

Azure ALZ - 300

([GITHUB](#))

Expand built in archetype definitions

Resoruce Count: 221

Total Policy Count: 336

Scope: Dynamically modify the built-in archetype definitions using the archetype extensions and archetype exclusions.

Below is the examples of custom parameters that can be added in the archetypes.

```
{
  "es_landing_zones": {
    "policy_assignments": [
      "Deny-IP-Forwarding",
      "Deny-RDP-From-Internet",
      "Deny-Storage-http",
      "Deny-Subnet-Without-Nsg",
      "Deploy-AKS-Policy",
      "Deploy-SQL-DB-Auditing",
      "Deploy-VM-Backup",
      "Deploy-SQL-Security",
      "Deny-Priv-Escalation-AKS",
      "Deny-Priv-Containers-AKS",
      "Deny-http-Ingress-AKS"
    ],
    "policy_definitions": [],
    "policy_set_definitions": [],
    "role_definitions": [],
    "archetype_config": {
      "parameters": {},
      "access_control": {}
    }
  }
}
```

In this POC, we have used two types of settings which consisted of extension of parameters and exclusion of the policy assignment.

1. Here we have assigned the **Deny-Resource-Locations** parameter. For this we added the parameter in the built-in archetype `es_landing_zones`.

```
{
  "extend_es_landing_zones": {
    "policy_assignments": ["Deny-Resource-Locations"],
    "policy_definitions": [],
    "policy_set_definitions": [],
    "role_definitions": [],
    "archetype_config": {
      "parameters": {
        "Deny-Resource-Locations": {
          "listOfAllowedLocations": ["eastus", "westus"]
        }
      },
      "access_control": {}
    }
  }
}
```

2. Here we have assigned 3 custom policies **Deny-Priv-Escalation-AKS**, **Deny-Priv-Containers-AKS** and **Deny-http-Ingress-AKS** from the built-in archetype `es_landing_zones`

```
{
  "exclude_es_landing_zones": {
    "policy_assignments": [
      "Deny-Priv-Escalation-AKS",
      "Deny-Priv-Containers-AKS",
      "Deny-http-Ingress-AKS"
    ],
    "policy_definitions": [],
    "policy_set_definitions": [],
    "role_definitions": [],
    "archetype_config": {
      "parameters": {},
      "access_control": {}
    }
  }
}
```

Deployment Steps:

- We logged into cloud-shell and followed the documentation from git hub and created the below configurations

Main.tf

```
# We strongly recommend using the required_providers block to set the
# Azure Provider source and version being used.

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

provider "azurerm" {
  features {}
}

# You can use the azurerm_client_config data resource to dynamically
# extract connection settings from the provider configuration.

data "azurerm_client_config" "core" {}

# Call the caf-enterprise-scale module directly from the Terraform Registry
# pinning to the latest version

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        = "myorg"
root_name      = "My Organization"
library_path   = "${path.root}/lib"
}
```

archetype_extension_es_landing_zones.tmpl.json











```
sarang [ ~/extend ]$ cat lib/archetype_extension_es_landing_zones.tmpl.json
{
  "extend_es_landing_zones": {
    "policy_assignments": ["Deny-Resource-Locations"],
    "policy_definitions": [],
    "policy_set_definitions": [],
    "role_definitions": [],
    "archetype_config": {
      "parameters": {
        "Deny-Resource-Locations": {
          "listOfAllowedLocations": ["eastus", "westus"]
        }
      },
      "access_control": {}
    }
  }
}
```

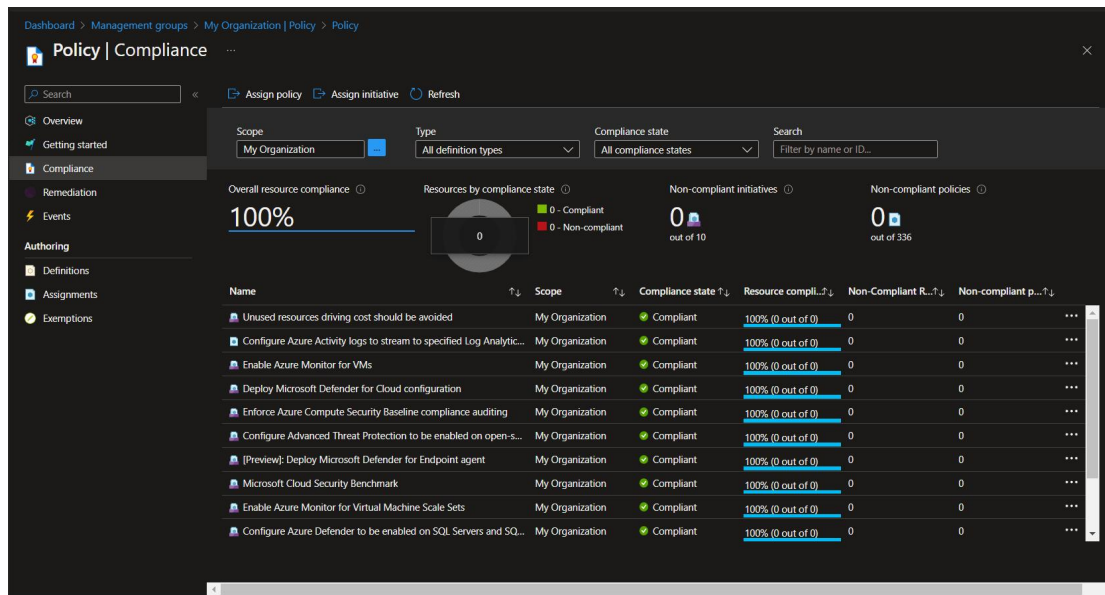
archetype_exclusion_es_landing_zones.tmpl.json

```
sarang [ ~/extend ]$ cat lib/archetype_exclusion_es_landing_zones.tmpl.json
{
  "exclude_es_landing_zones": {
    "policy_assignments": [
      "Deny-Priv-Escalation-AKS",
      "Deny-Priv-Containers-AKS",
      "Deny-http-Ingress-AKS"
    ],
    "policy_definitions": [],
    "policy_set_definitions": [],
    "role_definitions": [],
    "archetype_config": {
      "parameters": {},
      "access_control": {}
    }
  }
}
```

Below are the list of roles and policies that were created and assigned

Showing 1 subscriptions in 9 groups

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	...
 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	...



Name	Definition location	Policies	Type	Definition type
Deploy SQL Database security Alert Policies configuration with email admin ...	My Organization		Custom	Policy
Deploy Diagnostic Settings for Redis Cache to Log Analytics workspace	My Organization		Custom	Policy
Deploy Diagnostic Settings for Network Interfaces to Log Analytics workspace	My Organization		Custom	Policy
SQL servers deploys a specific min TLS version requirement	My Organization		Custom	Policy
Deploy Diagnostic Settings for Log Analytics to Log Analytics workspace	My Organization		Custom	Policy
Deny public IPs for Databricks cluster	My Organization		Custom	Policy
Deny the creation of private DNS	My Organization		Custom	Policy
Subnets should have a Network Security Group	My Organization		Custom	Policy
Deploy Diagnostic Settings for VPN Gateway to Log Analytics workspace	My Organization		Custom	Policy
Deploy Diagnostic Settings for Traffic Manager to Log Analytics workspace	My Organization		Custom	Policy
Deploy Diagnostic Settings for Logic Apps integration service environment t...	My Organization		Custom	Policy
Deploy SQL Database vulnerability Assessments	My Organization		Custom	Policy
Audit the creation of Private Link Private DNS Zones	My Organization		Custom	Policy

Deploy Virtual Network with peering to the hub	My Organization	Custom	Policy
Unused App Service plans driving cost should be avoided	My Organization	Custom	Policy
Deploy Diagnostic Settings for Automation to Log Analytics workspace	My Organization	Custom	Policy
Management port access from the Internet should be blocked	My Organization	Custom	Policy
Deny AKS cluster creation in Azure Machine Learning	My Organization	Custom	Policy
Unused Public IP addresses driving cost should be avoided	My Organization	Custom	Policy
Deploy Diagnostic Settings for Machine Learning workspace to Log Analytic...	My Organization	Custom	Policy
Deploy Diagnostic Settings for Application Gateway to Log Analytics worksp...	My Organization	Custom	Policy
Deploy Diagnostic Settings for Azure Data Explorer Cluster to Log Analytics ...	My Organization	Custom	Policy
Deploy Diagnostic Settings for AVD Application group to Log Analytics work...	My Organization	Custom	Policy
Deploy Diagnostic Settings for SQL Managed Instances to Log Analytics wor...	My Organization	Custom	Policy
Deploy Diagnostic Settings for Container Registry to Log Analytics workspace	My Organization	Custom	Policy
Azure SQL Database should have the minimal TLS version set to the highest ...	My Organization	Custom	Policy

	Name ↑↓	Definition location ↑↓	Policies ↑↓	Type ↑↓	Definition type ↑↓	
Definitions	Management port access from the internet should be blocked	My Organization		Custom	Policy	
Assignments	Deny AKS cluster creation in Azure Machine Learning	My Organization		Custom	Policy	
Exemptions	Unused Public IP addresses driving cost should be avoided	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for Machine Learning workspace to Log Analytics wor...	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for Application Gateway to Log Analytics worksp...	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for Azure Data Explorer Cluster to Log Analytics ...	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for AVD Application group to Log Analytics work...	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for SQL Managed Instances to Log Analytics wor...	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for Container Registry to Log Analytics workspace	My Organization		Custom	Policy	
	Azure SQL Database should have the minimal TLS version set to the highest ...	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for SQL Elastic Pools to Log Analytics workspace	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for Cosmos DB to Log Analytics workspace	My Organization		Custom	Policy	
	Control private endpoint connections to Azure Machine Learning	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for App Service Plan to Log Analytics workspace	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for HDInsight to Log Analytics workspace	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for API Management to Log Analytics workspace	My Organization		Custom	Policy	

	Deploy Diagnostic Settings for Event Grid subscriptions to Log Analytics wor...	My Organization		Custom	Policy	
	Deny public access of Azure Machine Learning clusters via SSH	My Organization		Custom	Policy	
	KeyVault SoftDelete should be enabled	My Organization		Custom	Policy	
	MySQL database servers enforce SSL connections.	My Organization		Custom	Policy	
	Azure Cache for Redis Append and the enforcement that enableNonSslPort i...	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for Database for PostgreSQL to Log Analytics wo...	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for Data Factory to Log Analytics workspace	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for ExpressRoute to Log Analytics workspace	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for Analysis Services to Log Analytics workspace	My Organization		Custom	Policy	
	Azure Database for PostgreSQL server deploy a specific min TLS version req...	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for Azure Function App to Log Analytics worksp...	My Organization		Custom	Policy	
	Unused Disks driving cost should be avoided	My Organization		Custom	Policy	
	Deploy SQL database auditing settings	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for AVD Workspace to Log Analytics workspace	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for Cognitive Services to Log Analytics workspace	My Organization		Custom	Policy	

	Deploy a route table with specific user defined routes	My Organization		Custom	Policy	
	AppService append sites with minimum TLS version to enforce.	My Organization		Custom	Policy	
	Azure Cache for Redis only secure connections should be enabled	My Organization		Custom	Policy	
	Deny non-premium Databricks sku	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for Container Instances to Log Analytics workspa...	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for Database for MySQL to Log Analytics worksp...	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for Data Lake Analytics to Log Analytics workspa...	My Organization		Custom	Policy	
	Deny public access behind vnet to Azure Machine Learning workspace	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for AVD Host Pools to Log Analytics workspace	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for SignalR to Log Analytics workspace	My Organization		Custom	Policy	
	Enforces high business impact Azure Machine Learning Workspaces	My Organization		Custom	Policy	
	Web Application should only be accessible over HTTPS	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for App Service to Log Analytics workspace	My Organization		Custom	Policy	
	Function App should only be accessible over HTTPS	My Organization		Custom	Policy	

	Enforces high business impact Azure Machine Learning Workspaces	My Organization		Custom	Policy	
	Web Application should only be accessible over HTTPS	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for App Service to Log Analytics workspace	My Organization		Custom	Policy	
	Function App should only be accessible over HTTPS	My Organization		Custom	Policy	
	Storage Account set to minimum TLS and Secure transfer should be enabled	My Organization		Custom	Policy	
	No child resources in Automation Account	My Organization		Custom	Policy	
	Deny Databricks workspaces without Vnet injection	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for Event Grid Topic to Log Analytics workspace	My Organization		Custom	Policy	
	Deploy an Azure DDoS Network Protection	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for Firewall to Log Analytics workspace	My Organization		Custom	Policy	
	Deploy Azure Firewall Manager policy in the subscription	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for Virtual Network to Log Analytics workspace	My Organization		Custom	Policy	
	Deploy Diagnostic Settings for Relay to Log Analytics workspace	My Organization		Custom	Policy	
	Deploy a default budget on all subscriptions under the assigned scope	My Organization		Custom	Policy	

Name ↑↓	Definition location ↑↓	Policies ↑↓	Type ↑↓	Definition type ↑↓	Gi
Deploy a default budget on all subscriptions under the assigned scope	My Organization		Custom	Policy	
Application Gateway should be deployed with WAF enabled	My Organization		Custom	Policy	
Deploy Windows Domain Join Extension with keyvault configuration	My Organization		Custom	Policy	
Public network access should be disabled for MariaDB	My Organization		Custom	Policy	
Deny vNet peering to non-approved vNets	My Organization		Custom	Policy	
Deploy Microsoft Defender for Cloud Security Contacts	My Organization		Custom	Policy	
Deploy Diagnostic Settings for Virtual Machines to Log Analytics workspace	My Organization		Custom	Policy	
API App should only be accessible over HTTPS	My Organization		Custom	Policy	
Deploy Diagnostic Settings for Power BI Embedded to Log Analytics worksp...	My Organization		Custom	Policy	
Deploy Diagnostic Settings for Azure Bastion to Log Analytics workspace	My Organization		Custom	Policy	
Deploy Diagnostic Settings for AVD Scaling Plans to Log Analytics workspace	My Organization		Custom	Policy	
Deploy Virtual Machine Auto Shutdown Schedule	My Organization		Custom	Policy	
Azure Machine Learning should have disabled public network access	My Organization		Custom	Policy	
Deploy Diagnostic Settings for VWAN S2S VPN Gateway to Log Analytics w...	My Organization		Custom	Policy	
Deploy Diagnostic Settings for Time Series Insights to Log Analytics worksp...	My Organization		Custom	Policy	

<input type="checkbox"/>	Cognitive Services QnA Make...	Let's you create, edit, import and export a KB. You cannot publish or delete ...	BuiltInRole	AI + Machine Learning	View	...
<input type="checkbox"/>	Cognitive Services QnA Make...	Let's you read and test a KB only.	BuiltInRole	AI + Machine Learning	View	...
<input type="checkbox"/>	Cognitive Services Speech Co...	Full access to Speech projects, including read, write and delete all entities, f...	BuiltInRole	AI + Machine Learning	View	...
<input type="checkbox"/>	Cognitive Services Speech Us...	Access to the real-time speech recognition and batch transcription APIs, rea...	BuiltInRole	AI + Machine Learning	View	...
<input type="checkbox"/>	Cognitive Services User	Lets you read and list keys of Cognitive Services.	BuiltInRole	AI + Machine Learning	View	...
<input type="checkbox"/>	Azure Event Hubs Data Owner	Allows for full access to Azure Event Hubs resources.	BuiltInRole	Analytics	View	...
<input type="checkbox"/>	Azure Event Hubs Data Recei...	Allows receive access to Azure Event Hubs resources.	BuiltInRole	Analytics	View	...
<input type="checkbox"/>	Azure Event Hubs Data Sender	Allows send access to Azure Event Hubs resources.	BuiltInRole	Analytics	View	...
<input type="checkbox"/>	Data Factory Contributor	Create and manage data factories, as well as child resources within them.	BuiltInRole	Analytics	View	...
<input type="checkbox"/>	Data Purger	Can purge analytics data	BuiltInRole	Analytics	View	...
<input type="checkbox"/>	HDInsight Cluster Operator	Lets you read and modify HDInsight cluster configurations.	BuiltInRole	Analytics	View	...
<input type="checkbox"/>	HDInsight Domain Services C...	Can Read, Create, Modify and Delete Domain Services related operations ne...	BuiltInRole	Analytics	View	...
<input type="checkbox"/>	Log Analytics Contributor	Log Analytics Contributor can read all monitoring data and edit monitoring ...	BuiltInRole	Analytics	View	...
<input type="checkbox"/>	Log Analytics Reader	Log Analytics Reader can view and search all monitoring data as well as and...	BuiltInRole	Analytics	View	...
<input type="checkbox"/>	Classic Virtual Machine Contr...	Lets you manage classic virtual machines, but not access to them, and not t...	BuiltInRole	Compute	View	...
<input type="checkbox"/>	Virtual Machine Administrato...	View Virtual Machines in the portal and login as administrator	BuiltInRole	Compute	View	...
<input type="checkbox"/>	Virtual Machine Contributor	Lets you manage virtual machines, but not access to them, and not the virtu...	BuiltInRole	Compute	View	...
<input type="checkbox"/>	Virtual Machine User Login	View Virtual Machines in the portal and login as a regular user.	BuiltInRole	Compute	View	...
<input type="checkbox"/>	acrDelete	acr delete	BuiltInRole	Containers	View	...
<input type="checkbox"/>	acrImageSigner	acr image signer	BuiltInRole	Containers	View	...

<input type="checkbox"/>	Azure Kubernetes Service Clu...	List cluster user credential action.	BuiltInRole	Containers	View	...
<input type="checkbox"/>	Azure Kubernetes Service Co...	Grants access to read and write Azure Kubernetes Service clusters	BuiltInRole	Containers	View	...
<input type="checkbox"/>	Azure Kubernetes Service RB...	Lets you manage all resources under cluster/namespace, except update or d...	BuiltInRole	Containers	View	...
<input type="checkbox"/>	Azure Kubernetes Service RB...	Lets you manage all resources in the cluster.	BuiltInRole	Containers	View	...
<input type="checkbox"/>	Azure Kubernetes Service RB...	Allows read-only access to see most objects in a namespace. It does not all...	BuiltInRole	Containers	View	...
<input type="checkbox"/>	Azure Kubernetes Service RB...	Allows read/write access to most objects in a namespace.This role does not ...	BuiltInRole	Containers	View	...
<input type="checkbox"/>	Cosmos DB Account Reader ...	Can read Azure Cosmos DB Accounts data	BuiltInRole	Databases	View	...
<input type="checkbox"/>	Cosmos DB Operator	Lets you manage Azure Cosmos DB accounts, but not access data in them. ...	BuiltInRole	Databases	View	...
<input type="checkbox"/>	CosmosBackupOperator	Can submit restore request for a Cosmos DB database or a container for an ...	BuiltInRole	Databases	View	...
<input type="checkbox"/>	CosmosRestoreOperator	Can perform restore action for Cosmos DB database account with continuo...	BuiltInRole	Databases	View	...
<input type="checkbox"/>	DocumentDB Account Contr...	Lets you manage DocumentDB accounts, but not access to them.	BuiltInRole	Databases	View	...
<input type="checkbox"/>	Redis Cache Contributor	Lets you manage Redis caches, but not access to them.	BuiltInRole	Databases	View	...
<input type="checkbox"/>	SQL DB Contributor	Lets you manage SQL databases, but not access to them. Also, you can't ma...	BuiltInRole	Databases	View	...
<input type="checkbox"/>	SQL Managed Instance Contr...	Lets you manage SQL Managed Instances and required network configurati...	BuiltInRole	Databases	View	...
<input type="checkbox"/>	SQL Security Manager	Lets you manage the security-related policies of SQL servers and databases...	BuiltInRole	Databases	View	...
<input type="checkbox"/>	SQL Server Contributor	Lets you manage SQL servers and databases, but not access to them, and n...	BuiltInRole	Databases	View	...
<input type="checkbox"/>	DevTest Labs User	Lets you connect, start, restart, and shutdown your virtual machines in your ...	BuiltInRole	Devops	View	...
<input type="checkbox"/>	Lab Creator	Lets you create new labs under your Azure Lab Accounts.	BuiltInRole	Devops	View	...
<input type="checkbox"/>	Owner	Grants full access to manage all resources, including the ability to assign rol...	BuiltInRole	General	View	...
<input type="checkbox"/>	Contributor	Grants full access to manage all resources, but does not allow you to assign ...	BuiltInRole	General	View	...

<input type="checkbox"/>	Microsoft Sentinel Responder	Microsoft Sentinel Responder	BuiltInRole	Security	View	...
<input type="checkbox"/>	Security Admin	Security Admin Role	BuiltInRole	Security	View	...
<input type="checkbox"/>	Security Assessment Contrib...	Lets you push assessments to Security Center	BuiltInRole	Security	View	...
<input type="checkbox"/>	Security Detonation Chambe...	Allowed to publish and modify platforms, workflows and toolsets to Secur...	BuiltInRole	Security	View	...
<input type="checkbox"/>	Security Detonation Chambe...	Allowed to query submission info and files from Security Detonation Chamb...	BuiltInRole	Security	View	...
<input type="checkbox"/>	Security Detonation Chambe...	Allowed to create and manage submissions to Security Detonation Chamber	BuiltInRole	Security	View	...
<input type="checkbox"/>	Security Detonation Chambe...	Allowed to create submissions to Security Detonation Chamber	BuiltInRole	Security	View	...
<input type="checkbox"/>	Security Manager (Legacy)	This is a legacy role. Please use Security Administrator instead	BuiltInRole	Security	View	...
<input type="checkbox"/>	Security Reader	Security Reader Role	BuiltInRole	Security	View	...
<input type="checkbox"/>	Avere Contributor	Can create and manage an Avere vFXT cluster.	BuiltInRole	Storage	View	...
<input type="checkbox"/>	Avere Operator	Used by the Avere vFXT cluster to manage the cluster	BuiltInRole	Storage	View	...
<input type="checkbox"/>	Backup Contributor	Lets you manage backup service,but can't create vaults and give access to o...	BuiltInRole	Storage	View	...
<input type="checkbox"/>	Backup Operator	Lets you manage backup services, except removal of backup, vault creation ...	BuiltInRole	Storage	View	...
<input type="checkbox"/>	Backup Reader	Can view backup services, but can't make changes	BuiltInRole	Storage	View	...
<input type="checkbox"/>	Classic Storage Account Cont...	Lets you manage classic storage accounts, but not access to them.	BuiltInRole	Storage	View	...
<input type="checkbox"/>	Classic Storage Account Key ...	Classic Storage Account Key Operators are allowed to list and regenerate ke...	BuiltInRole	Storage	View	...
<input type="checkbox"/>	Data Box Contributor	Lets you manage everything under Data Box Service except giving access to...	BuiltInRole	Storage	View	...
<input type="checkbox"/>	Data Box Reader	Lets you manage Data Box Service except creating order or editing order de...	BuiltInRole	Storage	View	...
<input type="checkbox"/>	Data Lake Analytics Developer	Lets you submit, monitor, and manage your own jobs but not create or dele...	BuiltInRole	Storage	View	...
<input type="checkbox"/>	Reader and Data Access	Lets you view everything but will not let you delete or create a storage acco...	BuiltInRole	Storage	View	...

<input type="checkbox"/>	Name ↑↓	Description ↑↓
<input type="checkbox"/>	[MYORG] Application-Owners	Contributor role granted for application/operations team at resource group level
<input type="checkbox"/>	[MYORG] Network-Management	Platform-wide global connectivity management: virtual networks, UDRs, NSGs, NVAs, VPN, Azure ExpressRoute, and others
<input type="checkbox"/>	[MYORG] Network-Subnet-Contrib...	Enterprise-scale custom Role Definition. Grants full access to manage Virtual Network subnets, but no other network resources.
<input type="checkbox"/>	[MYORG] Security-Operations	Security Administrator role with a horizontal view across the entire Azure estate and the Azure Key Vault purge policy.
<input type="checkbox"/>	[MYORG] Subscription-Owner	Delegated role for subscription owner generated from subscription Owner role
<input type="checkbox"/>	Owner	Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.
<input type="checkbox"/>	Contributor	Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image .
<input type="checkbox"/>	Reader	View all resources, but does not allow you to make any changes.
<input type="checkbox"/>	Access Review Operator Service R...	Lets you grant Access Review System app permissions to discover and revoke access as needed by the access review process.
<input type="checkbox"/>	AcrDelete	acr delete
<input type="checkbox"/>	AcrImageSigner	acr image signer
<input type="checkbox"/>	AcrPull	acr pull
<input type="checkbox"/>	AcrPush	acr push
<input type="checkbox"/>	AcrQuarantineReader	acr quarantine data reader
<input type="checkbox"/>	AcrQuarantineWriter	acr quarantine data writer
<input type="checkbox"/>	AgFood Platform Sensor Partner C...	Provides contribute access to manage sensor related entities in AgFood Platform Service
<input type="checkbox"/>	AgFood Platform Service Admin	Provides admin access to AgFood Platform Service

<input type="checkbox"/>	Owner	Grants full access to manage all resources, including the ability to...	BuiltInRole	General	View	...
<input type="checkbox"/>	Contributor	Grants full access to manage all resources, but does not allow yo...	BuiltInRole	General	View	...
<input type="checkbox"/>	Reader	View all resources, but does not allow you to make any changes.	BuiltInRole	General	View	...
<input type="checkbox"/>	Access Review Operator Service Role	Lets you grant Access Review System app permissions to discove...	BuiltInRole	None	View	...
<input type="checkbox"/>	AcrDelete	acr delete	BuiltInRole	Containers	View	...
<input type="checkbox"/>	AcrImageSigner	acr image signer	BuiltInRole	Containers	View	...
<input type="checkbox"/>	AcrPull	acr pull	BuiltInRole	Containers	View	...
<input type="checkbox"/>	AcrPush	acr push	BuiltInRole	Containers	View	...
<input type="checkbox"/>	AcrQuarantineReader	acr quarantine data reader	BuiltInRole	Containers	View	...
<input type="checkbox"/>	AcrQuarantineWriter	acr quarantine data writer	BuiltInRole	Containers	View	...
<input type="checkbox"/>	AgFood Platform Sensor Partner Contr...	Provides contribute access to manage sensor related entities in A...	BuiltInRole	None	View	...
<input type="checkbox"/>	AgFood Platform Service Admin	Provides admin access to AgFood Platform Service	BuiltInRole	AI + Machine Learning	View	...
<input type="checkbox"/>	AgFood Platform Service Contributor	Provides contribute access to AgFood Platform Service	BuiltInRole	AI + Machine Learning	View	...
<input type="checkbox"/>	AgFood Platform Service Reader	Provides read access to AgFood Platform Service	BuiltInRole	AI + Machine Learning	View	...
<input type="checkbox"/>	AnyBuild Builder	Basic user role for AnyBuild. This role allows listing of agent infor...	BuiltInRole	None	View	...
<input type="checkbox"/>	API Management Developer Portal Co...	Can customize the developer portal, edit its content, and publish it.	BuiltInRole	None	View	...
<input type="checkbox"/>	API Management Service Contributor	Can manage service and the APIs	BuiltInRole	Integration	View	...
<input type="checkbox"/>	API Management Service Operator Role	Can manage service but not the APIs	BuiltInRole	Integration	View	...
<input type="checkbox"/>	API Management Service Reader Role	Read-only access to service and APIs	BuiltInRole	Integration	View	...

<input type="checkbox"/>	API Management Workspace API Deve...	Has read access to entities in the workspace and read and write a...	BuiltInRole	None	View	...
<input type="checkbox"/>	API Management Workspace API Prod...	Has read access to entities in the workspace and read and write a...	BuiltInRole	None	View	...
<input type="checkbox"/>	API Management Workspace Contribu...	Can manage the workspace and view, but not modify its member...	BuiltInRole	None	View	...
<input type="checkbox"/>	API Management Workspace Reader	Has read-only access to entities in the workspace. This role shoul...	BuiltInRole	None	View	...
<input type="checkbox"/>	App Compliance Automation Administ...	App Compliance Automation Administrator Role	BuiltInRole	None	View	...
<input type="checkbox"/>	App Compliance Automation Reader	App Compliance Automation Reader Role	BuiltInRole	None	View	...
<input type="checkbox"/>	App Configuration Data Owner	Allows full access to App Configuration data.	BuiltInRole	Integration	View	...
<input type="checkbox"/>	App Configuration Data Reader	Allows read access to App Configuration data.	BuiltInRole	Integration	View	...
<input type="checkbox"/>	Application Group Contributor	Contributor of the Application Group.	BuiltInRole	Other	View	...
<input type="checkbox"/>	Application Insights Component Contri...	Can manage Application Insights components	BuiltInRole	Monitor	View	...
<input type="checkbox"/>	Application Insights Snapshot Debugger	Gives user permission to use Application Insights Snapshot Debu...	BuiltInRole	Monitor	View	...
<input type="checkbox"/>	Attestation Contributor	Can read write or delete the attestation provider instance	BuiltInRole	Security	View	...
<input type="checkbox"/>	Attestation Reader	Can read the attestation provider properties	BuiltInRole	Security	View	...
<input type="checkbox"/>	Automation Contributor	Manage azure automation resources and other resources using a...	BuiltInRole	None	View	...
<input type="checkbox"/>	Automation Job Operator	Create and Manage Jobs using Automation Runbooks.	BuiltInRole	Management + Gover...	View	...
<input type="checkbox"/>	Automation Operator	Automation Operators are able to start, stop, suspend, and resu...	BuiltInRole	Management + Gover...	View	...
<input type="checkbox"/>	Automation Runbook Operator	Read Runbook properties - to be able to create Jobs of the runb...	BuiltInRole	Management + Gover...	View	...
<input type="checkbox"/>	Autonomous Development Platform D...	Grants permissions to upload and manage new Autonomous Dev...	BuiltInRole	Preview	View	...
<input type="checkbox"/>	Autonomous Development Platform D...	Grants full access to Autonomous Development Platform data.	BuiltInRole	Preview	View	...
<input type="checkbox"/>	Autonomous Development Platform D...	Grants read access to Autonomous Development Platform data.	BuiltInRole	Preview	View	...
<input type="checkbox"/>	Avere Contributor	Can create and manage an Avere vFXT cluster.	BuiltInRole	Storage	View	...
<input type="checkbox"/>	Avere Operator	Used by the Avere vFXT cluster to manage the cluster	BuiltInRole	Storage	View	...

<input type="checkbox"/>	Azure Extension for SQL Server Deploy...	Microsoft.AzureArcData service role to enable deployment of Az...	BuiltInRole	None	View	...
<input type="checkbox"/>	Azure Front Door Domain Contributor	Can manage Azure Front Door domains, but can't grant access to...	BuiltInRole	None	View	...
<input type="checkbox"/>	Azure Front Door Domain Reader	Can view Azure Front Door domains, but can't make changes.	BuiltInRole	None	View	...
<input type="checkbox"/>	Azure Front Door Secret Contributor	Can manage Azure Front Door secrets, but can't grant access to ...	BuiltInRole	None	View	...
<input type="checkbox"/>	Azure Front Door Secret Reader	Can view Azure Front Door secrets, but can't make changes.	BuiltInRole	None	View	...
<input type="checkbox"/>	Azure Kubernetes Fleet Manager Contr...	Grants access to read and write Azure Kubernetes Fleet Manager ...	BuiltInRole	None	View	...
<input type="checkbox"/>	Azure Kubernetes Fleet Manager RBAC...	This role grants admin access - provides write permissions on mo...	BuiltInRole	None	View	...
<input type="checkbox"/>	Azure Kubernetes Fleet Manager RBAC...	Lets you manage all resources in the fleet manager cluster.	BuiltInRole	None	View	...
<input type="checkbox"/>	Azure Kubernetes Fleet Manager RBAC...	Allows read-only access to see most objects in a namespace. It d...	BuiltInRole	None	View	...
<input type="checkbox"/>	Azure Kubernetes Fleet Manager RBAC...	Allows read/write access to most objects in a namespace.This rol...	BuiltInRole	None	View	...
<input type="checkbox"/>	Azure Kubernetes Service Cluster Admi...	List cluster admin credential action.	BuiltInRole	Containers	View	...
<input type="checkbox"/>	Azure Kubernetes Service Cluster Moni...	List cluster monitoring user credential action.	BuiltInRole	None	View	...
<input type="checkbox"/>	Azure Kubernetes Service Cluster User ...	List cluster user credential action.	BuiltInRole	Containers	View	...
<input type="checkbox"/>	Azure Kubernetes Service Contributor ...	Grants access to read and write Azure Kubernetes Service clusters	BuiltInRole	Containers	View	...
<input type="checkbox"/>	Azure Kubernetes Service Policy Add-o...	Deploy the Azure Policy add-on on Azure Kubernetes Service clus...	BuiltInRole	None	View	...
<input type="checkbox"/>	Azure Kubernetes Service RBAC Admin	Lets you manage all resources under cluster/namespace, except ...	BuiltInRole	Containers	View	...
<input type="checkbox"/>	Azure Kubernetes Service RBAC Cluster...	Lets you manage all resources in the cluster.	BuiltInRole	Containers	View	...
<input type="checkbox"/>	Azure Kubernetes Service RBAC Reader	Allows read-only access to see most objects in a namespace. It d...	BuiltInRole	Containers	View	...
<input type="checkbox"/>	Azure Kubernetes Service RBAC Writer	Allows read/write access to most objects in a namespace.This rol...	BuiltInRole	Containers	View	...
<input type="checkbox"/>	Azure Maps Contributor	Grants access all Azure Maps resource management.	BuiltInRole	None	View	...
<input type="checkbox"/>	Azure Maps Data Contributor	Grants access to read, write, and delete access to map related dat...	BuiltInRole	Web	View	...
<input type="checkbox"/>	Azure Maps Data Reader	Grants access to read map related data from an Azure maps acco...	BuiltInRole	Web	View	...

<input type="checkbox"/>	Tronic Manager Contributor	Lets you manage tronic manager profiles, but does not let you c...	BuiltInRole	Networking	View	...
<input type="checkbox"/>	User Access Administrator	Lets you manage user access to Azure resources.	BuiltInRole	General	View	...
<input type="checkbox"/>	Video Indexer Restricted Viewer	Has access to view and search through all video's insights and tra...	BuiltInRole	None	View	...
<input type="checkbox"/>	Virtual Machine Administrator Login	View Virtual Machines in the portal and login as administrator	BuiltInRole	Compute	View	...
<input type="checkbox"/>	Virtual Machine Contributor	Lets you manage virtual machines, but not access to them, and n...	BuiltInRole	Compute	View	...
<input type="checkbox"/>	Virtual Machine Local User Login	View Virtual Machines in the portal and login as a local user confi...	BuiltInRole	None	View	...
<input type="checkbox"/>	Virtual Machine User Login	View Virtual Machines in the portal and login as a regular user.	BuiltInRole	Compute	View	...
<input type="checkbox"/>	VM Scanner Operator	Role that provides access to disk snapshot for security analysis.	BuiltInRole	None	View	...
<input type="checkbox"/>	Web Plan Contributor	Lets you manage the web plans for websites, but not access to th...	BuiltInRole	Web	View	...
<input type="checkbox"/>	Web PubSub Service Owner	Full access to Azure Web PubSub Service REST APIs	BuiltInRole	Preview	View	...
<input type="checkbox"/>	Web PubSub Service Reader	Read-only access to Azure Web PubSub Service REST APIs	BuiltInRole	Preview	View	...
<input type="checkbox"/>	Website Contributor	Lets you manage websites (not web plans), but not access to them.	BuiltInRole	Web	View	...
<input type="checkbox"/>	Windows Admin Center Administrator ...	Let's you manage the OS of your resource via Windows Admin C...	BuiltInRole	None	View	...
<input type="checkbox"/>	Windows365NetworkInterfaceContribu...	Create NICs and join it to virtual machine in another tenant. This ...	BuiltInRole	None	View	...
<input type="checkbox"/>	Windows365NetworkUser	Read the virtual network informations, and join the virtual networ...	BuiltInRole	None	View	...
<input type="checkbox"/>	Windows365SubscriptionReader	Read subscriptions, images, azure firewalls. This role is used in Wi...	BuiltInRole	None	View	...
<input type="checkbox"/>	Workbook Contributor	Can save shared workbooks.	BuiltInRole	Monitor	View	...
<input type="checkbox"/>	Workbook Reader	Can read workbooks.	BuiltInRole	Monitor	View	...
<input type="checkbox"/>	WorkloadBuilder Migration Agent Role	WorkloadBuilder Migration Agent Role.	BuiltInRole	None	View	...

<input type="checkbox"/>	Site Recovery Reader	Lets you view Site Recovery status but not perform other manage...	BuiltInRole	Management + Gover...	View	...
<input type="checkbox"/>	Spatial Anchors Account Contributor	Lets you manage spatial anchors in your account, but not delete ...	BuiltInRole	Mixed Reality	View	...
<input type="checkbox"/>	Spatial Anchors Account Owner	Lets you manage spatial anchors in your account, including deleti...	BuiltInRole	Mixed Reality	View	...
<input type="checkbox"/>	Spatial Anchors Account Reader	Lets you locate and read properties of spatial anchors in your acc...	BuiltInRole	Mixed Reality	View	...
<input type="checkbox"/>	SQL DB Contributor	Lets you manage SQL databases, but not access to them. Also, yo...	BuiltInRole	Databases	View	...
<input type="checkbox"/>	SQL Managed Instance Contributor	Lets you manage SQL Managed Instances and required network ...	BuiltInRole	Databases	View	...
<input type="checkbox"/>	SQL Security Manager	Lets you manage the security-related policies of SQL servers and ...	BuiltInRole	Databases	View	...
<input type="checkbox"/>	SQL Server Contributor	Lets you manage SQL servers and databases, but not access to th...	BuiltInRole	Databases	View	...
<input type="checkbox"/>	SqlDb Migration Role	Role for SqlDb migration	BuiltInRole	None	View	...
<input type="checkbox"/>	SqlMI Migration Role	Role for SqlMI migration	BuiltInRole	None	View	...
<input type="checkbox"/>	SqlVM Migration Role	Role for SqlVM migration	BuiltInRole	None	View	...
<input type="checkbox"/>	Storage Account Backup Contributor	Lets you perform backup and restore operations using Azure Bac...	BuiltInRole	Storage	View	...
<input type="checkbox"/>	Storage Account Contributor	Lets you manage storage accounts, including accessing storage a...	BuiltInRole	Storage	View	...
<input type="checkbox"/>	Storage Account Key Operator Service ...	Storage Account Key Operators are allowed to list and regenerat...	BuiltInRole	Storage	View	...
<input type="checkbox"/>	Storage Blob Data Contributor	Allows for read, write and delete access to Azure Storage blob co...	BuiltInRole	Storage	View	...
<input type="checkbox"/>	Storage Blob Data Owner	Allows for full access to Azure Storage blob containers and data, i...	BuiltInRole	Storage	View	...
<input type="checkbox"/>	Storage Blob Data Reader	Allows for read access to Azure Storage blob containers and data	BuiltInRole	Storage	View	...
<input type="checkbox"/>	Storage Blob Delegator	Allows for generation of a user delegation key which can be used...	BuiltInRole	Storage	View	...
<input type="checkbox"/>	Storage File Data Privileged Contributor	Customer has read, write, delete and modify NTFS permission acc...	BuiltInRole	None	View	...
<input type="checkbox"/>	Storage File Data Privileged Reader	Customer has read access on Azure Storage file shares.	BuiltInRole	None	View	...
<input type="checkbox"/>	Storage File Data SMB Share Contributor	Allows for read, write, and delete access in Azure Storage file shar...	BuiltInRole	Storage	View	...
<input type="checkbox"/>	Storage File Data SMB Share Elevated ...	Allows for read, write, delete and modify NTFS permission access ...	BuiltInRole	Storage	View	...

<input type="checkbox"/>	Purview role 2 (Deprecated)	Deprecated role.	BuiltInRole	Preview	View	...
<input type="checkbox"/>	Purview role 3 (Deprecated)	Deprecated role.	BuiltInRole	Preview	View	...
<input type="checkbox"/>	Quota Request Operator	Read and create quota requests, get quota request status, and cr...	BuiltInRole	Management + Gover...	View	...
<input type="checkbox"/>	Reader and Data Access	Lets you view everything but will not let you delete or create a st...	BuiltInRole	Storage	View	...
<input type="checkbox"/>	Redis Cache Contributor	Lets you manage Redis caches, but not access to them.	BuiltInRole	Databases	View	...
<input type="checkbox"/>	Remote Rendering Administrator	Provides user with conversion, manage session, rendering and di...	BuiltInRole	Mixed Reality	View	...
<input type="checkbox"/>	Remote Rendering Client	Provides user with manage session, rendering and diagnostics ca...	BuiltInRole	Mixed Reality	View	...
<input type="checkbox"/>	Reservation Purchaser	Lets you purchase reservations	BuiltInRole	Management + Gover...	View	...
<input type="checkbox"/>	Resource Policy Contributor	Users with rights to create/modify resource policy, create support...	BuiltInRole	Management + Gover...	View	...
<input type="checkbox"/>	Role Based Access Control Administrat...	Manage access to Azure resources by assigning roles using Azure...	BuiltInRole	None	View	...
<input type="checkbox"/>	SaaS Hub Contributor	SaaS Hub contributor can manage SaaS Hub resource	BuiltInRole	None	View	...
<input type="checkbox"/>	Scheduled Patching Contributor	Provides access to manage maintenance configurations with mai...	BuiltInRole	None	View	...
<input type="checkbox"/>	Scheduler Job Collections Contributor	Lets you manage Scheduler job collections, but not access to the...	BuiltInRole	Other	View	...
<input type="checkbox"/>	Schema Registry Contributor (Preview)	Read, write, and delete Schema Registry groups and schemas.	BuiltInRole	Preview	View	...
<input type="checkbox"/>	Schema Registry Reader (Preview)	Read and list Schema Registry groups and schemas.	BuiltInRole	Preview	View	...
<input type="checkbox"/>	Search Index Data Contributor	Grants full access to Azure Cognitive Search index data.	BuiltInRole	Web	View	...
<input type="checkbox"/>	Search Index Data Reader	Grants read access to Azure Cognitive Search index data.	BuiltInRole	Web	View	...
<input type="checkbox"/>	Search Service Contributor	Lets you manage Search services, but not access to them.	BuiltInRole	Web	View	...
<input type="checkbox"/>	Security Admin	Security Admin Role	BuiltInRole	Security	View	...
<input type="checkbox"/>	Security Assessment Contributor	Lets you push assessments to Security Center	BuiltInRole	Security	View	...
<input type="checkbox"/>	Security Detonation Chamber Publisher	Allowed to publish and modify platforms, workflows and toolsets...	BuiltInRole	Security	View	...
<input type="checkbox"/>	Security Detonation Chamber Reader	Allowed to query submission info and files from Security Detonat...	BuiltInRole	Security	View	...
<input type="checkbox"/>	Security Detonation Chamber Submissi...	Allowed to create and manage submissions to Security Detonatio...	BuiltInRole	Security	View	...

<input type="checkbox"/>	Managed Application Operator Role	Lets you read and perform actions on Managed Application reso...	BuiltInRole	Management + Gover...	View	...
<input type="checkbox"/>	Managed Applications Reader	Lets you read resources in a managed app and request JIT access.	BuiltInRole	Management + Gover...	View	...
<input type="checkbox"/>	Managed HSM contributor	Lets you manage managed HSM pools, but not access to them.	BuiltInRole	Security	View	...
<input type="checkbox"/>	Managed Identity Contributor	Create, Read, Update, and Delete User Assigned Identity	BuiltInRole	Identity	View	...
<input type="checkbox"/>	Managed Identity Operator	Read and Assign User Assigned Identity	BuiltInRole	Identity	View	...
<input type="checkbox"/>	Managed Services Registration assign...	Managed Services Registration Assignment Delete Role allows th...	BuiltInRole	Management + Gover...	View	...
<input type="checkbox"/>	Management Group Contributor	Management Group Contributor Role	BuiltInRole	Management + Gover...	View	...
<input type="checkbox"/>	Management Group Reader	Management Group Reader Role	BuiltInRole	Management + Gover...	View	...
<input type="checkbox"/>	Media Services Account Administrator	Create, read, modify, and delete Media Services accounts; read-o...	BuiltInRole	Web	View	...
<input type="checkbox"/>	Media Services Live Events Administrat...	Create, read, modify, and delete Live Events, Assets, Asset Filters, ...	BuiltInRole	Web	View	...
<input type="checkbox"/>	Media Services Media Operator	Create, read, modify, and delete Assets, Asset Filters, Streaming L...	BuiltInRole	Web	View	...
<input type="checkbox"/>	Media Services Policy Administrator	Create, read, modify, and delete Account Filters, Streaming Polici...	BuiltInRole	Web	View	...
<input type="checkbox"/>	Media Services Streaming Endpoints A...	Create, read, modify, and delete Streaming Endpoints; read-only ...	BuiltInRole	Web	View	...
<input type="checkbox"/>	Microsoft Sentinel Automation Contrib...	Microsoft Sentinel Automation Contributor	BuiltInRole	Security	View	...
<input type="checkbox"/>	Microsoft Sentinel Contributor	Microsoft Sentinel Contributor	BuiltInRole	Security	View	...
<input type="checkbox"/>	Microsoft Sentinel Playbook Operator	Microsoft Sentinel Playbook Operator	BuiltInRole	None	View	...
<input type="checkbox"/>	Microsoft Sentinel Reader	Microsoft Sentinel Reader	BuiltInRole	Security	View	...
<input type="checkbox"/>	Microsoft Sentinel Responder	Microsoft Sentinel Responder	BuiltInRole	Security	View	...
<input type="checkbox"/>	Microsoft.Kubernetes connected cluste...	Microsoft.Kubernetes connected cluster role.	BuiltInRole	None	View	...
<input type="checkbox"/>	Monitoring Contributor	Can read all monitoring data and update monitoring settings.	BuiltInRole	Monitor	View	...
<input type="checkbox"/>	Monitoring Data Reader	Can access the data in an Azure Monitor Workspace.	BuiltInRole	None	View	...
<input type="checkbox"/>	Monitoring Metrics Publisher	Enables publishing metrics against Azure resources	BuiltInRole	Monitor	View	...

<input type="checkbox"/>	Impact Reporter	Allows access to create/report, read and delete impacts	BuiltInRole	None	View	***
<input type="checkbox"/>	Integration Service Environment Contri...	Lets you manage integration service environments, but not acces...	BuiltInRole	Integration	View	***
<input type="checkbox"/>	Integration Service Environment Devel...	Allows developers to create and update workflows, integration ac...	BuiltInRole	Integration	View	***
<input type="checkbox"/>	Intelligent Systems Account Contributor	Lets you manage Intelligent Systems accounts, but not access to ...	BuiltInRole	Integration	View	***
<input type="checkbox"/>	IoT Hub Data Contributor	Allows for full access to IoT Hub data plane operations.	BuiltInRole	Internet of things	View	***
<input type="checkbox"/>	IoT Hub Data Reader	Allows for full read access to IoT Hub data-plane properties	BuiltInRole	Internet of things	View	***
<input type="checkbox"/>	IoT Hub Registry Contributor	Allows for full access to IoT Hub device registry.	BuiltInRole	Internet of things	View	***
<input type="checkbox"/>	IoT Hub Twin Contributor	Allows for read and write access to all IoT Hub device and modul...	BuiltInRole	Internet of things	View	***
<input type="checkbox"/>	Key Vault Administrator	Perform all data plane operations on a key vault and all objects in...	BuiltInRole	Security	View	***
<input type="checkbox"/>	Key Vault Certificates Officer	Perform any action on the certificates of a key vault, except mana...	BuiltInRole	Security	View	***
<input type="checkbox"/>	Key Vault Contributor	Lets you manage key vaults, but not access to them.	BuiltInRole	Security	View	***
<input type="checkbox"/>	Key Vault Crypto Officer	Perform any action on the keys of a key vault, except manage per...	BuiltInRole	Security	View	***
<input type="checkbox"/>	Key Vault Crypto Service Encryption User	Read metadata of keys and perform wrap/unwrap operations. On...	BuiltInRole	Security	View	***
<input type="checkbox"/>	Key Vault Crypto User	Perform cryptographic operations using keys. Only works for key ...	BuiltInRole	Security	View	***
<input type="checkbox"/>	Key Vault Reader	Read metadata of key vaults and its certificates, keys, and secrets...	BuiltInRole	Security	View	***
<input type="checkbox"/>	Key Vault Secrets Officer	Perform any action on the secrets of a key vault, except manage ...	BuiltInRole	Security	View	***
<input type="checkbox"/>	Key Vault Secrets User	Read secret contents. Only works for key vaults that use the 'Azur...	BuiltInRole	Security	View	***
<input type="checkbox"/>	Knowledge Consumer	Knowledge Read permission to consume Enterprise Graph Knowl...	BuiltInRole	None	View	***
<input type="checkbox"/>	Kubernetes Agentless Operator	Grants Microsoft Defender for Cloud access to Azure Kubernetes ...	BuiltInRole	None	View	***
<input type="checkbox"/>	Kubernetes Cluster - Azure Arc Onboar...	Role definition to authorize any user/service to create connected...	BuiltInRole	Management + Gover...	View	***
<input type="checkbox"/>	Kubernetes Extension Contributor	Can create, update, get, list and delete Kubernetes Extensions, an...	BuiltInRole	Management + Gover...	View	***

<input type="checkbox"/>	Classic Virtual Machine Contributor	Lets you manage classic virtual machines, but not access to them...	BuiltInRole	Compute	View	***
<input type="checkbox"/>	ClearDB MySQL DB Contributor	Lets you manage ClearDB MySQL databases, but not access to th...	BuiltInRole	None	View	***
<input type="checkbox"/>	Code Signing Certificate Profile Signer	Sign files with a certificate profile. This role is in preview and subj...	BuiltInRole	None	View	***
<input type="checkbox"/>	Code Signing Identity Verifier	Manage identity or business verification requests. This role is in p...	BuiltInRole	None	View	***
<input type="checkbox"/>	Cognitive Services Contributor	Lets you create, read, update, delete and manage keys of Cogniti...	BuiltInRole	AI + Machine Learning	View	***
<input type="checkbox"/>	Cognitive Services Custom Vision Cont...	Full access to the project, including the ability to view, create, edi...	BuiltInRole	AI + Machine Learning	View	***
<input type="checkbox"/>	Cognitive Services Custom Vision Depl...	Publish, unpublish or export models. Deployment can view the pr...	BuiltInRole	AI + Machine Learning	View	***
<input type="checkbox"/>	Cognitive Services Custom Vision Labe...	View, edit training images and create, add, remove, or delete the ...	BuiltInRole	AI + Machine Learning	View	***
<input type="checkbox"/>	Cognitive Services Custom Vision Read...	Read-only actions in the project. Readers can't create or update t...	BuiltInRole	AI + Machine Learning	View	***
<input type="checkbox"/>	Cognitive Services Custom Vision Trainer	View, edit projects and train the models, including the ability to p...	BuiltInRole	AI + Machine Learning	View	***
<input type="checkbox"/>	Cognitive Services Data Reader (Previe...	Lets you read Cognitive Services data.	BuiltInRole	Preview	View	***
<input type="checkbox"/>	Cognitive Services Face Recognizer	Lets you perform detect, verify, identify, group, and find similar o...	BuiltInRole	AI + Machine Learning	View	***
<input type="checkbox"/>	Cognitive Services Immersive Reader U...	Provides access to create Immersive Reader sessions and call APIs	BuiltInRole	None	View	***
<input type="checkbox"/>	Cognitive Services Language Owner	Has access to all Read, Test, Write, Deploy and Delete functions u...	BuiltInRole	None	View	***
<input type="checkbox"/>	Cognitive Services Language Reader	Has access to Read and Test functions under Language portal	BuiltInRole	None	View	***
<input type="checkbox"/>	Cognitive Services Language Writer	Has access to all Read, Test, and Write functions under Language ...	BuiltInRole	None	View	***
<input type="checkbox"/>	Cognitive Services LUIS Owner	Has access to all Read, Test, Write, Deploy and Delete functions u...	BuiltInRole	None	View	***
<input type="checkbox"/>	Cognitive Services LUIS Reader	Has access to Read and Test functions under LUIS.	BuiltInRole	None	View	***
<input type="checkbox"/>	Cognitive Services LUIS Writer	Has access to all Read, Test, and Write functions under LUIS	BuiltInRole	None	View	***
<input type="checkbox"/>	Cognitive Services Metrics Advisor Ad...	Full access to the project, including the system level configuration.	BuiltInRole	AI + Machine Learning	View	***
<input type="checkbox"/>	Cognitive Services Metrics Advisor User	Access to the project.	BuiltInRole	AI + Machine Learning	View	***
<input type="checkbox"/>	Cognitive Services OpenAI Contributor	Full access including the ability to fine-tune, deploy and generate...	BuiltInRole	None	View	***
<input type="checkbox"/>	Cognitive Services OpenAI User	Ability to view files, models, deployments. Readers can't make an...	BuiltInRole	None	View	***

RoleAssignmentId	Scope	Display Name	RoleDefinitionName	RoleDefinitionId	ObjectId	ObjectType
3ddf8e6c-77e0-56fe-8272-1de3cfc86b62	/providers/Microsoft.Management/Groups/myorg	Deploy - AzActivity-Log	Monitoring Contributor	/providers/Microsoft.Authorization/roleDefinitions/749f88d5-cbae-40b8-bcfc-e573ddc772fa	d46f61dd-3bb0-4fbf-af91-75bca6710509	ServicePrincipal
bae9bc8f-1fb7-536b-a5d3-352b50b98a56	/providers/Microsoft.Management/Groups/myorg	Deploy - AzActivity-Log	Log Analytics Contributor	/providers/Microsoft.Authorization/roleDefinitions/92aaf0da-9dab-42b6-94a3-d43ce8d16293	d46f61dd-3bb0-4fbf-af91-75bca6710509	ServicePrincipal
aec4006b-6bb1-54ae-86c1-9f37d10f701f	/providers/Microsoft.Management/Groups/myorg	Deploy - MDEndpoint	Contributor	/providers/Microsoft.Authorization/roleDefinitions/b24988ac-6180-42a0-ab88-20f7382dd24c	88d6a30a-9352-428b-b0a5-60f256d9b2e2	ServicePrincipal
84b46374-a84a-5435-b4fa-3e5e8b3436da	/providers/Microsoft.Management/Groups/myorg	Deploy - MDConfig	Log Analytics Contributor	/providers/Microsoft.Authorization/roleDefinitions/92aaf0da-9dab-42b6-94a3-d43ce8d16293	190c4081-bca5-4c1f-9c02-d4758bab6ea7	ServicePrincipal
0bff38e2-2896-5b87-ac56-4939b3acb8fa	/providers/Microsoft.Management/Groups/myorg	Deploy - MDConfig	Contributor	/providers/Microsoft.Authorization/roleDefinitions/b24988ac-6180-42a0-ab88-20f7382dd24c	190c4081-bca5-4c1f-9c02-d4758bab6ea7	ServicePrincipal
aad22f3b-7860-592b-8478-da0539df7fe4	/providers/Microsoft.Management/Groups/myorg	Deploy - MDConfig	Azure Kubernetes Service Policy Add-on Deployment	/providers/Microsoft.Authorization/roleDefinitions/18ed5180-3e48-46fd-8541-4ea054d57064	190c4081-bca5-4c1f-9c02-d4758bab6ea7	ServicePrincipal
3e183228-ff7d-5294-be28-1d3ca0e19cd8	/providers/Microsoft.Management/Groups/myorg	Deploy - MDConfig	Security Admin	/providers/Microsoft.Authorization/roleDefinitions/fb1c8493-542b-48eb-b624-b4c8fea62acd	190c4081-bca5-4c1f-9c02-d4758bab6ea7	ServicePrincipal
d1871679-ef08-5cc9-b620-e50d2ffb2902	/providers/Microsoft.Management/Groups/myorg	Deploy - MDConfig	Azure Kubernetes Service Contributor Role	/providers/Microsoft.Authorization/roleDefinitions/ed7f3fbd-7b88-4dd4-9017-9adb7ce333f8	190c4081-bca5-4c1f-9c02-d4758bab6ea7	ServicePrincipal
28d1bbb2-5a95-576b-85de-98980838dfbd	/providers/Microsoft.Management/Groups/myorg	Deploy - MDConfig-OssDb	Contributor	/providers/Microsoft.Authorization/roleDefinitions/b24988ac-6180-42a0-ab88-20f7382dd24c	539e542d-825d-4cb5-a43f-42e1bd4f7479	ServicePrincipal
5610687b-b15b-5d48-bd61-4408dc349e44	/providers/Microsoft.Management/Groups/myorg	Deploy - MDConfig-SqlAtp	SQL Security Manager	/providers/Microsoft.Authorization/roleDefinitions/056cd41c-7e88-42e1-933e-88ba6a50c9c3	44809f8f-bca6-423c-9e26-7ab88ebbf28	ServicePrincipal
f41cafe7-6f85-5086-8ecd-f10c219a9fed	/providers/Microsoft.Management/Groups/myorg	Deploy - Resource-Diag	Monitoring Contributor	/providers/Microsoft.Authorization/roleDefinitions/749f88d5-cbae-40b8-bcfc-e573ddc772fa	888b69d8-f1e2-4459-bcff-0953f59c9b19	ServicePrincipal
aeccabd7-b572-5fe2-	/providers/Microsoft.Management	Deploy -	Log Analytics Contributor	/providers/Microsoft.Authorization/roleDefinitions	888b69d8-f1e2-4459-	ServicePrincipal

b1ad-659525941097	t/managementGroups/myorg	Resource-Diag		/92aaf0da-9dab-42b6-94a3-d43ce8d16293	bcff-0953f59c9b19	principal
17a099f4-cf89-58a8-b6ca-0a673fbdd4fe	/providers/Microsoft.Management/managementGroups/myorg	Deploy-VM-Monitoring	Log Analytics Contributor	/providers/Microsoft.Authorization/roleDefinitions/92aaf0da-9dab-42b6-94a3-d43ce8d16293	2b076c26-b45e-44be-8ab9-6c6b8d85d7dc	ServicePrincipal
55ffe1be-e389-5d46-9488-8d6915a8b60e	/providers/Microsoft.Management/managementGroups/myorg	Deploy-VMSS-Monitoring	Log Analytics Contributor	/providers/Microsoft.Authorization/roleDefinitions/92aaf0da-9dab-42b6-94a3-d43ce8d16293	4cdac29d-09e4-4292-ae0f-1915174e9741	ServicePrincipal
1e6eb635-dc9a-54d5-9bb5-7506132bff67	/providers/Microsoft.Management/managementGroups/myorg	Deploy-VMSS-Monitoring	Virtual Machine Contributor	/providers/Microsoft.Authorization/roleDefinitions/9980e02c-c2be-4d73-94e8-173b1dc7cf3c	4cdac29d-09e4-4292-ae0f-1915174e9741	ServicePrincipal
20b87dbc-9b70-5379-ad61-97a3ccecc927	/providers/Microsoft.Management/managementGroups/myorg	Enforce-ACSB	Contributor	/providers/Microsoft.Authorization/roleDefinitions/b24988ac-6180-42a0-ab88-20f7382dd24c	fe598c95-d45a-4119-9d12-cd5a35e47f7f	ServicePrincipal