Active: Cloud

To index and profile network assets in a cloud infrastructure or in a combination of cloud and traditional infrastructure,. This discovery type will enable you to monitor a cloud network in as much detail as a typical corporate network. Cloud Discovery leverages the service provider's APIs to create devices for all running instances. Cloud Discovery findings are reported in the same manner as all other Asset Manager discovery types.

Cloud credentials are encrypted within Asset Manager, yet are accessible to the cloud provider. This means that all APIs that return a cloud-discovery configuration, including those that export a collector configuration or system configuration, do not include cloud credential "secrets." Rather, clientSecrets and secretKeys are reported as "null" or left empty.

Currently, Cloud Discovery uses the Scout you configure, yet the particular Scout's interface cannot be specified.

AWS Permissions

Within AWS, users must be, at a minimum, AWS IAM group members with the AWS Policy of AmazonEC2ReadOnlyAccess.

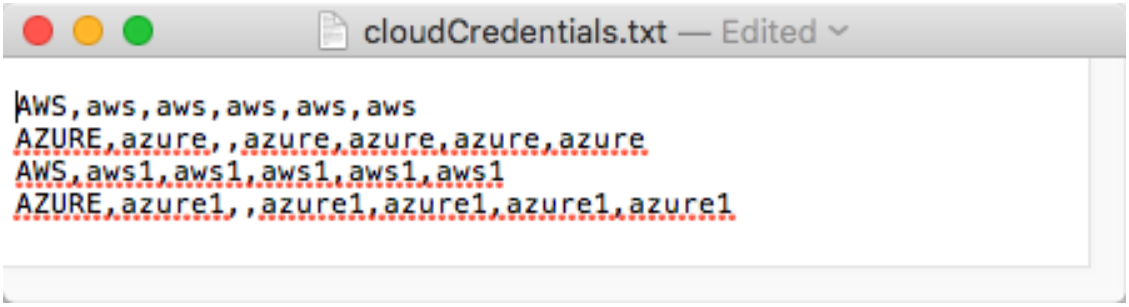
Prerequisites before configuring **Azure** Cloud Scanner.

1. Follow this link to create the **App Registration** in the Azure Portal. https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal
2. `User.Read` access is sufficient, as this permission is assigned to the app registration by default.
3. Copy the **secret Key** (Not secret ID) somewhere safe. You will need it for the below steps & It won't show up again when you leave the AZ Portal.
4. Browse to the Overview blade of your newly created App Registration.
5. Copy the **Application (client) ID** & **Directory (tenant) ID** to a Notepad.
6. Follow the steps in *Configuring Cloud Discovery* instructions to enter the credentials.

Configuring Cloud Discovery

To configure Cloud Discovery:

1. Browse to **Settings** > **Zones**.
2. Select the zone and collector you want to perform Cloud Discovery.
3. Click the **Cloud** tab.
   Cloud discovery is disabled by default.
4. Click **Edit** to open the **Edit Cloud Discovery Configuration** dialog box.
5. Select the **Enable Cloud Discovery** checkbox.
6. Click **Update**.
   The configuration is saved.
7. Click **Credentials**.
8. You can drag and drop or **Upload** your cloud credentials as a plain text file, ordered as you would have them read by Asset Manager (i.e., top will be read first). You may download a sample file to see the formatting.
9. Save your results and exit. Cloud Discovery starts immediately.



AWS Parameters

1. Alias:
2. Cloud Credential Type: AWS
3. Access Key:
4. Secret Key:
5. Regions (optional):
6. Service Name: ec-2

Azure Parameters

1. Alias:
2. Cloud Credential Type: Azure
3. Resource Groups (optional):
4. Client ID:
5. Tenant ID:
6. Client Secret:
7. Subscription ID: