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"
    1,
    "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

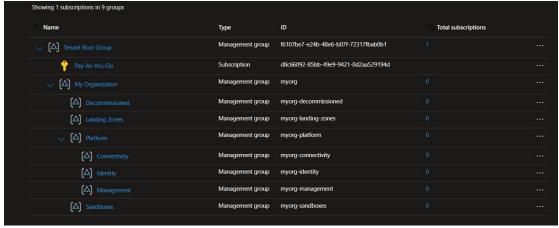
```
# We strongly recommend using the required providers block to set the # Azure Provider source and version being used.
terraform {
   required_providers {
     azurerm = {
  source = "hashicorp/azurerm"
  version = ">= 3.54.0"
provider "azurerm" {
   features {}
# You can use the azurerm_client_config data resource to dynamically
\ensuremath{\text{\#}} 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"
```

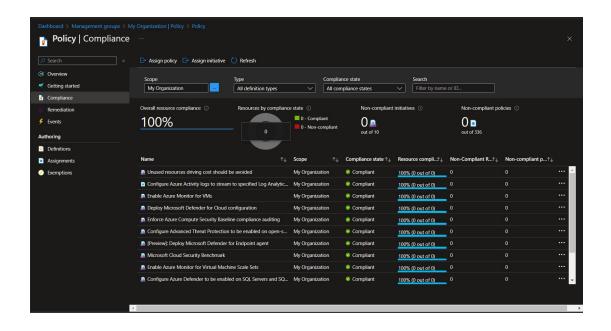
archetype_extension_es_landing_zones.tmpl.json

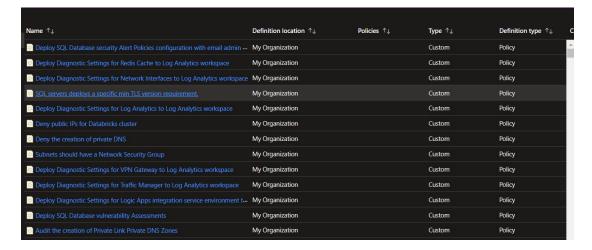
archetype_exclusion_es_landing_zones.tmpl.json

```
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







			N/ - 1/5
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 ↑↓ Ca	
 Definitions 	Management port access from the Internet should be blocked	my Organization		Lustom	POIICY	
 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 Analyt	ic My Organization		Custom	Policy	
	Deploy Diagnostic Settings for Application Gateway to Log Analytics work	sp My Organization		Custom	Policy	
	Deploy Diagnostic Settings for Azure Data Explorer Cluster to Log Analytic	s My Organization		Custom	Policy	
	Deploy Diagnostic Settings for AVD Application group to Log Analytics wo	rk My Organization		Custom	Policy	
	Deploy Diagnostic Settings for SQL Managed Instances to Log Analytics w	or My Organization		Custom	Policy	
	Deploy Diagnostic Settings for Container Registry to Log Analytics worksp	ace My Organization		Custom	Policy	
	Azure SQL Database should have the minimal TLS version set to the higher	st My Organization		Custom	Policy	
	Deploy Diagnostic Settings for SQL Elastic Pools to Log Analytics workspace	e 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	e My Organization		Custom	Policy	
	Deploy Diagnostic Settings for HDInsight to Log Analytics workspace	My Organization		Custom	Policy	
	Deploy Disgnostic Settings for ADI Management to Log Analytics workspa	ne My ∩rnanization		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 enableNonSsIPort 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

- Madig Line Am (Madigue Col. D. C. La Mariero And Sale) (A Madigue Col. And Madigue Col.	CAMP TO STANCE OF		
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

lame ↑↓	Definition location ↑↓	Policies ↑↓	Type ↑↓	Definition type ↑↓	Ci
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	ы
Deploy Windows Domain Join Extension with keyvault configuration	My Organization		Custom	Policy	Ш
Public network access should be disabled for MariaDB	My Organization		Custom	Policy	
Deny vNet peering to non-approved vNets	My Organization		Custom	Policy	Ш
Deploy Microsoft Defender for Cloud Security Contacts	My Organization		Custom	Policy	Ш
Deploy Diagnostic Settings for Virtual Machines to Log Analytics workspace	My Organization		Custom	Policy	Ш
API App should only be accessible over HTTPS	My Organization		Custom	Policy	П
Deploy Diagnostic Settings for Power BI Embedded to Log Analytics worksp	My Organization		Custom	Policy	Ш
Deploy Diagnostic Settings for Azure Bastion to Log Analytics workspace	My Organization		Custom	Policy	П
Deploy Diagnostic Settings for AVD Scaling Plans to Log Analytics workspace	My Organization		Custom	Policy	Ш
Deploy Virtual Machine Auto Shutdown Schedule	My Organization		Custom	Policy	
Azure Machine Learning should have disabled public network access	My Organization		Custom	Policy	Ш
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	

Cognitive Services QnA Make Let's you o	create, edit, import and export a KB. You cannot publish or delete	BuiltInRole	Al + Machine Learning	View	777
Cognitive Services QnA Make Let's you r	ead and test a KB only.	BuiltInRole	Al + Machine Learning		
Cognitive Services Speech Co Full access	to Speech projects, including read, write and delete all entities, f	BuiltInRole	Al + Machine Learning		
Cognitive Services Speech Us Access to	the real-time speech recognition and batch transcription APIs, rea	BuiltInRole	Al + Machine Learning		
Cognitive Services User Lets you re	ead and list keys of Cognitive Services.	BuiltInRole	Al + Machine Learning	View	
Azure Event Hubs Data Owner Allows for	full access to Azure Event Hubs resources.	BuiltInRole	Analytics		
Azure Event Hubs Data Recei Allows rec	eive access to Azure Event Hubs resources.	BuiltInRole	Analytics		
Azure Event Hubs Data Sender Allows sen	nd access to Azure Event Hubs resources.	BuiltInRole	Analytics		
Data Factory Contributor Create and	d manage data factories, as well as child resources within them.	BuiltInRole	Analytics		
Data Purger Can purge	analytics data	BuiltInRole	Analytics		
HDInsight Cluster Operator Lets you re	ead and modify HDInsight cluster configurations.	BuiltInRole	Analytics		
HDInsight Domain Services C Can Read,	Create, Modify and Delete Domain Services related operations ne	BuiltInRole	Analytics		
Log Analytics Contributor Log Analytics	tics Contributor can read all monitoring data and edit monitoring \dots	BuiltInRole	Analytics		
Log Analytics Reader Log Analytics	tics Reader can view and search all monitoring data as well as and	BuiltInRole	Analytics		
Classic Virtual Machine Contr Lets you m	nanage classic virtual machines, but not access to them, and not $t\dots$	BuiltInRole	Compute		
☐ Virtual Machine Administrato View Virtu	al Machines in the portal and login as administrator	BuiltInRole	Compute		
Virtual Machine Contributor Lets you m	nanage virtual machines, but not access to them, and not the virtu	BuiltInRole	Compute		
Virtual Machine User Login View Virtu	al Machines in the portal and login as a regular user.	BuiltInRole	Compute		
AcrDelete acr delete		BuiltInRole	Containers		
AcrlmageSigner acr image	signer	BuiltInRole	Containers		

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

Secure S	Ī	Microsoft Sentinel Responder	Microsoft Sentinel Responder	BuiltInRole	Security		
Security Centrolates Chambos. Allowed to specification and sociates to Security. Security Chambos Chambos. Allowed to serve administration on the face to security Chambos. Security Chambos Chambos. Allowed to serve administration on the face to security Chambos Chambos. Allowed to security Chambos Chambos. Allowed to security Chambos Chambos. Allowed to come chambos chambos. Chamb		Security Admin	Security Admin Role	BuiltInRole	Security		
Searchy (Secretarion Chambors Allowers to page y paintenance per and the front security pelectriston frame Searchy New 11		Security Assessment Contrib	Lets you push assessments to Security Center	BuiltInRole	Security		
Socially Nethination Chambos Allowed to create and invariage administrance to Secretly Discontine Chambos Socially Nethination Chambos Netherold Discontine National Secretify (Netherold Chambos Netherold Discontine National Secretify National Secretific National Secr		Security Detonation Chambe	Allowed to publish and modify platforms, workflows and toolsets to Secu	rit BuiltInRole	Security		
Security Memory (seport) This is injury risk Prises or Control Security Memory (seport) This is injury risk Prises or Security Prises or Security Memory (seport) This is injury risk Prises or Security Prises or Sec	8	Security Detonation Chambe	Allowed to query submission info and files from Security Detonation Cha	nb BuiltInRole	Security		
Security Markinger (Legacy) This is Alegacy role. Preserve Security Administrator instead Buildricke Security Veva 11		Security Detonation Chambe	Allowed to create and manage submissions to Security Detonation Cham	ber BuiltInRole	Security		
Security Nazier Security N		Security Detonation Chambe	Allowed to create submissions to Security Detonation Chamber	BuiltInRole	Security		
Averes Contribution Can create and manage in where sh'll dautes Buildrivide Storage View 1-1	3	Security Manager (Legacy)	This is a legacy role. Please use Security Administrator instead	BuiltInRole	Security		
Acres Operator		Security Reader	Security Reader Role	BuiltInRole	Security		
Biskup Centribution Lest you manage brokers perrocubut can't consider walful and give access to c Builtrivide. Shorage Wee 1-1	3	Avere Contributor	Can create and manage an Avere vFXT cluster.	BuiltInRole	Storage		
Stackup Operator Lets you make you bedook pervices, but cont make changes Stackup Operator Can ver brokep pervices, but cont make changes Stackup Design Pervices Can ver brokep pervices, but cont make changes Stackup Design Pervices Can ver brokep pervices, but cont acres to them. Builthistick Storage Were 11		Avere Operator	Used by the Avere vFXT cluster to manage the cluster	BuiltInRole	Storage		
Bischap Reader Carr view bedrup services, but carn make changes Builtrificide Storage View 11	3	Backup Contributor	Lets you manage backup service, but can't create vaults and give access to	o BuiltInRole	Storage		
Classic Storage Account Core. Lets you manage clearly is closury a account for your force to them. Builtrifule Sorage Vision 11		Backup Operator	Lets you manage backup services, except removal of backup, vault creation	on BuiltInRole	Storage		
Classic Storage Account Ry Classic Storage Account Key Operations are allowed to list and repensate kee Buttirible Scrape View		Backup Reader	Can view backup services, but can't make changes	BuiltInRole	Storage		
Data Box Certifibutor Lets you manage everything under Data Box Service except giving access to Bullimitude Storage View 111		Classic Storage Account Cont	Lets you manage classic storage accounts, but not access to them.	BuiltInRole	Storage		
Data Bion Reader Lets you missage Data Son Service except creating order or editing order do Builtifible Storage View 11 Data Lake Analysis Devologer Lets you size from frontion, and manage your own yields but not create or order Builtifible Storage View 11		Classic Storage Account Key	Classic Storage Account Key Operators are allowed to list and regenerate	ke BuiltInRole	Storage		
Data Lake Analytics Developer Lets you submit, mornitor, and manage your comitée but not create or dele Builthfible Storage View 11		Data Box Contributor	Lets you manage everything under Data Box Service except giving access	to BuiltInRole	Storage		
Name 1; Description 1;		Data Box Reader	Lets you manage Data Box Service except creating order or editing order	de BuiltInRole	Storage		
Name 12 Description 12		Data Lake Analytics Developer	Lets you submit, monitor, and manage your own jobs but not create or d	ele BuiltInRole	Storage		
M/ORIG Application - Owners Contributor role granted for application/operations team at resource group level		Reader and Data Access	Lets you view everything but will not let you delete or create a storage ac	co BuiltInRole	Storage		
M/ORIG Application Owners Contributor role granted for application/operations team at resource group level	-						
M/ORIG Application Owners Contributor role granted for application/operations team at resource group level		□ Name ↑.	Description A				
MPCORG Deterwork Management Retform wide global connectivity management virtual networks, UDIo, NSGs, NNAs, VPN, Azure ExpressRoute, and others MPCORG Deterwork Subrect Contrib. Enterprise scale custom Role Definition, Grants full access to manage Virtual Network subnects, but no other network resources. MPCORG Subscription Owner Delegated role for subscription owner role Owner Grants full access to manage all resources, including the ability to assign roles in Azure RBAC. 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. Access Review Operator Service. Let you grant Access Review System app permissions to discover and revoke access as needed by the access review process. Anti-Delete An	3	_					
MPTORICS) Network Subnect Contribut. Enterprise scale custom Role Definition. Grants full access to manage Virtual Network subnects, but no other network resources. MPTORICS) Subcaription-Owner Desperation	ž	=					
IMPORIG Security Operations Security Administrator role with a horizontal view across the entire Azure estate and the Azure Key Yoult purpe policy.	1	_					
MYCRG Subscription Owner Delegated role for subscription owner generated from subscription Owner role	1					esources.	
Contributor Grants full access to manage all resources, including the ability to assign roles in Azure RBAC. 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. Reader View all resources, but does not allow you to make any changes. 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. Acribule Acribule acr pull Acribulh Acribulh Acribulh Acribulh Acribulh Acribulh Acribulh Apfood Platform Service Platform Acribulh Apfood Platform Service Admin Provides admin access to Apfood Platform Service Contributor Grants full access to manage all resources, including the ability to. Builtinible General View Acribulh Acribulh Acribulh Apfood Platform Service Admin Apfood Platform Service Admin Apfood Platform Service Admin Acribulh Apfood Platform Service Admin Acribulh Acribul	4	=			ire Key Vault purge policy.		
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. Reader View all resources, but does not allow you to make any changes. Access Review Operator Service R. Let you grant Access Review System app permissions to discover and revoke access as needed by the access review process. Archolate acr delete acr delete AcrinageSigner acr image signer Acribush acr push Acribush acr push Acribush acr quarantine data reader Acribush acr quarantine data writer Agricod Platform Service Admin Provides admin access to harinage all resources, including the ability to. Builtinificite General View *** Contributor Grants full access to manage all resources, including the ability to. Builtinificite General View *** Acribated Contributor Grants full access to manage all resources, including the ability to. Builtinificite General View *** Access Review Operator Service Role Lets you grant Access Review System app permissions to discove. Builtinificite General View *** Access Review Operator Service Role Lets you grant Access Review System app permissions to discove. Builtinificite Containers View *** Acribated acr delete acr delete acr delete acr animage signer Builtinificite Containers View *** Acribated acr push acribated acr quarantine data reader Builtinificite Containers View *** Acribated acr push Builtinificite Containers View *** Acribated Containers View *** Acribated Containers View *** Acribated Resource State data writer Builtinificite Containers View *** Acribated Acribated Partier Contrib. Provides contribute access to manage sensor related entities in A. Builtinificite Containers View *** Apricod Platform Service Contributor Provides contribute access to Agricod Platform Service Builtinificite Containers View *** Apricod Platform Service Contributor Provides contribute access to Agricod Platform Service Builtinificite A Harbarine Learning View *** Apricod Platform Service Contributor R		=					
Reader View all resources, but does not allow you to make any changes. 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. AcrDelete acr delete AcrDual acr pual AcrDual acr pual AcrDual acr pual AcrDuah as puah AcrQuarantine-Reader acr quarantine data reader AcrQuarantine-Reader acr quarantine data writer Apf-ood Platform Service Admin Provides admin access to Agricode Platform Service Contributor Grants full access to manage all resources, including the ability to Builtinficile General View *** Contributor Grants full access to manage all resources, but does not allow you. Builtinficile General View *** AcrOuse Review Operator Service Admin AcrOuse acr delete AcrOuse Grants full access to manage all resources, but does not allow you. Builtinficile General View *** Acrouse Review Operator Service Role Let you grant Access Review System app permissions to discove. Builtinficile General View *** AcrOuse Acrouse Review Operator Service Role Let you grant Access Review System app permissions to discove. Builtinficile Containers View *** AcrPull acr public acr public acres to manage singer Builtinficile Containers View *** AcrPull acr public acr public Review Contribute access to manage service to manage service or Builtinficile Containers View *** AcrPula acr public Acropation Provides admin access to manage service or manage service or Builtinficile Containers View *** Apricod Platform Service Admin Provides admin access to Manages service Platform Service Builtinficile A Hachine Learning View *** Apricod Platform Service Rodori Provides access to manage service to trainers Service View *** Apricod Platform Service Rodori Provides access to Agricod Platform Service Builtinficile A Hachine Learning View *** Apricod Platform Service Rodori Provides contribute access to Agricod Platform Service Builtinficile A Hachine Learning View *** Apricod Platform Service Rodori Provides contribute	1						
Accross Review Operator Service R. Acr Delete	2			o assign roles in Azure R	BAC, manage assignments	in Azure Blueprints, o	or share image .
Acribate air delete arr pull a							
AcrimageSigner acr image signer AcrimageSigner	2	_		nd revoke access as need	ded by the access review p	rocess.	
AcrQuarantineReader acr quarantine data reader AcrQuarantineReader acr quarantine data reader AcrQuarantineReader acr quarantine data writer Agfood Platform Sensor Partner C. Provides contribute access to manage sensor related entities in Agfood Platform Service Agfood Platform Service Admin Provides admin access to Magfood Platform Service Contributor Grants full access to manage all resources, including the ability to BuiltinRole General View *** Contributor Grants full access to manage all resources, but does not allow you. BuiltinRole General View *** Reader View all resources, but does not allow you to make any changes. BuiltinRole General View *** Access Review Operator Service Role Lets you grant Access Review System app permissions to discove. BuiltinRole Containers View *** AcrDelete acr delete acr delete BuiltinRole Containers View *** AcrDelete acr pull BuiltinRole Containers View *** AcrQuarantineReader acr pull BuiltinRole Containers View *** AcrQuarantineReader acr quarantine data reader BuiltinRole Containers View *** AcrQuarantineReader acr quarantine data writer BuiltinRole Containers View *** AcrQuarantineWriter acr quarantine data writer BuiltinRole Containers View *** Apfood Platform Service Partner Contri. Provides contribute access to manage sensor related entities in A BuiltinRole Al + Machine Learning View *** Apfood Platform Service Contributor Provides contribute access to Apfood Platform Service BuiltinRole Al + Machine Learning View *** Apfood Platform Service Contributor Provides read access to Apfood Platform Service BuiltinRole None View *** Apfood Platform Service Reader Provides read access to Apfood Platform Service BuiltinRole None View *** Apfood Platform Service Contributor Can causemize the developer portal, edit its content, and publish it. BuiltinRole Integration View *** Apf Management Service Contributor Can manage service and the APIs BuiltinRole Integration View ***							
AcrQuarantineReader acr quarantine data reader AcrQuarantineWriter acr quarantine data writer Agrood Platform Service Admin Carants full access to manage all resources, including the ability to BuiltinRole General View Agrood Platform Service Admin Contributor Grants full access to manage all resources, but does not allow you. BuiltinRole General View Agrood Platform Service New Agrood Platform Service New Agrood Platform Service New Agreement Service Role Lets you grant Access Review System app permissions to discove. BuiltinRole Containers View Agrood Platform Service New Agrood Platform Service Role Lets you grant Access Review System app permissions to discove. BuiltinRole Containers View Acrdinage Signer acr image signer BuiltinRole Containers View Acrdinage Signer acr image signer BuiltinRole Containers View Acrdinage Signer acr pull BuiltinRole Containers View Acrdinage Signer Acrdinage Signer BuiltinRole Containers View Acrdinage Signer Service Signer Signer Service Signer S	ě	_					
AcrQuarantineReader ac quarantine data reader AcrQuarantineWriter acr quarantine data writer AgFood Platform Sensor Partner C Provides admin access to Majood Platform Senvice AgFood Platform Service Admin Provides admin access to AgFood Platform Service Provides admin access to Majood Platform Ser		=					
AcrQuarantineWriter acr quarantine data writer AgFood Platform Service Admin Provides contribute access to manage sensor related entities in AgFood Platform Service Provides admin access to AgFood Platform Service Owner Grants full access to manage all resources, including the ability to BuiltinRole General View *** Contributor Grants full access to manage all resources, but does not allow yo BuiltinRole General View *** Reader View all resources, but does not allow yo BuiltinRole General View *** Access Review Operator Service Role Lets you grant Access Review System app permissions to discove BuiltinRole None View *** AcrDelete acr delete acr delete acr delete BuiltinRole Containers View *** AcrImageSigner acr image signer BuiltinRole Containers View *** AcrQuarantineReader acr quarantine data reader BuiltinRole Containers View *** AcrQuarantineReader acr quarantine data writer BuiltinRole Containers View *** AcrQuarantineWriter acr quarantine data writer BuiltinRole Containers View *** Apfood Platform Service Admin Provides contribute access to manage sensor related entities in A BuiltinRole None View *** Apfood Platform Service Admin Provides admin access to Agfood Platform Service BuiltinRole Al + Machine Learning View *** Apfood Platform Service Contributor Provides contribute access to Agfood Platform Service BuiltinRole Al + Machine Learning View *** Apfood Platform Service Reader Provides contribute access to Agfood Platform Service BuiltinRole Al + Machine Learning View *** Apfood Platform Service Reader Provides contribute access to Agfood Platform Service BuiltinRole Al + Machine Learning View *** Apfood Platform Service Reader Provides contribute access to Agfood Platform Service BuiltinRole Al + Machine Learning View *** Apfood Platform Service Reader Provides contribute access to Agfood Platform Servic	ě	=					
AgFood Platform Service Admin Provides contribute access to manage sensor related entities in AgFood Platform Service AgFood Platform Service Admin Provides admin access to AgFood Platform Service Provides and the APIs Provides Provides		=					
AgFood Platform Service Admin Provides admin access to AgFood Platform Service Owner Grants full access to manage all resources, including the ability to BuiltinRole General View ***	1	=					
Owner Grants full access to manage all resources, including the ability to BuiltinRole General View Contributor Grants full access to manage all resources, but does not allow you. BuiltinRole General View Reader View all resources, but does not allow you to make any changes. BuiltinRole General View Access Review Operator Service Role Lets you grant Access Review System app permissions to discove BuiltinRole None View AcrDelete acr delete BuiltinRole Containers View AcrDelete acr image signer acr image signer BuiltinRole Containers View AcrPull acr pull BuiltinRole Containers View AcrPull acr push BuiltinRole Containers View AcrQuarantineReader acr quarantine data reader BuiltinRole Containers View AcrQuarantineWriter acr quarantine data writer BuiltinRole Containers View Agfood Platform Sensor Partner Contri Provides contribute access to manage sensor related entities in A BuiltinRole None View Agfood Platform Service Admin Provides admin access to Agfood Platform Service BuiltinRole Al + Machine Learning View Agfood Platform Service Contributor Provides read access to Agfood Platform Service BuiltinRole Al + Machine Learning View Apfood Platform Service Reader Provides read access to Agfood Platform Service BuiltinRole None View Apfood Platform Service Reader Provides read access to Agfood Platform Service BuiltinRole None View Apflood Platform Service Contributor Provides read access to Agfood Platform Service BuiltinRole None View Apflood Platform Service Contributor Can customize the developer portal, edit its content, and publish it. BuiltinRole None View Apflood Platforn Service Contributor Can manage service and the APIs BuiltinRole Integration View Apfl Management Service Operator Role Can manage service but not the APIs BuiltinRole Integration View				ood Platform Service			
Contributor Grants full access to manage all resources, but does not allow you. BuiltInRole General View Reader View all resources, but does not allow you to make any changes. BuiltInRole General View Access Review Operator Service Role Lets you grant Access Review System app permissions to discove BuiltInRole None View AcrDeelete acr delete BuiltInRole Containers View AcrDualee AcrPull acr pull BuiltInRole Containers View AcrPull acr pull BuiltInRole Containers View AcrQuarantineReader acr quarantine data reader BuiltInRole Containers View AcrQuarantineReader acr quarantine data reader BuiltInRole Containers View AcrQuarantineWriter acr quarantine data writer BuiltInRole Containers View AgGood Platform Sensor Partner Contri Provides contribute access to manage sensor related entities in A BuiltInRole None View AgGood Platform Service Admin Provides admin access to AgGood Platform Service BuiltInRole Al + Machine Learning View AgGood Platform Service Reader Provides read access to AgGood Platform Service BuiltInRole Al + Machine Learning View ApgGood Platform Service Reader Provides read access to AgGood Platform Service BuiltInRole None View ApgBuild Builder Basic user role for AnyBuild. This role allows listing of agent infor BuiltInRole None View APJ Management Developer Portal Co Can customize the developer portal, edit its content, and publish it. BuiltInRole None View APJ Management Service Contributor Can manage service and the APIs BuiltInRole Integration View		AgFood Platform Service Admir	Provides admin access to AgFood Platform Service				
Contributor Grants full access to manage all resources, but does not allow you. BuiltInRole General View Reader View all resources, but does not allow you to make any changes. BuiltInRole General View Access Review Operator Service Role Lets you grant Access Review System app permissions to discove BuiltInRole None View AcrDeelete acr delete BuiltInRole Containers View AcrDualee AcrPull acr pull BuiltInRole Containers View AcrPull acr pull BuiltInRole Containers View AcrQuarantineReader acr quarantine data reader BuiltInRole Containers View AcrQuarantineReader acr quarantine data reader BuiltInRole Containers View AcrQuarantineWriter acr quarantine data writer BuiltInRole Containers View AgGood Platform Sensor Partner Contri Provides contribute access to manage sensor related entities in A BuiltInRole None View AgGood Platform Service Admin Provides admin access to AgGood Platform Service BuiltInRole Al + Machine Learning View AgGood Platform Service Reader Provides read access to AgGood Platform Service BuiltInRole Al + Machine Learning View ApgGood Platform Service Reader Provides read access to AgGood Platform Service BuiltInRole None View ApgBuild Builder Basic user role for AnyBuild. This role allows listing of agent infor BuiltInRole None View APJ Management Developer Portal Co Can customize the developer portal, edit its content, and publish it. BuiltInRole None View APJ Management Service Contributor Can manage service and the APIs BuiltInRole Integration View					NAME SOMEON AND ADDRESS OF THE PARTY OF THE	W. Branco	
Reader View all resources, but does not allow you to make any changes. BuiltInRole General View Access Review Operator Service Role Lets you grant Access Review System app permissions to discove BuiltInRole None View AcrDelete acr delete BuiltInRole Containers View AcrDelete acr image signer BuiltInRole Containers View AcrPull acr pull BuiltInRole Containers View AcrQuarantineReader acr quarantine data reader BuiltInRole Containers View AcrQuarantineReader acr quarantine data writer BuiltInRole Containers View AcrQuarantineWriter acr quarantine data writer BuiltInRole Containers View AgFood Platform Sensor Partner Contri Provides contribute access to manage sensor related entities in A BuiltInRole None View AgFood Platform Service Admin Provides admin access to AgFood Platform Service BuiltInRole Al + Machine Learning View AgFood Platform Service Contributor Provides contribute access to AgFood Platform Service BuiltInRole Al + Machine Learning View ApFood Platform Service Reader Provides read access to AgFood Platform Service BuiltInRole Al + Machine Learning View ApFood Platform Service Reader Provides read access to AgFood Platform Service BuiltInRole Al + Machine Learning View ApFood Platform Service Reader Provides read access to AgFood Platform Service BuiltInRole None View API Management Developer Portal Co Can customize the developer portal, edit its content, and publish it. BuiltInRole Integration View API Management Service Operator Role Can manage service and the APIs BuiltInRole Integration View							
Access Review Operator Service Role Lets you grant Access Review System app permissions to discove BuiltInRole Containers View AcrDelete AcrDelete acr delete BuiltInRole Containers View AcrImageSigner AcrImageSigner AcrImageSigner AcrImageSigner AcrImageSigner AcrImageSigner AcrImageSigner AcrImageSigner AcrOpull AcrPush AcrPush AcrQuarantineReader AcrQuarantineReader AcrQuarantineReader AcrQuarantineReader AcrQuarantineWriter AcrQuarantineWriter AcrQuarantineWriter AcrQuarantineWriter AcrQuarantineService Admin Provides contribute access to manage sensor related entities in A BuiltInRole None View Agrood Platform Service Admin Provides admin access to Agrood Platform Service BuiltInRole Al + Machine Learning View Agrood Platform Service Contributor Provides contribute access to Agrood Platform Service BuiltInRole Al + Machine Learning View Agrood Platform Service Reader Provides read access to Agrood Platform Service BuiltInRole Al + Machine Learning View Aprode Platform Service Reader Provides read access to Agrood Platform Service BuiltInRole Al + Machine Learning View Aprimagement Developer Portal Co Can customize the developer portal, edit its content, and publish it. BuiltInRole None View Aprimagement Service Contributor Can manage service and the APIs BuiltInRole Integration View Aprimagement Service Operator Role Can manage service but not the APIs BuiltInRole Integration View Aprimagement Service Operator Role Can manage service but not the APIs BuiltInRole Integration View Aprimagement Service Operator Role Can manage service but not the APIs BuiltInRole Integration View Aprimagement Service Operator Role Can manage service but not the APIs BuiltInRole Integration View Aprimagement Service Operator Role Can manage service but not the APIs BuiltInRole Integration View Aprimagement Service Operator Role Can manage service but not the APIs	l						100
AcrDelete acr delete BuiltInRole Containers View AcrDelete acr delete BuiltInRole Containers View AcrDelete acr image signer BuiltInRole Containers View AcrDell acr pull BuiltInRole Containers View AcrDell acr push BuiltInRole Containers View AcrQuarantineReader acr quarantine data reader BuiltInRole Containers View AcrQuarantineWriter acr quarantine data writer BuiltInRole Containers View AgFood Platform Sensor Partner Contri Provides contribute access to manage sensor related entities in A BuiltInRole None View AgFood Platform Service Admin Provides admin access to AgFood Platform Service BuiltInRole Al + Machine Learning View AgFood Platform Service Contributor Provides contribute access to AgFood Platform Service BuiltInRole Al + Machine Learning View AgFood Platform Service Reader Provides read access to AgFood Platform Service BuiltInRole Al + Machine Learning View ApFood Platform Service Reader Provides read access to AgFood Platform Service BuiltInRole None View API Management Developer Portal Co Can customize the developer portal, edit its content, and publish it. BuiltInRole None View API Management Service Contributor Can manage service and the APIs BuiltInRole Integration View							111
AcrImageSigner acr image signer BuiltInRole Containers View AcrPull acr pull BuiltInRole Containers View AcrPush acr push BuiltInRole Containers View AcrQuarantineReader acr quarantine data reader BuiltInRole Containers View AcqQuarantineWriter acr quarantine data writer BuiltInRole Containers View AgFood Platform Sensor Partner Contri Provides contribute access to manage sensor related entities in A BuiltInRole None View AgFood Platform Service Admin Provides admin access to AgFood Platform Service BuiltInRole Al + Machine Learning View AgFood Platform Service Contributor Provides contribute access to AgFood Platform Service BuiltInRole Al + Machine Learning View AgFood Platform Service Reader Provides read access to AgFood Platform Service BuiltInRole Al + Machine Learning View ApFood Platform Service Reader Provides read access to AgFood Platform Service BuiltInRole Al + Machine Learning View API Management Developer Portal Co Can customize the developer portal, edit its content, and publish it. BuiltInRole None View API Management Service Contributor Can manage service and the APIs BuiltInRole Integration View		Ξ					-
AcrPull acr pull BuiltnRole Containers View AcrPush acr push BuiltnRole Containers View AcrQuarantineReader acr quarantine data reader BuiltnRole Containers View AcrQuarantineWriter acr quarantine data writer BuiltnRole Containers View Apfood Platform Sensor Partner Contri Provides contribute access to manage sensor related entities in A BuiltnRole None View Agfood Platform Service Admin Provides admin access to Agfood Platform Service BuiltnRole AI + Machine Learning View Agfood Platform Service Contributor Provides contribute access to Agfood Platform Service BuiltnRole AI + Machine Learning View Agfood Platform Service Reader Provides read access to Agfood Platform Service BuiltnRole AI + Machine Learning View Apfood Platform Service Reader Provides read access to Agfood Platform Service BuiltnRole AI + Machine Learning View Apfl Management Developer Portal Co Can customize the developer portal, edit its content, and publish it. BuiltnRole None View API Management Service Contributor Can manage service and the APIs BuiltnRole Integration View API Management Service Operator Role Can manage service but not the APIs BuiltnRole Integration View							-
AcrQuarantineReader acr quarantine data reader BuiltInRole Containers View AcrQuarantineWriter acr quarantine data writer BuiltInRole Containers View AgFood Platform Sensor Partner Contri Provides contribute access to manage sensor related entities in A BuiltInRole None View AgFood Platform Service Admin Provides admin access to AgFood Platform Service BuiltInRole AI + Machine Learning View AgFood Platform Service Contributor Provides contribute access to AgFood Platform Service BuiltInRole AI + Machine Learning View AgFood Platform Service Reader Provides read access to AgFood Platform Service BuiltInRole AI + Machine Learning View AgFood Platform Service Reader Provides read access to AgFood Platform Service BuiltInRole AI + Machine Learning View API Management Developer Portal Co Can customize the developer portal, edit its content, and publish it. BuiltInRole None View API Management Service Contributor Can manage service and the APIs BuiltInRole Integration View API Management Service Operator Role Can manage service but not the APIs BuiltInRole Integration View	Į						
AcrQuarantineReader acr quarantine data reader BuiltInRole Containers View AcrQuarantineWriter acr quarantine data writer BuiltInRole Containers View AgFood Platform Sensor Partner Contri Provides contribute access to manage sensor related entities in A BuiltInRole None View AgFood Platform Service Admin Provides admin access to AgFood Platform Service BuiltInRole Al + Machine Learning View AgFood Platform Service Contributor Provides contribute access to AgFood Platform Service BuiltInRole Al + Machine Learning View AgFood Platform Service Reader Provides read access to AgFood Platform Service BuiltInRole Al + Machine Learning View AgFood Platform Service Reader Provides read access to AgFood Platform Service BuiltInRole Al + Machine Learning View API Management Developer Portal Co Can customize the developer portal, edit its content, and publish it. BuiltInRole None View API Management Service Contributor Can manage service and the APIs BuiltInRole Integration View API Management Service Operator Role Can manage service but not the APIs BuiltInRole Integration View	l	=					
AcrQuarantineWriter acr quarantine data writer BuiltInRole Containers View AgFood Platform Sensor Partner Contri Provides contribute access to manage sensor related entities in A BuiltInRole None View AgFood Platform Service Admin Provides admin access to AgFood Platform Service BuiltInRole Al + Machine Learning View AgFood Platform Service Contributor Provides contribute access to AgFood Platform Service BuiltInRole Al + Machine Learning View AgFood Platform Service Reader Provides read access to AgFood Platform Service BuiltInRole Al + Machine Learning View ArgFood Platform Service Reader Provides read access to AgFood Platform Service BuiltInRole Al + Machine Learning View ArgFood Platform Service Reader Provides read access to AgFood Platform Service BuiltInRole None View API Management Developer Portal Co Can customize the developer portal, edit its content, and publish it. BuiltInRole None View API Management Service Contributor Can manage service and the APIs BuiltInRole Integration View API Management Service Operator Role Can manage service but not the APIs BuiltInRole Integration View							
AgFood Platform Sensor Partner Contri Provides contribute access to manage sensor related entities in A BuiltInRole None View AgFood Platform Service Admin Provides admin access to AgFood Platform Service BuiltinRole Al + Machine Learning View AgFood Platform Service Contributor Provides contribute access to AgFood Platform Service BuiltinRole Al + Machine Learning View AgFood Platform Service Reader Provides read access to AgFood Platform Service BuiltinRole Al + Machine Learning View ArgBood Platform Service Reader Provides read access to AgFood Platform Service BuiltinRole None View API Management Developer Portal Co Can customize the developer portal, edit its content, and publish it. BuiltinRole None View API Management Service Contributor Can manage service and the APIs BuiltinRole Integration View API Management Service Operator Role Can manage service but not the APIs BuiltinRole Integration View		=					
AgFood Platform Service Admin Provides admin access to AgFood Platform Service BuiltInRole AI + Machine Learning View AgFood Platform Service Contributor Provides contribute access to AgFood Platform Service BuiltInRole AI + Machine Learning View AgFood Platform Service Reader Provides read access to AgFood Platform Service BuiltInRole AI + Machine Learning View AnyBuild Builder Basic user role for AnyBuild. This role allows listing of agent infor BuiltInRole None View API Management Developer Portal Co Can customize the developer portal, edit its content, and publish it. BuiltInRole None View API Management Service Contributor Can manage service and the APIs BuiltInRole Integration View API Management Service Operator Role Can manage service but not the APIs BuiltInRole Integration View							
AgFood Platform Service Contributor Provides contribute access to AgFood Platform Service BuiltInRole Al + Machine Learning View *** AgFood Platform Service Reader Provides read access to AgFood Platform Service BuiltInRole Al + Machine Learning View *** AnyBuild Builder Basic user role for AnyBuild. This role allows listing of agent infor BuiltInRole None View *** API Management Developer Portal Co Can customize the developer portal, edit its content, and publish it. BuiltInRole None View *** API Management Service Contributor Can manage service and the APIs BuiltInRole Integration View *** API Management Service Operator Role Can manage service but not the APIs BuiltInRole Integration View ***							400
ApFood Platform Service Reader Provides read access to ApFood Platform Service BuiltInRole AI + Machine Learning View AryBuild Builder Basic user role for AnyBuild. This role allows listing of agent infor BuiltInRole None View API Management Developer Portal Co Can customize the developer portal, edit its content, and publish it. BuiltInRole None View API Management Service Contributor Can manage service and the APIs BuiltInRole Integration View API Management Service Operator Role Can manage service but not the APIs BuiltInRole Integration View	l						
API Management Service Contributor API Management Service Operator Role API Managemen							
API Management Service Operator Role API Management Service Operator							477
API Management Service Contributor Can manage service and the APIs BuiltInRole Integration View API Management Service Operator Role Can manage service but not the APIs BuiltInRole Integration View							
API Management Service Operator Role Can manage service but not the APIs BuiltInRole Integration View		_					400
		=					
API Management Service Reader Role Read-only access to service and APIs BuiltInRole Integration View		_					
	l	API Management Service Reader F	tole Kead-only access to service and APIs	BuiltInRole	Integration	View	***

API Management Workspace API Deve	Has read access to entities in the workspace and read and write a	. BuiltInRole	None		
API Management Workspace API Prod	Has read access to entities in the workspace and read and write a	. BuiltinRole	None		
API Management Workspace Contribu	Can manage the workspace and view, but not modify its member	BuiltInRole	None		
API Management Workspace Reader	Has read-only access to entities in the workspace. This role shoul	BuiltInRole	None		
App Compliance Automation Administ	App Compliance Automation Administrator Role	BuiltInRole	None		
App Compliance Automation Reader	App Compliance Automation Reader Role	BuiltinRole	None		
App Configuration Data Owner	Allows full access to App Configuration data.	BuiltInRole	Integration		
App Configuration Data Reader	Allows read access to App Configuration data.	BuiltInRole	Integration		
Application Group Contributor	Contributor of the Application Group.	BuiltInRole	Other		
Application Insights Component Contri	Can manage Application Insights components	BuiltInRole	Monitor		
Application Insights Snapshot Debugger	Gives user permission to use Application Insights Snapshot Debu	BuiltInRole	Monitor		
Attestation Contributor	Can read write or delete the attestation provider instance	BuiltInRole	Security		
Attestation Reader	Can read the attestation provider properties	BuiltInRole	Security		
Automation Contributor	Manage azure automation resources and other resources using a	BuiltInRole	None		
Automation Job Operator	Create and Manage Jobs using Automation Runbooks.	BuiltInRole	Management + Gover		
Automation Operator	Automation Operators are able to start, stop, suspend, and resu	BuiltInRole	Management + Gover		
Automation Runbook Operator	Read Runbook properties - to be able to create Jobs of the runb	BuiltInRole	Management + Gover		
Autonomous Development Platform D	Grants permissions to upload and manage new Autonomous Dev	. BuiltInRole	Preview		
	Grants full access to Autonomous Development Platform data.	BuiltInRole	Preview		
	Grants read access to Autonomous Development Platform data.	BuiltInRole	Preview		
Avere Contributor	Can create and manage an Avere vFXT cluster.	BuiltInRole	Storage		
Avere Operator	Used by the Avere vFXT cluster to manage the cluster	BuiltInRole	Storage		
	22.2 Section 2011 (1975) (Intelligence of the Control of the Contr	MONINGS AND THE STREET		10711	
		and water			
Azure Extension for SQL Server Deploy	. Microsoft.AzureArcData service role to enable deployment of Az	BuiltInRole	,	1101	
Azure Extension for SQL Server Deploy Azure Front Door Domain Contributor	. Microsoft.AzureArcData service role to enable deployment of Az Can manage Azure Front Door domains, but can't grant access to		None	View	
_ =		BuiltInRole	None None	View	
Azure Front Door Domain Contributor	Can manage Azure Front Door domains, but can't grant access to	BuiltinRole BuiltinRole	None None None	View View View	•••
Azure Front Door Domain Contributor Azure Front Door Domain Reader	Can manage Azure Front Door domains, but can't grant access to Can view Azure Front Door domains, but can't make changes.	BuiltInRole BuiltInRole BuiltInRole	None None None	View View View View	***
Azure Front Door Domain Contributor Azure Front Door Domain Reader Azure Front Door Secret Contributor Azure Front Door Secret Reader	Can manage Azure Front Door domains, but can't grant access to Can view Azure Front Door domains, but can't make changes. Can manage Azure Front Door secrets, but can't grant access to Can view Azure Front Door secrets, but can't make changes.	BuiltInRole BuiltInRole BuiltInRole BuiltInRole	None None None None	View View View View	
Azure Front Door Domain Contributor Azure Front Door Domain Reader Azure Front Door Secret Contributor Azure Front Door Secret Reader Azure Kubernetes Fleet Manager Contr.	Can manage Azure Front Door domains, but can't grant access to Can view Azure Front Door domains, but can't make changes. Can manage Azure Front Door secrets, but can't grant access to Can view Azure Front Door secrets, but can't make changes.	BuiltinRole BuiltinRole BuiltinRole BuiltinRole BuiltinRole	None None None None None	View View View View View	
Azure Front Door Domain Contributor Azure Front Door Domain Reader Azure Front Door Secret Contributor Azure Front Door Secret Reader Azure Kubernetes Fleet Manager Contr	Can manage Azure Front Door domains, but can't grant access to Can view Azure Front Door domains, but can't make changes. Can manage Azure Front Door secrets, but can't grant access to Can view Azure Front Door secrets, but can't make changes. Grants access to read and write Azure Kubernetes Fleet Manager	BuittinRole BuittinRole BuittinRole BuittinRole BuittinRole BuittinRole	None None None None None None None None	View View View View View View View View	
Azure Front Door Domain Contributor Azure Front Door Domain Reader Azure Front Door Secret Contributor Azure Front Door Secret Reader Azure Kubernetes Fleet Manager Contr Azure Kubernetes Fleet Manager RBAC	Can manage Azure Front Door domains, but can't grant access to Can view Azure Front Door domains, but can't grant access to Can manage Azure Front Door secrets, but can't grant access to Can view Azure Front Door secrets, but can't make changes. Grants access to read and write Azure Kubernetes Fleet Manager This role grants admin access - provides write permissions on mo	BuiltinRole BuiltinRole BuiltinRole BuiltinRole BuiltinRole BuiltinRole BuiltinRole BuiltinRole	None None None None None None None None	View View View View View View View View	
Azure Front Door Domain Contributor Azure Front Door Domain Reader Azure Front Door Secret Contributor Azure Front Door Secret Reader Azure Kubernetes Fleet Manager Contr. Azure Kubernetes Fleet Manager RBAC. Azure Kubernetes Fleet Manager RBAC. Azure Kubernetes Fleet Manager RBAC.	Can manage Azure Front Door domains, but can't grant access to Can view Azure Front Door domains, but can't make changes. Can manage Azure Front Door secrets, but can't grant access to Can view Azure Front Door secrets, but can't make changes. Grants access to read and write Azure Kubernetes Fleet Manager This role grants admin access - provides write permissions on mo Lets you manage all resources in the fleet manager cluster.	BuiltinRole BuiltinRole BuiltinRole BuiltinRole BuiltinRole BuiltinRole BuiltinRole BuiltinRole BuiltinRole	None None None None None None None None	View View View View View View View View	
Azure Front Door Domain Contributor Azure Front Door Domain Reader Azure Front Door Secret Contributor Azure Front Door Secret Reader Azure Kubernetes Fleet Manager Contr. Azure Kubernetes Fleet Manager RBAC. Azure Kubernetes Fleet Manager RBAC. Azure Kubernetes Fleet Manager RBAC.	Can manage Azure Front Door domains, but can't grant access to Can view Azure Front Door domains, but can't make changes. Can manage Azure Front Door secrets, but can't grant access to Can view Azure Front Door secrets, but can't make changes. Grants access to read and write Azure Kubernetes Fleet Manager This role grants admin access - provides write permissions on mo Lets you manage all resources in the fleet manager cluster. Allows read-only access to see most objects in a namespace. It d Allows read/write access to most objects in a namespace. This rol	BuiltinRole	None None None None None None None None	View View View View View View View View	
Azure Front Door Domain Contributor Azure Front Door Domain Reader Azure Front Door Secret Contributor Azure Front Door Secret Reader Azure Kubernetes Fleet Manager Contr. Azure Kubernetes Fleet Manager RBAC	Can manage Azure Front Door domains, but can't grant access to Can view Azure Front Door domains, but can't make changes. Can manage Azure Front Door secrets, but can't grant access to Can view Azure Front Door secrets, but can't make changes. Grants access to read and write Azure Kubernetes Fleet Manager This role grants admin access - provides write permissions on mo Lets you manage all resources in the fleet manager cluster. Allows read-only access to see most objects in a namespace. It d Allows read/write access to most objects in a namespace. This rol	BuiltInRole	None None None None None None None None	View View View View View View View View	
Azure Front Door Domain Contributor Azure Front Door Domain Reader Azure Front Door Secret Contributor Azure Front Door Secret Reader Azure Kubernetes Fleet Manager Contr. Azure Kubernetes Fleet Manager RBAC	Can manage Azure Front Door domains, but can't grant access to Can view Azure Front Door domains, but can't grant access to Can manage Azure Front Door secrets, but can't grant access to Can view Azure Front Door secrets, but can't grant access to Can view Azure Front Door secrets, but can't make changes. Grants access to read and write Azure Kubernetes Fleet Manager This role grants admin access - provides write permissions on mo Lets you manage all resources in the fleet manager cluster. Allows read-only access to see most objects in a namespace. It d Allows read/write access to most objects in a namespace. This rol List cluster admin credential action. List cluster monitoring user credential action.	BuiltInRole	None None None None None None None None	View View View View View View View View	
Azure Front Door Domain Contributor Azure Front Door Domain Reader Azure Front Door Secret Contributor Azure Front Door Secret Reader Azure Kubernetes Fleet Manager Contr. Azure Kubernetes Fleet Manager RBAC. Azure Kubernetes Sevice Cluster Admi Azure Kubernetes Service Cluster Moni Azure Kubernetes Service Cluster Moni Azure Kubernetes Service Cluster User	Can manage Azure Front Door domains, but can't grant access to Can view Azure Front Door domains, but can't grant access to Can manage Azure Front Door secrets, but can't grant access to Can view Azure Front Door secrets, but can't grant access to Can view Azure Front Door secrets, but can't make changes. Grants access to read and write Azure Kubernetes Fleet Manager This role grants admin access - provides write permissions on mo Lets you manage all resources in the fleet manager cluster. Allows read-only access to see most objects in a namespace. It d Allows read/write access to most objects in a namespace. This rol List cluster admin credential action. List cluster monitoring user credential action.	BuiltInRole	None None None None None None None None	View View View View View View View View	
Azure Front Door Domain Contributor Azure Front Door Domain Reader Azure Front Door Secret Contributor Azure Front Door Secret Reader Azure Front Door Secret Reader Azure Kubernetes Fleet Manager Contr. Azure Kubernetes Fleet Manager RBAC. Azure Kubernetes Fleet Manager RBAC. Azure Kubernetes Fleet Manager RBAC. Azure Kubernetes Sevice Guster Admi. Azure Kubernetes Service Guster Moni. Azure Kubernetes Service Guster User Azure Kubernetes Service Guster User Azure Kubernetes Service Contributor	Can manage Azure Front Door domains, but can't grant access to Can view Azure Front Door domains, but can't grant access to Can manage Azure Front Door secrets, but can't grant access to Can view Azure Front Door secrets, but can't make changes. Grants access to read and write Azure Kubernetes Fleet Manager This role grants admin access - provides write permissions on mo Lets you manage all resources in the fleet manager cluster. Allows read-only access to see most objects in a namespace. It d Allows read/write access to most objects in a namespace. This rol List cluster admin credential action. List cluster monitoring user credential action.	BuiltInRole	None None None None None None None None	View View View View View View View View	
Azure Front Door Domain Contributor Azure Front Door Domain Reader Azure Front Door Secret Contributor Azure Front Door Secret Reader Azure Kubernetes Fleet Manager Contr. Azure Kubernetes Fleet Manager RBAC. Azure Kubernetes Sevice Cluster Admi. Azure Kubernetes Service Cluster Moni. Azure Kubernetes Service Cluster User Azure Kubernetes Service Contributor Azure Kubernetes Service Contributor Azure Kubernetes Service Policy Add-o	Can manage Azure Front Door domains, but can't grant access to Can view Azure Front Door domains, but can't grant access to Can manage Azure Front Door secrets, but can't grant access to Can view Azure Front Door secrets, but can't make changes. Grants access to read and write Azure Kubernetes Fleet Manager This role grants admin access - provides write permissions on mo Lets you manage all resources in the fleet manager cluster. Allows read-only access to see most objects in a namespace. It d Allows read/write access to most objects in a namespace. This rol List cluster admin credential action. List cluster monitoring user credential action. Grants access to read and write Azure Kubernetes Service clusters	BuiltInRole	None None None None None None None None	View View View View View View View View	
Azure Front Door Domain Contributor Azure Front Door Domain Reader Azure Front Door Secret Contributor Azure Front Door Secret Reader Azure Front Door Secret Reader Azure Kubernetes Fleet Manager RBAC. Azure Kubernetes Service Cluster Admin. Azure Kubernetes Service Cluster Moni. Azure Kubernetes Service Contributor Azure Kubernetes Service Policy Add-o Azure Kubernetes Service RBAC Admin	Can manage Azure Front Door domains, but can't grant access to Can view Azure Front Door domains, but can't grant access to Can manage Azure Front Door secrets, but can't grant access to Can view Azure Front Door secrets, but can't make changes. Grants access to read and write Azure Kubernetes Fleet Manager This role grants admin access - provides write permissions on mo Lets you manage all resources in the fleet manager cluster. Allows read-only access to see most objects in a namespace. It d Allows read/write access to most objects in a namespace. This rol List cluster admin credential action. List cluster monitoring user credential action. Grants access to read and write Azure Kubernetes Service clusters Deploy the Azure Policy add-on on Azure Kubernetes Service clus	BuiltInRole	None None None None None None None None	View View View View View View View View	
Azure Front Door Domain Contributor Azure Front Door Domain Reader Azure Front Door Secret Contributor Azure Front Door Secret Reader Azure Front Door Secret Reader Azure Kubernetes Fleet Manager Contr. Azure Kubernetes Fleet Manager RBAC. Azure Kubernetes Service Cluster Admi. Azure Kubernetes Service Cluster Moni. Azure Kubernetes Service Contributor Azure Kubernetes Service Policy Add-o Azure Kubernetes Service RBAC Admin Azure Kubernetes Service RBAC Admin	Can manage Azure Front Door domains, but can't grant access to Can view Azure Front Door domains, but can't grant access to Can manage Azure Front Door secrets, but can't grant access to Can view Azure Front Door secrets, but can't grant access to Can view Azure Front Door secrets, but can't make changes. Grants access to read and write Azure Kubernetes Fleet Manager This role grants admin access - provides write permissions on mo Lets you manage all resources in the fleet manager cluster. Allows read-only access to see most objects in a namespace. It d Allows read/write access to most objects in a namespace. This rol List cluster admin credential action. List cluster monitoring user credential action. Grants access to read and write Azure Kubernetes Service clusters. Deploy the Azure Policy add-on on Azure Kubernetes Service clus Lets you manage all resources under cluster/namespace, except	BuiltInRole	None None None None None None None None	View View View View View View View View	
Azure Front Door Domain Contributor Azure Front Door Domain Reader Azure Front Door Secret Contributor Azure Front Door Secret Reader Azure Front Door Secret Reader Azure Kubernetes Fleet Manager RBAC. Azure Kubernetes Service Cluster Admi. Azure Kubernetes Service Cluster Moni. Azure Kubernetes Service Contributor. Azure Kubernetes Service Contributor. Azure Kubernetes Service Policy Add-o. Azure Kubernetes Service RBAC Admin Azure Kubernetes Service RBAC Cluster. Azure Kubernetes Service RBAC Cluster.	Can manage Azure Front Door domains, but can't grant access to Can view Azure Front Door domains, but can't grant access to Can manage Azure Front Door secrets, but can't grant access to Can view Azure Front Door secrets, but can't make changes. Grants access to read and write Azure Kubernetes Fleet Manager This role grants admin access - provides write permissions on mo Lets you manage all resources in the fleet manager cluster. Allows read-only access to see most objects in a namespace. It d Allows read/write access to most objects in a namespace. This rol List cluster admin credential action. List cluster monitoring user credential action. Grants access to read and write Azure Kubernetes Service clusters Deploy the Azure Policy add-on on Azure Kubernetes Service clust Lets you manage all resources under cluster/namespace, except Lets you manage all resources in the cluster.	BuiltInRole	None None None None None None None None	View View View View View View View View	
Azure Front Door Domain Contributor Azure Front Door Domain Reader Azure Front Door Secret Contributor Azure Front Door Secret Reader Azure Front Door Secret Reader Azure Kubernetes Fleet Manager RBAC. Azure Kubernetes Service Cluster Admi. Azure Kubernetes Service Cluster Moni. Azure Kubernetes Service Contributor. Azure Kubernetes Service Contributor. Azure Kubernetes Service Policy Add-o. Azure Kubernetes Service RBAC Admin Azure Kubernetes Service RBAC Cluster. Azure Kubernetes Service RBAC Cluster.	Can manage Azure Front Door domains, but can't grant access to Can view Azure Front Door domains, but can't grant access to Can manage Azure Front Door secrets, but can't grant access to Can view Azure Front Door secrets, but can't make changes. Grants access to read and write Azure Kubernetes Fleet Manager This role grants admin access - provides write permissions on mo Lets you manage all resources in the fleet manager cluster. Allows read-only access to see most objects in a namespace. It d Allows read/write access to most objects in a namespace. This rol List cluster admin credential action. List cluster user credential action. Grants access to read and write Azure Kubernetes Service clus Lets you manage all resources under cluster/namespace, except Lets you manage all resources in the cluster. Allows read-only access to see most objects in a namespace. It d Allows read-only access to see most objects in a namespace. It d	BuiltInRole	None None None None None None None None	View View View View View View View View	

Grants access to read map related data from an Azure maps acco... BuiltInRole

Azure Maps Data Reader

ITATIIC IMATIAGEI CONTINUITOI	Lets you manage tranic inanager profiles, but does not let you c	Bullulinole	networking	view	200
User Access Administrator	Lets you manage user access to Azure resources.	BuiltInRole	General		
☐ Video Indexer Restricted Viewer	Has access to view and search through all video's insights and tra	BuiltInRole	None		
Virtual Machine Administrator Login	View Virtual Machines in the portal and login as administrator	BuiltInRole	Compute		
Virtual Machine Contributor	Lets you manage virtual machines, but not access to them, and n	BuiltInRole	Compute		
Virtual Machine Local User Login	View Virtual Machines in the portal and login as a local user confi	BuiltInRole	None		
Virtual Machine User Login	View Virtual Machines in the portal and login as a regular user.	BuiltInRole	Compute		
☐ VM Scanner Operator	Role that provides access to disk snapshot for security analysis.	BuiltInRole	None		
Web Plan Contributor	Lets you manage the web plans for websites, but not access to th	BuiltInRole	Web		
Web PubSub Service Owner	Full access to Azure Web PubSub Service REST APIs	BuiltInRole	Preview		
Web PubSub Service Reader	Read-only access to Azure Web PubSub Service REST APIs	BuiltInRole	Preview		
Website Contributor	Lets you manage websites (not web plans), but not access to them.	BuiltInRole	Web		
Windows Admin Center Administrator	Let's you manage the OS of your resource via Windows Admin C	BuiltInRole	None		
Windows365NetworkInterfaceContribu	Create NICs and join it to virtual machine in another tenant. This	BuiltInRole	None		
Windows365NetworkUser	Read the virtual network informations, and join the virtual networ	BuiltInRole	None		
Windows365SubscriptionReader	Read subscriptions, images, azure firewalls. This role is used in Wi	BuiltInRole	None		
Workbook Contributor	Can save shared workbooks.	BuiltInRole	Monitor		
Workbook Reader	Can read workbooks.	BuiltInRole	Monitor		
WorkloadBuilder Migration Agent Role	WorkloadBuilder Migration Agent Role.	BuiltInRole	None		
	·	·	·	·	

Site Recovery Reader	Lets you view Site Recovery status but not perform other manage	Duilsta Dala	Management + Gover	Year	
					-
Spatial Anchors Account Contributor	Lets you manage spatial anchors in your account, but not delete	BuiltInRole	Mixed Reality		***
Spatial Anchors Account Owner	Lets you manage spatial anchors in your account, including deleti	BuiltInRole	Mixed Reality		***
Spatial Anchors Account Reader	Lets you locate and read properties of spatial anchors in your acc	BuiltInRole	Mixed Reality		****
SQL DB Contributor	Lets you manage SQL databases, but not access to them. Also, yo	BuiltInRole	Databases		***
SQL Managed Instance Contributor	Lets you manage SQL Managed Instances and required network	BuiltInRole	Databases		***
SQL Security Manager	Lets you manage the security-related policies of SQL servers and	BuiltInRole	Databases		all.
SQL Server Contributor	Lets you manage SQL servers and databases, but not access to th	BuiltInRole	Databases		***
SqlDb Migration Role	Role for SqlDb migration	BuiltInRole	None		200
SqIMI Migration Role	Role for SqlMI migration	BuiltInRole	None		***
SqIVM Migration Role	Role for SqlVM migration	BuiltInRole	None		7***
Storage Account Backup Contributor	Lets you perform backup and restore operations using Azure Bac	BuiltInRole	Storage		***
Storage Account Contributor	Lets you manage storage accounts, including accessing storage a	BuiltInRole	Storage		***
Storage Account Key Operator Service	Storage Account Key Operators are allowed to list and regenerat	BuiltInRole	Storage		****
Storage Blob Data Contributor	Allows for read, write and delete access to Azure Storage blob co	BuiltInRole	Storage		****
Storage Blob Data Owner	Allows for full access to Azure Storage blob containers and data, i	BuiltInRole	Storage		***
Storage Blob Data Reader	Allows for read access to Azure Storage blob containers and data	BuiltInRole	Storage		****
Storage Blob Delegator	Allows for generation of a user delegation key which can be used	BuiltInRole	Storage		***
Storage File Data Privileged Contributor	Customer has read, write, delete and modify NTFS permission acc	. BuiltInRole	None		
Storage File Data Privileged Reader	Customer has read access on Azure Storage file shares.	BuiltInRole	None		***
Storage File Data SMB Share Contributor	Allows for read, write, and delete access in Azure Storage file shar	BuiltInRole	Storage		****
Storage File Data SMB Share Elevated	Allows for read, write, delete and modify NTFS permission access	BuiltInRole	Storage		***

Purview role 2 (Deprecated)	Deprecated role.	BuiltInRole	Preview		***
Purview role 3 (Deprecated)	Deprecated role.	BuiltInRole	Preview		
Quota Request Operator	Read and create quota requests, get quota request status, and cr	BuiltInRole	Management + Gover		***
Reader and Data Access	Lets you view everything but will not let you delete or create a st	BuiltInRole	Storage		***
Redis Cache Contributor	Lets you manage Redis caches, but not access to them.	BuiltInRole	Databases		***
Remote Rendering Administrator	Provides user with conversion, manage session, rendering and di	BuiltInRole	Mixed Reality		***
Remote Rendering Client	Provides user with manage session, rendering and diagnostics ca	BuiltInRole	Mixed Reality		***
Reservation Purchaser	Lets you purchase reservations	BuiltInRole	Management + Gover		***
Resource Policy Contributor	Users with rights to create/modify resource policy, create support	BuiltInRole	Management + Gover		***
Role Based Access Control Administrat	Manage access to Azure resources by assigning roles using Azure	BuiltInRole	None		111
SaaS Hub Contributor	SaaS Hub contributor can manage SaaS Hub resource	BuiltInRole	None		•••
Scheduled Patching Contributor	Provides access to manage maintenance configurations with mai	BuiltInRole	None		***
Scheduler Job Collections Contributor	Lets you manage Scheduler job collections, but not access to the	BuiltInRole	Other		***
Schema Registry Contributor (Preview)	Read, write, and delete Schema Registry groups and schemas.	BuiltInRole	Preview		***
Schema Registry Reader (Preview)	Read and list Schema Registry groups and schemas.	BuiltInRole	Preview		***
Search Index Data Contributor	Grants full access to Azure Cognitive Search index data.	BuiltInRole	Web		***
Search Index Data Reader	Grants read access to Azure Cognitive Search index data.	BuiltInRole	Web		***
Search Service Contributor	Lets you manage Search services, but not access to them.	BuiltInRole	Web		***
Security Admin	Security Admin Role	BuiltInRole	Security		***
Security Assessment Contributor	Lets you push assessments to Security Center	BuiltInRole	Security		***
Security Detonation Chamber Publisher	Allowed to publish and modify platforms, workflows and toolsets	BuiltInRole	Security		***
Security Detonation Chamber Reader	Allowed to query submission info and files from Security Detonat	BuiltInRole	Security		***
Security Detonation Chamber Submissi	Allowed to create and manage submissions to Security Detonatio	BuiltInRole	Security	View	
Managed Application Operator Role	Lets you read and perform actions on Managed Application reso	BuiltInRole	Management + Gover	View	,,,
Managed Application Operator Role Managed Applications Reader	Lets you read and perform actions on Managed Application reso Lets you read resources in a managed app and request JIT access.	BuiltInRole BuiltInRole	Management + Gover Management + Gover		
_					
Managed Applications Reader	Lets you read resources in a managed app and request JIT access.	BuiltInRole	Management + Gover		
Managed Applications Reader Managed HSM contributor	Lets you read resources in a managed app and request JIT access. Lets you manage managed HSM pools, but not access to them.	BuiltInRole BuiltInRole	Management + Gover Security		
Managed Applications Reader Managed HSM contributor Managed Identity Contributor	Lets you read resources in a managed app and request JIT access. Lets you manage managed HSM pools, but not access to them. Create, Read, Update, and Delete User Assigned Identity	BuiltInRole BuiltInRole BuiltInRole BuiltInRole	Management + Gover Security Identity		
Managed Applications Reader Managed HSM contributor Managed Identity Contributor Managed Identity Operator	Lets you read resources in a managed app and request JIT access. Lets you manage managed HSM pools, but not access to them. Create, Read, Update, and Delete User Assigned Identity Read and Assign User Assigned Identity	BuiltInRole BuiltInRole BuiltInRole BuiltInRole	Management + Gover Security Identity Identity		
Managed Applications Reader Managed HSM contributor Managed Identity Contributor Managed Identity Operator Managed Services Registration assign	Lets you read resources in a managed app and request JIT access. Lets you manage managed HSM pools, but not access to them. Create, Read, Update, and Delete User Assigned Identity Read and Assign User Assigned Identity Managed Services Registration Assignment Delete Role allows th	BuiltInRole BuiltInRole BuiltInRole BuiltInRole BuiltInRole	Management + Gover Security Identity Identity Management + Gover		
Managed Applications Reader Managed HSM contributor Managed Identity Contributor Managed Identity Operator Managed Identity Operator Managed Services Registration assign	Lets you read resources in a managed app and request JIT access. Lets you manage managed HSM pools, but not access to them. Create, Read, Update, and Delete User Assigned Identity Read and Assign User Assigned Identity Managed Services Registration Assignment Delete Role allows th Management Group Contributor Role	BuiltInRole BuiltInRole BuiltInRole BuiltInRole BuiltInRole BuiltInRole BuiltInRole BuiltInRole	Management + Gover Security Identity Identity Management + Gover Management + Gover		
Managed Applications Reader Managed HSM contributor Managed Identity Contributor Managed Identity Operator Managed Services Registration assign Management Group Contributor Management Group Reader Media Services Account Administrator	Lets you read resources in a managed app and request JIT access. Lets you manage managed HSM pools, but not access to them. Create, Read, Update, and Delete User Assigned Identity Read and Assign User Assigned Identity Managed Services Registration Assignment Delete Role allows th Management Group Contributor Role Management Group Reader Role	BuitInRole	Management + Gover Security Identity Identity Management + Gover Management + Gover		
Managed Applications Reader Managed HSM contributor Managed Identity Contributor Managed Identity Operator Managed Services Registration assign Management Group Contributor Management Group Reader Media Services Account Administrator	Lets you read resources in a managed app and request JIT access. Lets you manage managed HSM pools, but not access to them. Create, Read, Update, and Delete User Assigned Identity Read and Assign User Assigned Identity Managed Services Registration Assignment Delete Role allows th Management Group Contributor Role Management Group Reader Role Create, read, modify, and delete Media Services accounts; read-o	BuittnRote	Management + Gover Security Identity Identity Management + Gover Management + Gover Web		
Managed Applications Reader Managed HSM contributor Managed Identity Contributor Managed Identity Operator Managed Services Registration assign Management Group Contributor Management Group Reader Media Services Account Administrator Media Services Live Events Administrat	Lets you read resources in a managed app and request JIT access. Lets you manage managed HSM pools, but not access to them. Create, Read, Update, and Delete User Assigned Identity Read and Assign User Assigned Identity Managed Services Registration Assignment Delete Role allows th Management Group Contributor Role Management Group Reader Role Create, read, modify, and delete Media Services accounts; read-o Create, read, modify, and delete Live Events, Assets, Asset Filters,	BuittnRole	Management + Gover Security Identity Identity Management + Gover Management + Gover Web Web		
Managed Applications Reader Managed HSM contributor Managed Identity Contributor Managed Identity Operator Managed Services Registration assign Management Group Contributor Management Group Reader Media Services Account Administrator Media Services Media Operator Media Services Media Operator Media Services Policy Administrator	Lets you read resources in a managed app and request JIT access. Lets you manage managed HSM pools, but not access to them. Create, Read, Update, and Delete User Assigned Identity Read and Assign User Assigned Identity Managed Services Registration Assignment Delete Role allows th Management Group Contributor Role Management Group Reader Role Create, read, modify, and delete Media Services accounts; read-o Create, read, modify, and delete Live Events, Assets, Asset Filters, Create, read, modify, and delete Assets, Asset Filters, Streaming L	BuiltInRole	Management + Gover Security Identity Identity Management + Gover Management + Gover Web Web Web		
Managed Applications Reader Managed HSM contributor Managed Identity Contributor Managed Identity Operator Managed Identity Operator Managed Services Registration assign Management Group Contributor Management Group Reader Media Services Account Administrator Media Services Live Events Administrat Media Services Media Operator Media Services Policy Administrator Media Services Streaming Endpoints A	Lets you read resources in a managed app and request JIT access. Lets you manage managed HSM pools, but not access to them. Create, Read, Update, and Delete User Assigned Identity Read and Assign User Assigned Identity Managed Services Registration Assignment Delete Role allows th Management Group Contributor Role Management Group Reader Role Create, read, modify, and delete Media Services accounts; read-o Create, read, modify, and delete Live Events, Assets, Asset Filters, Create, read, modify, and delete Assets, Asset Filters, Streaming L Create, read, modify, and delete Account Filters, Streaming Polici	BuiltInRole	Management + Gover Security Identity Identity Management + Gover Management + Gover Web Web Web Web		
Managed Applications Reader Managed HSM contributor Managed Identity Contributor Managed Identity Operator Managed Identity Operator Managed Services Registration assign Management Group Contributor Management Group Reader Media Services Account Administrator Media Services Live Events Administrat Media Services Media Operator Media Services Policy Administrator Media Services Streaming Endpoints A	Lets you read resources in a managed app and request JIT access. Lets you manage managed HSM pools, but not access to them. Create, Read, Update, and Delete User Assigned Identity Read and Assign User Assigned Identity Managed Services Registration Assignment Delete Role allows th Management Group Contributor Role Management Group Reader Role Create, read, modify, and delete Media Services accounts; read-o Create, read, modify, and delete Live Events, Assets, Asset Filters, Create, read, modify, and delete Asceunt Filters, Streaming L Create, read, modify, and delete Account Filters, Streaming Polici Create, read, modify, and delete Streaming Endpoints; read-only	BuiltInRole	Management + Gover Security Identity Identity Management + Gover Management + Gover Web Web Web Web Web		
Managed Applications Reader Managed HSM contributor Managed Identity Contributor Managed Identity Operator Managed Services Registration assign Management Group Contributor Management Group Reader Media Services Account Administrator Media Services Live Events Administrat Media Services Media Operator Media Services Streaming Endpoints A Microsoft Sentinel Automation Contrib	Lets you read resources in a managed app and request JIT access. Lets you manage managed HSM pools, but not access to them. Create, Read, Update, and Delete User Assigned Identity Read and Assign User Assigned Identity Managed Services Registration Assignment Delete Role allows th Management Group Contributor Role Management Group Reader Role Create, read, modify, and delete Media Services accounts; read-o Create, read, modify, and delete Live Events, Assets, Asset Filters, Create, read, modify, and delete Assets, Asset Filters, Streaming L Create, read, modify, and delete Streaming Endpoints; read-only Microsoft Sentinel Automation Contributor	BuiltInRole	Management + Gover Security Identity Identity Management + Gover Management + Gover Web Web Web Web Web Security		
Managed Applications Reader Managed HSM contributor Managed Identity Contributor Managed Identity Operator Managed Services Registration assign Management Group Contributor Management Group Reader Media Services Account Administrator Media Services Live Events Administrat Media Services Media Operator Media Services Streaming Endpoints A Microsoft Sentinel Automation Contrib Microsoft Sentinel Automation Contrib	Lets you read resources in a managed app and request JIT access. Lets you manage managed HSM pools, but not access to them. Create, Read, Update, and Delete User Assigned Identity Read and Assign User Assigned Identity Managed Services Registration Assignment Delete Role allows th Management Group Contributor Role Management Group Reader Role Create, read, modify, and delete Media Services accounts; read-o Create, read, modify, and delete Live Events, Assets, Asset Filters, Create, read, modify, and delete Assets, Asset Filters, Streaming L Create, read, modify, and delete Account Filters, Streaming Polici Create, read, modify, and delete Streaming Endpoints; read-only Microsoft Sentinel Automation Contributor Microsoft Sentinel Contributor	BuiltInRole	Management + Gover Security Identity Identity Management + Gover Management + Gover Web Web Web Web Web Web Security Security		
Managed Applications Reader Managed HSM contributor Managed Identity Contributor Managed Identity Operator Managed Services Registration assign Management Group Contributor Management Group Reader Media Services Account Administrator Media Services Live Events Administrat Media Services Media Operator Media Services Streaming Endpoints A Microsoft Sentinel Automation Contrib Microsoft Sentinel Contributor	Lets you read resources in a managed app and request JIT access. Lets you manage managed HSM pools, but not access to them. Create, Read, Update, and Delete User Assigned Identity Read and Assign User Assigned Identity Managed Services Registration Assignment Delete Role allows th Management Group Contributor Role Management Group Reader Role Create, read, modify, and delete Media Services accounts; read-o Create, read, modify, and delete Live Events, Assets, Asset Filters, Create, read, modify, and delete Assets, Asset Filters, Streaming L Create, read, modify, and delete Account Filters, Streaming Polici Create, read, modify, and delete Streaming Endpoints; read-only Microsoft Sentinel Automation Contributor Microsoft Sentinel Contributor Microsoft Sentinel Playbook Operator	BuiltInRole	Management + Gover Security Identity Identity Management + Gover Management + Gover Web Web Web Web Web Web Security None		
Managed Applications Reader Managed HSM contributor Managed Identity Contributor Managed Identity Operator Managed Services Registration assign Management Group Contributor Management Group Reader Media Services Account Administrator Media Services Media Operator Media Services Media Operator Media Services Streaming Endpoints A Microsoft Sentinel Automation Contrib Microsoft Sentinel Contributor Microsoft Sentinel Playbook Operator Microsoft Sentinel Reader Microsoft Sentinel Responder	Lets you read resources in a managed app and request JIT access. Lets you manage managed HSM pools, but not access to them. Create, Read, Update, and Delete User Assigned Identity Read and Assign User Assigned Identity Managed Services Registration Assignment Delete Role allows th Management Group Contributor Role Management Group Reader Role Create, read, modify, and delete Media Services accounts; read-o Create, read, modify, and delete Live Events, Assets, Asset Filters, Create, read, modify, and delete Assets, Asset Filters, Streaming L Create, read, modify, and delete Account Filters, Streaming Polici Create, read, modify, and delete Streaming Endpoints; read-only Microsoft Sentinel Automation Contributor Microsoft Sentinel Contributor Microsoft Sentinel Playbook Operator Microsoft Sentinel Reader	BuiltInRole	Management + Gover Security Identity Identity Management + Gover Management + Gover Web Web Web Web Web Web Security Security None Security Security Security		
Managed Applications Reader Managed HSM contributor Managed Identity Contributor Managed Identity Operator Managed Services Registration assign Management Group Contributor Management Group Reader Media Services Account Administrator Media Services Media Operator Media Services Media Operator Media Services Streaming Endpoints A Microsoft Sentinel Automation Contrib Microsoft Sentinel Contributor Microsoft Sentinel Playbook Operator Microsoft Sentinel Reader Microsoft Sentinel Responder	Lets you read resources in a managed app and request JIT access. Lets you manage managed HSM pools, but not access to them. Create, Read, Update, and Delete User Assigned Identity Read and Assign User Assigned Identity Managed Services Registration Assignment Delete Role allows th Management Group Contributor Role Management Group Reader Role Create, read, modify, and delete Media Services accounts; read-o Create, read, modify, and delete Live Events, Assets, Asset Filters, Create, read, modify, and delete Assets, Asset Filters, Streaming L Create, read, modify, and delete Account Filters, Streaming Polici Create, read, modify, and delete Streaming Endpoints; read-only Microsoft Sentinel Automation Contributor Microsoft Sentinel Contributor Microsoft Sentinel Playbook Operator Microsoft Sentinel Reader Microsoft Sentinel Responder	BuiltInRole	Management + Gover Security Identity Identity Management + Gover Management + Gover Web Web Web Web Web Security Security None Security Security Security Security		
Managed Applications Reader Managed HSM contributor Managed Identity Contributor Managed Identity Operator Managed Services Registration assign Management Group Contributor Media Services Account Administrator Media Services Live Events Administrator Media Services Policy Administrator Media Services Policy Administrator Media Services Streaming Endpoints A Microsoft Sentinel Automation Contrib Microsoft Sentinel Playbook Operator Microsoft Sentinel Reader Microsoft Sentinel Reader Microsoft Sentinel Responder	Lets you read resources in a managed app and request JIT access. Lets you manage managed HSM pools, but not access to them. Create, Read, Update, and Delete User Assigned Identity Read and Assign User Assigned Identity Managed Services Registration Assignment Delete Role allows th Management Group Contributor Role Management Group Reader Role Create, read, modify, and delete Media Services accounts; read-o Create, read, modify, and delete Live Events, Assets, Asset Filters, Create, read, modify, and delete Assets, Asset Filters, Streaming L Create, read, modify, and delete Account Filters, Streaming Polici Create, read, modify, and delete Streaming Endpoints; read-only Microsoft Sentinel Automation Contributor Microsoft Sentinel Playbook Operator Microsoft Sentinel Reader Microsoft Sentinel Responder Microsoft Sentinel Responder Microsoft.Kubernetes connected cluster role.	BuittnRole	Management + Gover Security Identity Identity Management + Gover Management + Gover Web Web Web Web Web Security Security None Security None		
Managed Applications Reader Managed HSM contributor Managed Identity Contributor Managed Identity Operator Managed Services Registration assign Management Group Contributor Management Group Reader Media Services Account Administrator Media Services Live Events Administrator Media Services Policy Administrator Media Services Policy Administrator Media Services Streaming Endpoints A Microsoft Sentinel Automation Contrib Microsoft Sentinel Contributor Microsoft Sentinel Playbook Operator Microsoft Sentinel Reader Microsoft Sentinel Responder Microsoft Sentinel Responder Microsoft Sentinel Responder Microsoft Suthernetes connected cluste Monitoring Contributor	Lets you read resources in a managed app and request JIT access. Lets you manage managed HSM pools, but not access to them. Create, Read, Update, and Delete User Assigned Identity Read and Assign User Assigned Identity Managed Services Registration Assignment Delete Role allows th Management Group Contributor Role Management Group Reader Role Create, read, modify, and delete Media Services accounts; read-o Create, read, modify, and delete Live Events, Assets, Asset Filters, Create, read, modify, and delete Assets, Asset Filters, Streaming L Create, read, modify, and delete Account Filters, Streaming Polici Create, read, modify, and delete Streaming Endpoints; read-only Microsoft Sentinel Automation Contributor Microsoft Sentinel Contributor Microsoft Sentinel Playbook Operator Microsoft Sentinel Reader Microsoft Sentinel Responder Microsoft Sentinel Responder Microsoft Sentinel Responder Microsoft Lubernetes connected cluster role.	BuiltInRole	Management + Gover Security Identity Identity Management + Gover Management + Gover Web Web Web Web Web Security Security None Security None Monitor		

Impact Reporter	Allows access to create/report, read and delete impacts	BuiltInRole	None	View	***
	Lets you manage integration service environments, but not access		Integration		
	Allows developers to create and update workflows, integration ac		Integration		
	r Lets you manage Intelligent Systems accounts, but not access to		Integration		
Intelligent Systems Account Contributor					
	Allows for full access to IoT Hub data plane operations.	BuiltInRole	Internet of things		
loT Hub Data Reader	Allows for full read access to IoT Hub data-plane properties	BuiltInRole	Internet of things		
☐ IoT Hub Registry Contributor	Allows for full access to IoT Hub device registry.	BuiltInRole	Internet of things		
loT Hub Twin Contributor	Allows for read and write access to all IoT Hub device and modul	BuiltInRole	Internet of things		
Key Vault Administrator	Perform all data plane operations on a key vault and all objects in	n BuiltInRole	Security		
Key Vault Certificates Officer	Perform any action on the certificates of a key vault, except mana	BuiltInRole	Security		
Key Vault Contributor	Lets you manage key vaults, but not access to them.	BuiltInRole	Security		
Key Vault Crypto Officer	Perform any action on the keys of a key vault, except manage per	r BuiltInRole	Security		
Key Vault Crypto Service Encryption Use	er Read metadata of keys and perform wrap/unwrap operations. Or	n BuiltInRole	Security		
Key Vault Crypto User	Perform cryptographic operations using keys. Only works for key	BuiltInRole	Security		
Key Vault Reader	Read metadata of key vaults and its certificates, keys, and secrets	BuiltInRole	Security		
Key Vault Secrets Officer	Perform any action on the secrets of a key vault, except manage.	BuiltInRole	Security		
Key Vault Secrets User	Read secret contents. Only works for key vaults that use the 'Azur	r BuiltInRole	Security		
☐ Knowledge Consumer	Knowledge Read permission to consume Enterprise Graph Knowl		None		
Kubernetes Agentless Operator	Grants Microsoft Defender for Cloud access to Azure Kubernetes		None		
	Role definition to authorize any user/service to create connected.		Management + Gover.		
Kubernetes Extension Contributor	Can create, update, get, list and delete Kubernetes Extensions, an		Management + Gover.		
Kubernetes Extension Contributor	Can deate, upuate, get, list and delete Rubernetes Extensions, an	BullutiNote	ivianagement + Gover.	view	
Aud V Download fold assignments —	FOR COLUMN O WILLIAM NO INCHIONE WILLIAM				
	Lets you manage classic virtual machines, but not access to them, E		mpute Vie		***
	Lets you manage ClearDB MySQL databases, but not access to th E				
Code Signing Certificate Profile Signer	Sign files with a certificate profile. This role is in preview and subj	BuiltInRole No	ne Vie		***
100.00					-
Code Signing Identity Verifier	Manage identity or business verification requests. This role is in p	BuiltInRole No	ne Vie		***
	Manage identity or business verification requests. This role is in p E Lets you create, read, update, delete and manage keys of Cogniti E		ne Vie + Machine Learning Vie		
Cognitive Services Contributor		BuiltInRole Al			***
Cognitive Services Contributor Cognitive Services Custom Vision Cont	Lets you create, read, update, delete and manage keys of Cogniti	BuiltInRole Al	+ Machine Learning Vie		
Cognitive Services Custom Vision Cont Cognitive Services Custom Vision Depl	Lets you create, read, update, delete and manage keys of Cogniti Efull access to the project, including the ability to view, create, edi E	BuiltInRole Al BuiltInRole Al BuiltInRole Al	+ Machine Learning Vie + Machine Learning Vie		
Cognitive Services Custom Vision Cont Cognitive Services Custom Vision Depl Cognitive Services Custom Vision Labe	Lets you create, read, update, delete and manage keys of Cogniti E Full access to the project, including the ability to view, create, edi E Publish, unpublish or export models. Deployment can view the pr E	BuiltInRole Al BuiltInRole Al BuiltInRole Al BuiltInRole Al	+ Machine Learning Vie + Machine Learning Vie + Machine Learning Vie		
Cognitive Services Contributor Cognitive Services Custom Vision Cont Cognitive Services Custom Vision Depl Cognitive Services Custom Vision Labe Cognitive Services Custom Vision Read	Lets you create, read, update, delete and manage keys of Cogniti E Full access to the project, including the ability to view, create, edi E Publish, unpublish or export models. Deployment can view the pr E View, edit training images and create, add, remove, or delete the E	BuittinRole Al BuittinRole Al BuittinRole Al BuittinRole Al BuittinRole Al	+ Machine Learning Viet + Machine Learning Viet + Machine Learning Viet + Machine Learning Viet		
Cognitive Services Contributor Cognitive Services Custom Vision Cont Cognitive Services Custom Vision Depl Cognitive Services Custom Vision Labe Cognitive Services Custom Vision Read	Lets you create, read, update, delete and manage keys of Cogniti E Full access to the project, including the ability to view, create, edi E Publish, unpublish or export models. Deployment can view the pr E View, edit training images and create, add, remove, or delete the E Read-only actions in the project. Readers can't create or update t E View, edit projects and train the models, including the ability to p E	BuiltinRole Al	+ Machine Learning Vie + Machine Learning Vie + Machine Learning Vie + Machine Learning Vie + Machine Learning Vie		
Cognitive Services Custom Vision Cont Cognitive Services Custom Vision Depl Cognitive Services Custom Vision Labe Cognitive Services Custom Vision Read Cognitive Services Custom Vision Trainer Cognitive Services Data Reader (Previe	Lets you create, read, update, delete and manage keys of Cogniti E Full access to the project, including the ability to view, create, edi E Publish, unpublish or export models. Deployment can view the pr E View, edit training images and create, add, remove, or delete the E Read-only actions in the project. Readers can't create or update t E View, edit projects and train the models, including the ability to p E	BuiltinRole Al	+ Machine Learning Vie		
Cognitive Services Contributor Cognitive Services Custom Vision Cont Cognitive Services Custom Vision Depl Cognitive Services Custom Vision Labe Cognitive Services Custom Vision Read Cognitive Services Custom Vision Trainer Cognitive Services Data Reader (Previe Cognitive Services Face Recognizer	Lets you create, read, update, delete and manage keys of Cogniti E Full access to the project, including the ability to view, create, edi E Publish, unpublish or export models. Deployment can view the pr E View, edit training images and create, add, remove, or delete the E Read-only actions in the project. Readers can't create or update t E View, edit projects and train the models, including the ability to p E Lets you read Cognitive Services data.	BuiltinRole Al	+ Machine Learning Vir + Machine Learning Vir view Vir + Machine Learning Vir + Machine Learning Vir		
Cognitive Services Custom Vision Cont Cognitive Services Custom Vision Depl Cognitive Services Custom Vision Depl Cognitive Services Custom Vision Labe Cognitive Services Custom Vision Read Cognitive Services Custom Vision Trainer Cognitive Services Data Reader (Previe Cognitive Services Face Recognizer Cognitive Services Immersive Reader U	Lets you create, read, update, delete and manage keys of Cogniti E Full access to the project, including the ability to view, create, edi E Publish, unpublish or export models. Deployment can view the pr E View, edit training images and create, add, remove, or delete the E Read-only actions in the project. Readers can't create or update t E View, edit projects and train the models, including the ability to p E Lets you read Cognitive Services data. Lets you perform detect, verify, identify, group, and find similar o E	BuiltinRole Al	+ Machine Learning Vii - Machine Learning Vii		
Cognitive Services Custom Vision Cont Cognitive Services Custom Vision Depl Cognitive Services Custom Vision Depl Cognitive Services Custom Vision Read Cognitive Services Custom Vision Trainer Cognitive Services Custom Vision Trainer Cognitive Services Data Reader (Previe Cognitive Services Face Recognizer Cognitive Services Immersive Reader U Cognitive Services Language Owner	Lets you create, read, update, delete and manage keys of Cogniti E Full access to the project, including the ability to view, create, edi E Publish, unpublish or export models. Deployment can view the pr E View, edit training images and create, add, remove, or delete the E Read-only actions in the project. Readers can't create or update t E View, edit projects and train the models, including the ability to p E Lets you read Cognitive Services data. Lets you perform detect, verify, identify, group, and find similar o E Provides access to create Immersive Reader sessions and call APIs Has access to all Read, Test, Write, Deploy and Delete functions u E	BuiltinRole Al	+ Machine Learning Vivi + Machine Learning Vivi - Machine Learning Vivi		
Cognitive Services Custom Vision Cont Cognitive Services Custom Vision Depl Cognitive Services Custom Vision Depl Cognitive Services Custom Vision Read Cognitive Services Custom Vision Trainer Cognitive Services Custom Vision Trainer Cognitive Services Data Reader (Previe Cognitive Services Immersive Reader U Cognitive Services Language Owner Cognitive Services Language Reader	Lets you create, read, update, delete and manage keys of Cogniti E Full access to the project, including the ability to view, create, edi E Publish, unpublish or export models. Deployment can view the pr E View, edit training images and create, add, remove, or delete the E Read-only actions in the project. Readers can't create or update t E View, edit projects and train the models, including the ability to p E Lets you read Cognitive Services data. Lets you perform detect, verify, identify, group, and find similar o E Provides access to create Immersive Reader sessions and call APIs Has access to all Read, Test, Write, Deploy and Delete functions u E	BuiltinRole Al BuiltinRole No BuiltinRole No	+ Machine Learning Vir + Machine Learning Vir ne Vir ne Vir ne Vir		
Cognitive Services Custom Vision Cont Cognitive Services Custom Vision Cont Cognitive Services Custom Vision Depl Cognitive Services Custom Vision Labe Cognitive Services Custom Vision Read Cognitive Services Custom Vision Trainer Cognitive Services Data Reader (Previe Cognitive Services Face Recognizer Cognitive Services Immersive Reader U Cognitive Services Language Owner Cognitive Services Language Reader Cognitive Services Language Writer	Lets you create, read, update, delete and manage keys of Cogniti E Full access to the project, including the ability to view, create, edi E Publish, unpublish or export models. Deployment can view the pr E View, edit training images and create, add, remove, or delete the E Read-only actions in the project. Readers can't create or update t E View, edit projects and train the models, including the ability to p E Lets you read Cognitive Services data. E Lets you perform detect, verify, identify, group, and find similar o E Provides access to create Immersive Reader sessions and call APIs Has access to all Read, Test, Write, Deploy and Delete functions u E Has access to Read and Test functions under Language portal	BuiltinRole Al BuiltinRole No BuiltinRole No	+ Machine Learning Vir + Machine Learning Vir ne Vir ne Vir ne Vir		
Cognitive Services Custom Vision Cont Cognitive Services Custom Vision Depl Cognitive Services Custom Vision Labe Cognitive Services Custom Vision Read Cognitive Services Custom Vision Trainer Cognitive Services Custom Vision Trainer Cognitive Services Face Recognizer Cognitive Services Immersive Reader U Cognitive Services Language Owner Cognitive Services Language Writer Cognitive Services Language Writer Cognitive Services Language Writer	Lets you create, read, update, delete and manage keys of Cogniti E Full access to the project, including the ability to view, create, edi E Publish, unpublish or export models. Deployment can view the pr E View, edit training images and create, add, remove, or delete the E Read-only actions in the project. Readers can't create or update t E View, edit projects and train the models, including the ability to p E Lets you read Cognitive Services data. Lets you perform detect, verify, identify, group, and find similar o E Provides access to create Immersive Reader sessions and call APIs Has access to Read and Test functions under Language portal Has access to Read and Test functions under Language E Has access to all Read, Test, and Write functions under Language E Has access to all Read, Test, Write, Deploy and Delete functions u E	BuiltinRole Al BuiltinRole No BuiltinRole No	+ Machine Learning Vii - Machine Vii - Machi		
Cognitive Services Custom Vision Cont Cognitive Services Custom Vision Depl Cognitive Services Custom Vision Depl Cognitive Services Custom Vision Labe Cognitive Services Custom Vision Read Cognitive Services Custom Vision Trainer Cognitive Services Custom Vision Trainer Cognitive Services Data Reader (Previe Cognitive Services Immersive Reader U Cognitive Services Language Owner Cognitive Services Language Writer Cognitive Services LUIS Owner Cognitive Services LUIS Reader	Lets you create, read, update, delete and manage keys of Cogniti E Full access to the project, including the ability to view, create, edi E Publish, unpublish or export models. Deployment can view the pr E View, edit training images and create, add, remove, or delete the E Read-only actions in the project. Readers can't create or update t E View, edit projects and train the models, including the ability to p E Lets you read Cognitive Services data. Lets you perform detect, verify, identify, group, and find similar o E Provides access to create Immersive Reader sessions and call APIs Has access to Read and Test functions under Language portal Has access to all Read, Test, Write, Deploy and Delete functions u E Has access to all Read, Test, write, Deploy and Delete functions u E Has access to Read and Test functions under Language E Has access to Read and Test functions under LUIS.	BuiltinRole Al BuiltinRole No BuiltinRole No BuiltinRole No	+ Machine Learning Vii ne Vii		
Cognitive Services Custom Vision Cont Cognitive Services Custom Vision Depl Cognitive Services Custom Vision Depl Cognitive Services Custom Vision Read Cognitive Services Custom Vision Read Cognitive Services Custom Vision Trainer Cognitive Services Custom Vision Trainer Cognitive Services Data Reader (Previe Cognitive Services Immersive Reader U Cognitive Services Inguage Owner Cognitive Services Language Writer Cognitive Services LUIS Owner Cognitive Services LUIS Reader Cognitive Services LUIS Reader	Lets you create, read, update, delete and manage keys of Cogniti E Full access to the project, including the ability to view, create, edi E Publish, unpublish or export models. Deployment can view the pr E View, edit training images and create, add, remove, or delete the E Read-only actions in the project. Readers can't create or update t E View, edit projects and train the models, including the ability to p E Lets you read Cognitive Services data. Lets you perform detect, verify, identify, group, and find similar o E Provides access to create Immersive Reader sessions and call APIs Has access to Read and Test functions under Language portal Has access to all Read, Test, Write, Deploy and Delete functions u E Has access to all Read, Test, write, Deploy and Delete functions u E Has access to Read and Test functions under Language E Has access to Read and Test functions under LUIS.	BuiltinRole AI BuiltinRole No	+ Machine Learning Vii ne Vii		
Cognitive Services Custom Vision Cont Cognitive Services Custom Vision Depl Cognitive Services Custom Vision Depl Cognitive Services Custom Vision Read Cognitive Services Custom Vision Read Cognitive Services Custom Vision Trainer Cognitive Services Custom Vision Trainer Cognitive Services Data Reader (Previe Cognitive Services Immersive Reader U Cognitive Services Inguage Owner Cognitive Services Language Writer Cognitive Services LUIS Owner Cognitive Services LUIS Reader Cognitive Services LUIS Reader	Lets you create, read, update, delete and manage keys of Cognitis E Full access to the project, including the ability to view, create, edis E Publish, unpublish or export models. Deployment can view the pr E View, edit training images and create, add, remove, or delete the E Read-only actions in the project. Readers can't create or update t E View, edit projects and train the models, including the ability to p E Lets you read Cognitive Services data. Lets you perform detect, verify, identify, group, and find similar o E Provides access to create Immersive Reader sessions and call APIs Has access to all Read, Test, Write, Deploy and Delete functions u E Has access to all Read, Test, and Write functions under Language E Has access to Read and Test functions under LUIS. Has access to Read and Test functions under LUIS. E Has access to All Read, Test, and Write functions under LUIS E Full access to the project, including the system level configuration.	BuiltinRole AI BuiltinRole No	+ Machine Learning Vii - Machine Vii - Machine Learning Vii - Machine Vii - Machine Learning Vii - Machine Vii - Machine Learning Vii - M		
Cognitive Services Custom Vision Cont Cognitive Services Custom Vision Cont Cognitive Services Custom Vision Depl Cognitive Services Custom Vision Depl Cognitive Services Custom Vision Read Cognitive Services Custom Vision Trainer Cognitive Services Data Reader (Previe Cognitive Services Face Recognizer Cognitive Services Immersive Reader U Cognitive Services Language Owner Cognitive Services Language Writer Cognitive Services LUIS Owner Cognitive Services LUIS Owner Cognitive Services LUIS Writer Cognitive Services LUIS Writer Cognitive Services Metrics Advisor Ad Cognitive Services Metrics Advisor User	Lets you create, read, update, delete and manage keys of Cognitis E Full access to the project, including the ability to view, create, edis E Publish, unpublish or export models. Deployment can view the pr E View, edit training images and create, add, remove, or delete the E Read-only actions in the project. Readers can't create or update t E View, edit projects and train the models, including the ability to p E Lets you read Cognitive Services data. E Lets you perform detect, verify, identify, group, and find similar o E Provides access to create Immersive Reader sessions and call APIs Has access to all Read, Test, Write, Deploy and Delete functions u E Has access to all Read, Test, and Write functions under Language E Has access to Read and Test functions under LUIS. E Has access to Read and Test functions under LUIS. E Full access to the project, including the system level configuration. E Full access to the project, including the system level configuration.	BuiltinRole AI BuiltinRole No	+ Machine Learning Vii ne Vii + Machine Learning Vii - Machine Learning		
Cognitive Services Custom Vision Cont Cognitive Services Custom Vision Depl Cognitive Services Custom Vision Depl Cognitive Services Custom Vision Depl Cognitive Services Custom Vision Read Cognitive Services Custom Vision Trainer Cognitive Services Data Reader (Previe Cognitive Services Para Reader (Previe Cognitive Services Inmersive Reader U Cognitive Services Language Owner Cognitive Services Language Writer Cognitive Services Lulis Owner Cognitive Services LUIS Writer Cognitive Services LUIS Writer Cognitive Services Metrics Advisor Ad Cognitive Services Metrics Advisor User Cognitive Services Metrics Advisor User	Lets you create, read, update, delete and manage keys of Cognitis E Full access to the project, including the ability to view, create, edis E Publish, unpublish or export models. Deployment can view the pr E View, edit training images and create, add, remove, or delete the E Read-only actions in the project. Readers can't create or update t E View, edit projects and train the models, including the ability to p E Lets you read Cognitive Services data. Lets you perform detect, verify, identify, group, and find similar o E Provides access to create Immersive Reader sessions and call APIs Has access to all Read, Test, Write, Deploy and Delete functions u E Has access to all Read, Test, and Write functions under Language E Has access to Read and Test functions under LUIS. Has access to Read and Test functions under LUIS. E Has access to All Read, Test, and Write functions under LUIS E Full access to the project, including the system level configuration.	BuiltinRole AI BuiltinRole No BuiltinRole AI BuiltinRole AI	+ Machine Learning Vii - Machine Learning		

		Displ				Ob
RoleAssig nmentId	Scope	ayNa me	RoleDefinit ionName	RoleDefinitionId	ObjectId	jec tTy pe
3ddf8e6c-	/providors/Naioro	Deploy		/providors/NAisrosoft Aut	d46f61dd-	•
77e0-56fe-	/providers/Micro soft.Managemen	-	Monitoring	/providers/Microsoft.Aut horization/roleDefinitions	3bb0-4fbf-	Serv iceP
8272-	t/managementGr	AzActi	Contributor	/749f88d5-cbae-40b8-	af91-	rinci
1de3cfc86b 62	oups/myorg	vity- Log		bcfc-e573ddc772fa	75bca6710 509	pal
bae9bc8f-	/providors/Niero	Deploy		/providors/NAisrosoft Aut	d46f61dd-	Comi
1fb7-536b-	/providers/Micro soft.Managemen	-	Log Analytics	/providers/Microsoft.Aut horization/roleDefinitions	3bb0-4fbf-	Serv iceP
a5d3- 352b50b98	t/managementGr	AzActi	Contributor	/92aaf0da-9dab-42b6-	af91-	rinci
a56	oups/myorg	vity- Log		94a3-d43ce8d16293	75bca6710 509	pal
aec4006b-	/providers/Micro	Deploy		/providers/Microsoft.Aut	88d6a30a-	Serv
6bb1-54ae-	soft.Managemen	-		horization/roleDefinitions	9352-428b-	iceP
86c1- 9f37d10f70	t/managementGr	MDEn dpoint	Contributor	/b24988ac-6180-42a0-	b0a5- 60f256d9b	rinci
1 f	oups/myorg	dpoint s		ab88-20f7382dd24c	2e2	pal
84b46374- a84a-5435-	/providers/Micro	Deploy		/providers/Microsoft.Aut	190c4081- bca5-4c1f-	Serv
b4fa-	soft.Managemen	- MDFC-	Log Analytics	horization/roleDefinitions	9c02-	iceP
3e5e8b343	t/managementGr oups/myorg	Config	Contributor	/92aaf0da-9dab-42b6- 94a3-d43ce8d16293	d4758bab6	rinci pal
6da 0bff38e2-	oups,,o8	oo8		5 .us u .sscou_ss	ea7 190c4081-	μα.
2896-5b87-	/providers/Micro	Deploy		/providers/Microsoft.Aut	bca5-4c1f-	Serv
ac56-	soft.Managemen	- MDFC-	Contributor	horization/roleDefinitions/b24988ac-6180-42a0-	9c02-	iceP rinci
4939b3acb	t/managementGr oups/myorg	Config		ab88-20f7382dd24c	d4758bab6	pal
8fa aad22f3b-	7 7 6		Azure		ea7 190c4081-	
7860-592b-	/providers/Micro	Deploy	Kubernetes	/providers/Microsoft.Aut	bca5-4c1f-	Serv
8478-	soft.Managemen t/managementGr	- MDFC-	Service Policy	horization/roleDefinitions /18ed5180-3e48-46fd-	9c02-	iceP rinci
da0539df7f	oups/myorg	Config	Add-on	8541-4ea054d57064	d4758bab6	pal
e4 3e183228-	1 / / 3	Ü	Deployment		ea7 190c4081-	•
ff7d-5294-	/providers/Micro	Deploy		/providers/Microsoft.Aut	bca5-4c1f-	Serv
be28-	soft.Managemen t/managementGr	- MDFC-	Security Admin	horization/roleDefinitions/fb1c8493-542b-48eb-	9c02-	iceP rinci
1d3ca0e19c	oups/myorg	Config	, commi	b624-b4c8fea62acd	d4758bab6	pal
d8 d1871679-		_	Azure		ea7 190c4081-	
ef08-5cc9-	/providers/Micro	Deploy	Kubernetes	/providers/Microsoft.Aut	bca5-4c1f-	Serv
b620-	soft.Managemen t/managementGr	- MDFC-	Service	horization/roleDefinitions/ed7f3fbd-7b88-4dd4-	9c02-	iceP rinci
e50d2ffb29 02	oups/myorg	Config	Contributor Role	9017-9adb7ce333f8	d4758bab6 ea7	pal
28d1bbb2-			Role		539e542d-	
5a95-576b-	/providers/Micro soft.Managemen	Deploy		/providers/Microsoft.Aut horization/roleDefinitions	825d-4cb5-	Serv iceP
85de-	t/managementGr	- MDFC-	Contributor	/b24988ac-6180-42a0-	a43f-	rinci
98980838df bd	oups/myorg	OssDb		ab88-20f7382dd24c	42e1bd4f7 479	pal
5610687b-	/providers/Micro	Deploy		/providers/Microsoft.Aut	44809f8f-	Serv
b15b-5d48- bd61-	soft.Managemen	-	SQL Security	horization/roleDefinitions	bca6-423c- 9e26-	iceP
4408dc349	t/managementGr	MDFC-	Manager	/056cd41c-7e88-42e1-	7ab88ebbff	rinci
e44	oups/myorg	SqlAtp		933e-88ba6a50c9c3	28	pal
f41cafe7-	/providers/Micro	Deploy		/providers/Microsoft.Aut	888b69d8-	Serv
6f85-5086- 8ecd-	soft.Managemen	- Resour	Monitoring	horization/roleDefinitions	f1e2-4459- bcff-	iceP
f10c219a9f	t/managementGr	ce-	Contributor	/749f88d5-cbae-40b8-	0953f59c9b	rinci
ed	oups/myorg	Diag		bcfc-e573ddc772fa	19	pal
aeccabd7- b572-5fe2-	/providers/Micro	Deploy	Log Analytics Contributor	/providers/Microsoft.Aut horization/roleDefinitions	888b69d8- f1e2-4459-	Serv
n212-2167-	soft.Managemen	-	Contributor	ווטוזבמנוטוון וטופטפווווונוטחג	1167-4403-	iceP

b1ad- 659525941 097	t/managementGr oups/myorg	Resour ce- Diag		/92aaf0da-9dab-42b6- 94a3-d43ce8d16293	bcff- 0953f59c9b 19	rinci pal
17a099f4- cf89-58a8- b6ca- 0a673fbdd 4fe	/providers/Micro soft.Managemen t/managementGr oups/myorg	Deploy -VM- Monit oring	Log Analytics Contributor	/providers/Microsoft.Aut horization/roleDefinitions /92aaf0da-9dab-42b6- 94a3-d43ce8d16293	2b076c26- b45e-44be- 8ab9- 6c6b8d85d 7dc	Serv iceP rinci pal
55ffe1be- e389-5d46- 9488- 8d6915a8b 60e	/providers/Micro soft.Managemen t/managementGr oups/myorg	- VMSS- Monit oring	Log Analytics Contributor	/providers/Microsoft.Aut horization/roleDefinitions /92aaf0da-9dab-42b6- 94a3-d43ce8d16293	4cdac29d- 09e4-4292- ae0f- 1915174e9 741	Serv iceP rinci pal
1e6eb635- dc9a-54d5- 9bb5- 7506132bff 67	/providers/Micro soft.Managemen t/managementGr oups/myorg	- VMSS- Monit oring	Virtual Machine Contributor	/providers/Microsoft.Aut horization/roleDefinitions /9980e02c-c2be-4d73- 94e8-173b1dc7cf3c	4cdac29d- 09e4-4292- ae0f- 1915174e9 741	Serv iceP rinci pal
20b87dbc- 9b70-5379- ad61- 97a3ccecc9 27	/providers/Micro soft.Managemen t/managementGr oups/myorg	Enforc e- ACSB	Contributor	/providers/Microsoft.Aut horization/roleDefinitions /b24988ac-6180-42a0- ab88-20f7382dd24c	fe598c95- d45a-4119- 9d12- cd5a35e47f 7f	Serv iceP rinci pal