About the Cisco Dynamic Attributes Connector

The Cisco Secure Dynamic Attributes Connector enables you to collect data (such as networks and IP addresses) from cloud providers and send it to the FMC (FMC) so it can be used in access control rules.

The following topics provide background about the dynamic attributes connector:

About the Cisco Secure Dynamic Attributes Connector

The Cisco Secure Dynamic Attributes Connector enables you to use service tags and categories from various cloud service platforms in Firepower Management Center (FMC) access control rules.

Supported connectors

We currently support:

Table 1: List of supported connectors by Cisco Secure Dynamic Attributes Connector version and platform

CSDAC version/platform	AWS.	Git-Hub	Google Cloud	Azure	Azure Service Tags	Microsoft Office 365	VMware vCenter
Version 1.1 (on-premises)	Yes	No	No	Yes	Yes	Yes	Yes
Version 2.0 (on-premises)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cloud-delivered (Cisco Defense Orchestrator)	Yes	Yes	Yes	Yes	Yes	Yes	No

More information about connectors:

- Amazon Web Services (AWS)

  For more information, see a resource like Tagging AWS resources on the Amazon documentation site.

- Microsoft Azure

  For more information, see this page on the Azure documentation site.

- Microsoft Azure service tags

  For more information, see a resource like Virtual network service tags on Microsoft TechNet.

- Office 365

  For more information, see Office 365 URLs and IP address ranges on docs.microsoft.com.

- VMware categories and tags managed by vCenter and NSX-T

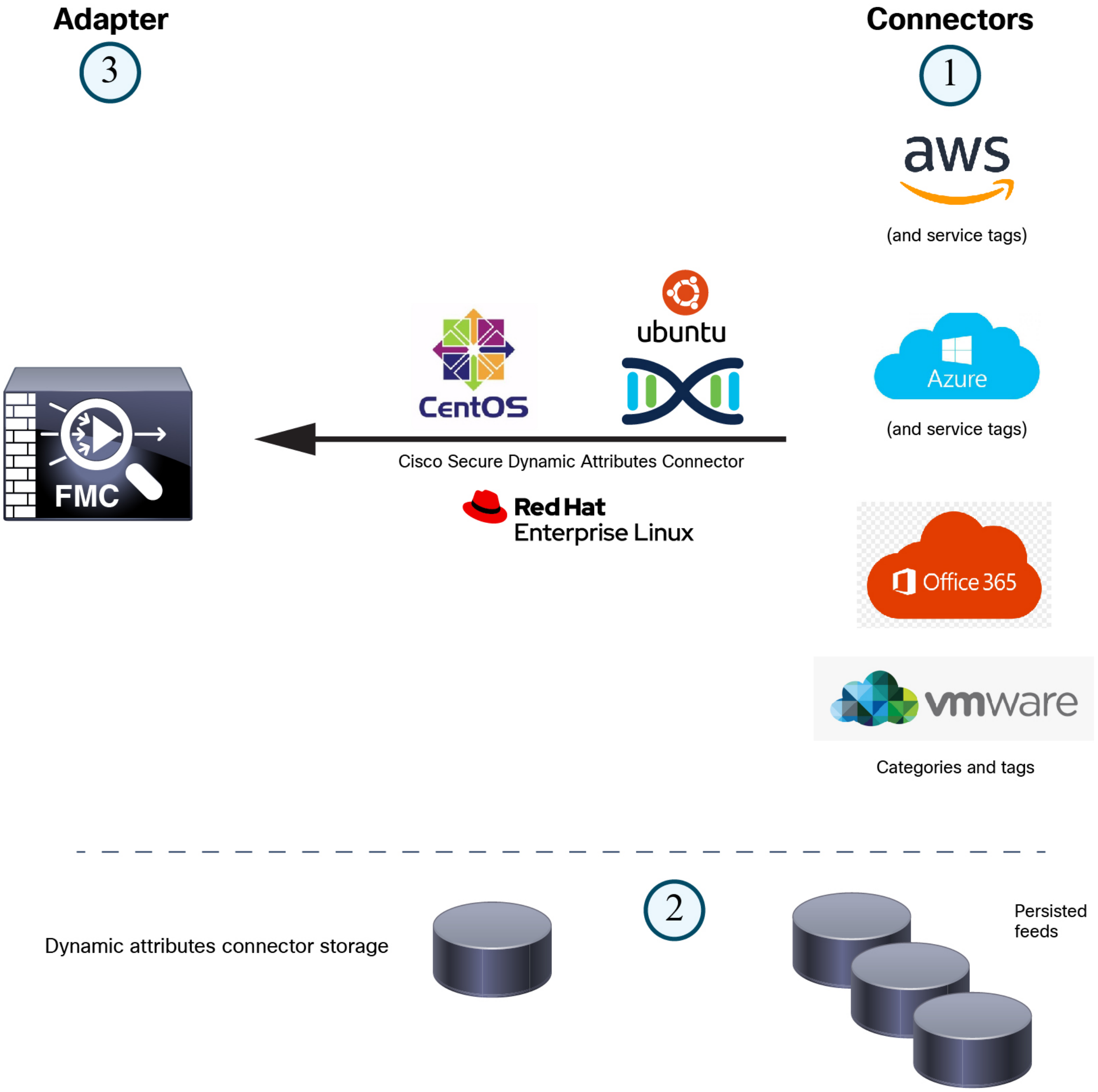
  For more information, see a resource like vSphere Tags and Attributes in the VMware documentation site.

How it works

Network constructs such as IP address are not reliable in virtual, cloud and container environments due to the dynamic nature of the workloads and the inevitability of IP address overlap. Customers require policy rules to be defined based on non-network constructs such as VM name or security group, so that firewall policy is persistent even when the IP address or VLAN changes.

You can collect these tags and attributes using dynamic attributes connector Docker containers running on an Ubuntu virtual machine. Install the dynamic attributes connector on the Ubuntu host using an Ansible collection.

The following figure shows how the system functions at a high level.



1. *Connectors* contain the tags and containers to query.

   For example, typically these tags define dynamically allocated network and IP addresses for which you cannot create access control rules. Persisted feeds from the connectors are stored on the dynamic attributes connector for fast access.

2. Tag information is persisted on the dynamic attributes connector where you create *dynamic attribute filters* that define which information is important to use in access control rules.

   For example, if AWS defines networks for the Accounting and Finance Departments virtual machines, you can create a dynamic attributes filter that specifies only the Finance network.

3. The adapter defined by the dynamic attributes connector receives those dynamic attributes filters as *dynamic objects* and enables you to use them in access control rules.