Utilisation de l'interface de commande en ligne

Ce chapitre décrit comment utiliser l'interface de ligne de commande sur l'ASA.

Remarque L'interface de ligne de commande utilise une syntaxe similaire et d'autres conventions que l'interface de ligne de commande de Cisco IOS, mais le système d'exploitation d'ASA n'est pas une version du logiciel Cisco IOS. Ne supposez pas qu'une commande de l'interface de ligne de commande Cisco IOS fonctionne avec l'ASA ou a la même fonction sur celui-ci.

- Mode pare-feu et mode de contexte de sécurité, à la page 1
- Modes de commande et invites, à la page 2
- Formatage de la syntaxe, à la page 3
- Commandes abrégées, à la page 4
- Modification de la ligne de commande, à la page 4
- Exécution de la commande, à la page 4
- Aide sur les commandes, à la page 4
- Afficher la configuration d'exécution, à la page 5
- Filtrer la sortie de la commande show et more, à la page 5
- Redirection et ajout de la sortie de la commande show, à la page 6
- Obtention d'un nombre de lignes pour la sortie de la commande show, à la page 7
- Pagination de la sortie de commande, à la page 8
- Ajouter des commentaires, à la page 8
- Fichiers de configuration de texte, à la page 8
- Ensembles de caractères pris en charge, à la page 10

Mode pare-feu et mode de contexte de sécurité

L'ASA fonctionne dans une combinaison des modes suivants :

- Mode pare-feu transparent ou pare-feu routé

  Le mode de pare-feu détermine si l'ASA fonctionne en tant que pare-feu de couche 2 ou 3.

- Mode contexte multiple ou contexte simple

Le mode de contexte de sécurité détermine si l'ASA fonctionne en tant que périphérique unique ou sous plusieurs contextes de sécurité, qui agissent comme des périphériques virtuels.

Certaines commandes ne sont disponibles que dans certains modes.

Modes de commande et invites

L'interface de ligne de commande d'ASA comprend des modes de commande. Certaines commandes ne peuvent être saisies que dans certains modes. Par exemple, pour saisir des commandes qui affichent des renseignements sensibles, vous devez saisir un mot de passe et passer en mode privilégié. Ensuite, pour vous assurer que les modifications de configuration ne sont pas saisies accidentellement, vous devez passer en mode de configuration. Toutes les commandes inférieures peuvent être saisies dans les modes supérieurs. Par exemple, vous pouvez saisir une commande EXEC privilégée en mode de configuration globale.

Remarque Les différents types d'invites sont tous des invites par défaut et, lorsqu'ils sont configurés, ils peuvent être différents.

- Lorsque vous êtes dans la configuration système ou en mode de contexte unique, l'invite commence par le nom d'hôte :

  ```
  ciscoasa
  ```

- Lors de l'impression de la chaîne d'invite, la configuration de l'invite est analysée et les valeurs de mot clé configurées sont imprimées dans l'ordre dans lequel vous avez défini la commande d'invite. Les arguments de mot clé peuvent être les suivants et dans n'importe quel ordre : nom d'hôte, domaine, contexte, priorité, état.

  prompt hostname context priority state

- Lorsque vous êtes dans un contexte, l'invite commence par le nom d'hôte suivi du nom de contexte :

  ```
  ciscoasa/context
  ```

L'invite change en fonction du mode d'accès :

- Mode d'exécution de l'utilisateur

  Le mode d'exécution de l'utilisateur vous permet de voir les paramètres ASA minimum. L'invite du mode d'exécution de l'utilisateur s'affiche comme suit lorsque vous accédez à l'ASA pour la première fois :

  ```
  ciscoasa>

  ciscoasa/context>
  ```

- mode d'exécution privilégié

  Le mode d'exécution privilégié vous permet de voir tous les paramètres actuels jusqu'à votre niveau de privilège. Toute commande en mode d'exécution de l'utilisateur fonctionnera en mode d'exécution

privilégié. Saisissez la commande **enable** en mode d'exécution de l'utilisateur, qui nécessite un mot de passe, pour démarrer le mode d'exécution privilégié. L'invite comprend le signe de numéro (#) :

```
ciscoasa#

ciscoasa/context#
```

- Mode de configuration globale

  Le mode de configuration globale vous permet de modifier la configuration de l'ASA. Toutes les commandes d'exécution de l'utilisateur, d'exécution privilégiée et de configuration globale sont disponibles dans ce mode. Saisissez la commande **configure terminal** en mode d'exécution privilégié pour démarrer le mode de configuration globale. L'invite change comme suit :

  ```
  ciscoasa(config)#

  ciscoasa/context(config)#
  ```

- Modes de configuration spécifiques aux commandes

  À partir du mode de configuration globale, certaines commandes entrent dans un mode de configuration spécifique à la commande. Toutes les commandes d'exécution de l'utilisateur, d'exécution privilégiée, de configuration globale et de configuration spécifique à la commande sont disponibles dans ce mode. Par exemple, la commande **interface** entre en mode de configuration d'interface. L'invite change comme suit :

  ```
  ciscoasa(config-if)#

  ciscoasa/context(config-if)#
  ```

Formatage de la syntaxe

Les descriptions de la syntaxe des commandes utilisent les conventions répertoriées dans le tableau suivant.

Tableau 1 : Conventions de syntaxe

Convention	Description
gras	Le texte en caractères gras indique les commandes et les mots clés à entrer mot à mot, comme illustré.
italique	Le texte en italique indique les arguments pour lesquels vous devez fournir des valeurs.
[x]	Les éléments indiqués entre crochets sont optionnels (mot clé ou argument).
|	Une barre verticale indique un choix parmi un ensemble facultatif ou obligatoire de mots clés ou d'arguments.
[x | y]	Les mots-clés ou arguments inscrits entre crochets et séparés par une barre verticale indiquent un choix optionnel.

Convention	Description
{x | y}	Les mots-clés ou arguments inscrits entre accolades et séparés par une barre verticale indiquent un choix obligatoire.
[x {y | z}]	Les ensembles de crochets ou d'accolades imbriqués indiquent des choix facultatifs ou obligatoires parmi des éléments facultatifs ou obligatoires. Des accolades et une barre verticale entre crochets indiquent un choix obligatoire dans un élément facultatif.

Commandes abrégées

Vous pouvez abréger la plupart des commandes en utilisant le moins de caractères uniques possible pour une commande. Par exemple, vous pouvez saisir **wr t** pour afficher la configuration au lieu de saisir la commande complète **write terminal**, ou vous pouvez saisir **en** pour démarrer le mode privilégié et **conf t** pour démarrer le mode de configuration. De plus, vous pouvez saisir **0** pour représenter **0.0.0.0**.

Modification de la ligne de commande

L'ASA utilise les mêmes conventions de modification de ligne de commande que le logiciel Cisco IOS. Vous pouvez afficher toutes les commandes saisies précédemment avec la commande **show history** ou individuellement avec la commande de flèche vers le haut ou **^p**. Une fois que vous avez examiné une commande saisie précédemment, vous pouvez avancer dans la liste avec la commande de flèche vers le bas ou **^n**. Lorsque vous atteignez une commande que vous souhaitez réutiliser, vous pouvez la modifier ou appuyer sur la touche **Entrer** (Entrée) pour la lancer. Vous pouvez également supprimer le mot à gauche du curseur avec **^w** ou effacer la ligne avec **^u**.

L'ASA autorise jusqu'à 512 caractères dans une commande; les caractères supplémentaires sont ignorés.

Exécution de la commande

Pour terminer une commande ou un mot clé après avoir saisi une chaîne partielle, appuyez sur la touche **Tab** (Onglet). L'ASA ne termine la commande ou le mot clé que si la chaîne partielle ne correspond qu'à une seule commande ou mot clé. Par exemple, si vous saisissez **s** et appuyez sur la touche **Tab** (Onglet), l'ASA ne termine pas la commande, car il correspond à plusieurs commandes. Cependant, si vous saisissez **dis**, la clé **Tab** (Onglet) complète la commande **disable**.

Aide sur les commandes

Les informations d'aide sont accessibles à partir de la ligne de commande en saisissant les commandes suivantes :

- **help** *command_name*

  Affiche l'aide pour la commande spécifique.

- *command_name* **?**

Affiche une liste des arguments disponibles.

- *string***?** (aucun espace)

  Répertorie les commandes possibles commençant par la chaîne.

- **?** et **+?**

  Répertorie toutes les commandes disponibles. Si vous saisissez **?**, l'ASA affiche uniquement les commandes disponibles pour le mode actuel. Pour afficher toutes les commandes disponibles, y compris celles des modes inférieurs, saisissez **+?**.

Remarque Si vous souhaitez inclure un point d'interrogation (?) dans une chaîne de commande, vous devez appuyer sur **Ctrl-V** avant de taper le point d'interrogation pour ne pas invoquer par inadvertance l'aide de l'interface de ligne de commande.

Afficher la configuration d'exécution

Pour afficher la configuration d'exécution, utilisez l'une des commandes suivantes :

- **show running-config** [**all**] [*command*]

  Si vous spécifiez **all**, tous les paramètres par défaut s'affichent également. Si vous spécifiez une *commande*, la sortie ne comprend que les commandes associées.

Remarque De nombreux mots de passe sont affichés sous la forme *xxx. Pour afficher les mots de passe en texte brut ou sous forme chiffrée, si une phrase secrète principale est activée, utilisez la commande **more**.

- **more system:running-config**

Filtrer la sortie de la commande show et more

Vous pouvez utiliser la barre verticale (|) avec n'importe quelle commande **show** et inclure une option de filtre et une expression de filtrage. Le filtrage est effectué en faisant correspondre chaque ligne de sortie à une expression régulière, comme le logiciel Cisco IOS. En sélectionnant différentes options de filtre, vous pouvez inclure ou exclure toute la sortie qui correspond à l'expression. Vous pouvez également afficher toute la sortie en commençant par la ligne qui correspond à l'expression.

La syntaxe pour l'utilisation des options de filtrage avec la commande **show** est la suivante :

show *command* | {**include**| **exclude** | **begin** | **grep** [**-v**]} *regexp*

ou

more system:running-config| {**include**| **exclude** | **begin** | **grep** [**-v**]} *regexp*

Remarque La commande **more** vous permet d'afficher le contenu de n'importe quel fichier, et non pas seulement la configuration d'exécution; consultez la référence de commande pour en savoir plus.

Dans cette chaîne de commande, la première barre verticale (|) est l'opérateur et doit être incluse dans la commande. Cet opérateur dirige la sortie de la commande **show** vers le filtre. Dans le schéma de syntaxe, les autres barres verticales (|) indiquent d'autres options et ne font pas partie de la commande.

L'option **include** inclut toutes les lignes de sortie qui correspondent à l'expression régulière. L'option **grep** sans **-v** a le même effet. L'option **exclude** exclut toutes les lignes de sortie correspondant à l'expression régulière. L'option **grep** avec **-v** a le même effet. L'option **begin** affiche toutes les lignes de sortie en commençant par la ligne qui correspond à l'expression régulière.

Remplacez *regexp* par n'importe quelle expression régulière de Cisco IOS. L'expression régulière n'est pas entre guillemets ou doubles guillemets, alors soyez prudent avec les espaces de fin, qui seront utilisés dans l'expression régulière.

Lors de la création d'expressions régulières, vous pouvez utiliser n'importe quel chiffre ou lettre que vous souhaitez faire correspondre. En outre, certains caractères du clavier appelés *métadonnée*s ont une signification particulière lorsqu'ils sont utilisés dans des expressions régulières.

Utilisez **Ctrl + V** pour échapper tous les caractères spéciaux de l'interface de ligne de commande, comme un point d'interrogation (?) ou un onglet. Par exemple, tapez **d[Ctrl+V]?g** pour saisir **d?g** dans la configuration.

Redirection et ajout de la sortie de la commande show

Si la sortie à afficher est importante, l'achèvement de la commande peut prendre beaucoup de temps. Par exemple, vous pourriez penser que le système est bloqué si vous essayez d'afficher un million d'entrées de contrôle d'accès ou un très grand tableau ASP.

Au lieu d'afficher la sortie d'une commande **show** à l'écran, vous pouvez la rediriger vers un fichier sur le périphérique ou dans un emplacement distant. Lors de la redirection vers un fichier sur le périphérique, vous pouvez également ajouter la sortie de la commande au fichier.

show *command* | {**append | redirect**} *url*

- **append** *url* ajoute la sortie à un fichier existant. Spécifiez le fichier en utilisant l'une des options suivantes :
  - **disk0:/**[[*path/*]*filename*] ou **flash:/**[[*path/*]*filename*] : **flash** et **disk0** indiquent la mémoire Flash interne. Vous pouvez utiliser l'une ou l'autre de ces options.
  - **disk1:/**[[*path/*]*filename*] : iIndique la mémoire externe.
- **redirect** *url* crée le fichier spécifié ou le remplace si le fichier existe déjà.
  - **disk0:/**[[*path/*]*filename*] ou **flash:/**[[*path/*]*filename*] : **flash** et **disk0** indiquent la mémoire Flash interne. Vous pouvez utiliser l'une ou l'autre de ces options.
  - **disk1:/**[[*path/*]*filename*] : iIndique la mémoire externe.
  - **smb:/**[[*path/*]*filename*] : indique Server Message Block, un système de fichiers local de serveur UNIX.

- **ftp://**[[*user*[**:***password*]@] *server*[:*port*]/[*path/*] *filename*[**;type=***xx*]] : indique un serveur SCP. Le **type** peut être l'un des mots clés suivants : **ap** (Mode passif ASCII), **an** (Mode normal ASCII), **ip** (Par défaut – Mode passif binaire), **in** (Mode normal binaire).
- **scp://**[[*user*[:*password*]@] *server*[/*path*]/*filename*[**;int=***interface_name*]]—L'option **;int=***interface* contourne la recherche de routage et utilise toujours l'interface spécifiée pour atteindre le serveur Secure Copy (SCP).
- **tftp://**[[*user*[**:***password*]@] *server*[:*port*] /[*path/*]*filename*[**;int=***interface_name*]] : indique un serveur TFTP. ne peut pas contenir d'espaces. L'option **;int=***interface* contourne la recherche de routage et utilise toujours l'interface spécifiée pour atteindre le serveur TFTP.

Obtention d'un nombre de lignes pour la sortie de la commande show

Au lieu de voir la sortie réelle de la commande **show**, vous pouvez simplement souhaiter voir le nombre de lignes dans la sortie ou le nombre de lignes qui correspondent à une expression régulière. Vous pouvez ensuite comparer facilement le nombre de lignes avec celui des fois précédentes où vous avez saisi la commande. Cela peut constituer une vérification rapide lorsque vous effectuez des modifications de configuration. Vous pouvez soit utiliser le mot clé **count**, soit ajouter **-c** au mot clé grep.

show *command* | **count** [*regular_expression*]

show *command* | **grep -c** [*regular_expression*]

Remplacez *regular_expression* par n'importe quelle expression régulière de Cisco IOS. L'expression régulière n'est pas entre guillemets ou doubles guillemets, alors soyez prudent avec les espaces de fin, qui seront utilisés dans l'expression régulière. L'expression régulière est facultative; si vous n'en incluez pas, le nombre renvoie le nombre total de lignes dans la sortie non filtrée.

Lors de la création d'expressions régulières, vous pouvez utiliser n'importe quel chiffre ou lettre que vous souhaitez faire correspondre. En outre, certains caractères du clavier appelés métadonnées ont une signification particulière lorsqu'ils sont utilisés dans des expressions régulières. Utilisez Ctrl + V pour échapper tous les caractères spéciaux de l'interface de ligne de commande, comme un point d'interrogation (?) ou un onglet. Par exemple, tapez **d[Ctrl+V]?g** pour entrer **d?g** dans la configuration.

Par exemple, pour afficher le nombre total de toutes les lignes dans la sortie **show running-config** :

```
ciscoasa# show running-config | count
Number of lines which match regexp = 271
```

L'exemple suivant montre comment vous pouvez vérifier rapidement le nombre d'interfaces activées. Le premier montre comment utiliser le mot clé **grep** avec une expression régulière pour filtrer uniquement les lignes qui affichent un état opérationnel. L'exemple suivant ajoute l'option **-c** pour afficher simplement le nombre de lignes plutôt que les lignes de sortie.

```
ciscoasa# show interface | grep is up
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
Interface GigabitEthernet0/1 "inside", is up, line protocol is up

ciscoasa# show interface | grep -c is up
```

```
Number of lines which match regexp = 2
```

Pagination de la sortie de commande

Pour les commandes telles que **help** ou **?**, **show**, **show xlate** ou d'autres commandes qui fournissent de longues listes, vous pouvez déterminer si les informations affichent un écran et s'arrêtent ou permettent à la commande de s'exécuter jusqu'à la fin. La commande **pager** vous permet de choisir le nombre de lignes à afficher avant que l'invite More (Plus) ne s'affiche.

Lorsque la pagination est activée, l'invite suivante apparaît :

```
<--- More --->
```

L'invite More (Plus) utilise une syntaxe similaire à la commande UNIX **more** :

- Appuyez sur la barre **d'espace** pour afficher un autre écran.
- Appuyez sur la touche **Enter** (Entrée) pour afficher la ligne suivante.
- Appuyez sur la touche q pour revenir à la ligne de commande.

Ajouter des commentaires

Vous pouvez précéder une ligne de deux-points (:) pour créer un commentaire. Cependant, le commentaire ne s'affiche que dans le tampon de l'historique des commandes et non dans la configuration. Par conséquent, vous pouvez afficher le commentaire avec la commande **show history** ou en appuyant sur une touche de direction pour récupérer une commande précédente, mais comme le commentaire ne se trouve pas dans la configuration, la commande **write terminal** ne l'affiche pas.

Fichiers de configuration de texte

Cette section décrit comment formater un fichier texte de configuration que vous pouvez télécharger sur l'ASA.

Correspondance des commandes avec les lignes dans le fichier texte

Le fichier de configuration texte comprend des lignes correspondant aux commandes décrites dans ce guide.

Dans les exemples, les commandes sont précédées d'une invite d'interface de ligne de commande. L'invite dans l'exemple suivant est « ciscoasa(config)# » :

```
ciscoasa(config)# context a
```

Dans le fichier de configuration texte, vous n'êtes pas invité à saisir des commandes, l'invite est donc omise :

```
context a
```

Commandes de mode de configuration propres aux commandes

Les commandes de mode de configuration spécifiques aux commandes apparaissent en retrait sous la commande principale lorsqu'elles sont saisies dans la ligne de commande. Les lignes de votre fichier texte n'ont pas besoin d'être mises en retrait, tant que les commandes apparaissent directement après la commande principale. Par exemple, le texte suivant, qui n'est pas en retrait, se lit de la même manière que le texte en retrait :

```
interface gigabitethernet0/0
nameif inside
interface gigabitethernet0/1
    nameif outside
```

Saisies automatiques de texte

Lorsque vous téléchargez une configuration dans l'ASA, il insère certaines lignes automatiquement. Par exemple, l'ASA insère des lignes pour les paramètres par défaut ou pour l'heure à laquelle la configuration a été modifiée. Vous n'avez pas besoin de saisir ces entrées automatiques lorsque vous créez votre fichier texte.

Commande de ligne

Dans la plupart des cas, les commandes peuvent être placées dans n'importe quel ordre dans le fichier. Cependant, certaines lignes, telles que les ACE, sont traitées dans l'ordre dans lequel elles s'affichent, et l'ordre peut affecter la fonction de la liste d'accès. D'autres commandes peuvent également avoir des exigences de commande. Par exemple, vous devez d'abord saisir la commande **nameif** pour une interface, car de nombreuses commandes ultérieures utilisent le nom de l'interface. De plus, les commandes dans un mode de configuration spécifique aux commandes doivent suivre directement la commande principale.

Commandes non incluses dans la configuration du texte

Certaines commandes n'insèrent pas de lignes dans la configuration. Par exemple, une commande d'exécution telle que **show running-config** n'a pas de ligne correspondante dans le fichier texte.

Mots de passe

Les mots de passe de connexion, d'activation et d'utilisateur sont automatiquement chiffrés avant d'être stockés dans la configuration. Par exemple, la forme chiffrée du mot de passe « cisco » pourrait ressembler à jMorNbK0514fadBh. Vous pouvez copier les mots de passe de configuration sur un autre ASA dans sa forme chiffrée, mais vous ne pouvez pas déchiffrer les mots de passe vous-même.

Si vous saisissez un mot de passe non chiffré dans un fichier texte, l'ASA ne le chiffre pas automatiquement lorsque vous copiez la configuration sur l'ASA. L'ASA le chiffre uniquement lorsque vous enregistrez la configuration en cours d'exécution à partir de la ligne de commande à l'aide de la commande **copy running-config startup-config** ou **write memory**.

Plusieurs fichiers de contexte de Security

Pour plusieurs contextes de sécurité, la configuration complète comprend les éléments suivants :

- Les configurations du contexte de sécurité
- La configuration système, qui identifie les paramètres de base de l'ASA, y compris une liste de contextes
- Le contexte d'administration, qui fournit des interfaces réseau pour la configuration système

  La configuration système ne comprend aucune interface ni aucun paramètre réseau pour elle-même. Au contraire, lorsque le système doit accéder à des ressources réseau (comme le téléchargement des contextes à partir du serveur), il utilise un contexte désigné comme contexte d'administration.

Chaque contexte est similaire à une configuration en mode de contexte unique. La configuration système diffère de la configuration de contexte en ce que la configuration système comprend des commandes système uniquement (comme une liste de tous les contextes) alors que d'autres commandes typiques sont absentes (comme de nombreux paramètres d'interface).

Ensembles de caractères pris en charge

L'interface de ligne de commande d'ASA prend actuellement en charge uniquement le codage UTF-8. UTF-8 est le schéma de codage particulier pour les symboles Unicode. Il a été conçu pour être compatible avec un sous-ensemble de symboles ASCII. Les caractères ASCII sont représentés dans UTF-8 comme des caractères d'un octet. Tous les autres caractères sont représentés dans UTF-8 sous forme de symboles multioctets.

Les caractères ASCII imprimables (0x20 à 0x7e) sont entièrement pris en charge. Les caractères ASCII imprimables sont les mêmes que ceux de la norme ISO 8859-1. UTF-8 est un super-ensemble d'ISO 8859-1, de sorte que les 256 premiers caractères (0-255) sont identiques à ISO 8859-1. L'interface de ligne de commande d'ASA prend en charge jusqu'à 255 caractères (caractères multioctets) de la norme ISO 8859-1.

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.