**ELC (Estée Lauder Companies) – Azure Network Security - Proof of Concept (POC)**

**Submitted to**

Text, logo

Description automatically generated

**By**

A logo with colorful dots

Description automatically generated

**Wipro Technologies**

**23-02-2024**

**Revision History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date of Revision** | **Description of Change** | **Reason for Change** | **Reviewed By** |
| 1.1 |  | Initial Draft | NA | Siva |
|  |  |  |  |  |
|  |  |  |  |  |

**Author/Reviewer/Approvals**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Designation** | **Responsibility** | **Date** |
| Siva Rami Reddy | Wipro Cloud Security Engineer | Author |  |
| Kannan Kuppusamy | Wipro Project Manager | Review and Approval |  |
| Felix Jebamani | Wipro Architects | Review and Approval |  |
| Jamshid Abedi | ELC ED, Global Head of Security Engineer | Review and Approval |  |

Table of Contents

[1) Executive Summary 3](#_Toc159613701)

[2) Problem Statement without PIM in Service Principles 3](#_Toc159613702)

[3) Resolution with Azure DevOps – PIM 3](#_Toc159613703)

[3.1 Steps to Create a CI/CD Pipeline Using Privileged Identity Management. 3](#_Toc159613704)

[4) HLD Architecture Diagram 8](#_Toc159613705)

[5) Service Principle in Azure & Service Principle in Azure DevOps 8](#_Toc159613706)

[5.1 Steps to create the Service Principle in Azure and Azure DevOps 9](#_Toc159613707)

[6) PIM Introduction 12](#_Toc159613708)

[6.1 Steps to Create a PIM for Azure DevOps Pipeline 12](#_Toc159613709)

# **Executive Summary**

Privileged Identity Management (PIM) is a service in Azure Active Directory (Azure AD) that enables users to manage, control, and monitor access to important resources in an organization. Azure DevOps is a key resource for any organization as it stores Application Lifecycle Management artifacts (code, work item, pipelines, packages, test data etc.) of an organization.

# **Problem Statement without PIM in Service Principles**

Access with Full privilege shouldn't be available to anyone and forever. Access needs to be enabled on a need basis for certain periods. This presentation is prepared to enable the Project collection access for users in Azure DevOps with PIM, access would be granted in aligned with Azure PIM standards and controls.

# **Resolution with Azure DevOps – PIM**

Deploy the Azure infrastructure through a CI/CD workflow with ARM templates. CI/CD authenticates with a service principle. We often deploy resource-group-wide or subscription-wide deployments which require Owner or Contributor permissions to apply ARM templates. Controlling the DevOps pipeline with PIM both through the CLI and service principles PIM will check the approval required to execute the pipeline through the automation.

## Steps to Create a CI/CD Pipeline Using Privileged Identity Management.

1. Login into <https://dev.azure.com/>
2. Create New Organization and new private project.

**A screenshot of a computer

Description automatically generated**

1. Create a new repository and push the source code files and folders into Azure Repos.

**A screenshot of a computer

Description automatically generated**

1. Create a new CI/CD pipeline and click on releases pipeline.

A person sitting at a desk with a dog and a computer

Description automatically generated

1. Click on new option for to create the release pipeline.

A screenshot of a computer

Description automatically generated

1. Rename the pipeline name as per organization standards.

**A screenshot of a computer

Description automatically generated**

1. Please add the tasks templates as per below image to deploy the pipeline.

**A screenshot of a computer

Description automatically generated**

1. Add the below templates to the release pipeline.

**A screenshot of a computer

Description automatically generated**

1. Please save the pipeline and click on create the release pipeline.

**A screenshot of a computer

Description automatically generated**

1. Deployment is done and click on logs to check the errors.

**A screenshot of a computer

Description automatically generated**

# **HLD Architecture Diagram**

**A diagram of a computer application

Description automatically generated**

# **Service Principle in Azure & Service Principle in Azure DevOps**

Azure service principal is a security identity used by user-created apps, services, and automation tools to access specific Azure resources. Think of it as a 'user identity' (login and password or certificate) with a specific role, and tightly controlled permissions to access your resources. It only needs to be able to do specific things, unlike a general user identity. It improves security if you only grant it the minimum permissions level needed to perform its management tasks.

To make the integration between Azure Pipelines and Azure cloud, we need to setup what is called service connection. there are multiple service connections available on Azure DevOps, but for our purpose we are talking about the Azure Resource Manager (ARM) Service Connection. We need Service principal details from azure like Client ID, App ID, Tenant ID, to establish a connection from Azure DevOps Pipelines to Azure.

## Steps to create the Service Principle in Azure and Azure DevOps

1. Login into Azure Portal <https://portal.azure.com/>
2. Click on Azure Cloud Shell and execute the command “az ad sp create-for-rbac -n “your app name” ”.

**A screenshot of a computer

Description automatically generated**

1. Copy and paste all the Credentials at one place.

**A black screen with yellow and blue text

Description automatically generated**

1. Open azure devops portal and select the project to create the service principle to establish a service connection between azure devops and azure portal.

**A screenshot of a computer

Description automatically generated**

1. Click on service connection under the project settings.

**A screenshot of a computer

Description automatically generated**

1. Please fill the details service connection details below.

**A screenshot of a computer

Description automatically generated**

# **PIM Introduction**

PIM is a service in Azure Active Directory (Azure AD), part of Entra, for managing access to privileged resources. PIM enables you to manage, control, and monitor access to important resources in your organization. Such resources include those in Azure AD, Azure, and other Microsoft Online Services, such as Microsoft 365 or Microsoft Intune**.**

## Steps to Create a PIM for Azure DevOps Pipeline

**A screenshot of a computer

Description automatically generated**

1. Please add the subscription and resource group details

**A screenshot of a computer

Description automatically generated**

1. Please click on the assignments and add the assignments to restrict the user.

A screenshot of a computer

Description automatically generated

1. Once click on the assignments, please add the custom role and select a service connection which we created.

A screenshot of a computer

Description automatically generated

1. Please mention the timing to user, how long the user must access the service.

A close-up of a computer screen

Description automatically generated