Azure Regions

EastUS	WestUS
Primary	Region Pair for DR

Naming Convention

bsteph27 team to update before implementation approval.

(Resource Type) (Environment) (Azure Region) (Workload/Applicaiton) (Instance ###)

The components are applied as applicable to the resource type.
Examples:
Resource Group – rg-prod-wus-net
Virtual Machine – vm-prod-app-001
Storage Account – saprodwusdiag

Resources follow the recommended abbreviation for Azure resource types.
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/resource-abbreviations

Tagging

bsteph27 team to update before implementation approval.

Tag Name	Value	Description	Required	Inheritance
BuildDate	YYYY-MM-DD	Date the resource is provisioned	Yes	
EnviTier	Production	Environmental identifier		Sub
AppName	WebApp01	Name of the project or product line		Rg
Owner	user@<Client>	Email address or distribution list	Yes	
Department	Accounting	Departmental Identifier	Yes	

redapt

Management Hierarchy
- Resource organization
  - Management Group structure
  - Subscription design
- Identity (IAM/RBAC)
- Governance disciplines
  - Policy assignment locations
- Additional Azure features & services

Tenant Root Group

mg-bsteph27-contrib
mg-bsteph27-reader
Policy (enforced)
Regulatory Compliance (audit)

mg-bsteph27

mg-prod-contrib
mg-prod-reader
Policy (enforced)
mg-production

mg-stg-contrib
mg-stg-reader
Policy (enforced)
mg-staging

mg-dev-contrib
mg-dev-reader
Policy (enforced)
mg-development

mg-platform

mg-plt-contrib
mg-plt-reader
Policy (enforced)

sub-management

sub-mgmt-contrib
sub-mgmt-reader
Security Center (Defender)

EastUS

Resource Group
rg-eus-shared

Log Analytics Workspace
la-eus-shared
* Dashboards
* Queries
* Alerting

Automation Account
aa-eus-shared
* Change Tracking
* Inventory Management
* Update Management

Resource Group
rg-eus-identity

Availability Set
as-eus-adds

Domain Controller

Azure AD Connect

Key Vault
kv-eus-shared

Resource Group
rg-eus-network

Virtual Network
vnet-eus-management

Subnet
snet-shared

Subnet
snet-identity

sub-connectivity

sub-conn-contrib
sub-conn-reader
Security Center (Defender)

EastUS

Resource Group
rg-eus-network

Virtual Network
vnet-eus-hub

GatewaySubnet

AzureFirewall

AzureBastion
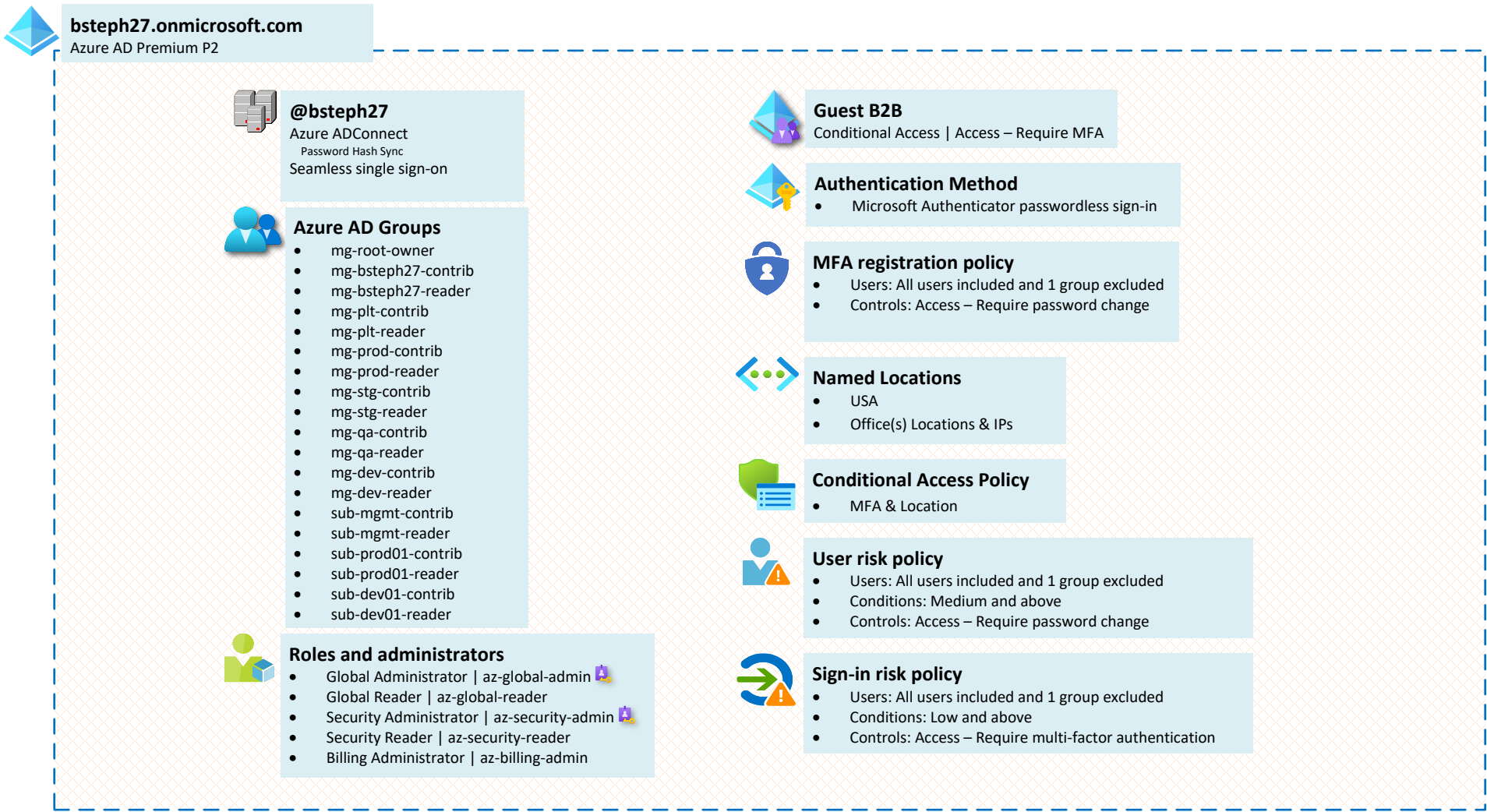
bsteph27 team to update before implementation approval.
- Resource Group structure for Landing Zone

Azure AD
- Identity (IAM/RBAC)

bsteph27.onmicrosoft.com
Azure AD Premium P2

@bsteph27
Azure ADConnect
Password Hash Sync
Seamless single sign-on

Azure AD Groups
- mg-root-owner
- mg-bsteph27-contrib
- mg-bsteph27-reader
- mg-plt-contrib
- mg-plt-reader
- mg-prod-contrib
- mg-prod-reader
- mg-stg-contrib
- mg-stg-reader
- mg-qa-contrib
- mg-qa-reader
- mg-dev-contrib
- mg-dev-reader
- sub-mgmt-contrib
- sub-mgmt-reader
- sub-prod01-contrib
- sub-prod01-reader
- sub-dev01-contrib
- sub-dev01-reader

Roles and administrators
- Global Administrator | az-global-admin
- Global Reader | az-global-reader
- Security Administrator | az-security-admin
- Security Reader | az-security-reader
- Billing Administrator | az-billing-admin

Guest B2B
Conditional Access | Access – Require MFA

Authentication Method
- Microsoft Authenticator passwordless sign-in

MFA registration policy
- Users: All users included and 1 group excluded
- Controls: Access – Require password change

Named Locations
- USA
- Office(s) Locations & IPs

Conditional Access Policy
- MFA & Location

User risk policy
- Users: All users included and 1 group excluded
- Conditions: Medium and above
- Controls: Access – Require password change

Sign-in risk policy
- Users: All users included and 1 group excluded
- Conditions: Low and above
- Controls: Access – Require multi-factor authentication
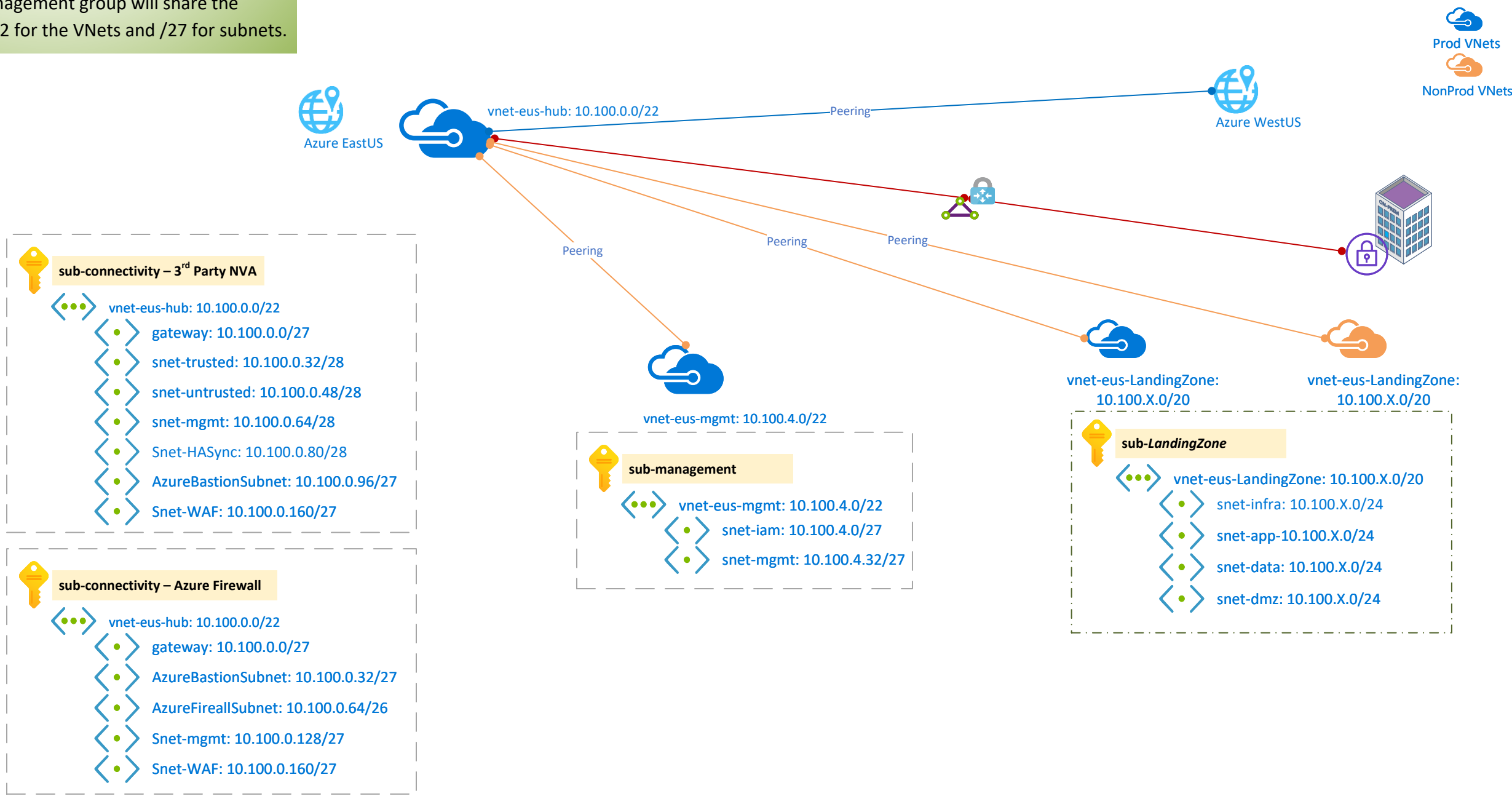
VNet & Subnet Ip Address Breakdown

Each region will be contained in a /16
VNets - /20 (4094 available IPs)
Subnets - /24 (250 available IPs)
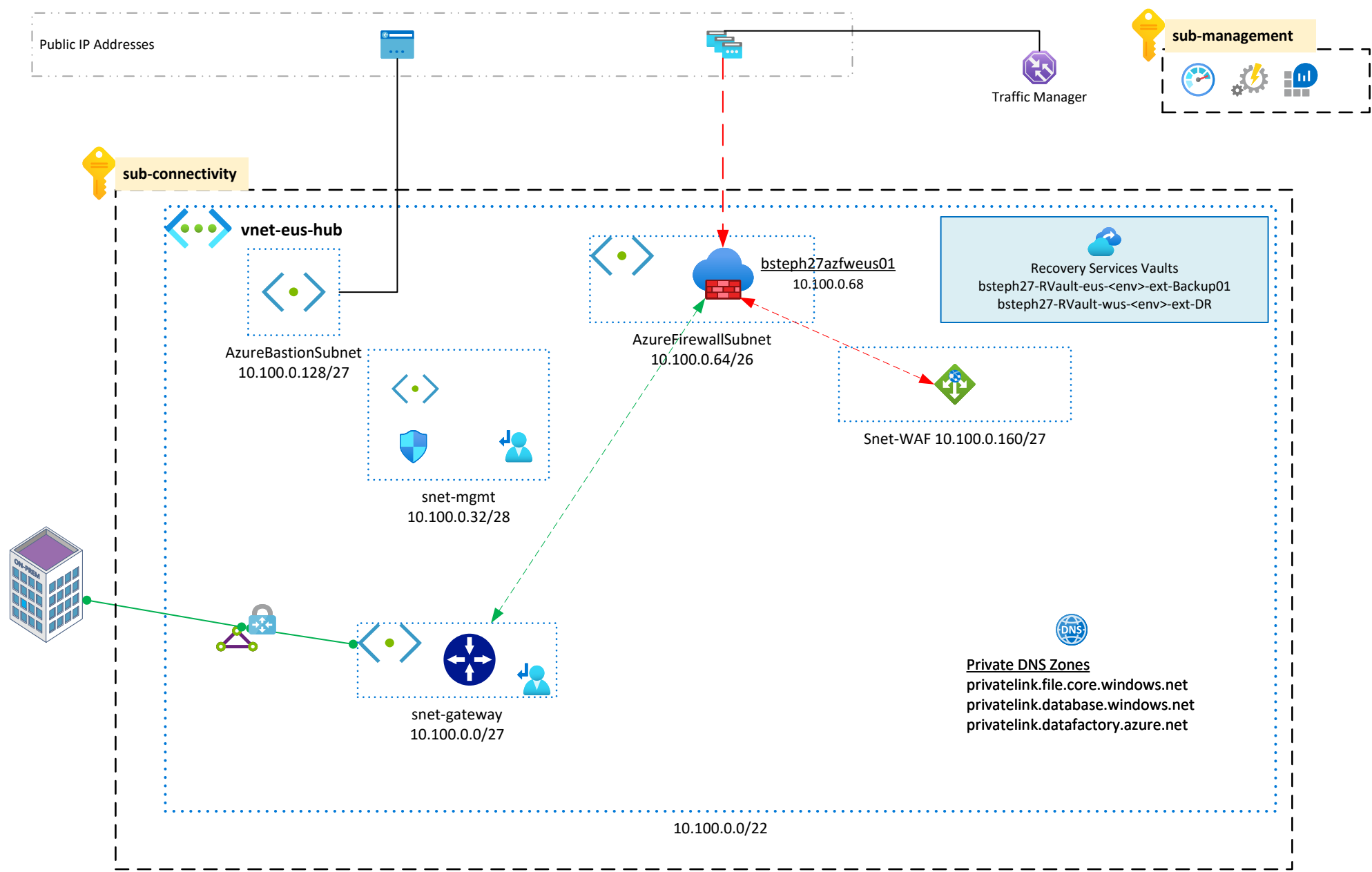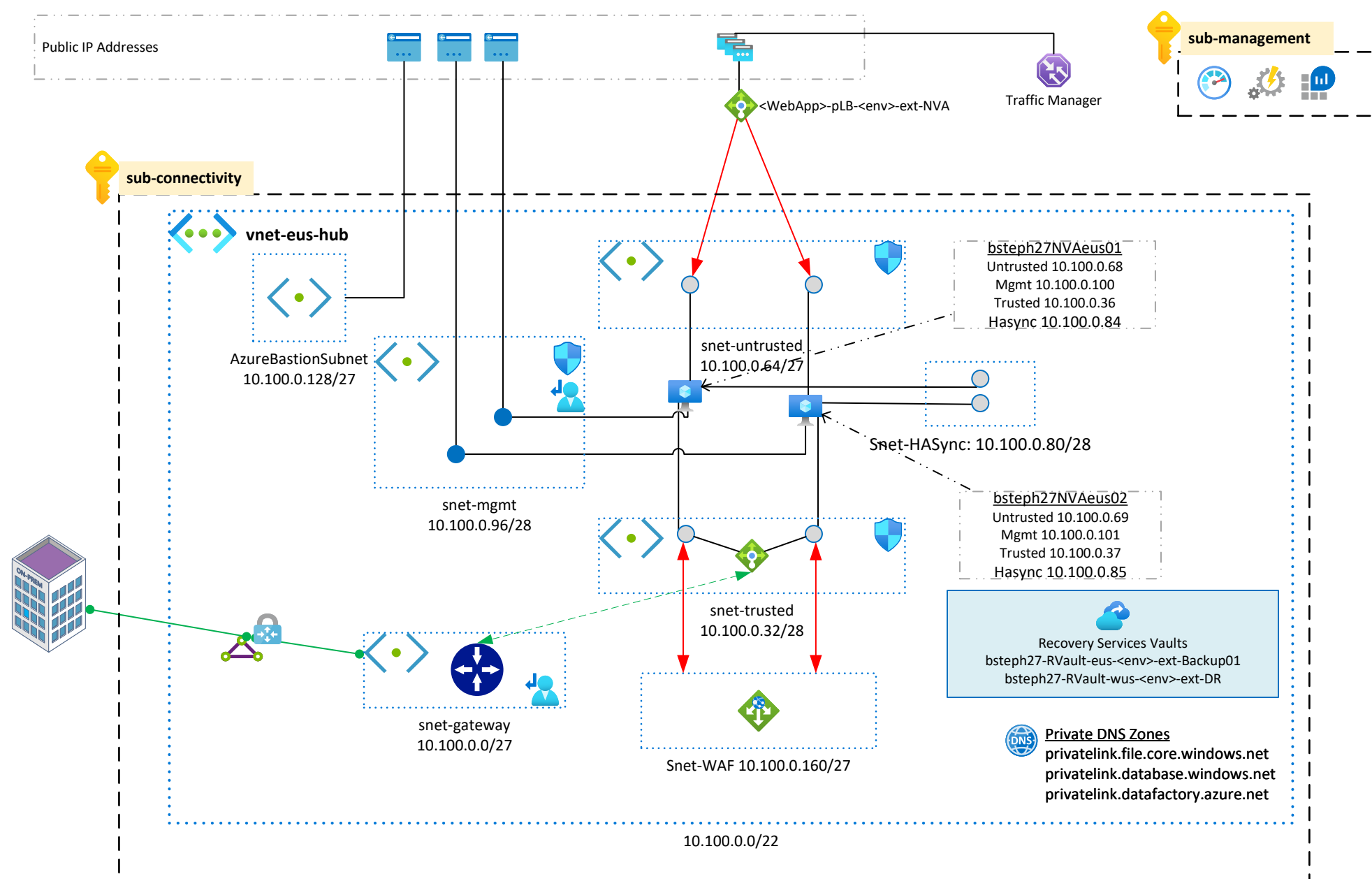
10.<region>.<VNet>.<app/svc>

Note: The platform management group will share the
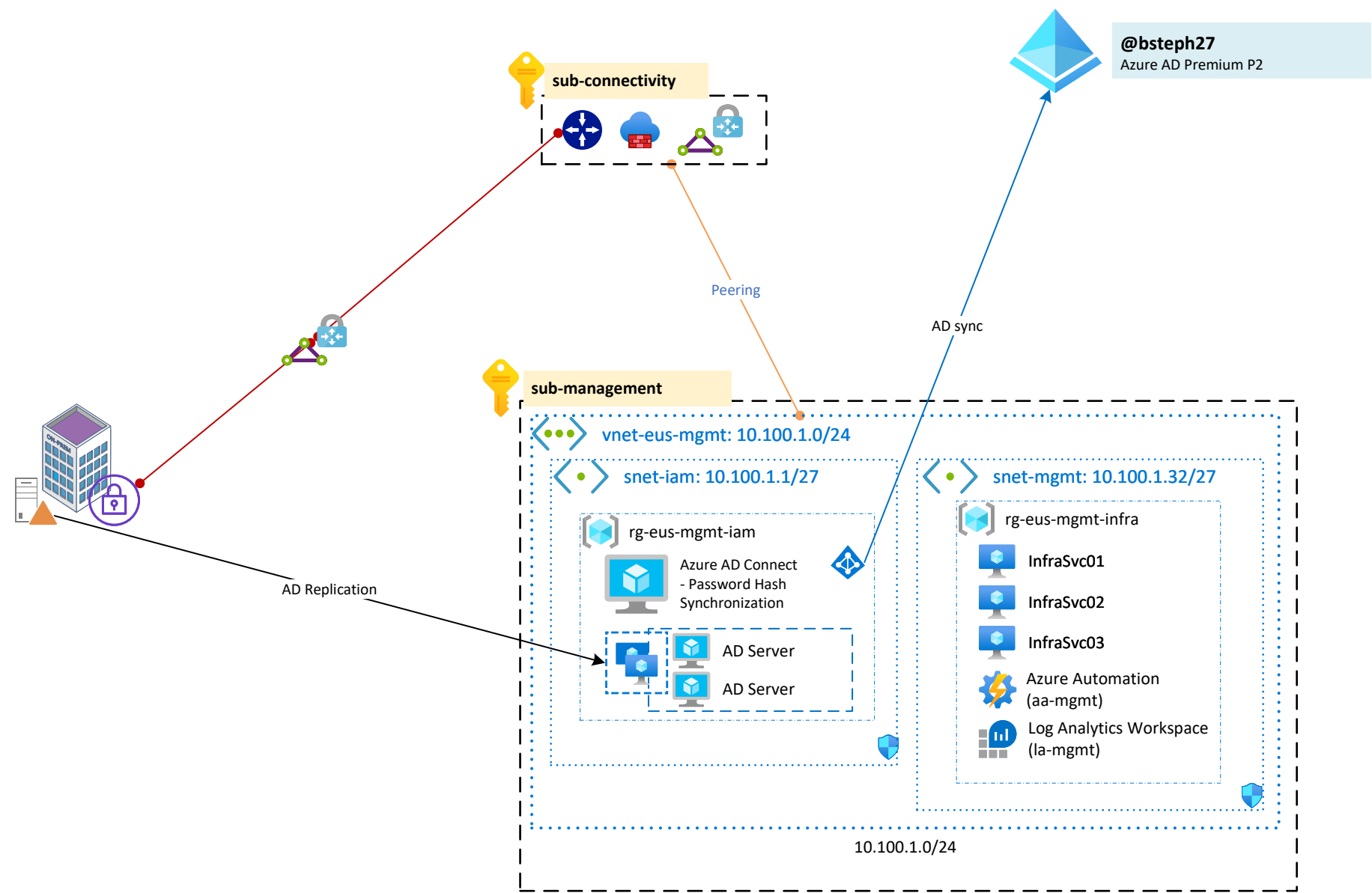same /20 space using /22 for the VNets and /27 for subnets.

Prod VNets

NonProd VNets

Azure EastUS

vnet-eus-hub: 10.100.0.0/22

Peering — Azure WestUS

Peering

Peering

Peering

sub-connectivity – 3rd Party NVA

vnet-eus-hub: 10.100.0.0/22
- gateway: 10.100.0.0/27
- snet-trusted: 10.100.0.32/28
- snet-untrusted: 10.100.0.48/28
- snet-mgmt: 10.100.0.64/28
- Snet-HASync: 10.100.0.80/28
- AzureBastionSubnet: 10.100.0.96/27
- Snet-WAF: 10.100.0.160/27

sub-connectivity – Azure Firewall

vnet-eus-hub: 10.100.0.0/22
- gateway: 10.100.0.0/27
- AzureBastionSubnet: 10.100.0.32/27
- AzureFireallSubnet: 10.100.0.64/26
- Snet-mgmt: 10.100.0.128/27
- Snet-WAF: 10.100.0.160/27

vnet-eus-mgmt: 10.100.4.0/22

sub-management

vnet-eus-mgmt: 10.100.4.0/22
- snet-iam: 10.100.4.0/27
- snet-mgmt: 10.100.4.32/27

vnet-eus-LandingZone:
10.100.X.0/20

vnet-eus-LandingZone:
10.100.X.0/20

sub-*LandingZone*

vnet-eus-LandingZone: 10.100.X.0/20
- snet-infra: 10.100.X.0/24
- snet-app-10.100.X.0/24
- snet-data: 10.100.X.0/24
- snet-dmz: 10.100.X.0/24

bsteph27 team to update before implementation approval.
- Subnet structure
- Subnet IP Addressing

Public IP Addresses

Traffic Manager

sub-management

sub-connectivity

vnet-eus-hub

bsteph27azfweus01
10.100.0.68

Recovery Services Vaults
bsteph27-RVault-eus-<env>-ext-Backup01
bsteph27-RVault-wus-<env>-ext-DR

AzureBastionSubnet
10.100.0.128/27

AzureFirewallSubnet
10.100.0.64/26

Snet-WAF 10.100.0.160/27

snet-mgmt
10.100.0.32/28

Private DNS Zones
privatelink.file.core.windows.net
privatelink.database.windows.net
privatelink.datafactory.azure.net

snet-gateway
10.100.0.0/27

10.100.0.0/22

Public IP Addresses

<WebApp>-pLB-<env>-ext-NVA

Traffic Manager

sub-management

sub-connectivity

vnet-eus-hub

AzureBastionSubnet
10.100.0.128/27

bsteph27NVAeus01
Untrusted 10.100.0.68
Mgmt 10.100.0.100
Trusted 10.100.0.36
Hasync 10.100.0.84

snet-untrusted
10.100.0.64/27

Snet-HASync: 10.100.0.80/28

snet-mgmt
10.100.0.96/28

bsteph27NVAeus02
Untrusted 10.100.0.69
Mgmt 10.100.0.101
Trusted 10.100.0.37
Hasync 10.100.0.85

snet-trusted
10.100.0.32/28

Recovery Services Vaults
bsteph27-RVault-eus-<env>-ext-Backup01
bsteph27-RVault-wus-<env>-ext-DR

snet-gateway
10.100.0.0/27

Snet-WAF 10.100.0.160/27

Private DNS Zones
privatelink.file.core.windows.net
privatelink.database.windows.net
privatelink.datafactory.azure.net

10.100.0.0/22

sub-connectivity

sub-management

Peering

sub-*LandingZone*

vnet-*LandingZone*-eus

Recovery Services Vaults
bsteph27-RVault-Prod-Ext-eus-Backup01
bsteph27-RVault-Prod-Ext-wus-DR

snet-infra: 10.100.X.0/24

saprodeusdiag

Azure Files
bsteph27fileseus01

snet-app: 10.100.X.0/24

AppSvr01

AppSvr02

AppSvr03

snet-data: 10.100.X.0/24

Azure SQL Databases

snet-dmz: 10.100.X.0/24

WebSvr01

WebSvr02

WebSvr03

10.100.X.0/20

Storage Sync Service

Business continuity and disaster recovery (BCDR)
- Operations baseline

Azure Backup
- Azure Virtual Machine
- SQL in Azure VM
- Azure Storage (Azure Files)

Policies
DefaultPolicy
- Frequency - Daily @ 23:00
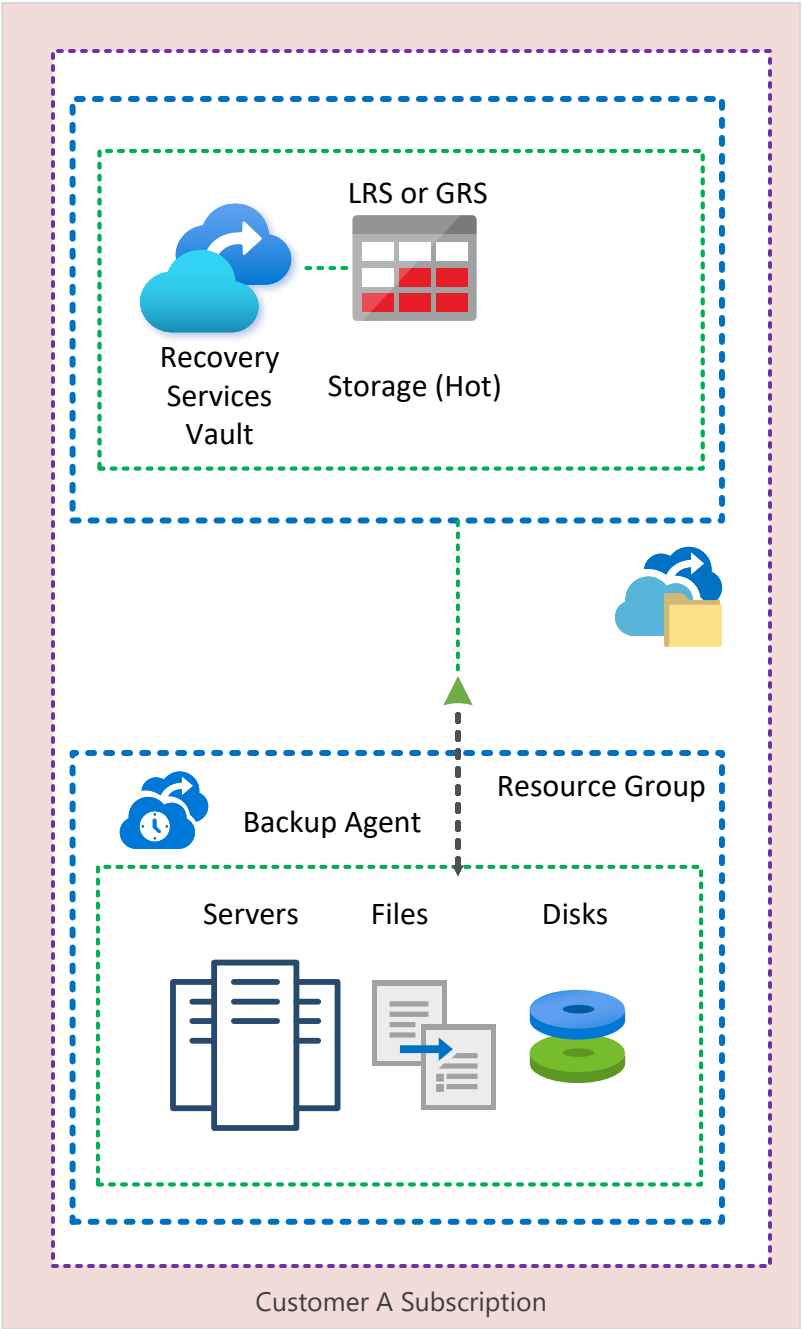- Retention - Daily – 7 | Weekly – 4

Recovery Services vaults
- Replication
- Recovery Plan

Recovery Point Objective (RPO)
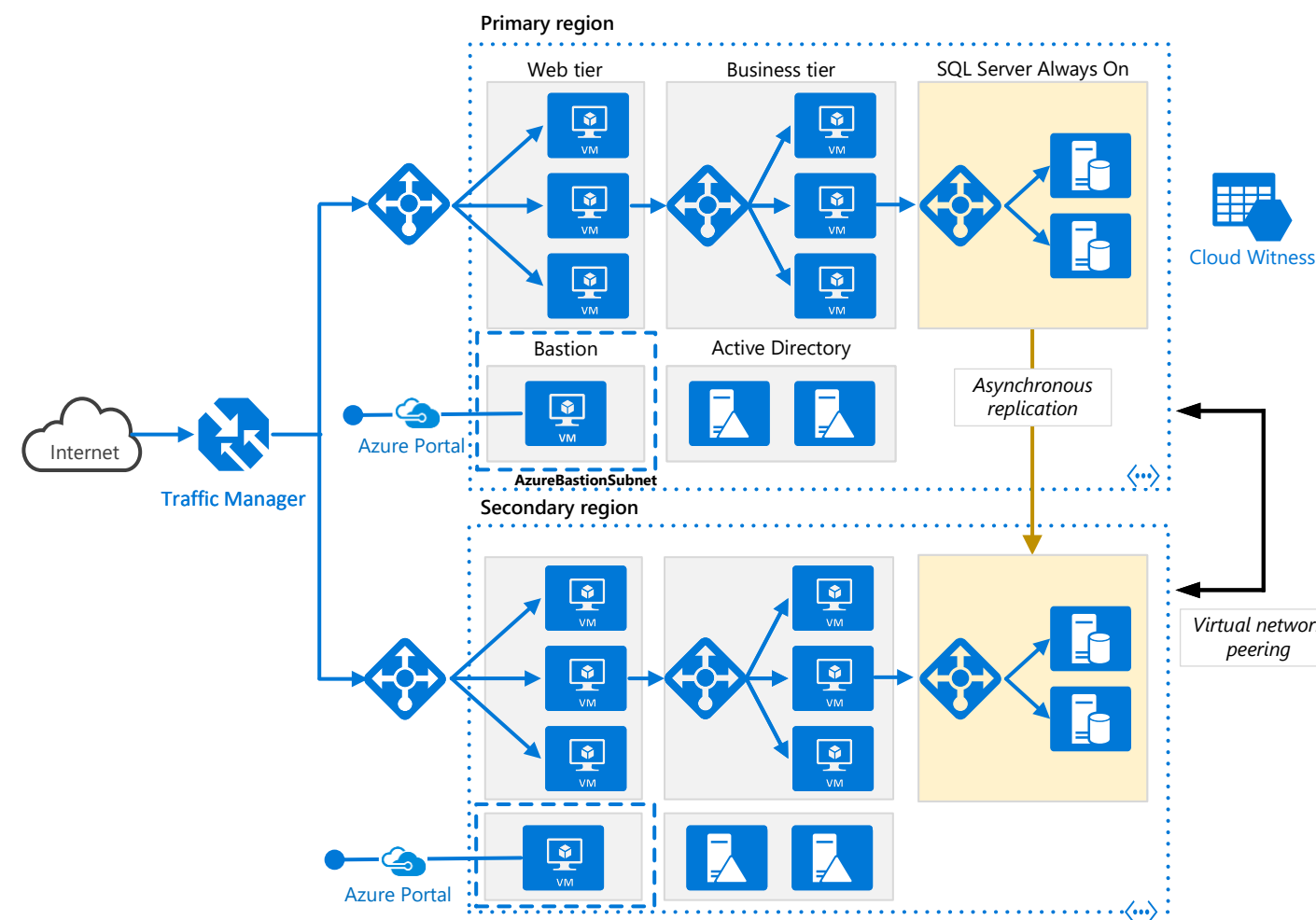- 1 - 24 hours (via ASR)
- May change per Customer

Recovery Time Objective (RTO)
- 1 – 24 hours
- May change per Customer

LRS or GRS

Recovery Services Vault

Storage (Hot)

Resource Group

Backup Agent

Servers   Files   Disks

Customer A Subscription

Application High Availability
- Example diagram of available configurations in Azure to support high availability of an application across Azure regions.

Azure Windows Virtual Desktop
- Topology and connectivity

sub-connectivity

bsteph27.onmicrosoft.com
Azure AD Premium P2

Business Group

Peering

WVD Authentication

sub-management

vnet-eus-mgmt: 10.100.1.0/24

snet-wvd: 10.101.20.0/24

WVD Host Pool (Personal)

WVD Host Pool (Shared)

Azure Files

Storage Account

Storage Account

snet-iam: 10.100.1.1/27

@bsteph27

Desktop Authentication