Azure Foundation

Cloud Solution Architecture (CSA)
State and Local Government (SLG)

Microsoft

Agenda:

- Architecture Overview
- Security and Delegation
- Department
- Locations
- Patterns
  - Virtual Networks
  - Storage Accounts
  - Images
  - Identity
  - System Management
- Operations Management Suite
  - Azure Site Recovery
  - Azure Backup
  - Log Analytics
  - Reporting

Microsoft Azure

Application innovation
Accelerate innovation with the cloud

Data and intelligence
Power decisions & apps with insights

Openness and flexibility
Build freely, deploy anywhere

Trust
Protect your business

Enrollment Pre Requisites

- A Class B (/16) IP space per Department.
- Two Account Administrator service account assigned to each Department.
- A supported VPN device.
- A business and technical stakeholder to review configuration settings.

Common Issues and Limitations

- When Adding another Enterprise, Department or Account Administrator the portal gives an error message “Invalid Account”.

This is caused because the setting on the Enrollment Tab for “Auth Level” isn’t set to “Work or School Account Cross Tenant”

- When Adding an Enterprise Administrator an error that the person is already a Department Administrator.

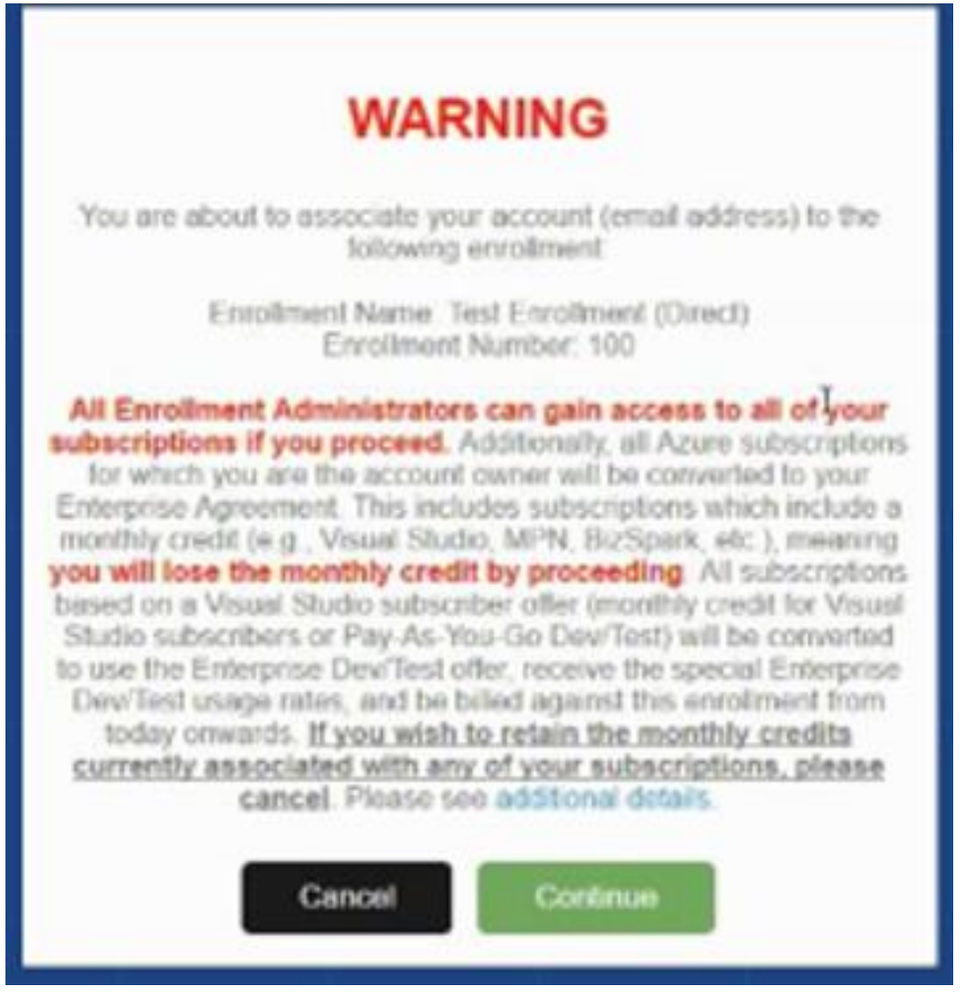
The Department Administrator needs to be different, find a backup and make the backup be the Department Administrator.

- An Account owner can only own one account.

If an account allows “work or School Account Cross Tenant” there is a risk if another organization’s Account Owner has subscriptions, those subscriptions will migrate to your EA.

Important Information about Account Owners

- The first time you login to the EA Portal as an account owner you will see this Warning Message:
- It is important to read and understand because your existing subscriptions are about to be converted ad benefits can be lost.
- A Visual Studio subscriber who is added as an Account Owner will lose their individual monthly Azure credit until they take further action.



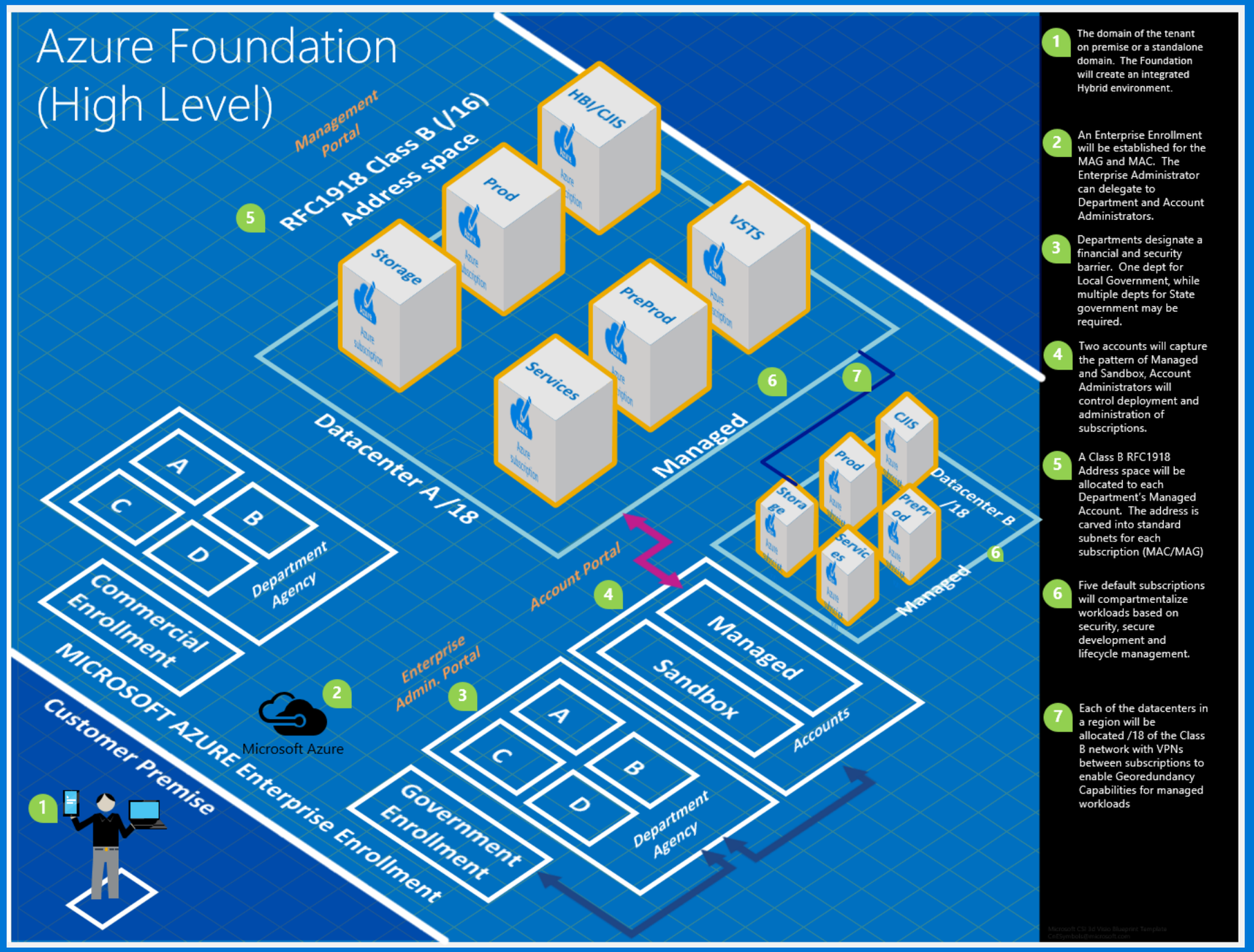
Financial Reporting for Enterprise Enrollment

There is a brief demo here.

https://channel9.msdn.com/blogs/EA.Azure.com/Using-the-EA-Azure-Power-BI-Link

- To Set up a demo, use Enrollment Number “100” and the key.
- Practice what your customer is seeing (see notes)
- Azure Government Onboarding
- Blog Post on PowerBI

Azure Foundation Pattern


Azure Foundation
(High Level)
Management Portal
RFC1918 Class B (/16) Address space
5
HBI/CIIS
Prod
Storage
VSTS
PreProd
Services
Datacenter A /18
6
Managed
7
CIIS
Prod
Storage
Services
PreProd
Datacenter B /18
Managed
6
A
B
C
D
Department Agency
Commercial Enrollment
Account Portal
4
Enterprise Admin. Portal
3
Managed
Sandbox
Accounts
Government Enrollment
Department Agency
2
Microsoft Azure
MICROSOFT AZURE Enterprise Enrollment
Customer Premise
1
1 The domain of the tenant on premise or a standalone domain. The Foundation will create an integrated Hybrid environment.
2 An Enterprise Enrollment will be established for the MAG and MAC. The Enterprise Administrator can delegate to Department and Account Administrators.
3 Departments designate a financial and security barrier. One dept for Local Government, while multiple depts for State government may be required.
4 Two accounts will capture the pattern of Managed and Sandbox, Account Administrators will control deployment and administration of subscriptions.
5 A Class B RFC1918 Address space will be allocated to each Department's Managed Account. The address is carved into standard subnets for each subscription (MAC/MAG)
6 Five default subscriptions will compartmentalize workloads based on security, secure development and lifecycle management.
7 Each of the datacenters in a region will be allocated /18 of the Class B network with VPNs between subscriptions to enable Georedundancy Capabilities for managed workloads

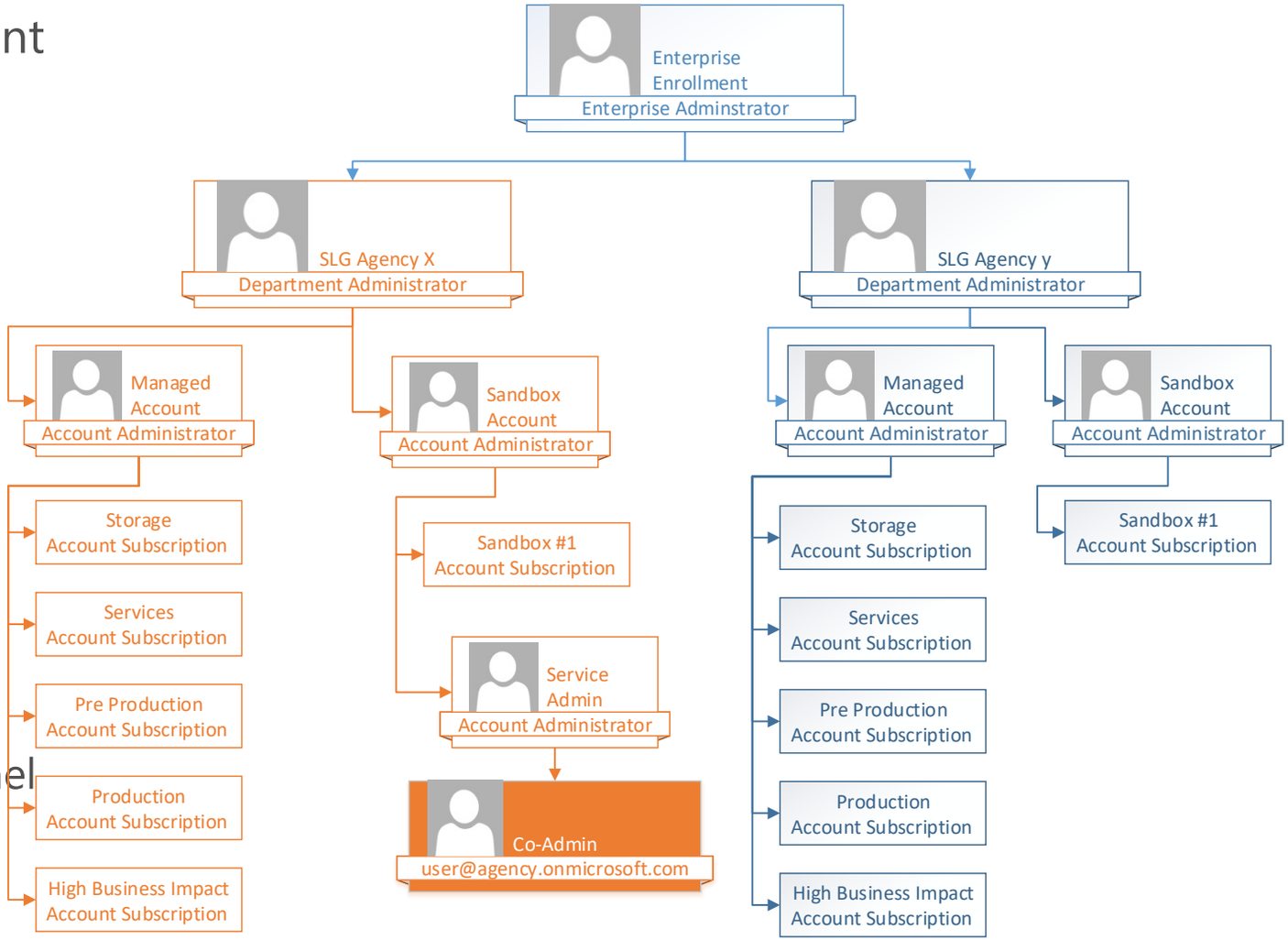
Pattern Overview Per Department

- Configuration of at least 1 Department and one Account
- Assign one Department Administrator (DA) that is different than the Enterprise Administrator. Maybe not a named user as people change.
- Create five subscriptions
  - Production, this is where production workloads will go, example, Sharepoint Farm
  - HBI/CJIS, this is where production high business impact (HBI) or Criminal Justice Information System CJIS workloads will go, example, Evidence Management System
  - Preproduction, this is where Application Lifecycle Management (ALM) workloads go, such as Test servers
  - Services, are production workloads that are required to be accessible by everyone, yet have extremely sensitive data (level 5 Password data), example Windows Active Directory Domain Controllers.
  - Storage, where on premise (non-Azure) storage is maintained, example StorSimple.
- Deploy Secure Single Sign-on for O365 Identity

Enterprise Enrollment – Departments

- Each agency will have their own Department with a Department Administrator (DA) (as required)*
- There will be two accounts, one for Managed and Sandbox Workloads
- There are five default subscriptions that each Managed Account
  - Services (Level 0 data)
  - Production (workloads)
  - CIJS (highly sensitive)
  - Hybrid Storage
  - Preproduction (dev, test, qa)

*If an Agency is administered by the same personnel there may be no benefits to defining a New Dept.

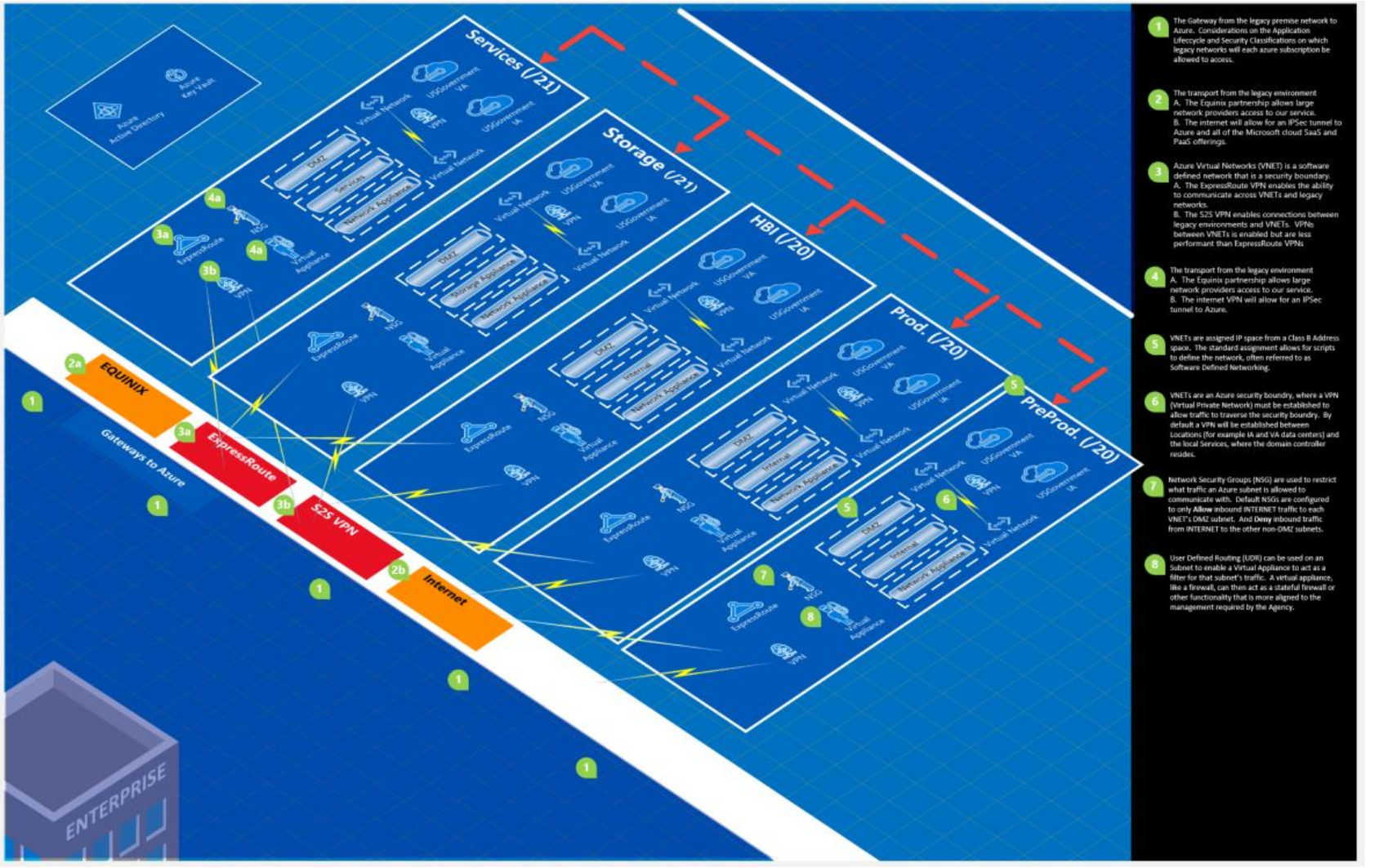


Subscription Subnets:

1. Production
2. CJIS
3. Preproduction
4. Storage
5. Services

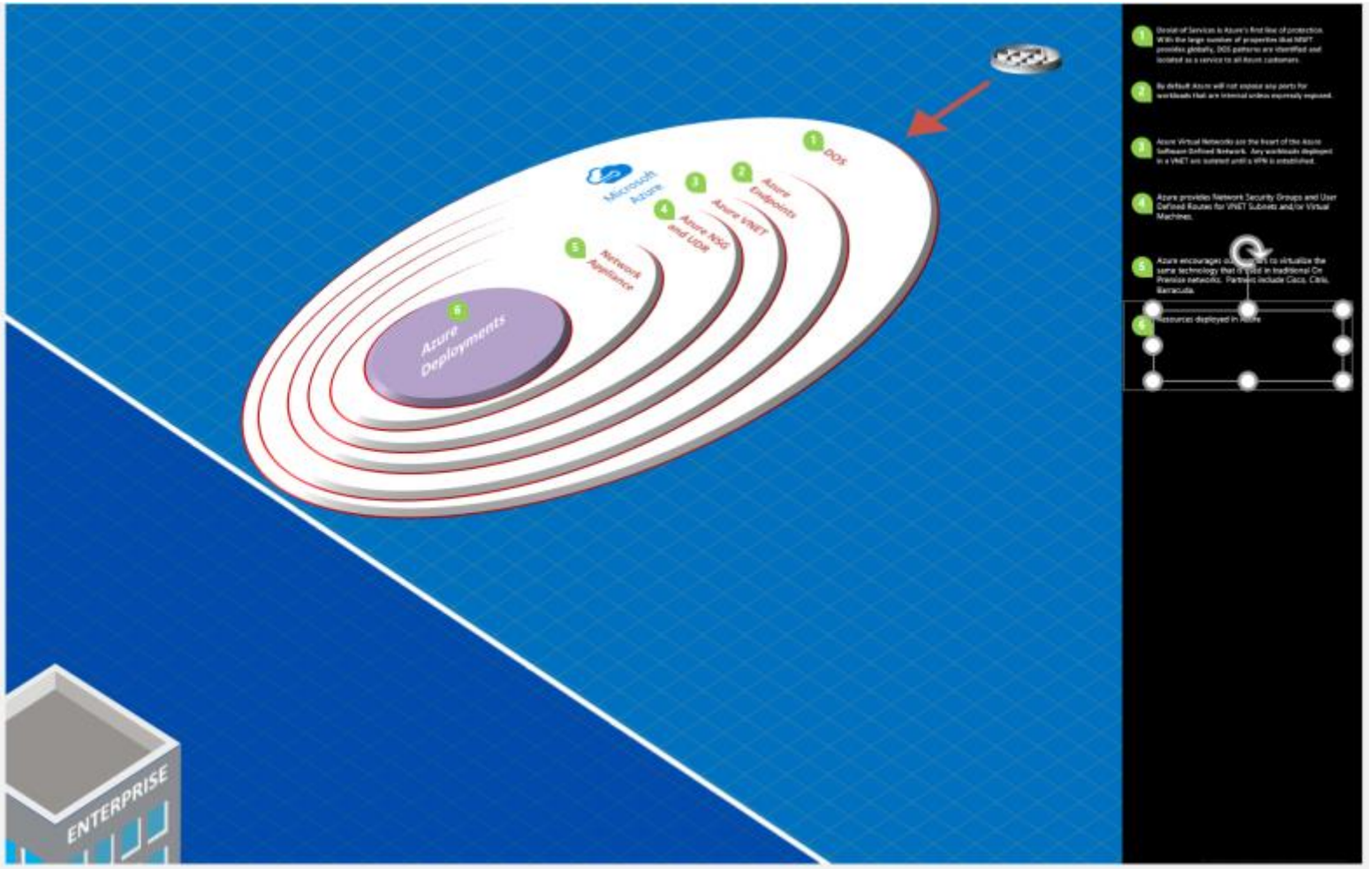
XML Configuration

- Update Spreadsheet
- Search and Replace
- Two Step process
  - Create the VNET
  - Create the Gateway



Network Security Groups

- Network Security Group:
  - External Subnet DMZ (deny all unless expressly permitted)
  - Internal Networks
    - Web
    - App
    - Database
    - User Tiers



Advanced Networking

Endpoints

- Remote Desktop Client (Jumpbox)
- Web Application Proxy (WAP) for Modern Authentication
- PowerShell

VPN

- On Premise network to Azure
- Azure Datacenters (Connection between IA and VA)
- Local Datacenter Services (Connection to the Domain Controllers)

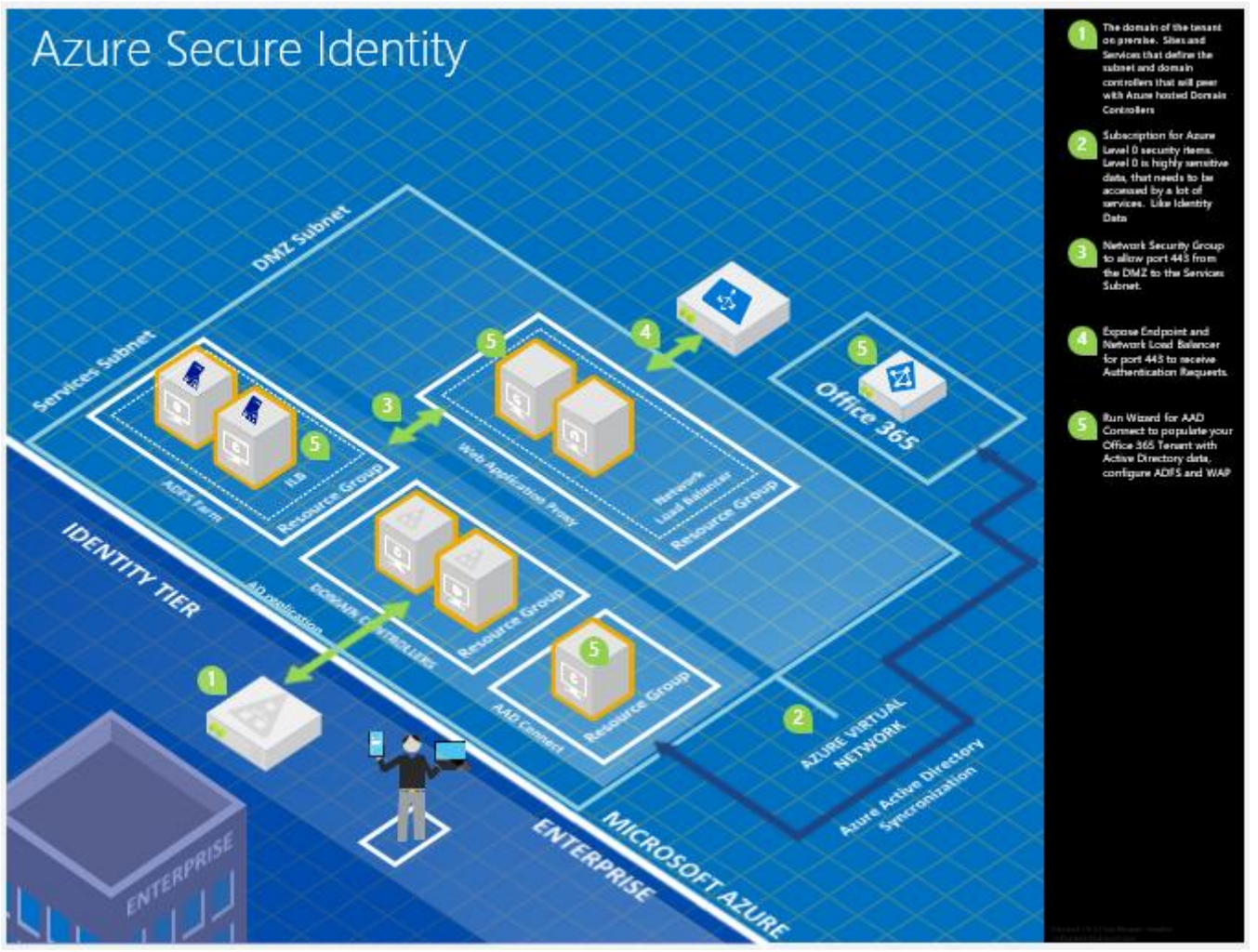
ExpressRoute

- Private Peering
- VNET Peering (coming soon)

Secure Identity Hosted in Azure:

- 2 Domain Controllers
- 1 AAD Connect Server
- 2 ADFS Servers
- Network Security Groups (NSG)
- Virtual Private Network (VPNs)
- Optional: Advanced Threat Analytics. (ATA)

NOTE: Promotion and configuration of servers is the customer's Domain Admin's responsibility.



Commercial and Government Cloud Integration

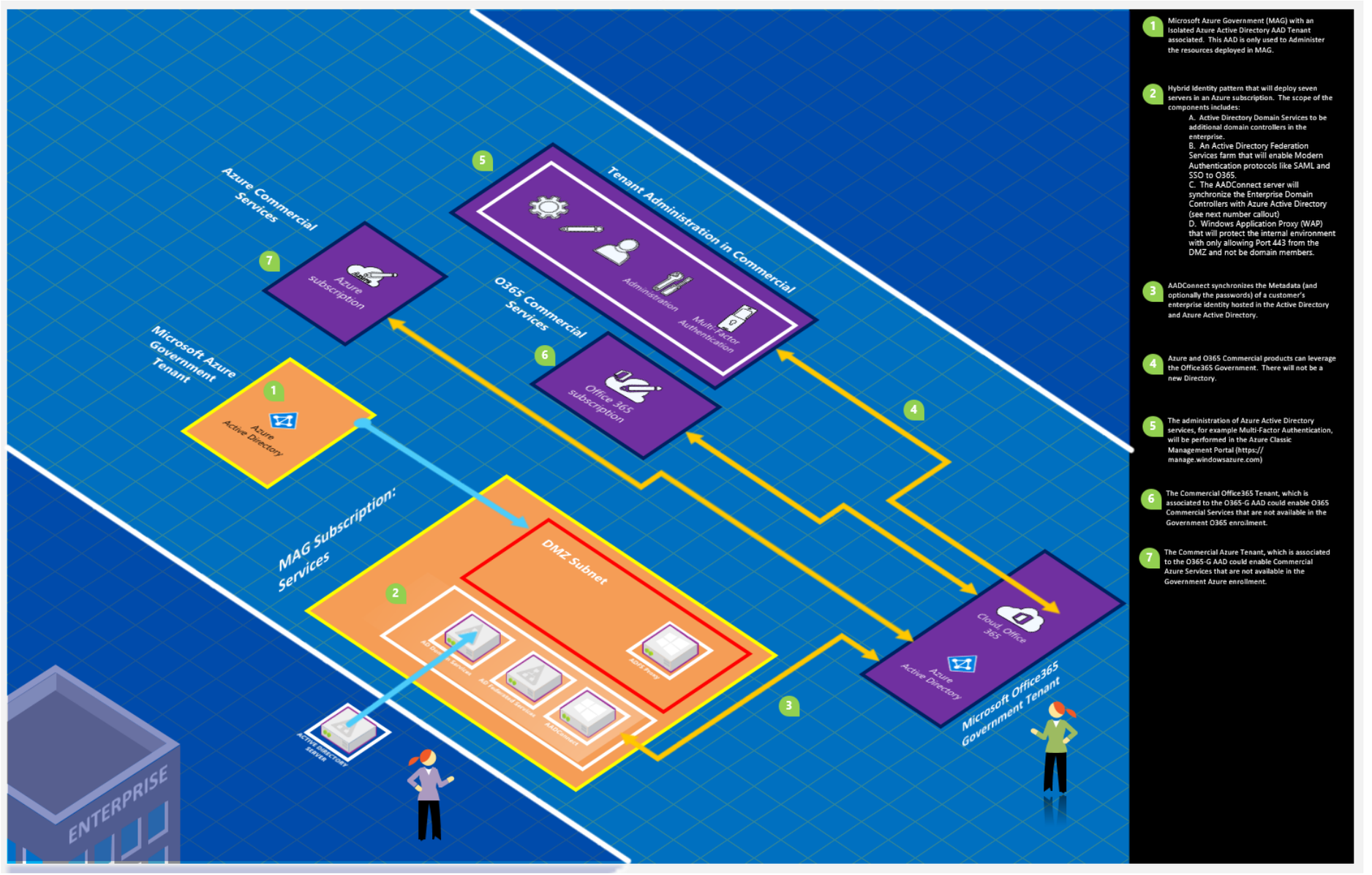
Management of multiple Enrollments

Azure Commercial Cloud

Azure Government Cloud.

For these customers, having both the MAC and MAG enrollment configured is required.

Azure Active Directory Integration



Introduction to the Spreadsheet

- Where: SLG Azure SharePoint "Foundation"
- Create a copy in your own customer directory
- Workbooks in the Spreadsheet

- Pricing Template
- Enterprise Enrollment Setup Notes
- Departments to Configure
- Subscriptions To Create
- Locations where workloads will be deployed
- VNET Pattern based on Class B
- Subnet Pattern
- Local Network Definition (Routing Table)
- Network Security Groups
- Network Security Rules
- Storage Accounts
- Users
- Server Build Sheets
- Azure Specs

Pricing Template

Modeling a workload will help give a customer confidence that running in Azure is cost effective.

Your copy of the spreadsheet is linked to the central price list.

Features:

- Workload, consider this the “tag” for tracking costs.
- SKU, look at the Azure Specs tab for a list of services and the estimated price based on Level D pricing.
- Monthly Transition, if the customer needs to build or move the workload and it will take months, this column is for the
- Ops Costs is based on the number of VMs
- Year 1 Costs takes into affect the Transition Costs.
- Preproduction allocation can be based on different methodology, consider your story.

Setup Notes

The EA Portal and Account Portal have a Read Only API, otherwise it is a “click, click, click” interface.

Naming conventions are formulas that help you work with your customers

This is a template, it can be modified.

When the network team offers to design the IP addresses, the foundation pattern is now an example and all the work needs to be reproduced.

VNET Design

RFC 1918 IPv4 addresses

10.0.0.0/8 or

172.16.0.0/16

Goal: Avoid Conflict

Typical response: “we are only putting a few things in Azure why do I need 65,000+ hosts?”

The pattern gives up to four Azure locations a highly available georedundant secure network layout for most workloads.

This pattern requires only column M and N need to be modified.

Server Build Sheets

Patterns are modelled in a spreadsheet giving a safe level of abstraction.

Common Workloads

Identity Pattern (7 Servers)

SharePoint Pattern (11 Servers)

Naming Conventions are formulas

This is not a battle worth fighting, the goal of a good name is to be unique and informative.

Ask to validate the naming convention, use ours or yours.

The entries will feed your pricing template.

Implement the spreadsheet

Get a partner!

- Microsoft Premier “Azure Faststart”
- Catapult “Cloud Foundation”
- Planet “Cloud Foundation”
- Do you have a partner already?
- Standard SOW (work in progress)
- AzureFoundation GitHub Repository for example templates that work in the Microsoft Azure Government (MAG) community cloud

How to Access Azure

Portals

- Enterprise Enrollment Portal: https://ea.azure.com
- MAG Account Portal: https://account.windowsazure.us
- MAC Account Portal: https://account.windowsazure.com
- MAC Azure Management: https://manage.windowsazure.com
- MAG Azure Management: https://manage.windowsazure.us
- MAC Support: http://aka.ms/AzureEntSupport
- MAG Support: http://aka.ms/azuregovsupport
- Office Portal: https://portal.office.com
- Managing Azure Subscriptions with PowerShell here has some additional discussion
- Getting Started with Azure PowerShell for Azure Government blog here.

Portal, PowerShell, CLI, and JSON

- Visual Studio and PowerShell ISE
- Security Keys, Published Settings File
- Portal Role Management
- Azure Resource Management (ARM)

Enterprise Portal

- Use the answers provided in the Department worksheet in the AzureFoundation Spreadsheet (AFS) to setup the Enterprise Enrollment.
- Leverage the “Notes” worksheet in the AFS for step by step guidance.
- Make “Service” users for Department and Account Administrator roles, it seems losing passwords or organizational change as users move to new roles causes unexpected delays.
- Global Administrators in the Azure Active Directory is very powerful, consider they can reset anyone’s password and impersonate that person, including the Enterprise Administrators.

Account Portal

- This is where subscriptions are made and renamed to align to the Azure Foundation pattern.
- Every subscription name should be unique, use the naming convention agreed to in the spreadsheet.
- Before changing the “Service Admin” for the subscription, consider that using the Account Administrator as the standard will allow for people to change roles.

Management Portal

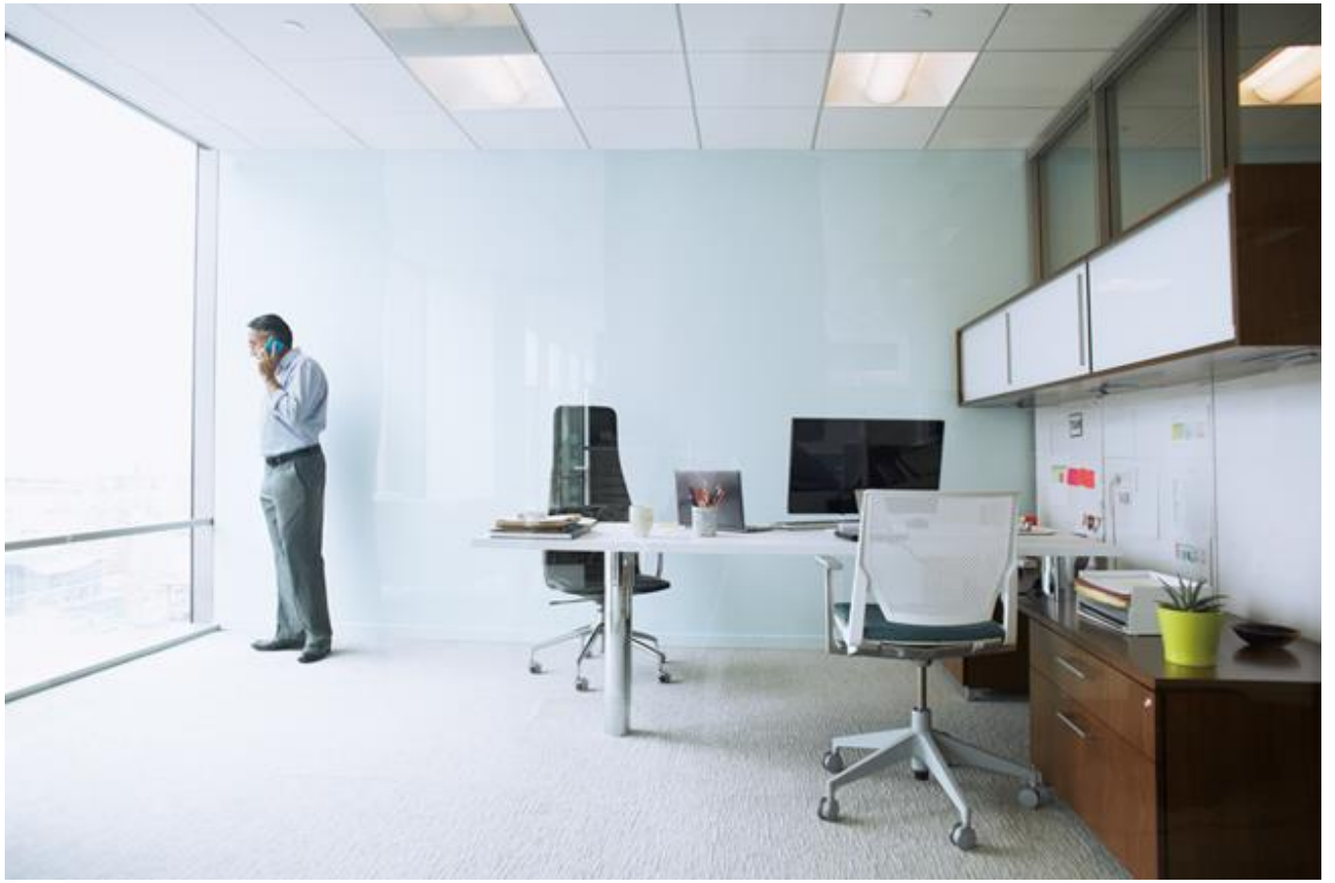
- This is the subscription. The subscription is where workload is deployed in Azure.
- Set up the Co-Administrator for each Subscription, assign the partner at a minimum.
- Security disclaimer, anyone who is a Co-Admin in the classic portal can download certificates and make changes to subscription even after they lose Co-Admin access. Change the keys as Partners and employees change roles.

PowerShell Access

- Most of the patterns are configured with PowerShell.
- The Azure Virtual Network PowerShell and XML
- The Azure Network Security Group defaults for each VNET. Make it so the DMZ is the only subnet where workload can be accessed from the Internet.
- The Identity Pattern PowerShell
- NOTE: Everything in MAG is Classic, but the Commercial Side is ARM, with Role Based Access Control. ARM is where we want to go!

Future Goals

- Replace the spreadsheet with an Application and wizard
- Have PowerShell managed in Visual Studio Team Services
- More Workloads, added to the AzureFoundation Library.



Operations

Stakeholder Personas

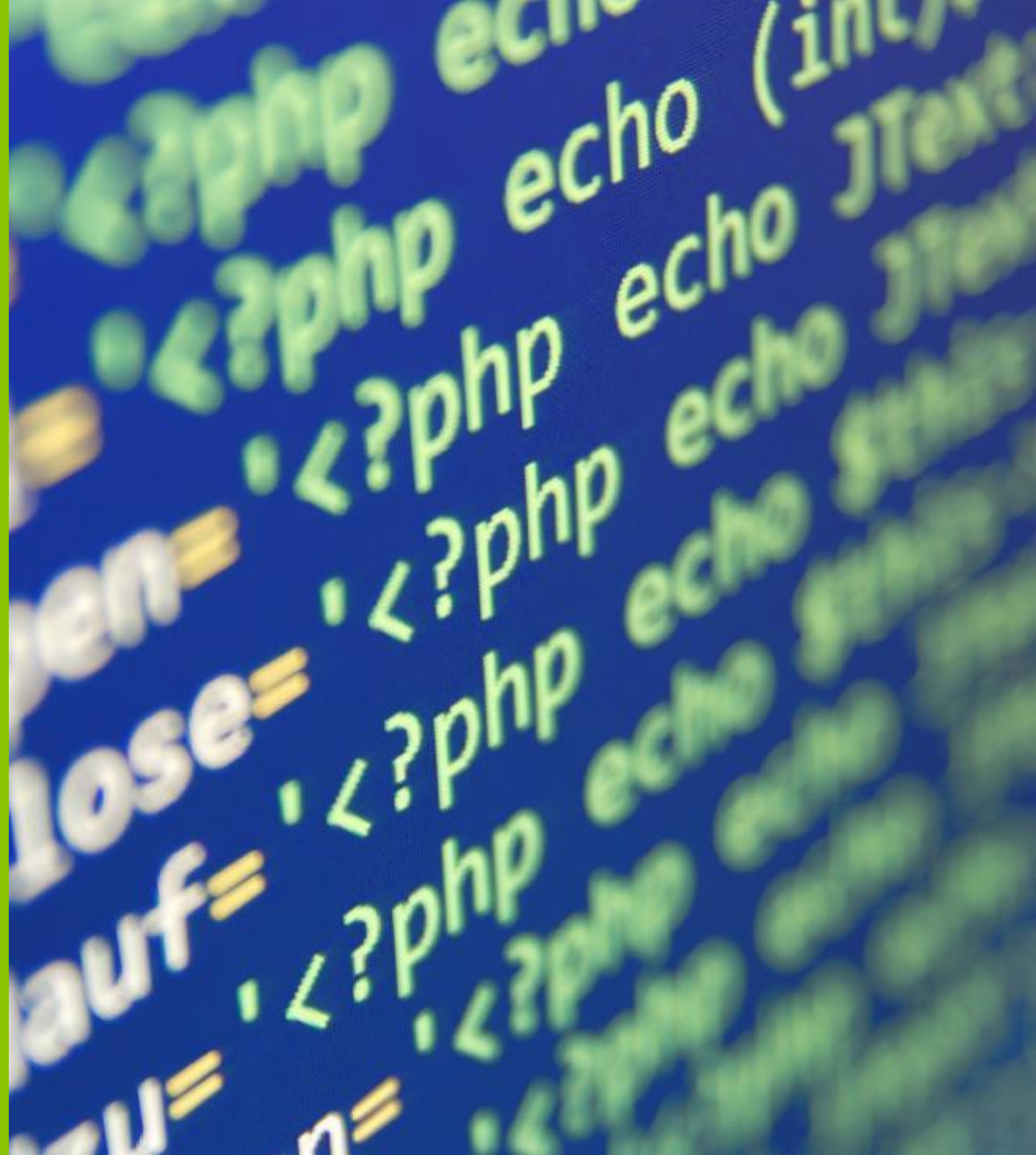
- Information System Security Manager (ISSM)
- Agency assessors
- Operations/Implementation Team
- Authorizing Official

https://blogs.msdn.microsoft.com/azuregov/2016/08/11/stakeholders-in-the-authorization-to-operate-process/

Azure Management Suite

The Azure Government Cloud IAAS environment is a: Robust , Secure, Stable computing environment. However, it is extension of your Mission Critical Data Center that needs to be Managed, Monitored, Backed-up and DR enabled for 24X7 operations

To meet and exceed these requirements Microsoft recommends the included Azure Management Suite of products. These products are not required to run your workloads in Azure, but will provide you a well managed environment



Microsoft Operations Management Suite (OMS)

Simplified IT management for any enterprise

Gain control over any hybrid cloud. Manage Microsoft Azure or Amazon Web Services (AWS), Windows Server or Linux, VMware or OpenStack—all with Microsoft Operations Management Suite (OMS), our cost-effective, all-in-one cloud IT management solution.

Microsoft OMS: is the IT management solution for the hybrid cloud. Used alone or to extend your existing System Center deployment, OMS gives you the maximum flexibility and control for cloud-based management of your infrastructure. With OMS, you can manage any instance in any cloud, including on-premises, Azure, AWS, Windows Server, Linux, VMware, and OpenStack, at a lower cost than competitive solutions. Built for the cloud-first world, OMS offers a new approach to managing your enterprise that is the fastest, most cost-effective way to meet new business challenges and accommodate new workloads, applications and cloud environments.

- Simplicity: A single portal for all your management tasks. No infrastructure to maintain.
- Time to value: Onboard fast. No content to create. Connects to your on-premises datacenter.
- Easy to integrate: Add new servers, or connect to your existing management tools within minutes.
- Hybrid and open: Manage workloads across Windows and Linux, hybrid and public clouds, Azure and AWS.
- Optimized for System Center: Complements your System Center investment to unleash new management scenarios.

Key Capabilities

- Provides enterprise-class, realtime operational intelligence across hybrid environments.
- Simplifies cloud management with process automation and monitoring of resources.
- Better ensures preparedness in the event of a disaster with cloud-based availability.
- Protects privacy and security of data, while delivering software and services to manage the IT infrastructure.

Azure Site Recovery

Full Featured Disaster Recovery

- Protect-to-and-Recover-in-Azure: Replicate and failover your on-premises applications to Azure, negating the need to build and manage a second datacenter for recovery. Reduce expenses and only pay for compute when you need it.
- N-Tier Application Consistency: Detect and stage mult-tier applications and restore them as a group, with specified startup ordering and the ability to insert scripts to bypass the need for manual configurations.
- Application Replication Support: Benefit from using SQL AlwaysON and Active Directory replication when your databases and infrastructure components need the least possible RTO. Leverage ASR's inbuilt replication technologies when the same replication technology for all tiers is adequate to meet your application's recovery objectives.
- No Impact Recovery Plan Testing: Perform periodic DR drills and testing without any impact to the production or recovery virtual machine.

One-Click Orchestrated Recovery

- Automated Failover and Manual Actions: Leverage scripts and Azure Automation Runbooks to achieve optimal RTO and reduce human errors during recover

- Automated Failback and Reverse Replication: Failing back to your primary datacenter is just as important as the initial failover. With ASR it is as easy as one click, and comes with the same data protection guarantee as failovers.

Automated VM Protection and Replication

Enable policy-based replication and protection for thousands of virtual machines using a few simple steps

- At-Scale Configuration: Configure protection and disaster recovery networking settings that apply to your applications or your entire datacenter for seamless recovery.
- Low Recovery Point Objective (RPO): Achieve near-synchronous RPOs, as low as 30s, even when using Azure as your recovery site.
- Quick Recovery: Recover from disruptions within minutes and benefit from Azure's 99.9% uptime guarantee.
- Data Security and Secure Transmission: Data is encrypted when in transit and at rest in Azure.

Remote Health Monitoring and Extensibility

With ASR, you also get proactive, continuous monitoring and alerting on issues before your business is impacted. Meet audit and compliance requirements using our robust reporting capabilities. Leverage our capacity planning resources to better plan your resource provisioning and usage. With ASR's PowerShell support, you also get the ability to extend and integrate ASR's functionality.

Azure Backup

For Physical, Hybrid, and Cloud Environments

Azure Integrated Backup Solution

Azure Backup protects your data in the cloud and optionally can be integrated with System Center Data Protection Manager for advanced workload protection.

- Data protection schedules can be daily, monthly, weekly, and yearly with retention up to 99 years in Azure
- Protects workloads running in Azure, in VMs, or on physical servers
- Centralized monitoring and reporting across on premises and Azure

Advanced Workload Protection

- Protects files and folders from Windows Servers and Windows Clients
- Integrates with SCDPM protects enterprise workloads including SharePoint, Exchange, SQL Server, and Hyper-V VMs
- Protects guest workloads running in VMware environments
- DPM works seamlessly with the Hyper-V Volume Shadow Copy Services (VSS) writer to ensure that consistent versions of virtual machines are captured and protected without affecting virtual machine access
- Granular restore capability such as mailbox recovery for Exchange, DB level recovery for SQL, and ILR for SharePoint

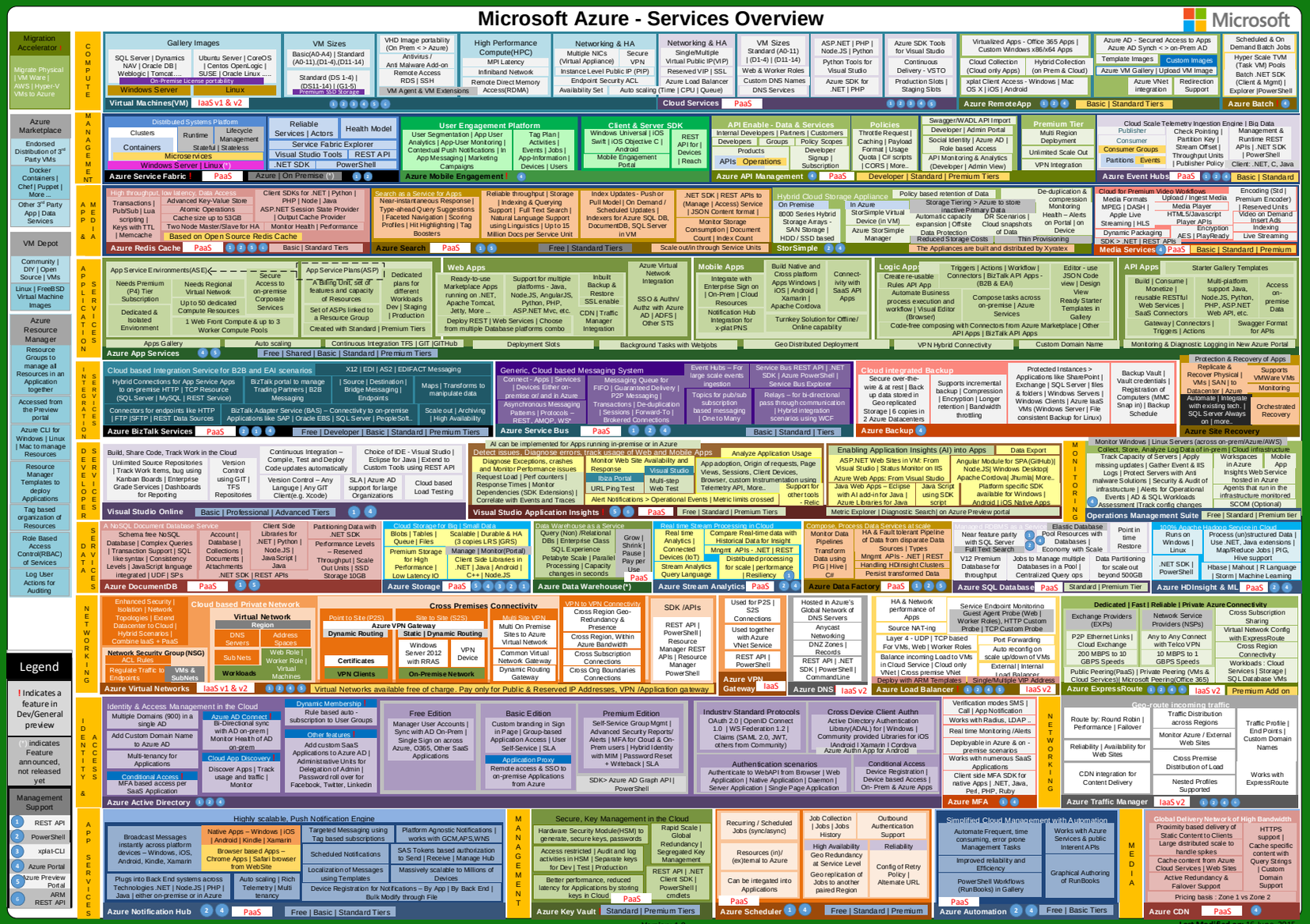
Automated, Reliable and Secure

- Scheduling: Customers can specify daily, weekly, monthly and yearly policies
- Retention: Data can be retained in Azure for up to 99 years
- Throttling: Network throttling can be configured so that optimal bandwidth usage happens during off-peak time
- Incremental: After the initial seeding, backups are incremental, ensuring that resources such as storage and bandwidth are efficiently used
- Compression: Data is compressed on the client side so there is less bandwidth consumption and less storage consumed
- Secure: Data is encrypted in your datacenter and stored encrypted in Azure – the encryption key is stored and managed locally
- Reliable: 3 copies of the data are stored to a single datacenter location and optionally at an additional, remote datacenter

Offline Seeding

Initial backups can be time-consuming and consume large amounts of bandwidth. With Azure Import/Export, the initial backup can be executed locally and then the physical media can be delivered to the nearest Azure datacenter

Azure Services Overview



Visualizing the security layers

Azure Deployments

Network Virtual Appliances

NSG & UDR

Virtual Network Isolation

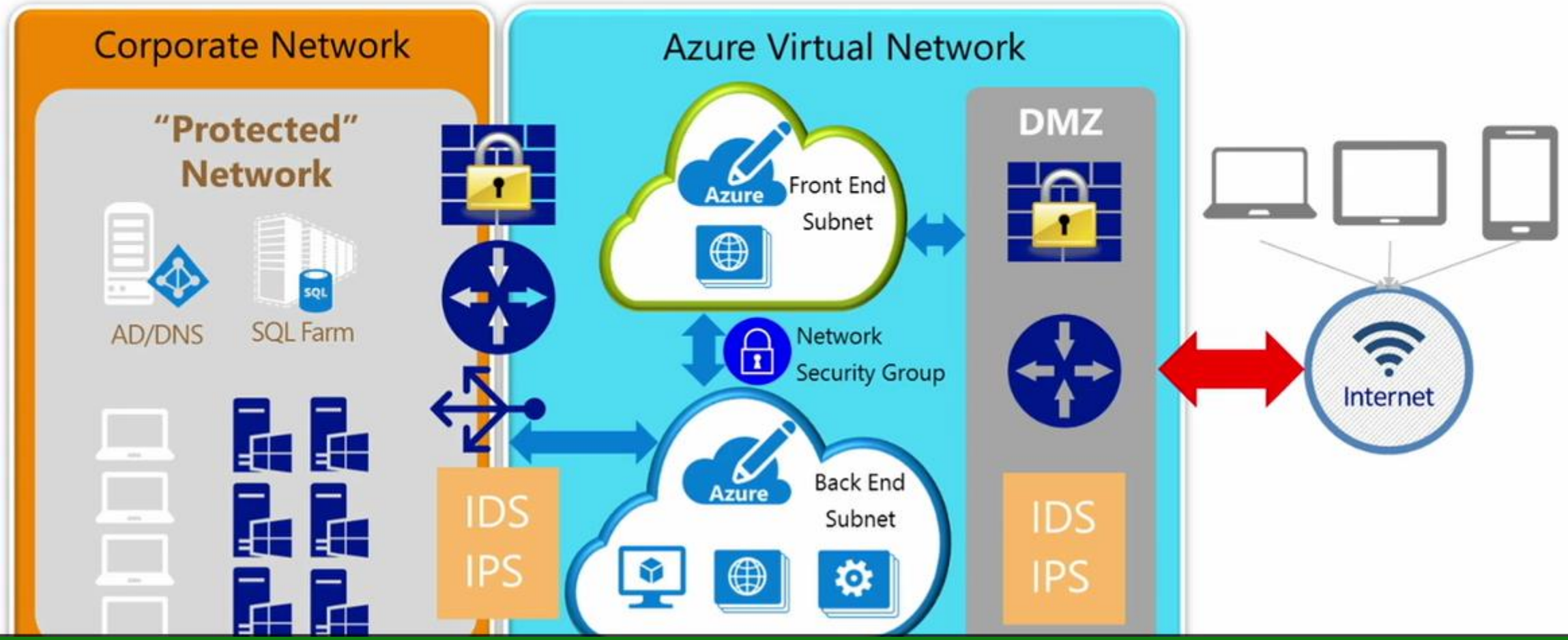
Endpoints

DDoS

Internet

Azure

Visualizing the Azure DMZ



NSG code walkthrough

```
# Create the NSG
New-AzureNetworkSecurityGroup -Name $NSGName -Location $DeploymentLocation `
    -Label "Security group for $VNetName subnets in $DeploymentLocation"

# Add NSG Rule to Deny Inbound Internet Traffic
Get-AzureNetworkSecurityGroup -Name $NSGName | `
    Set-AzureNetworkSecurityRule -Name "Isolate the $VNetName VNet from the Internet" `
        -Type Inbound -Priority 100 -Action Deny `
        -SourceAddressPrefix INTERNET -SourcePortRange '*' `
        -DestinationAddressPrefix VIRTUAL_NETWORK -DestinationPortRange '*' `
        -Protocol *

# Bind the NSG to a Subnet
Set-AzureNetworkSecurityGroupToSubnet -Name $NSGName -SubnetName $FESubnet `
    -VirtualNetworkName $VNetName
Set-AzureNetworkSecurityGroupToSubnet -Name $NSGName -SubnetName $BESubnet `
    -VirtualNetworkName $VNetName
```

Gartner

Gartner MQs	Microsoft
Business Intelligence and Analytics Platforms	●
Cloud Infrastructure as a Service (IaaS), Worldwide	●
CRM Customer Engagement Center	●
Data Warehouse and Data Management Solutions for Analytics	●
Disaster Recovery as a Service (DRaaS)	●
Enterprise Application Platform as a Service, Worldwide	●
Enterprise Content Management	●
Horizontal Portals	●
Identity and Access Management as a Service, Worldwide	●
Mobile App Development Platforms	●
Operational Database Management Systems	●
Public Cloud Storage Services, Worldwide	●
Sales Force Automation	●
Social Software in the Workplace	●
Unified Communications	●
Web Conferencing	●
X86 Server Virtualization Infrastructure	●