

Azure Enterprise-Scale / PCF V2

Low Level Design Document

# Contents

## Table of Contents

[1. Contents 2](#_Toc127876948)

[1.1. Table of Contents 2](#_Toc127876949)

[2. Document Control 4](#_Toc127876950)

[2.1. Document Information 4](#_Toc127876951)

[2.2. Distribution List 5](#_Toc127876952)

[2.3. Supporting Documents 5](#_Toc127876953)

[3. Exec Summary 5](#_Toc127876954)

[3.1. Overview 5](#_Toc127876955)

[3.2. Purpose 5](#_Toc127876956)

[3.3. Audience 5](#_Toc127876957)

[4. In Scope – Out scope of HaCT & Application Team 5](#_Toc127876958)

[4.1. Responsibility assignment matri6](#_Toc127876959)

[4.2. AD Group creation & Role Assignment 6](#_Toc127876960)

[4.3. Access and Approval for App Team members 6](#_Toc127876961)

[4.4. Creation/Deletion new AD Group 7](#_Toc127876962)

[4.5. Role Assignment 7](#_Toc127876963)

[4.6. Custom Role Creation 7](#_Toc127876964)

[5. Role Based Access Control 8](#_Toc127876965)

[6. AS-IS Architecture 8](#_Toc127876966)

[6.1. Azure Enterprise Scale@Uniper Architecture 8](#_Toc127876967)

[6.2. Azure Enterprise Scale@Uniper – HaCT Cloud Engineer RBAC Architecture 9](#_Toc127876968)

[6.3. Azure Enterprise Scale@Uniper – Application Team RBAC Architecture 9](#_Toc127876969)

[7. Application Team – AD Group Naming Convention 10](#_Toc127876970)

[7.1. How are Security AD Groups created? 10](#_Toc127876971)

[7.2. Naming Convention 10](#_Toc127876972)

[8. Default Authorization – Application Team 11](#_Toc127876973)

[8.1. RBAC – Application Team 11](#_Toc127876974)

[8.2. Azure AD Group Ownership and Membership 11](#_Toc127876975)

[9. Application Team - Role Based Access Control 12](#_Toc127876976)

[9.1. Application Support Engineers Default Access 12](#_Toc127876977)

[9.1.1. Lower Environment – DEV/SANDBOX 12](#_Toc127876978)

[9.1.2. Upper Environment – UAT/PROD 12](#_Toc127876979)

[10. Default Authorization – HaCT Team 13](#_Toc127876980)

[10.1. HaCT – Cloud Engineer – Default Access 13](#_Toc127876981)

[10.2. HaCT – Cloud Engineer - Role Specific Access 14](#_Toc127876982)

[10.3. HaCT – Automation Service Principal - Role Specific Access 15](#_Toc127876983)

[10.4. Azure AD Role – HaCT Security and IAM Team 15](#_Toc127876984)

[10.5. Approval Workflow 15](#_Toc127876985)

[11. Permission – Azure RBAC for PCFv2 16](#_Toc127876986)

[11.1. Permission Details of role 16](#_Toc127876987)

[11.1.1. Reader-Permissions 17](#_Toc127876988)

[11.1.2. Contributor - Permissions 17](#_Toc127876989)

[11.1.3. User Access Administrator -Permissions 17](#_Toc127876990)

[11.1.4. Support Request Contributor-Permissions 17](#_Toc127876991)

[11.1.5. Storage Blob Data Reader-Permissions 17](#_Toc127876992)

[11.1.6. Resource Policy Contributor-Permissions 18](#_Toc127876993)

[11.1.7. Network Contributor-Permissions 18](#_Toc127876994)

[11.1.8. Monitoring Contributor-Permissions 18](#_Toc127876995)

[12. Monitoring and Management 19](#_Toc127876996)

[12.1. Alerts on Critical role assignment 19](#_Toc127876997)

[12.1.1. Alert Rule 19](#_Toc127876998)

[12.1.2. Action Group 19](#_Toc127876999)

[12.1.3. Resource Group 19](#_Toc127877000)

[12.2. Alerts on creation of new custom role 19](#_Toc127877001)

[12.2.1. Alert Rule 19](#_Toc127877002)

[12.2.2. Action Group 19](#_Toc127877003)

[12.2.3. Resource Group 19](#_Toc127877004)

[12.3. Deployment alerts 19](#_Toc127877005)

[12.3.1. Alert Rule 19](#_Toc127877006)

[12.3.2. Action Group 20](#_Toc127877007)

[12.3.3. Resource Group 20](#_Toc127877008)

[13. Emergency Break-Glass account 20](#_Toc127877009)

[13.1. Introduction 20](#_Toc127877010)

[13.2. AS-IS – Break-Glass account Architecture 20](#_Toc127877011)

[13.3. Access – Emergency Break-Glass account 21](#_Toc127877012)

[13.3.1. Account Configuration 21](#_Toc127877013)

[13.4. SMEs: Who They Are and How to Contact Them 21](#_Toc127877014)

[13.5. Validation – Break Glass account 22](#_Toc127877015)

[14. Back-Up Plan 22](#_Toc127877016)

[14.1. Role Assignment of Application Team 22](#_Toc127877017)

[14.1.1. Purpose 22](#_Toc127877018)

[14.1.2. Technical Details 22](#_Toc127877019)

[14.1.3. Azure Resources 22](#_Toc127877020)

[14.1.4. Scheduler/Pipeline Trigger Details 22](#_Toc127877021)

[14.1.5. Service Principal details 23](#_Toc127877022)

[14.1.6. Service Principal Azure RBAC Permissions 23](#_Toc127877023)

[14.1.7. Service Principal Azure AD API Permissions 23](#_Toc127877024)

[14.2. Membership of AD group of Application Team 23](#_Toc127877025)

[14.2.1. Purpose 23](#_Toc127877026)

[14.2.2. Technical Details 23](#_Toc127877027)

[14.2.3. Azure Resources 23](#_Toc127877028)

[14.2.4. Scheduler/Pipeline Trigger Details 23](#_Toc127877029)

[14.2.5. Service Principal Details 24](#_Toc127877030)

[14.2.6. Service Principal Azure RBAC Permissions 24](#_Toc127877031)

[14.2.7. Service Principal Azure AD API Permissions 24](#_Toc127877032)

[15. Security - Microsoft Defender for Cloud 24](#_Toc127877033)

[15.1. Policies and Initiatives 24](#_Toc127877034)

[15.1.1. Guest account permission on azure resources 24](#_Toc127877035)

[15.1.2. Audit for compliance of minimum TLS version 25](#_Toc127877036)

[15.1.3. Security features – Storage Account 25](#_Toc127877037)

[15.1.4. Network Policy 25](#_Toc127877038)

[15.1.5. SQL Policy Initiatives 26](#_Toc127877039)

[15.1.6. KeyVault - Policy Initiatives 26](#_Toc127877040)

[16. Disclaimer and Important notes 26](#_Toc127877041)

[Appendix – A Glossary 27](#_Toc127877042)

# Document Control

## Document Information

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Version | Name | Role | Comments |
| 02/05/2023 | 0.1 | Shobana Jayabalan | AKS Admin |  |
| 15/03/2023 | 1.0 | Shobana Jayabalan | AKS Admin |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table 1: Document Information

## Distribution List

|  |  |  |
| --- | --- | --- |
| Distributed to | Role | Company |
|  | Cloud Security Architect | UNIPER |
|  |  |  |
|  |  |  |
|  |  |  |

Table 2: Distribution List

## Supporting Documents

|  |  |
| --- | --- |
| **Document Name** | **Version** |
| Azure Enterprise-Scale / PCF V2  High Level Design Document | Version 1.0 |

Table 3: Supporting Documents

# Exec Summary

## Overview

Uniper has Azure AD at present, which is synced with On-Premises active directory. RBAC is an authorisation system built on Azure Resource Manager that provides fine-grained access management of Azure resources. Using RBAC, you can restrict access based on the need to know and least privilege security principles. Access management for cloud resources is a critical function for UNIPER when using cloud services.

Role-based access control provides each worker privileges based on what role they have in the organization.

## Purpose

This LLD documents covers RBAC requirements, detailed RBAC structure, RBAC configurations and maintenance of these RBAC infrastructure with respect to AKS which will be deployed in Enterprise Scale@Uniper, its management groups and landing zone subscriptions.

## Audience

The intended audience for this document will be UNIPER architects and UNIPER Enterprise Scale@Uniper project management.

# In Scope – Out scope of HaCT & Application Team

## RACI Matrix for Landing Zone subscriptions

|  |  |  |
| --- | --- | --- |
| **R = Responsibilities A = Accountable C = Consulted I = Informed** | **Application Team** | **HaCT Cloud Engineer** |
| Requesting for new AD group creation other than default | R, A |  |
| Create of role assignment other than default | R, A | C, I |
| Deletion of role assignment other than default | R, A | C, I |
| Access for Application member | R, A |  |
| Process of Approval flow | R, A |  |
| Custom role binding | R,A,C | I |
| Excluding/Exemption of Policy | C, I | R, A |

Table 4: Responsibility assignment matrix

## AD Group creation & Role Assignment

|  |
| --- |
| **HaCT Responsibilities** |
| 1. HaCT Team will be creating AD Group and performing default role assignments to Application Team on their ordered subscription.(only suggestions by AKS team and changes as per over time )  If in case application team needs any AD – reach Ad team |
|  |
|  |

Table 5: In/Out Scope - AD Group creation and Role Assignment

## Access and Approval for App Team members

|  |  |
| --- | --- |
| **Responsibilities** | |
| **Application Team** | **HaCT Team** |
| Application Manager is responsible to grant access to Application Team member on the required subscription  Grant/Revoke access to Application team must be taken care by Application Manager.  Application Managers must assess permitted users and give application team members access. | HaCT Team will be creating the default AD Groups with access on the subscriptions ([section 7.2.](#_Naming_Convention)), assign App Manager as Owner of AD Groups of Contributor and Reader ad group & Member of Reader AD Group ([section 8.2.](#_Azure_AD_Group)). Will share the details to App Manager. |

Table 6: In/Out Scope - Access for App Team members

## Creation/Deletion new AD Group

|  |  |
| --- | --- |
| **Responsibilities** | |
| **Application Team** | **HaCT Team** |
| Application Team needs to contact the UNIPER Directory Service team. Catalog to place request using SNOW link - [Directory Service - Manage Active Directory groups](https://uniperprod.service-now.com.mcas.ms/unipersp?id=sc_cat_item_uni&sys_id=fc3fe7ab8742d5d0fc79c9d30cbb35f5) | HaCT is not responsible for creating the AD Group for Enterprise Scale@Uniper except for the default AD Groups. |
| AD Group should be Security type with proper description. | HaCT team will be removing the role assignment of other AD Group type role assignment except Security type ad groups |
| Addition/Removal of Members into the AD Group should be taken care by Application Team or via UNIPER Directory Service team. |  |

Table 7: In/Out Scope - Creation/Deletion new AD Group

## Role Assignment

|  |  |
| --- | --- |
| **Responsibilities** | |
| **Application Team** | **HaCT Team** |
| App Team's responsible to perform the role assignment for themselves on-demand | HaCT Team will be working on to identify other critical roles. If HaCT identifies Critical role, it will get appended to the list. |
| Application team are requested to use the Least privilege principle and perform the role assignment. Recommendation from HaCT is to check resource specific role and assign what is required to perform the activity.  We request that Application Team in roles that have critical/high privilege access, such as "Owner," "User Access Administrator," and "Resource Policy Contributor," refrain from using them across ESLZ subscriptions, resource groups, and resources. | If in case mentioned role assignments are identified during audit process, HaCT Team will removing immediately |
|  | On noticing role assignments apart from Reader for Application team members in PROD subscription, HaCT Team will be removing the respective role assignment. |

# Default Roles and responsibilities - managed containers

| **Role name** | **Description** | Responsibilities |
| --- | --- | --- |
| Cluster administrator | The cluster administrator role is assigned to the Cloud Management Center.  It creates and manages the AKS clusters. | * Fulfillment of container requests * Monitoring of cluster health * Upgrades and Patching (cluster, node pools, ingress controller, Kured daemon, Kubecost dashboard) * Resource management on cluster level * Namespace creation and namespace administrator assignment * Azure Security Policies and exceptions * Node pool creation and management * Management of system namespaces of cluster |
| Namespace administrator | The namespace administrator role is assigned to an application team.  It manages a namespace inside an AKS cluster. | * Monitor namespace and applications inside the namespace * Upgrades and patching of containers inside the namespace * Resource management on namespace level * Deployment of applications into cluster * Namespace Network policies * Testing cluster upgrades * Define and manage additional roles inside a namespace |
| Developer | The namespace administrator can define additional roles inside a cluster.  The developer role is an example of a role that could be defined. | * These depend completely on the role definition by the namespace administrator but cannot exceed it |

Customized RBAC witinin cluster :

Application can create their own custmozized RBAC

Pre-requisiste – Namespace Admin should create

Table 8: In/Out Scope - Role Assignment

## Custom Role Creation

|  |  |
| --- | --- |
| **Responsibilities** | |
| **Application Team** | **HaCT Team** |
| Not to create custom role, in most of the use case Contributor access will be sufficient for SPN to deploy/create/modify/update/delete. | When App team creates custom role, Custom role is also will be removed. App Team must place consultation call with HaCT Security & IAM team. In case of valid business justification, Post Service Owner, Application Team will be allowed to create custom role. |
| In case of custom role, request you to take consultation call with HaCT Security & IAM Team |  |

Table 9: In/Out Scope - Custom Role creation within cluster

# Role Based Access Control in Kubernetes

Role-based access control provides each application team member/HaCT Cloud Engineer privileges based on what role they have in the organization.

Hact Managed containers has been integrated with Azure Active Directory (AD) which helps customers to manage access to kubernetes resources based on existing identity and group membership. Your existing Azure AD users and groups can be provided access to AKS resources and with an integrated sign-on experience.

Kubernetes RBAC provides granular filtering of user actions. With this control mechanism:

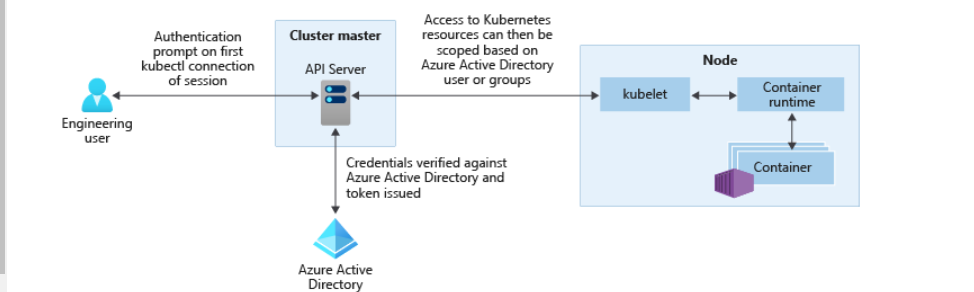
Assign users or user groups permission to create and modify resources or view logs from running application workloads.

Limit scope permissions to a single namespace or across the entire AKS cluster.

Create roles to define permissions, and then assign those roles to users with role bindings.

# AS-IS Architecture

## Azure Enterprise Scale@Uniper Architecture

  
Figure 1: ES@Uniper Architecture

Ref: <https://learn.microsoft.com/en-us/azure/aks/concepts-identity>

Figure 2: ES@Uniper - HaCT Cloud Engineer Access

## Azure Enterprise Scale@Uniper – Application Team RBAC Architecture

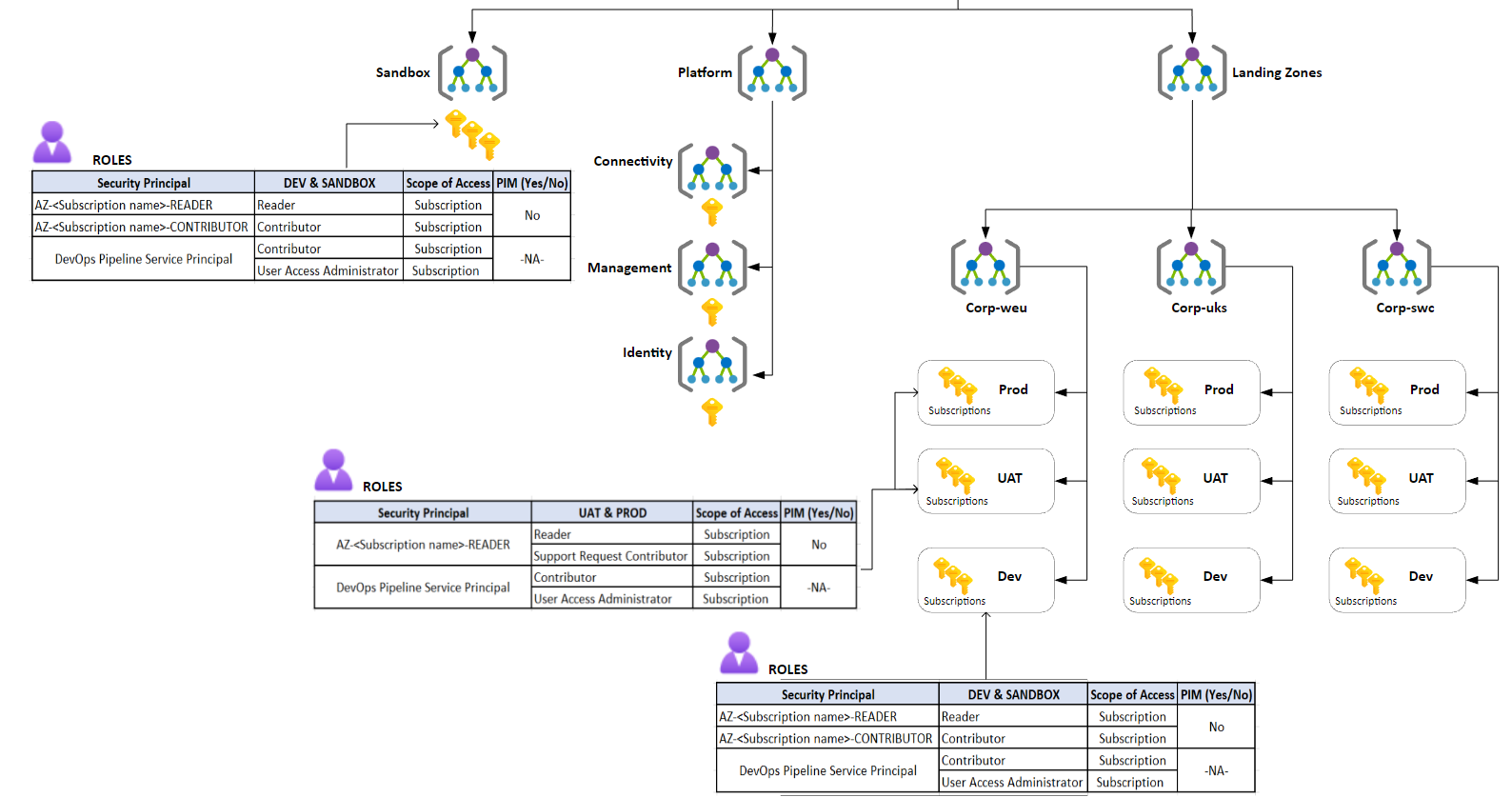


Figure 3: ES@Uniper - Application Team Access

Remark: Detailed explanation regarding the default role is provided under the [section 9](#_Application_Team_-).

# Application Team – AD Group Naming Convention

## How are Security AD Groups created?

## Naming Convention of POrtal access

Application Owners and Team Members order subscriptions by submitting requests to create subscriptions using catalogue services.

During the process of deployment of Subscriptions via IaC \*, respective AD Groups are created with the standard naming convention pattern and Application Managers are assigned as Owners/Member of AD Groups.

Remarks: \* Owned/Supported HaCT Automation Team

Detailed explanation about IaC will be covered in Low level design of HaCT Platform automation

AD Group creation and Role Assignment for application team are automated.

## Naming Convention of namespace access

PCFv2 security AD group convention pattern is used.

AZ- PCFv2-CORP-DEV-C\_MA3-DTFU081-01- READER

|  |  |  |
| --- | --- | --- |
| Azure | Subscription Name | Role Name |

* AZ-<Subscription name>-READER
* AZ-<Subscription name>-CONTRIBUTOR

Example : AZ-F\_OI3-B4-HaCT-AKS-PAAS-PREPROD-Reader

# Default Authorization – Application Team

Table 10: App Team - Default Role Description

## Azure AD Group Ownership and Membership

During the deployment of subscription and its respective AD groups, Application Manager will be configured as Owner of Reader and Contributor ad groups.

|  |  |  |
| --- | --- | --- |
|  | **Reader - AD Group** | **Contributor - AD Group** |
| ***Owner*** | App Manager | App Manager |
| ***Member*** | App Manager, \* | \* |

Table 11: AAD Group Member and Owner

**\***Application Manager can add his application team members into the AD Groups depending on the requirement.

# Application Team - Role Based Access Control

AAD groups and SPNs created during subscription deployment using IaC supported by the HaCT Automation Team which will enable application team members to access the application. The table below provides information about the role and scope of each AAD group and SPN created.

## Application Support Engineers Default Access

### Lower Environment – DEV/SANDBOX

|  |  |  |  |
| --- | --- | --- | --- |
| **Security Principal** | **DEV & SANDBOX** | **Scope of Access** | **PIM (Yes/No)** |
| AZ-<Subscription name>-READER | Reader | Subscription | No |
| AZ-<Subscription name>-CONTRIBUTOR | Contributor | Subscription |
| DevOps Pipeline Service Principal | Contributor | Subscription | -NA- |
| User Access Administrator | Subscription |

Table 12: Application Team Access - Lower Environment

**Business Justification/Reason of above role assignments:**

* Contributor access granted to application users and service principals to deployment of resources.
* UAM access is assigned to Application SP to create/delete the role assignments to Application team members and SPs.
* PIM is not implemented for Application team members in Lower environment

### Upper Environment – UAT/PROD

|  |  |  |  |
| --- | --- | --- | --- |
| **Security Principal** | **UAT & PROD** | **Scope of Access** | **PIM (Yes/No)** |
| AZ-<Subscription name>-READER | Reader | Subscription | No |
| Support Request Contributor | Subscription |
| DevOps Pipeline Service Principal | Contributor | Subscription | -NA- |
| User Access Administrator | Subscription |

1.Naming convention of cluster

The naming convention of cluster is as follows .

{type of resource}-{subscription purpose}-{region}-{instance}

Ex: AKS-data asset-dev-01

2. AD group naming convention

CLUSTER AD Group – Azure Portal Access

AZ-              cmcaks-pre-001-           76987-                                           DEV-                  AKSClusterUserRole

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Azure | Cluster Name | EAMID | Environment | Role Name |

AD Group – Namespace access

AZ-              data-asset-inventory-             76987-                                           DEV-             NameSpaceAdmin

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Azure | Namespace Name | EAMID | Environment | Role Name |

3.Vnet and Subnet naming convention

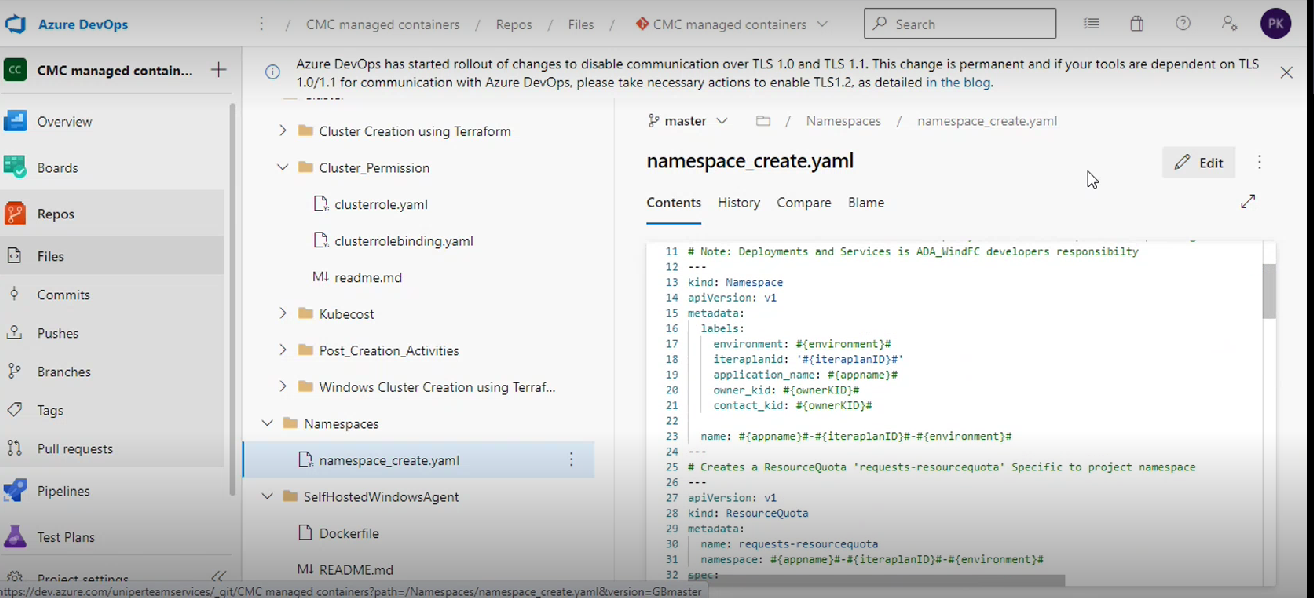
|  |  |  |
| --- | --- | --- |
| Asset Type | Scope | Format and examples |
| **Virtual network** | Resource group | *vnet-<subscription purpose>-<region>-<###>* |
|  |
| vnet-data asset-eastus2-001 |
| vnet-cmc-dev-001 |
| vnet-fuse-prd-001 |
| **Subnet** | Virtual network | *snet-<subscription purpose>-<region>-<###>* |
| snet-shared-dev-001 |
| snet-prod-prd-001 |
| snet-client-int-001 |
| **Load balancer** | Resource group | *lb-<app name or role>-<environment>-<###>* |
| lb-data asset-prod-001 |
| lb-cmc-dev-001 |

4. RBAC within the cluster

We have access two types of access.

1.Namespace level

We have a pipeline defined in our cmc managed containers to create namespace as below.

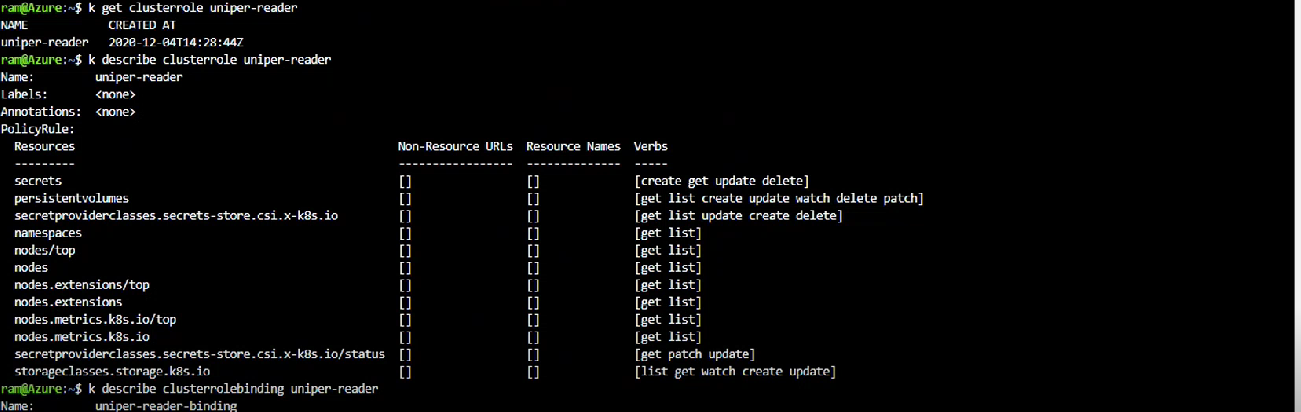


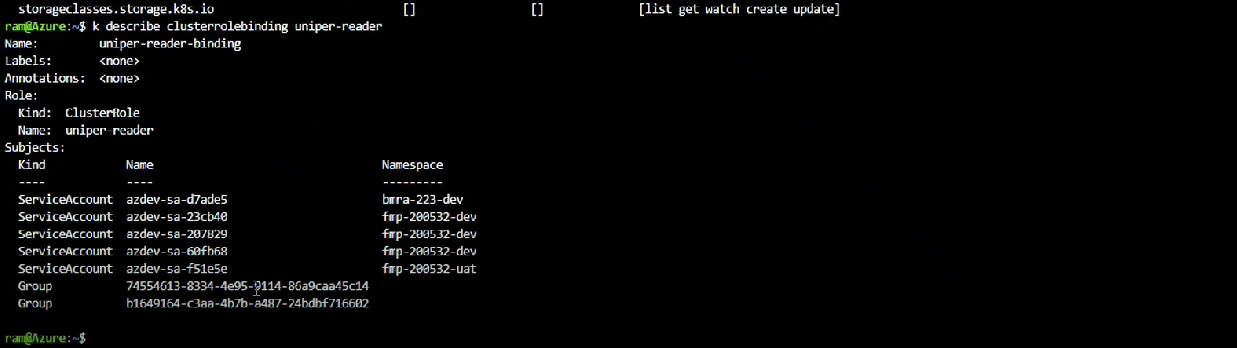
• It will create namespace , resource quota, role and rolebinding.

• Owner of that group have admin access they give permissions to the namespace.

2. Cluster level

We have one cluster role called uuniper reader.The people who are part the below group they can read the below resoucres.





6.Policies

Policies applied in cmc managed clusters are listed below and application team can refer this for policy assignments .

[AKS\_Policies](https://uniper-my.sharepoint.com/personal/n01187_uniper_energy/Documents/Microsoft%20Teams%20Chat%20Files/AKS_Policies.xlsx?web=1)

7. Log Analytics workspace

8. Upgrade/Patch of cluster on regular basis

Minor Upgrade is performed on quarterly basis followed by poc, pre and prd cluster .

Patch update is performed in an automated manner and we recommend the same in new clusters .

* As per this Wiki page [AKS Upgrade Communication Procedure](https://wiki.intranet.uniper.energy/sales/display/CF/AKS+Upgrade+Communication+Procedure) need to do upgrade AKS.
* Upgrade needs to be performed sequentially. It needs to be 1.19.x to 1.20.x to 1.21.x
* Every 3 months we need to upgrade AKS Cluster.
* Need to raise ticket with Microsoft team request for dedicated person during our upgradation process.

9. Monitoring of cluster

At present we have Kubecost , Prometheus installed in our cmc managed clusters and application team can make use of the same to implement the features .

Kubecost Installation reference to WIKI as below

[A Guide to Install Kubecost - Hosting Framework - Uniper Wiki](https://wiki.intranet.uniper.energy/sales/display/CF/A+Guide+to+Install+Kubecost)

Prometheus Installation reference to WIKI as below

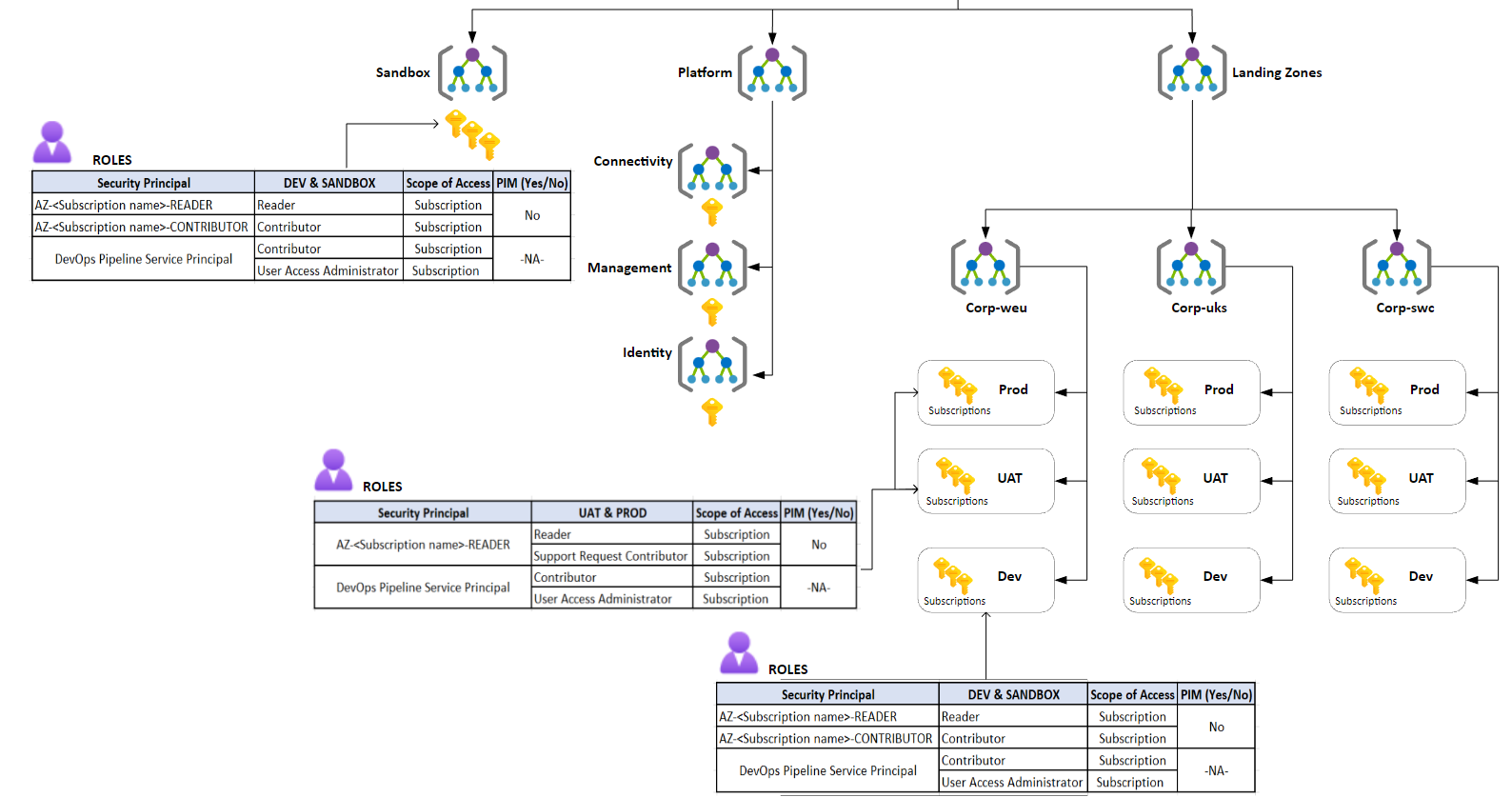
[A Guide to use Prometheus - Hosting Framework - Uniper Wiki](https://wiki.intranet.uniper.energy/sales/display/CF/A+Guide+to+use+Prometheus)

10.Introduction

Application team are assigned with Contributor access and they have permission to spin a new cluster and create role and role bindings

11.Resource Group

Application team should maintain separate RG for cluster creation .



Header name - Azure Enterprise Scale@Uniper – Application Team RBAC Architecture