Azure Identity Connector - Features

Introduction

The Azure Identity connector will crawl Azure identities (users and groups) from the specified Azure Active Directory and store them on a identity cache.

Environment and Access Requirements

Account Privileges

For the Azure Identity connector to be able to crawl the identities from the Azure AD that corresponds to the domain specified in the connection, it needs that the specified credentials have enough permissions to read said identities from the directory.

MS Graph Application permissions needed:

- **GroupMember.Read.All** / Application
- **User.Read.All** / Application

Other Requirements

The Aspire worker nodes must be able to reach the Azure AD specified in the connection.

> This component has been officially tested on local Windows and Linux.

Framework and Connector Features

Framework Features

Name	Supported
Content Crawling	no
Identity Crawling	yes
Snapshot-based Incrementals	no
Non-snapshot-based Incrementals	yes
Document Hierarchy	no

Connector Features

The Azure Identity connector has the following features:

- Lower casing of retrieved identities.
- Adding a special "Everyone" group.
- Filtering out external groups.

Crawled Identities

The Azure Identity connector is able to crawl the following objects:

Name	Type	Metadata	Content Fetch & Extraction	Description

User	document	- Name - Domain - Groups - Attributes	no	The users of the Azure AD.
Group	document	- Name - Domain - Attributes	yes	The groups of the Azure AD.

Attributes for users typically contain the user GUID but may contain additional data.

Attributes for groups typically contain their display name but may contain additional data.