Utilisateurs

Les périphériques gérés comprennent un compte **administrateur** par défaut pour l'accès 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.

Accès CLI

Les périphériques Firepower comprennent une interface de ligne de commande Firepower qui s'exécute sur Linux. Vous pouvez créer des utilisateurs internes sur les périphériques à l'aide de cette dernière. Vous pouvez établir des utilisateurs externes sur les périphériques défense contre les menaces à l'aide de centre de gestion.

⚠

Mise en garde Les utilisateurs avec un accès de niveau de configuration CLI peuvent accéder à l'interface Shell Linux à l'aide de la commande **expert** et obtenir les privilèges `sudoers` dans l'interface Shell Linux, ce qui peut présenter un risque pour la sécurité. Pour des raisons de sécurité du système, nous vous recommandons fortement :

- Utilisez l'interpréteur de commandes Linux uniquement sous la supervision du TAC ou lorsque la documentation utilisateur de Firepower vous le demande explicitement.
- Veillez à restreindre correctement la liste des utilisateurs avec accès à l'interface de ligne de commande.
- Lorsque vous accordez des privilèges d'accès à l'interface de ligne de commande, restreignez la liste des utilisateurs avec un accès de niveau Configuration.
- De ne pas ajouter d'utilisateurs directement dans l'interface Shell Linux; d'utiliser uniquement les procédures décrites dans ce chapitre.
- N'accédez pas aux périphériques Firepower à l'aide du mode expert de l'interface de commande en ligne, sauf sur instruction du TAC de Cisco ou conformément à des instructions explicites dans la documentation utilisateur du périphérique Firepower.

Rôles des utilisateurs de la CLI

Sur les périphériques gérés, l'accès utilisateur aux commandes de la CLI dépend du rôle que vous attribuez.

Aucun

L'utilisateur ne peut pas se connecter au périphérique sur la ligne de commande.

Configuration

L'utilisateur peut accéder à toutes les commandes, y compris les commandes de configuration. Faites preuve de prudence lorsque vous attribuez ce niveau d'accès aux utilisateurs.

Niveau de base

L'utilisateur peut accéder uniquement aux commandes non liées à la configuration. Seuls les utilisateurs internes et les utilisateurs RADIUS externes défense contre les menaces prennent en charge le rôle de base.

Exigences et conditions préalables pour les comptes d'utilisateur pour les périphériques

Prise en charge des modèles

- Défense contre les menaces : Utilisateurs internes et externes

Domaines pris en charge

N'importe quel

Rôles utilisateur

Configurer les utilisateurs externes : Super administrateur deou utilisateur Admin

Configurez les utilisateurs internes :Super administrateur ou Admin de la de configuration.

Lignes directrices et restrictions concernant les comptes d'utilisateur pour les périphériques

Noms des utilisateurs

- Vous ne pouvez pas ajouter le même nom d'utilisateur pour les utilisateurs internes et externes. Si le serveur externe utilise un nom d'utilisateur en double, le déploiement sur le périphérique échoue.
- Le nom d'utilisateur doit être valide pour Linux :
  - Au maximum, ils doivent comprendre 32 caractères alphanumériques (plus le tiret (-) et le trait de soulignement).
  - Tous les caractères doivent être en minuscules.
  - Il est impossible de commencer un nom d'utilisateur par un tiret (-). Un nom d'utilisateur ne peut pas se composer exclusivement de nombres. De plus, il ne peut pas inclure de point (.), de signe @ ou de barre oblique (/).

Valeurs par défaut

Tous les périphériques comprennent un utilisateur **administrateur** en tant que compte d'utilisateur local; vous ne pouvez pas supprimer l'utilisateur **admin**. Le mot de passe initial par défaut est **Admin123**; le système vous oblige à modifier ce dernier pendant le processus d'initialisation. Consultez le guide de démarrage correspondant à votre modèle pour plus d'informations sur l'initialisation du système.

Nombre de comptes d'utilisateurs

Vous pouvez créer un maximum de 43 comptes utilisateur pour les périphériques Firepower 1000 et 2100.

Ajouter un utilisateur interne au niveau de l'interface de ligne de commande

Utilisez l'interface de ligne de commande pour créer des utilisateurs internes sur le défense contre les menaces .

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande de l'appareil en utilisant un compte avec des privilèges de configuration.

Le compte d'utilisateur **admin** dispose des privilèges requis, mais tout compte doté de privilèges de configuration fonctionnera. Vous pouvez utiliser une session SSH ou le port de console.

Pour certains modèles de défense contre les menaces , le port de console vous place dans l'interface de ligne de commande FXOS. Utilisez la commande **connect ftd** pour accéder à l'interface de ligne de commande défense contre les menaces .

Étape 2 Créez un compte utilisateur.

configure user add *username* (nom d'utilisateur) {**basic** | **config**}

- *username* : Définit le nom d'utilisateur. Le nom d'utilisateur doit être valide pour Linux :
  - Au maximum, ils doivent comprendre 32 caractères alphanumériques (plus le tiret (-) et le trait de soulignement).
  - Tous les caractères doivent être en minuscules.
  - Il est impossible de commencer un nom d'utilisateur par un tiret (-). Un nom d'utilisateur ne peut pas se composer exclusivement de nombres. De plus, il ne peut pas inclure de point (.), de signe @ ou de barre oblique (/).
- **basic** : Donne à l'utilisateur un accès de base. Ce rôle ne permet pas à l'utilisateur d'entrer des commandes de configuration.
- **config** : Donne accès à la configuration utilisateur. Ce rôle donne à l'utilisateur tous les droits d'administrateur sur toutes les commandes.

Exemple :

Dans l'exemple suivant, un compte d'utilisateur nommé johncrichton est ajouté avec des droits d'accès de configuration. Le mot de passe ne s'affiche pas lorsque vous le saisissez.

```
> configure user add johncrichton config
Enter new password for user johncrichton: newpassword
Confirm new password for user johncrichton: newpassword
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
johncrichton      1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

Remarque Dites aux utilisateurs qu'ils peuvent changer leur mot de passe à l'aide de la commande **configure password**.

Étape 3 (Facultatif) Ajustez les caractéristiques du compte pour satisfaire à vos exigences de sécurité.

Vous pouvez utiliser les commandes suivantes pour modifier le comportement par défaut du compte.

- **configure user aging** *nom d'utilisateur max_days warn_days*

  Définit une date d'expiration pour le mot de passe de l'utilisateur. Précisez le nombre maximal de jours de la période de validité du mot de passe, suivi du nombre de jours de préavis (c.-à-d. le moment auquel l'utilisateur sera averti de l'expiration prochaine). Les deux valeurs sont comprises entre 1 et 9999, mais le nombre de jours de préavis doit être inférieur au nombre de jours de la période de validité maximale. Lorsque vous créez le compte, le mot de passe ne comporte aucune date d'échéance.

- **configure user forcereset** *username (nom d'utilisateur)*

Force l'utilisateur à modifier le mot de passe lors de la prochaine connexion.

- **configure user maxfailedlogins** *username number (numéro d'utilisateur)*

  Définit le nombre maximal de connexions échouées consécutives que vous autoriserez avant de verrouiller le compte (de 1 à 9999). Utilisez la commande **configure user unlock** pour déverrouiller des comptes. La valeur par défaut pour les nouveaux comptes est cinq échecs consécutifs de connexion.

- **configure user minpasswdlen** *username number (numéro d'utilisateur)*

  Définit une longueur de mot de passe minimale, qui peut aller de 1 à 127.

- **configure user strengthcheck** *username (nom d'utilisateur)* {**enable** | **disable**}

  Active ou désactive la vérification de la force du mot de passe, qui contraint un utilisateur à répondre à des critères de mot de passe spécifiques lors de la modification de son mot de passe. Lorsque le mot de passe d'un utilisateur expire ou si la commande **configure user forcereset** est utilisée, cette exigence est automatiquement activée lors de la prochaine connexion de l'utilisateur.

Étape 4 Gérez les comptes utilisateur au besoin.

Il arrive que des comptes soient verrouillés ou que vous deviez supprimer des comptes ou résoudre d'autres problèmes. Utilisez les commandes suivantes pour gérer les comptes d'utilisateur dans le système.

- **configure user access** *username (nom d'utilisateur)* {**basic** | **config**}

  Modifie les privilèges d'un compte d'utilisateur.

- **configure user delete** *username (nom d'utilisateur)*

  Supprime le compte spécifié.

- **configure user disable** *username (nom d'utilisateur)*

  Désactive le compte spécifié sans le supprimer. L'utilisateur ne peut pas se connecter tant que vous n'avez pas activé le compte.

- **configure user enable** *username (nom d'utilisateur)*

  Active le compte spécifié.

- **configure user password** *username (nom d'utilisateur)*

  Modifie le mot de passe de l'utilisateur spécifié. Les utilisateurs doivent normalement modifier leur propre mot de passe à l'aide de la commande **configure password**.

- **configure user unlock** *username (nom d'utilisateur)*

  Déverrouille un compte d'utilisateur qui a été verrouillé en raison du nombre maximal de tentatives de connexion échouées consécutives.

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.