Configurer le Connecteur d'attributs dynamiques Cisco Secure

Installez connecteur d'attributs dynamiques et configurez les connecteurs, les filtres d'attributs dynamiques et les adaptateurs pour fournir au centre de gestion des données dynamiques sur le réseau qui peuvent être utilisées dans les règles de contrôle d'accès.

Pour plus d'informations, consultez les rubriques suivantes :

Créer un connecteur

Un *connecteur* est une interface avec un service en nuage. Le connecteur récupère les informations réseau du service en nuage afin qu'elles puissent être utilisées dans les stratégies de contrôle d'accès sur le centre de gestion.

Nous prenons en charge les éléments suivants :

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

Voir l'une des sections suivantes pour plus d'informations.

Connecteur Amazon Web Services - À propos des autorisations des utilisateurs et des données importées

Le Connecteur d'attributs dynamiques Cisco Secure importe des attributs dynamiques d'AWS vers le centre de gestion pour les utiliser dans les politiques de contrôle d'accès.

Attributs dynamiques importés

Nous importons les attributs dynamiques suivants d'AWS :

- *Balises*, paires clé-valeur définies par l'utilisateur que vous pouvez utiliser pour organiser vos ressources AWS EC2.

  Pour plus d'informations, consultez la section Étiqueter vos ressources EC2 dans la documentation AWS.

- *Adresses IP* des machines virtuelles dans AWS.

Autorisations minimales requises

Le Connecteur d'attributs dynamiques Cisco Secure nécessite au minimum un utilisateur disposant d'une politique autorisant `ec2:DescribeTags` et `ec2:DescribeInstances` à importer des attributs dynamiques.

Créer un utilisateur AWS avec des autorisations minimales pour le Connecteur d'attributs dynamiques Cisco Secure

Cette tâche explique comment configurer un compte de service avec des autorisations minimales pour envoyer des attributs dynamiques au centre de gestion. Pour obtenir la liste de ces attributs, consultez.Connecteur Amazon Web Services - À propos des autorisations des utilisateurs et des données importées, à la page 2.

Avant de commencer

Vous devez déjà avoir configuré votre compte Amazon Web Services (AWS). Pour plus d'informations à ce sujet, consultez cet article dans la documentation AWS.

Étape 1 Connectez-vous à la console AWS en tant qu'utilisateur avec le rôle d'administrateur.

Étape 2 Dans le tableau de bord, cliquez sur **Sécurité, identité et conformité** > **IAM**.

Étape 3 Cliquez sur **Gestion de l'accès** > **Utilisateurs**.

Étape 4 Cliquez sur **Ajouter un utilisateur**.

Étape 5 Dans le champ **Nom d'utilisateur**, saisissez un nom pour identifier l'utilisateur.

Étape 6 Cliquez sur **Clé d'accès - Accès programmatique**.

Étape 7 Dans la page Définir les autorisations, cliquez sur **Suivant** sans accorder à l'utilisateur l'accès à quoi que ce soit ; vous le ferez plus tard.

Étape 8 Ajoutez des étiquettes à l'utilisateur si vous le souhaitez.

Étape 9 Cliquez sur **Créer un utilisateur**.

Étape 10 Cliquez sur **Télécharger .csv** pour télécharger la clé de l'utilisateur sur votre ordinateur.

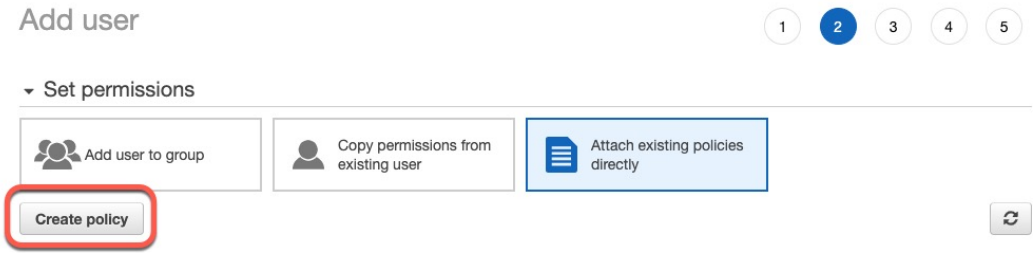
Remarque C'est la seule occasion dont vous disposez pour récupérer la clé de l'utilisateur.

Étape 11 Cliquez sur **Close** (Fermer).

Étape 12 Sur la page Gestion des identités et des accès (IAM), dans la colonne de gauche, cliquez sur **Gestion des accès** > **Politiques**.

Étape 13 Cliquez sur **Créer une politique**.

Étape 14 Sur la page Créer une politique, cliquez sur **JSON**.



Étape 15 Saisissez la politique suivante dans le champ :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeTags",
                "ec2:DescribeInstances"
            ],
            "Resource": "*"
        }
    ]
}
```

Étape 16 Cliquez sur **Next** (suivant).

Étape 17 Cliquez sur **Révision**.

Étape 18 Sur la page Révision de la politique, saisissez les informations demandées et cliquez sur **Créer une politique**.

Étape 19 Dans la page Politiques, saisissez tout ou partie du nom de la politique dans le champ de recherche et appuyez sur Entrée.

Étape 20 Cliquez sur la politique que vous venez de créer.

Étape 21 Cliquez sur **Actions** > **Rejoindre**.

Étape 22 Si nécessaire, saisissez tout ou partie du nom de l'utilisateur dans le champ de recherche et appuyez sur Entrée.

Étape 23 Cliquez sur **Rejoindre la politique**.

Prochaine étape

Créer un connecteur AWS, à la page 3.

Créer un connecteur AWS

Cette tâche explique comment configurer un connecteur qui envoie des données d'AWS à centre de gestion pour les utiliser dans les stratégies de contrôle d'accès.

Avant de commencer

Créez un utilisateur disposant au moins des privilèges décrits dans Créer un utilisateur AWS avec des autorisations minimales pour le Connecteur d'attributs dynamiques Cisco Secure, à la page 2.

Étape 1 Connectez-vous au connecteur d'attributs dynamiques.

Étape 2 Cliquez sur **Connecteurs**.

Étape 3 Effectuez l'une des actions suivantes :

- Ajouter un nouveau connecteur : cliquez sur Icône ajouter (), puis sur le nom du connecteur.
- Modifier ou supprimer un connecteur : Cliquez sur **Plus** (), puis sur **Modifier** ou **Supprimer** à la fin de la ligne.

Étape 4 Ensuite, entrez l'information suivante.

Valeur	Description
Nom	(Requis) Saisissez un nom pour identifier de manière unique ce connecteur.
Description	Description facultative
Intervalle d'envoi	(Valeur par défaut : 30 secondes) Intervalle auquel les mappages IP sont récupérés à partir d'AWS.
Région	(Requis) Saisissez votre code régional AWS.
Clé d'accès	(Requis) Saisissez votre clé d'accès.
Clé secrète	(Requis) Saisissez votre clé secrète.

Étape 5 cliquez sur **Test** et assurez-vous que l'essai réussit avant de sauvegarder le connecteur.

Étape 6 Cliquez sur **Save** (enregistrer).

Étape 7 Assurez-vous que **Ok** est affiché dans la colonne État.

Prochaine étape

Créer un adaptateur, à la page 16

Connecteur Azure : à propos des autorisations des utilisateurs et des données importées

Le Connecteur d'attributs dynamiques Cisco Secure importe des attributs dynamiques d'Azure vers le centre de gestion pour les utiliser dans les stratégies de contrôle d'accès.

Attributs dynamiques importés

Nous importons les attributs dynamiques suivants depuis Azure :

- *Balises*, paires clé-valeur associées aux ressources, aux groupes de ressources et aux abonnements.

Pour plus d'informations, consultez cette page de la documentation Microsoft.

- *Adresses IP* des machines virtuelles dans Azure.

Autorisations minimales requises

Le Connecteur d'attributs dynamiques Cisco Secure nécessite un utilisateur disposant au minimum du droit de **lecture** pour pouvoir importer des attributs dynamiques.

Créer un utilisateur Azure avec des permissions minimales pour le Connecteur d'attributs dynamiques Cisco Secure

Cette tâche explique comment configurer un compte de service avec des autorisations minimales pour envoyer des attributs dynamiques au centre de gestion. Pour obtenir la liste de ces attributs, consultez.Connecteur Azure : à propos des autorisations des utilisateurs et des données importées, à la page 4.

Avant de commencer

Vous devez déjà avoir un compte Microsoft Azure. Pour en configurer un, consultez cette page sur le site de documentation Azure.

Étape 1 Connectez-vous au portail Azure en tant que propriétaire de l'abonnement.

Étape 2 Cliquez sur **Azure Active Directory**.

Étape 3 Recherchez l'instance d'Azure Active Directory correspondant à l'application que vous souhaitez configurer.

Étape 4 Cliquez sur **Ajouter** > **Enregistrement de l'application**.

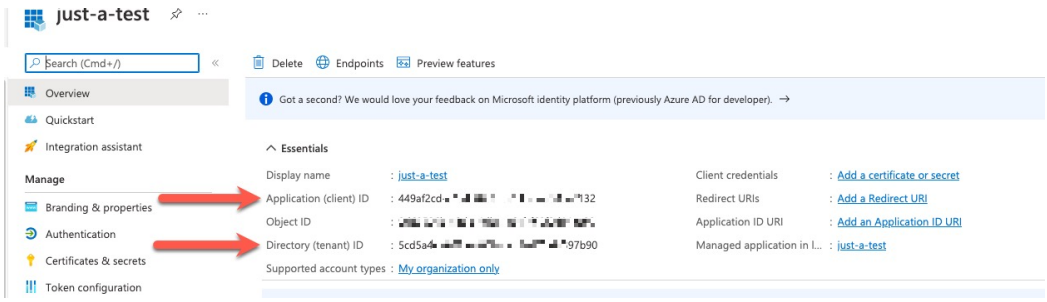
Étape 5 Dans le champ **Nom**, saisissez un nom pour identifier cette application.

Étape 6 Saisissez sur cette page les autres informations requises par votre organisation.

Étape 7 Cliquez sur **Register** (Inscrire).

Étape 8 Sur la page suivante, notez l'ID du client (également appelé *ID de l'application*) et l'ID du service partagé (également appelé *ID du répertoire*).

Voici un exemple.

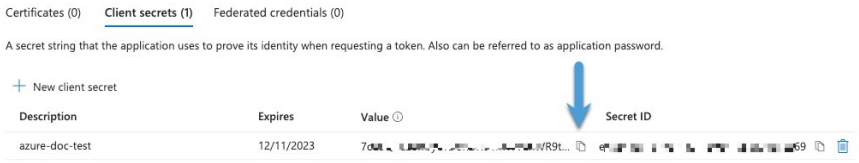


Étape 9 En regard des informations d'identification du client, cliquez sur **Ajouter un certificat ou un code secret**.

Étape 10 Cliquez sur **Nouveau code secret du client**.

Étape 11 Saisissez les informations demandées et cliquez sur **Ajouter**.

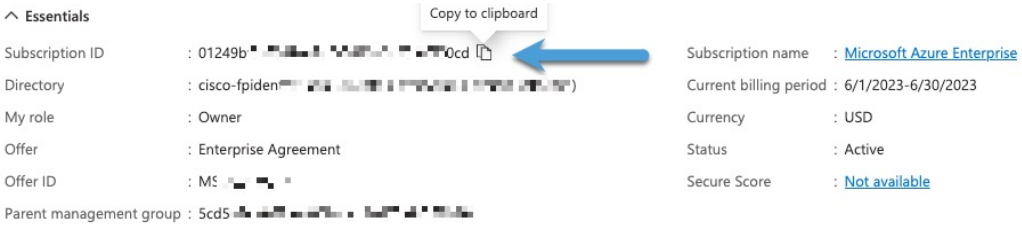
Étape 12 Copier la valeur du champ **Valeur** dans le presse-papiers. C'est cette valeur, *et non* l'**ID du code secret**, qui constitue le code secret du client.



Étape 13 Revenez à la page principale du portail Azure et cliquez sur **Abonnements**.

Étape 14 Cliquez sur le nom de votre abonnement.

Étape 15 Copier l'identifiant de l'abonnement dans le presse-papiers.



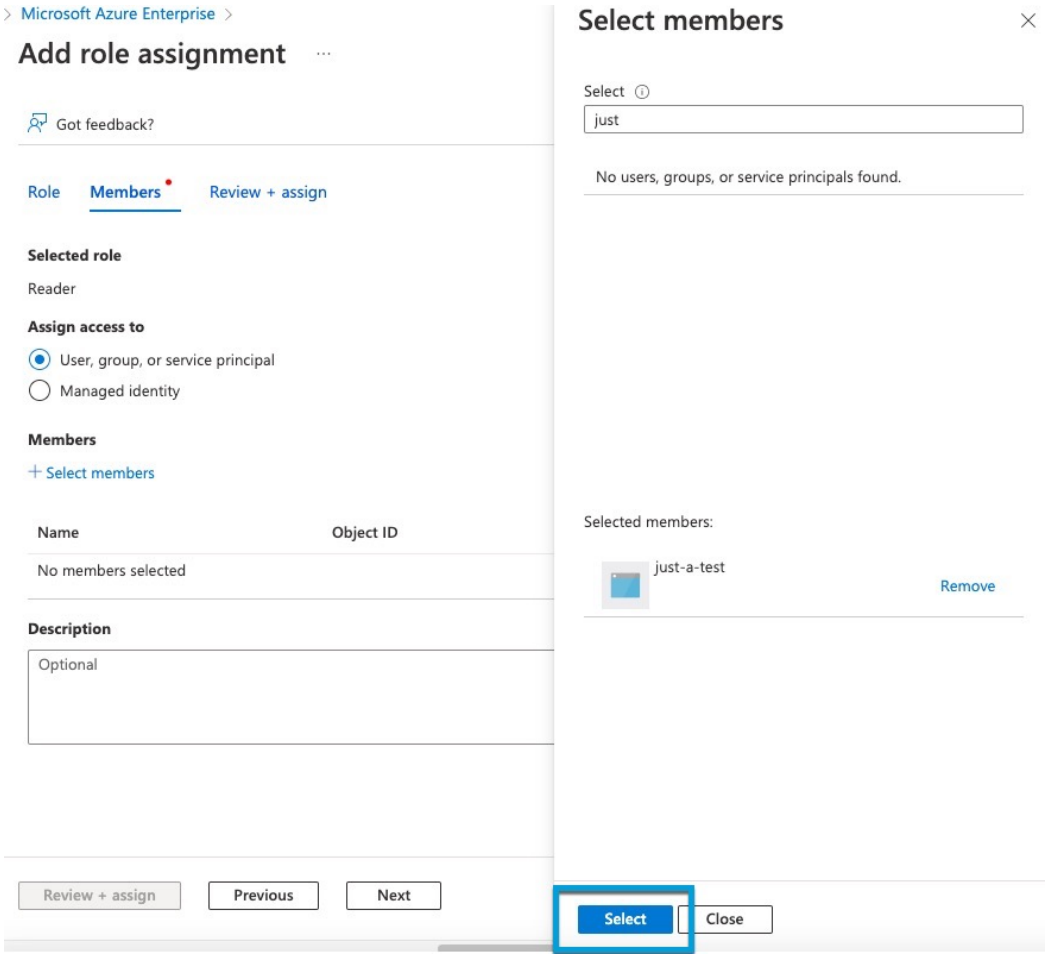
Étape 16 Cliquez sur **Contrôle d'accès (IAM)**.

Étape 17 Cliquez sur **Ajouter** > **Ajouter des affectations de rôles**.

Étape 18 Cliquez sur **Lecteur**, puis cliquez sur **Suivant**.

Étape 19 Cliquez sur **Sélectionner des membres**.

Étape 20 Dans la partie droite de la page, cliquez sur le nom de l'application que vous avez enregistrée et cliquez sur **Sélectionner**.



Étape 21 Cliquez sur **Examiner + Attribuer** et suivez les invites pour terminer l'action.

Prochaine étape

Consultez Créer un connecteur Azure, à la page 7.

Créer un connecteur Azure

Cette tâche explique comment créer un connecteur pour envoyer des données d'Azure à centre de gestion pour les utiliser dans les stratégies de contrôle d'accès.

Avant de commencer

Créez un utilisateur Azure disposant au moins des privilèges décrits dans la section Créer un utilisateur Azure avec des permissions minimales pour le Connecteur d'attributs dynamiques Cisco Secure, à la page 5.

Étape 1 Connectez-vous au connecteur d'attributs dynamiques.

Étape 2 Cliquez sur **Connecteurs**.

Étape 3 Effectuez l'une des actions suivantes :

- Ajouter un nouveau connecteur : cliquez sur Icône ajouter (), puis sur le nom du connecteur.
- Modifier ou supprimer un connecteur : Cliquez sur **Plus** (), puis sur **Modifier** ou **Supprimer** à la fin de la ligne.

Étape 4 Ensuite, entrez l'information suivante.

Valeur	Description
Nom	(Requis) Saisissez un nom pour identifier de manière unique ce connecteur.
Description	Description facultative
Intervalle d'envoi	(Valeur par défaut : 30 secondes) Intervalle de collecte des mappages d'IP depuis Azure.
ID d'abonnement	(Requis) Saisissez votre identifiant d'abonnement Azure.
ID du locataire	(Requis) Saisissez votre identifiant de service partagé.
ID du client	(Requis) Saisissez votre numéro de client.
Secret du client	(Requis) Saisissez votre code secret client.

Étape 5 Cliquez sur**Test** et assurez-vous que **Test connection succeeded** s'affiche avant que vous n'enregistriez le connecteur.

Étape 6 Cliquez sur **Save** (enregistrer).

Étape 7 Assurez-vous que **Ok** est affiché dans la colonne État.

Prochaine étape

Créer un adaptateur, à la page 16

Créer un connecteur de balises de service Azure

Cette rubrique explique comment créer un connecteur pour les balises de service Azure vers centre de gestion à utiliser dans les stratégies de contrôle d'accès. Les associations d'adresses IP avec ces balises sont mises à jour chaque semaine par Microsoft.

Pour plus d'informations, consultez Balises de service de réseau virtuel sur Microsoft TechNet.

Étape 1 Connectez-vous au connecteur d'attributs dynamiques.

Étape 2 Cliquez sur **Connecteurs**.

Étape 3 Effectuez l'une des actions suivantes :

- Ajouter un nouveau connecteur : cliquez sur Icône ajouter (), puis sur le nom du connecteur.
- Modifier ou supprimer un connecteur : Cliquez sur **Plus** (), puis sur **Modifier** ou **Supprimer** à la fin de la ligne.

Étape 4 Ensuite, entrez l'information suivante.

Valeur	Description
Nom	(Requis) Saisissez un nom pour identifier de manière unique ce connecteur.
Description	Description facultative
Intervalle d'envoi	(Valeur par défaut : 30 secondes) Intervalle de collecte des mappages d'IP depuis Azure.
ID d'abonnement	(Requis) Saisissez votre identifiant d'abonnement Azure.
ID du locataire	(Requis) Saisissez votre identifiant de service partagé.
ID du client	(Requis) Saisissez votre numéro de client.
Secret du client	(Requis) Saisissez votre code secret client.

Étape 5 Cliquez sur**Test** et assurez-vous que **Test connection succeeded** s'affiche avant que vous n'enregistriez le connecteur.

Étape 6 Cliquez sur **Save** (enregistrer).

Étape 7 Assurez-vous que **Ok** est affiché dans la colonne État.

Prochaine étape

Créer un adaptateur, à la page 16

Créer un connecteur GitHub

Cette section explique comment créer un connecteur GitHub qui envoie des données à centre de gestion pour les utiliser dans les stratégies de contrôle d'accès. Les adresses IP associées à ces balises sont gérées par GitHub. Il n'est pas nécessaire de créer des filtres d'attributs dynamiques.

Pour en savoir plus, consultez la section À propos des adresses IP de GitHub.

Remarque Ne modifiez pas l'URL, car vous ne parviendriez pas à récupérer les adresses IP.

Étape 1 Connectez-vous au connecteur d'attributs dynamiques.

Étape 2 Cliquez sur **Connecteurs**.

Étape 3 Effectuez l'une des actions suivantes :

- Ajouter un nouveau connecteur : cliquez sur Icône ajouter (), puis sur le nom du connecteur.
- Modifier ou supprimer un connecteur : Cliquez sur **Plus** (), puis sur **Modifier** ou **Supprimer** à la fin de la ligne.

Étape 4 Saisissez un **nom** et une description facultative.

Étape 5 (Facultatif) Dans le champ **Intervalle d'extraction**, modifiez la fréquence, en secondes, à laquelle le connecteur d'attributs dynamiques récupère les adresses IP de GitHub. La valeur par défaut est de 21 600 secondes (6 heures).

Étape 6 cliquez sur **Test** et assurez-vous que l'essai réussit avant de sauvegarder le connecteur.

Étape 7 Cliquez sur **Save** (enregistrer).

Étape 8 Assurez-vous que **Ok** est affiché dans la colonne État.

Prochaine étape

Créer un adaptateur, à la page 16

Google Cloud Connector - À propos des autorisations des utilisateurs et des données importées

Le Connecteur d'attributs dynamiques Cisco Secure importe des attributs dynamiques de Google Cloud vers le centre de gestion pour les utiliser dans les règles de contrôle d'accès.

Attributs dynamiques importés

Nous importons les attributs dynamiques suivants de Google Cloud :

- *Étiquettes*, paires clé-valeur que vous pouvez utiliser pour organiser vos ressources Google Cloud.

  Pour plus d'informations, consultez la section Création et gestion des étiquettes dans la documentation de Google Cloud.

- *Balises réseau*, paires clé-valeur associées à une organisation, un dossier ou un projet.

  Pour plus d'informations, consultez la section Création et gestion des balises dans la documentation de Google Cloud.

- *Adresses IP* des machines virtuelles dans Google Cloud.

Autorisations minimales requises

Pour pouvoir importer des attributs dynamiques, il faut que l'utilisateur de Connecteur d'attributs dynamiques Cisco Secure dispose au minimum de l'autorisation **Basic** > **Viewer** (Consultation de base).

Créer un utilisateur Google Cloud avec des autorisations minimales pour le Connecteur d'attributs dynamiques Cisco Secure

Cette tâche explique comment configurer un compte de service avec des autorisations minimales pour envoyer des attributs dynamiques au centre de gestion. Pour obtenir la liste de ces attributs, consultez.Google Cloud Connector - À propos des autorisations des utilisateurs et des données importées, à la page 10.

Avant de commencer

Vous devez déjà avoir configuré votre compte Google Cloud. Pour plus d'informations à ce sujet, consultez la section Configuration de votre environnement dans la documentation de Google Cloud.

Étape 1 Connectez-vous à votre compte Google Cloud en tant qu'utilisateur ayant le rôle de propriétaire.

Étape 2 Cliquez sur **IAM et Admin** > **Comptes de service** > **Créer un compte de service**.

Étape 3 Saisissez l'information suivante :

- **Nom du compte de service** : Un nom pour identifier ce compte ; par exemple, **CSDAC**.
- **Identifiant du compte de service** : doit être renseigné avec une valeur unique après la saisie du nom du compte de service.
- **Description du compte de service** : Saisissez une description facultative.

Pour plus d'informations sur les comptes de service, consultez la section Comprendre les comptes de service dans la documentation de Google Cloud.

Étape 4 Cliquez sur **Créer et continuer**.

Étape 5 Suivez les invites à l'écran jusqu'à ce que la section Autoriser les utilisateurs à accéder à ce compte de service s'affiche.

Étape 6 Accorder à l'utilisateur le rôle**Basic** > **Viewer** (Consultation de base).

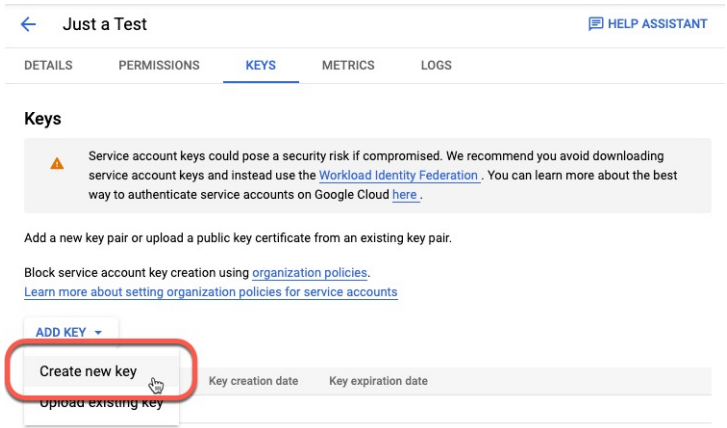
Étape 7 Cliquez sur **Done (Terminé)**.

La liste des comptes de service s'affiche.

Étape 8 Cliquez sur **Plus** (⋮) à la fin de la ligne du compte de service que vous avez créé.

Étape 9 Cliquez sur **Gérer les clés**.

Étape 10 Cliquez sur **Ajouter des clés** > **Créer une nouvelle clé**.



Étape 11 Cliquez sur **JSON**.

Étape 12 Cliquez sur **Create** (créer).

La clé JSON est téléchargée sur votre ordinateur.

Étape 13 Conservez la clé à portée de main lorsque vous configurez le connecteur GCP.

Prochaine étape

Consultez Créer un connecteur Google Cloud, à la page 12.

Créer un connecteur Google Cloud

Avant de commencer

Préparez les données de votre compte de service Google Cloud au format JSON ; elles sont nécessaires pour configurer le connecteur.

Étape 1 Connectez-vous au connecteur d'attributs dynamiques.

Étape 2 Cliquez sur **Connecteurs**.

Étape 3 Effectuez l'une des actions suivantes :

- Ajouter un nouveau connecteur : cliquez sur Icône ajouter (), puis sur le nom du connecteur.
- Modifier ou supprimer un connecteur : Cliquez sur **Plus** (), puis sur **Modifier** ou **Supprimer** à la fin de la ligne.

Étape 4 Ensuite, entrez l'information suivante.

Valeur	Description
Nom	(Requis) Saisissez un nom pour identifier de manière unique ce connecteur.
Description	Description facultative
Intervalle d'envoi	(Valeur par défaut : 30 secondes) Intervalle auquel les mappages IP sont récupérés à partir d'AWS.
Région GCP	(Requis) Saisissez la région GCP dans laquelle se trouve votre compte Google Cloud. Pour plus d'informations, consultez la rubrique Régions et zones de la documentation de Google Cloud.
Compte de service	Collez le code JSON de votre compte de service Google Cloud.

Étape 5 cliquez sur **Test** et assurez-vous que l'essai réussit avant de sauvegarder le connecteur.

Étape 6 Cliquez sur **Save** (enregistrer).

Étape 7 Assurez-vous que **Ok** est affiché dans la colonne État.

Prochaine étape

Créer un adaptateur, à la page 16

Créer un connecteur Office 365

Cette tâche explique comment créer un connecteur pour les balises Office 365 afin d'envoyer des données au centre de gestion à utiliser dans les stratégies de contrôle d'accès. Les adresses IP associées à ces balises sont mises à jour chaque semaine par Microsoft. Il n'est pas nécessaire de créer un filtre d'attributs dynamique pour utiliser les données.

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

Étape 1 Connectez-vous au connecteur d'attributs dynamiques.

Étape 2 Cliquez sur **Connecteurs**.

Étape 3 Effectuez l'une des actions suivantes :

- Ajouter un nouveau connecteur : cliquez sur Icône ajouter (), puis sur le nom du connecteur.
- Modifier ou supprimer un connecteur : Cliquez sur **Plus** (), puis sur **Modifier** ou **Supprimer** à la fin de la ligne.

Étape 4 Ensuite, entrez l'information suivante.

Valeur	Description
Nom	(Requis) Saisissez un nom pour identifier de manière unique ce connecteur.
Description	Description facultative
Intervalle d'envoi	(Valeur par défaut : 30 secondes) Intervalle de collecte des mappages d'IP depuis Azure.
URL de l'API de base	(Requis) Saisissez l'URL à partir de laquelle vous souhaitez récupérer les informations relatives à Office 365, si elle est différente de l'URL par défaut. Pour plus d'informations, consultez le service web Adresse IP et URL d'Office 365 sur le site de documentation de Microsoft.
Nom de l'instance	(Requis) Dans la liste, cliquez sur un nom d'instance. Pour plus d'informations, consultez le service web Adresse IP et URL d'Office 365 sur le site de documentation de Microsoft.
Désactiver les adresses IP optionnelles	(Requis) Saisissez **true** ou **false**.

Étape 5 cliquez sur **Test** et assurez-vous que l'essai réussit avant de sauvegarder le connecteur.

Étape 6 Cliquez sur **Save** (enregistrer).

Étape 7 Assurez-vous que **Ok** est affiché dans la colonne État.

Prochaine étape

Créer un adaptateur, à la page 16

Connecteur vCenter : à propos des autorisations des utilisateurs et des données importées

Le Connecteur d'attributs dynamiques Cisco Secure importe des attributs dynamiques de vCenter vers le centre de gestion pour les utiliser dans les stratégies de contrôle d'accès.

Attributs dynamiques importés

Nous importons les attributs dynamiques suivants de vCenter :

- *Système d'exploitation*
- *adresse MAC*
- *Adresses IP*
- *Balises NSX*

Autorisations minimales requises

Pour pouvoir importer des attributs dynamiques, il faut que l'utilisateur de Connecteur d'attributs dynamiques Cisco Secure ait au moins des droits en **lecture seule**.

Créer un connecteur vCenter

Cette tâche explique comment créer un connecteur pour VMware vCenter afin d'envoyer des données à centre de gestion utilisables dans les stratégies de contrôle d'accès.

Avant de commencer

Si vous utilisez des certificats non approuvés pour communiquer avec vCenter, consultez Obtenir de manière manuelle un certificat de Chaîne d'autorité de certification (CA), à la page 21.

Étape 1 Connectez-vous au connecteur d'attributs dynamiques.

Étape 2 Cliquez sur **Connecteurs**.

Étape 3 Effectuez l'une des actions suivantes :

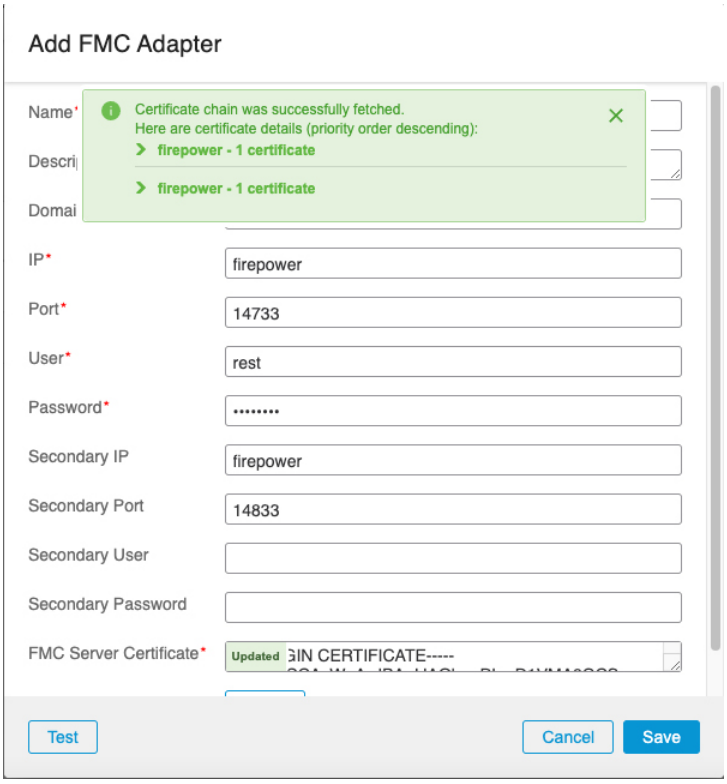
- Ajouter un nouveau connecteur : cliquez sur Icône ajouter (), puis sur le nom du connecteur.
- Modifier ou supprimer un connecteur : Cliquez sur **Plus** (), puis sur **Modifier** ou **Supprimer** à la fin de la ligne.

Étape 4 Ensuite, entrez l'information suivante.

Valeur	Description
Nom	(Requis) Saisissez un nom pour identifier de manière unique ce connecteur.
Description	Saisissez une description facultative.
Intervalle d'envoi	(Valeur par défaut : 30 secondes) Intervalle de récupération des mappages IP à partir de vCenter.
Hébergement	(Requis) Saisissez l'un des éléments suivants : • Nom d'hôte complet de vCenter • Adresse IP du vCenter • (Facultatif) Un port *Ne saisissez pas* de schéma (tel que **`https://`**) ni de barre oblique de fin. Par exemple, **`myvcenter.exemple.com`** ou **`192.0.2.100:9090`**

Valeur	Description
Utilisateur	(Requis) Saisissez le nom d'utilisateur d'un utilisateur ayant au minimum le rôle Lecture seule. Les noms d'utilisateurs sont sensibles à la casse.
Mot de passe	(Requis) Entrez le mot de passe de l'utilisateur.
IP NSX	Si vous utilisez vCenter Network Security Visualization (NSX), entrez son adresse IP.
Utilisateur NSX	Saisissez le nom d'utilisateur d'un utilisateur NSX ayant au moins le rôle d'auditeur.
Type NSX	Saisissez **NSX-T**.
Mot de passe NSX	Saisissez le mot de passe de l'utilisateur NSX.
Certificat vCenter	

Voici un exemple de récupération réussie d'une chaîne de certificats :



Le développement de la chaîne de l'autorité de certification en haut de la boîte de dialogue affiche les certificats de la manière suivante.

S'il n'est pas possible de récupérer le certificat de cette manière, vous pouvez obtenir la chaîne de certificats manuellement, comme indiqué dans la section Obtenir de manière manuelle un certificat de Chaîne d'autorité de certification (CA), à la page 21.

Étape 5 Cliquez sur**Test** et assurez-vous que **Test connection succeeded** s'affiche avant que vous n'enregistriez le connecteur.

Étape 6 Cliquez sur **Save** (enregistrer).

Prochaine étape

Créer un adaptateur, à la page 16

Créer un adaptateur

Un *adaptateur* est une connexion sécurisée à centre de gestion vers laquelle vous envoyez des informations sur le réseau à partir d'objets dans le nuage afin de les utiliser dans les stratégies de contrôle d'accès.

Tout d'abord, vous pouvez éventuellement récupérer la chaîne de l'autorité de certification, qui est nécessaire pour se connecter en toute sécurité à centre de gestion.

La recherche de la chaîne de l'autorité de certification ne nécessite que le nom d'hôte de centre de gestion; la création de l'adaptateur requiert un nom d'utilisateur, un mot de passe et d'autres informations.

Créer un utilisateur de Cisco Secure Firewall Management Center pour le connecteur d'attributs dynamiques

Nous vous recommandons de créer un utilisateur de centre de gestion dédié à l'adaptateur connecteur d'attributs dynamiques. La création d'un utilisateur de centre de gestion dédié permet d'éviter des problèmes tels que des déconnexions inattendues du centre de gestion, car le connecteur d'attributs dynamiques se connecte périodiquement à l'aide d'une API REST pour mettre à jour le centre de gestion avec des objets dynamiques nouveaux et actualisés.

L'utilisateur de centre de gestion doit avoir au moins les privilèges d'administrateur d'accès.

Étape 1 Connectez-vous au centre de gestion si vous ne l'avez pas encore fait.

Étape 2 Cliquez sur **System** (⚙) > **Utilisateurs**.

Étape 3 Cliquez sur **Créer un utilisateur**.

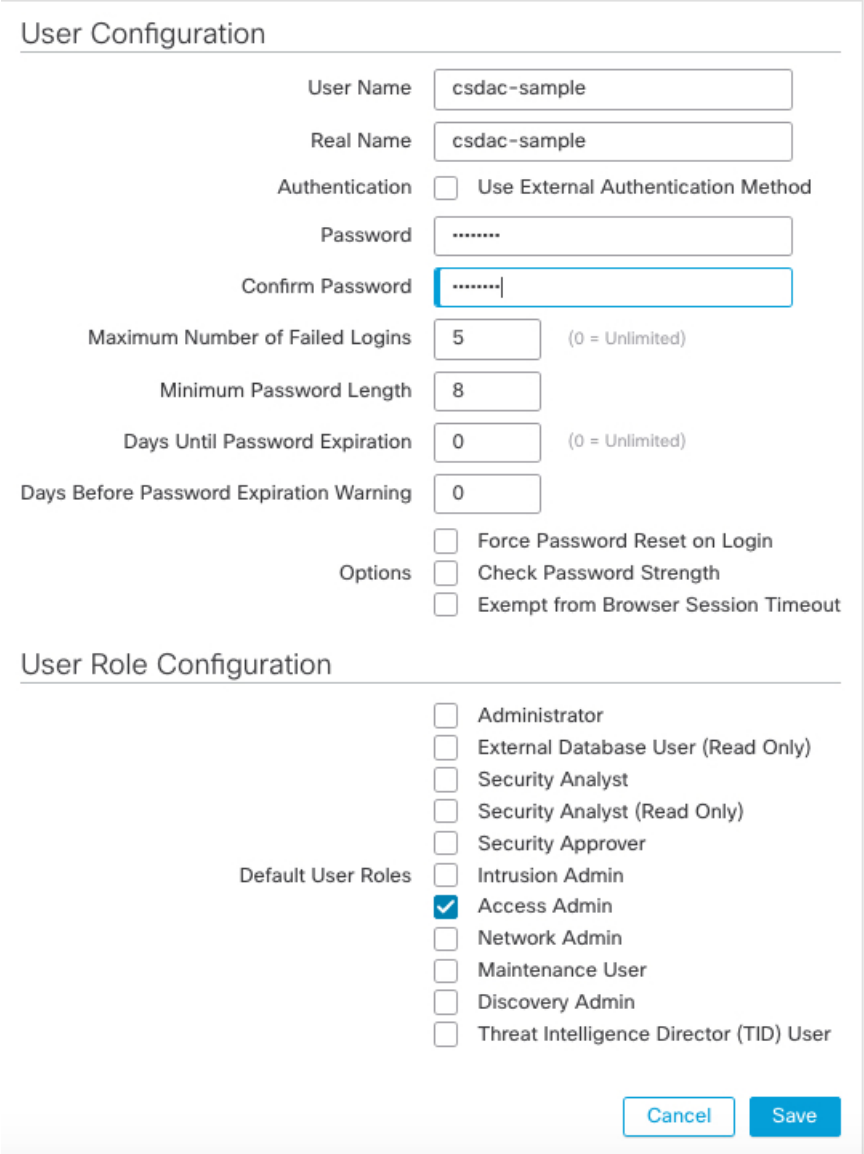
Étape 4 Saisissez les informations nécessaires à la création de l'utilisateur.

Étape 5 Sous Configuration du rôle de l'utilisateur, cochez l'un des rôles par défaut suivants ou un rôle personnalisé avec le même niveau de privilège :

- **Administrateur**

- **Administrateur d’accès**
- **Administrateur de réseau**

La figure suivante présente un exemple.



Vous pouvez également choisir un rôle personnalisé disposant de privilèges suffisants pour autoriser les actions REST ou un rôle par défaut différent disposant de privilèges suffisants. Pour plus d'informations sur les rôles par défaut, voir la section Rôles d'utilisateur dans le chapitre sur les comptes d'utilisateur.

Prochaine étape

Créer un adaptateur, à la page 16

Comment créer un adaptateur On-Prem Firewall Management Center

Cette rubrique explique comment créer un adaptateur pour transférer des objets dynamiques deconnecteur d'attributs dynamiques vers centre de gestion.

Avant de commencer

Consultez Créer un utilisateur de Cisco Secure Firewall Management Center pour le connecteur d'attributs dynamiques, à la page 16.

Étape 1 Connectez-vous au connecteur d'attributs dynamiques.

Étape 2 Cliquez sur **Adaptateurs**

Étape 3 Effectuez l'une des actions suivantes :

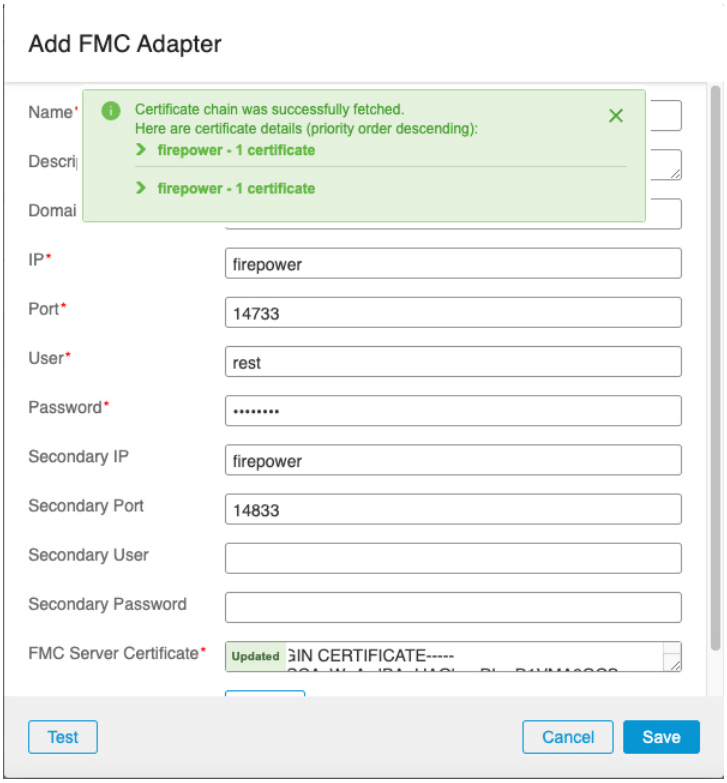
- Ajouter un nouveau connecteur : cliquez sur Icône ajouter (), puis sur le nom du connecteur.
- Modifier ou supprimer un connecteur : Cliquez sur **Plus** (), puis sur **Modifier** ou **Supprimer** à la fin de la ligne.

Étape 4 Ensuite, entrez l'information suivante.

Valeur	Description
Nom	(Requis) Saisissez un nom unique pour identifier cet adaptateur.
Description	Description facultative de l'adaptateur.
Domaine	Saisissez le domaine Cisco Secure Firewall Management Center Virtual dans lequel vous souhaitez créer des objets dynamiques. Laissez le champ vide pour créer des objets dynamiques dans le domaine Global. Par exemple, `Global/MySubdomain`
IP	(Requis) Saisissez le nom d'hôte ou l'adresse IP de Cisco Secure Firewall Management Center Virtual. Le nom d'hôte ou l'adresse IP que vous saisissez doit correspondre exactement au nom commun du certificat d'autorité de certification utilisé pour se connecter en toute sécurité.
Port	(Requis) Saisissez le port TLS utilisé par votre .Cisco Secure Firewall Management Center Virtual
Utilisateur	(Requis) Saisissez le nom d'un utilisateur Cisco Secure Firewall Management Center Virtual ayant au moins le rôle d'administrateur réseau.
Mot de passe	(Requis) Entrez le mot de passe de l'utilisateur.
Adresse IP secondaire	(Haute disponibilité uniquement). Saisissez le nom d hôte ou l'adresse IP secondaire de Cisco Secure Firewall Management Center Virtual. Le nom d'hôte ou l'adresse IP que vous saisissez doit correspondre exactement au nom commun du certificat d'autorité de certification utilisé pour se connecter en toute sécurité.
Port secondaire	(Haute disponibilité uniquement). Saisissez le port TLS utilisé par votre serveur secondaire Cisco Secure Firewall Management Center Virtual.

Valeur	Description
Utilisateur secondaire	(Haute disponibilité uniquement). Saisissez le nom d'un utilisateur secondaire de Cisco Secure Firewall Management Center Virtual ayant au moins le rôle d'administrateur réseau.
Mot de passe secondaire	(Haute disponibilité uniquement). Entrez le mot de passe de l'utilisateur.
Certificat de serveur	Cliquez sur **Récupérer** pour récupérer automatiquement le certificat.

Voici un exemple de récupération réussie d'une chaîne de certificats :



Le développement de la chaîne de l'autorité de certification en haut de la boîte de dialogue affiche les certificats de la manière suivante.

S'il n'est pas possible de récupérer le certificat de cette manière, vous pouvez obtenir la chaîne de certificats manuellement, comme indiqué dans la section Obtenir de manière manuelle un certificat de Chaîne d'autorité de certification (CA), à la page 21.

Étape 5 cliquez sur **Test** et assurez-vous que l'essai réussit avant de sauvegarder l'adaptateur

Étape 6 Cliquez sur **Save** (enregistrer).

Créer un adaptateur Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Cette rubrique explique comment créer un adaptateur pour transférer des objets dynamiques du connecteur d'attributs dynamiques vers un centre de gestion géré sur le Cisco Defense Orchestrator.

Avant de créer un Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), obtenez d'abord les informations suivantes : Obtenez votre URL de base et votre jeton API, à la page 20.

Obtenez votre URL de base et votre jeton API

Cette tâche explique comment obtenir l'URL et le jeton API de CDO nécessaires à la création d'un adaptateur Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Avant de commencer

Vous devez être un Super Administrateur de CDO pour effectuer les tâches décrites dans cette section.

Étape 1 Connectez-vous à CDO en tant qu'utilisateur ayant le rôle de Super Administrateur.

Étape 2 Dans le coin supérieur droit de la page, cliquez sur **Paramètres**.

Étape 3 Cliquez sur **Paramètres généraux**.

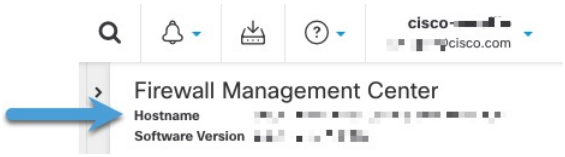
Étape 4 En regard du jeton API, cliquez sur **Actualiser**.

Étape 5 Copiez le jeton API dans un fichier texte pour une utilisation ultérieure.

Étape 6 Cliquez sur **Outils et services** > **Centre de gestion du pare-feu**.

Étape 7 Cliquez sur le nom du centre de gestion auquel envoyer les données connecteur d'attributs dynamiques.

Étape 8 La valeur du **Nom d'hôte**, précédée de **https://**, est l'URL de base.
Voici un exemple :



Prochaine étape

Comment créer un adaptateur Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), à la page 21.

Comment créer un adaptateur Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Cette tâche explique comment créer un adaptateur Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) qui envoie des données depuis le connecteur d'attributs dynamiques vers un périphérique géré par CDO.

Avant de commencer

Vous devez obtenir l'URL de base du centre de gestion et le jeton API de la part de CDO avant de pouvoir effectuer cette tâche. Pour en savoir plus, consultez Obtenez votre URL de base et votre jeton API, à la page 20.

Étape 1 Connectez-vous au connecteur d'attributs dynamiques.

Étape 2 Cliquez sur **Adaptateurs**

Étape 3 Effectuez l'une des actions suivantes :

- Ajouter un nouveau connecteur : cliquez sur Icône ajouter (), puis sur le nom du connecteur.
- Modifier ou supprimer un connecteur : Cliquez sur **Plus** (), puis sur **Modifier** ou **Supprimer** à la fin de la ligne.

Étape 4 Ensuite, entrez l'information suivante.

Valeur	Description
Nom	(Requis) Saisissez un nom unique pour identifier cet adaptateur.
Description	Description facultative de l'adaptateur.
Url de base	(Requis) Utilisez l'URL de base que vous avez trouvée dans Obtenez votre URL de base et votre jeton API, à la page 20.
Jeton API	(Requis) Utilisez le jeton API que vous avez trouvé dans Obtenez votre URL de base et votre jeton API, à la page 20.

Étape 5 cliquez sur **Test** et assurez-vous que l'essai réussit avant de sauvegarder l'adaptateur

Étape 6 Cliquez sur **Save** (enregistrer).

Prochaine étape

Créer des filtres d'attributs dynamiques, à la page 24.

Obtenir de manière manuelle un certificat de Chaîne d'autorité de certification (CA)

Si vous ne pouvez pas récupérer automatiquement la chaîne de l'autorité de certification, utilisez l'une des procédures suivantes spécifiques au navigateur pour obtenir une chaîne de certificat utilisée pour se connecter en toute sécurité à vCenter, NSX ou à Centre de gestion.

La *chaîne de certificats* est constituée du certificat racine et de tous les certificats subordonnés.

Vous devez utiliser l'une de ces procédures pour vous connecter aux éléments suivants :

- vCenter ou NSX

  Il n'est pas nécessaire d'obtenir une chaîne de certificats pour se connecter à Azure ou AWS.

- Centre de gestion

Avant d'utiliser cette procédure, consultez la section relative à l'extraction automatique de la chaîne de l'autorité de certification dans :

- Créer un connecteur vCenter, à la page 14

Obtenir une chaîne de certificats - Mac (Chrome et Firefox)

Utilisez cette procédure pour obtenir une chaîne de certificats à l'aide des navigateurs Chrome et Firefox sur Mac OS.

1. Ouvrez une fenêtre de terminal.
2. Entrez la commande suivante.

   ```
   security verify-cert -P url[:port]
   ```

   où url est l'URL (y compris le schéma) de vCenter ou de Centre de gestion. Par exemple :

   ```
   security verify-cert -P https://myvcenter.example.com
   ```

   Si vous accédez à vCenter ou à centre de gestion en utilisant NAT ou PAT, vous pouvez ajouter un port comme suit :

   ```
   security verify-cert -P https://myvcenter.example.com:12345
   ```

3. Enregistrer l'ensemble de la chaîne de certificats dans un fichier texte en clair.
   - *Inclure* tous les délimiteurs`----DÉBUT DU CERTIFICAT-----` et `-----FIN DU CERTIFICAT----`.
   - *Exclure* tout texte superflu (par exemple, le nom du certificat et tout texte contenu dans les crochets d'angle (< et >) ainsi que les crochets eux-mêmes.
4. Répétez ces tâches pour le vCenter et le Centre de gestion.

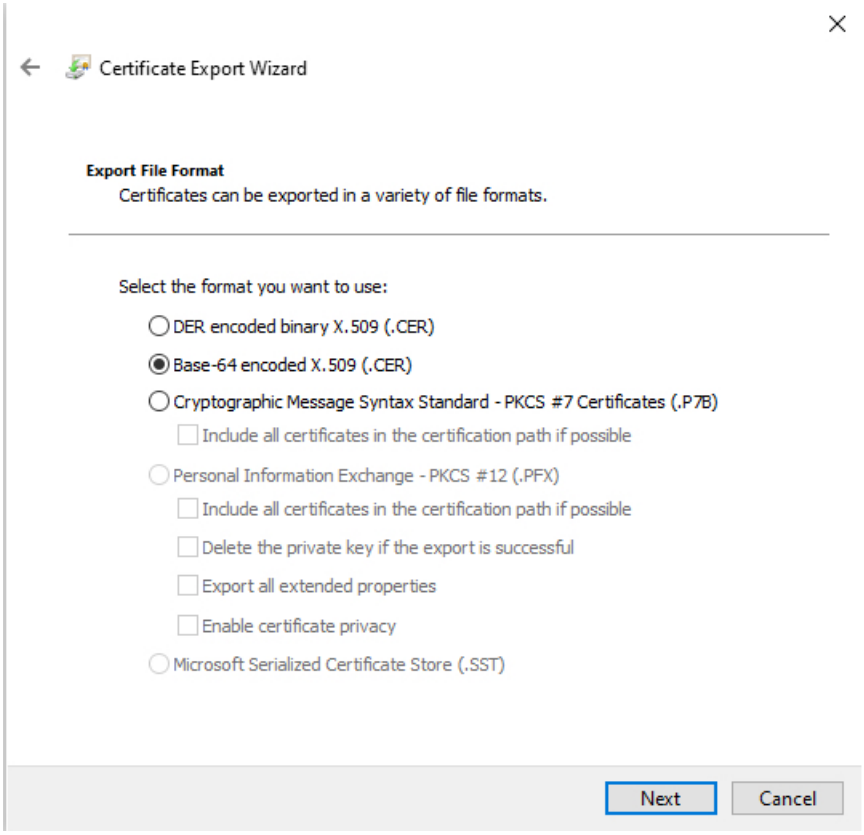
Obtenir une chaîne de certificats - Windows Chrome

Utilisez cette procédure pour obtenir une chaîne de certificats à l'aide du navigateur Chrome sous Windows.

1. Se connecter à vCenter ou à Centre de gestion en utilisant Chrome.
2. Dans la barre d'adresse du navigateur, cliquez sur le cadenas à gauche du nom d'hôte.
3. Cliquez sur **Certificats**.
4. Cliquez sur l'onglet **Chemin de certification**.
5. Cliquez sur le premier certificat de la chaîne.
6. Cliquez sur **Afficher le certificat**.
7. Cliquez sur l'onglet **Détails**.

8. Cliquez sur **Copier dans un fichier**.
9. Suivez les invites pour créer un fichier de certificat au format CER qui inclut l'ensemble de la chaîne de certificats.

   Lorsque vous êtes invité à choisir un format de fichier d'exportation, cliquez sur **Base 64-Encoded X.509 (.CER)** comme le montre la figure suivante.



10. Suivez les invites pour terminer l'exportation.
11. Ouvrez le certificat dans un éditeur de texte.
12. Répétez le processus pour tous les certificats de la chaîne.

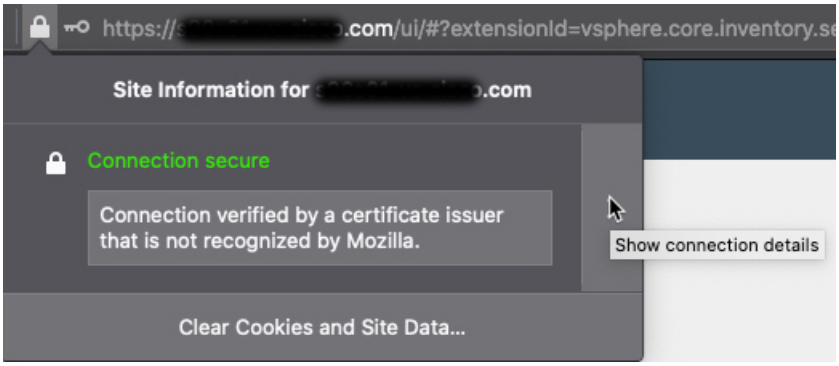
    Vous devez coller chaque certificat dans l'éditeur de texte dans l'ordre, du premier au dernier.
13. Répétez ces tâches pour le vCenter et le FMC.

Obtenir une chaîne de certificats - Firefox sous Windows

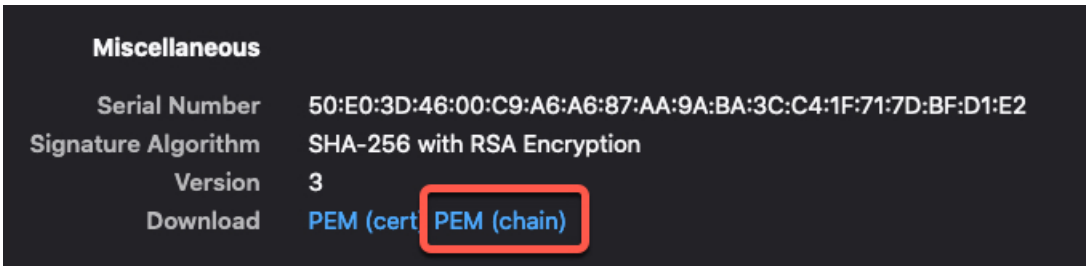
La procédure suivante permet d'obtenir une chaîne de certificats pour le navigateur Firefox sous Windows ou Mac OS.

1. Connectez-vous à vCenter ou à Centre de gestion en utilisant Firefox.
2. Cliquez sur le cadenas à gauche du nom de l'hôte.

3. Cliquez sur la flèche droite (**Afficher les détails de la connexion**). La figure suivante présente un exemple.



4. Cliquez sur **Plus d'informations**.
5. Cliquez sur **Afficher le certificat**.
6. Si la boîte de dialogue résultante comporte des onglets, cliquez sur l'onglet correspondant à l'autorité de certification de premier niveau.
7. Faites défiler jusqu'à la section Divers.
8. Cliquez sur **PEM (chaîne)** sur la ligne Téléchargement. La figure suivante présente un exemple.



9. Enregistrez le fichier.
10. Répétez ces tâches pour le vCenter et le Centre de gestion.

Créer des filtres d'attributs dynamiques

Les filtres d'attributs dynamiques que vous définissez à l'aide du connecteur d'attributs dynamiques Cisco Secure sont exposés dans le centre de gestion en tant qu'objets dynamiques pouvant être utilisés dans les politiques de contrôle d'accès. Par exemple, vous pouvez restreindre l'accès à un serveur AWS pour le service Finances aux seuls membres du groupe Finances défini dans Microsoft Active Directory.

Remarque Vous ne pouvez pas créer de filtres d'attributs dynamiques pour GitHub, Office 365, ou Balises de service Azure. Ces types d'objets en nuage fournissent leurs propres adresses IP.

Pour plus d'informations sur les règles de contrôle d'accès, consultez Créer des règles de contrôle d'accès à l'aide de filtres d'attributs dynamiques.

Avant de commencer

Effectuez toutes les tâches suivantes :

- Installer les logiciels prérequis
- Créer un connecteur, à la page 1
- Créer un adaptateur, à la page 16

Étape 1 Connectez-vous au connecteur d'attributs dynamiques.

Étape 2 Cliquez sur **Filtres d'attributs dynamiques**.

Étape 3 Effectuez l'une des actions suivantes :

- Ajouter un nouveau filtre : cliquez sur **Ajoutez** (+).
- Modifier ou supprimer un filtre : cliquez sur **Plus** (⋮), puis cliquez sur **Modifier** ou **Supprimer** à la fin de la ligne.

Étape 4 Ensuite, entrez l'information suivante.

Article	Description
Nom	Nom unique permettant d'identifier le filtre dynamique (en tant qu'objet dynamique) dans la stratégie de contrôle d'accès et dans le Gestionnaire d'objets centre de gestion (**Attributs externes** > **Objet dynamique**).
Personne rassembleuse	Dans la liste, cliquez sur le nom d'un connecteur à utiliser.
Requête	• Ajouter un nouveau filtre : cliquez sur **Ajoutez** (+). • Modifier ou supprimer un filtre : cliquez sur **Plus** (⋮), puis cliquez sur **Modifier** ou **Supprimer** à la fin de la ligne.

Étape 5 Pour ajouter ou modifier une requête, saisissez les informations suivantes.

Article	Description
Clé	Cliquez sur une clé dans la liste. Les clés sont extraites du connecteur.
Operation (Opération)	Cliquez sur l'un des éléments suivants : • **Égal à** pour faire correspondre exactement la clé à la valeur. • **Contient** pour faire correspondre la clé à la valeur si une partie de la valeur correspond.

Article	Description
Valeurs	Cliquez sur **N'importe lequel** ou **Tous** et cliquez sur une ou plusieurs valeurs de la liste. Cliquez sur **Ajouter une autre valeur** pour ajouter des valeurs à votre requête.

Étape 6 Cliquez sur **Afficher l'aperçu** pour afficher la liste des réseaux ou des adresses IP renvoyés par votre requête.

Étape 7 Lorsque vous avez terminé, cliquez sur **Enregistrer**.

Étape 8 (Facultatif) Vérifiez l'objet dynamique dans lecentre de gestion.

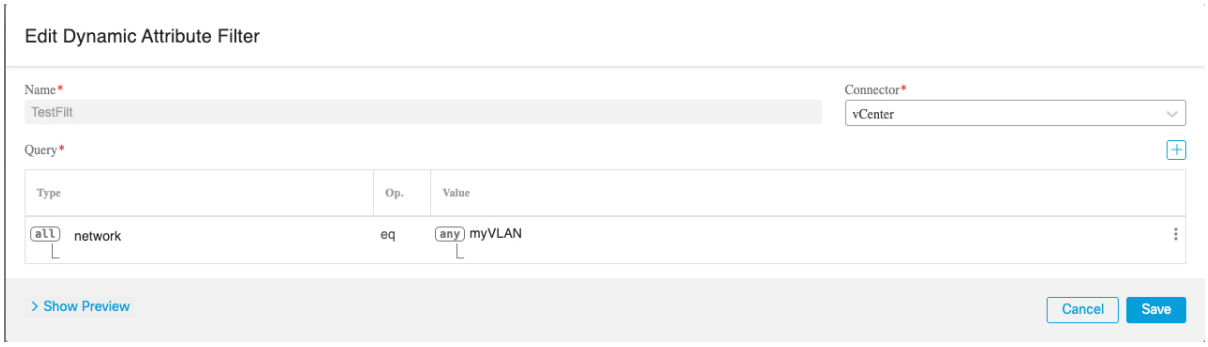
a) Connectez-vous à centre de gestion en tant qu'utilisateur ayant au moins le rôle d'administrateur de réseau.
b) Cliquez sur **Objets** > **Gestionnaire d'objets**.
c) Dans le volet gauche, cliquez sur **Attributs externes** > **Objet dynamique**.
La requête d'attribut dynamique que vous avez créée doit être affichée en tant qu'objet dynamique.

Exemples de filtres d'attributs dynamiques

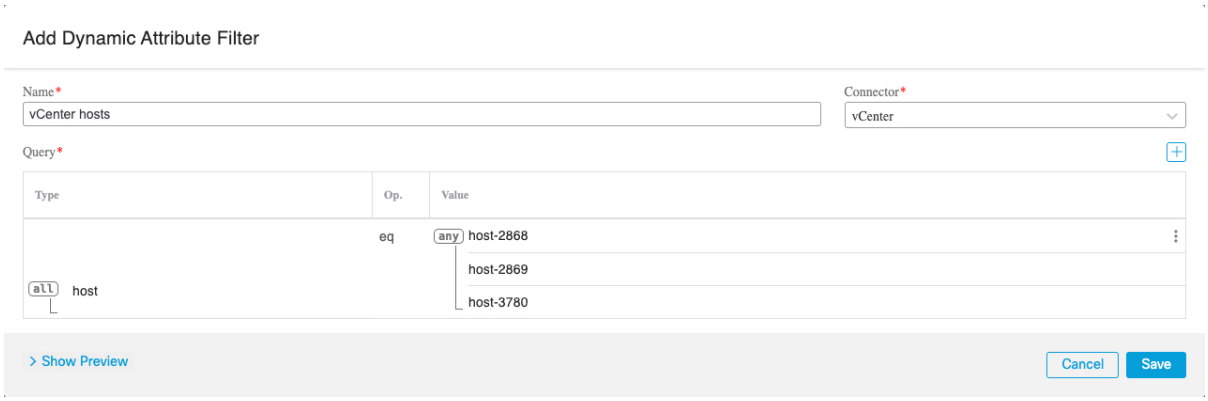
Cette rubrique présente quelques exemples de mise en place de filtres d'attributs dynamiques.

Exemples : vCenter

L'exemple suivant montre un critère : un VLAN.

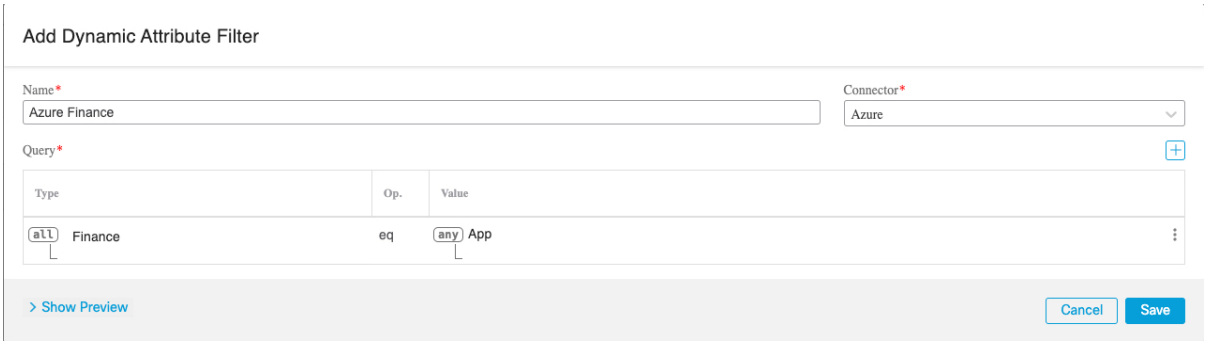


L'exemple suivant montre trois critères qui sont combinés avec OR : la requête correspond à n'importe lequel des trois hôtes.



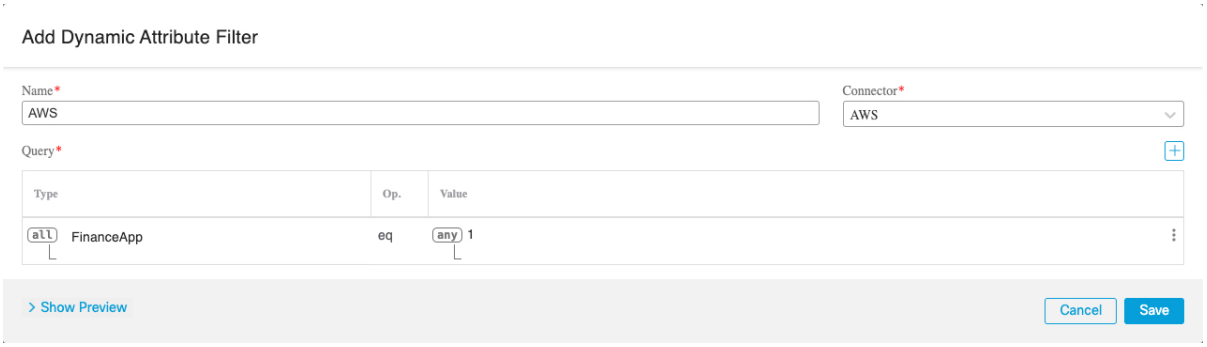
Exemple : Azure

L'exemple suivant présente un seul critère : un serveur étiqueté en tant qu'application financière.



Exemple : AWS

L'exemple suivant présente un seul critère : une FinanceApp avec une valeur de 1.



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.