Azure ALZ - 300

(Github)

Deploy Virtual WAN Resources With Custom Settings

Overview: Azure landing zones with connectivity resources based on the Virtual WAN network topology (Microsoft-managed) created in the current Subscription context, using custom configuration settings.

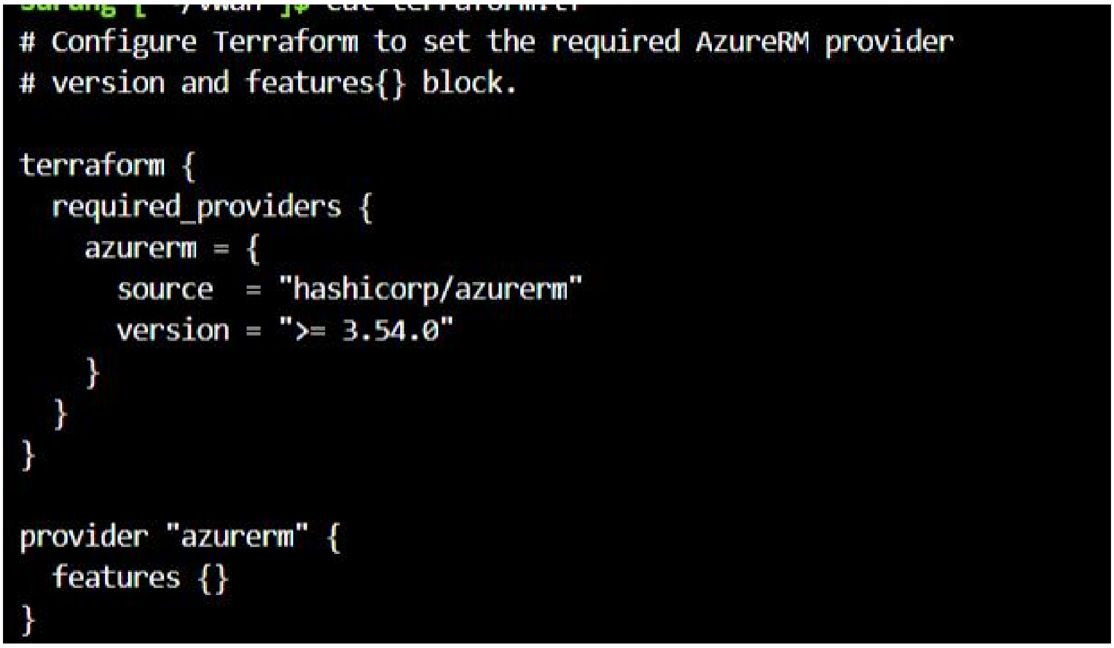
Resoruce Count: 302

Scope:

- Deploy a shared DDoS Network Protection plan in the northeurope region
- Deploy virtual hubs to northeurope and westeurope
- Deploy an ExpressRoute gateway and Azure Firewall to the virtual hub in northeurope
- Deploy a VPN gateway to the virtual hub in westeurope
- Ensure private DNS zones for private endpoints are enabled for northeurope and westeurope regions 1
- Set a different default location for connectivity resources (controlled through an input variable on the root module)
- Add custom resource tags for connectivity resources (controlled through an input variable on the root module)

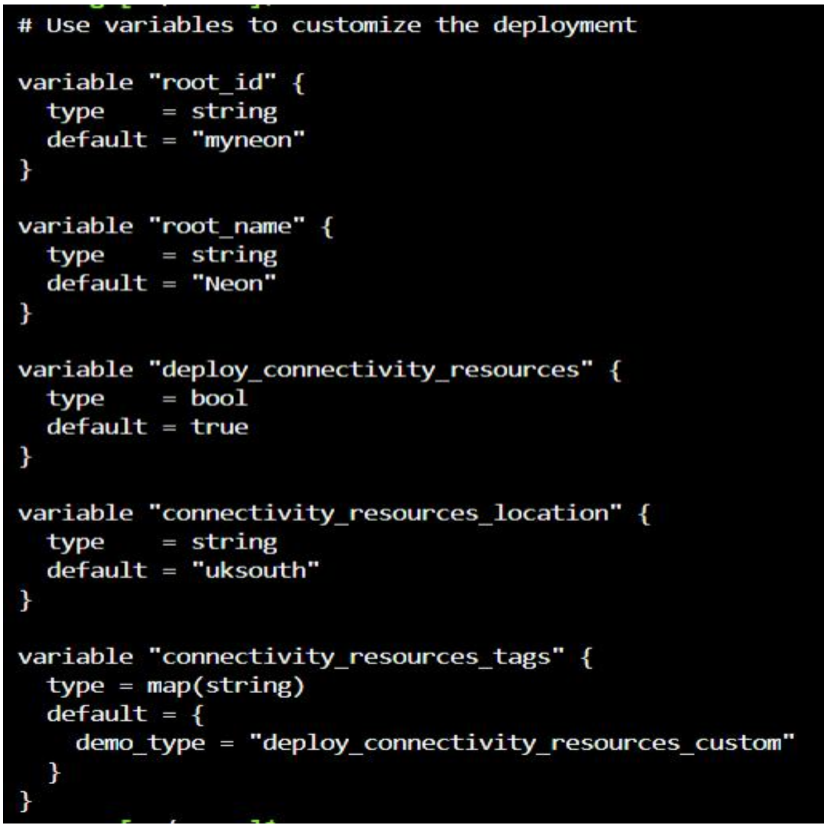
Steps:

1. The code is divided into 4 parts based on their configuration and uses.
2. terraform.tf



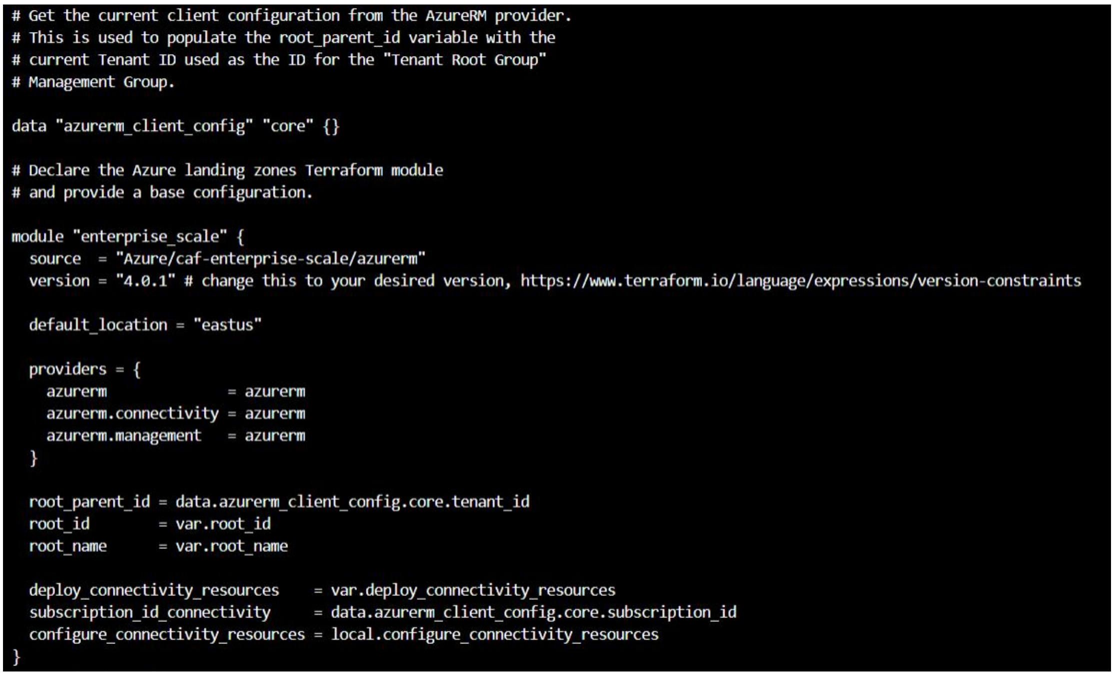
```
# Configure Terraform to set the required AzureRM provider
# version and features{} block.

terraform {
  required_providers {
    azurerm = {
      source  = "hashicorp/azurerm"
      version = ">= 3.54.0"
    }
  }
}

provider "azurerm" {
  features {}
}
```

3. variables.tf



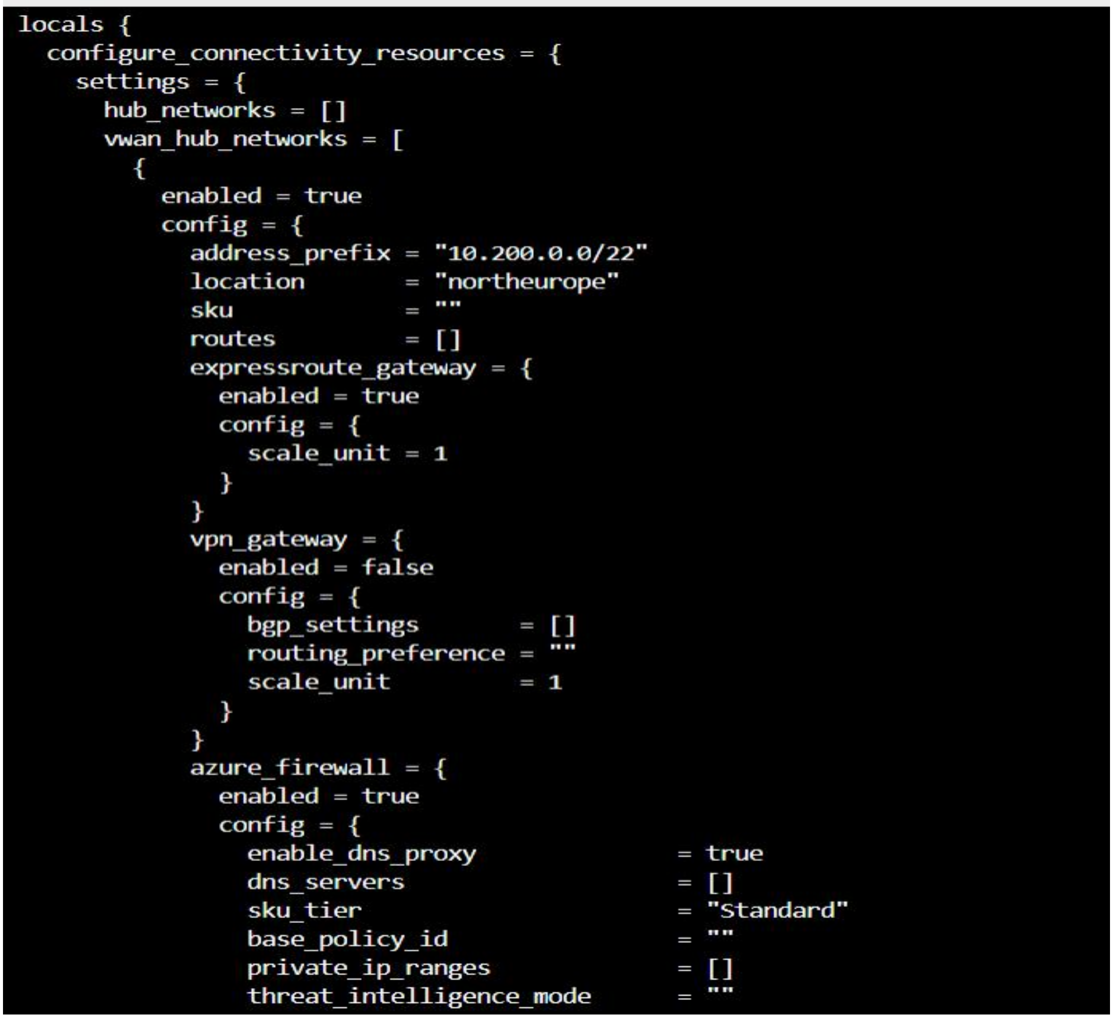
```
# Use variables to customize the deployment

variable "root_id" {
  type    = string
  default = "myneon"
}

variable "root_name" {
  type    = string
  default = "Neon"
}

variable "deploy_connectivity_resources" {
  type    = bool
  default = true
}

variable "connectivity_resources_location" {
  type    = string
  default = "uksouth"
}

variable "connectivity_resources_tags" {
  type = map(string)
  default = {
    demo_type = "deploy_connectivity_resources_custom"
  }
}
```

4. main.tf

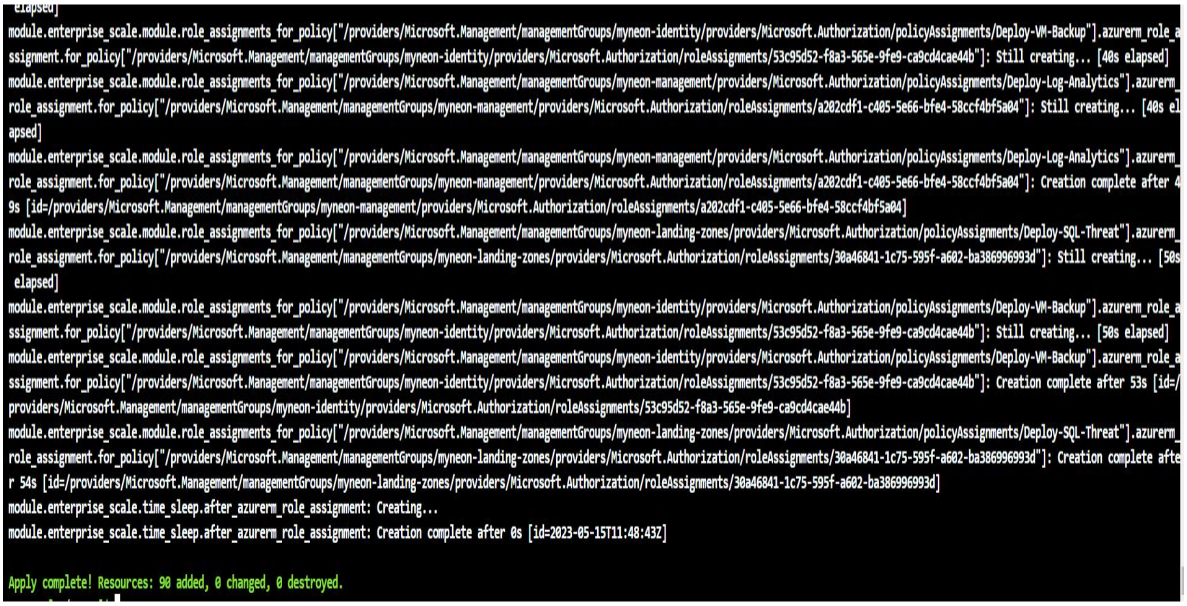


```
# Get the current client configuration from the AzureRM provider.
# This is used to populate the root_parent_id variable with the
# current Tenant ID used as the ID for the "Tenant Root Group"
# Management Group.

data "azurerm_client_config" "core" {}

# Declare the Azure landing zones Terraform module
# and provide a base configuration.

module "enterprise_scale" {
  source  = "Azure/caf-enterprise-scale/azurerm"
  version = "4.0.1" # change this to your desired version, https://www.terraform.io/language/expressions/version-constraints

  default_location = "eastus"

  providers = {
    azurerm              = azurerm
    azurerm.connectivity = azurerm
    azurerm.management   = azurerm
  }

  root_parent_id = data.azurerm_client_config.core.tenant_id
  root_id        = var.root_id
  root_name      = var.root_name

  deploy_connectivity_resources    = var.deploy_connectivity_resources
  subscription_id_connectivity     = data.azurerm_client_config.core.subscription_id
  configure_connectivity_resources = local.configure_connectivity_resources
}
```

5. settings.connectivity.tf



```
locals {
  configure_connectivity_resources = {
    settings = {
      hub_networks = []
      vwan_hub_networks = [
        {
          enabled = true
          config = {
            address_prefix = "10.200.0.0/22"
            location       = "northeurope"
            sku            = ""
            routes         = []
            expressroute_gateway = {
              enabled = true
              config = {
                scale_unit = 1
              }
            }
            vpn_gateway = {
              enabled = false
              config = {
                bgp_settings       = []
                routing_preference = ""
                scale_unit         = 1
              }
            }
            azure_firewall = {
              enabled = true
              config = {
                enable_dns_proxy              = true
                dns_servers                   = []
                sku_tier                      = "Standard"
                base_policy_id                = ""
                private_ip_ranges             = []
                threat_intelligence_mode      = ""
```



```
 elapsed]
module.enterprise_scale.module.role_assignments_for_policy["/providers/Microsoft.Management/managementGroups/myneon-identity/providers/Microsoft.Authorization/policyAssignments/Deploy-VM-Backup"].azurerm_role_a
ssignment.for_policy["/providers/Microsoft.Management/managementGroups/myneon-identity/providers/Microsoft.Authorization/roleAssignments/53c95d52-f8a3-565e-9fe9-ca9cd4cae44b"]: Still creating... [40s elapsed]
module.enterprise_scale.module.role_assignments_for_policy["/providers/Microsoft.Management/managementGroups/myneon-management/providers/Microsoft.Authorization/policyAssignments/Deploy-Log-Analytics"].azurerm_
role_assignment.for_policy["/providers/Microsoft.Management/managementGroups/myneon-management/providers/Microsoft.Authorization/roleAssignments/a202cdf1-c405-5e66-bfe4-58ccf4bf5a04"]: Still creating... [40s el
apsed]
module.enterprise_scale.module.role_assignments_for_policy["/providers/Microsoft.Management/managementGroups/myneon-management/providers/Microsoft.Authorization/policyAssignments/Deploy-Log-Analytics"].azurerm_
role_assignment.for_policy["/providers/Microsoft.Management/managementGroups/myneon-management/providers/Microsoft.Authorization/roleAssignments/a202cdf1-c405-5e66-bfe4-58ccf4bf5a04"]: Creation complete after 4
9s [id=/providers/Microsoft.Management/managementGroups/myneon-management/providers/Microsoft.Authorization/roleAssignments/a202cdf1-c405-5e66-bfe4-58ccf4bf5a04]
module.enterprise_scale.module.role_assignments_for_policy["/providers/Microsoft.Management/managementGroups/myneon-landing-zones/providers/Microsoft.Authorization/policyAssignments/Deploy-SQL-Threat"].azurerm_
role_assignment.for_policy["/providers/Microsoft.Management/managementGroups/myneon-landing-zones/providers/Microsoft.Authorization/roleAssignments/30a46841-1c75-595f-a602-ba386996993d"]: Still creating... [50s
 elapsed]
module.enterprise_scale.module.role_assignments_for_policy["/providers/Microsoft.Management/managementGroups/myneon-identity/providers/Microsoft.Authorization/policyAssignments/Deploy-VM-Backup"].azurerm_role_a
ssignment.for_policy["/providers/Microsoft.Management/managementGroups/myneon-identity/providers/Microsoft.Authorization/roleAssignments/53c95d52-f8a3-565e-9fe9-ca9cd4cae44b"]: Still creating... [50s elapsed]
module.enterprise_scale.module.role_assignments_for_policy["/providers/Microsoft.Management/managementGroups/myneon-identity/providers/Microsoft.Authorization/policyAssignments/Deploy-VM-Backup"].azurerm_role_a
ssignment.for_policy["/providers/Microsoft.Management/managementGroups/myneon-identity/providers/Microsoft.Authorization/roleAssignments/53c95d52-f8a3-565e-9fe9-ca9cd4cae44b"]: Creation complete after 53s [id=/
providers/Microsoft.Management/managementGroups/myneon-identity/providers/Microsoft.Authorization/roleAssignments/53c95d52-f8a3-565e-9fe9-ca9cd4cae44b]
module.enterprise_scale.module.role_assignments_for_policy["/providers/Microsoft.Management/managementGroups/myneon-landing-zones/providers/Microsoft.Authorization/policyAssignments/Deploy-SQL-Threat"].azurerm_
role_assignment.for_policy["/providers/Microsoft.Management/managementGroups/myneon-landing-zones/providers/Microsoft.Authorization/roleAssignments/30a46841-1c75-595f-a602-ba386996993d"]: Creation complete afte
r 54s [id=/providers/Microsoft.Management/managementGroups/myneon-landing-zones/providers/Microsoft.Authorization/roleAssignments/30a46841-1c75-595f-a602-ba386996993d]
module.enterprise_scale.time_sleep.after_azurerm_role_assignment: Creating...
module.enterprise_scale.time_sleep.after_azurerm_role_assignment: Creation complete after 0s [id=2023-05-15T11:48:43Z]

Apply complete! Resources: 90 added, 0 changed, 0 destroyed.
```

Below are the list of resources created

Count = 76

NAME	TYPE	RESOURCE GROUP	LOCATION	SUBSCRIPTION
myneon-ddos-northeurope	DDoS protection plan	myneon-ddos	North Europe	Pay-As-You-Go
myneon-ergw-northeurope	Microsoft.Network express route gateway	myneon-connectivity	North Europe	Pay-As-You-Go
myneon-fw-hub-northeurope	Firewall	myneon-connectivity	North Europe	Pay-As-You-Go
myneon-fw-hub-northeurope-policy	Firewall Policy	myneon-connectivity	North Europe	Pay-As-You-Go
myneon-vwan-uksouth	Virtual WAN	myneon-connectivity	UK South	Pay-As-You-Go
privatelink.adf.azure.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.afs.azure.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.agentsvc.azure-automation.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.analysis.windows.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.api.azureml.ms	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.azconfig.io	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.azure-api.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.azure-automation.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.azure-devices-provisioning.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.azure-devices.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.azurecr.io	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.azurehdinsight.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.azurehealthcareapis.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.azurestaticapps.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.azuresynapse.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.azurewebsites.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.batch.azure.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.blob.core.windows.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.cassandra.cosmos.azure.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.cognitiveservices.azure.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.database.windows.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.datafactory.azure.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.dev.azuresynapse.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.developer.azure-api.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go

privatelink.dfs.core.windows.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.dicom.azurehealthcareapis.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.digitaltwins.azure.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.directline.botframework.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.documents.azure.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.eventgrid.azure.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.file.core.windows.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.gremlin.cosmos.azure.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.guestconfiguration.azure.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.his.arc.azure.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.kubernetesconfiguration.azure.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.managedhsm.azure.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.mariadb.database.azure.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.media.azure.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.mongo.cosmos.azure.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.monitor.azure.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.mysql.database.azure.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.ne.backup.windowsazure.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.northeurope.azmk8s.io	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.northeurope.kusto.windows.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.notebooks.azure.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.ods.opinsights.azure.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.oms.opinsights.azure.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.pbidedicated.windows.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.postgres.database.azure.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.prod.migration.windowsazure.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.purview.azure.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.purviewstudio.azure.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.queue.core.windows.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.redis.cache.windows.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.redisenterprise.cache.azure.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.search.windows.net	Private DNS zone	myneon-dns	Global	Pay-As-

				You-Go
privatelink.service.signalr.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.servicebus.windows.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.siterecovery.windowsazure.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.sql.azuresynapse.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.table.core.windows.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.table.cosmos.azure.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.tip1.powerquery.microsoft.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.token.botframework.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.vaultcore.azure.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.we.backup.windowsazure.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.web.core.windows.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.webpubsub.azure.com	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.westeurope.azmk8s.io	Private DNS zone	myneon-dns	Global	Pay-As-You-Go
privatelink.westeurope.kusto.windows.net	Private DNS zone	myneon-dns	Global	Pay-As-You-Go

Below is the list of policy assignments
Count= 17

RoleAssignmentId	Scope	DisplayName	RoleDefinitionName	RoleDefinitionId	ObjectId	ObjectType
fde22a00-0a2d-5f7c-a56c-2af25e26efb4	/providers/Microsoft.Management/managementGroups/myneon	Deploy-AzActivity-Log	Log Analytics Contributor	/providers/Microsoft.Authorization/roleDefinitions/92aaf0da-9dab-42b6-94a3-d43ce8d16293	f885f9d7-2df7-4326-a9d3-1a8829422ef5	ServicePrincipal
3fd46377-b7b0-59e6-8ab4-c7631581c88f	/providers/Microsoft.Management/managementGroups/myneon	Deploy-AzActivity-Log	Monitoring Contributor	/providers/Microsoft.Authorization/roleDefinitions/749f88d5-cbae-40b8-bcfc-e573ddc772fa	f885f9d7-2df7-4326-a9d3-1a8829422ef5	ServicePrincipal
19182961-3fb9-5d13-9ba5-11831bc7a971	/providers/Microsoft.Management/managementGroups/myneon	Deploy-MDEndpoints	Contributor	/providers/Microsoft.Authorization/roleDefinitions/b24988ac-6180-42a0-ab88-20f7382dd24c	be2e750f-76b4-4899-9b34-8e42e59d9511	ServicePrincipal
dec212d5-a6bf-50c6-b042-137b8ba606d3	/providers/Microsoft.Management/managementGroups/myneon	Deploy-MDFC-Config	Azure Kubernetes Service Policy Add-on Deployment	/providers/Microsoft.Authorization/roleDefinitions/18ed5180-3e48-46fd-8541-4ea054d57064	fa45af36-a7ba-4730-85f5-74a6b429f37a	ServicePrincipal
1eca545e-	/providers/Micros	Deploy	Log Analytics	/providers/Micros	fa45af36-	ServicePr

05ff-5ba9-8da7-02162793fa15	oft.Management/managementGroups/myneon	-MDFC-Config	Contributor	oft.Authorization/roleDefinitions/92aaf0da-9dab-42b6-94a3-d43ce8d16293	a7ba-4730-85f5-74a6b429f37a	incipal
61fdf1cf-7e83-51b2-bf14-d52fea7bc695	/providers/Microsoft.Management/managementGroups/myneon	Deploy-MDFC-Config	Contributor	/providers/Microsoft.Authorization/roleDefinitions/b24988ac-6180-42a0-ab88-20f7382dd24c	fa45af36-a7ba-4730-85f5-74a6b429f37a	ServicePrincipal
a67be970-6cd9-5848-a268-d3b4d10d2545	/providers/Microsoft.Management/managementGroups/myneon	Deploy-MDFC-Config	Security Admin	/providers/Microsoft.Authorization/roleDefinitions/fb1c8493-542b-48eb-b624-b4c8fea62acd	fa45af36-a7ba-4730-85f5-74a6b429f37a	ServicePrincipal
45bda08a-0116-523d-81d1-0c88325289e7	/providers/Microsoft.Management/managementGroups/myneon	Deploy-MDFC-Config	Azure Kubernetes Service Contributor Role	/providers/Microsoft.Authorization/roleDefinitions/ed7f3fbd-7b88-4dd4-9017-9adb7ce333f8	fa45af36-a7ba-4730-85f5-74a6b429f37a	ServicePrincipal
ad09ad90-2c44-5ca3-a18e-446f0910bd4e	/providers/Microsoft.Management/managementGroups/myneon	Deploy-MDFC-OssDb	Contributor	/providers/Microsoft.Authorization/roleDefinitions/b24988ac-6180-42a0-ab88-20f7382dd24c	d4f43ab3-519a-4f98-98e3-87bc8dccd03c	ServicePrincipal
b69c9222-30ab-58c7-8ed0-683e1f133a7c	/providers/Microsoft.Management/managementGroups/myneon	Deploy-MDFC-SqlAtp	SQL Security Manager	/providers/Microsoft.Authorization/roleDefinitions/056cd41c-7e88-42e1-933e-88ba6a50c9c3	b4270844-e9d8-429f-b210-142a98ceaf76	ServicePrincipal
a0179097-3b26-5fc0-88eb-c6157fa01c34	/providers/Microsoft.Management/managementGroups/myneon	Deploy-Resource-Diag	Monitoring Contributor	/providers/Microsoft.Authorization/roleDefinitions/749f88d5-cbae-40b8-bcfc-e573ddc772fa	dbee51d4-052c-491c-a4b3-9e67f1b17934	ServicePrincipal
c02778d4-f1e7-5520-9b9b-8d50d5bf2a8f	/providers/Microsoft.Management/managementGroups/myneon	Deploy-Resource-Diag	Log Analytics Contributor	/providers/Microsoft.Authorization/roleDefinitions/92aaf0da-9dab-42b6-94a3-d43ce8d16293	dbee51d4-052c-491c-a4b3-9e67f1b17934	ServicePrincipal
4c0b7c1a-b5ca-5b8f-afc3-ac39718eaa20	/providers/Microsoft.Management/managementGroups/myneon	Deploy-VM-Monitoring	Log Analytics Contributor	/providers/Microsoft.Authorization/roleDefinitions/92aaf0da-9dab-42b6-94a3-d43ce8d16293	5ed543de-4ea0-4064-ae7a-e717430ff08c	ServicePrincipal
12a38c11-8d02-5696-8b15-cf2b8bc98eb1	/providers/Microsoft.Management/managementGroups/myneon	Deploy-VMSS-Monitoring	Virtual Machine Contributor	/providers/Microsoft.Authorization/roleDefinitions/9980e02c-c2be-4d73-94e8-173b1dc7cf3c	94afc77b-8e1d-4aa4-a22b-9818f729b5be	ServicePrincipal
44e228fb-9284-5532-af5f-f884209dc5	/providers/Microsoft.Management/managementGroups/myneon	Deploy-VMSS-Monit	Log Analytics Contributor	/providers/Microsoft.Authorization/roleDefinitions/92aaf0da-9dab-42b6-	94afc77b-8e1d-4aa4-a22b-9818f729b5b	ServicePrincipal

a4		oring		94a3-d43ce8d16293	e	
2cfd6bdb-aaa9-5c65-a96d-35c597f4cbd8	/providers/Microsoft.Management/managementGroups/myneon	Enforce-ACSB	Contributor	/providers/Microsoft.Authorization/roleDefinitions/b24988ac-6180-42a0-ab88-20f7382dd24c	851bc8ae-36de-4e46-b660-e9d388ab2cbe	ServicePrincipal