

Deploy Identity Resources with Custom Settings

**PREPARED BY :
FAIZAN**

In this example, we take the base Deploy Identity resources configuration and make the following changes:

- Add input variable on the root module for enabling/disabling Identity resources
- Add a local variable for `configure_identity_resources` and set custom values for the following:
 - Disable the **DeployIfNotExists** policy used to deploy and configure Azure Backup for Virtual Machines.

Steps:-

Created 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 {}
}
```

Created variables.tf

```
# Use variables to customize the deployment

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

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

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

Created main.tf

The main.tf file contains the `azurerm_client_config` resource, which is used to determine the **Tenant ID** and **Subscription ID** values from your user connection to Azure.

```
# 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 = "<version>" # change this to your desired version, https://www.terraform.io/language/expressions/version-constraints

  default_location = "<YOUR_LOCATION>"

  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_identity_resources = var.deploy_identity_resources
  subscription_id_identity  = data.azurerm_client_config.core.subscription_id
  configure_identity_resources = local.configure_identity_resources
}
```

Created setting/.identity.tf

```
# Configure the identity resources settings.
locals {
  configure_identity_resources = {
    settings = {
      identity = {
        enabled = true
        config = {
          enable_deny_public_ip           = true
          enable_deny_rdp_from_internet   = true
          enable_deny_subnet_without_nsg  = true
          enable_deploy_azure_backup_on_vms = false
        }
      }
    }
  }
}
```

Policy Assignment configuration

Check the following Policy Assignments to see how these have been configured with settings matching your Identity resources configuration set by **configure_identity_resources**:

- Scope = identity
 - Deny-Public-IP
 - Deny-RDP-From-Internet
 - Deny-Subnet-Without-Nsg
 - Deploy-VM-Backup

These Policy Assignments should all be assigned with custom parameter values based on your configuration, with **enforcement_mode** correctly set.

Configure backup on virtual machines without a given tag to a new recovery services vault with a default policy ...

Edit Policy Assignment

Basics Parameters Remediation Non-compliance messages Review + save

Scope

Scope [Learn more about setting the scope](#)

Identity

Exclusions

Optionally select resources to exclude from the policy assignment.

Basics

Policy definition

Configure backup on virtual machines without a given tag to a new recovery services vault with a default policy

Assignment name *

Configure backup on virtual machines without a given tag to a new recovery services vault with a default policy

Assignment ID

/providers/Microsoft.Management/managementGroups/myorg-identity/providers/Microsoft.Authorization/policyAssignments/Deploy-VM-Backup

Description










Enforce backup for all virtual machines by deploying a recovery services vault in the same location and resource group as the virtual machine. Doing this is useful when different application teams in your organization are allocated separate resource groups and need to manage their own backups and restores. You can optionally exclude virtual machines containing a specified tag to control the scope of assignment. See <https://aka.ms/AzureVMAppCentricBackupExcludeTag>.

Policy enforcement

Enabled Disabled

Assigned by

Deployed management group

↑↓ Name	ID	↑↓ Total subscriptions
✓  My Organization	myorg	1
 Decommissioned	myorg-decommissioned	0
 Landing Zones	myorg-landing-zones	0
✓  Platform	myorg-platform	1
 Connectivity	myorg-connectivity	0
✓  Identity	myorg-identity	1
 csu-tf-identity		
 Management	myorg-management	0
 Sandboxes	myorg-sandboxes	0

[+ Add](#)
[↓ Download role assignments](#)
[≡ Edit columns](#)
[↻ Refresh](#)
[✕ Remove](#)
[🗨 Feedback](#)

Check access
 [Role assignments](#)
[Roles](#)
[Deny assignments](#)
[Classic administrators](#)

Type : **All**

Role : **All**

Scope : **All scopes**

Group by : **Role**

17 items (1 Users, 16 Managed Identities)

<input type="checkbox"/>	Name	Type	Role	Scope	Condition
▼	Azure Kubernetes Service Contributor Role				
<input type="checkbox"/>	Deploy-MDFC-Config	App	Azure Kubernetes Service Contributor Role ⓘ	This resource	None
▼	Azure Kubernetes Service Policy Add-on Deployment				
<input type="checkbox"/>	Deploy-MDFC-Config	App	Azure Kubernetes Service Policy Add-on Deployment ⓘ	This resource	None
▼	Contributor				
<input type="checkbox"/>	Deploy-MDEndpoints	App	Contributor ⓘ	This resource	Add
<input type="checkbox"/>	Deploy-MDFC-Config	App	Contributor ⓘ	This resource	Add
<input type="checkbox"/>	Deploy-MDFC-OssDb	App	Contributor ⓘ	This resource	Add
<input type="checkbox"/>	Enforce-ACSB	App	Contributor ⓘ	This resource	Add
▼	Log Analytics Contributor				
<input type="checkbox"/>	Deploy-AzActivity-Log	App	Log Analytics Contributor ⓘ	This resource	Add
<input type="checkbox"/>	Deploy-MDFC-Config	App	Log Analytics Contributor ⓘ	This resource	Add
<input type="checkbox"/>	Deploy-Resource-Diag	App	Log Analytics Contributor ⓘ	This resource	Add
<input type="checkbox"/>	Deploy-VM-Monitoring	App	Log Analytics Contributor ⓘ	This resource	Add
<input type="checkbox"/>	Deploy-VMSS-Monitoring	App	Log Analytics Contributor ⓘ	This resource	Add
▼	Monitoring Contributor				
<input type="checkbox"/>	Deploy-AzActivity-Log	App	Monitoring Contributor ⓘ	This resource	Add
<input type="checkbox"/>	Deploy-Resource-Diag	App	Monitoring Contributor ⓘ	This resource	Add
▼	Owner				
<input type="checkbox"/>	Faizan Momin mominfaizan458_gmail.com...	User	Owner ⓘ	This resource	Add
▼	SQL Security Manager				
<input type="checkbox"/>	Deploy-MDFC-SqlAtp	App	SQL Security Manager ⓘ	This resource	Add
▼	Security Admin				
<input type="checkbox"/>	Deploy-MDFC-Config	App	Security Admin ⓘ	This resource	Add
▼	Virtual Machine Contributor				
<input type="checkbox"/>	Deploy-VMSS-Monitoring	App	Virtual Machine Contributor ⓘ	This resource	Add