Revision and Signoff Sheet

Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Change Reference |
| 12 May 2020 | Sumit Kumar | 0.1 | Initial Draft |
|  |  |  |  |

Reviewers

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Name | Version Approved | Position |
| 19 May 2020 | Rajan Bhayana | 0.1 | Cloud Solution Architect |
| 19 May 2020 | Tae Hwang | 0.1 | Cloud Solution Architect |

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 |
| Pre-Prod | 10.0.64.0/19 | 10.0.64.0 - 10.0.95.255 | NA | 10.0.64.0/26 |  |  |  | 10.0.66.0/23 | 10.0.68.0/23 | 10.0.70.0/23 | 10.0.64.64/26 10.0.64.128/25 10.0.65.0/24 10.0.72.0/21 10.0.80.0/20 |
| Non-Prod (Ent Dev/Test Sub) | 10.0.96.0/19 | 10.0.96.0 - 10.0.127.255 | NA | 10.0.96.0/26 |  |  |  | 10.0.98.0/23 | 10.0.100.0/23 | 10.0.102.0/23 | 10.0.96.64/26 10.0.96.128/25 10.0.97.0/24 10.0.104.0/21 10.0.112.0/20 |

Table 1 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 |
| auehubshdnsg2 | auehubrsg01 | DenyOutbound | 4092 | 10.0.0.0/16 | 10.0.0.0/16 | 1-65535 | \* | Deny | Outbound | \* |
| auehubshdnsg2 | auehubrsg01 | AllowSubnetOutbound | 4091 | 10.0.1.0/24 | 10.0.1.0/24 | \* | \* | Allow | Outbound | \* |
| auehubshdnsg2 | auehubrsg01 | 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 | \* |
| auehubshdnsg3 | auehubrsg01 | DenyOutbound | 4092 | 10.0.0.0/16 | 10.0.0.0/16 | 1-65535 | \* | Deny | Outbound | \* |
| auehubshdnsg3 | auehubrsg01 | AllowSubnetOutbound | 4091 | 10.0.2.0/23 | 10.0.2.0/23 | \* | \* | Allow | Outbound | \* |
| auehubshdnsg3 | auehubrsg01 | 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 | \* |
| auehubshdnsg4 | auehubrsg01 | DenyOutbound | 4092 | 10.0.0.0/16 | 10.0.0.0/16 | 1-65535 | \* | Deny | Outbound | \* |
| auehubshdnsg4 | auehubrsg01 | AllowSubnetOutbound | 4091 | 10.0.4.0/23 | 10.0.4.0/23 | \* | \* | Allow | Outbound | \* |

Table 2 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 |
| auehubshdnsg2 | aueprdrsg01 | DenyOutbound | 4092 | 10.0.0.0/16 | 10.0.0.0/16 | 1-65535 | \* | Deny | Outbound | \* |
| auehubshdnsg2 | aueprdrsg01 | AllowSubnetOutbound | 4091 | 10.0.34.0/23 | 10.0.34.0/23 | \* | \* | Allow | Outbound | \* |
| auehubshdnsg2 | aueprdrsg01 | AllowWebToAppSubnet | 4090 | 10.0.34.0/23 | 10.0.36.0/23 | \* | \* | Allow | Outbound | \* |
| auehubshdnsg2 | aueprdrsg01 | 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 | \* |
| aueprdappnsg3 | aueprdrsg01 | DenyOutbound | 4092 | 10.0.0.0/16 | 10.0.0.0/16 | 1-65535 | \* | Deny | Outbound | \* |
| aueprdappnsg3 | aueprdrsg01 | AllowSubnetOutbound | 4091 | 10.0.36.0/23 | 10.0.36.0/23 | \* | \* | Allow | Outbound | \* |
| aueprdappnsg3 | aueprdrsg01 | AllowAppToDataSubnet | 4090 | 10.0.36.0/23 | 10.0.38.0/23 | \* | \* | Allow | Outbound | \* |
| aueprdappnsg3 | aueprdrsg01 | 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 | \* |
| aueprddtansg4 | aueprdrsg01 | DenyOutbound | 4092 | 10.0.0.0/16 | 10.0.0.0/16 | 1-65535 | \* | Deny | Outbound | \* |
| aueprddtansg4 | aueprdrsg01 | AllowSubnetOutbound | 4091 | 10.0.38.0/23 | 10.0.38.0/23 | \* | \* | Allow | Outbound | \* |
| aueprddtansg4 | aueprdrsg01 | 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 3 Prod NSG Rules

* + 1. Pre-Prod NSG Rules

The following table covers NSG rules applied within Pre-Prod Subscription. NSG and Subnet association details are captured under Table 8 Pre-Prod Subnets.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| NSGName | ResourceGroup | RuleName | Priority | SourceAddressPrefix | DestinationAddressPrefix | DestinationPortRange | Protocol | Access | Direction | SourcePortRange |
| aueppdwebnsg2 | aueppdrsg01 | DenyOutbound | 4092 | 10.0.0.0/16 | 10.0.0.0/16 | 1-65535 | \* | Deny | Outbound | \* |
| aueppdwebnsg2 | aueppdrsg01 | AllowSubnetOutbound | 4091 | 10.0.66.0/23 | 10.0.66.0/23 | \* | \* | Allow | Outbound | \* |
| aueppdwebnsg2 | aueppdrsg01 | AllowWebToAppSubnet | 4090 | 10.0.66.0/23 | 10.0.68.0/23 | \* | \* | Allow | Outbound | \* |
| aueppdwebnsg2 | aueppdrsg01 | 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 | \* |
| aueppdappnsg3 | aueppdrsg01 | DenyOutbound | 4092 | 10.0.0.0/16 | 10.0.0.0/16 | 1-65535 | \* | Deny | Outbound | \* |
| aueppdappnsg3 | aueppdrsg01 | AllowSubnetOutbound | 4091 | 10.0.68.0/23 | 10.0.68.0/23 | \* | \* | Allow | Outbound | \* |
| aueppdappnsg3 | aueppdrsg01 | AllowAppToDataSubnet | 4090 | 10.0.68.0/23 | 10.0.70.0/23 | \* | \* | Allow | Outbound | \* |
| aueppdappnsg3 | aueppdrsg01 | 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 | \* |
| aueppddtansg4 | aueppdrsg01 | DenyOutbound | 4092 | 10.0.0.0/16 | 10.0.0.0/16 | 1-65535 | \* | Deny | Outbound | \* |
| aueppddtansg4 | aueppdrsg01 | AllowSubnetOutbound | 4091 | 10.0.70.0/23 | 10.0.70.0/23 | \* | \* | Allow | Outbound | \* |
| aueppddtansg4 | aueppdrsg01 | 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 4 Pre-Prod 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 9 Non-Prod Subnets.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| NSGName | ResourceGroup | RuleName | Priority | SourceAddressPrefix | DestinationAddressPrefix | DestinationPortRange | Protocol | Access | Direction | SourcePortRange |
| auenpddevnsg2 | auenpdrsg01 | DenyOutbound | 4092 | 10.0.0.0/16 | 10.0.0.0/16 | 1-65535 | \* | Deny | Outbound | \* |
| auenpddevnsg2 | auenpdrsg01 | AllowDevOutbound | 4091 | 10.0.98.0/23 | 10.0.98.0/23 | \* | \* | Allow | Outbound | \* |
| auenpddevnsg2 | auenpdrsg01 | 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 | \* |
| auenpdtstnsg3 | auenpdrsg01 | DenyOutbound | 4092 | 10.0.0.0/16 | 10.0.0.0/16 | 1-65535 | \* | Deny | Outbound | \* |
| auenpdtstnsg3 | auenpdrsg01 | AllowUATOutbound | 4091 | 10.0.100.0/23 | 10.0.100.0/23 | \* | \* | Allow | Outbound | \* |
| auenpdtstnsg3 | auenpdrsg01 | 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 | \* |
| auenpdsdxnsg4 | auenpdrsg01 | DenyOutbound | 4092 | 10.0.0.0/16 | 10.0.0.0/16 | 1-65535 | \* | Deny | Outbound | \* |
| auenpdsdxnsg4 | auenpdrsg01 | AllowSBXOutbound | 4091 | 10.0.102.0/23 | 10.0.102.0/23 | \* | \* | Allow | Outbound | \* |
| auenpdsdxnsg4 | auenpdrsg01 | 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 5 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 | auehubbasnsg1 | auehubudr1 |  |
| auehubshdsnt2 | 10.0.1.0/24 | auehubshdnsg2 | auehubudr2 | auehubnat01 |
| auehubshdsnt3 | 10.0.2.0/23 | auehubshdnsg3 | auehubudr3 | auehubnat01 |
| auehubshdsnt4 | 10.0.4.0/23 | auehubshdnsg4 | auehubudr4 | auehubnat01 |
| auehubagwsnt5 | 10.0.0.128/26 | auehubagwnsg5 | auehubudr5 |  |
| AzureFirewallSubnet | 10.0.6.0/24 |  |  |  |

Table 6 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 | aueprdbasnsg01 |  |  |
| aueprdwebsnt2 | 10.0.34.0/23 | aueprdwebnsg2 | aueprdudr2 | aueprdnat01 |
| aueprdappsnt3 | 10.0.36.0/23 | aueprdappnsg3 | aueprdudr3 | aueprdnat01 |
| aueprddtasnt4 | 10.0.38.0/23 | aueprddtansg4 | aueprdudr4 | aueprdnat01 |

Table 7 Prod Subnets

* + 1. Pre-Prod Subnets

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SubnetName | Prefixes | NetworkSecurityGroup | UDRName | NatGateway |
| AzureBastionSubnet | 10.0.64.0/26 | aueppdbasnsg01 |  |  |
| aueppdwebsnt2 | 10.0.66.0/23 | aueppdwebnsg2 | aueppdudr2 | aueppdnat01 |
| aueppdappsnt3 | 10.0.68.0/23 | aueppdappnsg3 | aueppdudr3 | aueppdnat01 |
| aueppddtasnt4 | 10.0.70.0/23 | aueppddtansg4 | aueppdudr4 | aueppdnat01 |

Table 8 Pre-Prod Subnets

* + 1. Non-Prod Subnets

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SubnetName | Prefixes | NetworkSecurityGroup | UDRName | NatGateway |
| AzureBastionSubnet | 10.0.96.0/26 | auenpdbasnsg01 |  |  |
| auenpddevsnt2 | 10.0.98.0/23 | auenpddevnsg2 | auenpdudr2 | auenpdnat01 |
| auenpdtstsnt3 | 10.0.100.0/23 | auenpdtstnsg3 | auenpdudr3 | auenpdnat01 |
| auenpdsdxsnt4 | 10.0.102.0/23 | auenpdsdxnsg4 | auenpdudr4 | auenpdnat01 |

Table 9 Non-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 |
| auehubvgw01 | HighPerformance | ExpressRoute | auehubvgwpip01 | auehubvnet01 | Dynamic |

Table 10 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 | auehubexr01 | 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 | auehubbtn01 | AzureBastionSubnet | auehubbtnpip01 |
| Production | bastion | aueprdbtn01 | AzureBastionSubnet | aueprdbtnpip01 |
| PreProd | bastion | aueppdbtn01 | AzureBastionSubnet | aueppdbtnpip01 |
| NonProd | bastion | auenpdbtn01 | AzureBastionSubnet | auenpdbtnpip01 |

Table 11 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 | auehubagw01 | WAF\_v2 | auehubagwpip01 | 2 | WafPol01 | auehubagwsnt5 | auehubagwpip01 |

* 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 | auehubfwl01 | AzureFirewallSubnet | auehubfwlpip01 |

Table 12 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 | auehubnat01 | auehubnatpip04 |
| Production | Nat Gateway | aueprdnat01 | aueprdnatpip02 |
| PreProd | Nat Gateway | aueppdnat01 | aueppdnatpip02 |
| NonProd | Nat Gateway | auenpdnat01 | auenpdnatpip02 |

Table 13 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 | aehubla01 |
| HUB | Azure Backup Vault | aehubvault01 |
| Production | Azure Backup Vault | aeprdvault01 |
| PreProd | Azure Backup Vault | aeppdvault01 |
| NonProd | Azure Backup Vault | aenpdvault01 |

* 1. Naming Convention

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

Location Code – Aue

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

For e.g. Hub NAT Gateway Name – ‘Auehubnat01’

|  |  |
| --- | --- |
| 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 14 Service Codes and Naming Conventions