Revision and Signoff Sheet

Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Change Reference |
| 12 DEC 2020 | Theo | 0.1 | Initial Draft |
|  |  |  |  |

Table of Contents

[1 Introduction 3](#_Toc42241370)

[1.1 Virtual networks & Subnets 3](#_Toc42241371)

[1.2 Network Security Groups 4](#_Toc42241372)

[1.2.1 HUB NSG Rules 4](#_Toc42241373)

[1.2.2 Prod NSG Rules 5](#_Toc42241374)

[1.2.3 Pre-Prod NSG Rules 6](#_Toc42241375)

[1.2.4 Prod NSG Rules 7](#_Toc42241376)

[1.2.5 Hub Subnets 8](#_Toc42241377)

[1.2.6 Prod Subnets 8](#_Toc42241378)

[1.2.7 Pre-Prod Subnets 8](#_Toc42241379)

[1.2.8 Non-Prod Subnets 8](#_Toc42241380)

[1.3 Virtual Network Gateway 9](#_Toc42241381)

[1.4 Express Route 9](#_Toc42241382)

[1.5 Bastion 9](#_Toc42241383)

[1.6 Application Gateway 9](#_Toc42241384)

[1.7 Azure Firewall 10](#_Toc42241385)

[1.8 NAT Gateway 10](#_Toc42241386)

[1.9 Other Services 10](#_Toc42241387)

[1.10 Naming Convention 10](#_Toc42241388)

1. Introduction

The purpose of this document is to cover parameter value details that are used for each of the components/services deployed using Azure Scaffold Json template available on GitHub repo (<https://github.com/rajanbhayana/AzureScaffoldingHubAndSpokeTemplate>)

* 1. Virtual networks & Subnets

The following table provides IP prefixes allocated for vNets and all subnets allocation to deployed Azure Services, such as Bastion, App Gateway, Firewall, multiple Tiers etc.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Azure Subs | Address Space | IP Range | Gateway Subnet | AzureBastion Subnet | Azure Firewall | Shared | Application Gateway | Web Tier | App Tier | Data Tier | Free/ Available Prefixes |
| HUB | 10.0.0.0/19 | 10.0.0.0 - 10.0.31.255 | 10.0.0.0/26 | 10.0.0.64/27 | 10.0.6.0/23 | 10.0.1.0/24 10.0.2.0/23 10.0.4.0/23 | 10.0.0.128/26 |  |  |  | 10.0.0.96/27 10.0.0.192/26 10.0.8.0/21 10.0.16.0/20 |
| Production | 10.0.32.0/19 | 10.0.32.0 - 10.0.63.255 | NA | 10.0.32.0/26 |  |  |  | 10.0.34.0/23 | 10.0.36.0/23 | 10.0.38.0/23 | 10.0.32.64/26 10.0.32.128/25 10.0.33.0/24 10.0.40.0/21 10.0.48.0/20 |

Table Virtual Networks & Subnets

* 1. Network Security Groups

The following sample NSG rules will be created, and these rules can be altered in the json template to meet specific technical requirements.

* Subnet to Subnet connectivity is allowed through NSG rules
* Traffic from ‘VirtualNetwork’ tag to ‘10.0.4.0/23’ is allowed on Domain Controller specific ports with an assumption that ‘10.0.4.0/23’ will be hosting Active directory domain controllers.
* Traffic from App Tier Subnet to Web Tier Subnet has been allowed.
* Traffic from App Tier Subnet to Data Tier Subnet has been allowed.
  + 1. HUB NSG Rules

The following table covers NSG rules applied within Hub Subscription. NSG and Subnet association details are captured under Table 6 Hub Subnets.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| NSGName | ResourceGroup | RuleName | Priority | SourceAddressPrefix | DestinationAddressPrefix | DestinationPortRange | Protocol | Access | Direction | SourcePortRange |
| dbs-hubshdnsg2 | dbs-hubrsg01 | DenyOutbound | 4092 | 10.0.0.0/16 | 10.0.0.0/16 | 1-65535 | \* | Deny | Outbound | \* |
| dbs-hubshdnsg2 | dbs-hubrsg01 | AllowSubnetOutbound | 4091 | 10.0.1.0/24 | 10.0.1.0/24 | \* | \* | Allow | Outbound | \* |
| dbs-hubshdnsg2 | dbs-hubrsg01 | AllowClientToDC | 3500 | VirtualNetwork | 10.0.4.0/23 | 53,88,123,135,137,138,139,389,445,464,636,3268,3269,49152-65535 | \* | Allow | Outbound | \* |
| dbs-hubshdnsg3 | dbs-hubrsg01 | DenyOutbound | 4092 | 10.0.0.0/16 | 10.0.0.0/16 | 1-65535 | \* | Deny | Outbound | \* |
| dbs-hubshdnsg3 | dbs-hubrsg01 | AllowSubnetOutbound | 4091 | 10.0.2.0/23 | 10.0.2.0/23 | \* | \* | Allow | Outbound | \* |
| dbs-hubshdnsg3 | dbs-hubrsg01 | AllowClientToDC | 3500 | VirtualNetwork | 10.0.4.0/23 | 53,88,123,135,137,138,139,389,445,464,636,3268,3269,49152-65535 | \* | Allow | Outbound | \* |
| dbs-hubshdnsg4 | dbs-hubrsg01 | DenyOutbound | 4092 | 10.0.0.0/16 | 10.0.0.0/16 | 1-65535 | \* | Deny | Outbound | \* |
| dbs-hubshdnsg4 | dbs-hubrsg01 | AllowSubnetOutbound | 4091 | 10.0.4.0/23 | 10.0.4.0/23 | \* | \* | Allow | Outbound | \* |

Table HUB NSG Rules

* + 1. Prod NSG Rules

The following table covers NSG rules applied within Prod Subscription. NSG and Subnet association details are captured under Table 7 Prod Subnets.Table 6 Hub Subnets

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| NSGName | ResourceGroup | RuleName | Priority | SourceAddressPrefix | DestinationAddressPrefix | DestinationPortRange | Protocol | Access | Direction | SourcePortRange |
| dbs-hubshdnsg2 | dbs-prdrsg01 | DenyOutbound | 4092 | 10.0.0.0/16 | 10.0.0.0/16 | 1-65535 | \* | Deny | Outbound | \* |
| dbs-hubshdnsg2 | dbs-prdrsg01 | AllowSubnetOutbound | 4091 | 10.0.34.0/23 | 10.0.34.0/23 | \* | \* | Allow | Outbound | \* |
| dbs-hubshdnsg2 | dbs-prdrsg01 | AllowWebToAppSubnet | 4090 | 10.0.34.0/23 | 10.0.36.0/23 | \* | \* | Allow | Outbound | \* |
| dbs-hubshdnsg2 | dbs-prdrsg01 | AllowClientToDC | 3500 | VirtualNetwork | 10.0.4.0/23 | 53,88,123,135,137,138,139,389,445,464,636,3268,3269,49152-65535 | \* | Allow | Outbound | \* |
| dbs-prdappnsg3 | dbs-prdrsg01 | DenyOutbound | 4092 | 10.0.0.0/16 | 10.0.0.0/16 | 1-65535 | \* | Deny | Outbound | \* |
| dbs-prdappnsg3 | dbs-prdrsg01 | AllowSubnetOutbound | 4091 | 10.0.36.0/23 | 10.0.36.0/23 | \* | \* | Allow | Outbound | \* |
| dbs-prdappnsg3 | dbs-prdrsg01 | AllowAppToDataSubnet | 4090 | 10.0.36.0/23 | 10.0.38.0/23 | \* | \* | Allow | Outbound | \* |
| dbs-prdappnsg3 | dbs-prdrsg01 | AllowClientToDC | 3500 | VirtualNetwork | 10.0.4.0/23 | 53,88,123,135,137,138,139,389,445,464,636,3268,3269,49152-65535 | \* | Allow | Outbound | \* |
| dbs-prddtansg4 | dbs-prdrsg01 | DenyOutbound | 4092 | 10.0.0.0/16 | 10.0.0.0/16 | 1-65535 | \* | Deny | Outbound | \* |
| dbs-prddtansg4 | dbs-prdrsg01 | AllowSubnetOutbound | 4091 | 10.0.38.0/23 | 10.0.38.0/23 | \* | \* | Allow | Outbound | \* |
| dbs-prddtansg4 | dbs-prdrsg01 | AllowClientToDC | 3500 | VirtualNetwork | 10.0.4.0/23 | 53,88,123,135,137,138,139,389,445,464,636,3268,3269,49152-65535 | \* | Allow | Outbound | \* |

Table Prod NSG Rules

* + 1. Hub Subnets

The following table provide details of Subnets, NSG, UDR and NAT Gateway association and mapping for Hub Subscription.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SubnetName | Prefixes | NetworkSecurityGroup | UDRName | NatGateway |
| GatewaySubnet | 10.0.0.0/26 |  |  |  |
| AzureBastionSubnet | 10.0.0.64/27 | dbs-hubbasnsg1 | dbs-hubudr1 |  |
| dbs-hubshdsnt2 | 10.0.1.0/24 | dbs-hubshdnsg2 | dbs-hubudr2 | dbs-hubnat01 |
| dbs-hubshdsnt3 | 10.0.2.0/23 | dbs-hubshdnsg3 | dbs-hubudr3 | dbs-hubnat01 |
| dbs-hubshdsnt4 | 10.0.4.0/23 | dbs-hubshdnsg4 | dbs-hubudr4 | dbs-hubnat01 |
| dbs-hubagwsnt5 | 10.0.0.128/26 | dbs-hubagwnsg5 | dbs-hubudr5 |  |
| AzureFirewallSubnet | 10.0.6.0/24 |  |  |  |

Table Hub Subnets

* + 1. Prod Subnets

The following table provide details of Subnets, NSG, UDR and NAT Gateway association and mapping for Prod subscription.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SubnetName | Prefixes | NetworkSecurityGroup | UDRName | NatGateway |
| AzureBastionSubnet | 10.0.32.0/26 | dbs-prdbasnsg01 |  |  |
| dbs-prdwebsnt2 | 10.0.34.0/23 | dbs-prdwebnsg2 | dbs-prdudr2 | dbs-prdnat01 |
| dbs-prdappsnt3 | 10.0.36.0/23 | dbs-prdappnsg3 | dbs-prdudr3 | dbs-prdnat01 |
| dbs-prddtasnt4 | 10.0.38.0/23 | dbs-prddtansg4 | dbs-prdudr4 | dbs-prdnat01 |

Table Prod Subnets

* 1. Virtual Network Gateway

The following table provide details of parameter for vNet Gateway deployed in the Hub Subscription.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| name | sku | gatewayType | publicIpAddressId | subnetId | privateIPAllocationMethod |
| dbs-hubvgw01 | HighPerformance | ExpressRoute | dbs-hubvgwpip01 | dbs-hubvnet01 | Dynamic |

Table vNet Gateway

* 1. Express Route

The following table provide details of parameter for Express Route deployed in the Hub Subscription.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Subscription | ResourceType | circuitName | serviceProviderName | peeringLocation | bandwidthInMbps | sku\_tier | sku\_family |
| HUB | ExpressRoute | dbs-hubexr01 | Equinix | Sydney | 50 | Standard | MeteredData |

* 1. Bastion

The following table provide parameter details for Bastion service for all environments.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Subscription | ResourceType | bastionHostName | subnetId | publicIpAddressName |
| HUB | bastion | dbs-hubbtn01 | AzureBastionSubnet | dbs-hubbtnpip01 |
| Production | bastion | dbs-prdbtn01 | AzureBastionSubnet | dbs-prdbtnpip01 |
| PreProd | bastion | dbs-ppdbtn01 | AzureBastionSubnet | dbs-ppdbtnpip01 |
| NonProd | bastion | dbs-npdbtn01 | AzureBastionSubnet | dbs-npdbtnpip01 |

Table Azure Bastion Service

* 1. Application Gateway

The following table provide parameter details for Application Gateway service which will be provisioned in the Hub subscription.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Subs | Resource Type | name | sku name | publicIpAddressId | capacity | AGWafPol01 | subnet | FrontendIPConfiguration |
| HUB | ApplicationGateway | dbs-hubagw01 | WAF\_v2 | dbs-hubagwpip01 | 2 | WafPol01 | dbs-hubagwsnt5 | dbs-hubagwpip01 |

* 1. Azure Firewall

The following table provide parameter details for Azure Firewall service which will be provisioned in the Hub subscription.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Subscription | ResourceType | name | subnet | publicIpAddressId |
| HUB | AzureFirewall | dbs-hubfwl01 | AzureFirewallSubnet | dbs-hubfwlpip01 |

Table Azure Firewall

* 1. NAT Gateway

The following table provide parameter details for NAT Gateway service which will be deployed in the Hub subscription.

|  |  |  |  |
| --- | --- | --- | --- |
| Subscription | ResourceType | NATGatewayName | publicIpAddressName |
| HUB | Nat Gateway | dbs-hubnat01 | dbs-hubnatpip04 |
| Production | Nat Gateway | dbs-prdnat01 | dbs-prdnatpip02 |

Table NAT Gateway

* 1. Other Services

The following table provides parameter details for Log Analytics and Azure Backup Vault services.

|  |  |  |
| --- | --- | --- |
| Subscription | ResourceType | Name |
| HUB | Log Analytics | dbs-hubla01 |
| HUB | Azure Backup Vault | dbs-hubvault01 |
| Production | Azure Backup Vault | dbs-prdvault01 |

* 1. Naming Convention

The following table covers Naming Codes used in the Azure Scaffold templates for naming convention purpose.

Location Code – Dbs

Naming Convention – <LocationCode><SubscriptionCode><ServiceCode><Numbers ..0..1>

For e.g. Hub NAT Gateway Name – ‘Dbs-hubnat01’

|  |  |
| --- | --- |
| ServiceName | Code |
| HUB Sub | hub |
| Production Sub | prd |
| PreProd Sub | ppd |
| NonProd Sub | npd |
| VirtualNetwork | vnet |
| NSG | nsg |
| UDR | udr |
| ResourceGroup | rsg |
| AzureBastionSubnet | bas |
| perimeter | prm |
| shared | shd |
| web | web |
| app | app |
| data | dta |
| ApplicationGateway | agw |
| Subnet | snt |
| Development | dev |
| Test/UAT | tst |
| Sandbox | sdx |
| vNetGateway | vgw |
| PublicIPAddress | pip |
| ExpressRoute | exr |
| bastion | btn |
| AzureFirewall | fwl |
| NAT Gateway | nat |

Table Service Codes and Naming Conventions