Utilisateurs

Le centre de gestion comprend les comptes **administrateurs** par défaut pour l'accès au Web et à l'interface de ligne de commande. Ce chapitre explique comment créer des comptes utilisateur personnalisés.

À propos des utilisateurs

Vous pouvez ajouter des comptes utilisateur personnalisés sur les périphériques gérés, en tant qu'utilisateurs internes ou externes sur un serveur LDAP ou RADIUS. Chaque appareil géré gère des comptes d'utilisateur distincts. Par exemple, lorsque vous ajoutez un utilisateur à centre de gestion, cet utilisateur n'a accès qu'à centre de gestion; vous ne pouvez pas ensuite utiliser ce nom d'utilisateur pour vous connecter directement à un périphérique géré. Vous devez ajouter un utilisateur séparément sur le périphérique géré.

Utilisateurs internes et externes

Les périphériques gérés prennent en charge deux types d'utilisateurs :

- Internal user (utilisateur interne) : le périphérique vérifie une base de données locale pour l'authentification de l'utilisateur.
- External user (utilisateur externe) : si l'utilisateur n'est pas présent dans la base de données locale, le système interroge un serveur d'authentification LDAP ou RADIUS externe.

Rôles d'utilisateur

Rôles de l'utilisateur de l'Interface Web

Cisco Defense Orchestrator (CDO) propose divers rôles utilisateur : lecture seule, modification seulement, déploiement seulement, administrateur et super administrateur. Les rôles d'utilisateur sont configurés pour chaque utilisateur sur chaque détenteur. Si un utilisateur CDO a accès à plusieurs détenteurs, ils peuvent avoir le même ID d'utilisateur, mais des rôles différents sur des détenteurs différents. Un utilisateur peut avoir un rôle en lecture seule sur un détenteur et un rôle de super administrateur sur un autre. Lorsque l'interface ou la documentation fait référence à un utilisateur en lecture seule, à déploiement seulement, à modification

seulement, à un utilisateur administrateur ou super administrateur, nous décrivons le niveau d'autorisation de cet utilisateur sur un détenteur particulier. Notez que vous ne pouvez pas créer de rôles utilisateur dans la solution Firewall Management Center fournie en nuage, car elle utilise les rôles utilisateur CDO.

Lecture seule

Les utilisateurs en lecture seule peuvent afficher toutes les configurations de périphériques, mais pas les modifier.

Déployer seulement

Les utilisateurs de déploiement seulement peuvent auditer les modifications en file d'attente apportées aux configurations des périphériques et les déployer, mais ne peuvent pas les modifier.

Modification seulement

Les utilisateurs en modification seule peuvent apporter des modifications à toutes les configurations de périphériques, mais ne peuvent pas les déployer sur les périphériques.

Super admin et admin

Les utilisateurs super administrateurs et administrateurs peuvent accéder à l'ensemble des éléments du produit. La différence entre les utilisateurs super administrateurs et administrateurs, c'est que les super administrateurs peuvent créer des comptes pour d'autres utilisateurs sur un détenteur et modifier les rôles d'utilisateur existants, ce que les administrateurs ne peuvent pas faire.

Pour en savoir plus sur les rôles d'utilisateur dans CDO, consultez Rôles d'utilisateurs.

Le tableau suivant fait correspondre les rôles d'utilisateur dans Centre de gestion de pare-feu local à leurs rôles équivalents dans la solution Firewall Management Center en nuage, CDO.

Astuces Nous vous recommandons de lire le tableau uniquement si vous connaissez les rôles d'utilisateur définis dans Centre de gestion de pare-feu local.

Tableau 1 : Mise en correspondance des rôles des utilisateurs de Cisco Secure Firewall Management Center et de Firewall Management Center en nuage

Rôle d'utilisateur Centre de gestion de pare-feu local	Rôle équivalent de l'utilisateur Firewall Management Center en nuage	Capacités
Administrateur d'accès, administrateur de découverte, administrateur de prévention des intrusions, utilisateur de maintenance	Modification seulement	Vous pouvez rechercher, filtrer ou afficher les éléments suivants : • Politiques de contrôle d'accès et fonctionnalités associées • Politique de prévention des intrusions • Règles d'intrusion • Règle de découverte du réseau • Détecteurs personnalisés • Politiques de corrélation • Objets • Ensemble de règles • Interfaces • Configurations VPN • Paramètres liés à la surveillance et à la maintenance Vous pouvez sauvegarder ou restaurer un périphérique, mais ne pouvez pas déployer de politiques sur les périphériques.
Administrateur	Super administrateur	Vous pouvez accéder à toutes les fonctionnalités de Firewall Management Center en nuage et effectuer des tâches, notamment créer, lire, modifier ou supprimer des politiques ou des objets et déployer ces modifications sur les périphériques. Vous pouvez également modifier des rôles d'utilisateur ou créer des enregistrements d'utilisateur dans CDO.

Rôle d'utilisateur Centre de gestion de pare-feu local	Rôle équivalent de l'utilisateur Firewall Management Center en nuage	Capacités
Administrateur de réseau	Admin	Vous pouvez accéder à toutes les fonctionnalités de Firewall Management Center en nuage et effectuer des tâches, notamment créer, lire, modifier ou supprimer des politiques ou des objets et déployer ces modifications sur les périphériques. Cependant, vous ne pouvez pas modifier des rôles d'utilisateur ni créer d'enregistrements d'utilisateur dans CDO.
Analyste en sécurité, Analyste en sécurité (lecture seule)	Lecture seule	Vous pouvez afficher les informations sur le périphérique, les politiques, les objets et les paramètres associés, mais ne pouvez pas effectuer ce qui suit : • Créer ou modifier des objets • Créer ou modifier des politiques • Modifier la configuration des périphériques • Sauvegarder ou restaurer des périphériques
Approbateur de sécurité	Déployer seulement	Vous pouvez afficher la plupart des paramètres et déployer des modifications progressives sur les périphériques, mais ne pouvez pas créer ou modifier des objets ou des politiques.

Créer un fichier d'utilisateur CDO avec votre nom d'utilisateur CDO

Seul un utilisateur CDO avec des privilèges de « Super administrateur » peut créer une fiche d'utilisateur CDO. Le super administrateur doit créer l'enregistrement d'utilisateur avec la même adresse de courriel que celle spécifiée dans la tâche **Créez votre nom d'utilisateur CDO** ci-dessus.

Utilisez la procédure suivante pour créer un enregistrement d'utilisateur avec un rôle utilisateur approprié :

Procedure

Étape 1 Connectez-vous au CDO.

Étape 2 Dans la barre de navigation CDO, cliquez sur **Settings** (paramètres) » **User Management (gestion des utilisateurs)**.

Étape 3 Cliquez sur le bouton bleu Plus ( ) pour ajouter un nouvel utilisateur à votre détenteur.

Étape 4 Fournissez l'adresse de courriel de l'utilisateur.

Note L'adresse courriel de l'utilisateur doit correspondre à l'adresse courriel du compte Cisco Secure Log-On.

Étape 5 Sélectionnez le rôle de l'utilisateur dans le menu déroulant.

Étape 6 Cliquez sur **OK**.

Résolution de problèmes liés aux connexions d'authentification LDAP

Si vous créez un objet d'authentification LDAP et qu'il ne parvient pas à se connecter au serveur que vous sélectionnez ou ne récupère pas la liste des utilisateurs souhaités, vous pouvez régler les paramètres dans l'objet.

Si la connexion échoue lorsque vous la testez, essayez les suggestions suivantes pour dépanner votre configuration :

- Utilisez les messages affichés en haut de l'écran de l'interface Web et dans la sortie du test pour déterminer quelles zones de l'objet sont à l'origine du problème.
- Vérifiez que le nom d'utilisateur et le mot de passe que vous avez utilisés pour l'objet sont valides :
  - Vérifiez que vous avez les droits pour accéder au répertoire indiqué dans votre nom distinctif de base en vous connectant au serveur LDAP à l'aide d'un navigateur LDAP tiers.
  - Vérifiez que le nom d'utilisateur est unique dans l'arborescence d'informations d'annuaire pour le serveur LDAP.
  - Si vous voyez une erreur de liaison LDAP 49 dans la sortie du test, la liaison d'utilisateur pour l'utilisateur a échoué. Essayez de vous authentifier sur le serveur à l'aide d'une application tierce pour voir si la liaison échoue également avec cette connexion.
- Vérifiez que vous avez correctement identifié le serveur :
  - Vérifiez que l'adresse IP du serveur ou le nom d'hôte est correct.
  - Vérifiez que vous avez un accès TCP/IP depuis votre appareil local au serveur d'authentification auquel vous souhaitez vous connecter.
  - Vérifiez que l'accès au serveur n'est pas bloqué par un pare-feu et que le port que vous avez configuré dans l'objet est ouvert.

- Si vous utilisez un certificat pour vous connecter via TLS ou SSL, le nom d'hôte de ce dernier doit correspondre au nom d'hôte utilisé dans ce champ.
- Vérifiez que vous n'avez pas utilisé d'adresse IPv6 pour la connexion au serveur si vous authentifiez l'accès de l'interface de ligne de commande.
- Si vous avez utilisé les valeurs par défaut du type de serveur, vérifiez que vous utilisez le bon type de serveur et cliquez à nouveau sur **Set Defaults** (définir les valeurs par défaut) pour réinitialiser les valeurs par défaut.

- Si vous avez saisi votre nom distinctif de base, cliquez sur **fetch DNs** (Récupérer les DN) pour récupérer tous les noms distinctifs de base disponibles sur le serveur et sélectionnez le nom dans la liste.
- Si vous utilisez des filtres, des attributs d'accès ou des paramètres avancés, vérifiez qu'ils sont valides et saisis correctement.
- Si vous utilisez des filtres, des attributs d'accès ou des paramètres avancés, essayez de supprimer chaque paramètre et testez l'objet sans lui.
- Si vous utilisez un filtre de base ou un filtre d'accès au niveau de l'interface de ligne de commande, assurez-vous que le filtre est mis entre parenthèses et que vous utilisez un opérateur de comparaison valide (maximum de 450 caractères, parenthèses comprises).
- Pour tester un filtre de base plus restreint, essayez de lui définir le nom distinctif de base pour que l'utilisateur récupère uniquement cet utilisateur.
- Si vous utilisez une connexion chiffrée :
  - Vérifiez que le nom du serveur LDAP dans le certificat correspond au nom d'hôte que vous utilisez pour vous connecter.
  - Vérifiez que vous n'avez pas utilisé une adresse IPv6 avec une connexion au serveur chiffrée.
- Si vous utilisez un utilisateur de test, assurez-vous que le nom d'utilisateur et le mot de passe sont saisis correctement.
- Si vous utilisez un utilisateur de test, supprimez les informations d'authentification de l'utilisateur et testez l'objet.
- Testez la requête que vous utilisez en vous connectant au serveur LDAP et en utilisant la syntaxe :

```
ldapsearch -x -b 'base_distinguished_name'
-h LDAPserver_ip_address -p port -v -D
'user_distinguished_name' -W 'base_filter'
```

Par exemple, si vous essayez de vous connecter au domaine de sécurité sur `myrte.exemple.com` en utilisant l'utilisateur `domaineadmin@myrte.exemple.com` et un filtre de base de (`cn=*`), vous pouvez tester la connexion à l'aide de l'instruction suivante :

```
ldapsearch -x -b 'CN=security,DC=myrtle,DC=example,DC=com'
-h myrtle.example.com -p 389 -v -D
'domainadmin@myrtle.example.com' -W '(cn=*)'
```

Si vous pouvez tester votre connexion avec succès, mais que l'authentification ne fonctionne pas après le déploiement d'une politique de paramètres de plateforme, vérifiez que l'authentification et l'objet que vous

souhaitez utiliser sont tous deux activés dans la politique de paramètres de plateforme qui est appliquée au périphérique.

Si vous réussissez à vous connecter, mais que vous souhaitez ajuster la liste des utilisateurs récupérés par votre connexion, vous pouvez ajouter ou modifier un filtre de base ou un filtre d'accès au niveau de l'interface de ligne de commande, ou utiliser un DN de base plus ou moins restrictive.

Lors de l'authentification d'une connexion au serveur Active Directory (AD), le journal des événements de connexion indique rarement le trafic LDAP bloqué, bien que la connexion au serveur AD soit réussie. Ce journal de connexion incorrect se produit lorsque le serveur AD envoie un paquet de réinitialisation en double. L'appareil Défense contre les menaces identifie le deuxième paquet de réinitialisation dans le cadre d'une nouvelle demande de connexion et enregistre la connexion avec l'action Block (bloquer).

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.