Connecteur d'attributs dynamiques Cisco Secure

Les rubriques suivantes expliquent comment configurer et utiliser Connecteur d'attributs dynamiques Cisco Secure.

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 (CDO).

Connecteurs pris en charge

Nous prenons actuellement en charge :

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.

- 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.

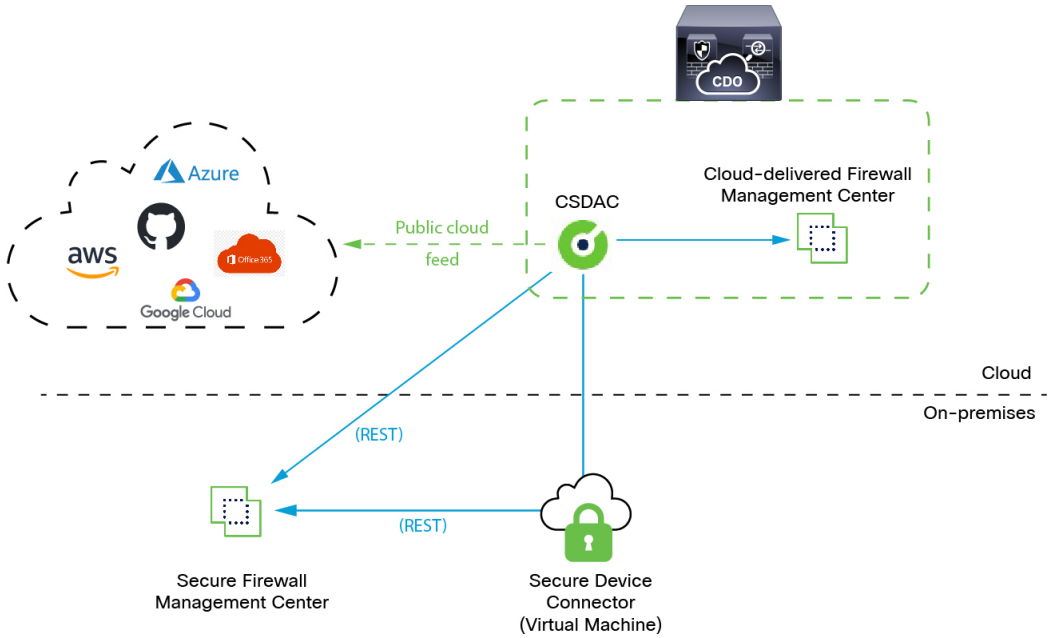
- Adresses IP Office 365

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

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).

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



- Le système prend en charge certains fournisseurs de nuage public.

  Cette rubrique traite des *connecteurs* pris en charge (qui sont les connexions à ces fournisseurs).

- *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 .

    Ce type de périphérique de 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.

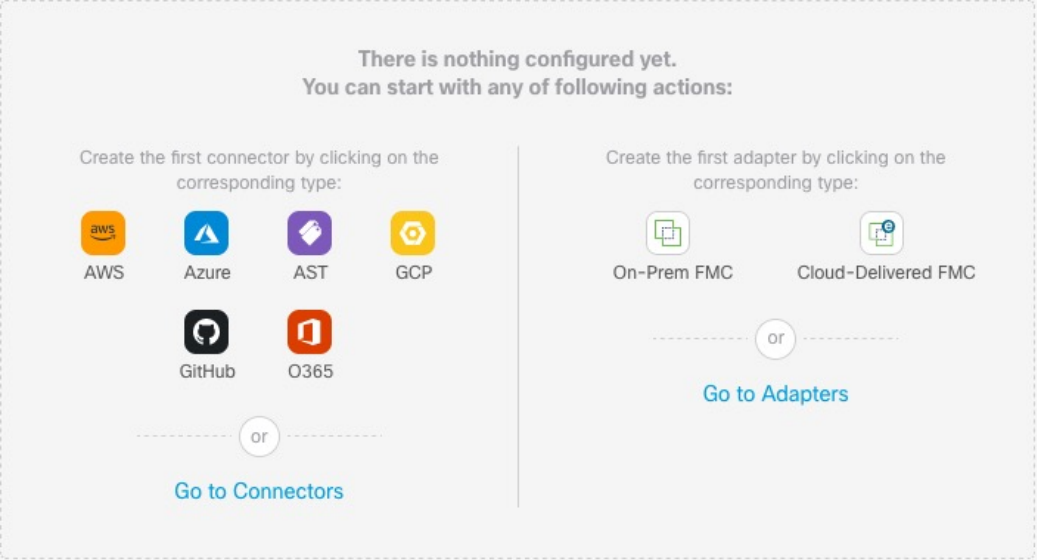
Historique pour le Connecteur d'attributs dynamiques Cisco Secure

Caractéristiques	Centre de gestion Min.	Cisco Secure Firewall Management Center Min.	Détails
	N’importe lequel	7.3.0	Cette fonctionnalité a été introduite. Le Connecteur d'attributs dynamiques Cisco Secure est maintenant inclus dans le Cisco Secure Firewall Management Center. Vous pouvez utiliser les connecteur d'attributs dynamiques pour obtenir les adresses IP des plateformes en nuage telles que Microsoft Azure dans les règles de contrôle d’accès sans avoir à déployer sur des périphériques gérés. Pour de plus amples renseignements : • Le connecteur d'attributs dynamiques inclus avec ce produit : À propos du connecteur d'attributs dynamiques Cisco Secure, à la page 1 • connecteur d'attributs dynamiques autonome : Guide de configuration du connecteur d'attributs dynamiques Cisco Secure Nouvel écran ou écran modifié : **Intégration** > **Connecteur d'attributs dynamiques Cisco**

À propos du tableau de bord

Pour accéder au tableau de bord Connecteur d'attributs dynamiques Cisco Secure, connectez-vous à CDO et cliquez sur **Outils et services** > **Connecteur d'attributs dynamiques** > **Tableau de bord** en haut de la page.

La page Dashboard (tableau de bord) Connecteur d'attributs dynamiques Cisco Secure vous donne un aperçu de l’état de vos connecteurs, adaptateurs et filtres. Voici un exemple du tableau de bord d’un système non configuré :



Voici certaines des choses que vous pouvez faire avec le tableau de bord :

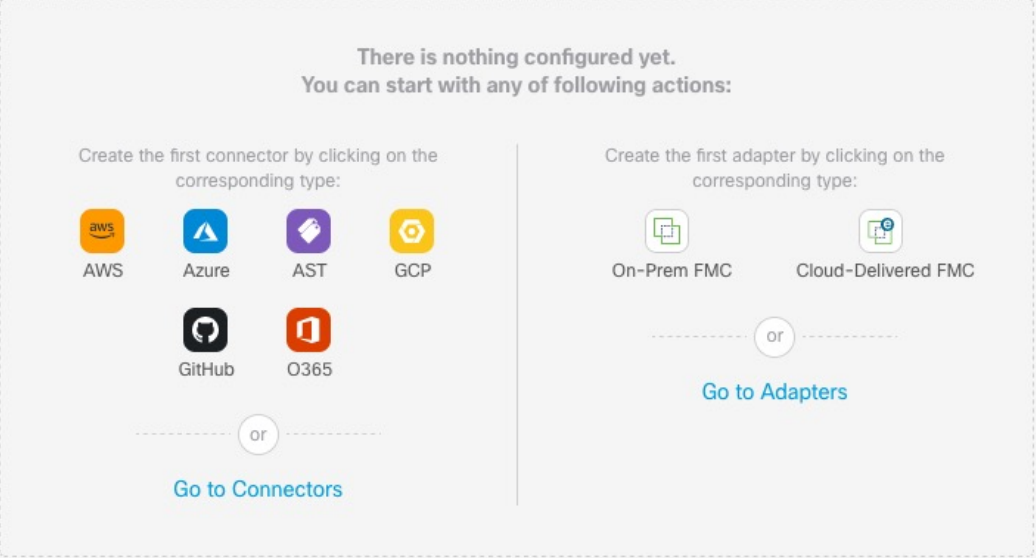
- Ajouter, modifier et supprimer des connecteurs,des filtres d’attributs dynamiquesdes adaptateurs.
- Découvrez comment les connecteurs,les filtres d’attributs dynamiquesles adaptateurs sont liés les uns aux autres.
- Affichez les avertissements et les erreurs.

Thèmes connexes

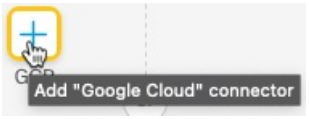
- Tableau de bord d’un système non configuré, à la page 4
- Tableau de bord d’un système configuré, à la page 5
- Ajouter, modifier ou supprimer des connecteurs, à la page 7
- Ajouter, modifier ou supprimer des filtres d'attributs dynamiques, à la page 8
- Ajouter, modifier ou supprimer des adaptateurs, à la page 10

Tableau de bord d’un système non configuré

Exemple de page Connecteur d'attributs dynamiques Cisco Secure de tableau de bord d’un système non configuré :



Le tableau de bord affiche initialement tous les types de connecteurs et d'adaptateurs que vous pouvez configurer pour votre système. Vous pouvez effectuer l'une des opérations suivantes :

- Passez le pointeur de la souris sur un connecteur ou un adaptateur et cliquez sur 

pour en créer un nouveau.
- Cliquez sur **Go to Connectors** (accéder aux connecteurs) pour ajouter, modifier ou supprimer des connecteurs (utile pour la création, la modification ou la suppression de plusieurs connecteurs à la fois).

  Pour en savoir plus, consultez Créer un connecteur, à la page 11.
- Cliquez sur **Go to Adapters** (accéder aux adaptateurs) pour ajouter, modifier ou supprimer des adaptateurs (utile pour la création, la modification ou la suppression de plusieurs adaptateurs en même temps).

  Pour en savoir plus, consultez Créer un adaptateur, à la page 25.

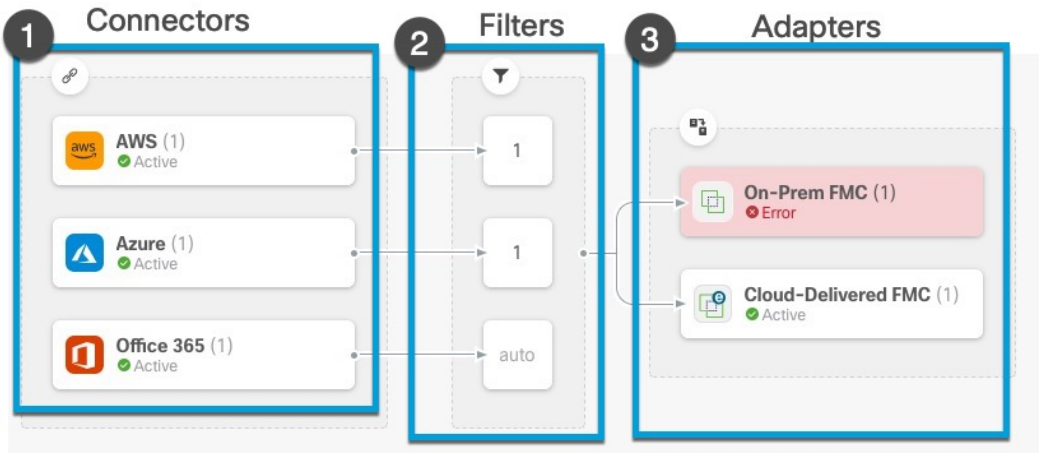
Thèmes connexes

- Tableau de bord d'un système configuré, à la page 5
- Ajouter, modifier ou supprimer des connecteurs, à la page 7
- Ajouter, modifier ou supprimer des filtres d'attributs dynamiques, à la page 8
- Ajouter, modifier ou supprimer des adaptateurs, à la page 10

Tableau de bord d'un système configuré

Exemple de page de tableau de bord Connecteur d'attributs dynamiques Cisco Secure d'un système configuré :

Cliquez sur une zone de la figure pour en savoir plus ou cliquez sur l'un des liens qui suivent la figure.



1 Créer un connecteur, à la page 11
2 Créer des filtres d'attributs dynamiques, à la page 27
3 Créer un adaptateur, à la page 25

Le tableau de bord affiche les éléments suivants (de gauche à droite) :

Colonne Connecteurs	Colonne de filtres	Colonne Adaptateurs
Liste de connecteurs avec un numéro indiquant combien de connecteurs de chaque type sont configurés. Les connecteurs collectent des attributs dynamiques qui pourraient être envoyés à l'adaptateur configuré. Les filtres d'attributs dynamiques spécifient les données qui sont envoyées. Cliquez sur pour afficher plus d'informations sur tous les connecteurs configurés. Vous pouvez également cliquer sur le nom d'un connecteur pour ajouter, modifier ou supprimer des connecteurs. ou pour afficher des renseignements détaillés les concernant. Pour en savoir plus, consultez Ajouter, modifier ou supprimer des connecteurs, à la page 7.	Liste des filtres d'attributs dynamiques associés à chaque connecteur avec un numéro indiquant le nombre de filtres associés à un connecteur. Cliquez sur pour afficher plus d'informations sur tous les filtres configurés. Vous pouvez également cliquer sur le nom d'un filtre pour ajouter, modifier ou supprimer des filtres. ou pour afficher des renseignements détaillés les concernant. Pour en savoir plus, consultez Ajouter, modifier ou supprimer des filtres d'attributs dynamiques, à la page 8.	Liste des adaptateurs Les adaptateurs reçoivent des objets dynamiques des connecteurs configurés à l'aide des filtres d'attributs dynamiques configurés; ces objets dynamiques peuvent être utilisés dans les politiques de contrôle d'accès sans qu'il soit nécessaire de les déployer. Cliquez sur pour afficher plus d'informations sur tous les adaptateurs configurés. Vous pouvez également cliquer sur le nom d'un adaptateur pour ajouter, modifier ou supprimer des adaptateurs. ou pour afficher des renseignements détaillés les concernant. Pour en savoir plus, consultez Ajouter, modifier ou supprimer des adaptateurs, à la page 10.

Remarque Certains connecteurs, comme Outlook 365 et les balises Azure Service, extraient automatiquement les objets dynamiques disponibles sans qu'il soit nécessaire d'utiliser des filtres d'attributs dynamiques. Ces connecteurs affichent **Auto** dans la colonne .

Le tableau de bord indique si un objet est disponible ou non. La page du tableau de bord est actualisée toutes les 15 secondes, mais vous pouvez cliquer sur **Actualisation** ( ) en haut de la page à tout moment pour l'actualiser immédiatement. Si le problème persiste, vérifiez votre connexion réseau.

Thèmes connexes

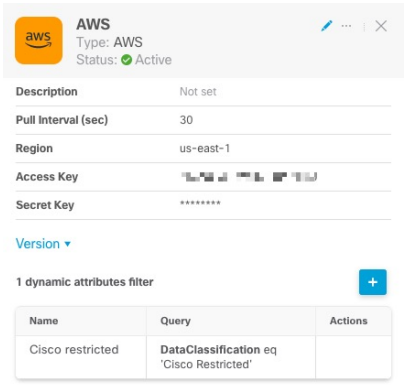
- Ajouter, modifier ou supprimer des connecteurs, à la page 7
- Ajouter, modifier ou supprimer des filtres d'attributs dynamiques, à la page 8
- Ajouter, modifier ou supprimer des adaptateurs, à la page 10

Ajouter, modifier ou supprimer des connecteurs

Le tableau de bord vous permet d'afficher ou de modifier les connecteurs. Vous pouvez cliquer sur le nom d'un connecteur pour afficher toutes les instances de ce connecteur ou vous pouvez cliquer sur pour accéder aux options supplémentaires suivantes :

- **Accédez aux connecteurs** pour afficher tous les connecteurs en même temps; vous pouvez y ajouter, modifier et supprimer des connecteurs.
- **Ajouter un connecteur** > ***type (*** ajouter un type de connecteur) pour ajouter un connecteur du type indiqué.

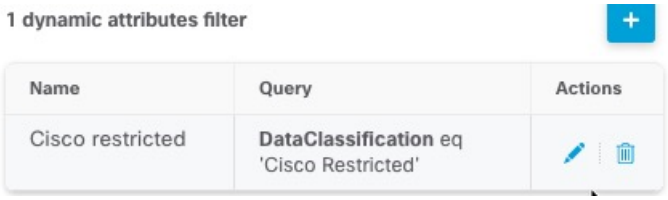
Cliquez sur un connecteur dans la colonne des connecteurs ( ) pour en savoir plus sur le connecteur; voici un exemple :



Vous avez les options suivantes :

- Cliquez sur Icône modifier ( ) pour modifier ce connecteur.
- Cliquez sur Icône Autres ( ) pour avoir accès à des options supplémentaires.
- Cliquez sur pour fermer le panneau.
- Cliquez sur **Version** pour afficher la version. Vous pouvez également copier la version dans le presse-papiers au besoin pour Cisco TAC.

Le tableau au bas du panneau vous permet d'ajouter des filtres d'attributs dynamiques; ou modifier ou supprimer des connecteurs connecteur d'attributs dynamiques. Voici un exemple :



Cliquez sur Icône ajouter ( ) pour ajouter un filtre d'attributs dynamiques pour ce connecteur. Pour en savoir plus, consultez Créer des filtres d'attributs dynamiques, à la page 27.

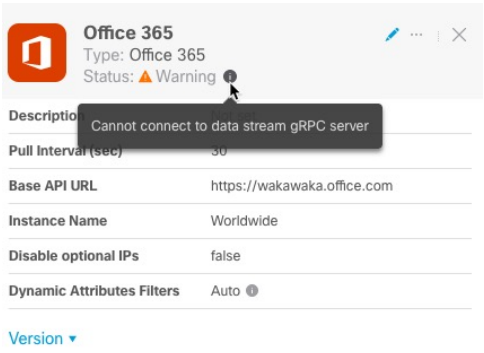
Passez le pointeur de la souris sur la colonne Actions pour modifier ou supprimer le connecteur indiqué.

Afficher les informations d'erreur

Pour afficher les renseignements d'erreur pour un connecteur :

1. Dans le tableau de bord, cliquez sur le nom du connecteur qui affiche l'erreur.
2. Dans le volet de droite, cliquez sur **Information** ( ).

   Voici un exemple.



3. Pour résoudre ce problème, modifiez les paramètres du connecteur comme indiqué dans Créer un connecteur Office 365, à la page 22.
4. Si vous ne pouvez pas résoudre le problème, cliquez sur **Version** et copiez la version dans un fichier texte.
5. Obtenez votre ID de détenteur CDO comme indiqué dans la section Obtenir votre identifiant de service partagé, à la page 32
6. Fournissez toutes ces informations au TAC de Cisco.

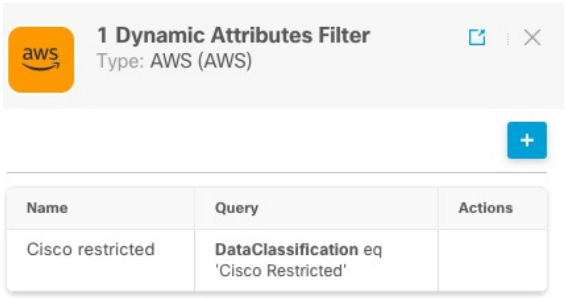
Ajouter, modifier ou supprimer des filtres d'attributs dynamiques

Le tableau de bord vous permet d'ajouter, de modifier ou de supprimer des filtres d'attributs dynamiques. Vous pouvez cliquer sur le nom d'un filtre pour afficher toutes les instances de ce filtre ou vous pouvez cliquer sur pour accéder aux options supplémentaires suivantes :

- **Accédez au filtres d'attributs dynamiques** pour afficher tous les filtres d'attributs dynamiques configurés. Vous pouvez ajouter, modifier ou supprimer des filtres d'attributs dynamiques à partir de là.
- **Ajouter des filtres d'attributs dynamiques** pour ajouter un filtre.

Pour plus d'informations sur l'ajout de filtres d'attributs dynamiques, consultez Créer des filtres d'attributs dynamiques, à la page 27.

Cliquez sur un adaptateur dans la colonne des filtres ( ) pour afficher plus d'informations à ce sujet; un exemple :



Remarque Certains connecteurs, comme Outlook 365 et les balises Azure Service, extraient automatiquement les objets dynamiques disponibles sans qu'il soit nécessaire d'utiliser des filtres d'attributs dynamiques. Ces connecteurs affichent **Auto** dans la colonne .

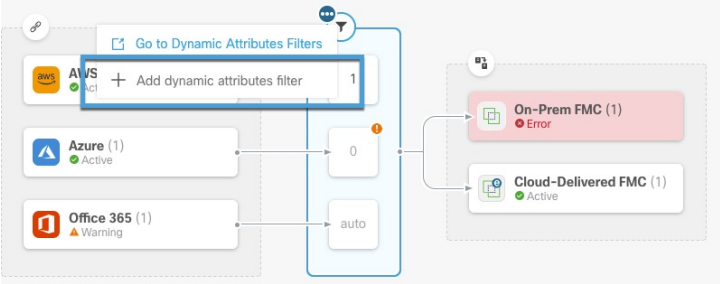
Vous avez les options suivantes :

- Cliquez sur une instance de filtre pour afficher des informations résumées sur les filtres d'attributs dynamiques associés à un connecteur.
- Cliquez sur Icône ajouter ( ) pour ajouter un nouveau filtre d'attributs dynamiques.

  Pour en savoir plus, consultez Créer des filtres d'attributs dynamiques, à la page 27.

- Cliquez sur dans la colonne des filtres ( ) pour indiquer qu'aucun filtre d'attribut dynamique n'est associé au connecteur indiqué. Sans filtres associés, le connecteur ne peut rien envoyer à centre de gestion.

  Une façon de résoudre le problème consiste à cliquer sur dans la colonne des filtres, puis à cliquer sur **Add Dynamic Attributes Filter** (Ajouter un filtre d'attributs dynamiques). Voici un exemple.



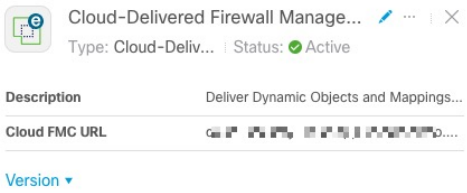
- Cliquez sur pour ajouter, modifier ou supprimer des filtres.
- Cliquez sur pour fermer le panneau.

Ajouter, modifier ou supprimer des adaptateurs

Le tableau de bord vous permet d'afficher ou de modifier les adaptateurs. Vous pouvez cliquer sur le nom d'un adaptateur pour afficher toutes les instances de ce dernier ou vous pouvez cliquer sur pour accéder aux options supplémentaires suivantes :

- **Go to Adapters (Accédez aux adaptateurs)** pour afficher tous les adaptateurs en même temps; vous pouvez ajouter, modifier et supprimer des adaptateurs à partir de là.
- **Add Adapter** > ***type*** (Ajouter un adaptateur de type) pour ajouter un adaptateur du type indiqué.

Cliquez sur un adaptateur dans la colonne Adapters ( ) pour afficher plus d'informations à son sujet. Voici un exemple :



Vous avez les options suivantes :

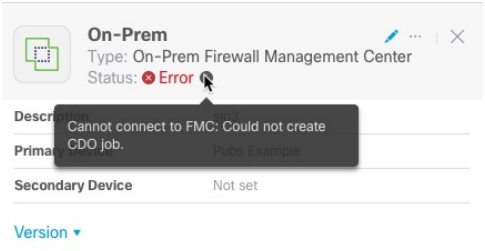
- Cliquez sur Icône modifier ( ) pour modifier ce connecteur.
- Cliquez sur Icône Autres ( ) pour avoir accès à des options supplémentaires.
- Cliquez sur **Version** pour afficher la version de connecteur d'attributs dynamiques. Vous pouvez également copier la version dans le presse-papiers au besoin pour Cisco TAC.
- Cliquez sur pour ajouter, modifier ou supprimer des adaptateurs. Vous pouvez également afficher les détails de l'erreur sur la page qui s'affiche.
- Cliquez sur pour fermer le panneau.

Afficher les informations d'erreur

Pour afficher les informations d'erreur pour un adaptateur :

1. Dans le tableau de bord, cliquez sur le nom de l'adaptateur qui affiche l'erreur.
2. Dans le volet de droite, cliquez sur **Information** ( ).

   Voici un exemple.



3. Pour résoudre cette erreur, assurez-vous que On-Prem Firewall Management Center est correctement intégré. Pour en savoir plus, consultez Intégrer un FMC dans *Gestion de FMC avec Cisco Defense Orchestrator* (lien vers la rubrique).
4. Si vous ne pouvez pas résoudre le problème, cliquez sur **Version** et copiez la version dans un fichier texte.
5. Obtenez votre ID de détenteur CDO comme indiqué dans la section Obtenir votre identifiant de service partagé, à la page 32
6. Fournissez toutes ces informations au TAC de Cisco.

Thèmes connexes

- Créer un adaptateur, à la page 25

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 CDO.

Nous prenons en charge les éléments suivants :

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 CDO 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 CDO. 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 11

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.

Procédure

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.

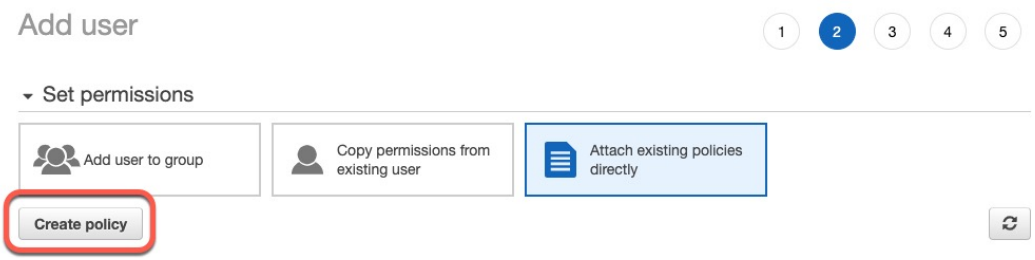
Remarque C'est la seule occasion dont vous disposez pour récupérer la clé de l'utilisateur.

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 13.

Créer un connecteur AWS

Cette tâche explique comment configurer un connecteur qui envoie des données d'AWS à CDO 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 12.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Cliquez sur **Outils et services** > **Connecteur d'attributs dynamiques** > **Connecteurs**.

Étape 3 Effectuez l'une des actions suivantes :

- Ajouter un nouveau connecteur : cliquez sur Icône ajouter (), puis sur le nom du connecteur.
- Modifier un connecteur : cliquez sur Icône modifier (Edit).
- Supprimer un connecteur : cliquez sur Icône supprimer (Delete).

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.

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 CDO 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 CDO. Pour obtenir la liste de ces attributs, consultez.Connecteur Azure : à propos des autorisations des utilisateurs et des données importées, à la page 14

Avant de commencer

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

Procédure

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**.

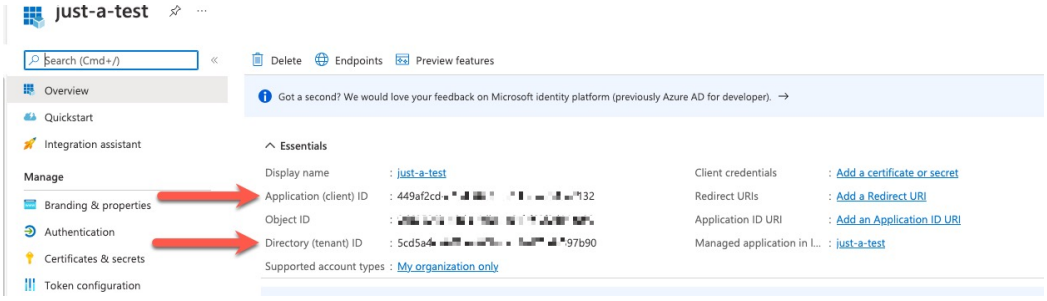
Étape 5 Dans le champ **Nom**, saisissez un nom pour identifier cette application.

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.

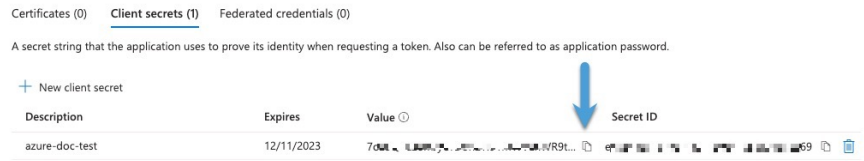


Étape 9 En regard des informations d'identification du client, cliquez sur **Ajouter un certificat ou un code secret**.

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

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

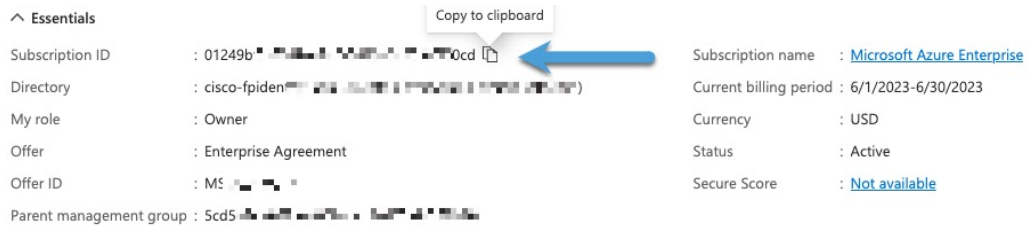
Étape 12 Copier la valeur du champ **Valeur** dans le presse-papiers. C'est cette valeur, *et non* l'**ID du code secret**, qui constitue le code secret du client.



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.



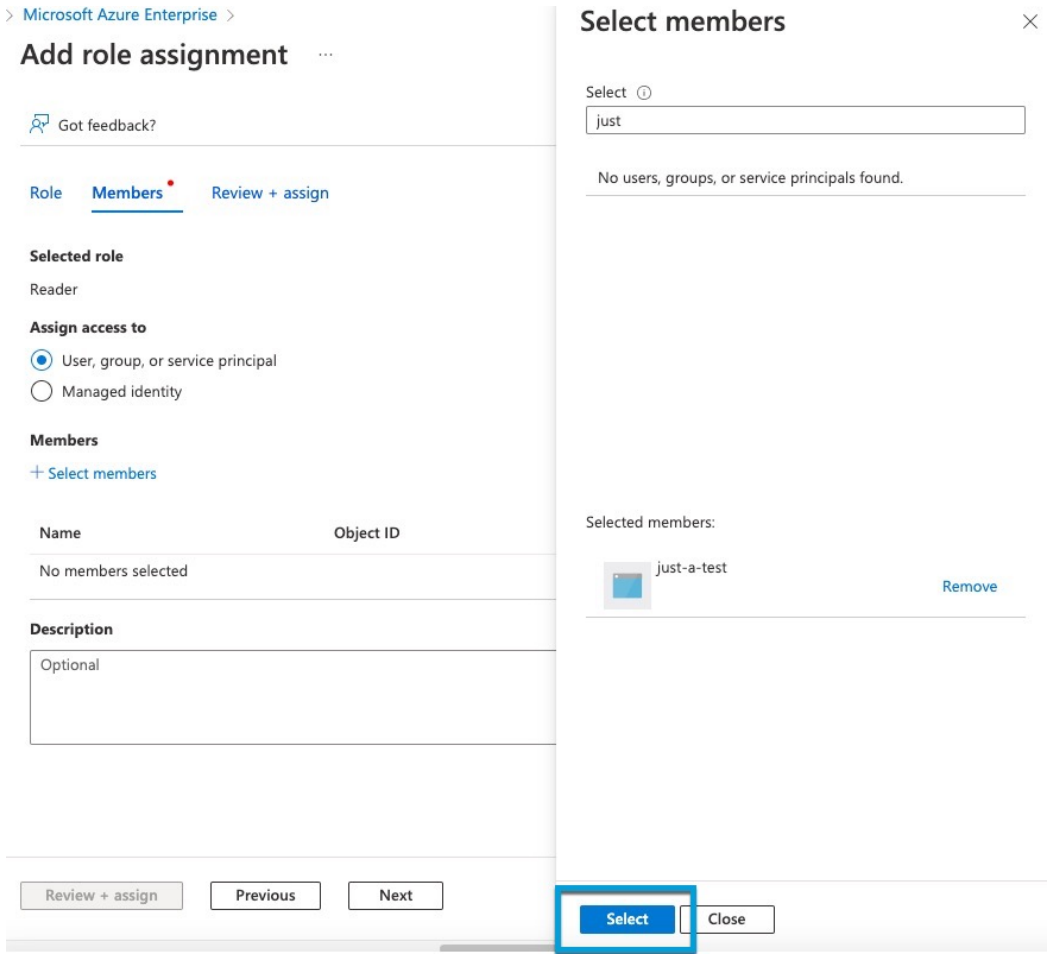
Étape 16 Cliquez sur **Contrôle d'accès (IAM)**.

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 17.

Créer un connecteur Azure

Cette tâche explique comment créer un connecteur pour envoyer des données d'Azure à CDO 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 14.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Cliquez sur **Outils et services** > **Connecteur d'attributs dynamiques** > **Connecteurs**.

Étape 3 Effectuez l'une des actions suivantes :

- Ajouter un nouveau connecteur : cliquez sur Icône ajouter ( ), puis sur le nom du connecteur.
- Modifier un connecteur : cliquez sur Icône modifier (Edit).
- Supprimer un connecteur : cliquez sur Icône supprimer (Delete).

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.

Créer un connecteur de balises de service Azure

Cette rubrique explique comment créer un connecteur pour les balises de service Azure vers CDO à utiliser dans les politiques 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.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Cliquez sur **Outils et services** > **Connecteur d'attributs dynamiques** > **Connecteurs**.

Étape 3 Effectuez l'une des actions suivantes :

- Ajouter un nouveau connecteur : cliquez sur Icône ajouter (), puis sur le nom du connecteur.
- Modifier un connecteur : cliquez sur Icône modifier (Edit).
- Supprimer un connecteur : cliquez sur Icône supprimer (Delete).

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.

Créer un connecteur GitHub

Cette section explique comment créer un connecteur GitHub qui envoie des données à CDO pour les utiliser dans les politiques 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.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Cliquez sur **Outils et services** > **Connecteur d'attributs dynamiques** > **Connecteurs**.

Étape 3 Effectuez l'une des actions suivantes :

- Ajouter un nouveau connecteur : cliquez sur Icône ajouter ( ), puis sur le nom du connecteur.
- Modifier un connecteur : cliquez sur Icône modifier (Edit).
- Supprimer un connecteur : cliquez sur Icône supprimer (Delete).

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.

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 CDO 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 CDO. Pour obtenir la liste de ces attributs, consultez.Google Cloud Connector - À propos des autorisations des utilisateurs et des données importées, à la page 19

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.

Procédure

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).

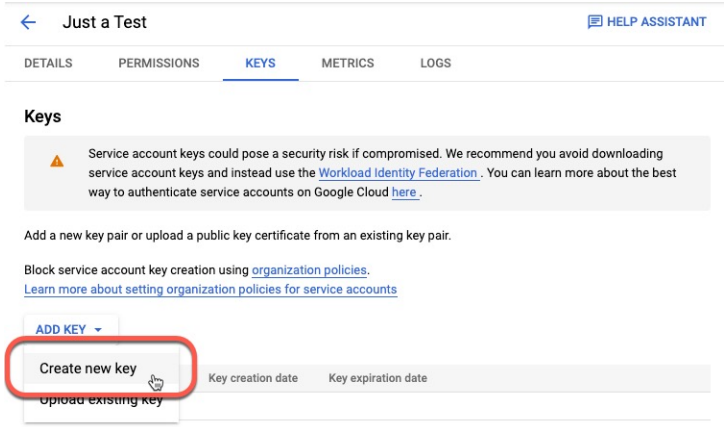
Étape 7 Cliquez sur **Done (Terminé)**.

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 21.

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.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Cliquez sur **Outils et services** > **Connecteur d'attributs dynamiques** > **Connecteurs**.

Étape 3 Effectuez l'une des actions suivantes :

- Ajouter un nouveau connecteur : cliquez sur Icône ajouter (), puis sur le nom du connecteur.
- Modifier un connecteur : cliquez sur Icône modifier (Edit).
- Supprimer un connecteur : cliquez sur Icône supprimer (Delete).

Étape 4 Ensuite, entrez l'information suivante.

Valeur	Description
Nom	(Requis) Saisissez un nom pour identifier de manière unique ce connecteur.

Valeur	Description
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.

Créer un connecteur Office 365

Cette tâche explique comment créer un connecteur pour les balises Office 365 afin d'envoyer des données au CDO 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.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Cliquez sur **Outils et services** > **Connecteur d'attributs dynamiques** > **Connecteurs**.

Étape 3 Effectuez l'une des actions suivantes :

- Ajouter un nouveau connecteur : cliquez sur Icône ajouter (), puis sur le nom du connecteur.
- Modifier un connecteur : cliquez sur Icône modifier (Edit).
- Supprimer un connecteur : cliquez sur Icône supprimer (Delete).

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.

Valeur	Description
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.

Créer un connecteur Webex

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

Pour en savoir plus, consultez la page de référence de port pour Webex Calling.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Cliquez sur **Outils et services** > **Connecteur d'attributs dynamiques** > **Connecteurs**.

Étape 3 Effectuez l'une des actions suivantes :

- Ajouter un nouveau connecteur : cliquez sur Icône ajouter ( ), puis sur le nom du connecteur.
- Modifier un connecteur : cliquez sur Icône modifier (Edit).
- Supprimer un connecteur : cliquez sur Icône supprimer (Delete).

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 de Webex.

Valeur	Description
IP réservées au fournisseur	(Requis) (Requis) Faites glisser le curseur sur Activé pour récupérer des adresses IP réservées.

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.

Créer un connecteur Zoom

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

Pour en savoir plus, consultez Paramètres du pare-feu réseau ou du serveur mandataire de Zoom.

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Cliquez sur **Outils et services** > **Connecteur d'attributs dynamiques** > **Connecteurs**.

Étape 3 Effectuez l'une des actions suivantes :

- Ajouter un nouveau connecteur : cliquez sur Icône ajouter (), puis sur le nom du connecteur.
- Modifier un connecteur : cliquez sur Icône modifier (Edit).
- Supprimer un connecteur : cliquez sur Icône supprimer (Delete).

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 de Zoom.
IP réservées au fournisseur	(Requis) Faites glisser le curseur sur Activé pour récupérer des adresses IP réservées.

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.

Créer un adaptateur

Un *adaptateur* est une connexion sécurisée à CDO 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.

Vous pouvez créer les adaptateurs suivants :

- *On-Prem Firewall Management Center* pour un périphérique sur site Centre de gestion.
- *Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)* pour les périphériques gérés par CDO.

Remarque Vous devez avoir le rôle d'utilisateur **Super Admin** pour créer le premier adaptateur de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). Pour visualiser ou modifier les adaptateurs existants, vous devez avoir un rôle d'utilisateur Admin ou Super Admin.

Comment créer un adaptateur On-Prem Firewall Management Center

Cette rubrique explique comment créer un adaptateur pour transférer des objets dynamiques de connecteur d'attributs dynamiques vers CDO.

Avant de commencer

Intégrer le gestionnaire de pare-feu à Cisco Defense Orchestrator, comme indiqué dans l'aide en ligne de la section *Intégrer un centre de gestion* dans la *gestion de la sécurité et des périphériques réseau avec Cisco Defense Orchestrator*.

Rôle d'utilisateur requis :

- Super administrateur

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Cliquez sur **Outils et services** > **Connecteur d'attributs dynamiques** > **Adaptateurs**.

Étape 3 Pour ajouter un adaptateur, cliquez sur Icône ajouter ( ) > Centre de gestion de pare-feu local.

Étape 4 Pour modifier ou supprimer un adaptateur, cliquez sur Icône modifier (Edit) ou sur Icône supprimer (Delete).

Étape 5 Ajoutez ou modifiez les informations suivantes.

Valeur	Description
Nom	(Requis) Saisissez un nom unique pour identifier cet adaptateur.
Description	Description facultative de l'adaptateur.

Valeur	Description
appareil principal	Dans la liste, cliquez sur l'adresse IP d'un centre de gestion associé à votre client.
Appareil secondaire	(Facultatif) Si vous avez un Centre de gestion de pare-feu localsecondaire, cliquez sur son nom dans la liste.

Étape 6 Cliquez sur **OK**.

Comment 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 de connecteur d'attributs dynamiques vers CDO.

Avant de commencer

Rôle d'utilisateur requis :

- Super administrateur

Procédure

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

Étape 2 Cliquez sur **Outils et services** > **Connecteur d'attributs dynamiques** > **Adaptateurs**.

Étape 3 Pour ajouter un adaptateur, cliquez sur Icône ajouter ( ) > Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Étape 4 Pour modifier ou supprimer un adaptateur, cliquez sur Icône modifier (Edit) ou sur Icône supprimer (Delete).

Étape 5 Modifiez les renseignements suivants.

Valeur	Description
Nom	(Requis) Saisissez un nom unique pour identifier cet adaptateur.
Description	Description facultative de l'adaptateur.
URL FMC du nuage	Dans la liste, cliquez sur l'URL de votre Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Étape 6 Cliquez sur **Test** et assurez-vous que l'essai réussit avant de sauvegarder l'adaptateur

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

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 CDO 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 Office 365, ou Balises Azure Service. 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, à la page 30.

Avant de commencer

Effectuez toutes les tâches suivantes :

- Créer un connecteur, à la page 11

Procédure

Étape 1 Cliquez sur **Filtres d'attributs dynamiques**.

Étape 2 Effectuez l'une des actions suivantes :

- Ajouter un nouveau filtre : cliquez sur Icône ajouter ( ).
- Modifier un filtre : cliquez sur Icône modifier (Edit)
- Supprimer un filtre : cliquez sur Icône supprimer (Delete)

Étape 3 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 CDO (**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 Icône ajouter ( ). • Modifier un filtre : cliquez sur Icône modifier (Edit)

Article	Description
	• Supprimer un filtre : cliquez sur Icône supprimer (Delete)

Étape 4 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.
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 5 Cliquez sur **Afficher l'aperçu** pour afficher la liste des réseaux ou des adresses IP renvoyés par votre requête.

Étape 6 Lorsque vous avez terminé, cliquez sur **Enregistrer**.

Étape 7 (Facultatif) Vérifiez l'objet dynamique dans le CDO.

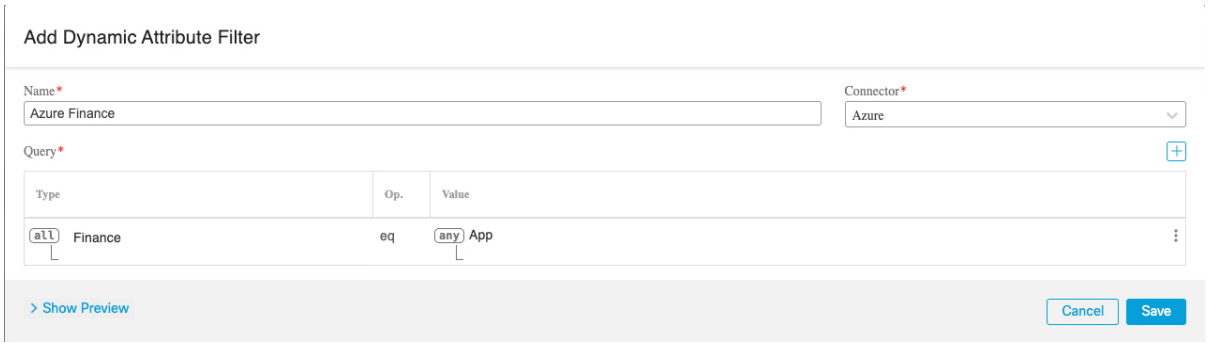
a) Connectez-vous à CDO.
b) Cliquez sur **Politiques** > **Politiques FTD**.
c) Cliquez sur **Objects (Objets)** > **Object Management** (Gestion d'objets).
d) Dans le volet gauche, cliquez sur **Attributs externes** > **Objet dynamique**.
La requête d'attribut dynamique que vous avez créée doit être 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.

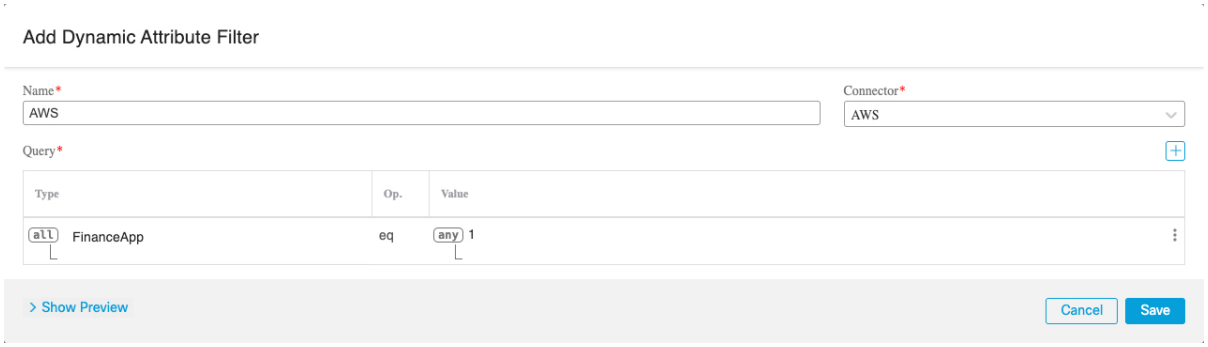
Exemple : Azure

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.



Utiliser des objets dynamiques dans les stratégies de contrôle d'accès

Le connecteur d'attributs dynamiques vous permet de configurer des filtres dynamiques, vus dans CDO comme des objets dynamiques, dans les règles de contrôle d'accès.

À propos des objets dynamiques dans les règles de contrôle d'accès

Un *objet dynamique* est automatiquement transféré du connecteur d'attributs dynamiques vers un adaptateur défini On-Prem Firewall Management Center ou Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) après avoir sauvegardé un filtre d'attributs dynamiques sur le connecteur.

Vous pouvez utiliser ces objets dynamiques dans la page de l'onglet Attributs dynamiques de la règle de contrôle d'accès, de la même manière que vous avez utilisé les balises de groupe de sécurité (SGT). Vous pouvez ajouter des objets dynamiques en tant qu'attributs de source ou de destination. Par exemple, dans une règle de blocage du contrôle d'accès, vous pouvez ajouter un objet dynamique Finance en tant qu'attribut de destination pour bloquer l'accès aux serveurs Finance pour tous les objets correspondant aux autres critères de la règle.

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

Créer des règles de contrôle d'accès à l'aide de filtres d'attributs dynamiques

Cette rubrique explique comment créer des règles de contrôle d'accès à l'aide d'objets dynamiques (ces objets dynamiques sont nommés d'après les filtres d'attributs dynamiques que vous avez créés précédemment).

Avant de commencer

Créer des filtres d'attributs dynamiques comme indiqué dans Créer des filtres d'attributs dynamiques, à la page 27.

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

Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Cliquez sur **Politiques** > **Politiques FTD**.

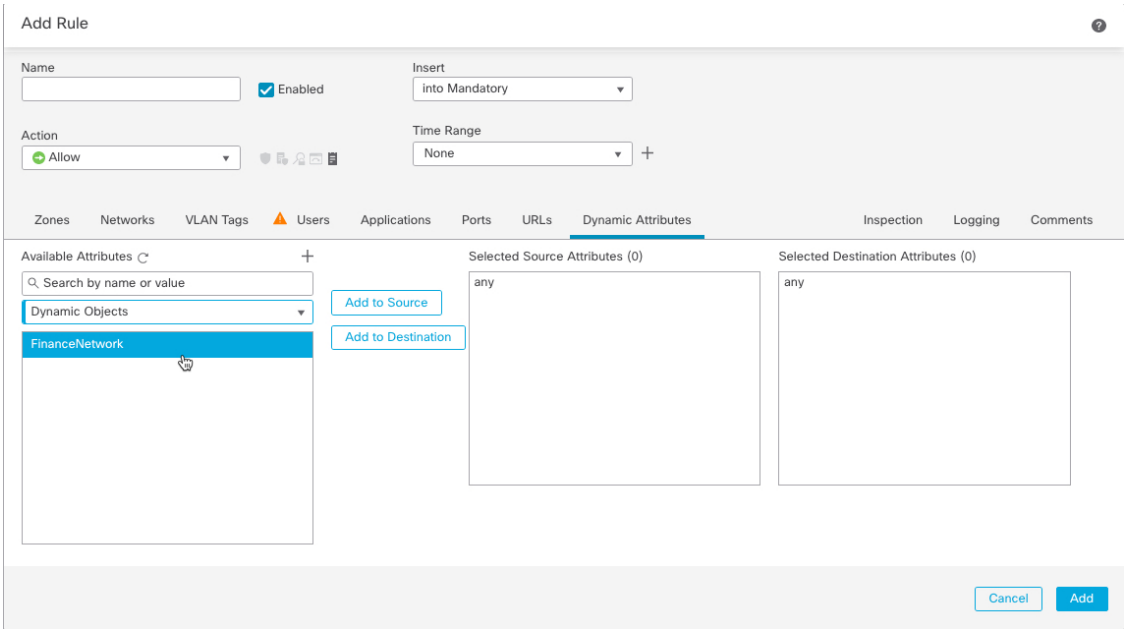
Étape 3 Cliquez sur **Modifier** (✎) à côté d'une stratégie de contrôle d'accès.

Étape 4 Cliquez sur **Add Rule** (ajouter une règle).

Étape 5 Cliquez sur l'onglet **Attributs dynamiques**.

Étape 6 Dans la section Attributs disponibles, dans la liste, cliquez sur **Objets dynamiques**.

La figure suivante présente un exemple.



L'exemple précédent montre un objet dynamique nommé `FinanceNetwork` qui correspond au filtre d'attribut dynamique créé dans Connecteur d'attributs dynamiques Cisco Secure.

Étape 7 Ajouter l'objet souhaité aux attributs de la source ou de la destination.

Étape 8 Ajoutez d'autres conditions à la règle si vous le souhaitez.

Prochaine étape

Chapitre Contrôle d'accès du *Guide de configuration des périphériques du centre de gestion du pare-feu sécurisé de Cisco* (lien vers le chapitre)

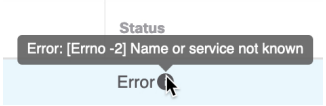
Dépanner le connecteur d'attributs dynamiques

Comment résoudre les problèmes liés à l'utilisation du connecteur d'attributs dynamiques, y compris en utilisant les outils fournis.

Dépanner les messages d'erreur

Problème : erreur de nom ou de service inconnu

Cette erreur est affichée sous forme d'infobulle lorsque vous passez la souris sur une condition d'erreur sur un adaptateur ou un connecteur. Voici un exemple; le vôtre pourrait être différent.

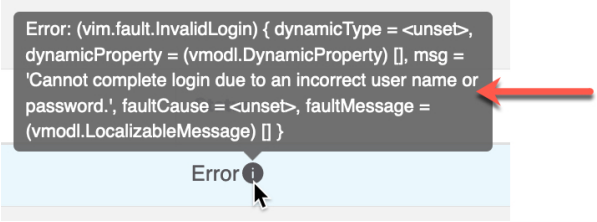


Solution : modifiez le connecteur et vérifiez la présence :

- d'une barre oblique à la fin d'un nom d'hôte
- Vérifiez que le mot de passe est correct

Problème : nom d'utilisateur ou mot de passe incorrect

Cette erreur est affichée sous forme d'infobulle lorsque vous passez la souris sur une condition d'erreur dans un connecteur.



Solution : modifiez le connecteur et changez le nom d'utilisateur ou le mot de passe.

Obtenir votre identifiant de service partagé

Si vous avez besoin d'aide pour utiliser Connecteur d'attributs dynamiques Cisco Secure, vous devez fournir votre identifiant de service partagé à Cisco TAC afin que nous puissions consulter vos journaux.

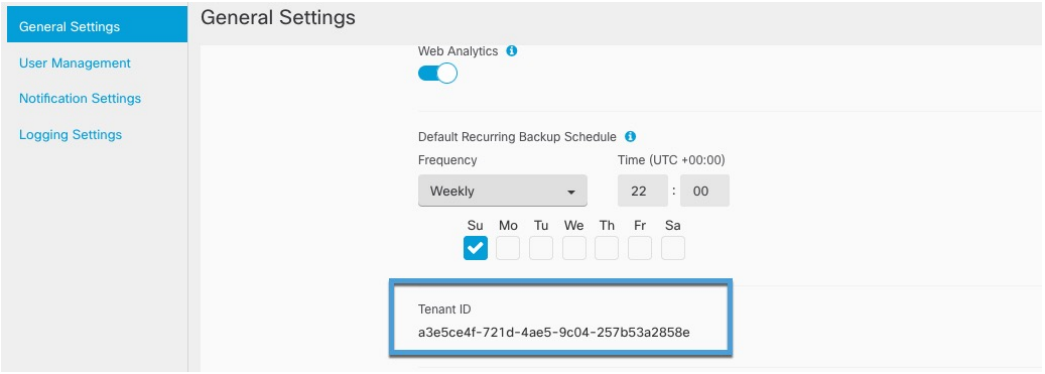
Procédure

Étape 1 Connectez-vous à CDO.

Étape 2 Cliquez sur **Paramètres** > **Paramètres généraux**.

Étape 3 Copiez votre identifiant de service partagé dans le presse-papiers pour le fournir à l'équipe Cisco TAC.

Voici un exemple.



Dépannage à l'aide de la ligne de commande

Pour vous aider à effectuer un dépannage avancé et à travailler avec l'assistance technique de Cisco, nous mettons à votre disposition les outils de dépannage suivants. Pour utiliser ces outils, connectez-vous en tant qu'utilisateur quelconque à l'hôte Ubuntu sur lequel le connecteur d'attributs dynamiques fonctionne.

Vérifier l'état du conteneur

Pour vérifier l'état des conteneurs Docker de connecteur d'attributs dynamiques, saisissez les commandes suivantes :

Voici un exemple de sortie :

Arrêter, démarrer ou redémarrer les conteneurs Docker de Connecteur d'attributs dynamiques

Si le **./muster-cli status** indique que les conteneurs sont en panne ou pour redémarrer les conteneurs en cas de problème, vous pouvez saisir les commandes suivantes :

Arrêter et redémarrer :

```
cd ~/csdac/app
sudo ./muster-cli stop
sudo ./muster-cli start
```

Démarrer seulement :

```
cd ~/csdac/app
sudo ./muster-cli start
```

Activer la journalisation du débogage et générer des fichiers de dépannage

Si l'assistance technique de Cisco vous le conseille, activez la journalisation du débogage et générez des fichiers de dépannage comme suit :

```
cd ~/csdac/app
sudo ./muster-cli debug-on
sudo ./muster-cli ts-gen
```

Le nom du fichier de dépannage est **ts-bundle-***horodatage***.tar** et est créé dans le même répertoire.

Le tableau suivant indique l'emplacement des fichiers de dépannage et des journaux dans le fichier de dépannage.

Emplacement	Ce qu'il contient :
/csdac/app/ts-bundle-*timestamp (horodatage)***/info**	Contenu de la base de données `etcd`
/csdac/app/ts-bundle-*timestamp (horodatage)***/logs**	Fichiers journaux des conteneurs
/csdac/app/ts-bundle-*timestamp (horodatage)***/status.log**	État du conteneur, versions et état de l'image

Vérifier les objets dynamiques

Pour vérifier que vos connecteurs créent des objets sur le CDO, vous pouvez utiliser la commande suivante sur le CDO en tant qu'administrateur :

```
sudo tail f /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log
```

Exemple : création réussie d'un objet

```
26-Aug-2021 12:41:35.912,[INFO],(DefenseCenterServiceImpl.java:1442)
com.cisco.nm.vms.api.dc.DefenseCenterServiceImpl, ajp-nio-127.0.0.1-9009-exec-10
** REST Request [ CSM ]
** ID : 18b25356-fd6b-4cc4-8d27-bbccb52a6275
** URL: POST /audit
{
  "version": "7.1.0",
  "requestId": "18b25356-fd6b-4cc4-8d27-bbccb52a6275",
  "data": {
    "userName": "csdac-centos7",
    "subsystem": "API",
    "message": "POST
https://myfmc.example.com/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f
/object/dynamicobjects Created (201) - The request has been fulfilled and resulted in a new
 resource being created",
    "sourceIP": "192.0.2.103",
    "domainUuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f",
    "time": "1629981695431"
  },
  "deleteList": []
}
```

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.