**Cloud Infrastructure and Entitlement Management (CIEM) Solution Accelerator**

**Introduction**

Cloud Infrastructure and Entitlement Management solution accelerator, enables you to synchronize the following Azure objects from an Azure Tenant to One Identity Manager

* Management Groups
* Subscriptions
* Resource Groups
* Resources
* Resource Types
* Locations
* Roles
* Role Assignments

Once the objects have been synchronized in to One Identity Manager, you would be able to view the Azure Object role assignments made for the Azure AD user / Azure Service Principal / Azure AD Group.

One Identity Manager SCIM connector is used to access the Azure objects. The SCIM connector should be installed on a synchronization server to synchronize the Azure objects. The SCIM connector connects to Starling Azure Infrastructure connector and retrieves the Azure objects. The Starling Azure Infrastructure connector uses the Azure Resource Management, Azure Management Groups and Azure Authorization REST API services to retrieve the needed Azure objects

**CIEM Version 1.0 – Released January 13th, 2022**

**Installation Pre-Requisites**

The following are the software pre-requisites for CIEM solution accelerator installation

* One Identity Manager 8.2
* One Identity Manager Active Directory (ADS) and Azure Active Directory (AAD) modules installed

**Transport Installation**

The following Transport need to be installed ***maintaining the order mentioned below***

1. 01\_AzPermissions\_Transport\_MSSQL\_PRDev\_OneIM820CIEM\_20220110\_0916
2. 02\_AzTables\_Transport\_MSSQL\_PRDev\_OneIM820CIEM\_20220110\_0931
3. 03\_AzDataModelDesigner\_Transport\_MSSQL\_PRDev\_OneIM820CIEM\_20220110\_0937
4. 04\_AzManagerUI\_Transport\_MSSQL\_PRDev\_OneIM820CIEM\_20220110\_0941
5. 05a\_Reports\_Transport\_MSSQL\_IAMSERVER\_OneIM\_20210920\_0827
6. 05b\_AzManagerReport\_Transport\_MSSQL\_STANDALONE2019\_OneIM\_20210920\_1842
7. 06\_AddAADOrgRefernceForAzLocationAndAzResourceTypes\_Transport\_MSSQL\_PRDev\_OneIM820CIEM\_20220111\_1018
8. 07\_AzDataModelUpdates\_Transport\_MSSQL\_PRDev\_OneIM820CIEM\_20220111\_1029
9. 08\_AzUIUpdates\_Transport\_MSSQL\_PRDev\_OneIM820CIEM\_20220111\_1035
10. 09\_AzSyncProjectTemplate\_Transport\_MSSQL\_PRDev\_OneIM82GA\_20220111\_1041
11. 10\_ReportUpdates\_Transport\_MSSQL\_PRDev\_OneIM82GA\_20220109\_1819

**Setting up Azure AD Service Principal needed for Starling Azure Infrastructure Connector**

An Azure AD Service Principal needs to be created in Azure with Reader Role Access for the Root Tenant Management Group. This Service Principal would be used by Starling to access the Azure objects through REST API. Following steps can be followed to set it up

1. Login to  [https://shell.azure.com](https://shell.azure.com/) , select "Bash" console.
2. Use the following command to create a Service Principal with Reader role access for the root Management Group

*az ad sp create-for-rbac -n "{sp\_name}" --role Reader –scopes providers/Microsoft.Management/managementGroups/{mngrp\_id}*

where ***{sp\_name}*** is the Service Principal name and ***{mngrp\_id}*** is the root management group id

Collect the values for ***"appId", "password"*** and ***"tenant"*** from the Azure CLI command response. This will be used for the ***"Client Id", "Client Secret" and "Tenant Id"*** attributes while configuring the Starling Azure Infrastructure Connector.

**Synchronization Pre-Requisites**

The following items **must** be completed prior to proceeding to set up a CIEM synchronization project

* Starling Azure Infrastructure connector configured against the Azure Tenant to be synchronized. For more information regarding setting up Starling and configuring Starling Azure Infrastructure Connector, refer to the ***Starling Connect Admin Guide***. For more information regarding creating Azure AD Service Principal in Azure with necessary Permissions that can be used to retrieve Azure objects by Starling, refer to the section ***Setting up Azure AD Service Principal needed for Starling Azure Infrastructure Connector*** in this document
* One Identity Manager Azure AD (AAD) module synchronization project setup and all Azure AD objects synchronized on to One Identity Manager. For more information regarding synchronizing Azure AD objects refer to the ***One Identity Manager Azure AD admin guide***
* SCIM Connector installed on the Synchronization Server

**Setting up CIEM Synchronization Project**

The following steps can be followed to setup the

1. Open the Synchronization Editor and create a new Synchronization Project
2. In the Choose Target System window, choose SCIM Connector
3. In the Create System Connection Screen, Enter the Starling Azure Infrastructure Connector Server URL, URI of service, Authentication Endpoint and choose OAUTH as the Authentication Type. Click Next
4. Enter the SCIM ClientID and Client Secret got from the Starling Azure Infrastructure Connector. Click Next and test the connection
5. In the Target Product Selection screen, select ***SCIM Core V 2.0*** as the Target Product
6. In the Select Project Template screen, select ***Azure Infrastructure Synchronization*** as the template
7. In the Restrict Target System Access screen, select Read Only Access to Target System
8. In the Synchronization screen, select the Synchronization Server
9. Click finish to setup the Synchronization Project

**CIEM Synchronization Project Execution and viewing the results**

Once the CIEM Synchronization project has been setup, browse each endpoint in the Target System browser and make sure all objects are available. Perform a simulation followed by synchronization execution. Once the Synchronization is complete, login to One Identity Manager to see the results under the Menu ***Cloud infrastructure and Entitlement Management***