|  |  |  |  |
| --- | --- | --- | --- |
| **Enterprise Business Process** | Optum Connect | **Last Updated Date** | 17/09/2023 |
| **Revision #** | 1.0.0 | **Process Owner** | Charles Colstrom |
| **Written/Revised By** | Pranav Singh | | |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **The following are approved changes incorporated into the revision numbers indicated below** | | | |
| **Version No.** | **Date** | **Description of Change** | **Modified By** |
| 1.0 | 17/09/2023 | *Initial Release* | Pranav Singh |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1. Purpose 3](#_Toc145612316)

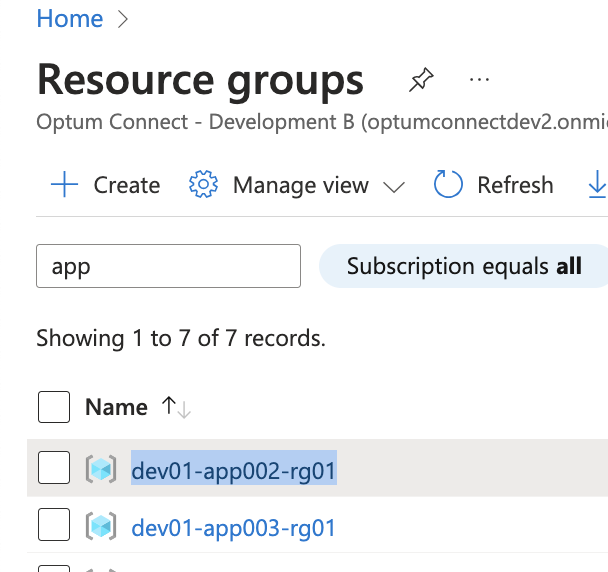
[2. Scope 3](#_Toc145612317)

[3. Network Architecture 3](#_Toc145612318)

[4. Azure Components 4](#_Toc145612319)

# <How to update this document guide- Remove this section after updating the document >

1. Update the name of the file
2. Update customername in header and footer
3. Update customername in section 2.
4. Update network architecture in section 3 using the standard design reference in this [link](https://uhgazure.sharepoint.com/:f:/r/sites/OptumConnectCOE/OCC%20Engineering%20SOP/Azure%20-%20CSP/Standard%20Customer%20Architecture%20Reference?csf=1&web=1&e=ETLqu4)
5. Update the resource names in section 4 by directly copying the name as shown in the image below, this will enable coping of the name with the link embedded.



1. Any other resources provisioned by OCC should be updated in the section 5 or altogether a separate document should be created mention the resources and architecture.

# Purpose

The purpose of this document is to record the Architecture and Azure Resources created by Optum Connect Cloud(OCC) Team before handing over the Azure Operations to the Cloud Ops/Green team.

# Scope

The OCE team will leverage this document to record the architecture and resources created when the **customername** Azure Tenant is onboarded to the Azure Subscription.

# Network Architecture

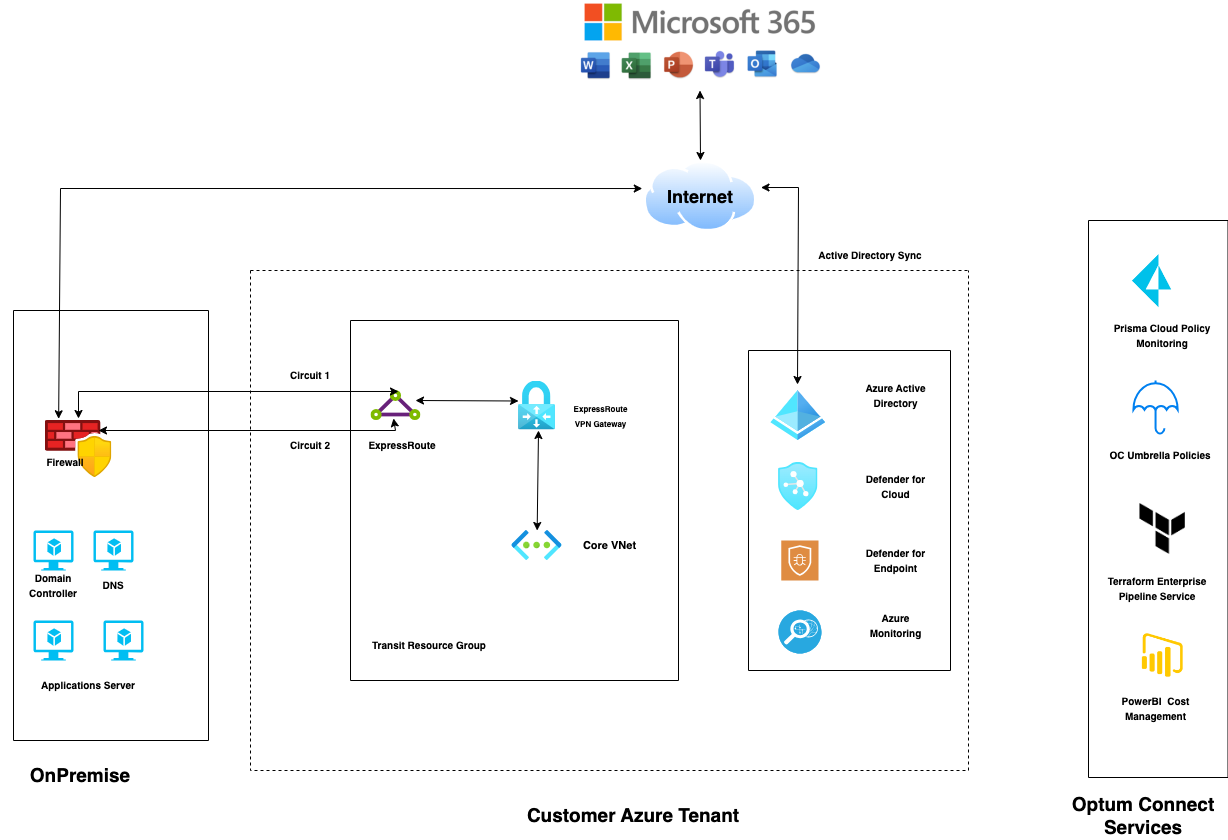
Optum Connect leverages Data Center extension as a primary objective while developing the network architecture. This involves hybrid connectivity using ExpressRoute and/or Site to site VPN. This approach also solves the problem of unified network connectivity and service reachability.

**Hybrid Network connectivity components**:

1. Resource Groups
2. Virtual Network (VNet)
3. Subnets (including Gateway Subnet)
4. Virtual Network Gateway
5. Express Route Circuit

The standard architecture also consists of following OCC essential service resources which are part of the CSP offerings:

1. AOBO Resource Groups (CSP Admin account activity monitoring and alerting)
2. AOBO alerting and notification using Azure Logic App
3. Microsoft Defender for Cloud CSPM
4. Log Analytics Workspace
5. Azure Policies (Umbrella Policies)

 **Core Architecture**

# Azure Components

1. **Resource Group**: [prd01-app001-rg01](https://portal.azure.com/#@eastmehealth.onmicrosoft.com/resource/subscriptions/12ff6d4c-3e25-4f76-8924-6017a664d82c/resourceGroups/prd01-app001-rg01)

To monitor and alert AOBO Account Activity and Log Microsoft Defender for Cloud Logs

1. Log Analytics Workspace [prodlogws01](https://portal.azure.com/#@eastmehealth.onmicrosoft.com/resource/subscriptions/12ff6d4c-3e25-4f76-8924-6017a664d82c/resourceGroups/prd01-app001-rg01/providers/Microsoft.OperationalInsights/workspaces/prodlogws01)
2. Logic App [prd-nlh-AOBO-alert-email](https://portal.azure.com/#@eastmehealth.onmicrosoft.com/resource/subscriptions/12ff6d4c-3e25-4f76-8924-6017a664d82c/resourceGroups/prd01-app001-rg01/providers/Microsoft.Logic/workflows/prd-nlh-AOBO-alert-email)
3. **Resource Group**: [prd01-app002-rg01](https://portal.azure.com/#@eastmehealth.onmicrosoft.com/resource/subscriptions/12ff6d4c-3e25-4f76-8924-6017a664d82c/resourceGroups/prd01-app002-rg01)

To manage hybrid network resources

1. Virtual Network [prd01-app002-vnet01](https://portal.azure.com/#@eastmehealth.onmicrosoft.com/resource/subscriptions/12ff6d4c-3e25-4f76-8924-6017a664d82c/resourceGroups/prd01-app002-rg01/providers/Microsoft.Network/virtualNetworks/prd01-app002-vnet01)

Address space: 10.1.1.1

Subnets:

* [GatewaySubnet](https://portal.azure.com/) - 10.18.1.0/27
* [prd01-app002-snet01](https://portal.azure.com/) - 10.18.1.32/27

1. Virtual Network Gateway [prd01-app002-vngw01](https://portal.azure.com/#@eastmehealth.onmicrosoft.com/resource/subscriptions/12ff6d4c-3e25-4f76-8924-6017a664d82c/resourceGroups/prd01-app002-rg01/providers/Microsoft.Network/virtualNetworkGateways/prd01-app002-vngw01)

Public IP: [prd01-app002-pip01](https://portal.azure.com/#@eastmehealth.onmicrosoft.com/resource/subscriptions/12ff6d4c-3e25-4f76-8924-6017a664d82c/resourceGroups/prd01-app002-rg01/providers/Microsoft.Network/publicIPAddresses/prd01-app002-pip01)

1. Express Route Circuit: [prd01-app002-erc01](https://portal.azure.com/#@eastmehealth.onmicrosoft.com/resource/subscriptions/12ff6d4c-3e25-4f76-8924-6017a664d82c/resourceGroups/prd01-app002-rg01/providers/Microsoft.Network/expressRouteCircuits/prd01-app002-erc01)

Peering: Azure Private Peering 10.11.0.0/30

1. Connection: [prd01-app002-erc01-vngw02-conn](https://portal.azure.com/#@eastmehealth.onmicrosoft.com/resource/subscriptions/12ff6d4c-3e25-4f76-8924-6017a664d82c/resourceGroups/prd01-app002-rg01/providers/Microsoft.Network/connections/prd01-app002-erc01-vngw02-conn)

Connection Between ExpressRoute Circuit and VPN Gateway

1. **Azure Policy**

Optum Connect Umbrella Policies to control the posture of the Azure Environment.

*See Appendix section for the list of the Umbrella Policies.*

1. **Microsoft Defender for Cloud (Security Center)**

* Enabled MDFC **Standard** Plan.
* Enabled **Auto Provisioning** of Agent

# Appendix

**OCC Umbrella Policies**:

|  |  |  |  |
| --- | --- | --- | --- |
| **Sl No.** | **Policy Name** | **Policy Type** | **Description** |
| 1. | occAdaptiveApplicationControls | AuditIfNotExists | Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps harden your machines against malware. To simplify the process of configuring and maintaining your rules, Security Centre uses machine learning to analyse the applications running on each machine and suggest the list of known-safe applications. |
| 2. | occClassicResourceDeny | Deny | Denies creation of any classic resources in the environment. |
| 3. | occEncryptionEnabled-DatalakeStore | Deny | Require encryption on Data Lake Store accounts. |
| 4. | occFunAppDenyHttp | Deny | Allows only https configuration in function apps. |
| 5. | occNSGAllowedPortsInbound | Audit | Audit security rules that allow port ranges inbound. |
| 6. | occNonGatewaySubnetRequireNSG | Audit | Audit non gateway subnets which do not have a Network Security Group (NSG) configured |
| 7. | occStorageAccountEncryption | Audit | Ensures file encryption for storage accounts. |
| 8. | occStorageAccountWithDefaultACL | Audit | Audit Storage Accounts without a Firewall. |
| 9. | occVMsNotUsingManagedDisks | Audit | Audit VMs that do not use managed disks. |
| 10. | occVulnerabilityAssessmentSolution-VMS | AuditIfNotExists | Audits virtual machines to detect whether they are running a supported vulnerability assessment solution. A core component of every cyber risk and security program is the identification and analysis of vulnerabilities. Azure Security Centre’s standard pricing tier includes vulnerability scanning for your virtual machines at no extra cost. Additionally, Security Centre can automatically deploy this tool for you. |
| 11. | occPublicIPsDenyonNics | Deny | Deny association of Public IP with NICs. |