Proprietary Notice

Point of Contact

AkzoNobel

Customer Operation Guide

for

Azure Virtual WAN

~~16th February 2022~~25th February 2022

Strictly Confidential

Name:	Sarah Gardner		
Title:	Solution Manager	Email:	sarah.gardner@orange.com
Tel:	+44 (0)208 321 4235	Mobile:	+44 (0) 7966861570
Address:	4th Floor, 1, Brunel Way, Slough, Berkshire, SL1 1FQ United Kingdom		
Website:	http://www.orange-business.com		

Table of Contents

1. Introduction

This operation guide is to provide guidance and assist operations team to perform their functions efficiently, reliably and consistently to support implementation of Microsoft Azure Virtual WAN [vWAN][1] product in AkzoNobel azure environments.

Purpose of this document is also to provide overview of vWAN solution delivered as part of the "Hub & Spoke Improvement Project" and serve as a guide for the operations team, to have complete visibility in to delivered solution and its operational aspects.

"HUB & Spoke Improvement Project", while delivering improved availability and enhanced security for the spokes (Azure Virtual Networks [vNets][2]), it also brought cultural shift, by providing separate test and production environments for the spokes.

AkzoNobel business teams will now have access to a separate test environment where they can spin up development/test spokes and do the testing before commissioning the services in production Azure Virtual WAN [vWAN] environment, where only production spokes will be connected, providing clear segregation among development/test and production environments. Both development/test and production environments are hosted in different Azure Subscriptions[3], to provide ability of granular and distinct control over resources hosted within each environment.

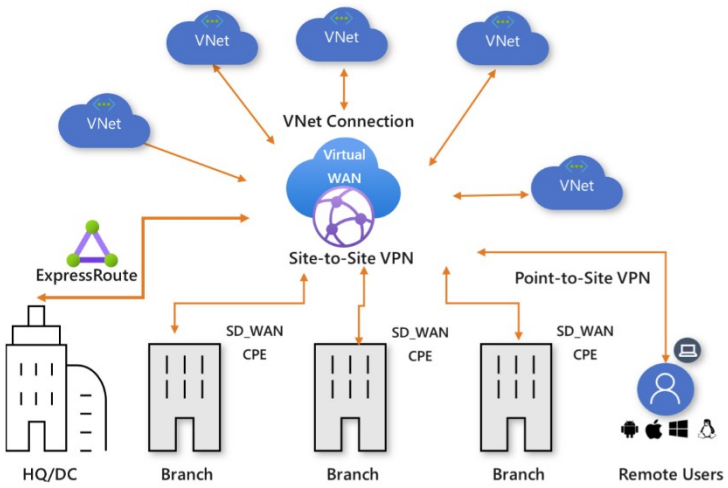
[1] https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about
[2] https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview
[3] https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/considerations/fundamental-concepts

2. Overview of Azure Virtual WAN [vWAN]

2.1 General Architecture

The Azure Virtual WAN architecture is a hub and spoke architecture with scale and performance built in for virtual networks, ExpressRoute circuits, branches, and users.

It enables a global transit network architecture, where the cloud hosted network 'hub' enables transitive connectivity between endpoints that may be distributed across different types of 'spokes'.



2.2 Azure Virtual WAN Resources

Following features can be enabled as part of an Azure Virtual WAN:

- Virtual Hub
- Secured Virtual Hub – Virtual HUB With Azure Firewall
- ExpressRoute Gateway
- Site-to-Site VPN Gateway
- Point-to-Site VPN Gateway
- Network Virtual Appliance (Limited Vendors)
- Security Partner Providers (Limited Vendors)
- Hub Virtual Network Connections

2.3 AkzoNobel Virtual WAN [vWAN] Setup

2.3.1 Spokes/Virtual Networks [vNets]

Spokes in this context are primarily the Azure Virtual Networks [vNets] spread across different Azure Subscriptions associated with AkzoNobel Azure Tenant/Account.

There are two Spokes (Central Finance SAP), which are hosted on non-AkzoNobel Tenant. Connectivity method for such spokes is also different and is specifically detailed later in this document for clarity.

Below, is the broad classification of spokes based on their requirements.

Type of Spokes	Description
Normal Spokes	All normal spokes are hosted within AkzoNobel Azure Tenant, however spread across among different Azure Subscriptions within the tenant as assigned for specific purposes. Additionally, these are the spokes, which either do not have Internet requirements or connect to Internet using Z-Scaler Service connected to Secured virtual Hub. These spokes do not have any user defined routes [UDRs] attached to them.
Spokes with Partial Local Internet Breakout	Like normal spokes, these spokes (virtual networks) are also hosted within AkzoNobel Azure Tenant, however these spokes use user defined routes [UDRs] to reach out to *specific public Prefixes* directly (as required) from the virtual network. However, these spokes still use Z-Scaler Service for General Internet Connectivity Requirements.
Spokes with Complete Local Internet Breakout	Like normal spokes, these spokes (virtual networks) are also hosted within AkzoNobel Azure Tenant, however these spokes use user defined routes [UDRs] to reach out to *general Internet* directly (for all their Internet needs) from the virtual network. These spokes do not use Z-Scaler Service.
Spokes hosted on Non-AkzoNobel Tenant	These are the Spokes which are hosted on Non AkzoNobel Azure Tenant. These have a unique way using which these are connected with Secured virtual Hub[4], and due to the nature of arrangement this connection is not visible in Azure Portal GUI in Virtual Network Connections on Secured Virtual Hub

Key Points:

[4] https://docs.microsoft.com/en-us/azure/virtual-wan/cross-tenant-vnet

[1.] In General, Spokes/vNets, migrated to vWAN solution, will have private traffic ~~(10.0.0.0/8,134.239.0.0/16,145.82.0.0/16,147.82.0.0/16)~~ secured using Azure Firewall.

Note:

- *Private traffic is any network communications that originate from and terminate within AkzoNobel networks. The IP address ranges shared by AkzoNobel CCC team are: 10.0.0.0/8, 134.239.0.0/16, 145.82.0.0/16 and 147.82.0.0/16*
- *There are some IP address ranges assigned to Azure virtual networks as part of 10.0.0.0/8 address space which are untrusted networks. No specific rules exist to identify and classify these.*

~~1.~~ In General, Spokes/vNets, migrated to vWAN solution, will have internet traffic secured using Z-Scaler Service connected to secured virtual Hub.

[2.]

Note: *Some Spokes may still have connectivity to Internet directly from vNET using user defined routes [UDRs], for their specific needs and this is guided by the Spoke Owners and their requirements.*

2.[3.] List of spokes/virtual networks in scope of migration to Azure Virtual WAN environment are listed in Appendix E

2.3.2 Azure Virtual WAN

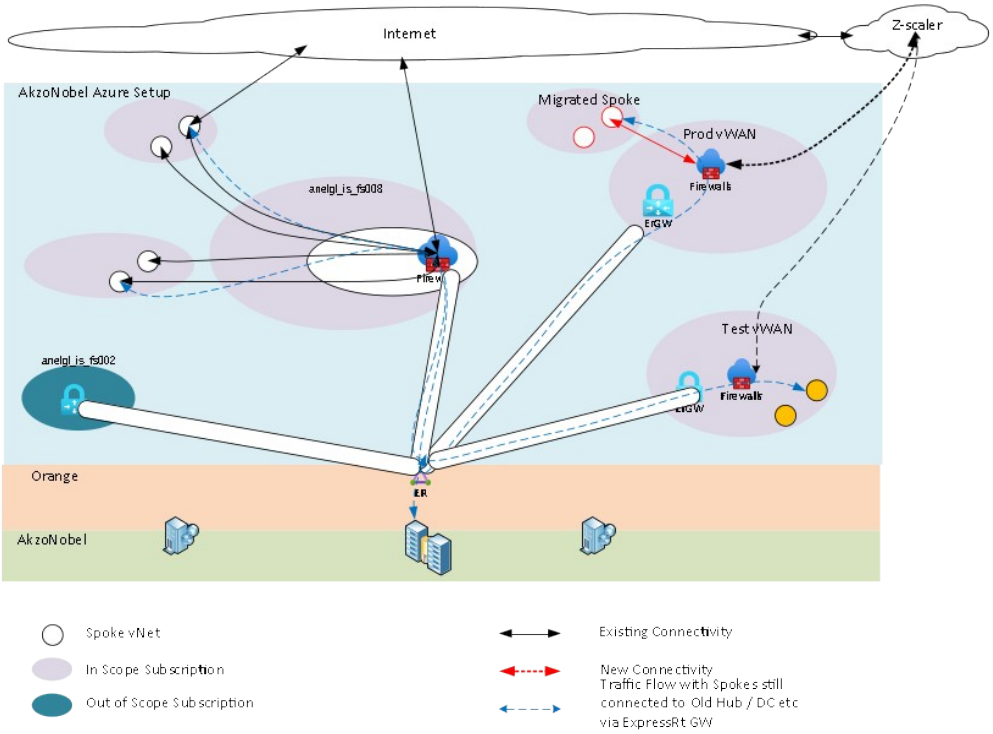
~~There are two types of Azure Virtual WANs:~~

- ~~Basic~~
- ~~Standard~~

~~The following table shows the available configurations for each type.~~

~~Virtual WAN Type~~	~~Hub Type~~	~~Configuration~~
~~Basic~~	~~Basic~~	~~Site-to-Site VPN Only~~
~~Standard~~	~~Standard~~	~~ExpressRoute~~ ~~Point-to-Site VPN~~ ~~Site-to-Site VPM~~ ~~Azure Firewall~~ ~~Network Virtual Appliance~~

As part of this project separate Test and Production "***Standard***" vWAN type environments have been deployed, with Secured Virtual Hub hosted in "West Europe" Azure region.



2.3.3 Secured Virtual Hub

Secured virtual hub is used to filter traffic between virtual networks (V2V), virtual networks and datacentre/branch offices (V2B) and traffic to the Internet (B2I/V2I). A secured virtual hub provides automated routing. There's no need to configure UDRs (user defined routes) to route traffic through ~~your~~ firewall.

Note: *The datacentre, branch offices address/networks are advertised to Virtual WAN through ExpressRoute setup through Orange BVPN.*

~~A vWAN environment can have only one secured virtual hub per region but can have multiple VHubs within a region. By default a VWAN provides full mesh connectivity between all hubs and regions by using the Microsoft Backbone.~~

Currently the project has delivered both test and production environments with a secure hub in the European region. Each environment has spokes/virtual networks connected to them.

Below listed features are enabled for each secured virtual hub:

- Azure Firewall
- ExpressRoute Gateway
- Special Site-to-Site VPN Gateway [with Security Partner Provider: ZScaler]

a. This is a special integration between Microsoft and Zscaler using a automated S2S VPN for the connection.

2.3.4 ExpressRoute Gateway

ExpressRoute Gateway is used to enable Peering of Secured virtual Hub in West EU with existing ExpressRoute Circuit in West EU region. This enables connectivity from secured virtual hub (West EU) to AkzoNobel On-Prem Environments and other ExpressRoute peered locations within AkzoNobel's Azure Tenant, such as previous Hub and Spoke Solution and such like.

New Address Prefixes Introduced

As Recommended, by Microsoft, secured virtual hubs have been allocated /23 address ranges for its internal usage. Below is the address allocation table for the development/test and production environments:

Note: *Usage of this /23 Address space is completely controlled by Microsoft, to enable connectivity among different features are not available for design considerations.*

Resource Type	Resource Group Name	Resource Name	Environment	Location	Network Prefix
vHub	to_10173	hub-01-we-test	Test	West EU	10.239.0.0/23
vHub	po_10173	hub-01-we-prod	Production	West EU	10.239.2.0/23
vNet	to_10173	cc-vnet-test01-we-test	Test	West EU	10.239.4.0/24
vNet	to_10173	cc-vnet-test02-we-test	Test	West EU	10.239.5.0/24

Any new prefix introduced to the Azure Tenant will need address prefix filters to be updated on ExpressRoute Circuit (see contacts for Express Route and Orange change control appendix C) to ensure these networks are learnt in AkzoNobel on-premises network. Under a change control process prefix filters were updated to start learning these prefixes in AkzoNobel on-premises networks.

2.3.5 Site-to-Site Virtual Private Network (VPN) Gateway

This service is indirectly enabled on the production environment secured virtual hub in order to support Security Partner Provider Service with Zscaler. Virtual Private Network Gateway service is enabled and configured using integration scripts from Microsoft and Zscaler using parameter information supplied during configuration.

AkzoNobel, uses Z-Scaler as a Security Partner Provider to extend, Proxy Internet Services to the spokes connected to secured virtual hubs in development/test and production environments.

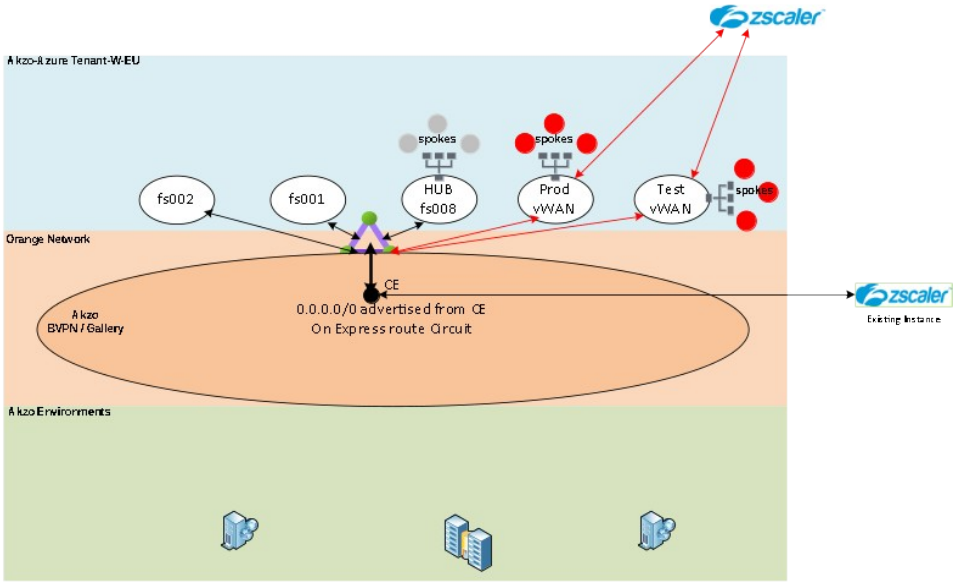
Note: When implementing in the test environment, a limitation was discovered in the integration implementation for the Zscaler service. In order to deliver this project the project team agreed with Akzo Noble to update the design, and not connect via the Zscaler service, and instead provide connectivity to internet via Azure Firewall. Test spokes breakout to internet directly using UDRs or via Azure firewall.

2.3.6 Security Partner Provider [Z-Scaler Service]

Secured Virtual Hub in production environment uses Site-to-Site Virtual Private Network Gateway to connect to Z-Scaler Service, which provides internet Services using Proxy Services. This VPN connectivity is done completely in the background and Microsoft manages the same via its own infrastructure backbone and AkzoNobel do not control any parameters of the same.

On ZIA portal (Z-Scaler, Akzo Tenant) (contact see Appendix C), two Azure locations have been created and they possess the same config as any other AkzoNobel sites for Proxy Internet Services.

Below Diagram Provides view of Z-Scaler connectivity with production vWAN environments.



To enable the Z-Scaler Service on secured virtual hub a Service Principal Account has been created on Azure AD to be used by ZIA (Z-Scaler Admin) portal. Below are the details of Service Principal Accounts, for production.

- ***ccc_Azure Virtual WAN Zscaler***

2.3.7 Azure Firewall

Azure Firewall is a cloud-native, ~~and~~ intelligent network firewall security service that provides the threat protection for cloud workloads running in Azure. It's a fully stateful, firewall as a service with built-in high availability and unrestricted cloud scalability. It

provides both east-west and north-south traffic inspection. Azure Firewall is offered in two SKUs:

- Standard
- Premium

For AkzoNobel "***Standard***" SKU of Azure Firewall [managed using Azure Firewall Manager] is used to secure all Private Traffic to and from Spokes and other services connected to the secured virtual hub.

Trusted Spokes/Virtual Networks

✓ All traffic originating from data center along with networks with below pre-fixes are considered trusted:
- *134.239.0.0/16*
- *145.82.0.0/16*
- *147.82.0.0/16*
- *10.0.0.0/8 [Except ones specifically listed as un-trusted]*

✓ In addition, traffic originated from HCL spokes/virtual networks listed below are also considered trusted:
- *znepn0001nv0001*
- *zncpn0001nv0001*

Untrusted Spokes

✓ Traffic originated from spokes/virtual networks listed below are considered un-trusted:

- *akz-lnd1-p-euwe-vnet-spoke*
- *akz-lnd2-p-euwe-vnet-spoke*
- *apim-vnet-sa-prod*
- *apim-vnet-us-prod*
- *apim-vnet-we-dev*
- *apim-vnet-we-prod*
- *apim-vnet-we-test*
- *dp-vnet-znf-we-prod*
- *dp-vnet-znf-we-test*
- *ecs-vnet-znf-we-prod*
- *ecs-vnet-znf-we-test*
- *elephant-vnet-znf-we-dev*
- *ocap-vnet-znf-deploy-we-prod*
- *ocap-vnet-znf-we-acc*
- *ocap-vnet-znf-we-dev*
- *ocap-vnet-znf-we-prod*
- *onehub-vnet-znf-we-dev*
- *onehub-vnet-znf-we-test*
- *sharedcolor-vnet-znf-we-prod*
- *sharedcolor-vnet-znf-we-test*
- *sharedgbs-vnet-znf-we-prod*
- *sharedgbs-vnet-znf-we-test*
- *sharediot-vnet-znf-we-prod*
- *sharediot-vnet-znf-we-test*
- *sharedisc-vnet-znf-we-prod*
- *sharedisc-vnet-znf-we-test*
- *sharedit-vnet-znf-we-prod*
- *sharedit-vnet-znf-we-test*
- *vnet-HEC42-ANO*
- *vnet-HEC44-ANO*

This list is complete at time of publishing and will change over time.

2.3.8 Azure Firewall Policy

Firewall Policy is the recommended method to configure your Azure Firewall. It can be managed using Central management using Firewall Manager. It's a global resource that can be used across multiple Azure Firewall instances in secured virtual hubs.

Azure Firewall supports Standard and Premium policies. The following table summarizes the difference between the two:

Policy Type	Feature Support	Firewall SKU Supported
Standard Policy	▪ ~~Netwsork~~Network rules, NAT rules, Application rules ▪ Custom DNS, DNS proxy ▪ IP Groups ▪ Web Categories ▪ Threat Intelligence	Standard or Premium
Premium Policy	All Standard feature support, plus: ▪ TLS Inspection ▪ Web Categories ▪ URL Filtering ▪ IDPS	Premium

For AkzoNobel "***Standard Policy***" has been implemented. All the firewall rules have been captured in firewall rule collections and these rule collections have been grouped under specific firewall rule collection groups.

Rule Collection Group Guidance

1. It has been agreed to create a separate rule collection group for each spoke listing both inbound and outbound rules.

[2.] The above approach might result ~~into~~ with duplication of rules, because of capturinged ~~in case a~~ rules required ~~applies~~ by ~~to~~ spokes being migrated. AkzoNobel team is okay to allow for this duplication of ~~have these~~ rules provided proper due diligence is done whenever a rule is updated or removed to ensure all ~~the copies~~ duplicates of the rule has been updated. ~~in case there are duplicate entries.~~

2.[3.] Naming convention for the Firewall rules have been specified and listed in ***Appendix A*** for reference.

Firewall Policy Design

Execution Order	Rule Summary
1	Allow "any" to NGW (HCL) shared services [ADFS, WAP, MFA, DNS]
2	Allow NGW (HCL) to "any" traffic
3	Allow specific spoke-to-spoke and spoke-to-on-prem traffic
4	Block known spokes for outbound traffic

5	Allow on-prem outbound traffic
Default	Deny all

2.3.9[2.3.8] Environments Configuration Attributes

2.3.9.1[2.3.8.1] Azure Virtual WAN Development/Test Environment:

Sr. No.	Attribute	Attribute Value
1	Subscription	ate_ccc_it_vwan
2	Resource Group	to_10173
3	Resource Group Region	West Europe
4	Virtual WAN Name	cc-vwan-global-test
5	Virtual WAN Type	Standard
6	Virtual Hub Region	West Europe
7	Virtual Hub Name	hub-01-we-test
8	Virtual Hub IP Address Space	10.239.0.0/23
9	Site-to-Site VPN Gateway Name	hub-01-vpng-we-test
10	Site-to-Site VPN Gateway Scale Units	1 scale unit - 500 Mbps x 2
11	ExpressRoute Gateway Name	hub-01-egw-we-test
12	ExpressRoute Gateway Scale Units	2 scale units - 4 Gbps
13	Virtual-to-Spoke Connection Name	hub-01-we-test/{spoke_name}
14	Azure Firewall Name	cc-hub-01-fw-we-test
15	Azure Firewall SKU Name	AZFW_Hub
16	Azure Firewall SKU Tier	Standard
17	Azure Firewall Policy Name	cc-policy-fw-01-we-test
18	Azure Firewall Policy Tier	Standard
19	User Defined Route Table - Name	cc-route-<identifier/functional name>-we-test

Sr. No.	Attribute	Attribute Value
20	User Defined Route Table - Region	West Europe
21	User Defined Route Table - Propagate gateway routes flag	True
22	Test Virtual Network 01 - Name	cc-vnet-test01-we-test
23	Test Virtual Network 01 - Region	West Europe
24	Test Virtual Network 01 - IP Address Space	10.239.4.0/24
25	Test Virtual Network 01 - Bastion Host Enabled	Disabled
26	Test Virtual Network 01 - DDoS Protection Enabled	Disabled
27	Test Virtual Network 01 - Firewall Enabled	Disabled
28	Test Virtual Network 01 - Subnet Name	cc-vnet-test01-testing-snet
29	Test Virtual Network 01 - Subnet Address Space	10.239.4.0/25
30	Test Virtual Network 02 - Name	cc-vnet-test02-we-test
31	Test Virtual Network 02 - Region	West Europe
32	Test Virtual Network 02 - IP Address Space	10.239.5.0/24
33	Test Virtual Network 02 - Bastion Host Enabled	Disabled
34	Test Virtual Network 02 - DDoS Protection Enabled	Disabled
35	Test Virtual Network 02 - Firewall Enabled	Disabled
36	Test Virtual Network 02 - Subnet Name	cc-vnet-test02-testing-snet
37	Test Virtual Network 02 - Subnet Address Space	10.239.5.0/25

Sr. No.	Attribute	Attribute Value
38	Virtual Machine 01 Name	znfto10173vn001
39	Virtual Machine 01 IP Address	10.239.4.4
40	Virtual Machine 02 Name	znfto10173vn002
41	Virtual Machine 02 IP Address	10.239.5.4
42	Private Endpoint Name	cc-pep-{target_resource_identifier}-we-test
43	Log Analytics Workspace Name	cc-log-we-test
44	Log Analytics Workspace SKU	PerGB2018

2.3.9.2[2.3.8.2] Azure Virtual WAN Production/DR Environment

Sr. No.	Attribute	Attribute Value
1	Subscription	ane_ccc_it_vwan
2	Resource Group	po_10173
3	Resource Group Region	West Europe
4	Virtual WAN Name	cc-vwan-global-prod
5	Virtual WAN Type	Standard
6	Virtual Hub Region	West Europe
7	Virtual Hub Name	hub-01-we-prod
8	Virtual Hub IP Address Space	10.239.2.0/23
9	Site-to-Site VPN Gateway Name	hub-01-vpng-we-prod
10	Site-to-Site VPN Gateway Scale Units	2 scale unit - 1 Gbps x 2
11	ExpressRoute Gateway Name	hub-01-egw-we-prod
12	ExpressRoute Gateway Scale Units	2 scale units - 4 Gbps
13	Virtual-to-Spoke Connection Name	hub-01-we-prod/{spoke_name}
14	Azure Firewall Name	cc-afw-hub-01-we-prod
15	Azure Firewall SKU Name	AZFW_Hub

Sr. No.	Attribute	Attribute Value
16	Azure Firewall SKU Tier	Standard
17	Azure Firewall Policy Name	cc-policy-fw-01-we-prod
18	Azure Firewall Policy Tier	Standard
19	Log Analytics Workspace Name	cc-log-we-prod
20	Log Analytics Workspace SKU	PerGB2018

2.3.10[2.3.9] Monitoring, Logging & Alerting:

~~There is no specific monitoring, logging and alerting requirements for the project. However~~ Azure Log Analytics Workspace have been created to capture diagnostic logs and performance metrics. Below listed sample shared dashboards have been created to monitor relevant components of the solution:

Environment	Log Analytics Workspace Name
Development/Test Virtual WAN	cc-log-we-test
Production/DR Virtual WAN	cc-log-we-prod

~~There are no specific monitoring dashboard requirements; hence a below listed sample shared dashboards have been created as a starter:~~

Environment	Shared Dashboard Name
Development/Test Virtual WAN	• ccc-vwan-afw-dashboard-we-test • ccc-vwan-egw-dashboard-we-test~~cc-vwan-afw-analytics-dashboard-we-test~~
Production/DR Virtual WAN	• ccc-vwan-afw-dashboard-we-prod • ccc-vwan-egw-dashboard-we-prod • ccc-vwan-vpng-dashboard-we-prod~~cc-vwan-afw-analytics-dashboard-we-prod~~

These dashboards capture~~d~~ below details:

~~for~~ For Azure Firewall:

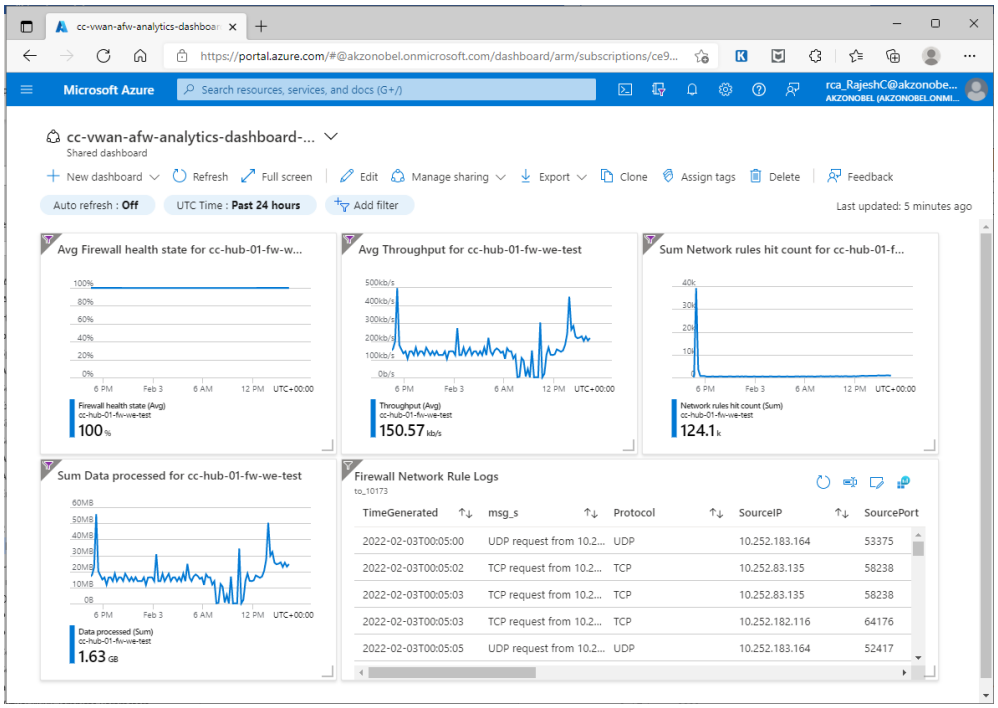
- Firewall Heath State
- Average Throughput
- Network Rules Hit Count
- Amount of Data Processed
- Firewall Network Rule Logs

For Express Route Gateway:

- Average CPU Utilisation
- Average Bits In/Out Per Second
- Total Frequency of Routes Changed
- Average Packets Per Second

For Site-to-Site VPN Gateway (Production Environment only):

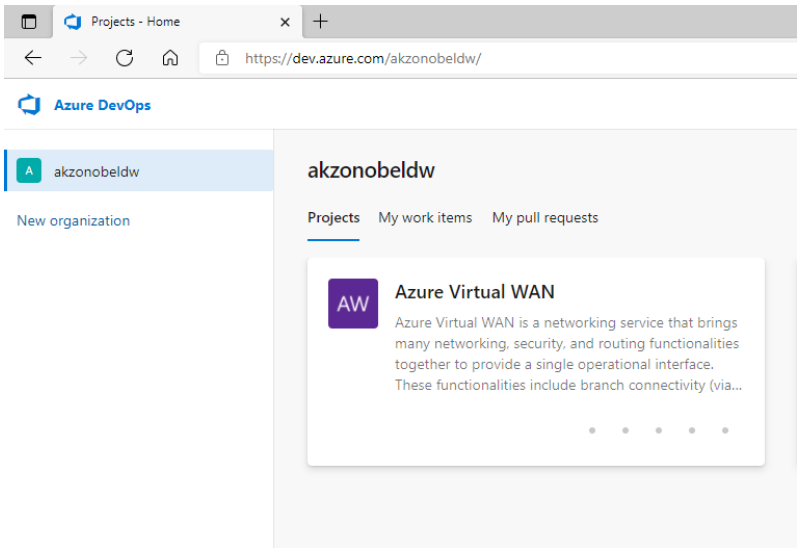
- Average S2S Gateway Bandwidth
-



3. DevOps Set-Up using Azure DevOps

3.1 DevOps Infrastructure

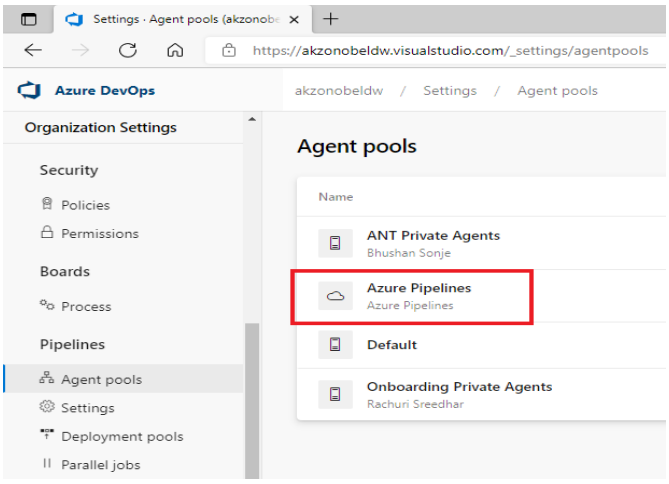
AkzoNobel uses Azure DevOps for implementing automation for development and implementation of Azure Virtual WAN solution. "***AkzoNobeldw***" is the organisation created for the purpose. Within "***AkzoNobeldw***" organization there is project created with name "***Azure Virtual WAN***" to maintain the source code and release pipelines for implementing Azure Virtual WAN solution.

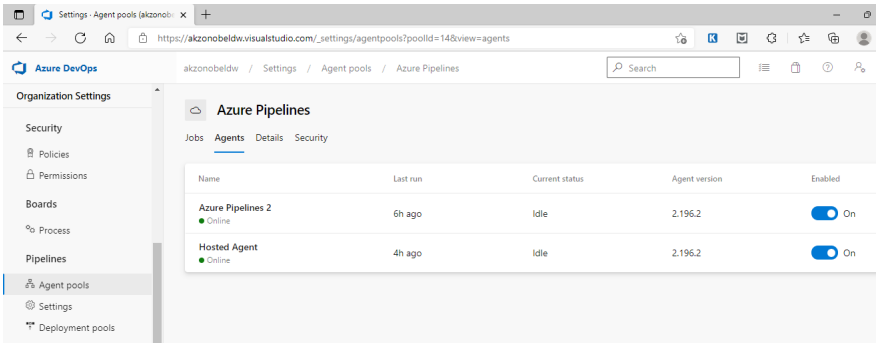


3.1.1 Organization Settings - Agents and Agent Pool

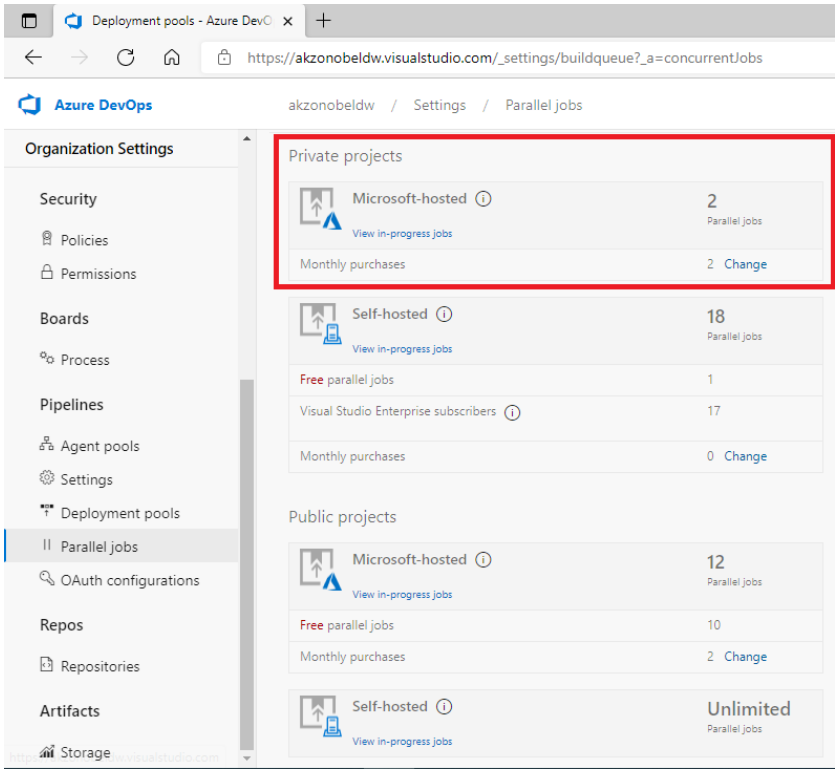
As advised by AkzoNobel, Microsoft Hosted Agents will be used to run the pipelines for carrying out release and deployment tasks for deploying and configuration of Azure Virtual WAN resources/components.

Note: *There still might be some configuration (e.g. Service Principles) that may need to be done using Azure portal.*





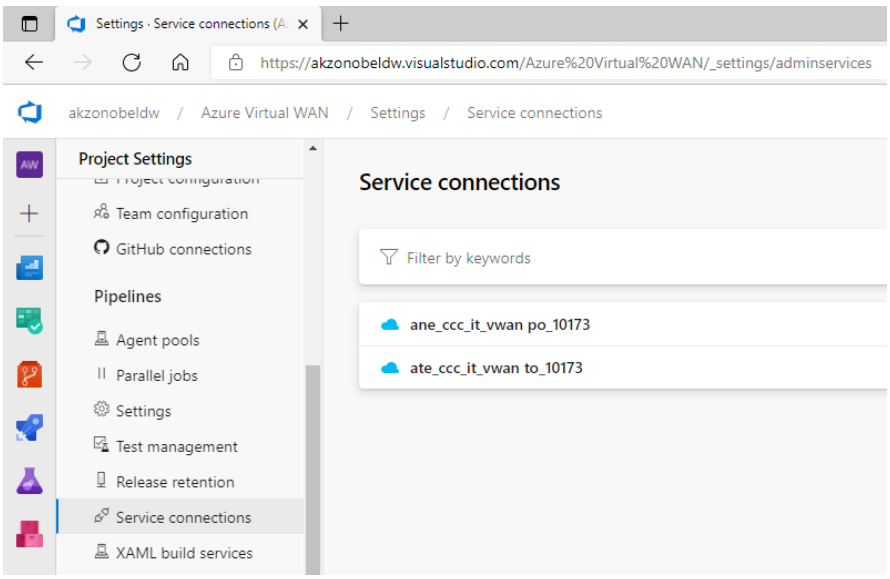
A maximum of 2 jobs can be run in parallel as per the organisation settings.



3.1.2 Project Settings - Service Connection Details

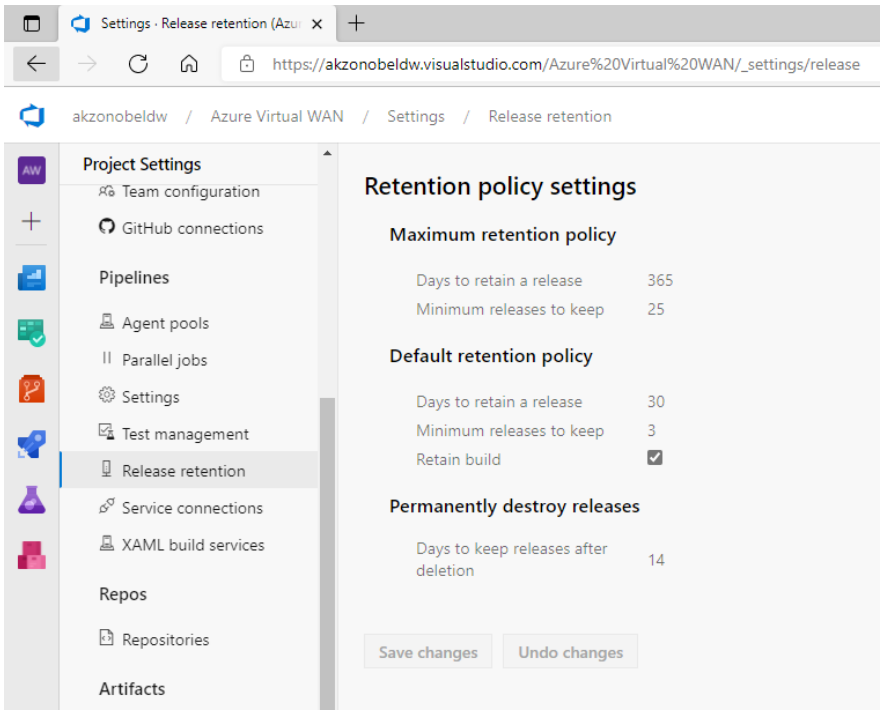
Project is provided with Service Connections created for both development/test & production environments.

Service Connection Details:



3.1.3 Project Settings - Release Retention

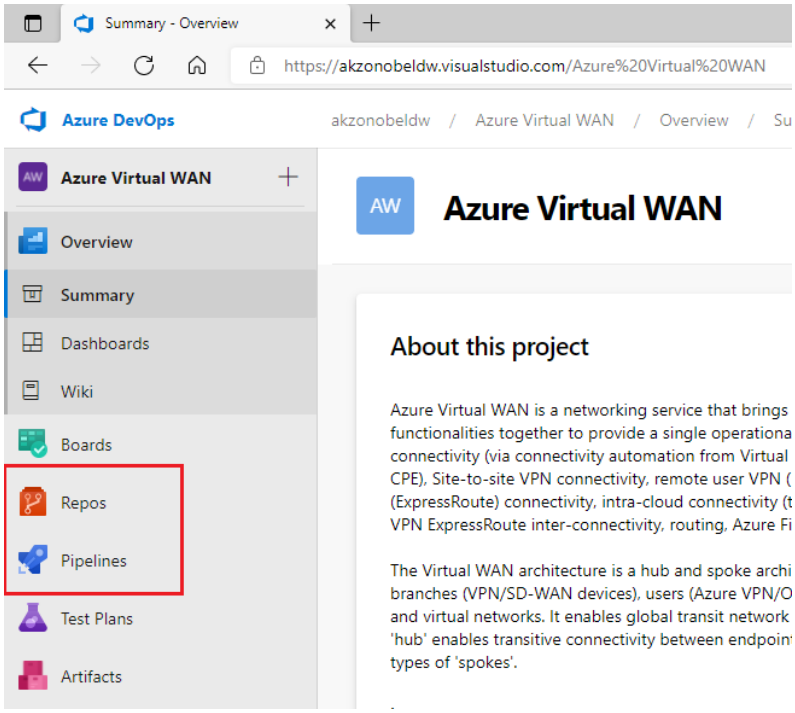
Below image highlights the settings related to release retention as part of project settings.



3.2 Source Code Repository

3.2.1 Source Code Organisation

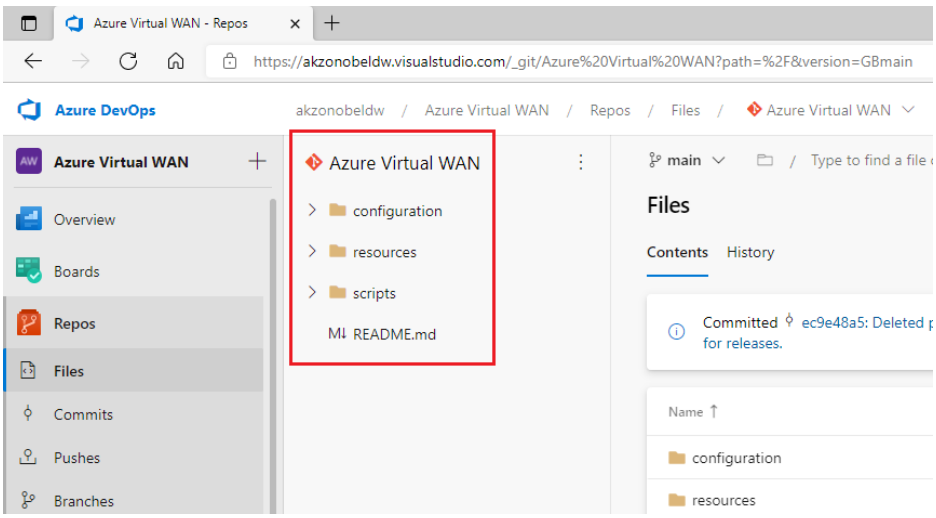
Azure DevOps Repos are used to maintain the source code versions and Azure DevOps Pipelines are used to maintain release pipelines for Azure Virtual WAN resources.



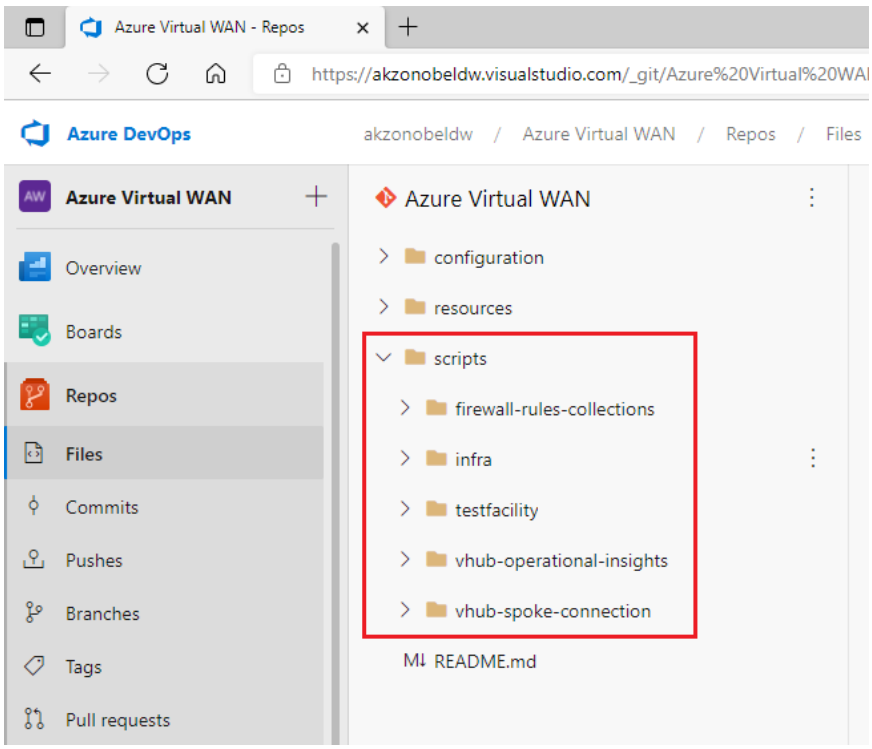
Azure Repos provides two types of version control:

- **Git:** distributed version control. Git in Azure Repos is standard Git. Any client and tools of choice can be used, such as Git for Windows, Mac, partners' Git services, and tools such as Visual Studio and Visual Studio Code.
- **Team Foundation Version Control (TFVC):** centralized version control. Azure Repos also supports Team Foundation Version Control (TFVC). TFVC is a centralized version control system. Typically, team members have only one version of each file on their dev machines. Historical data is maintained only on the server. Branches are path-based and created on the server.

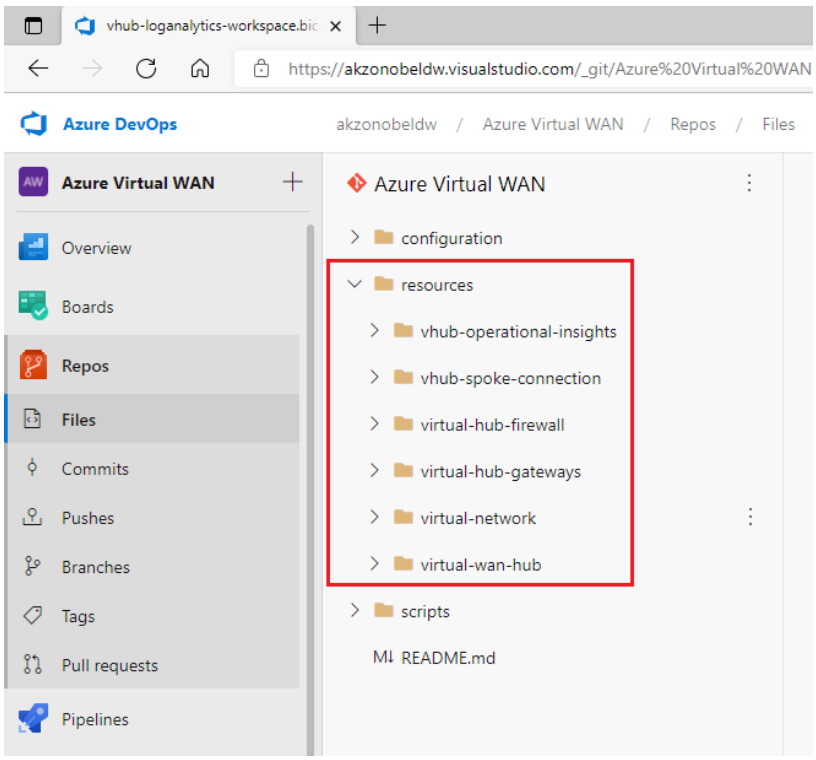
AkzoNobel is using Git features to maintain source code. Below is the top-level folder structure for maintaining various types of files in the repository.



- **Root Directory:** Azure Virtual WAN
- **scripts folder:** This folder contains the PowerShell script files used by release pipelines for deploying/configuring Azure Virtual WAN resources.
    - **scripts/infra/:** This folder contains PowerShell scripts for deploying Azure Virtual WAN, Virtual Hub, Azure Firewall Policy, Azure Firewall for Virtual Hub, ExpressRoute Gateway for the Virtual Hub and Site-to-Site VPN Gateway for Virtual Hub resources.
    - **scripts/firewall-rules-collections/:** This folder contains PowerShell script for deploying Azure Firewall Rule Collections Groups along with Rule Collections and Firewall Network-Rules within Azure Firewall Policy.
    - **scripts/vhub-spoke-connection/:** This folder contains PowerShell script for connecting a virtual network/spoke to secured virtual hub within Virtual WAN. The script automates securing all private traffic between secured virtual hub and virtual network using Azure Firewall. It also enables secure internet access using security partner provider [ZScaler]
    - **scripts/vhub-operational-insights/:** This folder contains PowerShell script for deploying Log Analytics Workspace. Note that Diagnostics Settings for each Virtual WAN resource to redirect logs and metrics data to this workspace is done through Azure Portal GUI.
    - **scripts/testfacility/:** This folder contains PowerShell script for deploying test virtual network with single subnet.



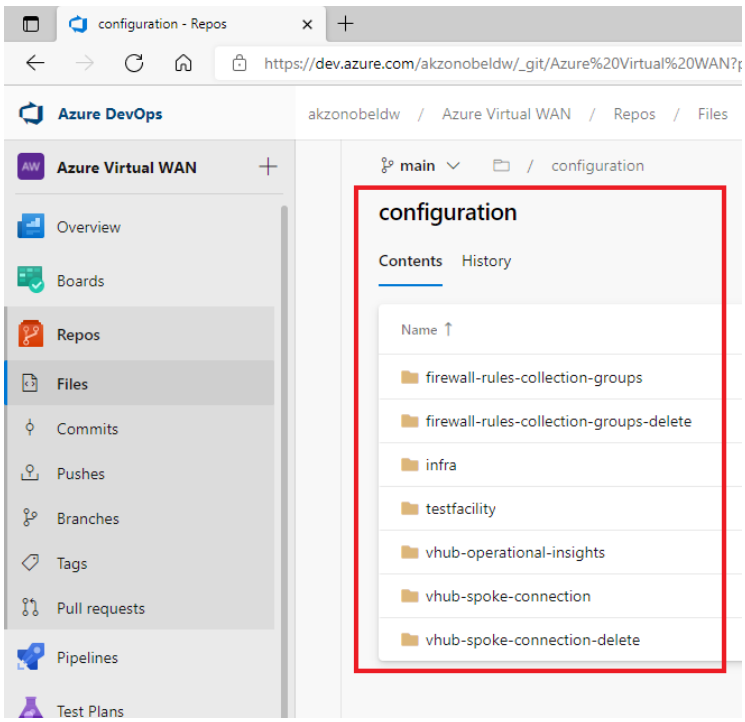
- **resources folder:** This folder contains the Bicep template files for various Azure Virtual WAN resources.
    - **resources/virtual-wan-hub/:** This folder contains Bicep ARM template file to be used to create Azure Virtual WAN and corresponding Virtual Hub.
    - **resources/virtual-hub-firewall/:** This folder contains Bicep ARM template file to be used to create Azure Firewall, Azure Firewall Policy, Azure Rules Collections Group along with Rule Collections & Firewall Network-Rules within Azure Firewall Policy and virtual hub security partner provider [ZScaler].
    - **resources/virtual-hub-gateways/:** This folder contains Bicep ARM template file to be used to create Azure Virtual hub site-to-site VPM Gateway and ExpressRoute Gateway resources.
    - **resources/vhub-spoke-connection/:** This folder contains Bicep ARM template file to be used for connecting a virtual network/spoke to secured virtual hub within Virtual WAN. The script automates securing all private traffic between secured virtual hub and virtual network using Azure Firewall. It also enables secure internet access using security partner provider [ZScaler]
    - **resources/vhub-operational-insights/:** This folder contains Bicep ARM template file to be used to create Log Analytics Workspace.
    - **resources/virtual-network/:** This folder contains Bicep ARM template file to be used to create test virtual network with single subnet.



- **configuration folder:** This folder contains the CSV format data files to be used to specify parameters values for Bicep template for deploying & configuration of Azure Virtual WAN resources.
    - **configuration/infra/**: This folder contains CSV data files to be used to specify parameters values for Bicep template for creating Azure Virtual WAN, Virtual Hub, Azure Firewall Policy, Azure Firewall for Virtual Hub, ExpressRoute Gateway for the Virtual Hub and Site-to-Site VPN Gateway for Virtual Hub resources.
    - **configuration/firewall-rules-collection-groups/*production-fw-rcgs*/network-rules/**: This folder contains CSV data files to be used to specify parameters values for Bicep template for creating/deploying Azure Firewall Rule Collections Groups along with Rule Collections and Firewall Network-Rules within Azure Firewall Policy in production vWAN environment.
    - **configuration/firewall-rules-collection-groups/*test-fw-rcgs*/network-rules/**: This folder contains CSV data files to be used to specify parameters values for Bicep template for creating/deploying Azure Firewall Rule Collections Groups along with Rule Collections and Firewall Network-Rules within Azure Firewall Policy in test vWAN environment.
    - **configuration/vhub-spoke-connection/production-vwan-vhub**: This folder contains CSV data files to be used to specify parameters values for Bicep template for connecting a virtual network/spoke to secured virtual hub within Virtual WAN in production vWAN environment.
    - **configuration/vhub-spoke-connection/test-vwan-vhub**: This folder contains CSV data files to be used to specify parameters values for Bicep

template for connecting a virtual network/spoke to secured virtual hub within Virtual WAN in test vWAN environment.

- **configuration/vhub-operational-insights/**: This folder contains CSV data files to be used to specify parameters values for Bicep template for creating Log Analytics Workspace. Note that Diagnostics Settings for each Virtual WAN resource to redirect logs and metrics data to this workspace is done through Azure Portal GUI.
- **configuration/testfacility/**: This folder contains CSV data files to be used to specify parameters values for Bicep template for creating test virtual network with single subnet.
- **configuration/firewall-rules-collection-groups-delete/*production-fw-rcgs-delete/***: This folder contains CSV data files to be used to specify parameters values for deleting Azure Firewall Rule Collections Groups along with Rule Collections and Firewall Network-Rules within Azure Firewall Policy in production vWAN environment.
- **configuration/firewall-rules-collection-groups-delete/*test-fw-rcgs-delete/***: This folder contains CSV data files to be used to specify parameters values for deleting Azure Firewall Rule Collections Groups along with Rule Collections and Firewall Network-Rules within Azure Firewall Policy in test vWAN environment.
- **configuration/vhub-spoke-connection-delete/production-vwan-vhub**: This folder contains CSV data files to be used to specify parameters values for deleting a virtual network/spoke to secured virtual hub connection within Virtual WAN in production vWAN environment.
- **configuration/vhub-spoke-connection-delete/test-vwan-vhub**: This folder contains CSV data files to be used to specify parameters values for Bicep template for deleting a virtual network/spoke to secured virtual hub connection within Virtual WAN in test vWAN environment.



3.3 CSV Data File Parameters & Format

3.3.1 Virtual WAN Template Parameters

This is a comma separated text file containing below set of parameters with headers.

Parameter	Description	Example
subscription	Azure Subscription where VirtualWAN needs to be created.	ate_ccc_it_vwan
resourceGroupName	Resource Group name where VirtualWAN needs to be created.	to_10173
vwanResourceName	The resource name.	cc-vwan-global-test
vwanType	The type of the VirtualWAN.	Standard
vwanLocation	Resource location.	West Europe

3.3.2 Virtual Hub Template Parameters

This is a comma separated text file containing below set of parameters with headers.

Parameter	Description	Example
subscription	Azure Subscription where Virtual Hub needs to be created.	ate_ccc_it_vwan
resourceGroupName	Resource Group name where Virtual Hub needs to be created.	to_10173
vwanName	The Virtual WAN name under which virtual Hub needs to be created.	cc-vwan-global-test
vhubName	The resource name.	hub-01-we-test
vhubAddressPrefix	Address Prefix for Virtual Hub.	10.239.0.0/23
vhubLocation	Resource location.	West Europe

3.3.3 Azure Firewall Policy Template Parameters

This is a comma separated text file containing below set of parameters with headers.

Parameter	Description	Example
subscription	Azure Subscription where Azure firewall Policy needs to be created.	ate_ccc_it_vwan
resourceGroupName	Resource Group name where Azure firewall Policy needs to be created.	to_10173
fwPolicyName	The resource name.	cc-policy-fw-01-we-test
fwPolicyNameLocation	Resource location.	West Europe

3.3.4 Azure Firewall Template Parameters

This is a comma separated text file containing below set of parameters with headers.

Parameter	Description	Example
subscription	Azure Subscription where Azure firewall needs to be created.	ate_ccc_it_vwan
resourceGroupName	Resource Group name where Azure Firewall needs to be created.	to_10173
vhubName	Virtual Hub name to which Azure firewall needs to be attached to. ***Assumption:*** *Virtual Hub is in the same subscription where Azure Firewall needs to be deployed.*	hub-01-we-test
vhubFwPolicyName	Firewall policy name to be attached to Azure firewall. ***Assumption:*** *Firewall policy is in the same subscription where Azure Firewall needs to be deployed.*	cc-policy-fw-01-we-test
vhubFirewallName	Resource Name	cc-hub-01-fw-we-test
vhubFirewallSkuName	Azure firewall SKU name.	AZFW_Hub
vhubFirewallSkuTier	Azure firewall SKU tier.	Standard
vhubFwPublicIpCount	Number of Public IP required. Minimum value is 1.	1
vhubFirewallLocation	Resource location.	West Europe

3.3.5 Virtual Hub Site-to-Site VPN Gateway Template Parameters

This is a comma separated text file containing below set of parameters with headers.

Parameter	Description	Example
subscription	Azure Subscription where Site-to-Site VPN gateway for Virtual Hub needs to be created.	ate_ccc_it_vwan
resourceGroupName	Resource Group name where Site-to-Site VPN gateway for Virtual Hub needs to be created.	to_10173
vhubName	The Virtual Hub name for which Site-to-Site VPN gateway needs to be created.	hub-01-we-test

Parameter	Description	Example
	Assumption: *Virtual Hub is in the same subscription where Site-to-Site VPN gateway needs to be deployed.*	
vhubVpnGatewayName	The resource name.	hub-01-vpng-we-test
vhubVpnGatewayScaleUnits	The scale unit for this VPN gateway. It represents the bandwidth allocation for the traffic flows.	1
vhubVpnGatewayLocation	Resource location.	West Europe

3.3.6 Virtual Hub ExpressRoute Gateway Template Parameters

This is a comma separated text file containing below set of parameters with headers.

Parameter	Description	Example
subscription	Azure Subscription where ExpressRoute gateway for Virtual Hub needs to be created.	ate_ccc_it_vwan
resourceGroupName	Resource Group name where ExpressRoute for Virtual Hub needs to be created.	to_10173
vhubName	The Virtual Hub name for which ExpressRoute gateway needs to be created. ***Assumption:*** *Virtual Hub is in the same subscription where ExpressRoute gateway needs to be deployed.*	hub-01-we-test
vhubXpressRouteGatewayName	The resource name.	hub-01-egw-we-test
vhubXpressRouteGatewayScaleUnitsMin	The minimum scale unit value for this VPN gateway. It represents the bandwidth allocation for the traffic flows.	2
vhubXpressRouteGatewayScaleUnitsMax	The maximum scale unit value for this VPN gateway. It represents the bandwidth allocation for the traffic flows.	4
vhubXpressRouteGatewayLocation	Resource location.	West Europe

3.3.7 Virtual Hub Security Partner Provider Template Parameters

This is a comma separated text file containing below set of parameters with headers.

Parameter	Description	Example
subscription	Azure Subscription where Security Partner Provider setting for Virtual Hub needs to be created.	ate_ccc_it_vwan
resourceGroupName	Resource Group name where Security Partner Provider setting for Virtual Hub	to_10173

Parameter	Description	Example
	needs to be created.	
vhubName	The Virtual Hub name for which Security Partner Provider setting needs to be created. ***Assumption:*** *Virtual Hub is in the same subscription where Security Partner Provider setting needs to be deployed.*	hub-01-we-test
vhubSecurityProviderName	The resource name.	Zscaler
vhubSecurityProvider	The Security Partner Provider name. ***Note:*** *This is case sensitive.*	Zscaler
vhubSecurityProviderLocation	Resource location.	West Europe

3.3.8 Virtual Hub to Spoke Connection Template Parameters

This is a comma separated text file containing below set of parameters with headers.

Parameter	Description	Example
subscription	Azure Subscription where Virtual Hub is deployed.	ate_ccc_it_vwan
resourceGroupName	Resource Group name where Virtual Hub is deployed.	to_10173
vhubName	The Virtual Hub name with which spoke needs to be connected.	hub-01-we-test
spokeVnetSubscription	Azure Subscription where Spoke is deployed.	ate_ccc_CCC
spokeVnetResourceGroup	Resource Group name where Spoke is deployed.	do_10003
spokeVnetName	Spoke Name	apim-vnet-we-dev
allowHubToRemoteVnetTransit	**(Deprecated)** VirtualHub to RemoteVnet transit enabled or not.	TRUE
allowRemoteVnetToUseHubVnetGateways	**(Deprecated)** Allow RemoteVnet to use Virtual Hub's gateways.	TRUE
enableInternetSecurity	Enable internet security Boolean flag.	FALSE

3.3.9 Spoke Specific Firewall Rules Collections Group Template Parameters

This is a text file containing below set of parameters with headers. It used two types of delimiters:

- Pipe **"|"** character to separate main parameter values
- Comma **","** character to separate multi-valued attribute values such as Protocols, Source/Destination addresses and port numbers.

Parameter	Description	Example
subscription	Azure Subscription where Azure Firewall Policy is deployed.	ate_ccc_it_vwan
resourceGroupName	Resource Group name where Azure Firewall Policy is deployed.	to_10173

Parameter	Description	Example
fwPolicyName	The Azure Firewall Policy name where rules collection groups need to be created.	cc-policy-fw-01-we-test
fwRuleCollectionGrpName	Rules Collection Group name.	rcg_sharedcolor-vnet-znf-we-test
fwRuleCollectionGrpPriority	Priority of the Firewall Policy Rule Collection Group resource.	400
fwRuleCollectionName	The name of the rule collection.	netrc_private-endpoint
fwRuleCollectionPriority	Priority of the Firewall Policy Rule Collection resource.	300
fwRuleCollectionAction	The action type of a rule. ***Note:*** *Allowed values are "Allow" and "Deny"*	Allow
fwRuleName	Name of the rule.	allow_any_private-endpoint
protocols	Comma separated list of Firewall Policy Rule Network Protocols. ***Note:*** *Allowed Values are: "TCP", "UDP", "ICMP"* *or* *"Any"*	TCP
sourceAddresses	Comma separated list of source IP addresses for this rule.	10.0.0.0/8, 134.239.0.0/16, 145.82.0.0/16, 147.82.0.0/16
destinationAddresses	Comma separated list of destination IP addresses	10.252.82.132, 10.252.82.133, 10.252.82.134
destinationPorts	Comma separated list of destination ports including ranges.	1433, 3389-3466

3.3.10 Log Analytics Workspace Template Parameters

This is a comma separated text file containing below set of parameters with headers.

Parameter	Description	Example
subscription	Azure Subscription where log analytics workspace needs to be deployed.	ate_ccc_it_vwan
resourceGroupName	Resource Group name where log analytics workspace needs to be deployed.	to_10173
vHubLogAnalyticsWorkspaceName	The log analytics workspace name.	cc-log-we-test
vHubLogAnalyticsWorkspaceSku	The log analytics workspace SKU.	PerGB2018
dataRetentionInDays	The workspace data retention in days. Allowed values are per pricing plan.	90
publicNetworkAccessForIngestion	The network access type for operating on the Log Analytics Workspace. By default it is Enabled. ***Note:*** *Allowed values are "Enabled" and "Disabled".*	Enabled
publicNetworkAccessForQuery	The network access type for operating on the Log Analytics Workspace. By default it is Enabled. ***Note:*** *Allowed values are "Enabled" and "Disabled".*	Enabled

Parameter	Description	Example
dailyQuotaGb	The workspace daily quota for ingestion.	1

3.3.11 Delete Firewall Rules Collection Group Template Parameters

This is a comma separated text file containing below set of parameters with headers.

Parameter	Description	Example
subscription	Azure Subscription where Azure Firewall Policy is deployed.	ate_ccc_it_vwan
resourceGroupName	Resource Group name where Azure Firewall Policy is deployed.	to_10173
fwPolicyName	The Azure Firewall Policy name where rules collection groups need to be created.	cc-policy-fw-01-we-test
fwRuleCollectionGrpName	Rules Collection Group name.	rcg_sharedcolor-vnet-znf-we-test

3.3.12 Delete Virtual Hub to Spoke Connection Template Parameters

This is a comma separated text file containing below set of parameters with headers.

Parameter	Description	Example
subscription	Azure Subscription where Virtual Hub is deployed.	ate_ccc_it_vwan
resourceGroupName	Resource Group name where Virtual Hub is deployed.	to_10173
vhubName	The Virtual Hub name with which spoke needs to be connected.	hub-01-we-test
spokeVnetName	Spoke Name	apim-vnet-we-dev

3.3.13 Test Virtual Network with Subnet Template Parameters

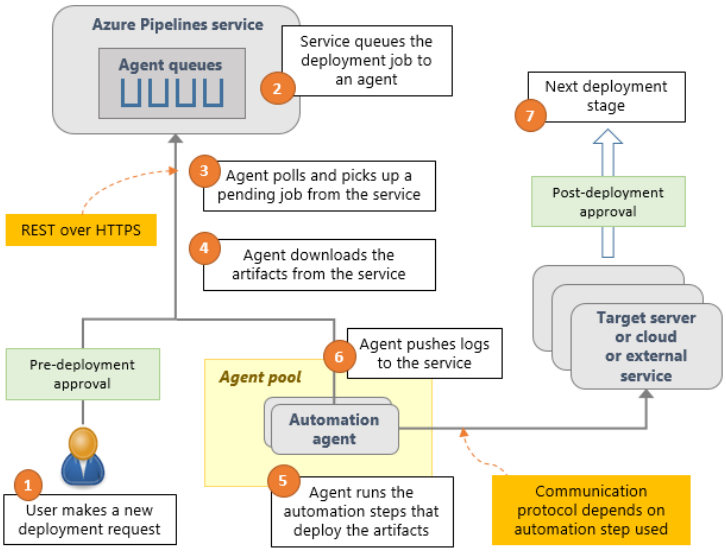
This is a comma separated text file containing below set of parameters with headers.

Parameter	Description	Example
subscription	Azure Subscription where Virtual Network needs to be created.	ate_ccc_it_vwan
resourceGroupName	Resource Group name where Virtual Network needs to be created.	to_10173
vnetName	The Virtual Network name	cc-vnet-test01-we-test
vnetAddressPrefix	The Virtual Network address prefixes	10.239.4.0/24
subnetName	The Virtual Network - Subnet name.	cc-vnet-test01-testing-snet
subnetAddressPrefix	The Virtual Network - Subnet address prefix.	10.239.4.0/25

3.4 Release Pipelines

In Azure Pipelines, you can set up fully automated release pipelines [Or use semi-automated pipelines with approvals and on-demand deployments] for testing, deploying, and approving software application releases to target server or cloud/external service. To author a release pipeline, user must specify the artifacts that make up the application and the release pipeline. Release pipelines store the data for pipelines, stages, tasks, releases, and deployments in Azure Pipelines.

Note: *An artifact is a deployable component of an application. It's typically produced through a Continuous Integration or a build pipeline. This project does not have build pipelines. All the files checked into the Azure Repos repository are already built and ready to be used to deploy Azure Virtual WAN resources.*



Azure Pipelines runs the following steps as part of every deployment:

1) ***Pre-deployment approval:*** When a new deployment request is triggered, Azure Pipelines checks whether a pre-deployment approval is required before deploying a release to a stage. If it's required, it sends out email notifications to the appropriate approvers.
2) ***Queue deployment job:*** Azure Pipelines schedules the deployment job on an available automation agent. An agent is a piece of software that can run tasks in the deployment.
3) ***Agent selection:*** An automation agent picks up the job. The agents for release pipelines are same as the agents that run builds in Azure Pipelines. A release pipeline can contain settings to select an appropriate agent at runtime.

4) ***Download artifacts:*** The agent downloads all the artifacts specified in that release, provided user haven't opted to skip the download. *The agent currently understands two types of artifacts: Azure Pipelines artifacts and Jenkins artifacts.*

5) ***Run the deployment tasks:*** The agent then runs all the tasks in the deployment job to deploy the app to the target servers for a stage.

6) ***Generate progress logs:*** The agent creates detailed logs for each step while running the deployment and pushes these logs back to Azure Pipelines.

7) ***Post-deployment approval:*** When deployment to a stage is complete, Azure Pipelines checks if there's a post-deployment approval required for that stage. If no approval is required, or upon completion of a required approval, it proceeds to trigger deployment to the next stage (in case applicable).

3.5 New Release Pipeline Creation Procedure

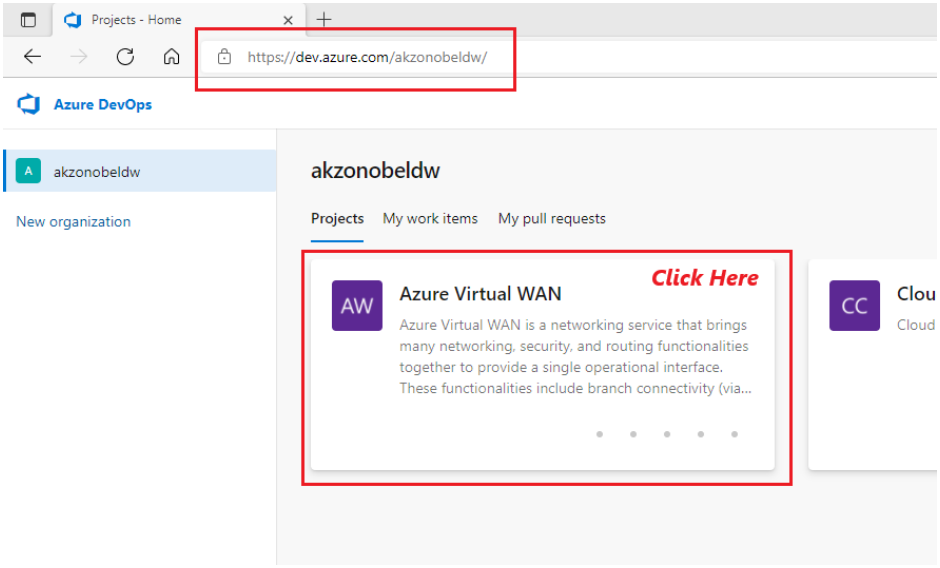
Follow the below listed procedure to create a new release pipeline for deploying and configuring Azure Virtual WAN resources as part of this project.

3.5.1 Pre-Requisites

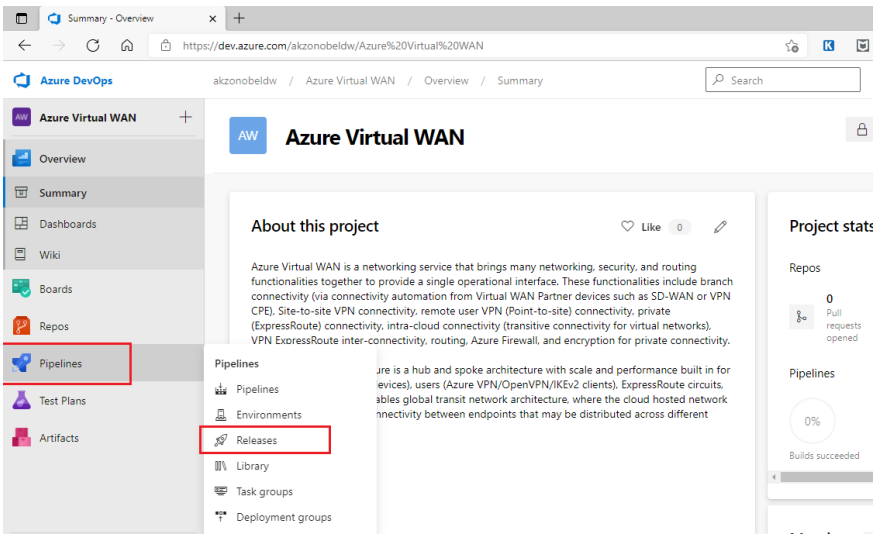
- The user has permissions to create Azure Release Pipelines.
- The service principles used for Azure Development/Test & Production Subscriptions have been created and have the below mentioned roles assigned to them:
  - ✓ Network Reader
  - ✓ Network Contributor
- The Bicep template file used for deploying and/or configuring the Azure Virtual WAN resources are already checked into Azure Repos project source code repository.
- The CSV data file used to be used to specify parameters values for Bicep template for deploying and/or configuring the Azure Virtual WAN resources are already checked into Azure Repos project source code repository.
- The PowerShell script used by Azure Pipelines agents for deploying and/or configuring the Azure Virtual WAN resources are already checked into Azure Repos project source code repository.

3.5.2 Procedure Steps

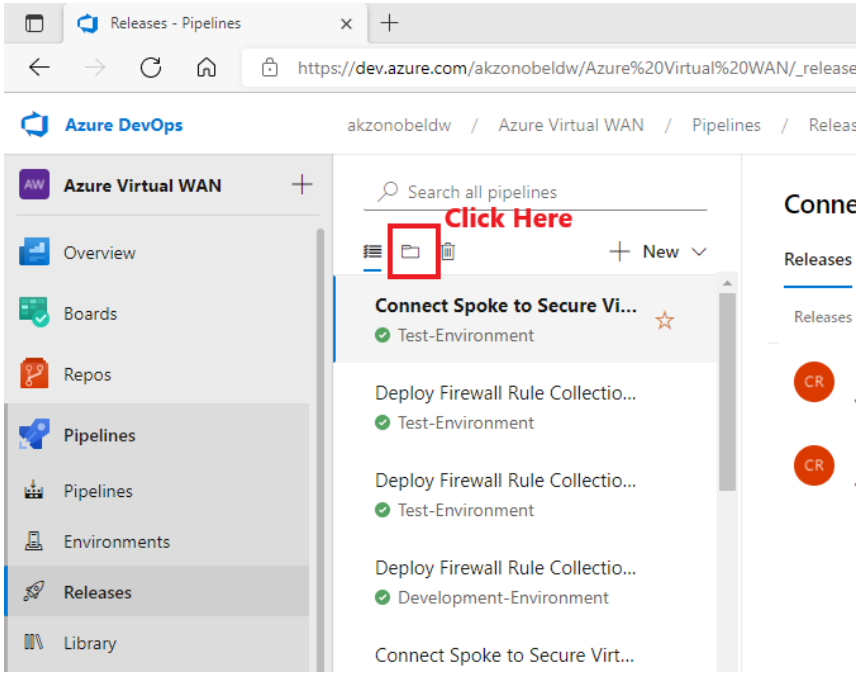
1. Login to Azure DevOps portal [https://dev.azure.com/AkzoNobeldw/] and navigate to the project “Azure Virtual WAN”.



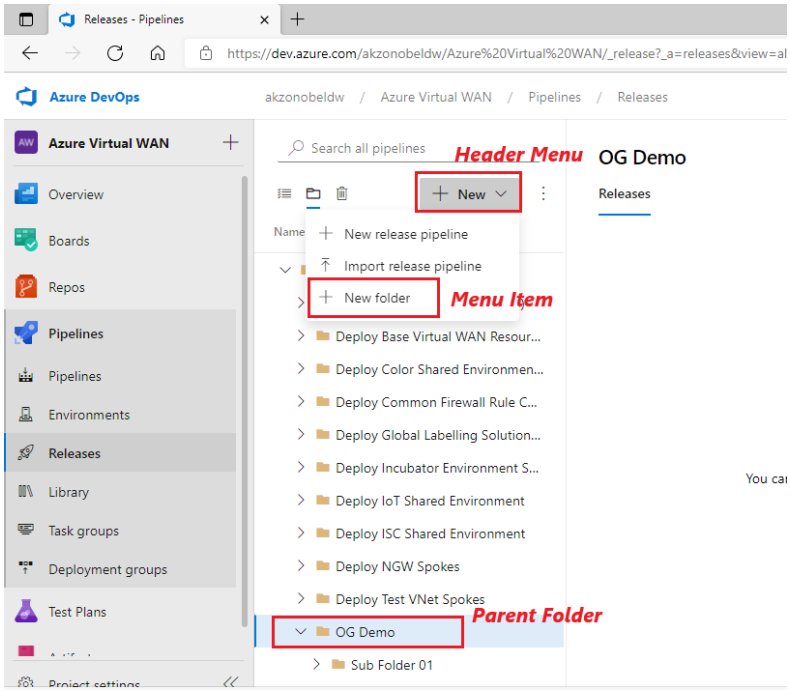
2. Navigate to Pipelines module and then to Release Pipelines sub-module.



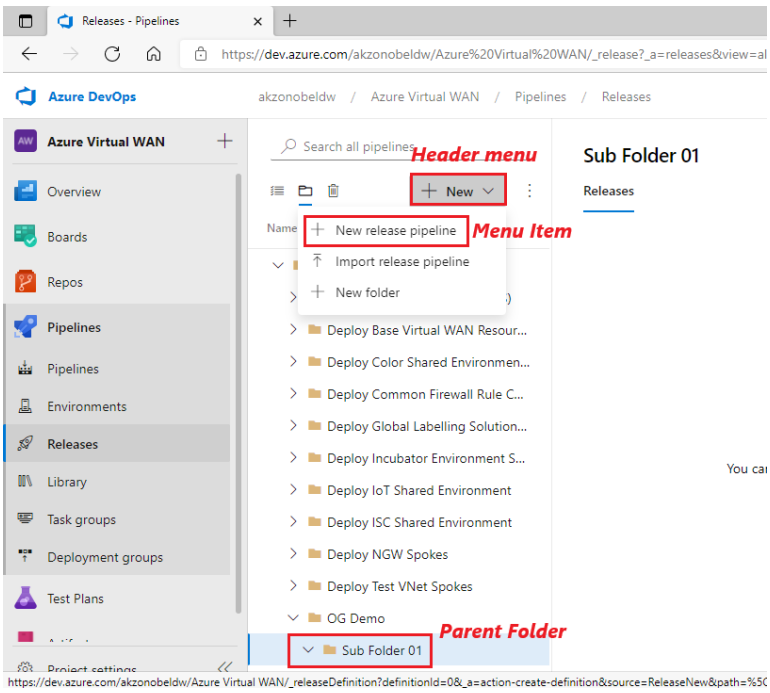
3. Navigate to Folder View of release pipelines. By default, the Azure DevOps portal displays List View of the pipelines.



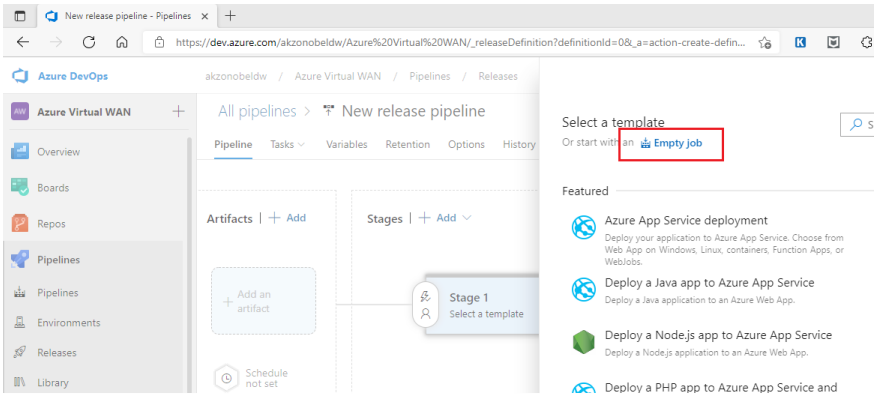
4. User will now be presented with folder view of pipelines. User must validate whether a folder exists where the pipeline is to be created by navigating the folder hierarchy. In case, the folder does not exist then, user should select the parent folder and create a new folder using header Menu option.



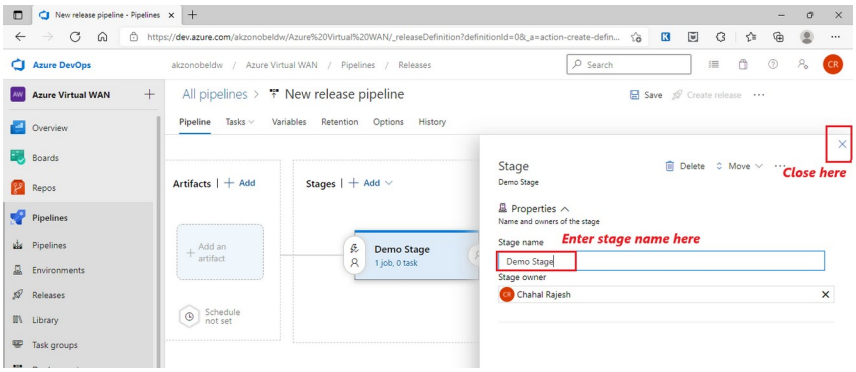
5. After creating folder where the pipeline needs to be created, navigate to the folder and then select “New release pipeline” menu item from the header menu.



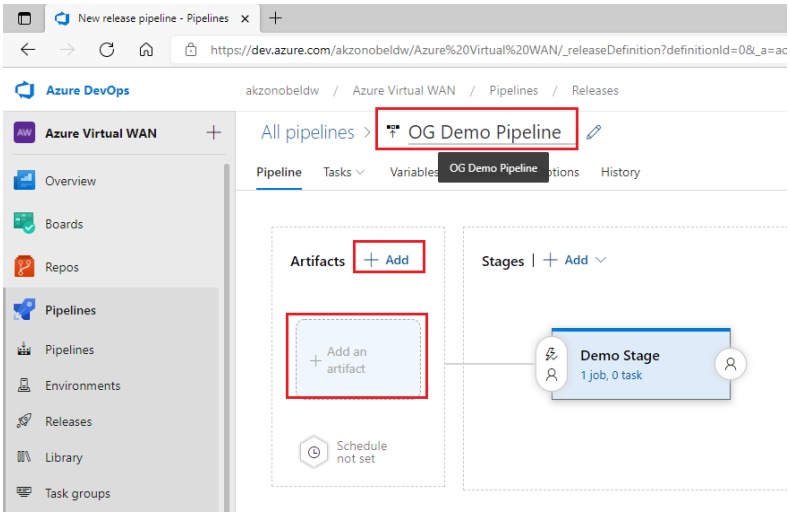
6. Now user will be presented with a screen to “Select a template”. Select “Empty job”.



7. On the resulting screen, specify “Stage name” and close the edit screen overlay.



8. In the main screen, enter the “New release pipeline” name. Click on “+Add” hyperlink or grayed out “Add an artifact” in Artifacts section of the page



9. On the resulting screen, select Source type as “Azure Repos Git” and select/enter the following values for the fields. After selecting/entering the information click on “ADD” button.

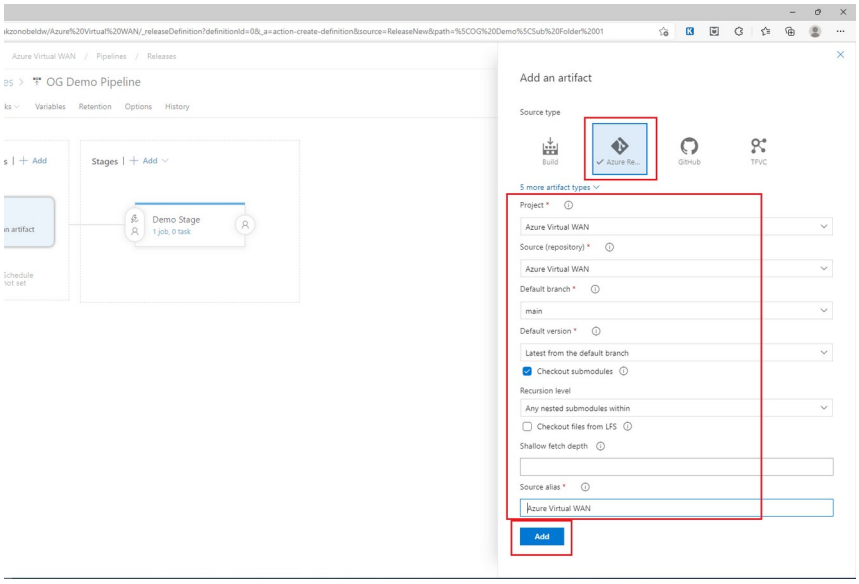
    a. **Project:** “Azure Virtual WAN”

    b. **Source (repository):** “Azure Virtual WAN”

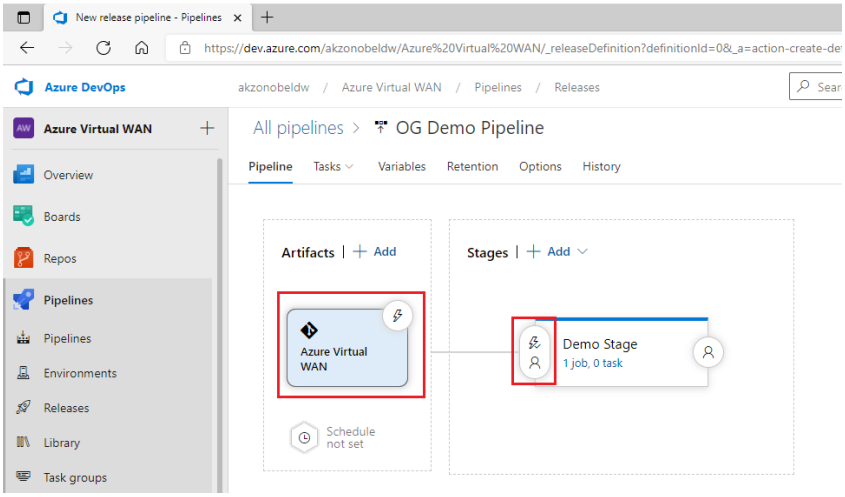
    c. **Default branch:** “main”

    d. **Default version:** “Latest from the default branch”. Also select “Checkout submodules” checkbox

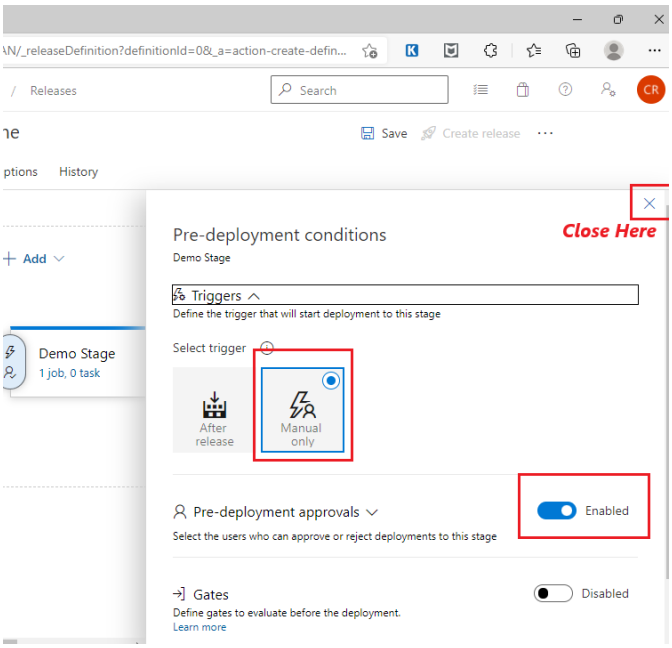
    e. **Source alias:** “Azure Virtual WAN”

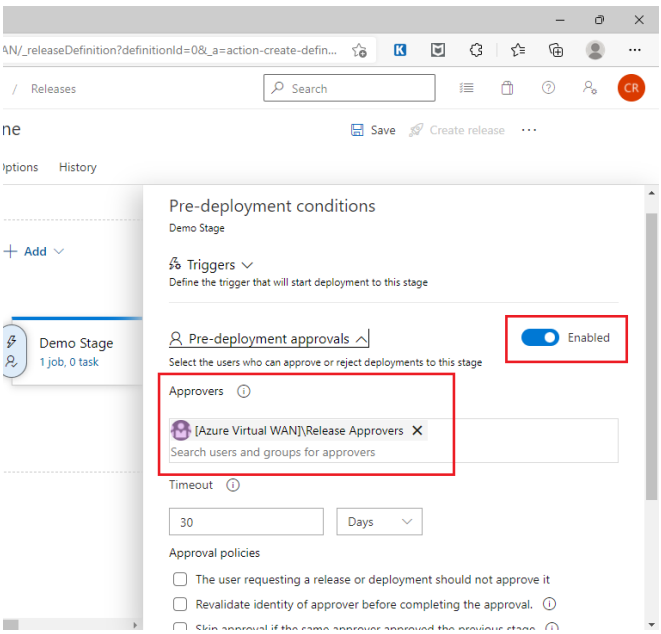


10. On the resulting screen Artifacts section should show “Azure Virtual WAN”. Now click on “Pre-deployment conditions” icons in the Stages section to change the trigger method and deployment Pre-Approvals and Post-Approval settings.

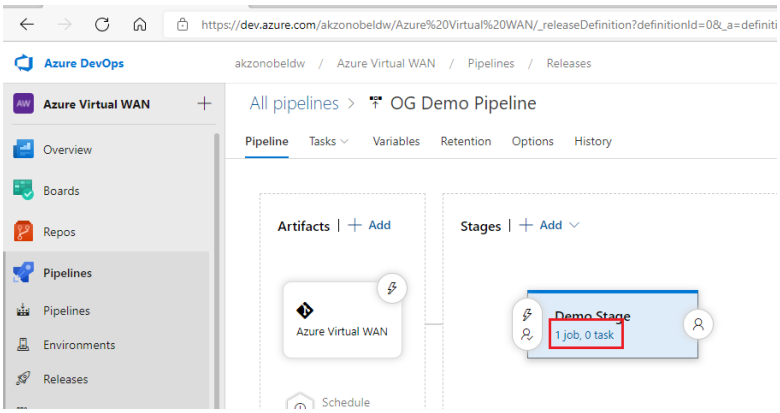


11. On the resulting screen overlay - Select trigger to "***Manual only***" and enable appropriate approvals.
    a. For test environment pipeline stages: No approvals required.
    b. For production environment pipeline stages: Pre-deployment approvals are required with approvers as "***[Azure Virtual WAN]\Release Approvers***" user group.

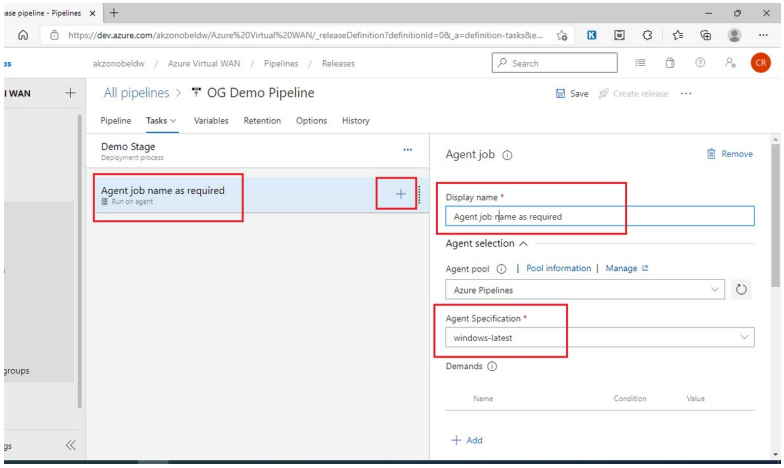




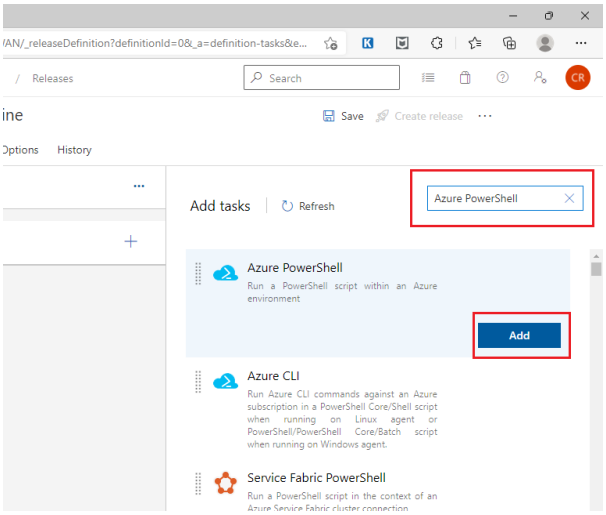
12. Close the screen overlay to come back to main page and click on view stage tasks “1 job, 0 task” hyperlink in Stages/Demo Stage sub-section.



13. On the resulting screen Click on the ribbon titled “Agent Job” and then
    a. Enter Display Name for the Job.
    b. Select “windows-latest” as Agent Specification
    c. Click on “+” icon on the ribbon



14. On the resulting screen overlay search and select “Azure PowerShell”. Click “Add”.



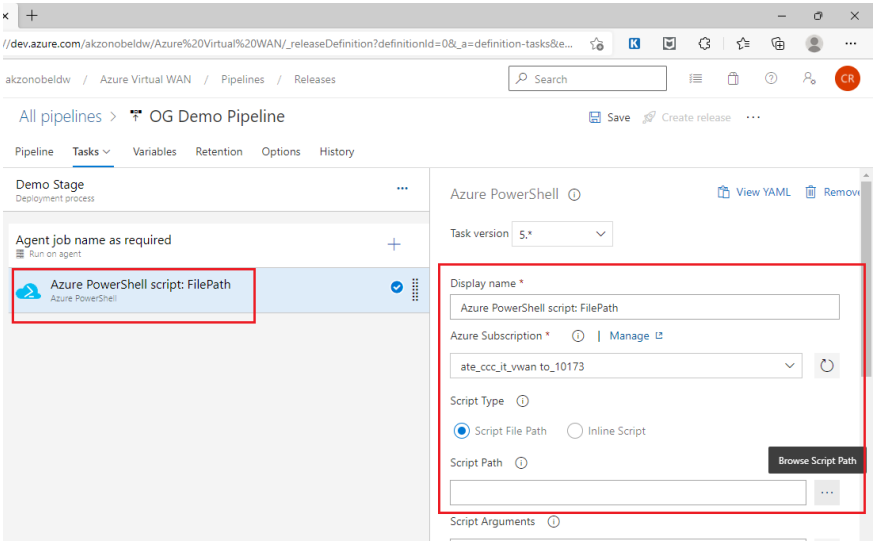
15. Click on the ribbon below the Agent Jon titled “Azure PowerShell script: FilePath” and on the new screen overlay, enter the below values:

    a. ***Display name:*** <<As Required>>

    b. ***Azure Subscription:*** <<Select “***ate_ccc_it_vwan to_10173***” for development/test environment and “***ane_ccc_it_vwan po_10173***” for production/DR environment>>

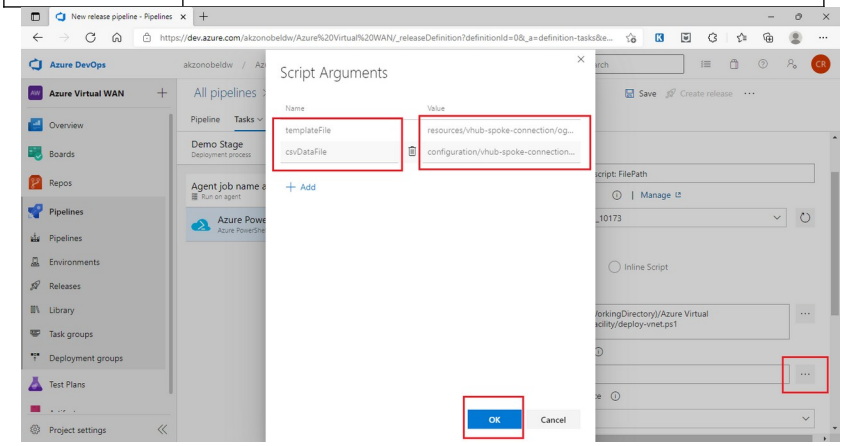
    c. Select Script Type as “***Script File Path***” radio button.

    d. Click Browse Script Path “…” icon next to *Script Path* text box and in the resulting pop-up window navigate the folder structure to select the PowerShell script to be used for the pipeline.

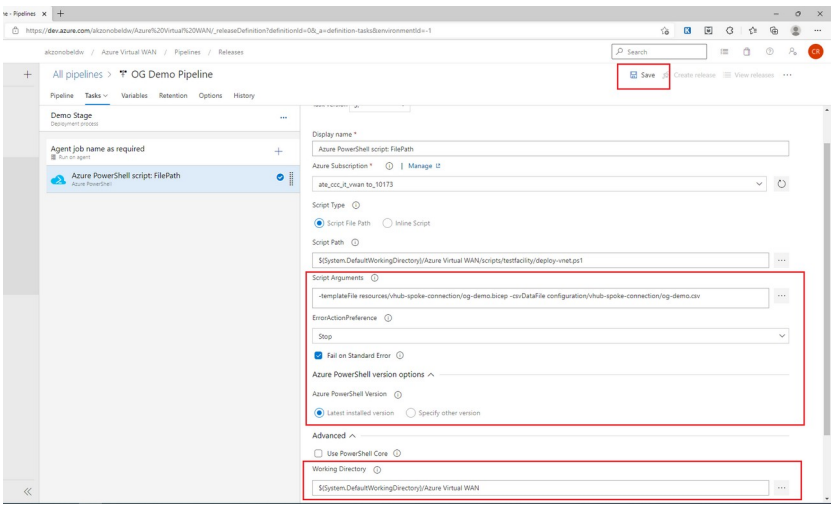


16. Click Edit Script Arguments "…" icon next to *Script Arguments* text box and in the resulting pop-up window click on "ADD" link to add script argument Name and Value. Please add two arguments.

Name	Value
templateFile	Path of Bicep template file relative to "Azure Virtual WAN" folder.
csvDataFile	Path of CSV data file containing Bicep template parameter values relative to "Azure Virtual WAN" folder



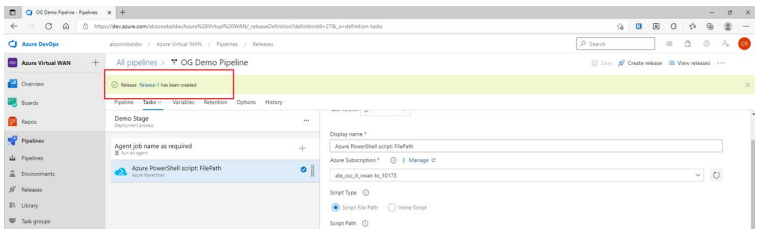
17. Select the checkbox "Fail on Standard Error". Select Azure PowerShell version as "Latest installed version" radio button. Next click on Browse Working Directory "…" icon next to Working Directory text box and in the resulting pop-up window navigate to and select the folder "Azure Virtual WAN (Azur Repos Git)" & click "OK". After that click on "Save" at the top of the page.



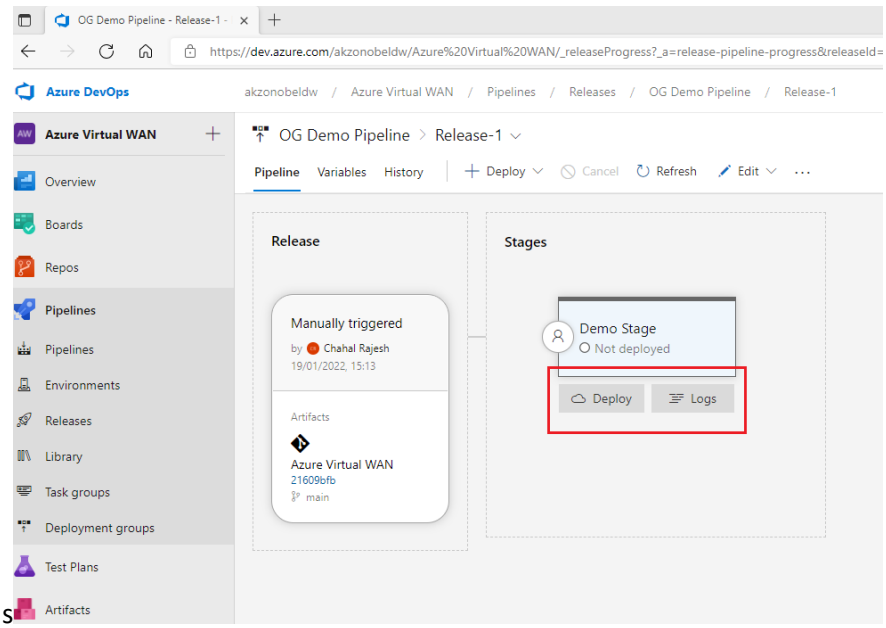
18. After entering the remarks for saving the Release pipeline has been created and saved.
19. To use this pipeline a new release needs to be created. This can be achieved by clicking “Create release” next to Save on top of the page. Enter the release remarks and click “Create” button.

    Note: This link will not be enabled until at lease the pipeline has been saved at least once.

20. Release has been created message will displayed on the main page.



21. Click on the Release hyperlink in the message or navigate to the release though the folder view of the pipelines.
22. On the resulting page hover mouse pointer over the Stage sub-section and two new button are displayed titles “Deploy” and “Logs”



23. Click on the “Deploy” button to deploy the release and “Logs” button to view the deployment logs

3.6 Edit Release Pipeline Procedure

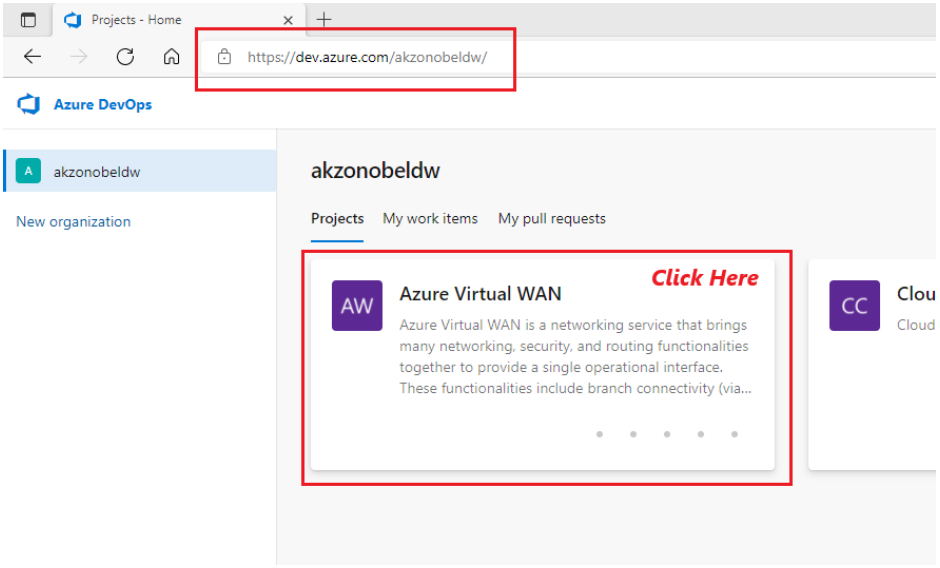
Follow the below listed procedure to edit an existing release pipeline for deploying and configuring Azure Virtual WAN resources as part of this project.

3.6.1 Pre-Requisites

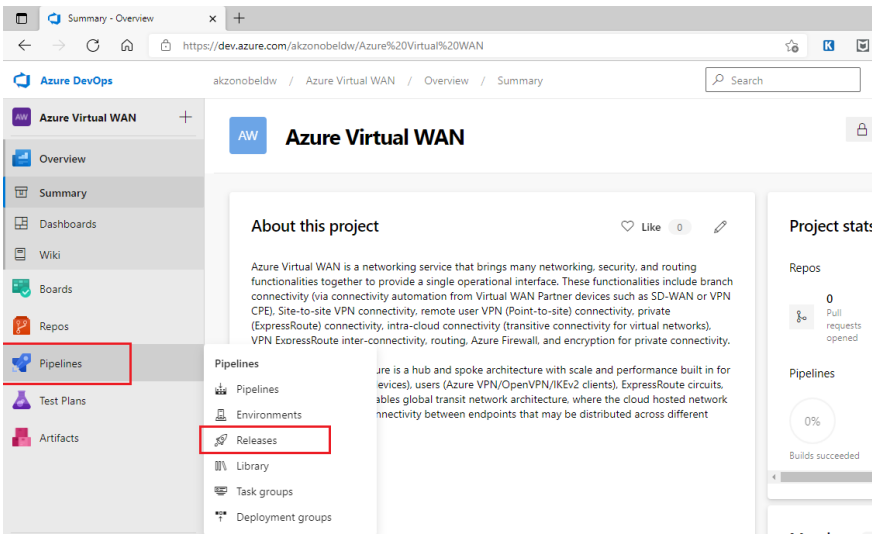
- The user has permissions to create Azure Release Pipelines.
- The service principles used for Azure Development/Test & Production Subscriptions have been created and have the below mentioned roles assigned to them:
  - ✓ Network Reader
  - ✓ Network Contributor
- The Bicep template file used for deploying and/or configuring the Azure Virtual WAN resources are already checked into Azure Repos project source code repository.
- The CSV data file used to be used to specify parameters values for Bicep template for deploying and/or configuring the Azure Virtual WAN resources are already checked into Azure Repos project source code repository.
- The PowerShell script used by Azure Pipelines agents for deploying and/or configuring the Azure Virtual WAN resources are already checked into Azure Repos project source code repository.

3.6.2 Procedure Steps

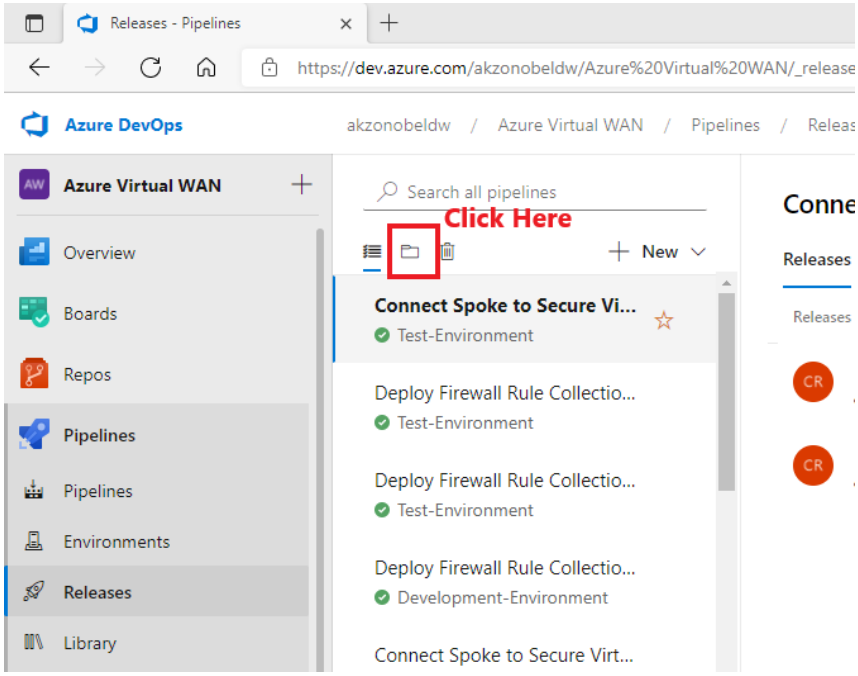
1. Login to Azure DevOps portal [https://dev.azure.com/AkzoNobeldw/] and navigate to the project “Azure Virtual WAN”.



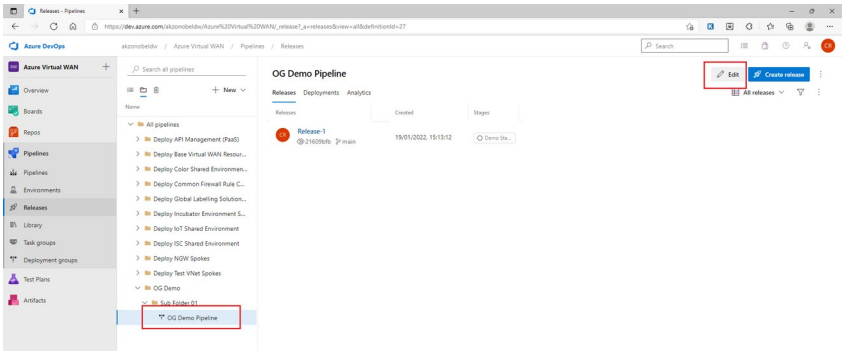
2. Navigate to Pipelines module and then to Release Pipelines sub-module.



3. Navigate to Folder View of release pipelines. By default, the Azure DevOps portal displays List View of the pipelines.



4. User will now be presented with folder view of pipelines. Navigate to the folder where pipeline is saved and then select the pipeline. Click on Edit link on the right-hand top corner of the resulting page.



5. Follow steps 7 onwards from the procedure to create a release pipeline to make and save updated to release pipeline.

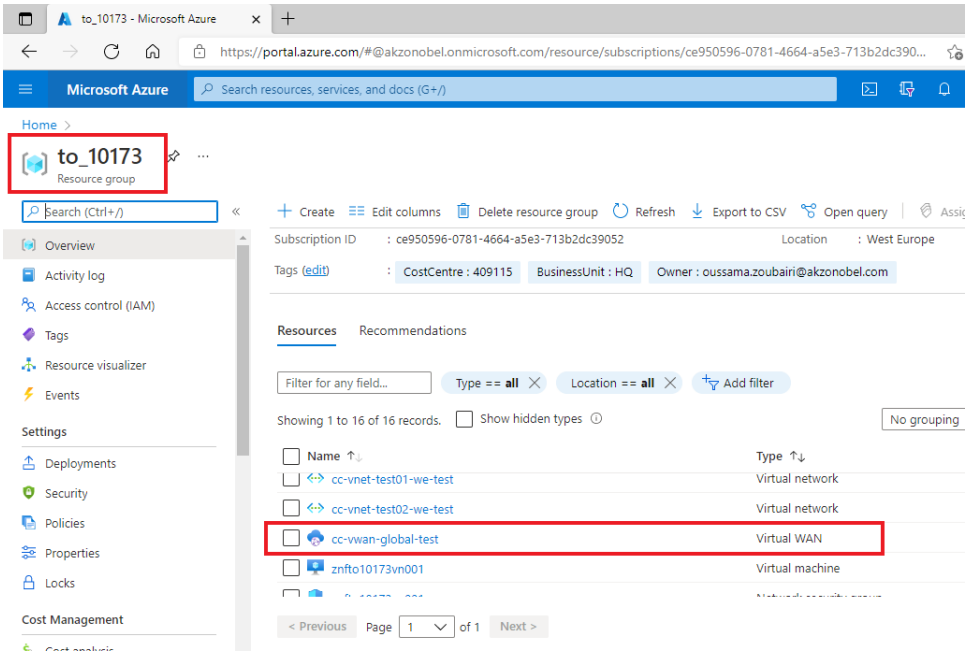
3.7 Addition of Private Traffic Prefixes for the Virtual Hub (using Azure Portal GUI)

As part of secured virtual hub, we need to add list of private addresses for which traffic flows need to be secured using Azure Firewall. Below steps needs to be followed to add/amend this setting using Azure Portal GUI.

1. Log in to Azure portal using https://portal.azure.com link.
2. Navigate to the appropriate subscription and resource group. For subscription name and resource group name in
    a. **Production/DR environment - refer section 2.3.9.2**

b. Development/test environment - refer section 2.3.9.1

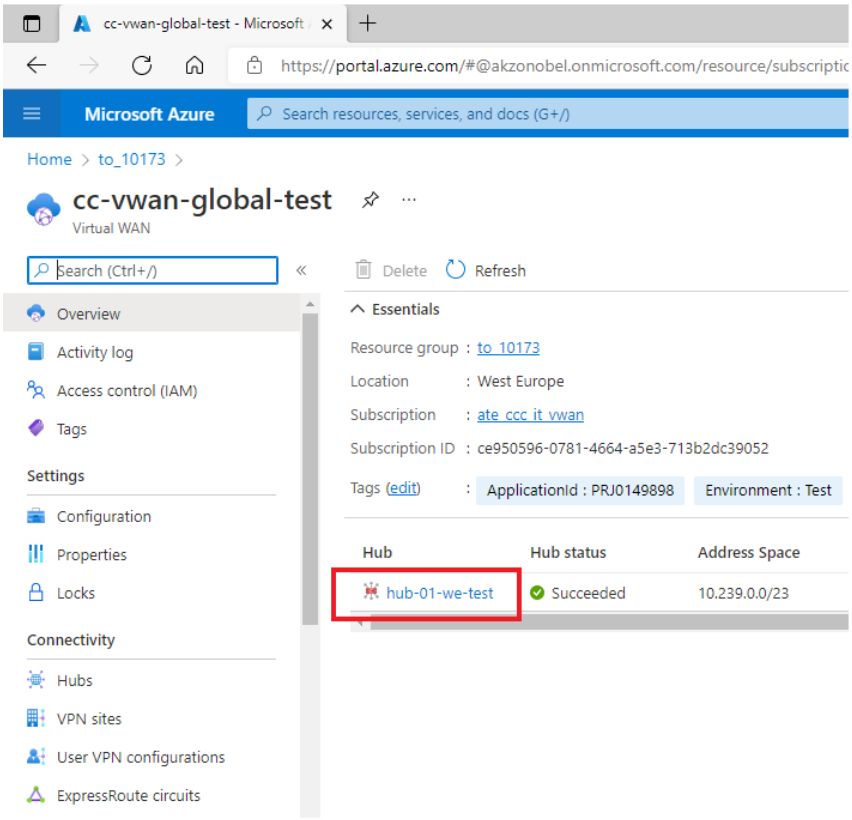
3. Click on the virtual wan resource



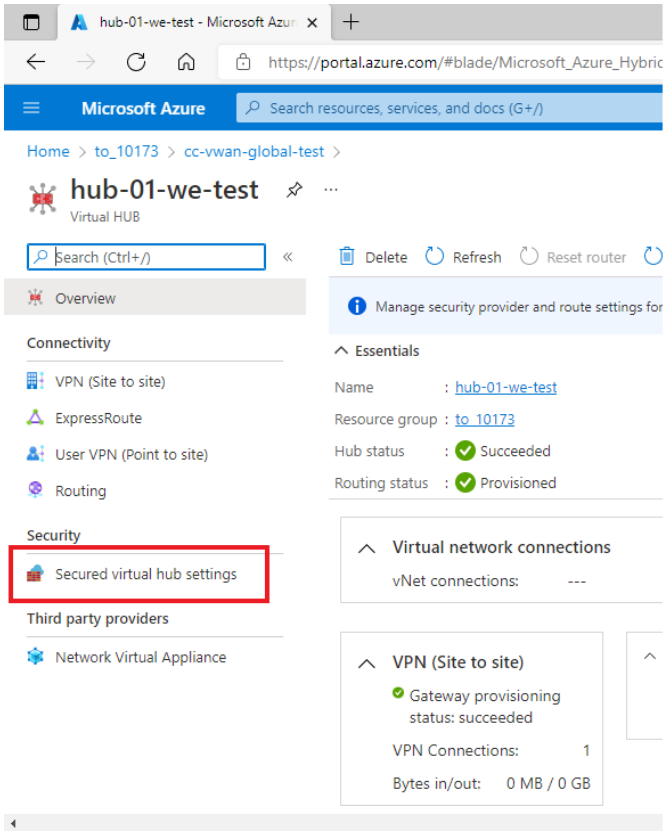
4. On virtual WAN overview page click on hub name. For virtual hub name in

a. **Production/DR environment - refer section 2.3.9.2**

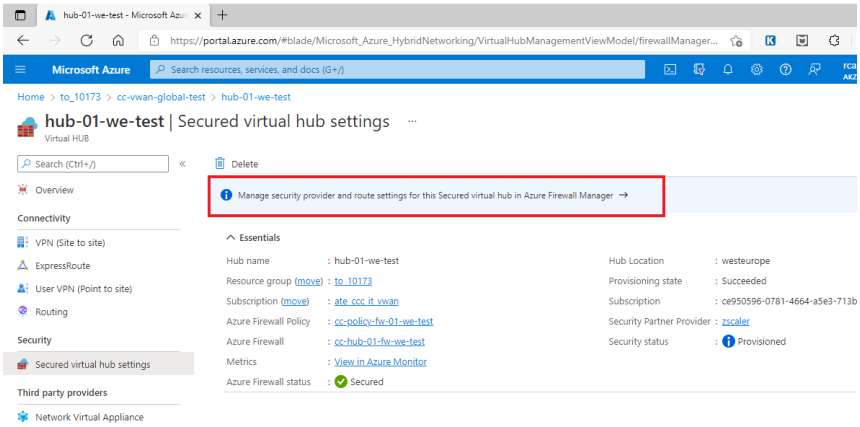
b. Development/test environment - refer section 2.3.9.1



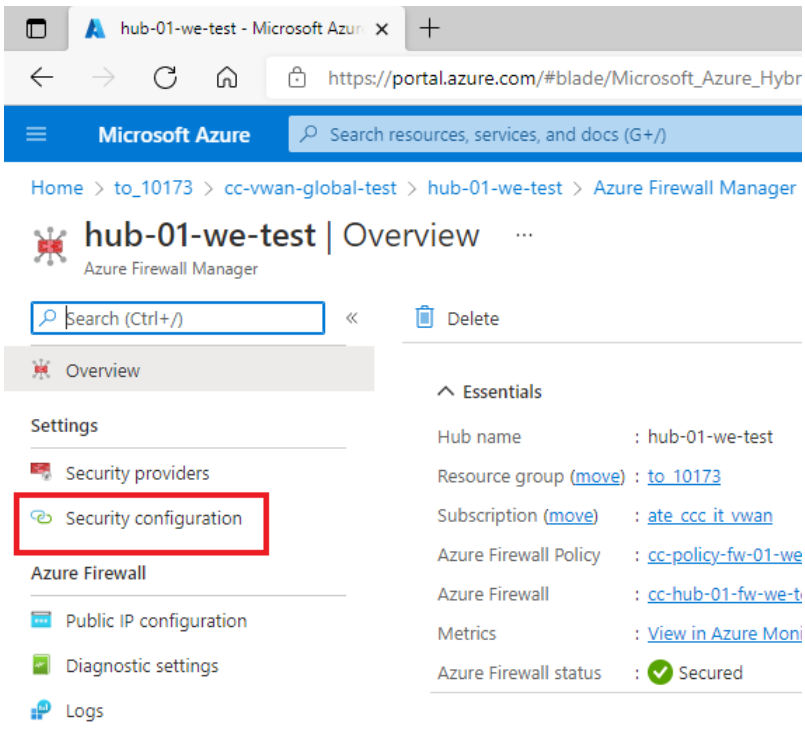
5. Click on “Secured Virtual Hub Settings” in left navigation pane.



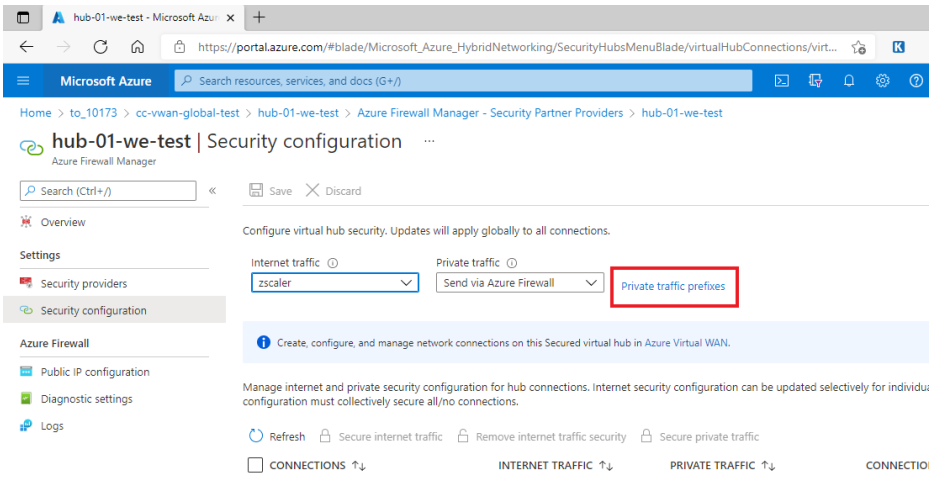
6. Click on Blue Ribbon in main page titled “*Manage security provider and route settings for this Secured virtual hub in Azure Firewall Manager →*”



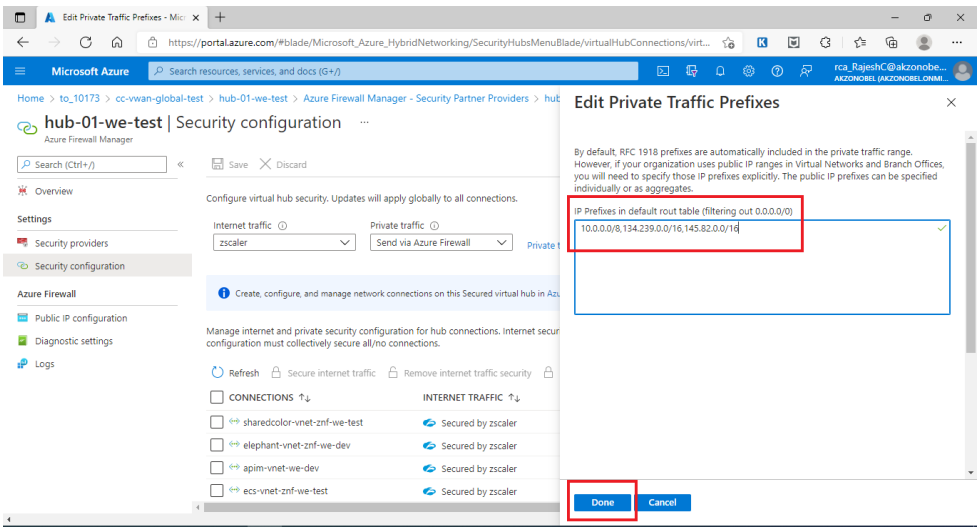
7. On the resulting page click on “Secure virtual hub” name for which private traffic needs to be secured.
8. On the hub overview page, click on “Security configuration” in left navigation pane.



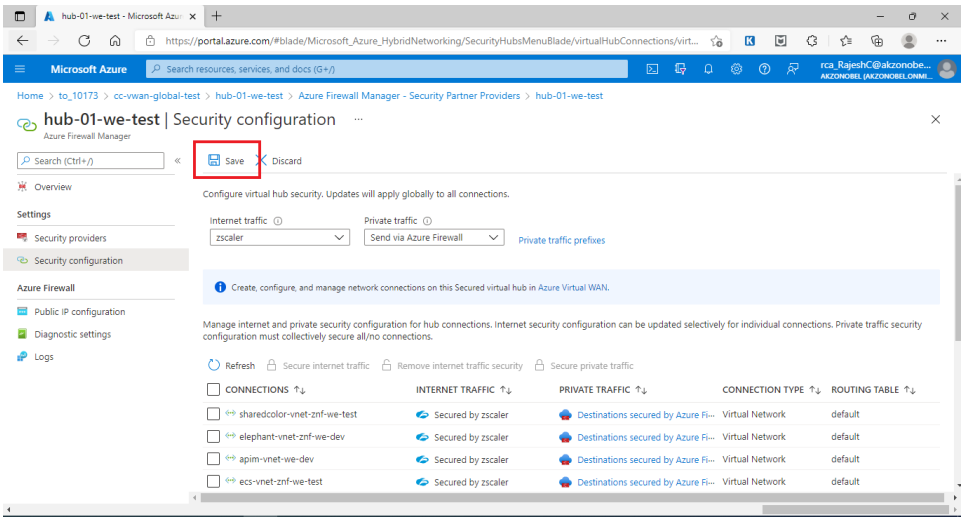
9. On the resulting page, in the main panel click on "***Private traffic prefixes***" hyperlink.



10. This will open an overlay window to specify list of private address prefixes. Enter the appropriate private address prefixes and click "Done".



11. Once the page overlay closes, Click on Save on the main page.



12. Keep monitoring the update notifications for the deployment progress. Once the changes are saved the private traffic prefixes are added for the Secured Virtual Hub.

3.8 Operational Tasks

3.8.1 General Guidelines

1. Always maintain the code in the Azure repos Git repository and follow version control best practices.
2. Whenever the code in the repository is updated; ensure that a new release is created for the release pipeline to ensure latest changes have been picked up before deploying the release.
3. Not all changes to the Azure Virtual WAN resources are made through Release pipelines. Some changes are made through the Azure Portal GUI and any changes to these should be handled through the same mechanism.
4. Below listed changes are done through Azure portal GUI:

a. Addition of Private Traffic Prefixes for the Virtual Hub security configurations. Refer section "3.7" for details on how to achieve the same.

b. Configuration of ExpressRoute circuit authorization key and peer circuit URI

c. View address prefixes advertised to ExpressRoute circuit

d. Enabling Diagnostic Settings for Azure resources to make use of Log Analytics Workspace.

3.8.2 Firewall Rule Changes [Addition/Updation/Deletion]

1. In the absence of service now a temporary process has been created to accommodate customer Firewall changes. ***Please refer Appendix B for details.***
2. Gather the changes to the firewall rules for a given spoke/virtual network and secure the required approvals for the change.
3. Update the CSV data file (in Azure repos Git) for firewall rule collection group corresponding to the spoke/virtual network.

   Note: *Please be aware that the CSV data file should have all the applicable rules for the corresponding spoke/virtual network at any given point in time as the entire rules collection group is considered as single entity and any unwanted removals from the data file is considered a valid change and the same rules will be removed from the firewall policy.*
4. Create new release for the release pipeline after committing the changes to Azure Repos Git.
5. Deploy the latest release. Please note that there might a deployment approval required if the change is applied to production environment.
6. Test the change.

3.8.3 Firewall Rule Collection Changes [Addition/Updation/Deletion]

1. In the absence of service now a temporary process has been created to accommodate customer Firewall changes. ***Please refer Appendix B for details.***
2. Gather the changes to the firewall rule collections for a given spoke/virtual network and secure the required approvals for the change.
3. Update the CSV data file (in Azure repos Git) for firewall rule collection group corresponding to the spoke/virtual network.

   Note: *Please be aware that the CSV data file should have all the applicable rule collections for the corresponding spoke/virtual network at any given point in time as the entire rules collection group is considered as single entity and any unwanted removals from the data file is considered a valid change and the same rule collections will be removed from the firewall policy.*
4. Create new release for the release pipeline after committing the changes to Azure Repos Git.

5. Deploy the latest release. Please note that there might a deployment approval required if the change is applied to production environment.
6. Test the change.

3.8.4 Deletion of Rules Collection Group

1. In the absence of service now a temporary process has been created to accommodate customer Firewall changes. ***Please refer Appendix B for details.***
2. Gather the firewall rules collection group to be deleted details and secure the required approvals for the change.
3. Update the CSV data file (in Azure repos Git) for firewall rules collection group deletion.
4. Create new release for the release pipeline after committing the changes to Azure Repos Git.
5. Deploy the latest release. Please note that there might a deployment approval required if the change is applied to production environment.
6. Test the change.

3.8.5 Adding New Virtual Network/Spoke to Secured Virtual Hub

1. Gather the required Virtual Network/Spoke details that needs to be connected to Secured Virtual Hub.
2. Gather a list of test scenarios to be used as pre-migration and post migration testing.
3. Prepare a spoke specific CSV data file for release pipeline to be used to connect spoke to virtual hub
4. Prepare a spoke specific firewall rules collection group CSV data file.
5. Add these files to Azure Repos Git source code repository as per the defined folder organization and structure.
6. Create new release pipelines for deploying the spoke specific firewall rules collection group. Refer section 3.5 for detailed steps on how to achieve this.
7. Create new release pipelines for connecting the spoke to virtual hub. Refer section 3.5 for detailed steps on how to achieve this.
8. Remove the spoke from legacy hub configuration (in case applicable).
9. Update the User Defined Route table (UDR) entries (as applicable).
10. Execute release pipeline to deploy firewall rules collection group.
11. Execute release pipeline to connect spoke/virtual network to secured virtual hub.
    a. The script & Bicep template automatically secure all private traffic though Azure Firewall.
    b. The script and Bicep template file secure the internet traffic through ZScaler based on a parameter value specified through CSV data file.

12. Test the changes to ensure all services in the newly attached spoke/virtual network are accessible.

3.8.6 Update Virtual Network/Spoke to Secured Virtual Hub Connection

3.8.6.1 Add/Remove Firewall rules

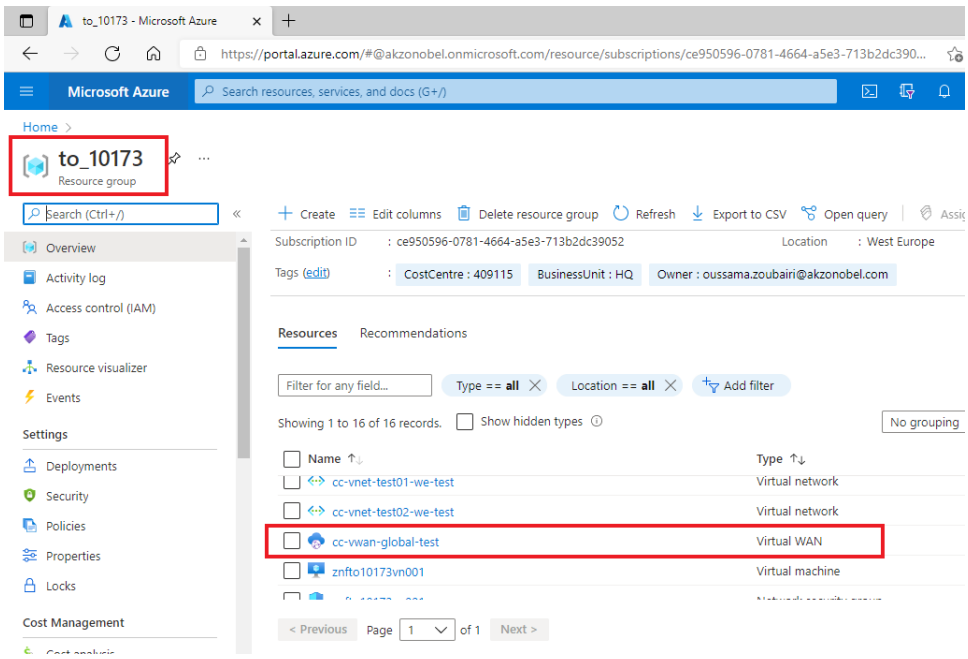
1. Refer section 3.8.2 for details.

3.8.6.2 Secure/Unsecure internet traffic (using Release Pipeline)

1. Update the Spoke Connection specific CSV data file to update value for "enableInternetSecurity" parameter.
2. Save and commit the changes to Azure Repos Git source code repository.
3. Create new release for the release pipeline after committing the changes to Azure Repos Git.
4. Deploy the latest release. Please note that there might a deployment approval required if the change is applied to production environment.
5. Test the change.

3.8.6.3 Secure/Unsecure internet traffic (using Azure Portal GUI)

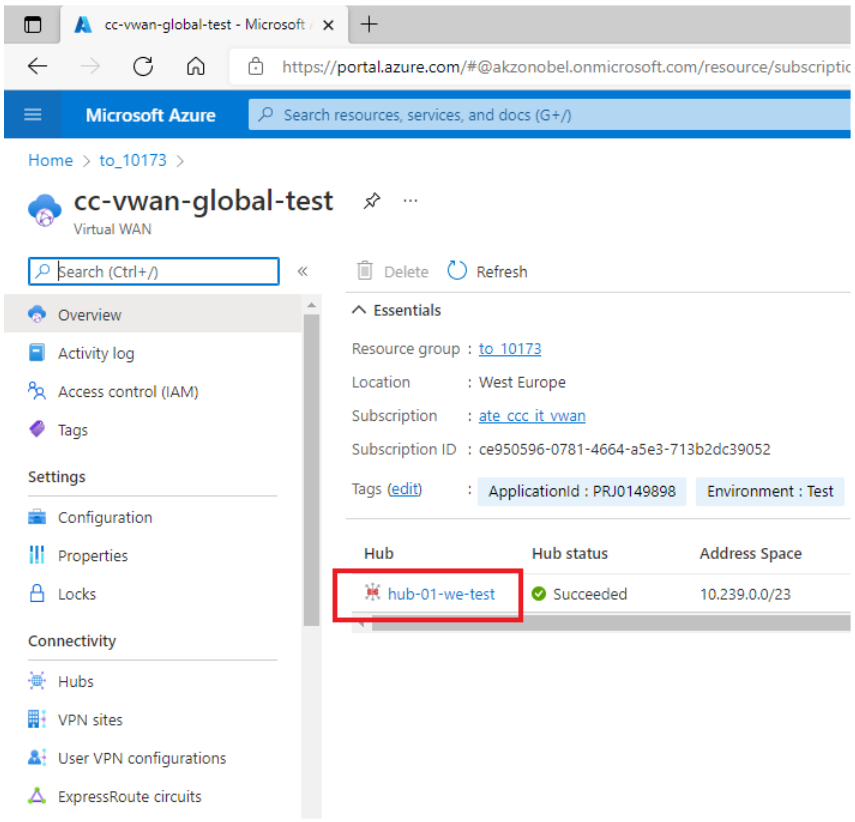
1. Log in to Azure portal using https://portal.azure.com link.
2. Navigate to the appropriate subscription and resource group. For subscription name and resource group name in
    a. **Production/DR environment - refer section 2.3.9.2**
    b. Development/test environment - refer section 2.3.9.1
3. Click on the virtual wan resource



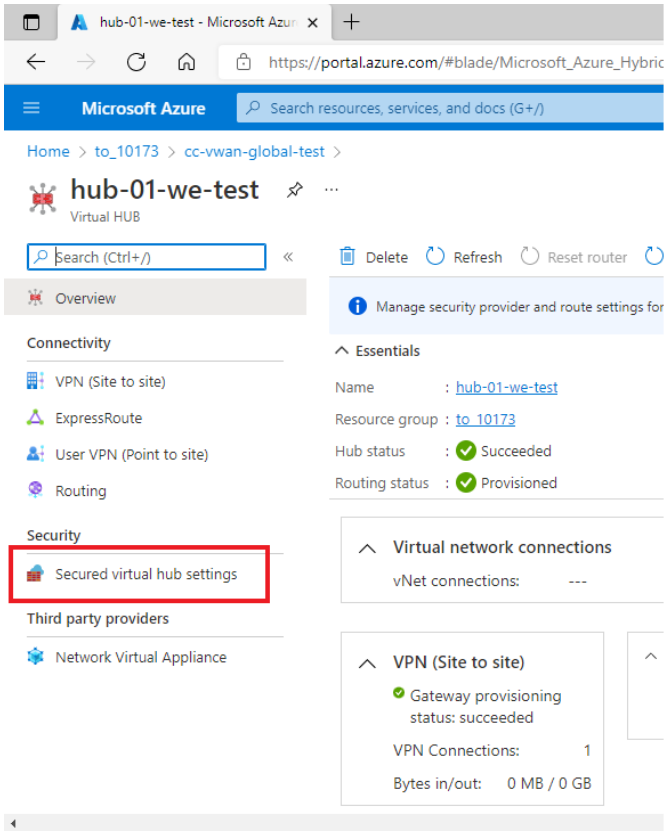
4. On virtual WAN overview page click on hub name. For virtual hub name in

   a. **Production/DR environment - refer section 2.3.9.2**

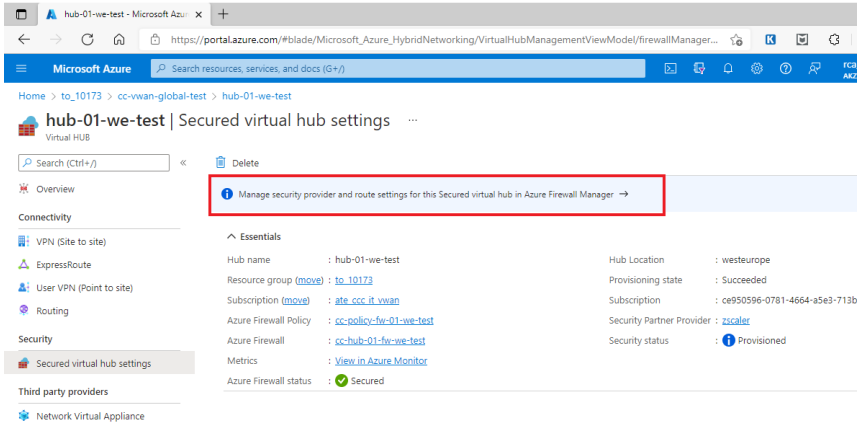
   b. Development/test environment - refer section 2.3.9.1



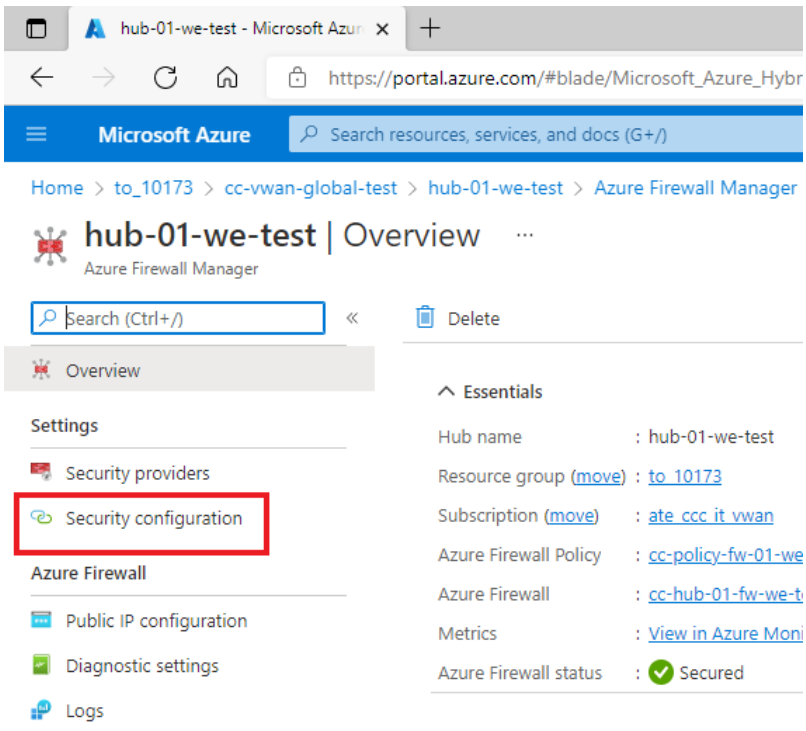
5. Click on “Secured Virtual Hub Settings” in left navigation pane.



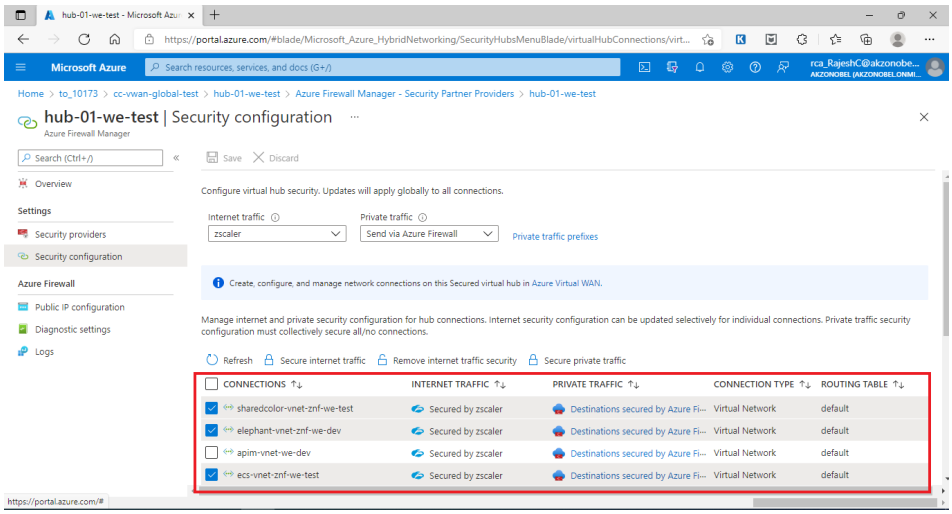
6. Click on Blue Ribbon in main page titled “Manage security provider and route settings for this Secured virtual hub in Azure Firewall Manager →”



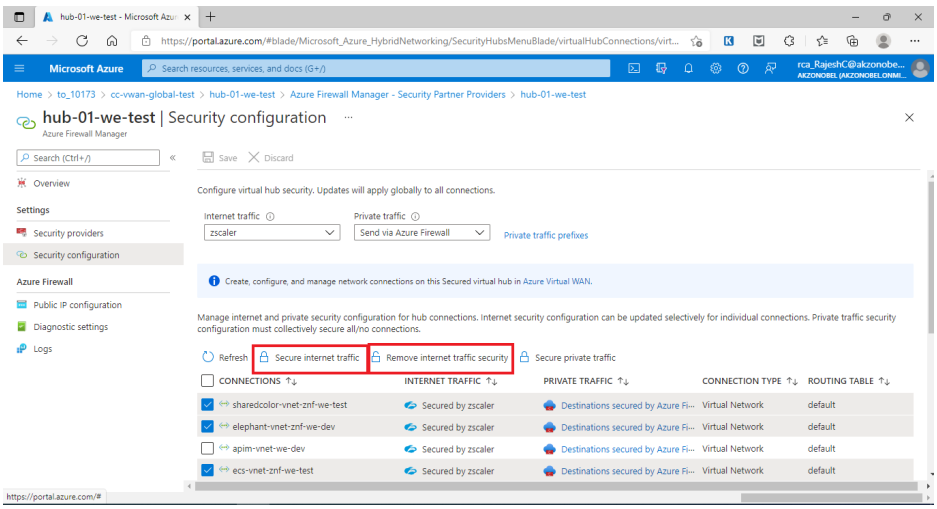
7. On the resulting page click on “Secure virtual hub” name for which private traffic needs to be secured.
8. On the hub overview page, click on “Security configuration” in left navigation pane.



9. On the resulting page, in the right pane, select the virtual network/spoke for which internet traffic needs to be secured/unsecured.



10. Click on either "***Secure internet traffic***" to secure the internet traffic or "***Remove internet traffic security***" to unsecure internet traffic.



11. Wait for the deployment complete notification on the Azure Portal GUI.

3.8.6.4 Unsecure Private Traffic

1. **All** the private traffic through the virtual hub will be secured always using Azure Firewall.

3.8.7 Delete Virtual Network/Spoke to Secured Virtual Hub Connection

1. Gather the required Virtual Network/Spoke details that needs to be disconnected from Secured Virtual Hub.
2. Gather a list of test scenarios to be used as pre-migration and post migration testing.
3. Prepare a spoke specific CSV data file for release pipeline to be used to disconnect spoke from virtual hub
4. Execute release pipeline to disconnect spoke/virtual network from secured virtual hub.
    a. Execute the release pipeline to delete firewall rules collection group associated with the virtual network/spoke being removed. Refer section 3.8.4 for details.
5. Test the change.

3.8.8 Tasks NOT in SCOPE but for Reference

3.8.8.1 Management of vNet NSG's / UDR's

Spoke application owners will continue to manage (add/ change/delete) their NSG and User Defined Route Table [UDR] entries.

***Note**: GSI will not get access to manage this.*

3.8.8.2 Monitoring ExpressRoute BW utilization

Orange Network Managed Service refer to key contact appendix C.

3.8.8.3 Monitoring Z-Scaler BW utilization

Data will be monitored on ZIA portal. For Orange Network Managed Service refer to key contact appendix C.

4. Managed Overview

4.1 Incident Management:

- ✓ AkzoNobel IT Service Desk will log Incident/ ticket with DCSC(L1) for reactive incident support. i.e. DCSC(L1) will be the SPOC for AkzoNobel IT service Desk
- ✓ DCSC (L1) will route the Incident/ ticket logged by AkzoNobel IT Service Desk to OGSI Team via Oceane to OGSI Queue for the resolution process.
- ✓ OGSI will do L2/L3 incident resolution support.
- ✓ OGSI will interwork with:
  - OEM for escalations or Third Party Vendor (if AkzoNobel engaged)
  - Assumption that vendor maintenance coverage in place.
- ✓ Orange Account team needs to ensure that Orange CS&O Clarify/Oceane ITSM Tool access is extended to OGSI.

Escalation matrix

Managed VWAN category definitions

Managed VWAN category definitions

Are found in the Annex 1H2-SLA Azure Networking MSP updated Feb 2022.

- ~~✓ AkzoNobel IT Service Desk will log Incident/ ticket with DCSC(L1) for reactive incident support. i.e. DCSC(L1) will be the SPOC for AkzoNobel IT service Desk~~
- ~~✓ DCSC (L1) will route the Incident/ ticket logged by AkzoNobel IT Service Desk to OGSI Team via Oceane to OGSI Queue for the resolution process.~~
- ~~✓ OGSI will do L2/L3 incident resolution support.~~
- ~~✓ OGSI will interwork with:~~
  - ~~OEM for escalations or Third Party Vendor (if AkzoNobel engaged)~~
  - ~~Assumption that vendor maintenance coverage in place.~~
- ~~✓ Orange Account team needs to ensure that Orange CS&O Clarify/Oceane ITSM Tool access is extended to OGSI.~~

~~Escalation matrix~~

~~TBA~~

[4.2] Change Management:

- ✓ Change Management will be applied to changes which are defined in the service catalogue as
  a. Simple Change (Standard Change)
  b. Change request triggered as part of solution to fix the Incident/Problem

- ✓ Change Catalogue will identify if change is Simple/Standard. For Change requests that are not mentioned in the catalogue, these will be considered as Complex or Project changes and will get handled through Order to Quote process (T&M Basis). As new changes are requested, they will be reviewed as potential simple / standard changes where possible.
- ✓ Anticipated Complex changes include migrating existing VNETS with active services, adding Secure Hub into new region and additional VWAN feature not used in the this project.
- ✓ An Akzo Nobel Service Now change will need to be raised for any spoke changes and communicated to spoke owners via Akzo points of contacts. The change approved and scheduled.
- ✓ If changes are required on Orange managed Zscaler or Express Route then connect with the Orange contact in the contact list and plan the technical change and create using template example below. Submit change to Shady Orange change manager see example attached and update Akzo managers regarding the tasks. Once approved then schedule and apply.

See examples below

4.2[4.3] Change Process management includes:

- ✓ Temporary manual change process will be used until change management ebonding is in place between OBS SNOW and AKZO SNOW - see appendix B for details
- ✓ New snow queue being created for changes / incidents workflow to be documented
- ✓ Customer Tool for changes to be raised. Training undertaken 9th Feb 2022 with GSI and tickets raised for prod migration.

  GSI have required access to the platform and tool.

Complex Changes Revised Feb 22

Item	Unit	OTC	MRC
SPOKE/VNET Add/Delete	Virtual Network - Service low complexity	€ 300,00	€ 100,00

	(No Active Services), using standard template		
SPOKE/VNET Migration	Virtual Network - Service high complexity	On quote	On quote
Site 2 Site VPN Connection	S2S VPN Gateway - Service high complexity	On quote	On quote
Point 2 Site VPN Connection	P2S Gateway - Service high Complexity	On quote	On quote
Virtual WAN Secure Hub (incl. Azure Firewall)	VWAN Secure Hub - Service high complexity	On quote	On quote
Virtual WAN Hub Add/Delete	VWAN Hub - Service high complexity	On quote	On quote
Automation script/ARM/bicep template - change	Change of a current powershell scripts, release pipelines or ARM/bicep templates	On quote	On quote
other	ie building new templates/scripts, connecting third party VNET's	On quote	On quote

Simple changes revised Feb 22

Item	Unit	OTC	MRC
Firewall rule - Add/modify/Delete	per rule Low Complexity - Capped on 20 rules per change	price included in service charge	price included in service charge

Dashboard data capture - log report	one time dashboard data capture, extract, analysis or report	price included in service charge	price included in service charge
Expressroute configuration - change	change of current ER configuration within hub	price included in service charge	price included in service charge
Zscaler configuration - change	change of current Zscaler configuration within hub	price included in service charge	price included in service charge
SPOKE/VNET connection - change	change of existing spoke connection	price included in service charge	price included in service charge

~~Complex changes~~

~~Complex changes~~

~~Item~~	~~Unit~~	~~OTC~~	~~MRC~~
~~SPOKE/VNET (No Active Services) Add/Delete~~	~~Virtual Network - Service low complexity using standard template~~	~~€ 300.00~~	~~€ 100.00~~
~~SPOKEVNET Migration~~	~~Virtual Network - Service High complexity~~	~~On quote~~	~~On quote~~
~~Site 2 Site VPN Connection~~	~~S2S VPN Gateway - Service High complexity~~	~~On quote~~	~~On quote~~
~~Point 2 Site VPN Connection~~	~~P2S Gateway - Service High Complexity~~	~~On quote~~	~~On quote~~
~~Virtual WAN Secure Hub (incl. Azure Firewall)~~	~~VWAN Secure Hub - Service High complexity~~	~~On quote~~	~~On quote~~
~~Virtual WAN Hub Add/Delete~~	~~VWAN Hub - Service High complexity~~	~~On quote~~	~~On quote~~
~~-~~	~~-~~		
~~other~~	~~e.g. migration legacy VNET, connecting third party VNET's~~	~~On quote~~	~~On quote~~

~~If AkzoNobel desires bulk changes, then this will be considered as project change and will be quoted on a time and material basis.~~

~~Simple/ standarrd operational~~

~~changes~~			
~~Item~~	~~Unit~~	~~OTC~~	~~MRC~~
~~FW Rule – Add/modify/Delete~~	~~per rule Low Complexity Capped # (50) Rules per change~~	~~price included in service charge~~	~~price included in service charge~~
~~etc~~	~~-~~	~~price included in service charge~~	~~price included in service charge~~
~~etc~~	~~-~~	~~price included in service charge~~	~~price included in service charge~~

4.3[4.4] Configuration Management:

✓ Configuration items are stored in customer Service Now

4.4[4.5] Release Management:

✓ Microsoft will release updates on their VWAN and implement internally within Microsoft.

✓ IP Addresses will be provided by Customer.

4.5[4.6] Service Now

Project team have discussed with AkzoNobel and Orange service now team and agreed naming convention.

Following describes what has been requested on orange side Dec 21 – will be updated

Short description: - Enhancement to Implement Incident ebonding between OBS SNOW and AkzoNobel SNOW for the new OBS VWAN Service (Virtual WAN Cloud Service)

Description: Implement Incident ebonding between OBS SNOW and AkzoNobel SNOW for the new OBS VWAN Service (Virtual WAN Cloud Service).

Details: OBS sold a brand new OBS service called OBS VWAN Service (Virtual WAN Cloud Service). For this new VWAN Service we need to establish Incident ebonding between OBS SNOW and AkzoNobel SNOW.

VWAN Incidents need to be assigned to the new OGSI VWAN queue, so that OBS OGSI India team will follow up with these incidents and have it fixed.

So according to our knowledge, the following need to be created in SNOW:

1) Add a new "Service Line" value called VWAN. The below table illustrates Orange Service Lines and the mapping to the AkzoNobel Service Model in AkzoNobel SNOW:

MyCIC ServiceNow Service Line	AkzoNobel L1 - Service Offering
VWAN	Network and Internet Access Service
MyCIC ServiceNow Service Line	**AkzoNobel L2 - Support Offering**
VWAN	Network Support
MyCIC ServiceNow Service Line	**AkzoNobel L3 - Supply Offering**
VWAN	Orange VWAN Supply

~~[2)]~~ 2) When a OBS SNOW incident is created with "service line" is VWAN, then OBS SNOW incident needs to be assigned to the existing "DCSC (L1)" queue called "CSD_Akzo_Nobel". ~~When a OBS SNOW incident is created with "service line" is VWAN, then OBS SNOW incident needs to be assigned to the new "OGSI VWAN" queue.~~

~~**Important:** This must be a separate queue then the existing OGSI MLAN queue.~~

~~So create new OGSI Queue called: **OGSI VWAN,** the mail address for this OGSI VWAN queue is: ogsi_akzo_vwan@easymail.orange.com~~

2)[3)] After SNOW VWAN incident is created, proper incident ebonding need to take place between OBS SNOW and AkzoNobel SNOW. so please implement appropriate ebonding using above service line mapping rule.

Note: since both DCSC (L1) and OGSI (L2) will manage andfix VWAN incidents from Oceane Platform, ebonding need to create as well a ticket in Oceane tool for VWAN service.

~~3) After SNOW VWAN incident is created, proper incident ebonding need to take place between OBS SNOW and AkzoNobel SNOW. so please implement appropriate ebonding using above service line mapping rule.~~

~~**Note:** since OGSI will manage VWAN incidents from OBS SNOW Platform, there is no need to ebond with Oceane tool for VWAN service.~~

[4)] ebonding should work both ways, so when customer initiates a ticket for VWAN service in AkzoNobel SNOW , it should automatically create a VWAN incident in OBS SNOW and vice versa so when OBS initiates a VWAN incident in OBS SNOW it should automatically create VWAN incident in AkzoNobel SNOW.

Agreed interim process whilst waiting fro service Now:

- DCSC will always be the SPOC level 1 for VWAN Incidents, they will do catch and dispatch to GSI India VWAN Team (level2) of Nitin.
- Nitin advised that DCSC can dispatch the Oceane VWAN tickets to existing GSI India Cloud Support queue "**ATQC85 – CSO MUM GSI Ser-Mgmt**" . GSI will then follow up on the Oceane subcase and fix the VWAN issue. Nitin advised that this is the standard way of working for incident management using Oceane.

- Raoul explained that we are in build phase to setup VWAN ebonding between customer Akzo SNOW and OBS SNOW on incident management, change management and CMDB. Nikita Patel is SNOW engineer working with customer on this.
- When ebonding is ready, Akzo DCSC will remain the SPOC (first level) for VWAN incidents, so DCSC and GSI India should still keep working within Oceane system as mentioned above.
- To visualize the process flow:

a) Temporary VWAN incident process (ebonding NOT ready):

Customer calls/mails DCSC about a VWAN incident-> DCSC opens a ticket in Oceane -> DCSC dispatch Oceane ticket (subcase) to GSI India Cloud Support queue "**ATQC85 – CSO MUM GSI Ser-Mgmt**" . GSI India will then follow up on the Oceane subcase and fix the VWAN issue.

b) Final VWAN incident process (when ebonding is ready between Akzo SNOW and OBS SNOW):

Customer opens a VWAN ticket in customer Akzonobel SNOW system-> corresponding OBS INC ticket is automatically created by ebonding in OBS SNOW system and assigned to "**CSD_ AkzoNobel**" queue of DCSC Cairo -> also SNOW-Oceane ebonding will automatically create an Oceane ticket in Oceane system and assigns it to existing DCSC Cairo queue -> DCSC will dispatch the Oceane VWAN ticket (subcase) to GSI India Cloud Support queue "**ATQC85 – CSO MUM GSI Ser-Mgmt**" . GSI India will then follow up on the Oceane subcase and fix the VWAN issue.

Managed Items	West Europé	~~North Europé~~	East US	Southeast Asia	Test Environment	Total
Virtual WAN Hub w/ Azure Firewall	1	0	1	1	1	4
VPN Connections to Third Parties	2	0	1	1	2	6
OBS Managed VNET's	1	0	1	1	4	7
Non-OBS Managed VNET's associated to VWAN Hub	31	0	0	0	0	31
Azure Firewall Instance	1	0	1	1	1	4
Total						

Changes
Infrastructure Changes - Fair Use Cap (24 hours per month)
Infrastructure Changes - Per Hour

Provide text due to spoke hub / hub spoke not being available at Microsoft East US and Southeast Asia has not been configured as part of current project.

Appendix A - Firewall Rules Naming Convention

Generic Guidelines

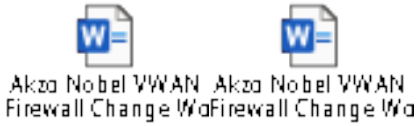
a. Names should be all lowercase.
b. Use "_" as separator.
c. Port ranges should be avoided but are tolerated (example 3200-3299 for SAP ABAP dispatcher communication).
d. For Port/Service, when standard or well-known ports are used, the service name is preferred over the port number – refer Service Name and Transport Protocol Port Number Registry (iana.org).
e. For PaaS services that have short and extended names, use short names [example SQL database "anratios (anrmmsqlsrveusdev/anratios) – use anratios"].
f. When a name cannot be unambiguously identified with the given convention (for rule collections for example), the spoke owner of the source should be asked for directions.

Item	Naming Convention	Examples	Comment
Rule Collection Group	rcg_{VNET name}	rcg_apim-vnet-we-dev rcg_apim-vnet-we-test rcg_akz-lnd1-p-euwe-vnet-spoke	
Network Rule Collection	netrc_{DestinationWorkload}	netrc_ds (ds here stands for Directory Services - the HCL spoke) netrc_sap netrc_onecolortool netrc_datafactory	The token {DestinationWorkload} should identify the purpose of the traffic (the destination); details of the traffic should be captured in the actual rule (child of the collection) There is some subjectivity in the use of the {DestinationWorkload} token but no convention is perfect.
Network Rule Name	{Allow/Deny}_{Source}_{Destination}_{Port/Service}	allow_adcn162_d365vmdevwed-1_8009 allow_adcn162_znlpo0265vn0001_http	Tokens {Source} and {Destination} for a virtual machine would be the VM name.

Item	Naming Convention	Examples	Comment
		allow_znlpo0265vn0001_akz-lnd1-d-backend_qmqp	For VMs within a specific subnet (specific for the rule being defined), the subnet could also be used.
		allow_znlpo0265vn0001_queueserver_qmqp	When a subnet is not specific enough for the rule being defined, a label could be used to identify the group of VMs.
		allow_akz-mgt1-p-logicapp-itsm_anratios_1433	For PaaS services, {Source} and {Destination} would be the name of the deployed resource.
Application Rule Collection	apprc_{DestinationService}	apprc_office365	The token {DestinationService} should identify the purpose of the destination service.
Application Rule Name	{Allow/Deny}_{Source}_{FQDNs}	allow_d365vmdevwed_office.net	Similarly as network rules, the token {Source} for a virtual machine would be the VM name; for VMs within a specific subnet (specific for the rule being defined), the subnet could also be used. When a subnet is not specific enough for the rule being defined, a label could be used to identify the group of VMs. For PaaS services, the token {Source} would be the name of the deployed resource.
NAT Rule Collection	natrc_{TransaledService}	natrc_sccm	The token {TransaledService} should identify the purpose of the translated service.
NAT Rule Name	{OriginalDest}_{TranslatedDest}	tms.AkzoNobel.com_znlpo0265vn0001 104.45.75.196_znlpo0265vn0001	The token {OriginalDest} could be the FQDN associated with the IP to be natted; if the FQDN is not available, the *original IP could be used instead. The token {TranslatedDest} for a virtual machine would be the VM name; for a PaaS Service it would be the name of the deployed resource.

Appendix B - Process for Customer Firewall Changes

Note: In the absence of service now a temporary process has been created to accommodate customer Firewall changes Feb 2022.



Teams - - > https://orange0.sharepoint.com/:f:/r/sites/AkzoNobel772/Documents%20partages/VWAN%20Build%20Project/GSI/Firewall%20Workflow?csf=1&web=1&e=Fb2uEC

Appendix C – Service Management

The escalation matrix of DCSC Cairo (L1) Operations will be as follows:

Level	Role	Name	Email	Desk phone	Mobile
Level 1 NBH Only From 7:00 AM to 4:00 PM GMT	Team Lead	heba.a.elsayed@orange.com	heba.a.elsayed@orange.com		
1 OBH	Shift lead	On duty Shift Leader	AkzoNobel.dcsc@orange.com	+202 2413 8573	
2	Head of AkzoNobel DCSC	Zakaria Fawzy	zakaria.fawzy@orange.com	+20222926431	+201287837776
3	Cluster Head - Benelux	Mohamed Emad	mohamede.emad@orange.com	+20222922386	+201272951267
4	Head of Service Desks	Amr Mohamed	amr.mohamed@orange.com	+20224634141	+201228789444
5	Head of Cairo MSC	Chirstopher McKay	christopher.mckay@orange.com	+44 2083214385	+44 7966861689

OGSI India (L2)

The OBS internal escalation matrix of OGSI (L2) Operations will be as follows-:

Escalation Level	Name	Role	Location	Contact details
1	Khurshed Bacha	Program / Operations manager - CoE Managed IT Services	India	Email: Khurshed.bacha@orange.com Phone: +91 9819723231
2	Nitin Thakur	Senior Program Manager – CoE Managed IT Services	India	Email: Nitin.Thakur@orange.com Phone: +91 9833879809
3	Sunil Bhatia	Head - COE Managed IT Services	India	Email: Sunil.Bhatia@orange.com Phone: +91-9833873177

Appendix DC - Key Contacts

Below are the key contacts list for reference.

Azure Monitor Services
Workspace and Events Alerting email: ogsi_akzo_vwan@easymail.orange.com

Important contacts

Role or Company	Name	Email	Contact Information
Z-Scaler	Tony Svensson	tony.svensson@orange.com	
Z-Scaler Support		support@zscaler.com	
Z-Scaler TAM (Technical Account Manager) Located in USA	Ishan Sharma	isharma@zscaler.com	001 (818) 724-8479
Z-Scaler Customer contact	'Jacobsen, J. (Jesper Tim)'	Jesper.Jacobsen@akzonobel.com	
Express Route	Tony Svensson	tony.svensson@orange.com	
DCSC	Dedicated Desk	akzonobel.dcsc@orange.com	
CSM Security	Mark Rus	mark.rus@orange.com	
	Bart Van Son	bart.vanson@orange.com	
CSM	Raoul Kaersenhout	raoul.kaersenhout@orange.com	+31 6 185 01 155
Orange Change Manager	Shady Salama	shady.salama@orange.com	
CCC Team	Randy Paulo	RandyAldrichIligan.Paulo@akzonobel.com	
ATOS, HCL and Central Finance (SAP)	Dino Bordonaro	Dino.Bordonaro@akzonobel.com	
ATOS contact in CCC (will help	Chaitanya Senapati	chaitanya.senapati@atos.net	

Role or Company	Name	Email	Contact Information
Microsoft ticket etc…) Spoke tests or spoke owner liaison			
Escalation for CCC and VWAN activities	Oussama Zoubairi	Oussama.Zoubairi@akzonobel.com	
		Spoke owners below but must have Dino and Randy ~~in~~in the ~~-~~loop	
HCL Lead Solutions Architect -DWP M&M Architecture	Subhajyoti Chakraborty	subhajyoti.c@hcl.com	+31620248288
Akzo SAP Spoke~~HCL~~	Jeroen Englelen	jeroen.engelen@akzonobel.com	
SAP	Pavan Koppula	pavan.koppula@sap.com	
SAP	Ramesh Kumar Venupal	rameshkumar.venugopal@sap.com	
ATOS	Gornicki, Radoslaw	radoslaw.gornicki@atos.net	
ATOS	Svyatoslav Poluyko	svyatoslav.poluyko.external@atos.net	

Appendix E – List of Spokes

List of Spokes/Virtual Networks in scope of migration to Azure Virtual WAN environment are listed below:

Environment	Spoke/Virtual Network Name	Address Space	Description
Development	apim-vnet-we-dev	10.252.182.64/26	API Management (PaaS)
Development	akz-lnd2-p-euwe-vnet-spoke	10.78.64.0/18	Atos (dev/test workload)
Development	elephant-vnet-znf-we-dev	10.253.2.0/24	Incubator Environment
Development	ocap-vnet-znf-we-dev	10.252.80.0/23	One Color Application Platform
Development	onehub-vnet-znf-we-dev	10.253.0.0/23	OneHUB Logic Apps Environment
Testing	apim-vnet-we-test	10.252.183.128/26	API Management (PaaS)
Testing	sharedcolor-vnet-znf-we-test	10.252.82.0/24	Color Shared Environment
Testing	dp-vnet-znf-we-test	10.252.244.0/22	Data Platform
Testing	sharedgbs-vnet-znf-we-test	10.252.95.0/26	GBS Shared Environment
Testing	ecs-vnet-znf-we-test	10.252.94.0/26	Global Labelling Solution
Testing	sharediot-vnet-znf-we-test	10.252.91.0/25	IoT Shared Environment
Testing	sharedisc-vnet-znf-we-test	10.252.92.0/25	Isc Shared Environment
Testing	sharedit-vnet-znf-we-test	10.252.83.0/24	IT Shared Environment
Testing	ocap-vnet-znf-we-acc	10.252.88.0/23	One Color Application Platform
Testing	onehub-vnet-znf-we-test	10.252.93.0/24	OneHUB Logic Apps Environment
Production	apim-vnet-sa-prod	10.252.207.192/26	API Management (PaaS)
Production	apim-vnet-us-prod	10.252.199.192/26	API Management (PaaS)
Production	apim-vnet-we-prod	10.252.183.192/26	API Management (PaaS)
Production	akz-lnd1-p-euwe-vnet-spoke	10.78.0.0/18	Atos (production)
Production	vnet-HEC44-ANO	10.252.228.0/22	Central Finance
Production	sharedcolor-vnet-znf-we-prod	10.252.86.0/24	Color Shared Environment
Production	dp-vnet-znf-we-prod	10.252.248.0/22	Data Platform
Production	sharedgbs-vnet-znf-we-prod	10.252.95.64/26	GBS Shared Environment
Production	ecs-vnet-znf-we-prod	10.252.94.64/26	Global Labelling Solution
Production	sharediot-vnet-znf-we-prod	10.252.91.128/25	IoT Shared Environment
Production	sharedisc-vnet-znf-we-prod	10.252.92.128/25	Isc Shared Environment
Production	sharedit-vnet-znf-we-prod	10.252.87.0/24	IT Shared Environment
Production	znepn0001nv0001	10.252.224.0/23	Next Generation Workplace (dmz)
Production	zncpn0001nv0001	10.252.208.0/20	Next Generation Workplace (internal)
Production	ocap-vnet-znf-deploy-we-prod	10.252.95.224/27	One Color Application Platform
Production	ocap-vnet-znf-we-prod	10.252.84.0/23	One Color Application Platform
DR	vnet-HEC42-ANO	10.252.232.0/22	Central Finance