloud Team:

*Cloud Innovation, Architecture, and Strategy*

*Evangelizes and drives adoption of the cloud investments across the larger organization while ensuring they are empowering and not handcuffing the business.*

*Cloud Security, Identity & Access Management*

*Definition, enforcement, and auditing of Security and Identity standards across the entire Cloud infrastructure.*

*Cloud Data Management & Protection*

*Ensuring data protection, backups, disaster recovery and business continuity as well as standard data security practices.*

*Cloud Governance & Compliance*

*Cloud governance assists with not only the financial management of cloud use, but also the enforcement and awareness of standards in the implementation.*

*Cloud Automation & Design Patterns*

*Support for the Business units through Azure Service Standards, quick start templates and configuration management.*

*Shared Service Offerings*

*Catalog of standard services provided through an automated provisioning interface enabling and empowering customers. (Networking, Security, Identity, Connectivity, Tenant Lifecycle Management, etc.)*

## Adoption Framework

Many times, defining the first steps forward for the cloud journey can be a challenge. Understanding where to get started first and what the priorities are can often provide unclear or overwhelming expectations at the beginning of the cloud journey. Built in concern with the Cloud Adoption Lifecycle is the Cloud Adoption Framework. This framework starts by decomposing the various high-level focus areas based on the Custodian and Consumer roles of the cloud. It is meant to assist and guide the process of adoption and help focus the conversations on the various areas of importance and responsibility.

*Cloud Adoption Framework*

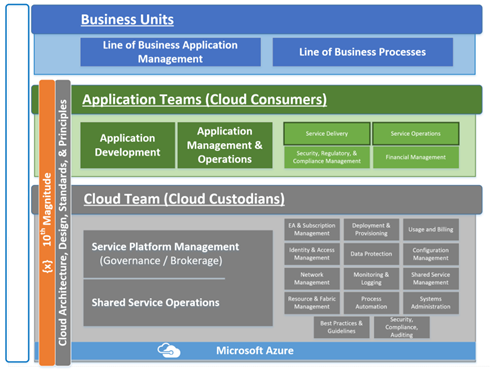


Within this framework 2 roles appear:

* Cloud Custodians (Cloud Team)
* Cloud Consumers (Business Units or Application Teams)

These roles have different definitions and contributions or responsibilities as part of the overall cloud journey.

The Custodian role focuses mostly around the horizontal and enterprise needs to enable the cloud, specifically Shared Service components to drive consistent and efficient sustainability. The Consumer role looks more vertical within their tenant structure and focuses on how to successfully deploy, lifecycle, and manage the workloads that are supporting business applications and workloads. Each role has their own components and each component requires definition on how both successfully implement workloads in the cloud.



|  |  |
| --- | --- |
| Cloud Team (Custodians)   * Enterprise Agreement and Subscription Management, Tenant Provisioning * Identity & Access Management * Financial Management – Usage and Billing * Network Management * Shared Services Management * Best Practices and Guidance * Security, Compliance, Auditing * Systems Administration * Data Protection | Application Teams (Consumers)   * Application Development * Application Management & Operations * Application Security, Regulatory & Compliance * Application Service Delivery * Application Service Operations |

|  |  |
| --- | --- |
| Cloud Consumers will also support responsibilities for the delivery and operations of their application platforms. This includes items such as capacity planning, data management, information security, CICD, and Application Performance Management. |  |

## Principles

Every journey to the cloud will hold several guiding principles to maintain a steady course. Here is a starting point to review for adoption:

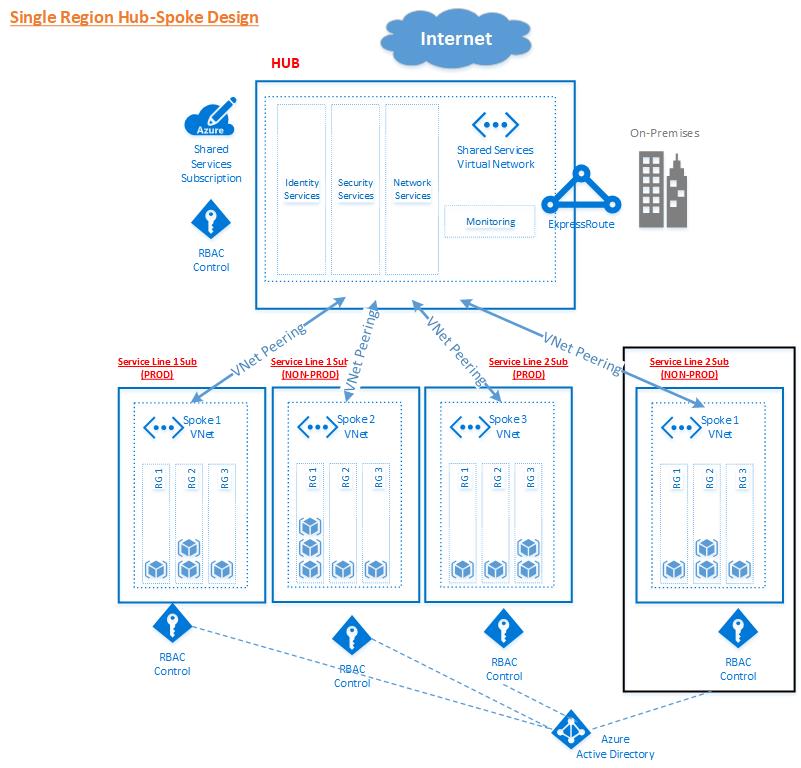
* Cloud Standards will support business requirements and development practices
* Cloud Strategy should build upon business objectives
* Clear rules and usage practices between Custodians and Consumers
* Adhere to Change Management expectations
* Continuous improvement cloud practices will be established
* Speed and Agility are critical for success
* Flexibility will lead to faster success
* New Technologies or capabilities lead to redefinition of expectations
* Secure by default & Least privilege access
* Solution Guidelines
  + Build for scalability, resiliency, and redundancy
  + Build for growth
  + Utilize Cloud native solutions where possible
  + Leverage existing hybrid toolset where necessary
  + Cloud First approach for new applications and Workloads

## Building and Executing the Plan

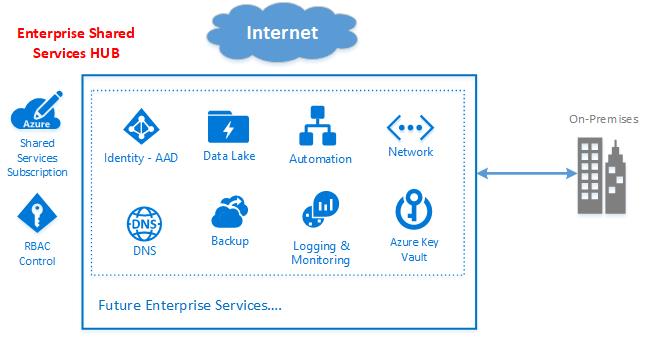
Now that the WHY has been framed, the next step of our journey is to build and execute the plan. Taking the current state of the public cloud and transforming it to the mature expectations that everyone has will be achieved thru an iterative and hands on process. The capabilities and components of the public cloud are fluid, change and update regularly to bring better and more features to be leveraged. The following documentation is to help guide that process of iteration and establish the starting point for us to launch from. We will take the current cloud environment and transform it into a stable, standardized, governed landing zone for enterprise production workloads. A key process to ensure that our core IT services can keep pace with the changing needs and wants of the business will be defined and cultivated thru the core cloud team. Ultimately creating a model that is scalable and flexible to support the business will be achieved by establishing and shifting to a shared services model. This model provides a defined set of Enterprise services to be shared with tenants in the Azure environment. Along with providing functional IT services, this model will help to build a foundation for the cloud and drive an appropriate layer of governance across the Enterprise cloud. The following portions of this document will focus on these aspects.

# Shared Services (HUB) design

The Shared Services Model is an approach that enables enterprises to successfully adopt the Azure cloud to scale, maximize cloud resource usage, reduce cost, and simplify aspects of governance. This model is based on Microsoft’s Virtual Data Center best practices and establishes a Hub-Spoke topology that provides shared services for downstream tenant consumption. It reduces duplication in terms of governance, networking, connectivity, and operations by centralizing not only the Azure services within a hub subscription model but looks to the establishment of a Cloud Team that will take on responsibility for the Shared Services administration and custodian broker and onboarding activities.



At the center of the shared services model is the Enterprise HUB which exists in its own subscription that will span globally across all Azure regions. It is recommended that H&P form a Cloud Team to take on management of the HUB. The HUB is purpose built to contain and offer all common services to the tenants that connect to it.



The benefits of the Shared Services model include:

* **Cost savings**by centralizing services that can be shared by multiple workloads, such as Active Directory Domain Controllers, Network virtual appliances (NVAs) and DNS servers, in a single location.
* **Overcome subscriptions limits**by peering VNets from different subscriptions to the central hub.
* **Separation of duties**between central IT (SecOps, InfraOps) and workloads (DevOps)
* **Separation of Non-Production and Production workloads**
* **Reduction of Operational Management** due to consolidation of shared services
* **Reduction of Dynamic Resource Consumption** for static/consistent services
* **Scalable and repeatable Cloud Architecture**
* **Consistent governance for consumption**

## Enterprise HUB and Shared Services

The HUB will be responsible for the delivery of all core services provided by the H&P cloud team. To provide a standardized service offering globally, the HUB should be replicated throughout all target regions with the same set of shared services. There will be no deviations in any region. Core shared services listed below are currently available in all Azure regions, any service that is not available throughout deployed Azure regions should be treated as an exception and incur additional scrutiny. This will allow the Cloud team to manage user expectations as to what services are provided. This will also allow for the opportunity to deploy an entire HUB using an ARM template. This type of automation will speed deployment and ensure that every HUB is deployed the same globally.

## Shared services to be offered (examples)

**Identity – AAD & IaaS AD:**  Azure Active Directory (Azure AD) is an identity and access management cloud solution that provides directory services, identity governance, and application access management. IaaS AD and Advanced Threat Analytics will also be provided.

**DNS**: Azure native DNS as well as H&P corporate DNS servers

**Network**: Express Route gateway connection links or VPN’s to H&P locations will be provided. If traffic inspection and firewall protection are needed it is recommended that these devices are placed within the HUB. This reduces overall cost and complexity by allowing all spokes to leverage these devices.

**Management:** It is recommended that there be a centralized OMS offering. OMS provides native tools to manage logs, alerting, automation, backup, and high availability.

The above services should be provided to tenants within the first iteration of the Enterprise HUB. As Azure continues to grow and more services are added it will be the H&P Cloud team who will decide if a new or existing service should be managed and provided through the Enterprise HUB. In addition to monitoring what Microsoft provides, the Cloud team should perform proactive monitoring of services that tenants are consuming as well as soliciting regular feedback from tenant owners about offerings that they would like to see offered as a shared service. Regular touchpoints will keep H&P IT and tenant owners engaged with one another and will help continue to evolve the shared service offering.

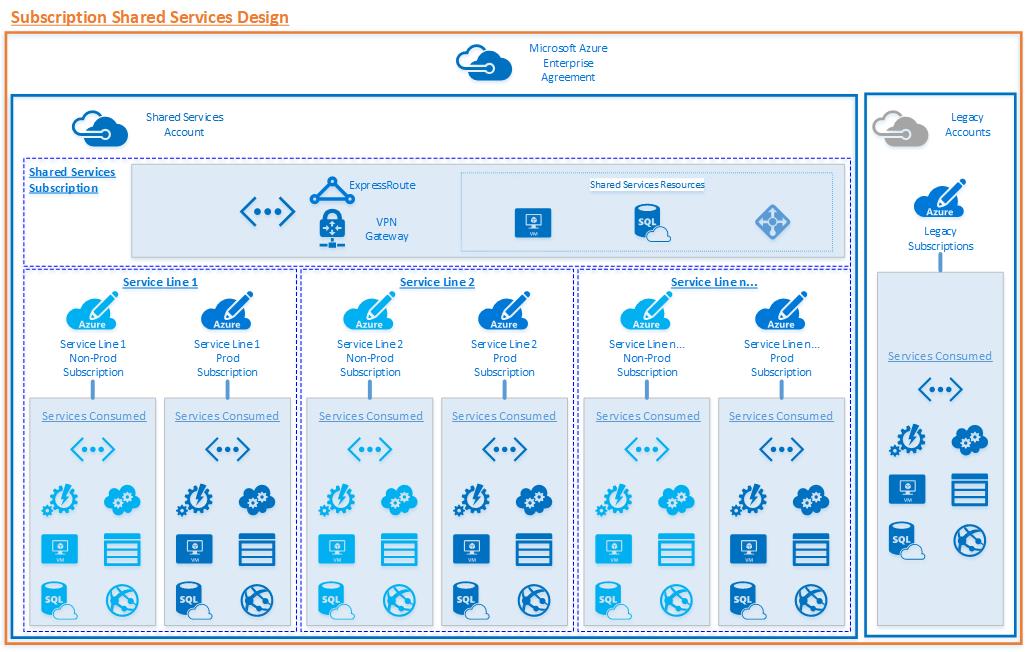
Enterprise Agreement and Subscription Hierarchy

The foundation of every Azure Enterprise is the Enterprise Enrollment and Subscription structure held within. This EA and Subscription hierarchy will define how an organization subdivides its environment and resources into groups to account for proper access, financials, and resource management characteristics. Its structure can also be accounted for to allow the organization to grow and scale without meeting the Azure limitations. The EA account and subscription hierarchy outlined here will allow for an organization to adopt the shared services model.

The goals of a new model will address those observations as well as account for the following:

* A shared services hosting model to reduce duplication, allow for a repeatable governance structure and processes, and outline transparent data points to be provided around resource management
* Establish a granular financial reporting model that allows tracking to the cost center
* Establish and support security best practices, including enterprise security posture
* Define Regional Replication partners and target approved azure regions for deployment
* If legacy accounts and subscriptions may exist – review and document their current abilities and gaps from the new shared services model; then align a path to support and incorporate them into the corporate standards.
* If legacy workloads will not be modified or adjusted without proper review, alignment, and understanding by current subscription and workload owners and a schedule set to remediate.
* The shared service subscription model will support both a multi-tenant non-prod/prod hosting model as well as a single-tenant non-prod/prod hosting model (where applicable)
* Avoid dynamic components of consumer requests and try to enforce static and reliable aspects of the architecture – Subscription management/provisioning, Hub/Spoke Networking delivery, Financial and inventory management, Auditing/Monitoring, etc.
* Eliminate single points of failure and missing availability requirements

Example of recommended account and subscription topology is pictured below:f



This model moves towards a shared service and tenant model that Service line/business unit participate in. Each group will be able to align workloads as production and non-production and place them in the appropriate subscription (production/non-production).

This allows for granular administration roles for non-prod vs. prod workloads at the highest or lowest levels, enables a runway for scale and growth, and transitions many of the dynamic components of an onboarding request to static and reliable foundational pieces of our delivery.

**Why use subscription as a logical descriptor?**

As part of the overall cloud design at H&P, we have chosen to leverage the subscription as a “logical description” of a service line/Business Unit within the organization. Major factors for this decision are continued segregation of service line/business unit and overall size of the organization. A single H&P subscription could exceed Azure limits especially when combining production and non-production workloads.

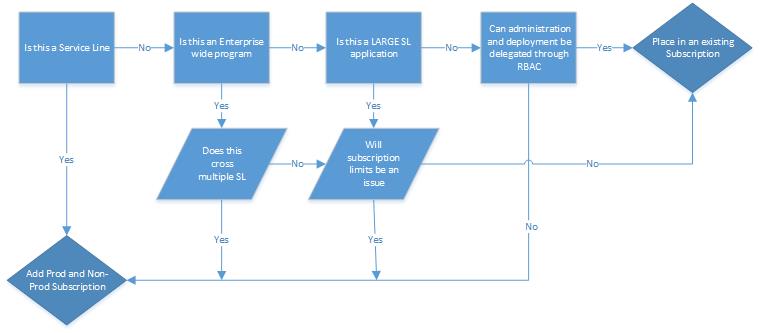
Because of these factors, we looked further down into what described the organization. A collection of separate and distinct service line/business unit make up H&P as a whole. Each service line functions as their own tower within the organization.

Service line/business unit were further broken down into a production and non-production subscription. The reasoning is as follows:

1. Workload Protection – Production workloads must be secure and safe
2. Azure Limits – Because of the size of a service line, limits still play a critical role determining the subscription breakdown
3. Security – By providing separate subscriptions for production and non-production workloads, we can provide a different security posture on the non-production subscription.

**Key Recommendation:** The major driver to allowing a non-service line to request a subscription should be to avoid subscription limits. Other than hard subscription limits, most concerns can be addressed within an existing SL subscription. If the environment were to fall into a “subscription as a service” offering, it could cause issues with IP addressing and statically assigning networks to tenants.

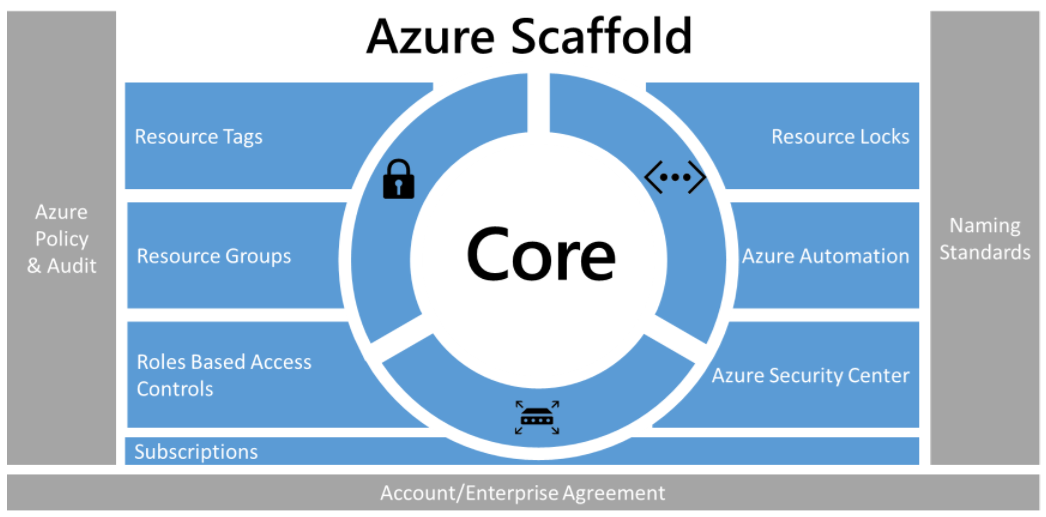
There are times when a service line is not the correct descriptor. Managing the logical boundary of the SL at the subscription will help with reporting, financial management, and administration. As Service line/business unit and H&P in general look for ways to reduce duplication efforts, draw on SL strengths, and integrate applications across H&P; service line boundaries will start to blur. Enterprise level programs can warrant their own subscription within Azure. In our subscription decision flow, Enterprise programs would cross multiple SL boundaries and there would also be concern that it could exceed Azure subscription limits. Creating subscriptions for the program would allow for easier financial management (reporting and billing) as well as address the concerns about resource group placement – what SL owns what portion of the workload and will more importantly address subscription limits.



|  |  |
| --- | --- |
| **Key Recommendations** | |
| **Enterprise Account/Subscription Best Practice Guidance** | * Keep Subscriptions to a minimum to reduce complexity * Do not create multiple subscriptions just to separate billing or RBAC * Do not use a subscription as a primary method for delegating administration * Avoid spanning applications across subscriptions (unless it is a “program subscription”) |

Governance and Security fundamentals within Azure

*“Cloud security is a shared responsibility - although Microsoft Azure delivers an extremely secure environment, YOU need to protect what you put IN the cloud—your workloads.”*



Working within the Azure Scaffold, security encompasses a few rungs.

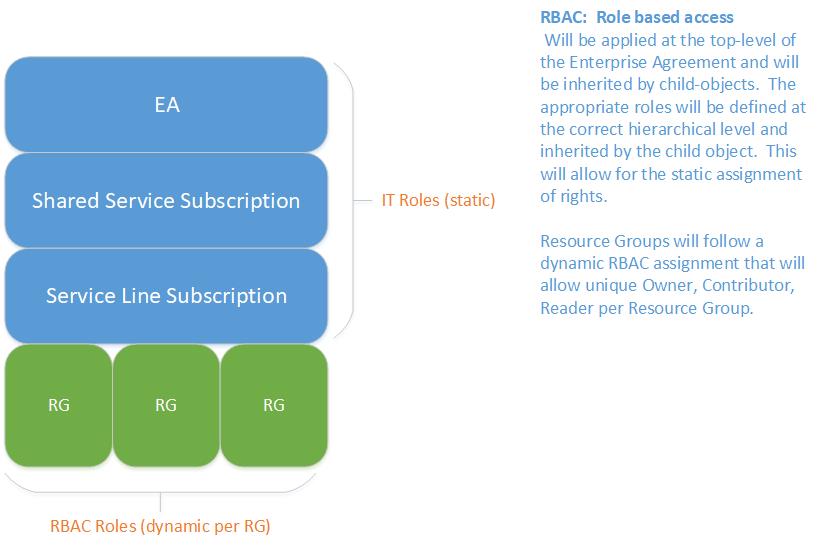
1. Role Based Access (RBAC)
2. Resource Locks
3. Azure Security Center (recommendation is to leverage free version because of current H&P toolsets)

Along with these rungs we can apply some broader security best practices to secure Azure workloads.

1. Segregation of Duties in Production (Can be applied at other subscription environments – ie. non-prod)
2. Least privilege access
3. Collecting data (logs) and alerting on meaningful action

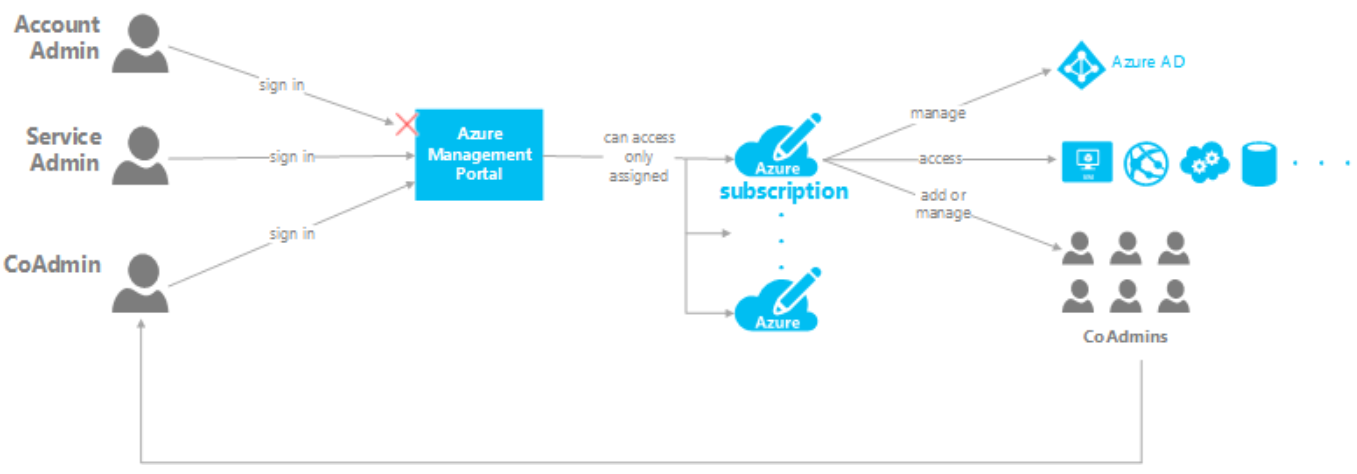
**Applying a consistent RBAC policy**

The goal of security-minded organizations should be to give employees the exact permissions they need to do their jobs. By creating a hierarchical RBAC policy we are able to provide a static implementation of rights higher up within the environment while allowing resource group/application owners to control their respective resources. Following the segregation of duties and least privilege models, services and resources can be secured and protected from modification and improper access.



**Enterprise IT Role Based Access (RBAC)**

Within the new HUB/SPOKE model it will be important that RBAC policies are enforced at different “levels” within the Azure environment. Enterprise RBAC (eRBAC) will be used for resources higher up the Azure stack – subscriptions and the EA portal. Subscription and EA portal modifications can have far-reaching impacts if changes are made. It is critical that the appropriate people only have access at these levels.



|  |  |  |  |
| --- | --- | --- | --- |
| **Enterprise IT RBAC** | | |  |
|  | **Group** | | **Role** |
| **Enterprise Subscription** | | Cloud Admin – Track Lead | Owner |
| **Shared Services Subscription** | | Enterprise IT | Contributor – mapped to appropriate Enterprise group |
| Cloud Admin – Track Lead | Owner |
| **Business Unit Subscription** | | Enterprise IT | Contributor – mapped to appropriate Enterprise group |
| Cloud Admin – Track Lead | Owner |

By leveraging RBAC at the resource group level, we will be providing the owner with the abilities they need to manage resources and access. At resource group creation, role groups for owner, contributor, and reader will be created and applied to all resource groups.

The following roles will be created:

|  |  |
| --- | --- |
| **Resource Group RBAC** | |
| **Role** | **Description** |
| **rg\_Owner** | Full access to all resources including the right to delegate access to others. |
| **rg\_Contributor** | Create and manage all types of Azure resources but can’t grant access to others. |
| **rg\_Reader** | Can view existing Azure resources. |

The “rg roles” will be populated with the owner’s corresponding Azure Active Directory group. During the creation of the tenant, if AAD groups are provided for the contributor and reader roles, they will be applied as well. Once the resource group has been turned over to the owner, the owner will have the ability to grant access as he/she see fit and define what groups belong to a particular role. This is an extremely important concept of the HUB/SPOKE model. This takes access administration out of the hands of the centralized IT group and places this administrative duty to the resource group owner. This allows the resource group owner to manage their roles as they see fit without the reliance on a central identity administration team.

Included in the ARM template base networking package is an RBAC template which will accept the input of a user or group RBAC object ID and assign that group either Owner, Contributor, or Reader access to a resource group.

**Azure Resource Policies**

Resource policies enable you to establish conventions for resources in your organization.  For example, you can specify that only certain types of virtual machines are allowed, require that all resources have a particular tag, restrict the deployment to a given (set of) region(s) or enforce that storage accounts are setup with encryption.

**How is it different from RBAC?**

There are a few key differences between policy and role-based access control (RBAC). RBAC focuses on user actions at different scopes. For example, you are added to the contributor role for a resource group at the desired scope, so you can make changes to that resource group. Policy focuses on resource properties during deployment. For example, through policies, you can control the types of resources that can be provisioned. Or, you can restrict the locations in which the resources can be provisioned. Unlike RBAC, policy is a default allow and explicit deny system.

# Azure Policy - Description

Azure Policy is a service in Azure that you use 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. Azure Policy meets this need by evaluating your resources for non-compliance with assigned policies. Once a policy is implemented, new and existing resources are evaluated for compliance.

Policy focuses on resource properties during deployment and for already existing resources. Unlike RBAC, it does not limit “who” can take action against a resource.

# Azure Policy Composition

A policy is comprised of two distinct parts

1. **Policy definition**

A policy definition is a JSON formatted template that defines what conditions it will enforce and what the effect will be if these conditions are met

1. **Policy assignment**

A policy assignment is a policy definition that has been assigned to take place within a specific scope. This scope could range from a management group to a resource group. The term scope refers to all the resource groups, subscriptions, or management groups that the policy definition is assigned to. Policy assignments are inherited by all child resources. This design means that a policy applied to a resource group is also applied to resources in that resource group. However, you can exclude a subscope from the policy assignment.

# Azure Policy Initiatives

## Initiative Definition

An initiative definition is a collection of policy definitions that are tailored towards achieving a singular overarching goal. Initiative definitions simplify managing and assigning policy definitions. They simplify by grouping a set of policies as one single item.

## Initiative assignment

Like a policy assignment, an initiative assignment is an initiative definition assigned to a specific scope. Initiative assignments reduce the need to make several initiative definitions for each scope.

# Recommendations

As the policy engine has matured and the types of resources that can be brought under compliance has expanded, 10th Magnitude has moved away from assigning individual policies in most cases. We have found that Azure Policies tend to have most impact when they are thought of as “a broad stoke that is applied at a high level”. One way to accomplish this is to think in terms of “Policy Initiatives”. This allows for a larger view of what is trying to be accomplished. Many policies could make up a single initiative and this grouping helps the implementer address a posture and not just a single element. Initiatives also significantly reduce clutter and noise in the Policy portal when viewing a subscription. Policies roll up to an initiative and are not front and center in the standard view. This helps with getting the pertinent information to the user while still allowing them to drill down when needed.

Policies are often used to try and account for every action or circumstance that an organization is trying to safeguard against. This mindset while well intended, almost always fails because of the complexity that it introduces. We have found that policy is best implemented when thought of as another lens to view your deployment. It should provide actionable data to the user and provide them a point of reference as to where they need to take action. In most cases it should not be used to enforce standards that have one-to-many parameters.

## Suggested Initiatives:

### 1. Security Center

Enabling security center by default creates the "ASC Default" initiative within the Azure policy center. This initiative has ~80 built-in policies that monitor compliance across VM, SQL, network, storage, accounts, etc. and feed this data into Azure Security Center.

### 2. Diagnostic Logging

Enabling diagnostic logging on resources and feeding that data in Log Analytics allows for a better view into the environment's overall health and potential issues. Having a single source of truth where all of your diagnostic data rests is critical for the operationalization of Azure. Azure dashboards, alerts, and monitors are dependent on having low-level diagnostic logs to function at peak

Create an initiative that checks that diagnostic logging is enabled and sending to the correct landing zones - Log Analytics, storage accounts, event hubs

### 3. Governance

Enabling policies that help to align your deployment with organizational standards. Governance policies should be used to assert standards on your Azure deployment.

Examples could be:

* Ensure that tags are on a resource
* Ensure that every resource has a cost center
* Do not deploy resources with a certain sku
* Enforce what region a resource can be deployed to

### 4. Network

Enabling policies that keep your networking assets in-line with your best practices. We tend to populate this initiative with policies that monitor, protect, and enforce our network posture.

For example, this initiative could contain policies to

* Validate that DDoS protection is enabled
* Network Watcher is enabled in the deployment region
* NSG's are applied to a vNet

**Azure Resource Locks**

Part of security is not only protecting high value assets from people outside of the organization but, also having safe-guards in place to protect from “friendly fire” within the organization. This is extremely important within the shared services subscription. By extracting common services from service line ownership and moving them to a central location for ALL lines of business to interact with, we have made them a crucial part of the Azure infrastructure within H&P. Another feature of Azure is the ability to apply a lock on a resource. There are two types of locks available:

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

With the change from a dynamic to a static environment, resource locks are an important tool to protect a resource without causing administrative overhead. Locks should be placed on high value assets that are static in nature – critical network infrastructure, VMs that host DNS or Active Directory.

**Logging for security**

Within Azure there are specific logs that will be important to capture to show changes within the environment that may pose a security violation. These logs are important for providing security around subscriptions.

Key Logs for subscription security:

* **Control/management logs -** give visibility into the Azure Resource Manager CREATE, UPDATE, and DELETE operations. [Azure Activity Logs](https://docs.microsoft.com/azure/monitoring-and-diagnostics/monitoring-overview-activity-logs) is an example of this type of log.
* **Data plane logs -**give visibility into the events raised as part of the usage of an Azure resource. Examples of this type of log are the Windows event System, Security, and Application logs in a virtual machine and the [Diagnostics Logs](https://docs.microsoft.com/azure/monitoring-and-diagnostics/monitoring-overview-of-diagnostic-logs) configured through Azure Monitor
* **Processed events -**give information about analyzed events/alerts that have been processed on your behalf. Examples of this type are [Azure Security Center Alerts](https://docs.microsoft.com/azure/security-center/security-center-managing-and-responding-alerts) where [Azure Security Center](https://docs.microsoft.com/azure/security-center/security-center-intro) has processed and analyzed your subscription and provides concise security alerts

Recommendation is that these logs are captured and sent to OMS or other logging solution (LogRhythym) for retention and further alerts/actions to be taken.

**Shared Services vs. Tenant model follows “security by default”**

One of the major benefits of adopting the Shared Service/Tenant model is that it builds in some default security boundaries and allows key services to be protected by default.

Following the tenant model, we limit the amount of damage that “friendly fire” can impact the business. Anything outside of a user’s tenant cannot be modified which provides a security boundary and keeps the rest of the organization safe.

Another key design feature of this model is that each service line will be provisioned a Production and a Non-Production subscription. This will allow for business-critical applications and data to be fully segregated from lesser environments that do not need to maintain a higher security profile.

**Microsoft Security Center**

Leverage and develop the use case surrounding Microsoft Security Center.

10M recommendation to continue with the standard version of security center in order to receive data on threat detection within:

* Networks
* Virtual Machines
* SQL Databases
* Windows crashes

This data should be sent to OMS for further dashboard buildouts and actions

**Security Maturation**

Security needs to be top of mind for an organization. As part of 10M’s recommendations we encourage the H&P cloud team to adhere to an accepted security framework. By continually updating the H&P security posture to follow a well-reviewed cloud based security framework, the number of vulnerabilities and attack vectors within the environment will continue to shrink.

Framework adoption should become a key initiative with H&P and would benefit from executive sponsorship. At this point in the organization’s cloud maturity, it may be more beneficial to look over a framework and start working to achieve an agreed upon number of controls. By developing a focus on security and gaining momentum through continually working to add security controls within the environment, it will be easier to transition to a fully scoped security initiative within the cloud.

\*10M has provided the **Cloud Consumer Security matrix** as an example of specific control statements and use cases recommendations for implementation (see appendix)

# Consumption and Financials

Managing a cloud infrastructure means looking at how you make budgetary decisions in a new way. Core to those decisions are being able to relate budgeted vs actual resource consumption. By collapsing workloads into appropriate subscription and applying a standardized tagging policy, we can visualize the data in a meaningful way and make an informed analysis. This tagging standard will also allow for further granularity for bill back and chargeback processes.

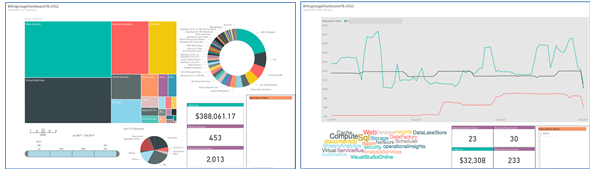
**Financial Overview:**

One of the major advantages of adopting the new Azure model will be the ability to perform granular financial analysis within the environment. There are a few important changes that will allow for this new type of modelling.

1. Tagging policy
   1. Cost center tag applied to resource group (enforced)
   2. Ability to separate full environments into a resource group to track financial spend
2. Production and Non-production workloads are split into separate subscriptions to all for more insight as to where consumption is happening

By adhering to tagging policies and deploying workloads within a tenant boundary we will be bringing a new lens on Azure consumption spending.

**Dashboards**



By following the Enterprise tagging standards per a tenant, we will be able to slice workloads out of subscriptions and show where spend/consumption is happening, down to the resource group level. Dashboards will be a critical component in aiding key business decisions around capacity planning and budgeting.

## Cloud Consumers

As the Azure environment at H&P evolves, one of the fundamental questions that the Cloud team will need to continually ask and answer is

Is this something that our consumers want and how does this help our customers?

By focusing our attention on the needs of our customers we will be better able to predict what is next for our platform and be a significant value add for the Enterprise.

A cloud consumer cares about and expects the following:

1. Having an easy way to request an Azure environment
2. Being able to deploy what they want, when they want, how they want
3. Having insight into what their resources/environment costs
4. Adopting enterprise standards without adding administrative overhead
5. Speed

A cloud custodian cares about and expects the following:

1. Understanding of the workload that is deployed
2. Enterprise standards adoption
3. Understanding the criticality and business impact of a workload
4. Defining the data that an application is consuming/creating

Moving towards Enterprise Application Robustness.

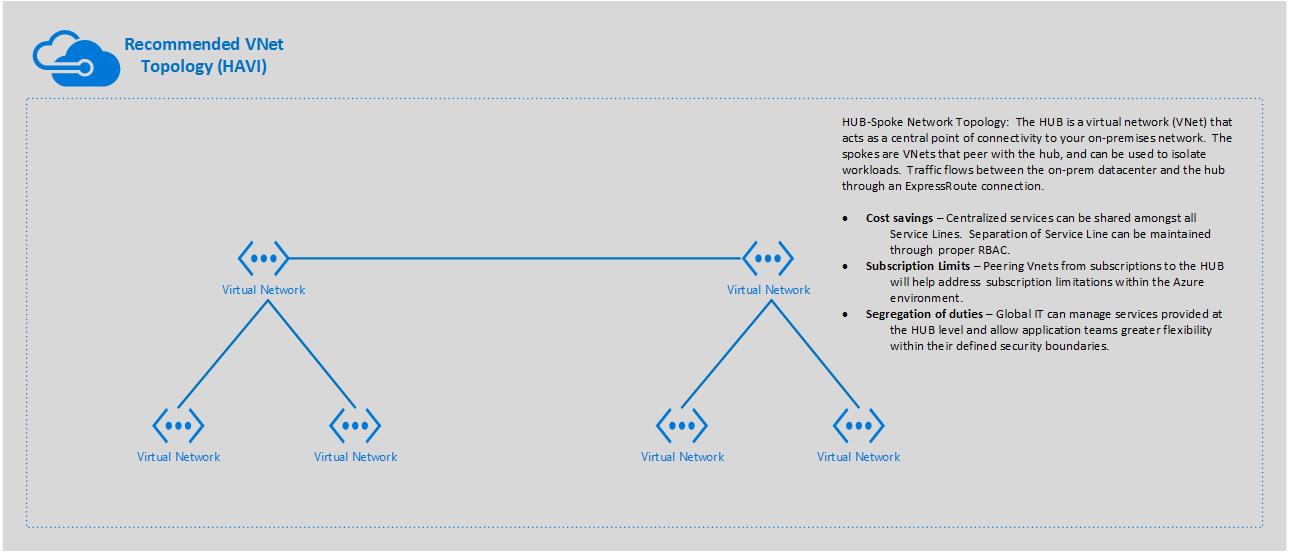
The goal of the new H&P Azure environment is to provide a completely stable and robust platform to application teams. While this is the goal, it is important to recognize that a platform with perfect uptime is not possible and we must account for that within application design, deployment, and operation.

Cloud consumers can proactively manage service interruptions by utilizing telemetry data and understanding how all of the resources within their workload function and their inter-dependencies.

|  |  |  |
| --- | --- | --- |
| **Recommendations** | | |
| **Goal** | **Action** | **Result** |
| Reduce outages and impacts to the business | Understand and take action against alerts provided within base monitoring profile | Improve MTTR (Mean time to resolution) for application workloads |
| Optimize application user experience | Develop telemetry monitoring on KPI (key performance indicators) within the application workload | * A better understanding of overall application health and performance. * Better understanding of where issues are occurring during an outage/problem * Ability to forecast growth needs of a workload based on performance data |

## Networking within the Shared Service (HUB) model

**HUB-to-HUB communication**



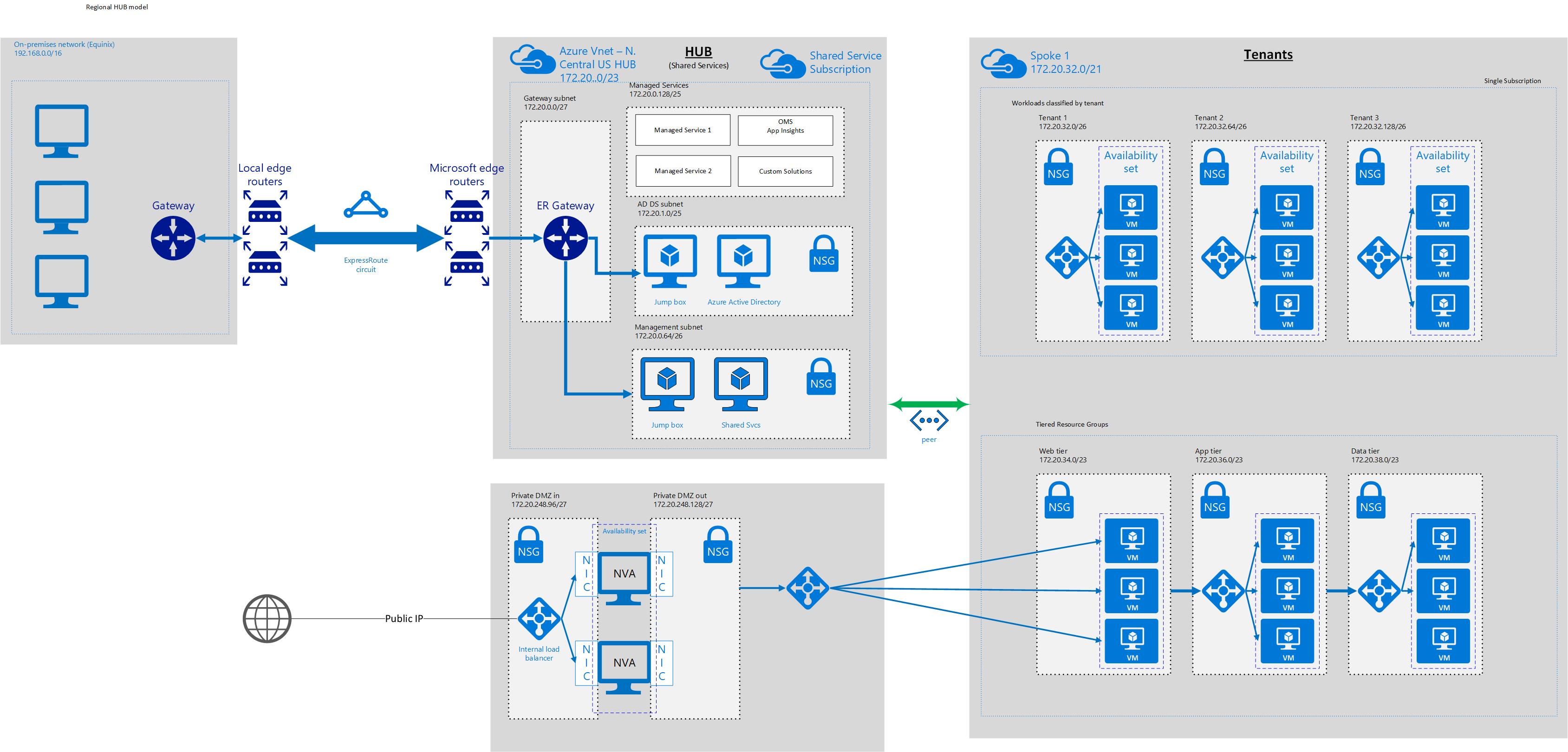
HUBs within the H&P Azure environment should be meshed and allow for HUB-to-HUB communication via ExpressRoute connections. This will allow for specific use-cases to be met, for example:

* **Replication** - An application that is globally deployed and requires replication of some item (IaaS or IaaS SQL) then it then can to travel over the private networking from hub to hub, over ExpressRoute connections managed at the HUB level.
* **Third Party NVA Networking** - GSLB, LB, or communication/redirection between those products over private networking.

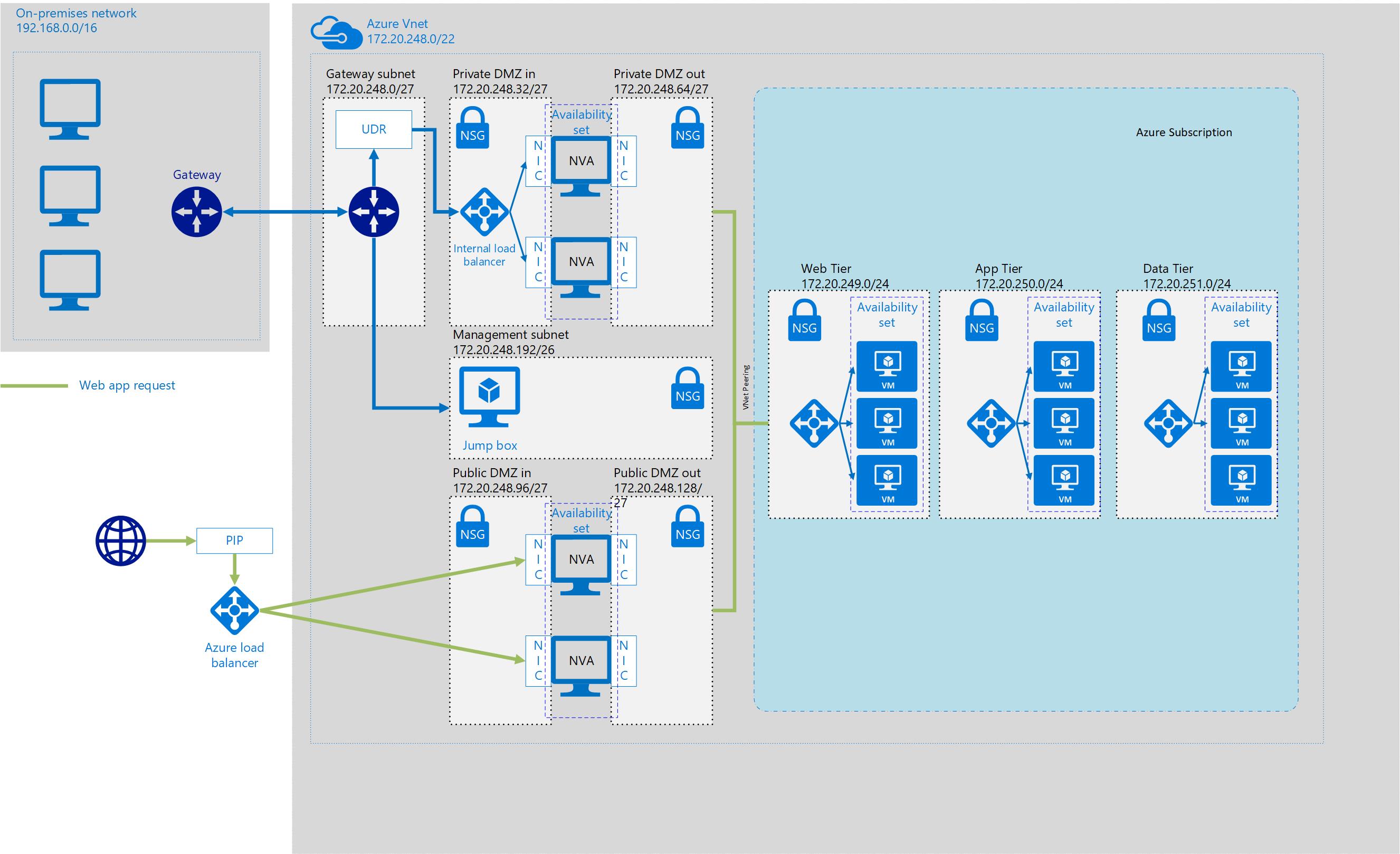
**Key Recommendations:**

* ExpressRoute connections should be made at the HUB level and limited to the “active” regions (N. Central US, West Europe, UK South). Secondary HUBs should be connected via VPN to reduce ExpressRoute costs and still allow for redundancy.
* It is strongly recommended that peering ONLY happen between a subscription (SPOKE) and the shared service subscription (HUB). Peering should not be done between subscriptions (SPOKES). This type of connection causes additional routing complexities and challenges and is not needed.

**HUB Network flow** (Example of centralized HUB offering)



DMZ offering (Example – Breakout from overall HUB diagram)

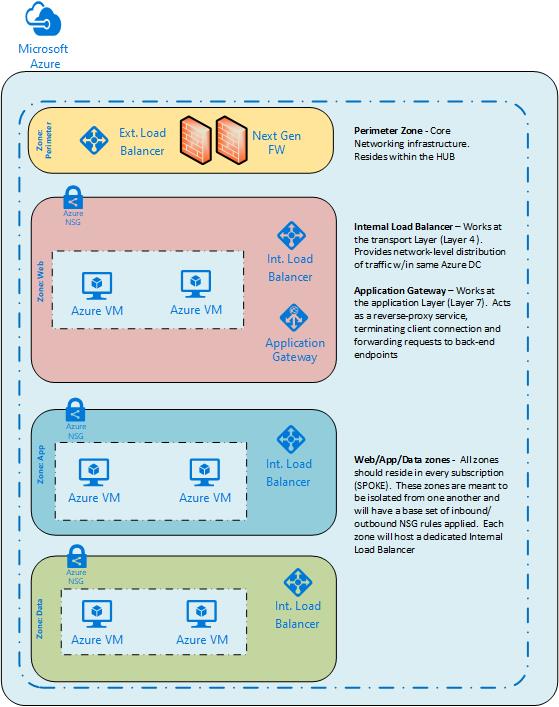


As part of the Shared Service offering, it is recommended that a public facing DMZ zone be provided. The DMZ would provide Internet facing communication between all Spokes within the H&P Azure environment.

|  |  |  |  |
| --- | --- | --- | --- |
| **Key Recommendations** | | | |
| **Topic** | **Business Input** | **Action** | **Risk** |
| Share DMZ amongst Spoke subscriptions |  | Create single DMZ tenant |  |
| Scale NVA appropriately within an availability set |  | Plan accordingly for growth | More difficult to expand NVA after the fact when not part of an availability set |
| Reduce traffic risk profiles (Internet vs. on-prem) |  | Create separate NVA sets for traffic originating from the Internet and traffic originating from on-prem |  |
| Determine DMZ need for overall business | Does DMZ need to be part of every HUB | Create single DMZ for ALL HUBS to share with a meshed HUB over ExpressRoute | Can run into latency |

**Network Traffic Flow (layered security model)**

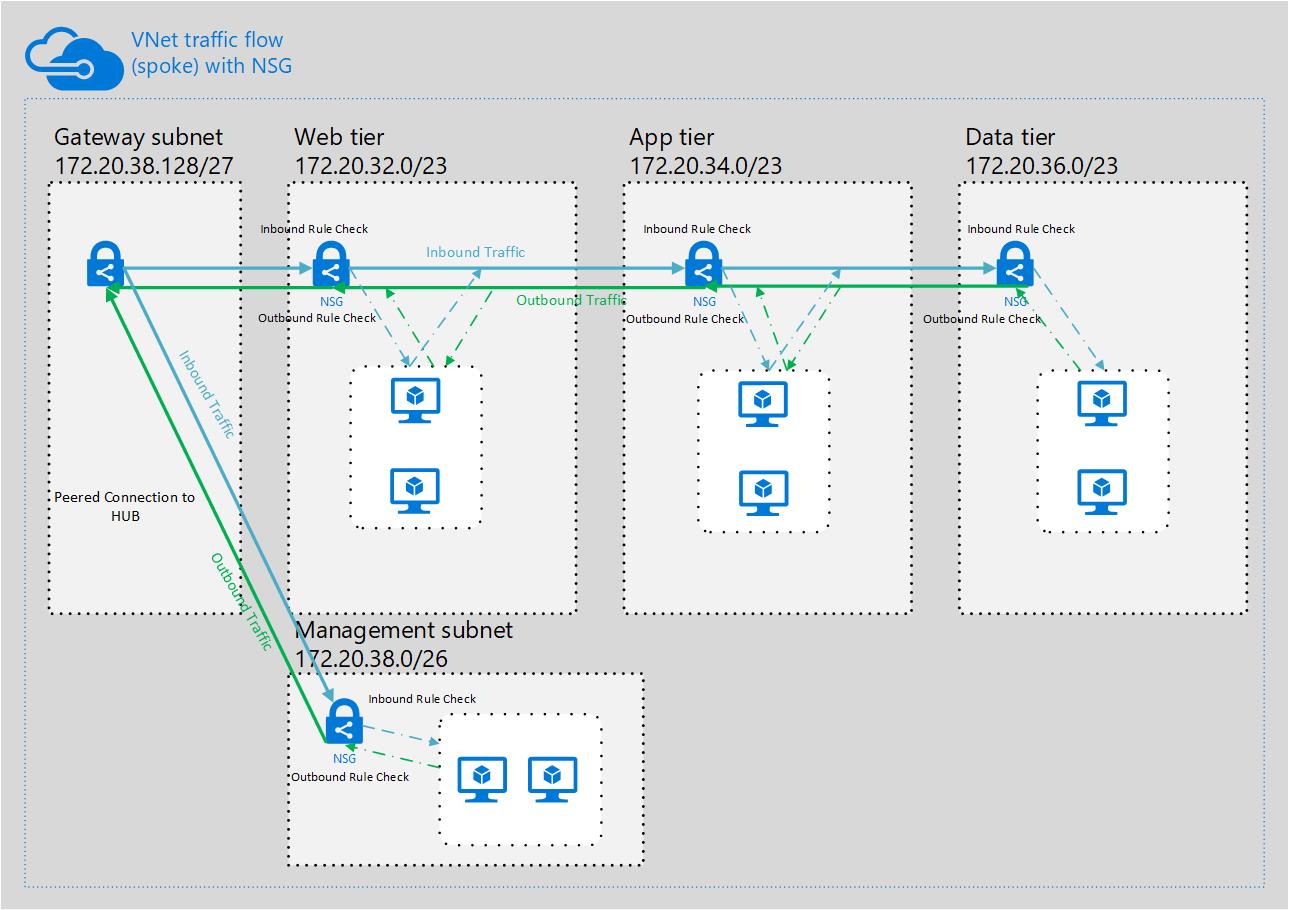
Best practice: Use Network segmentation and adhere to a three-tier design to protect data. Leverage NSG’s to control network access between subnets via inbound/outbound rulesets.



**Network Security Groups**

**Network Security Group (NSG):** is a set of Access Control rules that exist at the VM or subnet level that determine whether to allow or deny a packet.

Default network security groups will be applied at the web, application, and data levels for each business unit. This will allow for default rules to be placed at the subnet level to allow or deny traffic flows. This will also all for logs to be captured and sent to the shared subscription Log Analytics workspace for ingestion. This capture will show ingress and egress IP traffic and provide insights into the environment.



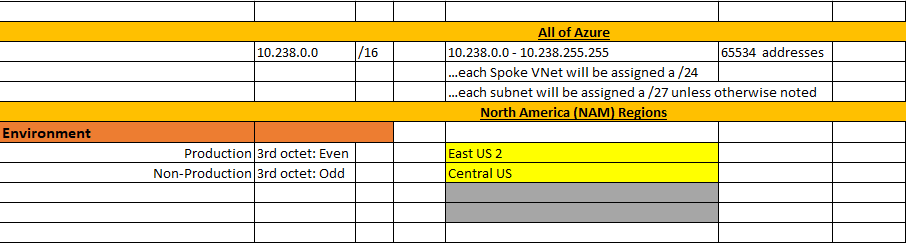
**Global IP Address Schema**

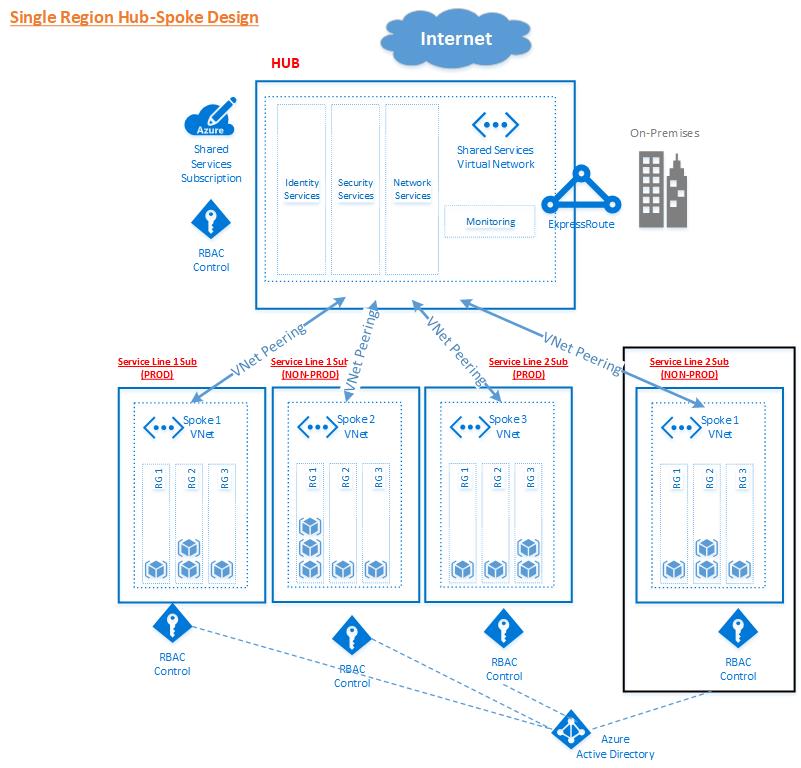
Once the region decisions had been made, we then were able to start assigning larger networks. The goal of providing larger network segments and dividing them up are:

1. Provide the correct number of IP addresses down to the tenant level
2. Plan for growth within a region
3. Reduction in required routing at the H&P core

Being able to describe networks at a higher level (/12 or /14 network) fulfills the above requirements

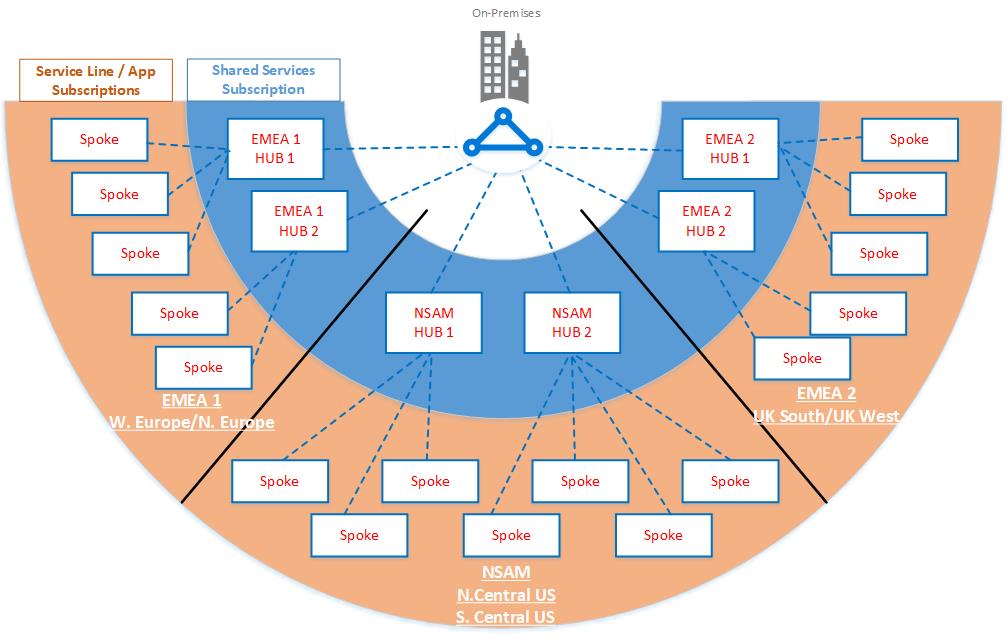
Below is the current IP address broken out for the NSAM region. This will be the first buildout of the model.





The diagram above depicts the VNet peering done from Enterprise HUB to the Service Line subscriptions. While the peering enables simplified routing and communication to/from other subscriptions (subscription cross-talk), we are also able to take advantage of statically assigning network segments to subscriptions. This assignment will be managed by the networking resources within the H&P Cloud team. Each Service Line spoke will be assigned a /21 segment. This segment size equates to 2046 addresses. Out of these addresses, smaller networks will be assigned to each tenant. Every tenant will have different needs as far as number of addresses are concerned so in order to supply addresses in the most efficient manner, we will adopt a two-sided assignment policy:

## HUB/Spoke subscription topology

****

Azure architectural decisions should be owned by the H&P cloud team. One of the critical environmental decisions is where workloads should be deployed. Understanding business drivers, services, and business continuity needs are key to choosing a deployment region. Once a region has been chosen there should be policies placed on the subscriptions that limit deployments to approved regions. If there is a business request and it is determined that there is a significant driver to deploy outside of an approved region, the policy lock can be removed at the resource group level to allow the deployment to continue. This should be an exception. Core services such as private network and identity should only be offered through peering subscriptions back to the Enterprise HUB.

The Enterprise HUB should be the centralized point where CORE services are provided. CORE services consist of private networking, ExpressRoute connections, identity, and other services provided by H&P on-prem systems.

The H&P cloud team will need to determine a set of criteria that will determine when to deploy a HUB to a new region. Reasons for deployment into a new region could be:

* New business that will depend on services being geographically close to end-user
* Data security requirements
* A service that is only available in a specific region (many applications within H&P need it and will also require CORE services)

It is recommended that the Cloud team handles all onboarding of tenants through and automated fashion, this can be the first stop gap as to determining when the deployment of a new regional HUB is warranted.

**Key Recommendation:**

* Each HUB be deployed to an Azure Paired region
* A separate HUB and Spoke environment will be built for POC and testing purposes

## Azure Paired regions

Azure operates in multiple geographies around the world. An Azure geography is a defined area of the world that contains at least one Azure Region. 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.

We recommend that you replicate workloads across regional pairs to benefit from Azure’s isolation and availability policies. For example, planned Azure system updates are deployed sequentially (not at the same time) across paired regions. That means that even in the rare event of a faulty update, both regions will not be affected simultaneously. Furthermore, in the unlikely event of a broad outage, recovery of at least one region out of every pair is prioritized.

Benefits of paired regions

**Platform-provided replication**- Some services such as Geo-Redundant Storage provide automatic replication to the paired region.

**Region recovery order**– In the event of a broad outage, recovery of one region is prioritized out of every pair. Applications that are deployed across paired regions are guaranteed to have one of the regions recovered with priority. If an application is deployed across regions that are not paired, recovery may be delayed – in the worst case the chosen regions may be the last two to be recovered.

**Sequential updates**– Planned Azure system updates are rolled out to paired regions sequentially (not at the same time) to minimize downtime, the effect of bugs, and logical failures in the rare event of a bad update.

For the H&P Azure deployment, we have broken down the required global deployment into three regions with corresponding regional pair:

|  |  |  |
| --- | --- | --- |
| **HUB Recommendations** | | |
| **Reduce organizational complexity** | Create a single HUB to be shared among all Service line/business unit | * Cost reduction * Less infrastructure to support * Single Cloud team * Service Line boundaries can be enforced with routing and RBAC |
| **Plan for disaster** | Deploy HUBs to paired regions | * Allows applications or workloads to leverage native Azure BCDR technologies |

## Dealing with legacy workloads within Azure

While the new HUB/SPOKE model is being built the business is still operating and that means that at some point there will be a need to migrate legacy workloads into the new shared service model. One of the tools that can be leveraged is an Azure to Azure migration using Azure Site Recovery (ASR). ASR allows for vm’s to be migrated between regions and can help to consolidate legacy workloads into approved H&P regions.

It will be critical to fully understand the current network topology and if it can be migrated into the new environment or will migrating workloads need new IP addressing. While planning the migration there are two options available

* **Use different IP address:** You can select to use a different IP address range for the replicated Azure VM network. In this scenario, the VM gets a new IP address after failover, and a DNS update is required.
* **Retain same IP address:** You might want to use the same IP address range as that in your primary on-premises site, for the Azure network after failover. Keeping the same IP addresses simplifies the recovery by reducing network related issues after failover. However, when you're replicating to Azure, you will need to update routes with the new location of the IP addresses after failover.

**Retaining IP addresses**

Site Recovery provides the capability to retain fixed IP addresses when failing over to Azure, with a subnet failover.

* With subnet failover, a specific subnet is present at Site 1 or Site 2, but never at both sites simultaneously.
* In order to maintain the IP address space in the event of a failover, you programmatically arrange for the router infrastructure to move the subnets from one site to another.
* During failover, the subnets move with the associated protected VMs. The main drawback is that in the event of a failure, you have to move the whole subnet.

**Key Recommendation:** Further discussion around current network topology and IP schema will be needed in order to plan appropriately for migrations.

## Monitoring and Logging

Diagnosing and troubleshooting issues in modern online applications is more complex than in traditional client-server applications because they include:

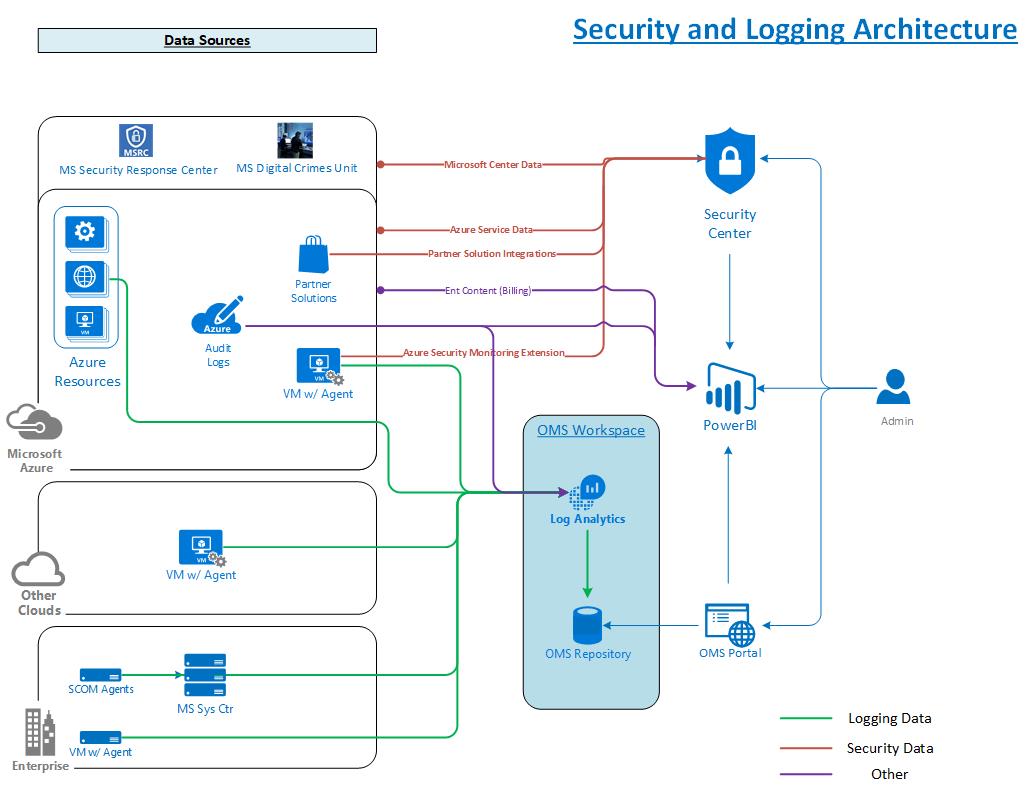
* Complex topologies with components running PaaS or IaaS infrastructure, on-premises, on mobile devices, or some combination of these
* Network traffic that traverses public and private networks; including devices with unpredictable connectivity
* Multiple storage technologies such as Microsoft Azure Storage Tables, Blobs, Queues, or Files in addition to other data stores such as relational databases.

A sound and complete monitoring and logging strategy is key to being able to quickly diagnose a problem within the Cloud and take action to resolve the issue. A strong logging foundation will enable us to capture relevant data and feed that into a monitoring strategy that alerts the correct teams at the correct time or takes action to resolve the issue without human intervention.

**Collecting logs within the Enterprise HUB**

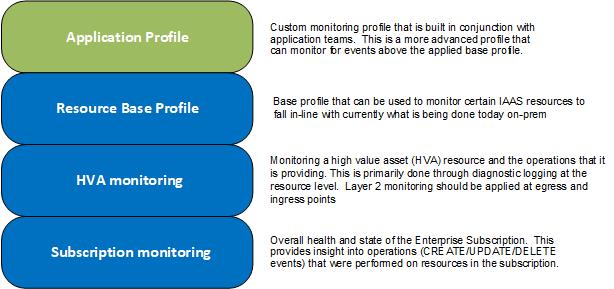
It is recommended that there be a central Log Analytics Repository within each HUB that will be the default location logs are forwarded to.

The Enterprise HUB will contain a Log Analytics workspace that can be leveraged by all tenants. This workspace will exist as the “single source of truth” within the H&P Azure environment. Further discovery/cost analysis will need to be completed in order to recommend a total Log Analytics design. Because of licensing constraints, it may be cost prohibitive to grant a workspace to each Service Line/Application within the organization. This type of model would be needed if limiting the scope of logs a particular user is granted is necessary. Licensing will also need to be a factor in granting a workspace at the tenant level if Application Insights is needed.



**Monitoring within the Enterprise HUB**

There are four “levels” that we will be concerned about monitoring within the environment:



By capturing logs and providing proactive monitoring at each one of the monitoring layers, we will be able to proactively alert and capture pertinent information for the subscription, HVA, resource, and application. This type of monitoring will enable quicker meant time to resolution for issues and a better overall understanding of the Azure environment at H&P.