

Override Module Role Assignments (Level 300)

By:
Sarfaraz Momin
(Cloud Engineer)

What is HITRUST & HIPAA?

HITRUST is a global security and risk management framework, whereas HIPAA is a U.S. law that governs health industry standards for protecting patient health information.

Strategy

This describes how to deploy your Azure landing zone with a custom configuration, including guidance on how to override the dynamically generated Role Assignments for a specific Policy Assignment with Managed Identity.

We will use the **Deploy-HITRUST-HIPAA** and **Deploy-SQL-Auditing** policy assignments as an example.

On deployment, the module will auto-generate the role assignments necessary for any Policy Assignment when a Managed Identity is required to support policies using **Modify** or **DeployIfNotExists** effects.

We will update the built-in configuration following these steps:

- Create the policy assignment definitions **Deploy-HITRUST-HIPAA** and **Deploy-SQL-Auditing**
- Create the custom archetype definition **customer_online**
- Override the dynamically generated Role Assignments for **Deploy-HITRUST-HIPAA** and **Deploy-SQL-Auditing** Policy Assignments in a custom Landing Zone Management Group.
- Enable the role assignment override with **custom_policy_roles**

Root module:

To make the code easier to maintain when extending your configuration, we recommend splitting the root module into multiple files. For the purpose of this example, we use the following:

- terraform.tf
- variables.tf
- main.tf
- lib/policy_assignments/policy_assignment_dhh_policy_set_definition.json
- lib/policy_assignments/policy_assignment_dsa_policy_set_definition.json
- lib/archetype_definitions/archetype_definition_customer_online.json

--CODE--

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 {}
}
```

variables.tf

```
# Use variables to customize the deployment
```

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

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

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_policy_roles = {
  "/providers/Microsoft.Authorization/policySetDefinitions/a169a624-5599-4385-a696-c8d643089fab" = [
    "/providers/Microsoft.Authorization/roleDefinitions/b24988ac-6180-42a0-ab88-20f7382dd24c",
    "/providers/Microsoft.Authorization/roleDefinitions/4d97b98b-1d4f-4787-a291-c67834d212e7"
  ],
  "/providers/Microsoft.Authorization/policyDefinitions/f4c68484-132f-41f9-9b6d-3e4b1cb55036" = [
    "/providers/Microsoft.Authorization/roleDefinitions/8e3af657-a8ff-443c-a75c-2fe8c4bcb635"
  ]
}

custom_landing_zones = {
  "${var.root_id}-customer-corp" = {
    display_name           = "Custom"
    parent_management_group_id = "${var.root_id}-landing-zones"
    subscription_ids       = []
    archetype_config = {
      archetype_id = "customer_online"
      parameters = {
        Deploy-HITRUST-HIPAA = {
          CertificateThumbprints           = jsonencode("")
          DeployDiagnosticSettingsforNetworkSecurityGroupsrgName = jsonencode("true")
          DeployDiagnosticSettingsforNetworkSecurityGroupsstoragePrefix = jsonencode(var.root_id)
          installedApplicationsOnWindowsVM = jsonencode("")
        },
        Deploy-SQL-Auditing = {
          retentionDays           = jsonencode("10")
          storageAccountsResourceGroup = jsonencode("")
        }
      }
    }
    access_control = {}
  }
}
}

```

Please edit `version = "<VERSION>"` & `default_location = "YOUR_LOCATION"`

lib/policy_assignments/policy_assignment_dhh_policy_set_definition.json

```

{
  "name": "Deploy-HITRUST-HIPAA",
  "type": "Microsoft.Authorization/policyAssignments",
  "apiVersion": "2019-09-01",
  "properties": {
    "description": "This assignment includes audit and virtual machine extension deployment policies that address a subset of HITRUST/HIPAA controls. Additional policies will be added in upcoming releases. For more information, visit https://aka.ms/hipaa-blueprint.",
    "displayName": "Assign policies for HITRUST and HIPAA controls",
    "notScopes": [],
    "parameters": {
      "installedApplicationsOnWindowsVM": {
        "value": null
      },
      "DeployDiagnosticSettingsforNetworkSecurityGroupsstoragePrefix": {
        "value": null
      },
      "DeployDiagnosticSettingsforNetworkSecurityGroupsrgName": {
        "value": null
      },
      "CertificateThumbprints": {
        "value": null
      }
    }
  }
}

```

```

    "policyDefinitionId": "/providers/Microsoft.Authorization/policySetDefinitions/a169a624-5599-4385-a696-c8d643089fab",
    "nonComplianceMessages": [
      {
        "message": "HITRUST/HIPAA controls audit and virtual machine extensions {enforcementMode} be deployed."
      }
    ],
    "scope": "${current_scope_resource_id}"
  },
  "location": "${default_location}",
  "identity": {
    "type": "SystemAssigned"
  }
}

```

lib/policy_assignments/policy_assignment_dsa_policy_set_definition.json

```

{
  "name": "Deploy-SQL-Auditing",
  "type": "Microsoft.Authorization/policyAssignments",
  "apiVersion": "2019-09-01",
  "properties": {
    "description": "Deploy Auditing on SQL servers.",
    "displayName": "Deploy Auditing on SQL servers",
    "notScopes": [],
    "parameters": {
      "retentionDays": {
        "value": null
      },
      "storageAccountsResourceGroup": {
        "value": null
      }
    },
    "policyDefinitionId": "/providers/Microsoft.Authorization/policyDefinitions/f4c68484-132f-41f9-9b6d-3e4b1cb55036",
    "nonComplianceMessages": [
      {
        "message": "SQL auditing {enforcementMode} be configured."
      }
    ],
    "scope": "${current_scope_resource_id}"
  },
  "location": "${default_location}",
  "identity": {
    "type": "SystemAssigned"
  }
}

```

lib/archetype_definitions/archetype_definition_customer_online.json

```

{
  "customer_online": {
    "policy_assignments": ["Deploy-HITRUST-HIPAA", "Deploy-SQL-Auditing"],
    "policy_definitions": [],
    "policy_set_definitions": [],
    "role_definitions": [],
    "archetype_config": {
      "parameters": {},
      "access_control": {}
    }
  }
}

```

Number of Role Definition's in This Deployment.**Count: 31****Number of Policies in This Deployment.****Count: 989****Number of Policy Assignments in This Deployment.****Count: 30****Number of Management Group Resources in This Deployment.****Count: 1****Number of Resources in This Deployment.****Count: 0****Tree Structure:**

```

lib
├── archetype_definitions
│   └── archetype_definition_customer_online.json
├── policy_assignments
│   ├── policy_assignment_dhh_policy_set_definition.json
│   └── policy_assignment_dsa_policy_set_definition.json
├── main.tf
├── terraform.tf
└── variables.tf

3 directories, 6 files

```

Terraform Init:

```

- Finding hashicorp/time versions matching ">= 0.7.0"...
- Installing hashicorp/azurerm v3.56.0...
- Installed hashicorp/azurerm v3.56.0 (signed by HashiCorp)
- Installing hashicorp/random v3.5.1...
- Installed hashicorp/random v3.5.1 (signed by HashiCorp)
- Installing azure/azapi v1.6.0...
- Installed azure/azapi v1.6.0 (signed by a HashiCorp partner, key ID 6F08918DE98478CF)
- Installing hashicorp/time v0.9.1...
- Installed hashicorp/time v0.9.1 (signed by HashiCorp)

Partner and community providers are signed by their developers.
If you'd like to know more about provider signing, you can read about it here:
https://www.terraform.io/docs/cli/plugins/signing.html

Terraform has created a lock file .terraform.lock.hcl to record the provider
selections it made above. Include this file in your version control repository
so that Terraform can guarantee to make the same selections by default when
you run "terraform init" in the future.

Terraform has been successfully initialized!

You may now begin working with Terraform. Try running "terraform plan" to see
any changes that are required for your infrastructure. All Terraform commands
should now work.

If you ever set or change modules or backend configuration for Terraform,
rerun this command to reinitialize your working directory. If you forget, other
commands will detect it and remind you to do so if necessary.
sarfaraz [ ~/test03 ]$

```

Terraform Plan:

```
+ name = "55ffe1be-e389-5d46-9488-8d6915a8b60e"
+ principal_id = (known after apply)
+ principal_type = (known after apply)
+ role_definition_id = "/providers/Microsoft.Authorization/roleDefinitions/92aaf0da-9dab-42b6-94a3-d43ce8d16293"
+ role_definition_name = (known after apply)
+ scope = "/providers/Microsoft.Management/managementGroups/myorg"
+ skip_service_principal_aad_check = (known after apply)
}

# module.enterprise_scale.module.role_assignments_for_policy["/providers/Microsoft.Management/managementGroups/myorg/providers/Microsoft.Authorization/policyAssignments/Enforce-ACSB"].azurerm_role_assignment_for_policy["/providers/Microsoft.Management/managementGroups/myorg/providers/Microsoft.Authorization/roleAssignments/20b87dbc-9b70-5379-ad61-97a3ccec927"] will be created
+ resource "azurerm_role_assignment" "for_policy" {
+ id = (known after apply)
+ name = "20b87dbc-9b70-5379-ad61-97a3ccec927"
+ principal_id = (known after apply)
+ principal_type = (known after apply)
+ role_definition_id = "/providers/Microsoft.Authorization/roleDefinitions/b24988ac-6180-42a0-ab88-20f7382dd24c"
+ role_definition_name = (known after apply)
+ scope = "/providers/Microsoft.Management/managementGroups/myorg"
+ skip_service_principal_aad_check = (known after apply)
}

Plan: 226 to add, 0 to change, 0 to destroy.
```

Note: You didn't use the -out option to save this plan, so Terraform can't guarantee to take exactly these actions if you run "terraform apply" now.

Terraform Apply:

```
module.enterprise_scale.module.role_assignments_for_policy["/providers/Microsoft.Management/managementGroups/myorg/providers/Microsoft.Authorization/policyAssignments/Deploy-WMS-Monitoring"].azurerm_role_assignment_for_policy["/providers/Microsoft.Management/managementGroups/myorg/providers/Microsoft.Authorization/roleAssignments/1e6b635-dc9a-54d5-9bb5-7506132bfff67"]: Creation complete after 23s [id=/providers/Microsoft.Management/managementGroups/myorg/providers/Microsoft.Authorization/roleAssignments/1e6b635-dc9a-54d5-9bb5-7506132bfff67]
module.enterprise_scale.module.role_assignments_for_policy["/providers/Microsoft.Management/managementGroups/myorg-landing-zones/providers/Microsoft.Authorization/policyAssignments/Enforce-TLS-SSL"].azurerm_role_assignment_for_policy["/providers/Microsoft.Management/managementGroups/myorg-landing-zones/providers/Microsoft.Authorization/roleAssignments/a9e21c47-edf5-588d-b83f-419dc94bd522"]: Creation complete after 23s [id=/providers/Microsoft.Management/managementGroups/myorg-landing-zones/providers/Microsoft.Authorization/roleAssignments/a9e21c47-edf5-588d-b83f-419dc94bd522]
module.enterprise_scale.module.role_assignments_for_policy["/providers/Microsoft.Management/managementGroups/myorg-connectivity/providers/Microsoft.Authorization/policyAssignments/Enable-DDoS-VNET"].azurerm_role_assignment_for_policy["/providers/Microsoft.Management/managementGroups/myorg-connectivity/providers/Microsoft.Authorization/roleAssignments/89ee154d-3218-5a7e-a0c5-1fedd34bad78"]: Creation complete after 23s [id=/providers/Microsoft.Management/managementGroups/myorg-connectivity/providers/Microsoft.Authorization/roleAssignments/89ee154d-3218-5a7e-a0c5-1fedd34bad78]
module.enterprise_scale.module.role_assignments_for_policy["/providers/Microsoft.Management/managementGroups/myorg/providers/Microsoft.Authorization/policyAssignments/Deploy-VM-Backup"].azurerm_role_assignment_for_policy["/providers/Microsoft.Management/managementGroups/myorg/providers/Microsoft.Authorization/roleAssignments/f41cafe7-6f85-5086-8ecd-f10c219a9fed"]: Creation complete after 24s [id=/providers/Microsoft.Management/managementGroups/myorg/providers/Microsoft.Authorization/roleAssignments/f41cafe7-6f85-5086-8ecd-f10c219a9fed]
module.enterprise_scale.module.role_assignments_for_policy["/providers/Microsoft.Management/managementGroups/myorg-platform/providers/Microsoft.Authorization/policyAssignments/36853221-c244-5b55-aa34-90b2d32241b0"]: Creation complete after 23s [id=/providers/Microsoft.Management/managementGroups/myorg-platform/providers/Microsoft.Authorization/roleAssignments/36853221-c244-5b55-aa34-90b2d32241b0]
module.enterprise_scale.module.role_assignments_for_policy["/providers/Microsoft.Management/managementGroups/myorg-management/providers/Microsoft.Authorization/policyAssignments/Deploy-Log-Analytics"].azurerm_role_assignment_for_policy["/providers/Microsoft.Management/managementGroups/myorg-management/providers/Microsoft.Authorization/roleAssignments/557bcae8-73b9-58d4-827d-ffc33004ac1a"]: Creation complete after 24s [id=/providers/Microsoft.Management/managementGroups/myorg-management/providers/Microsoft.Authorization/roleAssignments/557bcae8-73b9-58d4-827d-ffc33004ac1a]
module.enterprise_scale.time_sleep.after_azurerm_role_assignment: Creating...
module.enterprise_scale.time_sleep.after_azurerm_role_assignment: Creation complete after 0s [id=2023-05-16T07:05:59Z]

Apply complete! Resources: 41 added, 0 changed, 0 destroyed.
sarfaraz [ ~/test03 ]$
```

Terraform Destroy:

```
}

# module.enterprise_scale.module.role_assignments_for_policy["/providers/Microsoft.Management/managementGroups/myorg/providers/Microsoft.Authorization/policyAssignments/Enforce-ACSB"].azurerm_role_assignment_for_policy["/providers/Microsoft.Management/managementGroups/myorg/providers/Microsoft.Authorization/roleAssignments/20b87dbc-9b70-5379-ad61-97a3ccec927"] will be destroyed
- resource "azurerm_role_assignment" "for_policy" {
- id = "/providers/Microsoft.Management/managementGroups/myorg/providers/Microsoft.Authorization/roleAssignments/20b87dbc-9b70-5379-ad61-97a3ccec927" -> null
- name = "20b87dbc-9b70-5379-ad61-97a3ccec927" -> null
- principal_id = "4627cc78-f1de-4e04-82e8-986b042a7ecf" -> null
- principal_type = "ServicePrincipal" -> null
- role_definition_id = "/providers/Microsoft.Authorization/roleDefinitions/b24988ac-6180-42a0-ab88-20f7382dd24c" -> null
- role_definition_name = "Contributor" -> null
- scope = "/providers/Microsoft.Management/managementGroups/myorg" -> null
}

Plan: 0 to add, 0 to change, 226 to destroy.
```

--SCREEN'S--

Deploy-HITRUST-HIPAA

Home > Management groups > Custom

Custom | Access control (IAM) ...

[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**

Showing a filtered set of results. Total number of role assignments: 31

2 items

Name	Type	Role	Scope	Condition
Contributor				
<input type="checkbox"/> Deploy-HITRUST-HIPAA	App	Contributor ⓘ	This resource	Add
Network Contributor				
<input type="checkbox"/> Deploy-HITRUST-HIPAA	App	Network Contributor ⓘ	This resource	Add

Deploy-SQL-Auditing

Home > Management groups > Custom

Custom | Access control (IAM) ...

[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**

Showing a filtered set of results. Total number of role assignments: 31

1 items

Name	Type	Role	Scope	Condition
Owner				
<input type="checkbox"/> Deploy-SQL-Auditing	App	Owner ⓘ	This resource	Add

--END--