**Deploy Identity and access management using RBAC Template**

06/11/2024

**­­Documents Control**

Prepared For:

**Internal Only**

Prepared By:

**Nitin Kansara**

@cobweb.com

**Author**

|  |  |
| --- | --- |
| Author Name | Nitin Kansara |
| Email | Nitin.Kansara@cobweb.com |
| Telephone | +97144553135 |
| Web | [www.cobweb.com/ae](http://www.cobweb.com/ae) |
| Address | Cobweb Solutions Limited  Grosvenor Business Tower  Suite 1911  Barsha Heights  Dubai  P.O. Box 500449  United Arab Emirates |

**Document Validity**

|  |
| --- |
| Printed copy uncontrolled |

**Document History**

| **Version** | **Date** | **Revised By** | **Comments** |
| --- | --- | --- | --- |
| 1.0 | 06/11/2024 | Nitin Kansara | First Draft |
|  |  |  |  |

**Document Distribution**

| **Name** | **Title** | **Date of Issue** | **Version** |
| --- | --- | --- | --- |
|  |  | 06/11/2024 | 1.0 |
|  |  |  |  |

**Copyright & Confidentiality Notice**

*This document is Company Restricted and is not to be copied, distributed, stored, duplicated, or transmitted without the express written permission of Cobweb Solutions Limited Senior Management. All Trademarks are hereby acknowledged. All references to third party products, partners and existing Cobweb Solutions Limited clients should be considered as confidential and may not be distributed without Cobweb Solutions.*

Contents

[Introduction 4](#_Toc187314107)

[Define Roles and Permissions 4](#_Toc187314108)

[Global Admin 4](#_Toc187314109)

[RBAC template 6](#_Toc187314110)

[Considerations for RBAC in Landing Zone 7](#_Toc187314111)

[Steps to Deploy 7](#_Toc187314112)

# Introduction

The governance policies embedded within the template are essential for maintaining compliance and ensuring secure operations. These policies are implemented at various scopes, ensuring that all levels of the Azure environment adhere to the required guidelines. The template also integrates role-based access control (RBAC) to manage permissions effectively and assign roles to users, groups, or service principals. This setup enhances security by ensuring that access is appropriately granted and managed across the organization.

# Define Roles and Permissions

## Global Admin

Description: Full access to all resources and services in the Azure portal across subscriptions and management groups.

**Permissions:**

Management Group Level: Owner (full access to management group-level governance and operations tools).

Subscription Level: Owner (control over all resources within the subscription).

Resource Group Level: Owner (full administrative access).

Resource Level: Owner (full control over resources).

Azure Landing Zone Architect

Description: Responsible for the design and architecture of the Azure landing zone. Includes setting up the governance framework and initial configurations for subscriptions and policies.

**Permissions:**

Management Group Level: Contributor (can create and manage resources at the management group level).

Subscription Level: Contributor (able to create resources in a subscription).

Resource Group Level: Contributor (able to manage resources in the resource group).

Resource Level: Contributor (can modify resources but not delete or assign roles).

Azure Security Administrator

Description: Oversees the security and compliance aspects of the landing zone, including setting up policies, security controls, and access management.

**Permissions:**

Management Group Level: Security Administrator (access to security-related tools and resources).

Subscription Level: Security Administrator (can configure security policies at the subscription level).

Resource Group Level: Security Administrator (manage security controls for the resource group).

Resource Level: Reader (view-only access to resources, can check configurations without modifying them).

Azure Operations Manager

Description: Manages monitoring, automation, and operational tools in the landing zone, such as Azure Monitor, Azure Automation, and Log Analytics.

**Permissions:**

Management Group Level: Contributor (ability to configure and manage resources within the management group).

Subscription Level: Contributor (manage operational resources and monitoring settings).

Resource Group Level: Contributor (manage operational configurations).

Resource Level: Contributor (create and configure monitoring tools).

Azure Networking Administrator

Description: Manages all aspects related to networking within the landing zone, including virtual networks, network security groups, VPNs, etc.

**Permissions:**

Management Group Level: Contributor (can configure network-related resources at the management group level).

Subscription Level: Network Contributor (permissions to manage network resources such as VNets, subnets).

Resource Group Level: Network Contributor (manage resources like network interfaces, VPNs).

Resource Level: Network Contributor (can modify individual network resources).

Azure Cost Management and Billing Administrator

Description: Manages cost controls, budgets, and resource usage to optimize the Azure environment's financial health.

**Permissions:**

Management Group Level: Cost Management Contributor (view cost management data and reports).

Subscription Level: Billing Reader (can view billing details).

Resource Group Level: Reader (view resource usage and cost breakdowns).

Resource Level: Reader (view cost data at the resource level).

Azure Compliance Officer

Description: Ensures that the landing zone complies with internal and external regulations, including privacy laws and industry standards.

**Permissions:**

Management Group Level: Policy Contributor (can define and enforce policies and compliance controls at the management group level).

Subscription Level: Policy Contributor (can enforce subscription-level compliance policies).

Resource Group Level: Reader (can view compliance status but not modify configurations).

Resource Level: Reader (view compliance state and reports).

Azure Reader

Description: Read-only access for users who only need to view resources without making any changes.

**Permissions:**

Management Group Level: Reader (read-only access to the entire management group).

Subscription Level: Reader (can only view resources in the subscription).

Resource Group Level: Reader (view resources within resource groups).

Resource Level: Reader (view individual resources).

Azure Support Operator

Description: Responsible for escalating and managing support requests related to the landing zone.

**Permissions:**

Management Group Level: Reader (view-only access).

Subscription Level: Reader (view-only access).

Resource Group Level: Reader (can view resource configurations)

# RBAC template

|  |
| --- |
| JSON |
| *{*  *"roleAssignments": [*  *{*  *"role": "Owner",*  *"scope": "/subscriptions/{subscriptionId}",*  *"principal": "Global Admin"*  *},*  *{*  *"role": "Contributor",*  *"scope": "/subscriptions/{subscriptionId}",*  *"principal": "Azure Landing Zone Architect"*  *},*  *{*  *"role": "Security Administrator",*  *"scope": "/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}",*  *"principal": "Azure Security Administrator"*  *},*  *{*  *"role": "Contributor",*  *"scope": "/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}",*  *"principal": "Azure Operations Manager"*  *},*  *{*  *"role": "Network Contributor",*  *"scope": "/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}",*  *"principal": "Azure Networking Administrator"*  *},*  *{*  *"role": "Cost Management Contributor",*  *"scope": "/subscriptions/{subscriptionId}",*  *"principal": "Azure Cost Management and Billing Administrator"*  *},*  *{*  *"role": "Policy Contributor",*  *"scope": "/subscriptions/{subscriptionId}",*  *"principal": "Azure Compliance Officer"*  *},*  *{*  *"role": "Reader",*  *"scope": "/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}",*  *"principal": "Azure Reader"*  *},*  *{*  *"role": "Reader",*  *"scope": "/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}",*  *"principal": "Azure Support Operator"*  *}*  *]*  *}* |

# Considerations for RBAC in Landing Zone

1. Ensure that each role is assigned with the minimum permissions required for the user to perform their tasks, following the principle of **least privilege**.
2. Use **management groups** to apply governance controls across multiple subscriptions.
3. Use **Azure Policies** and **Blueprints** to enforce compliance and consistent configurations across the landing zone.
4. Regularly review and audit RBAC assignments to ensure access is granted only to those who need it.
5. Use **Azure AD Conditional Access** to enforce additional security measures based on user context and environment.

By implementing the RBAC structure in this manner, your Azure landing zone will be better secured, optimized for operational efficiency, and ready for compliance.

## Steps to Deploy

1. **Prerequisites**

* **Azure Subscription**: Ensure you have an active Azure subscription.
* **Azure CLI or Azure PowerShell**: Install Azure CLI or Azure PowerShell locally, or use the Azure Cloud Shell available in the Azure portal.
* **Access**: Ensure you have the necessary permissions to deploy resources in the chosen Azure subscription and resource group.

1. **Save the Template**
2. Copy the ARM template into a JSON file, e.g., vnet-template.json.
3. **Modify Parameters (Optional)**
4. Open the JSON file and adjust default parameter values if needed (e.g., location, address prefixes, etc.).
5. Alternatively, you can create a separate parameters.json file to provide parameter overrides during deployment. For example:

|  |
| --- |
| JSON |
| *{*  *"$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentParameters.json#",*  *"contentVersion": "1.0.0.0",*  *"parameters": {*  *"architectureType": {*  *"value": "SingleVNet"*  *},*  *"location": {*  *"value": "westus2"*  *},*  *"vnetAddressPrefix": {*  *"value": "10.0.0.0/16"*  *},*  *"subnetPrefix": {*  *"value": ["10.0.1.0/24", "10.0.2.0/24"]*  *}*  *}*  *}* |

1. **Deploy the Template**

You can deploy the ARM template using either the Azure Portal, Azure CLI, or PowerShell.

**Option 1: Deploy via Azure Portal**

1. Log in to the [Azure Portal](https://portal.azure.com).
2. Navigate to **"Deploy a custom template"**:
   * Search for "Template deployment" in the portal search bar.
   * Click on **"Create"** or **"Build your own template in the editor"**.
3. Upload the ALZ-RBAC.json file or paste its content into the editor.
4. Specify the parameters (e.g., architecture type, location) in the portal.
5. Click **Review + Create**, then **Create**.

**Option 2: Deploy via Azure CLI**

**Using Azure CLI**:

|  |
| --- |
| Bash |
| *az role definition create --role-definition @customRole.json*  *az role assignment create --assignee {user-object-id} --role "VM Manager" --scope "/subscriptions/{subscription-id}/resourceGroups/{resource-group-name}"* |

**Using PowerShell**:

|  |
| --- |
| Template |
| *New-AzRoleDefinition -InputFile "customRole.json"*  *New-AzRoleAssignment -ObjectId "<user-object-id>" -RoleDefinitionName "VM Manager" -Scope "/subscriptions/{subscription-id}/resourceGroups/{resource-group-name}"* |

1. **Verify Deployment**

* Navigate to the Azure Portal and open the RBAC permission at the subscription / resource / management group level.
* Confirm that the created custom roles are created and associated resources.