À propos du connecteur d'attributs dynamiques Cisco

Le Connecteur d'attributs dynamiques Cisco Secure vous permet de collecter des données (telles que les réseaux et les adresses IP) auprès des fournisseurs de services en nuage et de les envoyer à Ciso Secure Firewall Management Center (centre de gestion afin qu'elles puissent être utilisées dans les règles de contrôle d'accès).

Les rubriques suivantes fournissent des informations générales sur le connecteur d'attributs dynamiques :

• À propos du connecteur d'attributs dynamiques Cisco Secure, à la page 1

À propos du connecteur d'attributs dynamiques Cisco Secure

Le Connecteur d'attributs dynamiques Cisco Secure vous permet d'utiliser des balises et des catégories de services provenant de diverses plateformes de services en nuage dans les règles de contrôle d'accès Cisco Secure Firewall Management Center (centre de gestion).

Connecteurs pris en charge

Nous prenons actuellement en charge :

Tableau 1 : Liste des connecteurs pris en charge par version Connecteur d'attributs dynamiques Cisco Secure et plateforme

Version/plateforme CSDAC	AWS	Texte générique	GitHub	Google Cloud	Azure	Balises de service Azure	Microsoft Office 365	VMware vCenter	Webex Non	Zoom Non
Version 1.1 (sur site)	Oui	Non	Non	Non	Oui	Oui	Oui	Oui	Non	Non
Version 2.0 (sur site)	Oui	Non	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non

Plus d'informations sur les connecteurs :

• Amazon Web Services (AWS)

Pour plus d'informations, consultez une ressource telle que Étiqueter les ressources AWS sur le site de documentation d'Amazon.

- GitHub
- Google Cloud

  Pour plus d'informations, consultez la section Configuration de votre environnement dans la documentation de Google Cloud.

- Microsoft Azure

  Pour plus d'informations, consultez cette page sur le site de documentation Azure.

- Balises de service Microsoft Azure

  Pour plus d'informations, consultez une ressource telle que les Balises de service de réseau virtuel sur Microsoft TechNet.

- Office 365

  Pour plus d'informations, consultez la section URL et plages d'adresses IP d'Office 365 sur docs.microsoft.com.

- Catégories et balises VMware gérées par vCenter et NSX-T

  Pour plus d'informations, consultez une ressource telle que les Balises et attributs vSphere sur le site de documentation de VMware.

Sujets connexes

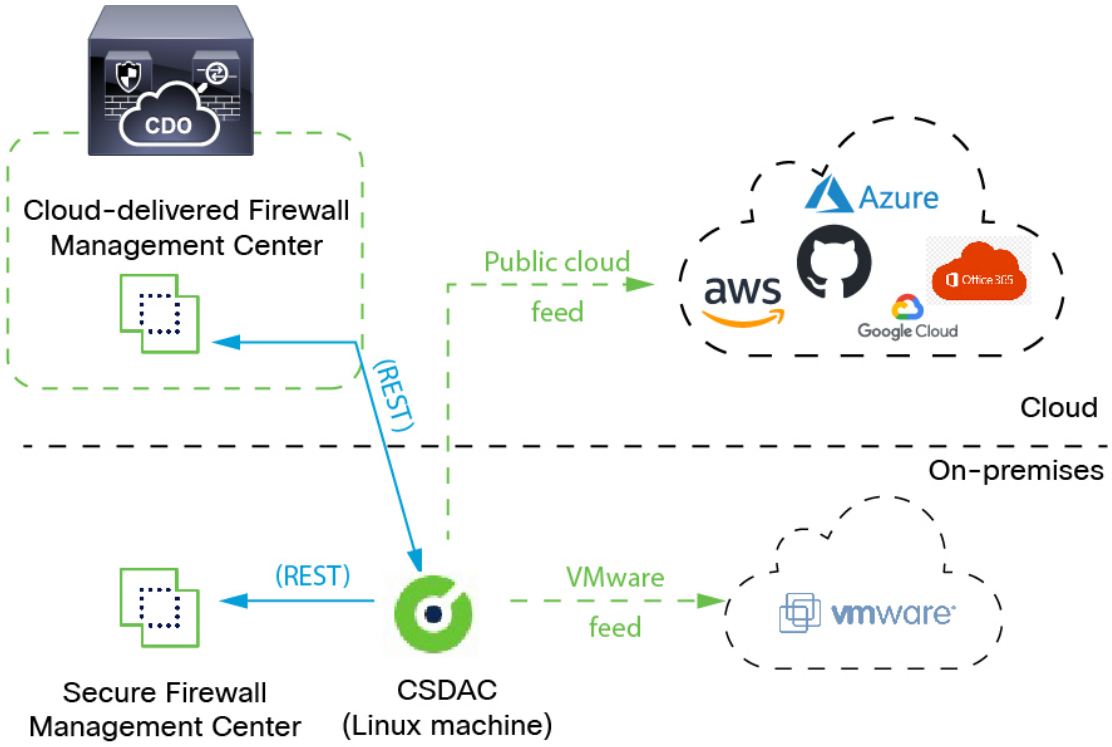
Installer les logiciels prérequis

Modalités

Les constructions de réseau telles que l'adresse IP ne sont pas fiables dans les environnements virtuels, en nuage et en conteneur en raison de la nature dynamique des charges de travail et de l'inévitable chevauchement des adresses IP. Les clients ont besoin que les règles soient définies sur la base d'éléments non liés au réseau, tels que le nom de la machine virtuelle ou le groupe de sécurité, afin que la politique de pare-feu soit maintenue même en cas de changement d'adresse IP ou de réseau local virtuel (VLAN).

Vous pouvez collecter ces balises et attributs à l'aide de conteneurs Docker du connecteur d'attributs dynamiques fonctionnant sur une machine virtuelle Ubuntu, CentOS ou Red Hat Enterprise Linux. Installer le connecteur d'attributs dynamiques sur l'hôte Ubuntu à l'aide d'une collection Ansible.

La figure suivante montre le fonctionnement du système d'un point de vue général.



1. Les *connecteurs* contiennent les balises et les conteneurs à interroger.

   Par exemple, ces balises définissent généralement des adresses réseau et IP attribuées dynamiquement pour lesquelles vous ne pouvez pas créer de règles de contrôle d'accès. Les flux persistants des connecteurs sont stockés sur connecteur d'attributs dynamiques pour un accès rapide.

2. Les informations relatives aux balises sont conservées sur le connecteur d'attributs dynamiques où vous créez des *filtres d'attributs dynamiques* qui définissent les informations importantes à utiliser dans les règles de contrôle d'accès.

   Par exemple, si AWS définit des réseaux pour les machines virtuelles des services comptables et des finances, vous pouvez créer un filtre d'attributs dynamique qui spécifie uniquement le réseau des finances.

3. *L'adaptateur* défini par connecteur d'attributs dynamiques reçoit ces filtres d'attributs dynamiques en tant qu'*objets dynamiques* et vous permet de les utiliser dans les règles de contrôle d'accès.

   Vous pouvez créer les types d'adaptateurs suivants :

   - On-Prem Firewall Management Center Dans le cas d'un périphérique de Centre de gestion.

     Ce type de périphérique de Centre de gestion peut être gérée par Cisco Defense Orchestrator (CDO) ou peut être autonome.

   - *Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)* pour les périphériques gérés par CDO.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.