

Combine Deployment Of Connectivity And Management Resources In Individual Subscription

By:
All DevOps Team
Date: 17/05/2023

Strategy

The POC included a deployment with multiple subscriptions for management resources and connectivity, keeping Virtual WAN without a Ddos protection as a base for connectivity within multiple regions.

The basic idea was to combine the previous deployment codes of VWAN and management groups and testing its working.

The outputs have been noted and POC is successful.

Further, we will add the identity resources based upon the plans and customize some settings.

This code will act as a base for further deployments in Phase 3.

To make the code easier to maintain when extending your configuration, we splitting the root module into multiple files.

For the purpose of this example, we use the following:

- `main.tf`
- `settings.connectivity.tf`
- `settings.management.tf`
- `terraform.tf`
- `variables.tf`

--CODE--

Tree Structure:

```
root@AZURE-DEPLOYMENT# tree alz_combined_connectivit_management/
alz_combined_connectivit_management/
├── main.tf
├── settings.connectivity.tf
├── settings.management.tf
├── terraform.tf
└── variables.tf

0 directories, 5 files
```

Main.tf

```
# Obtain client configuration from the "management" provider
data "azurerm_client_config" "management" {
  provider = azurerm.management
}

# Obtain client configuration from the "connectivity" provider
data "azurerm_client_config" "core" {}

# Map each module provider to their corresponding `azurerm` provider using the providers input
object
module "enterprise_scale" {
  source = "Azure/caf-enterprise-scale/azurerm"
  version = "4.0.1"

  default_location = "eastus"
  providers = {
    azurerm = azurerm
    azurerm.management = azurerm.management
    azurerm.connectivity = azurerm
  }

  # Set the required input variable `root_parent_id` using the Tenant ID from the un-aliased
  provider
  root_parent_id = data.azurerm_client_config.core.tenant_id
  root_id = var.root_id
  root_name = var.root_name

  # Enable deployment of the management resources, using the management
  # aliased provider to populate the correct Subscription ID
  deploy_management_resources = var.deploy_management_resources
  subscription_id_management = data.azurerm_client_config.management.subscription_id
  configure_management_resources = local.configure_management_resources
  deploy_connectivity_resources = var.deploy_connectivity_resources
  subscription_id_connectivity = data.azurerm_client_config.core.subscription_id
  configure_connectivity_resources = local.configure_connectivity_resources
}
```

settings.connectivity.tf

```
# Configure the connectivity resources settings.
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 = ""
          threat_intelligence_allowlist = []
          availability_zones = {
            zone_1 = true
            zone_2 = true
            zone_3 = true
          }
        }
      }
      spoke_virtual_network_resource_ids      = []
      secure_spoke_virtual_network_resource_ids = []
      enable_virtual_hub_connections          = false
    }
  },
  {
    enabled = true
    config = {
```

```
address_prefix = "10.201.0.0/22"
location        = "westeurope"
sku             = ""
routes          = []
expressroute_gateway = {
  enabled = false
  config = {
    scale_unit = 1
  }
}
vpn_gateway = {
  enabled = true
  config = {
    bgp_settings      = []
    routing_preference = ""
    scale_unit         = 1
  }
}
azure_firewall = {
  enabled = false
  config = {
    enable_dns_proxy      = true
    dns_servers           = []
    sku_tier               = "Standard"
    base_policy_id        = ""
    private_ip_ranges     = []
    threat_intelligence_mode = ""
    threat_intelligence_allowlist = []
    availability_zones = {
      zone_1 = true
      zone_2 = true
      zone_3 = true
    }
  }
}
spoke_virtual_network_resource_ids      = []
secure_spoke_virtual_network_resource_ids = []
enable_virtual_hub_connections          = false
},
]

dns = {
  enabled = true
  config = {
    location = null
    enable_private_link_by_service = {
      azure_api_management      = true
      azure_app_configuration_stores = true
      azure_arc                  = true
      azure_automation_dscandhybridworker = true
      azure_automation_webhook    = true
      azure_backup                = true
      azure_batch_account         = true
      azure_bot_service_bot       = true
      azure_bot_service_token     = true
    }
  }
}
```

```
azure_cache_for_redis = true
azure_cache_for_redis_enterprise = true
azure_container_registry = true
azure_cosmos_db_cassandra = true
azure_cosmos_db_gremlin = true
azure_cosmos_db_mongodb = true
azure_cosmos_db_sql = true
azure_cosmos_db_table = true
azure_data_explorer = true
azure_data_factory = true
azure_data_factory_portal = true
azure_data_health_data_services = true
azure_data_lake_file_system_gen2 = true
azure_database_for_mariadb_server = true
azure_database_for_mysql_server = true
azure_database_for_postgresql_server = true
azure_digital_twins = true
azure_event_grid_domain = true
azure_event_grid_topic = true
azure_event_hubs_namespace = true
azure_file_sync = true
azure_hdinsights = true
azure_iot_dps = true
azure_iot_hub = true
azure_key_vault = true
azure_key_vault_managed_hsm = true
azure_kubernetes_service_management = true
azure_machine_learning_workspace = true
azure_managed_disks = true
azure_media_services = true
azure_migrate = true
azure_monitor = true
azure_purview_account = true
azure_purview_studio = true
azure_relay_namespace = true
azure_search_service = true
azure_service_bus_namespace = true
azure_site_recovery = true
azure_sql_database_sqlserver = true
azure_synapse_analytics_dev = true
azure_synapse_analytics_sql = true
azure_synapse_studio = true
azure_web_apps_sites = true
azure_web_apps_static_sites = true
cognitive_services_account = true
microsoft_power_bi = true
signalr = true
signalr_webpubsub = true
storage_account_blob = true
storage_account_file = true
storage_account_queue = true
storage_account_table = true
storage_account_web = true
}
private_link_locations = [
  "northeurope",
```

```
    "westeurope",
  ]
  public_dns_zones                = []
  private_dns_zones               = []
  enable_private_dns_zone_virtual_network_link_on_hubs = true
  enable_private_dns_zone_virtual_network_link_on_spokes = true
  virtual_network_resource_ids_to_link = []
}
}
}

location = var.connectivity_resources_location
tags      = var.connectivity_resources_tags
advanced  = null
}
```

settings.management.tf

```
# Configure the management resources settings.
locals {
  configure_management_resources = {
    settings = {
      log_analytics = {
        enabled = true
        config = {
          retention_in_days                = var.log_retention_in_days
          enable_monitoring_for_vm         = true
          enable_monitoring_for_vmss       = true
          enable_solution_for_agent_health_assessment = true
          enable_solution_for_anti_malware   = true
          enable_solution_for_change_tracking = true
          enable_solution_for_service_map    = false
          enable_solution_for_sql_assessment = false
          enable_solution_for_sql_vulnerability_assessment = false
          enable_solution_for_sql_advanced_threat_detection = false
          enable_solution_for_updates        = true
          enable_solution_for_vm_insights    = true
          enable_sentinel                    = true
        }
      }
    }
  }
  security_center = {
    enabled = true
    config = {
      email_security_contact          = var.security_alerts_email_address
      enable_defender_for_app_services = true
      enable_defender_for_arm          = true
      enable_defender_for_containers   = false
      enable_defender_for_dns          = true
      enable_defender_for_key_vault    = true
      enable_defender_for_oss_databases = true
      enable_defender_for_servers      = true
      enable_defender_for_sql_servers  = true
      enable_defender_for_sql_server_vms = true
      enable_defender_for_storage      = true
    }
  }
}
```

```
    }  
  }  
}  
  
location = var.management_resources_location  
tags     = var.management_resources_tags  
advanced = null  
}  
}
```

Terraform.tf

```
terraform {  
  required_providers {  
    azurerm = {  
      source      = "hashicorp/azurerm"  
      version     = ">= 3.54.0"  
      configuration_aliases = [  
        azurerm.management,  
      ]  
    }  
  }  
}  
  
# Declare a standard provider block using your preferred configuration.  
# This will target the "default" Subscription and be used for the deployment of all "Core  
resources".  
provider "azurerm" {  
  features {}  
}  
  
# Declare an aliased provider block using your preferred configuration.  
# This will be used for the deployment of all "Connectivity resources" to the specified  
`subscription_id`.  
provider "azurerm" {  
  alias            = "management"  
  subscription_id = "bee810ca-7121-40a1-8465-71ec3b0d7449"  
  features {}  
}
```

Variables.tf

```
#VIRTUAL WAN  
variable "root_id" {  
  type    = string  
  default = "myorg"  
}  
  
variable "root_name" {  
  type    = string  
  default = "My Organization"  
}
```



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

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

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

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

variable "log_retention_in_days" {
  type    = number
  default = 50
}

variable "security_alerts_email_address" {
  type    = string
  default = "kuldip.gund@gmail.com" # Replace this value with your own email address.
}

variable "management_resources_location" {
  type    = string
  default = "eastus"
}

variable "management_resources_tags" {
  type = map(string)
  default = {
    demo_type = "deploy_management_resources_custom"
  }
}
```

--TERRAFORM SCREEN--

Terraform plan:

```
# module.enterprise_scale.module.role_assignments_for_policy["/providers/Microsoft.Management/managementGroups/myorg/providers/Microsoft.Authorization/roleDefinitions/b24988ac-6180-42a0-b249-88ac618042a0"]
m_role_assignment_for_policy["/providers/Microsoft.Management/managementGroups/myorg/providers/Microsoft.Authorization/roleDefinitions/b24988ac-6180-42a0-b249-88ac618042a0"]
+ resource "azurerms_role_assignment" "for_policy" {
  + id                        = (known after apply)
  + name                     = "20b87dbc-9b70-5379-ad61-97a3ccecc927"
  + principal_id             = (known after apply)
  + principal_type           = (known after apply)
  + role_definition_id       = "/providers/Microsoft.Authorization/roleDefinitions/b24988ac-6180-42a0-b249-88ac618042a0"
  + role_definition_name     = (known after apply)
  + scope                    = "/providers/Microsoft.Management/managementGroups/myorg"
  + skip_service_principal_aad_check = (known after apply)
}
```

Plan: 313 to add, 0 to change, 0 to destroy.

Terraform apply:

```
gw-westeurope"]: Still creating... [29m0s elapsed]
module.enterprise_scale.azure_rm_vpn_gateway.virtual_wan["/subscriptions/c771a68d-4f8b-4e76-be68-f8dbcd5872f1/resourceGroups/gw-westeurope"]: Creation complete after 29m9s [id=/subscriptions/c771a68d-4f8b-4e76-be68-f8dbcd5872f1/resourceGroups/gw-westeurope]

Apply complete! Resources: 313 added, 0 changed, 0 destroyed.
kuldip [ ~/combined_connectivity_mgmt ]$
```

Policy count	:	342
Resources	:	85
Resource group	:	03
Subscription	:	02

--AZURE SCREENS--

My Organization	Management group	myorg	2
Decommissioned	Management group	myorg-decommissioned	0
Landing Zones	Management group	myorg-landing-zones	0
Platform	Management group	myorg-platform	2
Connectivity	Management group	myorg-connectivity	1
core	Subscription	c771a68d-4f8b-4e76-be68-f8dbcd5872f1	
Identity	Management group	myorg-identity	0
Management	Management group	myorg-management	1
management	Subscription	bee810ca-7121-40a1-8465-71ec3b0d7449	
Sandboxes	Management group	myorg-sandboxes	

Activate Windows
Go to Settings to activate Windows.

management | Resource groups

Subscription

Search

+ Create Edit columns Refresh Export to CSV Open query Assign tags

Filter for any field... Location equals all Add filter

Showing 1 to 2 of 2 records.

No grouping

Name	Subscription	Location
myorg-mgmt	management	East US
test	management	East US

myorg-mgmt | Resource group

Overview

Activity log Access control (IAM) Tags Resource visualizer Events

Settings Deployments Security Policies Properties Locks Cost Management Cost analysis

+ Create Manage view Delete resource group Refresh Export to CSV Open query Assign tags Move Delete Export

Essentials

Resources Recommendations

Filter for any field... Type equals all Location equals all Add filter

Showing 1 to 10 of 10 records. Show hidden types

No grouping

Name	Type	Location
AgentHealthAssessment(myorg-la)	Solution	East US
AntiMalware(myorg-la)	Solution	East US
ChangeTracking(myorg-la)	Solution	East US
ContainerInsights(myorg-la)	Solution	East US
myorg-automation	Automation Account	East US 2
myorg-la	Log Analytics workspace	East US
Security(myorg-la)	Solution	East US
ServiceBusInsights(myorg-la)	Solution	East US

Policy | Assignments

Search < Assign policy Assign initiative Refresh

Overview
Getting started
Compliance
Remediation
Events
Authoring
Definitions
Assignments
Exemptions

Scope: 2 selected Definition type: All definition types Search: Filter by name or ID...

Total Assignments: 19 Initiative Assignments: 10 Policy Assignments: 9

Assignment name ↑↓	Scope ↑↓	Type ↑↓
Configure Azure Activity logs to stream to specified Log Analytics workspace	My Organization	Policy
[Preview]: Deploy Microsoft Defender for Endpoint agent	My Organization	Initiative
Deploy Microsoft Defender for Cloud configuration	My Organization	Initiative
Deny virtual machines and virtual machine scale sets that do not use managed disk	My Organization	Policy
Configure Advanced Threat Protection to be enabled on open-source relational databases	My Organization	Initiative
Unused resources driving cost should be avoided	My Organization	Initiative

Home >

Resource groups

Default Directory (kuid@pundgmai.com@microsoft.com)

+ Create Manage view Refresh Export to CSV Open query Assign tags

Filter for any field... Subscription equals all Location equals all Add filter

Showing 1 to 5 of 5 records. No grouping List view

Name ↑↓	Subscription ↑↓	Location ↑↓
cloud-shell-storage-centralindia	core	Central India
myorg-connectivity	core	East US
myorg-dns	core	East US
myorg-mgmt	management	East US
test	management	East US

myorg-connectivity

Resource group

Search + Create Manage view Delete resource group Refresh Export to CSV Open query Assign

Overview

- Activity log
- Access control (IAM)
- Tags
- Resource visualizer
- Events

Settings

- Deployments
- Security
- Policies
- Properties
- Locks

Cost Management

Essentials

Resources

Filter for any field... Type equals all Location equals all Add filter

Showing 1 to 4 of 4 records. Show hidden types No grouping List view

Name ↑↓	Type ↑↓	Location ↑↓
myorg-ergw-northeurope	Microsoft.Network express route...	North Europe
myorg-fw-hub-northeurope	Firewall	North Europe
myorg-fw-hub-northeurope-policy	Firewall Policy	North Europe
myorg-vwan-eastus	Virtual WAN	East US

--END--