Azure ALZ - 400

(GITHUB)

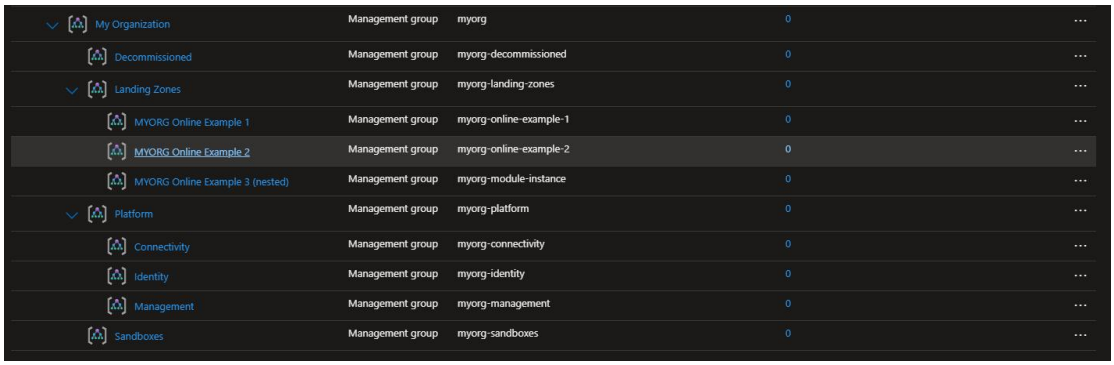
Deploy Using Module Nesting

Terraform Resoruce Count: 237
Total Policy Count: 384

Scope: Deploy Azure landing zone with a nested module instance.

Customization: We did two POCs, firstly we deployed nested module instance with one subscription and then with multiple subscription.

Below is the depiction of the deployment where we can see nested subsets for Landing zone with a single subscription.



Below is the code which is divided into 4 files as mentioned below

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 {}
}
```

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
  library_path   = "${path.root}/lib"

  custom_landing_zones = {
    "${var.root_id}-online-example-1" = {
      display_name               = "${upper(var.root_id)} Online Example 1"
      parent_management_group_id = "${var.root_id}-landing-zones"
      subscription_ids           = []
      archetype_config = {
        archetype_id   = "customer_online"
        parameters     = {}
        access_control = {}
      }
    }
```

```
  custom_landing_zones = {
    "${var.root_id}-online-example-1" = {
      display_name               = "${upper(var.root_id)} Online Example 1"
      parent_management_group_id = "${var.root_id}-landing-zones"
      subscription_ids           = []
      archetype_config = {
        archetype_id   = "customer_online"
        parameters     = {}
        access_control = {}
      }
    }
    "${var.root_id}-online-example-2" = {
      display_name               = "${upper(var.root_id)} Online Example 2"
      parent_management_group_id = "${var.root_id}-landing-zones"
      subscription_ids           = []
      archetype_config = {
        archetype_id = "customer_online"
        parameters = {
          Deny-Resource-Locations = {
            listOfAllowedLocations = ["eastus", ]
          }
          Deny-RSG-Locations = {
            listOfAllowedLocations = ["eastus", ]
          }
        }
        access_control = {}
      }
    }
  }
}

# Enterprise scale nested landing zone instance

module "enterprise_scale_nested_landing_zone" {
  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             = "${var.root_id}-landing-zones"
  root_id                    = var.root_id
  deploy_core_landing_zones = false
  library_path               = "${path.root}/lib"

  custom_landing_zones = {
    "${var.root_id}-module-instance" = {
      display_name               = "${upper(var.root_id)} Online Example 3 (nested)"
      parent_management_group_id = "${var.root_id}-landing-zones"
      subscription_ids           = []
      archetype_config = {
        archetype_id   = "customer_online"
        parameters     = {}
        access_control = {}
      }
    }
  }
```

Variables.tf

```
# Use variables to customize the deployment

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

variable "root_name" {
  type    = string
  default = "My Organization"
}
```

lib/archetype_definition_customer_online.json

```
sarang [ ~/nesting ]$ cat lib/archetype_definition_customer_online.json
{
  "customer_online": {
    "policy_assignments": ["Deny-Resource-Locations", "Deny-RSG-Locations"],
    "policy_definitions": [],
    "policy_set_definitions": [],
    "role_definitions": [],
    "archetype_config": {
      "parameters": {
        "Deny-Resource-Locations": {
          "listOfAllowedLocations": [
            "eastus",
            "eastus2",
            "westus",
            "northcentralus",
            "southcentralus"
          ]
        },
        "Deny-RSG-Locations": {
          "listOfAllowedLocations": [
            "eastus",
            "eastus2",
            "westus",
            "northcentralus",
            "southcentralus"
          ]
        }
      },
      "access_control": {}
    }
  }
}
```

Below is the depiction of the deployment whee we can see nested subsets for Landing zone with multiple subscription.

Main.tf

```
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-c

  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
  library_path   = "${path.root}/lib"

  custom_landing_zones = {
    "${var.root_id}-online-example-1" = {
      display_name               = "${upper(var.root_id)} Online Example 1"
      parent_management_group_id = "${var.root_id}-landing-zones"
      subscription_ids           = ["c771a68d-4f8b-4e76-be68-f8dbcd5872f1",]
      archetype_config = {
        archetype_id   = "customer_online"
        parameters     = {}
        access_control = {}
      }
    }
    "${var.root_id}-online-example-2" = {
      display_name               = "${upper(var.root_id)} Online Example 2"
      parent_management_group_id = "${var.root_id}-landing-zones"
      subscription_ids           = []
      archetype_config = {
        archetype_id = "customer_online"
        parameters = {
          Deny-Resource-Locations = {
            listOfAllowedLocations = ["eastus", ]
          }
          Deny-RSG-Locations = {
            listOfAllowedLocations = ["eastus", ]
          }
        }
        access_control = {}
      }
    }
  }
}
```

```
# Enterprise scale nested landing zone instance

module "enterprise_scale_nested_landing_zone" {
  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            = "${var.root_id}-landing-zones"
  root_id                   = var.root_id
  deploy_core_landing_zones = false
  library_path              = "${path.root}/lib"

  custom_landing_zones = {
    "${var.root_id}-module-instance" = {
      display_name               = "${upper(var.root_id)} Online Example 3 (nested)"
      parent_management_group_id = "${var.root_id}-landing-zones"
      subscription_ids           = ["bee810ca-7121-40a1-8465-71ec3b0d7449",]
      archetype_config = {
        archetype_id   = "customer_online"
        parameters     = {}
        access_control = {}
      }
    }
  }

  depends_on = [
    module.enterprise_scale,
  ]

}
```

Above we can subscription ids mentioned for the custom landing zones.

Deployment Depiction:

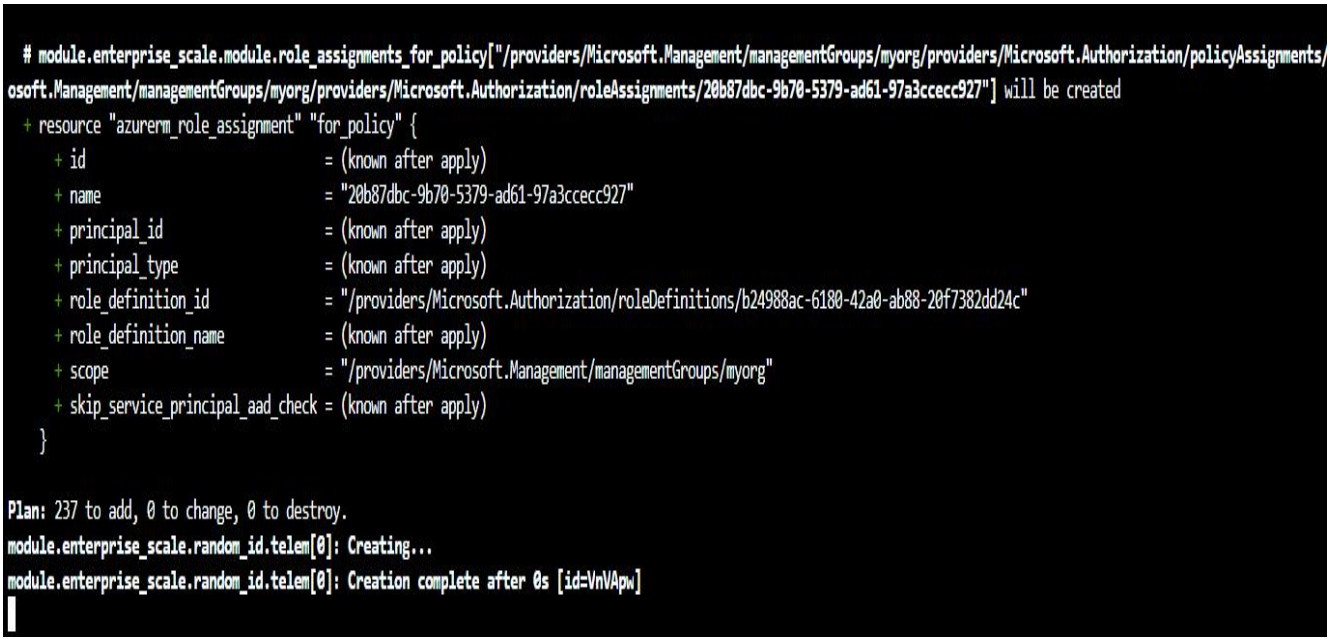
1. From main.tf, we have defined 3 custom landing zone namely myorg online-example-1,2,3. The example 1 and 2 are defined with one module and example 3 is deployed with a separate module.

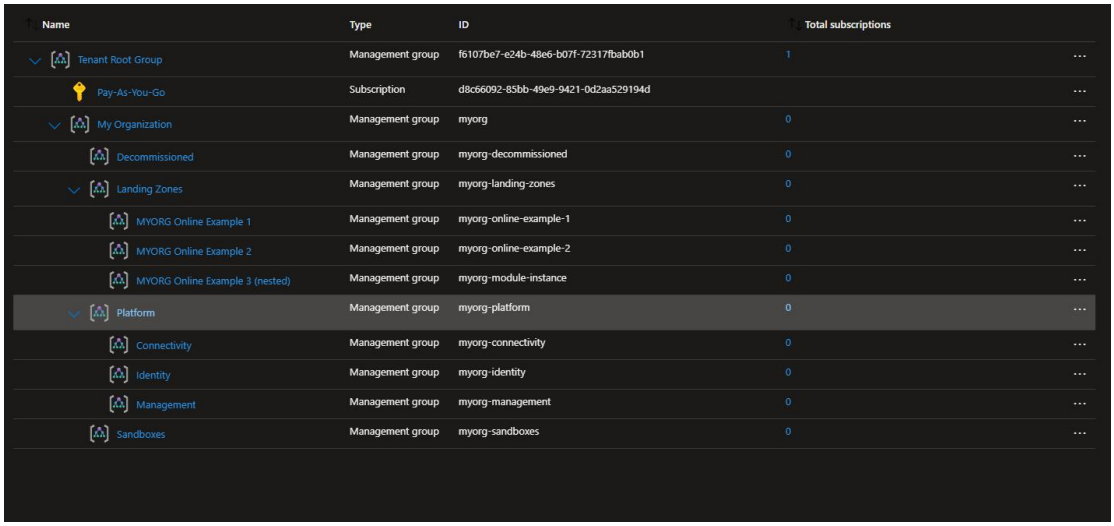
2. On affect of this, we can review creating custom landing zones in Landing Zone Management group.

3. From archetype_definition_customer_online.json, we have set policies for resource group and resource location.

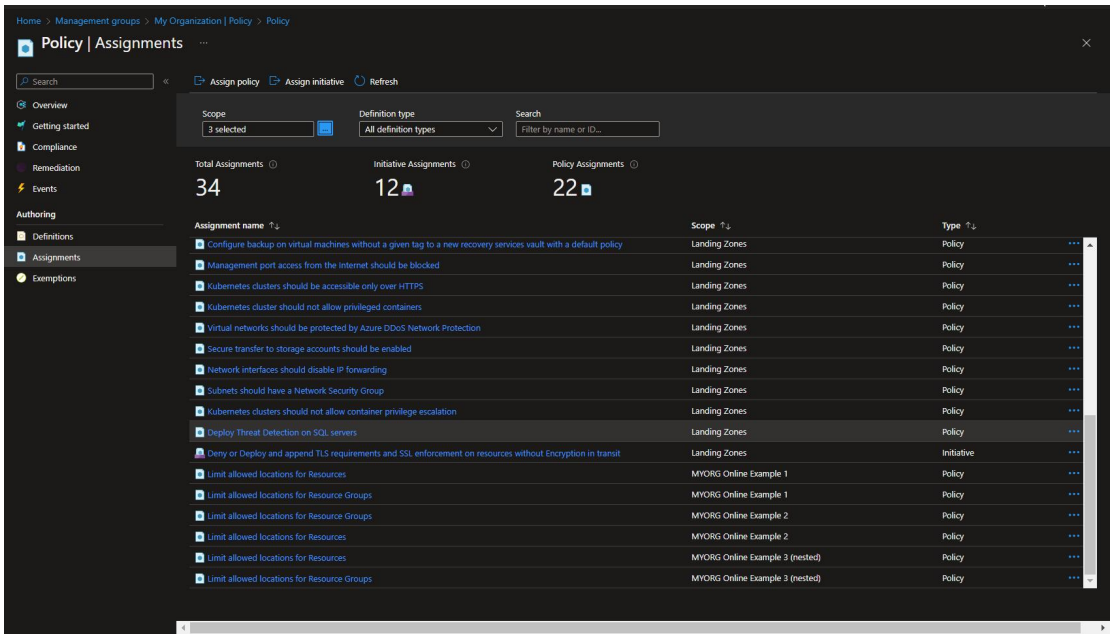
Below are the results

Single Subscription.





Name	Type	ID	Total subscriptions
Tenant Root Group	Management group	f6107be7-e24b-48e6-b07f-72317fbab0b1	1
Pay-As-You-Go	Subscription	d8c66092-85bb-49e9-9421-0d2aa529194d	
My Organization	Management group	myorg	0
Decommissioned	Management group	myorg-decommissioned	0
Landing Zones	Management group	myorg-landing-zones	0
MYORG Online Example 1	Management group	myorg-online-example-1	0
MYORG Online Example 2	Management group	myorg-online-example-2	0
MYORG Online Example 3 (nested)	Management group	myorg-module-instance	0
Platform	Management group	myorg-platform	0
Connectivity	Management group	myorg-connectivity	0
Identity	Management group	myorg-identity	0
Management	Management group	myorg-management	0
Sandboxes	Management group	myorg-sandboxes	0



Home > Management groups > My Organization | Policy > Policy

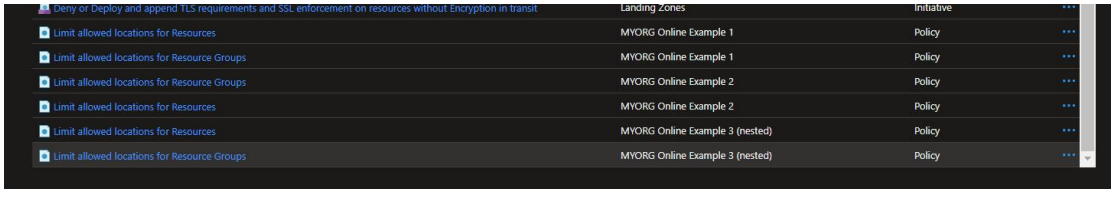
Policy | Assignments

Assign policy | Assign initiative | Refresh

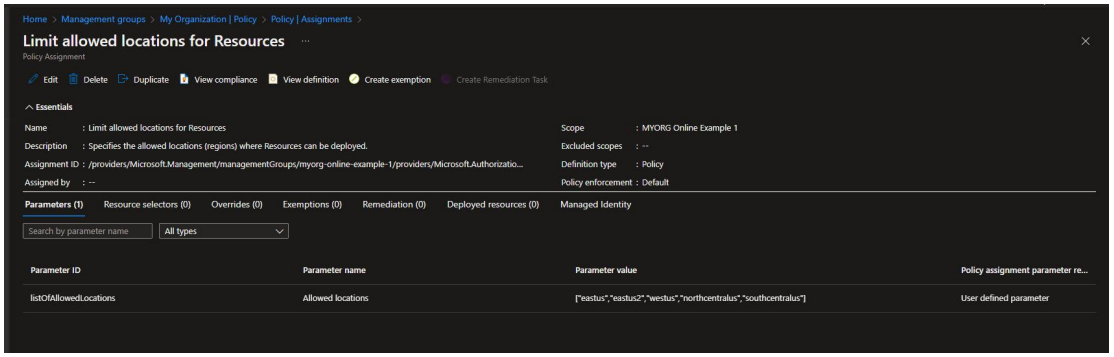
Scope: 3 selected | Definition type: All definition types | Search: Filter by name or ID...

Total Assignments: 34 | Initiative Assignments: 12 | Policy Assignments: 22

Assignment name	Scope	Type
Configure backup on virtual machines without a given tag to a new recovery services vault with a default policy	Landing Zones	Policy
Management port access from the internet should be blocked	Landing Zones	Policy
Kubernetes clusters should be accessible only over HTTPS	Landing Zones	Policy
Kubernetes cluster should not allow privileged containers	Landing Zones	Policy
Virtual networks should be protected by Azure DDoS Network Protection	Landing Zones	Policy
Secure transfer to storage accounts should be enabled	Landing Zones	Policy
Network interfaces should disable IP forwarding	Landing Zones	Policy
Subnets should have a Network Security Group	Landing Zones	Policy
Kubernetes clusters should not allow container privilege escalation	Landing Zones	Policy
Deploy Threat Detection on SQL servers	Landing Zones	Policy
Deny or Deploy and append TLS requirements and SSL enforcement on resources without Encryption in transit	Landing Zones	Initiative
Limit allowed locations for Resources	MYORG Online Example 1	Policy
Limit allowed locations for Resource Groups	MYORG Online Example 1	Policy
Limit allowed locations for Resource Groups	MYORG Online Example 2	Policy
Limit allowed locations for Resources	MYORG Online Example 2	Policy
Limit allowed locations for Resources	MYORG Online Example 3 (nested)	Policy
Limit allowed locations for Resource Groups	MYORG Online Example 3 (nested)	Policy



Deny or Deploy and append TLS requirements and SSL enforcement on resources without Encryption in transit	Landing Zones	Initiative
Limit allowed locations for Resources	MYORG Online Example 1	Policy
Limit allowed locations for Resource Groups	MYORG Online Example 1	Policy
Limit allowed locations for Resource Groups	MYORG Online Example 2	Policy
Limit allowed locations for Resources	MYORG Online Example 2	Policy
Limit allowed locations for Resources	MYORG Online Example 3 (nested)	Policy
Limit allowed locations for Resource Groups	MYORG Online Example 3 (nested)	Policy



Home > Management groups > My Organization | Policy > Policy | Assignments >

Limit allowed locations for Resources

Policy Assignment

Edit | Delete | Duplicate | View compliance | View definition | Create exemption | Create Remediation Task

Essentials

Name : Limit allowed locations for Resources
Description : Specifies the allowed locations (regions) where Resources can be deployed.
Assignment ID : /providers/Microsoft.Management/managementGroups/myorg-online-example-1/providers/Microsoft.Authorizatio...
Assigned by : --
Scope : MYORG Online Example 1
Excluded scopes : --
Definition type : Policy
Policy enforcement : Default

Parameters (1) | Resource selectors (0) | Overrides (0) | Exemptions (0) | Remediation (0) | Deployed resources (0) | Managed Identity

Search by parameter name | All types

Parameter ID	Parameter name	Parameter value	Policy assignment parameter re...
listOfAllowedLocations	Allowed locations	["eastus","eastus2","westus","northcentralus","southcentralus"]	User defined parameter

Multiple Subscriptions.