Référence de commande Cisco Firepower 4100/9300 FXOS

Dernière modification : 2025-08-19

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2017–2021 Cisco Systems, Inc. Tous droits réservés.

À propos du guide de référence des commandes de l'interface de ligne de commande FXOS

Ce guide s'inscrit dans un effort soutenu de documentation des multiples commandes de l'interface de ligne de commande FXOS et, en tant que tel, doit être considéré comme un travail en cours. Ce guide fera l'objet de republications régulières, au fur et à mesure de l'ajout de nouvelles descriptions de commandes et de la mise à jour ou correction des descriptions existantes.

Présentation de l'interface de ligne de commande

- Objets gérés, à la page 4
- Modes de commande, à la page 5
- Diagramme des connexions de l'interface de ligne de commande FXOS, à la page 7
- Commandes d'objets, à la page 8
- Compléter une commande, à la page 9
- Historique des commandes, à la page 10
- Valider, supprimer et afficher les commandes en attente, à la page 11
- Aide en ligne pour l'interface de ligne de commande, à la page 12
- Limites de session de l'interface de ligne de commande, à la page 13

Objets gérés

FXOS utilise un modèle d'objet géré, où les objets gérés sont des représentations abstraites d'entités physiques ou logiques qui peuvent être gérées. Par exemple, les châssis, les modules de sécurité, les modules de réseau, les ports et les processeurs sont des entités physiques représentées sous forme d'objets gérés, et les licences, les rôles d'utilisateur et les politiques de plateforme sont des entités logiques représentées sous forme d'objets gérés.

Les objets gérés peuvent présenter une ou plusieurs propriétés associées qui peuvent être configurées.

Modes de commande

L'interface de ligne de commande FXOS est organisée en une hiérarchie de modes de commande, le mode EXEC étant le mode le plus élevé de la hiérarchie. Les modes de niveau supérieur se divisent en modes de niveau inférieur. Pour passer des modes de niveau supérieur aux modes de niveau inférieur suivants, vous utilisez les commandes **create**, **enter** et **scope**. Pour remonter d'un niveau dans la hiérarchie des modes, vous utilisez la commande **up**. Vous pouvez également utiliser la commande **top** pour passer au niveau supérieur dans la hiérarchie des modes.

Remarque La plupart des modes de commande sont associés à des objets gérés, vous devez donc créer un objet avant de pouvoir accéder au mode associé à cet objet. Vous utilisez les commandes **create** et **enter** pour créer des objets gérés pour les modes auxquels vous accédez. Les commandes **scope** ne créent pas d'objets gérés et ne peuvent accéder qu'aux modes pour lesquels les objets gérés existent déjà.

Chaque mode contient un ensemble de commandes qui peuvent être saisies dans ce mode. La plupart des commandes disponibles dans chaque mode se rapportent à l'objet géré associé.

L'invite de l'interface de ligne de commande pour chaque mode affiche le chemin d'accès complet dans la hiérarchie des modes jusqu'au mode actuel. Cela vous aide à déterminer où vous êtes dans la hiérarchie du mode de commande et peut s'avérer un outil inestimable lorsque vous devez naviguer dans la hiérarchie.

Le tableau suivant répertorie les principaux modes de commande, les commandes utilisées pour accéder à chaque mode et l'invite de l'interface de ligne de commande associée à chaque mode.

Tableau 1 : Principaux modes de commande et invites

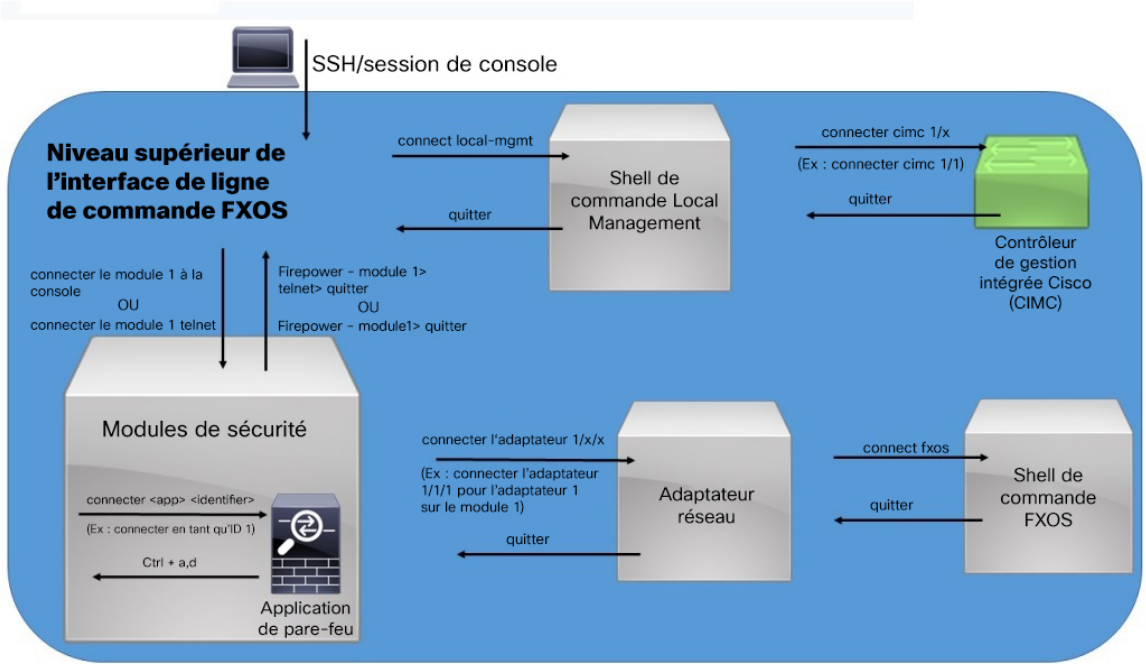
Nom du mode	Commandes utilisées pour y accéder	Invite du mode
EXEC	commande **top** de n'importe quel mode	`#`
Adaptateur	commande **scope adapter** du mode EXEC	`/adapter #`
Câblage	commande **scope cabling** du mode EXEC	`/cabling #`
Châssis	commande **scope chassis** du mode EXEC	`/chassis #`
Domaine de serveur Ethernet	commande **scope eth-server** du mode EXEC; cette commande et toutes les sous-commandes ne sont actuellement pas prises en charge	`/eth-server #`
Ethernet uplink (liaison ascendante Ethernet)	commande **scope eth-uplink** du mode EXEC	`/eth-uplink #`
Interconnexion de structure	commande **scope fabric-interconnect** du mode EXEC	`/fabric-interconnect #`
Micrologiciel	commande **scope firmware** du mode EXEC	`/firmware #`

Nom du mode	Commandes utilisées pour y accéder	Invite du mode
Interface Ethernet hôte	commande **scope host-eth-if** du mode EXEC **Remarque** Cette commande et toutes les sous-commandes ne sont pas prises en charge à ce niveau; les commandes de l'interface Ethernet hôte sont disponibles en mode `/adapter #`.	`/host-eth-if #`
Licence	commande **scope license** du mode EXEC	`/license #`
Surveillance	commande **scope monitoring** du mode EXEC	`/monitoring #`
Organisation	commande **scope org** du mode EXEC	`/org #`
Saisie de paquets	commande **scope packet-capture** du mode EXEC	`/packet-capture #`
Sécurité	commande **scope security** du mode EXEC	`/security #`
Serveur	commande **scope server** du mode EXEC	`/server #`
Profil de service	commande **scope service-profile** du mode EXEC **Remarque** Ne modifiez ni ne configurez les profils de service; à savoir, n'utilisez pas les ensembles de sous-commandes **create**, **set** ou **delete**.	`/service-profile #`
SSA	commande **scope ssa** du mode EXEC	`/ssa #`
Système	commande **scope system** du mode EXEC	`/system #`
HBA virtuel	commande **scope vhba** du mode EXEC **Remarque** Cette commande et toutes les sous-commandes ne sont actuellement pas prises en charge.	`/vhba #`
Carte réseau virtuelle	commande **scope vnic** du mode EXEC	`/vnic #`

Diagramme des connexions de l'interface de ligne de commande FXOS

Le diagramme suivant décrit les commandes qui peuvent être exécutées à partir du niveau supérieur de l'interface de ligne de commande FXOS pour accéder au shell de commande FXOS, au shell de commande de gestion locale, à l'adaptateur réseau, à Cisco Integrated Management Controller (CIMC) et à l'interface de ligne de commande du module de sécurité.

Illustration 1 : Firepower 4100/9300 Diagramme des connexions de l'interface de ligne de commande FXOS



Commandes d'objets

Quatre commandes générales sont disponibles pour la gestion des objets :

- **create** *objet*
- **delete** *objet*
- **enter** *objet*
- **scope** *objet*

Vous pouvez utiliser la commande **scope** avec n'importe quel objet géré, qu'il soit un objet permanent ou un objet d'instance d'utilisateur. Les autres commandes vous permettent de créer et de gérer des objets créés par l'utilisateur. Pour chaque commande **create** *objet* (créer un objet), il existe une commande **delete** *objet* (supprimer l'objet) et **enter** *objet* (entrer dans l'objet) correspondante.

Dans la gestion des objets générés par les utilisateurs, le comportement de ces commandes dépend de l'existence de l'objet, comme décrit dans les tableaux suivants :

Tableau 2 : Comportement de la commande si l'objet n'existe pas

Commande	Comportement
create *objet*	L'objet est créé et son mode de configuration, le cas échéant, est activé.
delete *objet*	Un message d'erreur est généré.
enter *objet*	L'objet est créé et son mode de configuration, le cas échéant, est activé.
scope *objet*	Un message d'erreur est généré.

Tableau 3 : Comportement de la commande si l'objet existe

Commande	Comportement
create *objet*	Un message d'erreur est généré.
delete *objet*	L'objet est supprimé.
enter *objet*	Permet d'entrer dans le mode de configuration de l'objet, si applicable.
scope *objet*	Permet d'entrer dans le mode de configuration de l'objet.

Compléter une commande

Vous pouvez utiliser la touche **Tab** dans n'importe quel mode pour compléter une commande. Lorsque vous saisissez partiellement un nom de commande et appuyez sur **Tab**, la commande est complétée automatiquement jusqu'à ce qu'un mot clé ou un argument soit nécessaire.

Historique des commandes

L'interface de ligne de commande stocke toutes les commandes utilisées dans la session en cours. Vous pouvez parcourir les commandes précédemment utilisées à l'aide des touches de de flèche ascendante ou descendante. La touche de flèche ascendante permet d'accéder à la commande précédente et la touche de flèche descendante à la commande suivante de l'historique. Lorsque vous atteignez la fin de l'historique, appuyer sur la flèche descendante n'a aucun effet.

Pour exécuter à nouveau une commande de l'historique, retrouvez-la dans l'historique pour la rappeler, puis appuyez sur **Entrée**. La commande est entrée comme si vous l'aviez saisie manuellement. Vous pouvez également rappeler une commande et la modifier avant d'appuyer sur **Entrée**.

Valider, supprimer et afficher les commandes en attente

Lorsque vous saisissez une commande de configuration dans l'interface de ligne de commande, cette dernière n'est pas appliquée tant que vous n'avez pas saisi la commande **commit-buffer**. Jusqu'à la validation, une commande de configuration est en attente et peut être supprimée en saisissant une commande **discard-buffer**.

Vous pouvez cumuler les modifications en attente dans plusieurs modes de commande et les appliquer en même temps à l'aide d'une commande **commit-buffer**. Vous pouvez afficher les commandes en attente en saisissant la commande **show configuration pending** dans n'importe quel mode de commande.

Remarque La validité de toutes les commandes en attente est vérifiée. Cependant, si une commande en attente échoue lors de la validation, les commandes restantes sont appliquées; les commandes ayant échoué sont signalées dans un message d'erreur.

Lorsque des commandes sont en attente, un astérisque (*) s'affiche avant l'invite de commande. L'astérisque disparaît lorsque vous saisissez la commande **commit-buffer**.

L'exemple suivant montre comment les invites changent au cours du processus de saisie des commandes :

```
Firepower# scope system
Firepower /system # scope services
Firepower /system/services # create ntp-server 192.168.200.101
Firepower /system/services* # show configuration pending
 scope services
+    create ntp-server 192.168.200.101
 exit
Firepower /system/services* # commit-buffer
Firepower /system/services #
```

Aide en ligne pour l'interface de ligne de commande

À tout moment, vous pouvez saisir le caractère **?** pour afficher les options disponibles à l'état actuel de la syntaxe de la commande.

Si vous n'avez rien saisi dans l'invite, le fait de saisir **?** répertorie toutes les commandes disponibles pour le mode dans lequel vous êtes. Si vous avez partiellement saisi une commande, le fait de saisir **?** répertorie tous les mots clés et les arguments disponibles pour votre position actuelle dans la syntaxe de la commande.

Limites de session de l'interface de ligne de commande

FXOS limite le nombre de sessions CLI actives simultanément à un total de 32 sessions. Cette valeur n'est pas configurable.

Enregistrer et filtrer la sortie d'une commande « show »

• Enregistrer et filtrer la sortie d'une commande « show », à la page 16

Enregistrer et filtrer la sortie d'une commande « show »

Enregistrer et filtrer la sortie d'une commande « show »

Vous pouvez enregistrer la sortie des commandes **show** en redirigeant la sortie vers un fichier texte. Vous pouvez filtrer la sortie des commandes **show** en canalisant la sortie vers les commandes de filtrage.

L'enregistrement et le filtrage de la sortie sont disponibles avec toutes les commandes **show**, mais sont plus utiles lorsqu'il s'agit de commandes qui produisent beaucoup de texte. Par exemple, vous pouvez afficher tout ou partie de la configuration à l'aide de la commande **show configuration**. La copie de la sortie de configuration fournit un moyen de sauvegarder et de restaurer une configuration.

Remarque Les commandes de type « show » (affichage) n'affichent pas les secrets (champs de mot de passe), donc si vous souhaitez coller une configuration dans un nouveau dispositif, vous devrez modifier la sortie d'affichage pour inclure les mots de passe réels.

Filtrer la sortie d'une commande « show »

Pour filtrer la sortie d'une commande **show**, utilisez les sous-commandes suivantes. Notez que dans la description de syntaxe suivante, la barre verticale initiale | après la commande **show** est le caractère de barre verticale et fait partie de la commande, et ne fait pas partie de la description de syntaxe. Les options de filtrage sont saisies après le caractère initial | de la commande.

show *commande* **|** {**begin** *expression* | **count** | **cut** *expression* | **egrep** *expression* | **end** *expression* | **exclude** *expression* | **grep** *expression* | **head** | **include** *expression* | **last** | **less** | **no-more** | **sort** *expression* | **tr** *expression* | **uniq** *expression* | **wc**}

Options de filtrage

Voici les sous-commandes de filtrage :

- **begin** : trouve la première ligne où le modèle spécifié est trouvé et affiche cette ligne et toutes les lignes suivantes.
- **count** : compte le nombre de lignes.
- **cut** : supprime (« coupe ») des parties de chaque ligne.
- **egrep** : affiche uniquement les lignes qui correspondent au modèle de type étendu.
- **end** : se termine par la ligne correspondant au modèle.
- **exclude** : exclut toutes les lignes qui correspondent au modèle et affiche toutes les autres lignes.
- **grep** : affiche uniquement les lignes qui correspondent au modèle.
- **head** : affiche les premières lignes.
- **include** : affiche uniquement les lignes qui correspondent au modèle.
- **last** : affiche les dernières lignes.
- **less** : filtres pour la pagination.
- **no-more** : désactive la pagination pour la sortie de la commande.

- **sort** : trie les lignes (trieur de flux).
- **tr** : déplace, compresse ou supprime les caractères.
- **uniq** : supprime toutes les lignes identiques successives, sauf une.
- **wc** : affiche le nombre de lignes, de mots et de caractères.

expression

Une expression, ou un modèle, est généralement une simple chaîne de texte. N'enveloppez pas l'expression dans des guillemets anglais simples ou doubles; ceux-ci seront considérés comme faisant partie de l'expression. De plus, les espaces de fin seront inclus dans l'expression.

Remarque Plusieurs de ces sous-commandes ont des options supplémentaires qui vous permettent de contrôler davantage le filtrage. Par exemple, avec **show configuration | head** et **show configuration | last**, vous pouvez utiliser le mot-clé **lines** pour modifier le nombre de lignes affichées; la valeur par défaut est 10. En guise d'exemple supplémentaire, avec **show configuration | sort**, vous pouvez ajouter l'option **-u** pour supprimer les lignes en double de la sortie. (Les descriptions complètes de ces options dépassent le cadre de ce document; reportez-vous à la sortie d'aide FXOS pour les différentes commandes et à l'aide Linux appropriée pour de plus amples informations.)

Exemples

L'exemple suivant montre comment déterminer le nombre de lignes actuellement dans le journal des événements du système :

```
FP9300-A# show sel 1/1 | count
3008
FP9300-A#
```

L'exemple suivant montre comment afficher les lignes du journal des événements du système qui incluent la chaîne « error » (erreur) :

```
FP9300-A# show sel 1/1 | include error
968 | 05/15/2016 16:46:25 | CIMC | System Event DDR4_P2_H2_EC
C #0x99 | Upper critical - going high | Asserted | Reading 20
000 >= Threshold 20000 error
FP9300-A#
```

Thèmes connexes

Enregistrer la sortie d'une commande « show », à la page 17

Enregistrer la sortie d'une commande « show »

Vous pouvez enregistrer la sortie des commandes **show** en redirigeant la sortie vers un fichier texte.

show *commande* [> {**ftp:** | **scp:** | **sftp:** | **tftp:** | **volatile:** | **workspace:**}] | [>> {**volatile:** | **workspace:**}]

Description de la syntaxe

> { **ftp:** | **scp:** | **sftp:** | **tftp:** | **volatile:** | **workspace:** }	Redirige la sortie de la commande **show** vers un fichier texte précisé en utilisant le protocole de transport sélectionné. Après avoir saisi la commande, vous serez invité à indiquer le nom ou l'adresse IP du serveur distant, le nom d'utilisateur, le chemin de fichier, etc. Si vous appuyez sur **Entrée** à ce stade, la sortie est enregistrée localement.
>> { **volatile:** | **workspace:** }	Ajoute la sortie de la commande **show** au fichier texte approprié, qui doit déjà exister.

Exemple

L'exemple suivant tente d'enregistrer la configuration actuelle dans l'espace de travail du système; un fichier de configuration existe déjà, que vous pouvez choisir d'exister ou non.

```
FP9300-A# show configuration > workspace
File already exists, overwrite (y/n)?[n]n
Reissue command with >> if you want to append to existing file

FP9300-A#
```

Thèmes connexes

Filtrer la sortie d'une commande « show », à la page 16

Commandes non prises en charge et restreintes

- Commandes non prises en charge, à la page 20
- Commandes restreintes, à la page 24

Commandes non prises en charge

Les commandes suivantes, lorsqu'elles sont visibles dans l'interface de ligne de commande, ne sont pas prises en charge. La saisie d'une de ces commandes n'a aucun effet.

Commandes EXEC (niveau supérieur)

`#` **restore-check**

`#` **scope eth-server** (et toutes les sous-commandes)

`#` **scope host-eth-if** (les sous-commandes **host-eth-if** sont disponibles en mode `/adapter`)

`#` **scope nh-test** (et toutes les sous-commandes)

`#` **set nh-test**

`#` **show nh-test**

`#` **show registry-repository**

`#` **show ucspe-tech-support**

`#` **ucspe-copy**

`#` **vhba** (et toutes les sous-commandes)

Commandes du mode châssis

`/chassis #` **scope iom**

`/chassis #` **show iom**

`/chassis #` **show post**

Commandes du mode interconnexion de structure

`/fabric-interconnect #` **scope fan**

`/fabric-interconnect #` **scope fan-module**

`/fabric-interconnect #` **scope psu**

`/fabric-interconnect #` **scope sw-uplink**

`/fabric-interconnect #` **show fan**

`/fabric-interconnect #` **show fan-module**

`/fabric-interconnect #` **show lan-neighbors**

`/fabric-interconnect #` **show psu**

`/fabric-interconnect #` **show san-neighbors**

`/fabric-interconnect #` **show sw-uplink**

Commandes du mode organisation

`/org #` **recommission server**

`/org #` **scope auth-profile**

`/org #` **scope fc-policy**

`/org #` **scope iqn-pool**

`/org #` **scope iscsi-policy**

`/org #` **scope kvm-mgmt-policy**

`/org #` **scope rackserver-disc-policy**

`/org #` **scope rackserver-mgmt-policy**

`/org #` **scope san-connectivity-policy**

`/org #` **scope storage-connection-policy**

`/org #` **scope udld-link-policy**

`/org #` **scope udld-system-settings**

`/org #` **scope uuid-suffix-pool**

`/org #` **scope vhba-beh-policy**

`/org #` **scope vhba-templ**

`/org #` **scope vmq-conn-policy**

`/org #` **scope wwn-pool**

`/org #` **show fc-policy**

`/org #` **show fc-zone**

`/org #` **show iqn-pool**

`/org #` **show rackserver-disc-policy**

`/org #` **show rackserver-mgmt-policy**

`/org #` **show san-connectivity-policy**

`/org #` **show udld-link-policy**

`/org #` **show udld-system-settings**

`/org #` **show uuid-suffix-pool**

`/org #` **show vhba-beh-policy**

`/org #` **show vhba-templ**

`/org #` **show vmq-conn-policy**

`/org #` **show wwn-pool**

Commandes du mode capture de paquets

`/packet-capture #` **show nh-test**

Commandes du mode sécurité

`/security #` **create role**

`/security #` **delete role**

Commandes du mode serveur

`/server #` **show flexflash-controller**

Commandes du mode profil de service

`/service-profile #` **disassociate**

`/service-profile #` **rename-to**

`/service-profile #` **scope dynamic-vnic-conn**

`/service-profile #` **scope ext-pooled-ip**

`/service-profile #` **scope ext-static-ip**

`/service-profile #` **scope fc-zone**

`/service-profile #` **scope iscsi-boot**

`/service-profile #` **scope vhba**

`/service-profile #` **set dynamic-vnic-conn-policy**

`/service-profile #` **set ext-mgmt-ip-pool-name**

`/service-profile #` **set ext-mgmt-ip-state**

`/service-profile #` **set iscsi-identity**

`/service-profile #` **set kvm-mgmt-policy**

`/service-profile #` **set san-connectivity-policy-name**

`/service-profile #` **set src-templ-name**

`/service-profile #` **show dynamic-vnic-conn**

`/service-profile #` **show dynamic-vnic-conn-policy**

`/service-profile #` **show ext-pooled-ip**

`/service-profile #` **show ext-static-ip**

`/service-profile #` **show fc-zone**

`/service-profile #` **show initiator-group**

`/service-profile #` **show iscsi-boot**

`/service-profile #` **show iscsi-identity**

`/service-profile #` **show mgmt-iface**

`/service-profile #` **show vhba**

`/service-profile #` **show vnic-iscsi**

Commandes du mode système

`/system #` **scope control-ep**

`/system #` **scope environment-features**

```
/system # scope storage-features
/system # scope vm-mgmt
/system # set virtual-ip
/system # show control-ep
```

Commandes restreintes

L'utilisation des commandes suivantes est restreinte. N'utilisez aucune de ces commandes à moins qu'un membre du centre d'assistance technique (TAC) de Cisco vous le demande.

Commandes du mode profil de service

Ne modifiez aucune configuration de profil de service; n'utilisez spécifiquement aucune des sous-commandes `/service-profile #` **create**, `/service-profile #` **delete** ou `/service-profile #` **set**.

PARTIE I

Commandes A – R

- Commandes A – C, à la page 27
- Commandes D – R, à la page 119

Commandes A – C

- acknowledge fault, à la page 29
- acknowledge server, à la page 30
- acknowledge slot, à la page 31
- activate firmware, à la page 32
- backup sel, à la page 33
- cancel, à la page 34
- clear lock-status, à la page 35
- clear message, à la page 36
- clear password-history, à la page 37
- clear sel, à la page 38
- commit-buffer, à la page 39
- connect adapter, à la page 40
- connect asa, à la page 42
- connect cimc, à la page 44
- connect ftd, à la page 46
- connect fxos, à la page 48
- connect local-mgmt, à la page 50
- connect module, à la page 52
- connect vdp, à la page 54
- create app-instance, à la page 56
- create bootstrap-key FIREWALL_MODE, à la page 57
- create bootstrap-key MANAGEMENT_TYPE, à la page 58
- create bootstrap-key PERMIT_EXPERT_MODE, à la page 59
- create bootstrap-key MANAGEMENT_TYPE, à la page 60
- create bootstrap-key-secret PASSWORD, à la page 61
- create bootstrap-key-secret REGISTRATION_KEY, à la page 62
- create bootstrap-key DNS_SERVERS, à la page 63
- create bootstrap-key FIREPOWER_MANAGER_IP, à la page 64
- create bootstrap-key SEARCH_DOMAINS, à la page 65
- create breakout, à la page 66
- create certreq, à la page 68
- create class, à la page 70
- create connection, à la page 73

- create destination, à la page 74
- create dns, à la page 76
- create hw-crypto, à la page 77
- create ip-block, à la page 78
- create ipv6-block, à la page 80
- create keyring, à la page 82
- create local-user, à la page 83
- create member-port, à la page 85
- create ntp-server, à la page 87
- create policy (callhome), à la page 88
- create policy (flow-control), à la page 91
- create port-channel, à la page 93
- create pre-login-banner, à la page 95
- create profile, à la page 97
- create property, à la page 99
- create resource-profile, à la page 101
- create server (scope ldap), à la page 103
- create snmp-trap, à la page 105
- create snmp-user, à la page 107
- create ssh-server, à la page 109
- create stats-threshold-policy, à la page 110
- create subinterface, à la page 112
- create theshold-value, à la page 115
- create trustpoint, à la page 117
- cycle, à la page 118

acknowledge fault

Pour confirmer une défaillance système, utilisez la commande **acknowledge fault**.

acknowledge fault *id*

Description de la syntaxe

fault *ID*	Numéro d'identification de la défaillance. La plage de valeurs valides s'étend de 0 à 18446744073709551615.

Modes de commande

Plusieurs modes

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez la commande **acknowledge fault** pour confirmer l'existence d'une défaillance.

Exemple

L'exemple suivant montre comment confirmer une défaillance :

```
firepower # acknowledge fault 11347599
firepower* # commit-buffer
firepower #
```

Commandes associées

Commande	Description
acknowledge server	Confirme un serveur sur l'appareil.
acknowledge slot	Confirme l'existence d'un logement dans l'appareil.
show fault	Affiche les informations sur la politique en matière de défaillances.

acknowledge server

Pour confirmer un serveur, utilisez la commande **acknowledge server**.

acknowledge server {*id* | *chassis*/*blade_id*}

Description de la syntaxe

server {*id* | *chassis*/*blade_id*}	Pour utiliser le numéro d'identification de serveur afin d'identifier le serveur à confirmer, fournissez l'*id*. Pour utiliser les numéros d'identification de châssis et de lame afin d'identifier le serveur à confirmer, saisissez *chassis*/*blade_id* au format n/n. **Remarque** Le numéro d'ID de châssis est toujours **1**.

Modes de commande

EXEC

scope chassis/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez la commande **acknowledge server** pour vérifier la présence d'un serveur sur votre réseau. Par exemple, vous pouvez confirmer un serveur récemment mis en service pour vous assurer qu'il existe.

En mode châssis, vous pouvez uniquement utiliser la variable *id* pour identifier le serveur à confirmer.

Exemple

L'exemple suivant montre comment confirmer un serveur dans le module 2 en mode châssis :

```
firepower# scope chassis 1
firepower /chassis # acknowledge server 2
firepower /chassis* # commit-buffer
firepower /chassis #
```

Commandes associées

Commande	Description
acknowledge fault	Confirme une défaillance système.
acknowledge slot	Vérifie la présence d'un logement récemment mis en service.
show server	Les commandes **show server** affichent diverses informations de configuration liées au serveur.

acknowledge slot

Pour confirmer un logement, utilisez la commande **acknowledge slot**.

acknowledge slot {*id* | *chassis*/*blade_id*}

Description de la syntaxe

En mode EXEC, utilisez les numéros d'identification du châssis et de la lame pour identifier le logement à confirmer; saisissez *chassis*/*blade_id* au format n/n.

Remarque
Le numéro d'ID de châssis est toujours **1**.

Modes de commande

EXEC

scope chassis/

scope fabric-interconnect/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez la commande **acknowledge slot** pour vérifier l'existence d'un logement récemment mis en service.

En mode châssis et interconnexion de structure, seule la variable *id* vous permet d'identifier le logement à confirmer.

En mode EXEC, seuls les numéros d'identification du châssis et du serveur lame (*chassis*/*blade_id*) vous permettent d'identifier le logement à confirmer.

Exemple

L'exemple suivant montre comment confirmer un logement en mode châssis :

```
firepower# scope chassis 1
firepower /chassis # acknowledge slot 2
firepower /chassis* # commit-buffer
firepower /chassis #
```

Commandes associées

Commande	Description
acknowledge fault	Confirme une défaillance système.
acknowledge server	Confirme l'existence d'un serveur sur votre réseau.

activate firmware

Pour activer un ensemble de micrologiciels, utilisez la commande **activate firmware**.

activate firmware *version*

Description de la syntaxe

version	Utilisez son numéro de version pour spécifier l'ensemble de micrologiciels à activer.

Modes de commande

scope system/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Dans le cadre du processus d'activation, toutes les sessions d'interface de ligne de commande.

Exemple

Cet exemple montre comment activer un ensemble de micrologiciels :

```
firepower# scope system
firepower /system # activate firmware 2.4(1.52)
As part of activation, all cli sessions will be terminated.
Continue with activation? (yes/no)
```

Commandes associées

Commande	Description
show firmware	Affiche les versions du micrologiciel et les informations d'état actuelles du système.
show server firmware	Affiche les versions du micrologiciel et les informations d'état actuelles du serveur.

backup sel

Pour sauvegarder le journal des événements système (SEL), utilisez la commande **backup sel**.

backup sel {*id* | *chassis*/*blade_id*}

Description de la syntaxe

id	ID du serveur. Sur les périphériques 9300, il peut y avoir jusqu'à 3 serveurs.
chassis/*blade_id*	Numéro de châssis et numéro de lame de l'appareil au format x/y. **Remarque** Le numéro d'ID de châssis est toujours **1**.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour sauvegarder le journal des événements système (SEL) d'un serveur.

Dans le mode de commande d'un serveur donné (/chassis/server), vous pouvez exécuter cette commande sans option.

Exemple

Cet exemple montre comment sauvegarder le journal des événements du serveur 2 dans le châssis 1 :

```
firepower# backup sel 1/2
firepower* # commit-buffer
firepower#
```

Commandes associées

Commande	Description
clear sel	Efface le journal des événements système d'un serveur.

cancel

Pour annuler une demande de réservation, utilisez la commande **cancel**.

cancel

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope license/scope reservation/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Si vous avez déjà généré le code d'autorisation, vous devez l'installer.

Exemple

Cet exemple montre comment annuler une demande de réservation :

```
firepower# scope license
firepower /license # scope reservation
firepower /license/reservation # cancel
Warning : If you have already generated the authorization code from CSSM, please abort the
 cancellation by issuing discard-buffer and then install the authorization code.
firepower /license/reservation* #
```

Commandes associées

Commande	Description
enable reservation	Active la réservation de licence permanente.
show license	Affiche les informations de licences actuelles.

clear lock-status

Pour effacer l'état de blocage d'un utilisateur, utilisez la commande **clear lock-status** en mode utilisateur local.

clear lock-status

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Utilisateur local (/security/local-user)

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Si un utilisateur (y compris les utilisateurs admin) dépasse le nombre maximal de tentatives de connexion, l'utilisateur est bloqué et doit attendre la durée spécifiée avant de pouvoir se connecter, sauf si vous effacez son statut de blocage.

Exemple

Cet exemple montre comment accéder au mode utilisateur local et spécifier la durée qu'un utilisateur bloqué doit attendre avant de pouvoir se connecter.

```
FP9300-A # scope security
FP9300-A # scope local-user test_user1
FP9300-A /security/local-user # clear lock-status
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

Commandes associées

Commande	Description
set max-login-attempts	Spécifie le nombre maximal de tentatives de connexion infructueuses avant qu'un utilisateur ne soit bloqué du système.
set user-account-unlock-time	Spécifie la durée pendant laquelle l'utilisateur reste bloqué du système après avoir atteint le nombre maximal de tentatives de connexion.

clear message

Pour effacer le texte de la bannière de préconnexion actuelle, utilisez la commande **clear message**; l'objet de bannière de préconnexion n'est pas supprimé.

clear message

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope security/scope banner/scope pre-login-banner/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Lorsque vous saisissez cette commande, le texte de la bannière de préconnexion est effacé; l'objet de bannière de préconnexion n'est pas supprimé.

Exemple

Cet exemple montre comment afficher la bannière de préconnexion actuelle, l'effacer, puis valider et confirmer votre modification :

```
firepower # scope security
firepower /security # scope banner
firepower /security/banner # scope pre-login-banner
firepower /security/banner/pre-login-banner # show

Pre login banner:
    Message
    -------
    Firepower-9300-2
Western Data Center

firepower /security/banner/pre-login-banner # clear message
firepower /security/banner/pre-login-banner* # commit
firepower /security/banner/pre-login-banner # show

Pre login banner:
    Message
    -------

firepower /security/banner/pre-login-banner #
```

Commandes associées

Commande	Description
create pre-login-banner	Crée une bannière à présenter avant l'écran de connexion; l'objet de bannière est initialement vide.
set message	Ajoute ou remplace les lignes de texte présentées comme bannière de préconnexion.

clear password-history

Pour effacer l'historique des mots de passe d'un utilisateur local, utilisez la commande **clear password-history**.

clear password-history

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode utilisateur local (/security/local-user)

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Seuls les utilisateurs dotés de privilèges d'administrateur ou AAA peuvent utiliser cette commande.

Exemple

Cet exemple montre comment accéder au mode utilisateur local et effacer l'historique des mots de passe de l'utilisateur.

```
FP9300-A # scope security
FP9300-A /security # scope local-user test_user
FP9300-A /security/local-user # clear password history
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

Commande	Description
create local-user	Crée un compte d'utilisateur local.
set password	Spécifie le mot de passe d'un compte d'utilisateur.

clear sel

Pour effacer le journal des événements système d'un serveur, utilisez la commande **clear sel**.

clear sel {*id* | *chassis_id* / *blade_id*}

Description de la syntaxe

id	(Facultatif) ID du serveur. Les appareils 9300 présentent un maximum de 3 serveurs.
chassis_id / *blade_id*	(Facultatif) Numéro de châssis et numéro de lame au format x/y. **Remarque** Le numéro d'ID de châssis est toujours **1**.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.4(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour effacer le journal des événements système (SEL) d'un serveur.

En mode de commande d'un serveur donné (/chassis/serveur), vous pouvez exécuter cette commande sans spécifier de serveur.

Exemple

Cet exemple montre comment effacer les journaux des événements système du serveur 1 dans le châssis 1 en mode organisation.

```
FP9300-A # scope org Test
FP9300-A /org # clear sel 1/1
FP9300-A /org* # commit-buffer
FP9300-A /org #
```

Commandes associées

Commande	Description
backup sel	Sauvegarde le journal des événements système (SEL).

commit-buffer

Pour enregistrer ou vérifier ces modifications de configuration, utilisez la commande **commit-buffer**.

commit-buffer [**verify-only**]

Description de la syntaxe

verify-only	(Facultatif) Vérifie/valide uniquement le contenu du tampon; le contenu n'est pas appliqué.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour exécuter ou vérifier toutes les modifications de configuration en attente. Si des modifications de configuration sont en attente, un astérisque (*) s'affiche avant l'invite de commande. Lorsque vous saisissez la commande **commit-buffer**, les commandes en attente sont validées et l'astérisque disparaît.

Exemple

Cet exemple montre comment enregistrer les modifications de configuration :

```
FP9300-A# create org 3
FP9300-A /org* # commit-buffer
FP9300-A /org #
```

Commandes associées

Commande	Description
discard-buffer	Annule et ignore toutes les modifications de configuration non validées.
show configuration pending	Affiche toutes les modifications de configuration en attente.

connect adapter

Pour vous connecter au shell de commande de l'adaptateur, utilisez la commande **connect adapter**.

connect adapter {*chassis/server/id* | *rack_server/id*}

Description de la syntaxe

chassis/server/id	Spécifie les ID de châssis, de serveur (module) et d'adaptateur (saisis au format n/n). Sur Firepower 9300, le numéro de module peut être 1, 2 ou 3. Sur Firepower 4100, il s'agit de 1. **Remarque** Le numéro d'ID de châssis est toujours **1**.
rack_server/id	Spécifie le numéro de rack et l'ID du module (saisis au format n/n).

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez **help** pour répertorier les commandes d'adaptateur mezzanine disponibles; utilisez la commande **help** pour afficher les informations sur une commande individuelle.

Pour plus de renseignements, consultez Liste des commandes connect adapter, à la page 732.

Remarque Lorsque vous vous connectez à un shell de commande d'adaptateur, l'invite de ligne de commande passe de votre invite par défaut, qui est le nom que vous avez attribué au périphérique, à `adapter n/n/n`, où `n/n/n` correspond à la combinaison châssis/serveur/ID de l'adaptateur que vous avez saisie pour la connexion.

Pour quitter le mode adaptateur, saisissez **exit**.

Exemple

L'exemple suivant montre comment se connecter au shell de commande de l'adaptateur et afficher les commandes disponibles :

```
firepower# connect adapter 1/1/1
adapter 1/1/1 # help
Available commands:
  connect             - Connect to remote debug shell
  exit                - Exit from subshell
  help                - List available commands
  history             - Show command history
  show-fwlist         - Show firmware versions on the adapter
  show-identity       - Show adapter identity
  show-phyinfo        - Show adapter phy info
  show-systemstatus   - Show adapter status
adapter 1/1/1 # exit
```

```
firepower#
```

Commandes associées

Commande	Description
exit	Vous ramène au mode CLI précédent.

connect asa

Pour vous connecter à l'interface de ligne de commande ASA, utilisez la commande **connect asa**.

connect asa [*name*]

Description de la syntaxe

name	(Facultatif) Spécifie le nom de l'instance d'application ASA, qui est identique au nom du périphérique logique.

Modes de commande

connect module/

Historique des commandes

Version	Modification
2.4(1)	Ajout de l'argument *name*.
1.1(4)	Commande ajoutée.

Instructions d'utilisation

Consultez la documentation ASA pour connaître les commandes disponibles à partir de l'interface de ligne de commande.

Pour quitter la console ASA, entrez **Ctrl-a, d**

Revenez au niveau de superviseur de l'interface de ligne de commande FXOS :

Quittez la console :

Saisissez **~**, puis **quit** pour quitter l'application Telnet.

Exemple :

```
asa> Ctrl-a, d
Firepower-module1> ~
telnet> quit
firepower#
```

Quittez la session Telnet :

Entrez **Ctrl-], .**

Exemple :

```
asa> Ctrl-a, d
Firepower-module1> Ctrl-], .
firepower#
```

Exemple

Cet exemple montre comment se connecter à l'interface de ligne de commande ASA sur le module 1 :

```
firepower# connect module 1 console
Telnet escape character is '~'.
```

```
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1> connect asa
asa>
```

Commandes associées

Commande	Description
connect ftd	Permet de se connecter à l'interface de ligne de commande Défense contre les menaces.
connect module	Permet de se connecter à l'interface de ligne de commande du module.
connect vdp	Permet de se connecter à l'interface de ligne de commande vDP.

connect cimc

Pour vous connecter au shell de commande CIMC (Cisco Integrated Management Controller), utilisez la commande **connect cimc**.

connect cimc {*chassis_id/blade_id* | *rack_id*}

Description de la syntaxe

chassis_id/blade_id	Spécifie les numéros de châssis et de module (saisis au format n/n). **Remarque** Le numéro d'ID de châssis est toujours **1**.
rack_id	Spécifie le numéro de rack.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Saisissez **help** pour répertorier les commandes de l'utilitaire de débogage du micrologiciel CIMC disponibles; saisissez **help** *command* pour afficher les informations sur une commande individuelle.

Remarque Lorsque vous vous connectez au shell de commande CIMC, l'invite de ligne de commande passe de votre invite par défaut, qui correspond au nom que vous avez attribué à l'appareil, à `[ xxx ]`, où `xxx` correspond à la dernière commande que vous avez saisie; consultez l'exemple suivant.

Saisissez **exit** pour arrêter l'utilitaire.

N'utilisez pas cet utilitaire, sauf si le centre d'assistance technique Cisco TAC vous le demande. Pour plus d'informations, consultez Liste des commandes connect cimc, à la page 737.

Exemple

L'exemple suivant montre comment se connecter au mode CIMC, puis répertorier les commandes disponibles :

```
firepower# connect cimc 1/1
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '^]'.

CIMC Debug Firmware Utility Shell [ support ]
[ help ]# help
_____________________________________________
          Debug Firmware Utility
_____________________________________________
Command List
_____________________________________________
```

```
alarms
cores
dimmbl
exit
i2cstats
images
mctools
memory
messages
mrcout
network
obfl
post
power
programmables
sensors
sel
fru
tasks
top
update
users
version
cert
sldp
help
help [COMMAND]
_____________________________________
 Notes:
"enter Key" will execute last command
"COMMAND ?" will execute help for that command
_____________________________________
[ help ]# exit
Connection closed by foreign host.
firepower#
```

Commandes associées

Commande	Description
exit	Vous ramène au mode CLI précédent.

connect ftd

Pour vous connecter à l'interface de ligne de commande Défense contre les menaces, utilisez la commande **connect ftd**.

connect ftd *name*

Description de la syntaxe

name	Spécifie le nom de l'instance d'application Défense contre les menaces, qui est identique au nom du périphérique logique. Si vous disposez de plusieurs instances d'un type d'application, vous devez spécifier le nom de l'instance. Pour afficher les noms des instances, entrez la commande sans nom.

Modes de commande

connect module/

Historique des commandes

Version	Modification
2.4(1)	Ajout de l'argument *name*. Le caractère d'échappement a été remplacé par **exit** à partir de **Ctrl-a, d**.
1.1(4)	Commande ajoutée.

Instructions d'utilisation

Consultez la documentation Défense contre les menaces pour connaître les commandes disponibles à partir de l'interface de ligne de commande.

Pour quitter la console Défense contre les menaces, saisissez **exit**. Pour les versions antérieures à la version 2.4(1), entrez **Ctrl-a, d**.

Revenez au niveau de superviseur de l'interface de ligne de commande FXOS :

Quittez la console :

Saisissez **~**, puis **quit** pour quitter l'application Telnet.

Exemple :

```
> exit
Firepower-module1> ~
telnet> quit
firepower#
```

Quittez la session Telnet :

Entrez **Ctrl-], .**

Exemple :

```
> exit
Firepower-module1> Ctrl-], .
firepower#
```

Exemple

Cet exemple montre comment se connecter à l'interface de ligne de commande Défense contre les menaces sur le module 1 :

```
firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1> connect ftd
>
```

Commandes associées

Commande	Description
connect asa	Permet de se connecter à l'interface de ligne de commande de l'appareil de sécurité adaptable Cisco.
connect module	Permet de se connecter à l'interface de ligne de commande du module.
connect vdp	Permet de se connecter à l'interface de ligne de commande vDP.

connect fxos

Pour vous connecter au shell de commande FXOS, utilisez la commande **connect fxos**.

connect fxos [**a**]

Description de la syntaxe

a	(Facultatif) Se connecte à la structure a. **Remarque** L'ID de structure est toujours **a**. Si vous omettez l'ID de structure, vous êtes connecté à la structure A.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Saisissez **?** pour répertorier les commandes du shell FXOS disponibles; saisissez *command* **?** pour afficher les informations sur une commande individuelle.

Remarque Lorsque vous vous connectez au shell de commande FXOS, l'invite de ligne de commande passe de votre invite par défaut, qui correspond au nom que vous avez attribué à l'appareil, à l'invite par défaut à laquelle est ajouté `(fxos)`; consultez l'exemple suivant.

Pour quitter le shell FXOS, saisissez **exit**.

Exemple

L'exemple suivant montre comment se connecter au shell de commande FXOS et afficher les commandes disponibles :

```
firepower# connect fxos
firepower(fxos)# ?
  clear         Reset functions
  cli           CLI commands
  debug         Debugging functions
  debug-filter  Enable filtering for debugging functions
  ethanalyzer   Configure cisco packet analyzer
  no            Negate a command or set its defaults
  ntp           NTP configuration
  show          Show running system information
  system        System management commands
  terminal      Set terminal line parameters
  test          Test command
  undebug       Disable Debugging functions (See also debug)
  end           Go to exec mode
  exit          Exit from command interpreter
  pop           Pop mode from stack or restore from name
```

```
  push           Push current mode to stack or save it under name
  where          Shows the cli context you are in

firepower(fxos)# exit
firepower#
```

Commandes associées

Commande	Description
connect local-mgmt	Se connecte à un shell de débogage distant tout en étant connecté à un adaptateur spécifique.
exit	Vous ramène au mode CLI précédent.

connect local-mgmt

Pour vous connecter au shell de commande de gestion locale, utilisez la commande **connect local-mgmt**.

connect local-mgmt [**a**]

Description de la syntaxe

a	(Facultatif) Se connecte à la structure a. **Remarque** L'ID de structure est toujours **a**. Si vous omettez l'ID de structure, vous êtes connecté à la structure A.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Saisissez **?** pour répertorier les commandes shell de gestion local disponibles; saisissez *command* **?** pour afficher les informations sur une commande individuelle.

Pour plus de renseignements, consultez Liste de commandes connect local-mgmt, à la page 756.

Remarque Lorsque vous vous connectez au shell de commande de gestion locale, l'invite de ligne de commande passe de votre invite par défaut, qui correspond au nom que vous avez attribué à l'appareil, à l'invite par défaut à laquelle est ajouté `(local-mgmt)` ; consultez l'exemple suivant.

Pour quitter le mode gestion locale, saisissez **exit**.

Exemple

L'exemple suivant montre comment se connecter au shell de commande de gestion locale et afficher les commandes disponibles :

```
firepower# connect local-mgmt
firepower(local-mgmt)#  ?
  cd                Change current directory
  clear             Clear managed objects
  cluster           Cluster mode
  connect           Connect to Another CLI
  copy              Copy a file
  cp                Copy a file
  delete            Delete managed objects
  dir               Show content of dir
  enable            Enable
  end               Go to exec mode
  erase             Erase
  erase-log-config  Erase the mgmt logging config file
  exit              Exit from command interpreter
```

```
  fips              FIPS compliance
  ls                Show content of dir
  mgmt-port         Management Port
  mkdir             Create a directory
  move              Move a file
  mv                Move a file
  ping              Test network reachability
  ping6             Test IPv6 network reachability
  pwd               Print current directory
  reboot            Reboots Fabric Interconnect
  restore-check     Check if in restore mode
  rm                Remove a file
  rmdir             Remove a directory
  run-script        Run a script
  show              Show system information
  shutdown          Shutdown
  ssh               SSH to another system
  tail-mgmt-log     tail mgmt log file
  telnet            Telnet to another system
  terminal          Terminal
  top               Go to the top mode
  traceroute        Traceroute to destination
  traceroute6       Traceroute to IPv6 destination
  verify            Verify Application Image

firepower(local-mgmt)# exit
firepower#
```

Commandes associées

Commande	Description
connect fxos	Se connecte au shell de commande FXOS.
exit	Vous ramène au mode CLI précédent.

connect module

Pour vous connecter à un shell de commande de module, utilisez la commande **connect module**.

connect module *module_id* {**console** | **telnet**}

Description de la syntaxe

console	Se connecte à la console série. L'avantage d'une connexion console réside dans sa persistance.
module_id	Sur les appareils 9300, le numéro de module peut être 1, 2 ou 3; sur les appareils 4100, il s'agit de 1.
telnet	Se connecte à l'aide d'une connexion Telnet. Les avantages de l'utilisation d'une connexion Telnet sont que vous pouvez avoir plusieurs sessions sur le module en même temps et que la vitesse de connexion est plus rapide.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
2.4(1)	Prise en charge de Telnet ajoutée.
1.1(1)	Commande ajoutée.

Instructions d'utilisation

À partir de l'interface de ligne de commande du module, vous pouvez vous connecter à l'interface de ligne de commande de l'application à l'aide de la commande **connect** *application*.

Saisissez **help** pour répertorier les commandes shell du module disponibles; saisissez **help** *command* pour afficher les informations sur une commande individuelle. Vous pouvez également utiliser **?** plutôt que **help** pour afficher les informations d'aide.

Remarque Lorsque vous vous connectez au shell de commande d'un module, l'invite de ligne de commande passe de votre invite par défaut, qui correspond au nom que vous avez attribué à l'appareil, à `Firepower-module`*n*, où *n* correspond au numéro du module auquel vous vous êtes connecté; consultez l'exemple suivant.

Pour plus de renseignements, consultez Liste des commandes connect module, à la page 762.

Exemples

L'exemple suivant montre comment se connecter à la console du module 1 et afficher les commandes disponibles :

```
firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
```

```
CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>?
    secure-login     => Enable blade secure login
    show             => Display system information. Enter show ? for options
    config           => Configure the system. Enter config ? for options
    terminalLength   => Terminal settings. Enter terminal ? for options
    ping             => Ping a host to check reachability
    nslookup         => Look up an IP address or host name with the DNS servers
    traceroute       => Trace the route to a remote host
    connect          => Connect to specific csp console (asa, etc)
    support          => System file operations
    help             => Get help on command syntax

Firepower-module1> ~
telnet> close
Connection closed.
firepower#
```

L'exemple suivant montre comment se connecter au module 1 à l'aide de Telnet et afficher les commandes disponibles :

```
firepower# connect module 1 telnet
Type exit or Ctrl-] followed by . to quit.
Firepower-module1>?
    secure-login     => Enable blade secure login
    show             => Display system information. Enter show ? for options
    config           => Configure the system. Enter config ? for options
    terminalLength   => Terminal settings. Enter terminal ? for options
    ping             => Ping a host to check reachability
    nslookup         => Look up an IP address or host name with the DNS servers
    traceroute       => Trace the route to a remote host
    connect          => Connect to specific csp console (asa, etc)
    support          => System file operations
    exit             => Exit the session
    help             => Get help on command syntax
Firepower-module1> <Ctrl-], .>
firepower#
```

Commandes associées

Commande	Description
connect asa	Permet de se connecter à l'interface de ligne de commande de l'appareil de sécurité adaptable Cisco.
connect ftd	Permet de se connecter à l'interface de ligne de commande Défense contre les menaces.
connect vdp	Permet de se connecter à l'interface de ligne de commande vDP.

connect vdp

Pour vous connecter à l'interface de ligne de commande Radware DefensePro (vDP), utilisez la commande **connect vdp**.

connect vdp [*name*]

Description de la syntaxe

name	(Facultatif) Spécifie le nom de l'instance d'application vDP, qui est identique au nom du périphérique logique ou de l'instance d'application principale.

Modes de commande

connect module/

Historique des commandes

Version	Modification
2.4(1)	Ajout de l'argument *name*.
1.1(4)	Commande ajoutée.

Instructions d'utilisation

Consultez la documentation vDP pour connaître les commandes disponibles à partir de l'interface de ligne de commande.

Pour quitter la console vDP, saisissez **Ctrl-], .**

Revenez au niveau de superviseur de l'interface de ligne de commande FXOS :

Quittez la console :

Saisissez **~**, puis **quit** pour quitter l'application Telnet.

Exemple :

```
> Ctrl-], .
Firepower-module1> ~
telnet> quit
firepower#
```

Quittez la session Telnet :

Entrez **Ctrl-], .**

Exemple :

```
> Ctrl-], .
Firepower-module1> Ctrl-], .
firepower#
```

Exemple

Cet exemple montre comment se connecter à l'interface de ligne de commande vDP sur le module 1 :

```
firepower# connect module 1 console
```

```
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1> connect vdp
```

Commandes associées

Commande	Description
connect asa	Permet de se connecter à l'interface de ligne de commande de l'appareil de sécurité adaptable Cisco.
connect ftd	Permet de se connecter à l'interface de ligne de commande Défense contre les menaces.
connect module	Permet de se connecter à l'interface de ligne de commande du module.

create app-instance

Pour définir une instance d'application, utilisez la commande **create app-instance**.

create app-instance *app_type app_name*

Description de la syntaxe

app_name	Nom de l'instance d'application, entre 1 et 64 caractères. Vous utiliserez ce nom de périphérique lorsque vous créerez le périphérique logique pour cette instance.
app_type	Type d'application, **asa**, **ftd**ou **vdp**.

Modes de commande

scope ssa/scope slot/

Historique des commandes

Version	Modification
2.4(1)	L'argument *app_name* est maintenant requis.
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous pouvez définir de nombreux paramètres pour cette instance d'application, notamment la version de l'image, le type de déploiement, le profil de ressource et le mode. Vous pouvez également activer, désactiver et redémarrer l'application.

Exemple

L'exemple suivant montre comment définir la version de l'image pour une instance d'application Défense contre les menaces :

```
firepower# scope ssa
firepower /ssa # scope slot 1
firepower /ssa/slot # create app-instance ftd MyDevice1
firepower /ssa/slot/app-instance* # set deploy-type container
firepower /ssa/slot/app-instance* # set resource-profile-name silver 1
firepower /ssa/slot/app-instance* # set startup-version 6.3.0
firepower /ssa/slot/app-instance* #
```

Commandes associées

Commande	Description
show app-attri	Affiche les attributs de l'application actuelle.

create bootstrap-key FIREWALL_MODE

Pour définir le mode pare-feu routé ou transparent dans la configuration de démarrage de Défense contre les menaces et ASA, utilisez la commande **create bootstrap-key FIREWALL_MODE**.

create bootstrap-key FIREWALL_MODE

Modes de commande

scope ssa/create logical-device/create mgmt-bootstrap/

Commande par défaut

Le mode par défaut est le mode routé.

Historique des commandes

Version	Modification
2.4(1)	Ajout de prise en charge pour ASA.
1.1(4)	Commande ajoutée pour Cisco FTD.

Instructions d'utilisation

Les paramètres de démarrage sont uniquement destinés au déploiement initial ou à la reprise sur sinistre. Pour un fonctionnement normal, vous pouvez modifier la plupart des valeurs dans la configuration de l'interface de ligne de commande de l'application.

Exemple

L'exemple suivant montre comment définir le mode sur le mode routé :

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
firepower /ssa/logical-device/mgmt-bootstrap* #
```

Commandes associées

Commande	Description
create logical-device	Crée le périphérique logique.
create mgmt-bootstrap	Crée la configuration de démarrage de l'application.
set value	Définit la valeur de cette commande.

create bootstrap-key MANAGEMENT_TYPE

Pour spécifier le gestionnaire, FMC, FDM ou CDO, dans la configuration de démarrage de Défense contre les menaces, utilisez la commande **create bootstrap-key MANAGEMENT_TYPE**.

create bootstrap-key MANAGEMENT_TYPE

Modes de commande

scope ssa/create logical-device/create mgmt-bootstrap/

Commande par défaut

Le gestionnaire par défaut est FMC.

Historique des commandes

Version	Modification
2.7(1)	Commande ajoutée pour Cisco FTD.

Instructions d'utilisation

Les paramètres de démarrage sont uniquement destinés au déploiement initial ou à la reprise sur sinistre. Pour un fonctionnement normal, vous pouvez modifier la plupart des valeurs dans la configuration de l'interface de ligne de commande de l'application.

Exemple

L'exemple suivant montre comment définir le gestionnaire sur FDM :

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key MANAGEMENT_TYPE
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value LOCALLY_MANAGED
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
firepower /ssa/logical-device/mgmt-bootstrap* #
```

L'exemple suivant montre comment définir le gestionnaire sur CDO :

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key MANAGEMENT_TYPE
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value CDO
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
firepower /ssa/logical-device/mgmt-bootstrap* #
```

Commandes associées

Commande	Description
create logical-device	Crée le périphérique logique.
create mgmt-bootstrap	Crée la configuration de démarrage de l'application.
set value	Définit la valeur de cette commande.

create bootstrap-key PERMIT_EXPERT_MODE

Pour autoriser le mode expert des sessions FTD SSH pour Défense contre les menaces, utilisez la commande **create bootstrap-key PERMIT_EXPERT_MODE**.

create bootstrap-key PERMIT_EXPERT_MODE

Modes de commande

scope ssa/create logical-device/create mgmt-bootstrap/

Commande par défaut

La valeur par défaut est « no » (non).

Historique des commandes

Version	Modification
2.4(1)	Commande ajoutée.

Instructions d'utilisation

Le mode expert fournit à Cisco FTD un accès au shell pour un dépannage avancé. Par défaut, pour les instances de contenant, le mode expert n'est disponible que pour les utilisateurs qui accèdent à l'interface de ligne de commande Cisco FTD à partir de l'interface de ligne de commande FXOS. Cette limitation est uniquement appliquée aux instances de conteneur pour augmenter l'isolement entre les instances. Utilisez le mode expert uniquement si une procédure documentée vous indique que c'est nécessaire ou si le Centre d'assistance technique (TAC) de Cisco vous demande de l'utiliser. Pour accéder à ce mode, utilisez la commande expert dans l'interface de ligne de commande Cisco FTD.

Exemple

L'exemple suivant montre comment activer le mode expert à partir de SSH :

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key PERMIT_EXPERT_MODE
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value yes
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
firepower /ssa/logical-device/mgmt-bootstrap* #
```

Commandes associées

Commande	Description
create logical-device	Crée le périphérique logique.
create mgmt-bootstrap	Crée la configuration de démarrage de l'application.
set value	Définit la valeur de cette commande.

create bootstrap-key MANAGEMENT_TYPE

create bootstrap-key-Secret CDO_ONBOARD

Modes de commande

scope ssa/create logical-device/create mgmt-bootstrap/

Historique des commandes

Version	Modification
2.13(1)	Commande ajoutée pour Cisco FTD.

Instructions d'utilisation

Les paramètres de démarrage sont uniquement destinés au déploiement initial ou à la reprise sur sinistre. Pour un fonctionnement normal, vous pouvez modifier la plupart des valeurs dans la configuration de l'interface de ligne de commande de l'application.

Exemple

L'exemple suivant montre comment définir la valeur d'intégration CDO pour l'appareil Cisco FTD :

```
Firepower /SSA-5 /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret CDO_ONBOARD
Firepower /SSA-5 /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
Firepower /SSA-5 /ssa/logical-device/mgmt-bootstrap/bootstrap-key* #
Enter a value:(the string "configure manager add cisco-sapphire.app.staging.cdo.cisco.com
TuNDBm6peReVDbU kOpZCgtJ1GqWKbD30 o9B064UXEwmr3AYAEpuflf4qE2E3JKY5 <display_name>" should
be
entered)
Confirm the value: (repeat the string)
Firepower /SSA-5 /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # commit-buffer
```

Commandes associées

Commande	Description
create logical-device	Crée le périphérique logique.
create mgmt-bootstrap	Crée la configuration de démarrage de l'application.
set value	Définit la valeur de cette commande.

create bootstrap-key-secret PASSWORD

Pour spécifier le mot de passe administrateur dans la configuration de démarrage pour Défense contre les menaces et ASA, utilisez la commande **create bootstrap-key-secret PASSWORD**.

create bootstrap-key-secret PASSWORD

Modes de commande

scope ssa/create logical-device/create mgmt-bootstrap/

Commande par défaut

Lorsque le mot de passe administrateur n'est pas défini.

Historique des commandes

Version	Modification
1.1(4)	Commande ajoutée pour Cisco FTD.
2.4(1)	Ajout de prise en charge pour ASA.

Instructions d'utilisation

L'utilisateur admin ASA et le mot de passe d'activation préconfigurés sont utiles pour la récupération du mot de passe. si vous avez un accès FXOS, vous pouvez réinitialiser le mot de passe de l'utilisateur admin en cas d'oubli.

Exemple

L'exemple suivant montre comment définir le mode sur le mode routé :

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # create bootstrap-key-secret
PASSWORD
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

Commandes associées

Commande	Description
create logical-device	Crée le périphérique logique.
create mgmt-bootstrap	Crée la configuration de démarrage de l'application.
set value	Définit la valeur de cette commande.

create bootstrap-key-secret REGISTRATION_KEY

Pour spécifier une clé d'enregistrement à partager entre l'appareil Défense contre les menaces et centre de gestion dans la configuration de démarrage, utilisez la commande **create bootstrap-key-secret REGISTRATION_KEY**.

create bootstrap-key-secret REGISTRATION_KEY

Modes de commande

scope ssa/create logical-device/create mgmt-bootstrap/

Commande par défaut

La clé enregistrée n'est pas générée.

Historique des commandes

Version	Modification
1.1(4)	Commande ajoutée pour Cisco FTD.

Instructions d'utilisation

Vous pouvez choisir n'importe quelle phrase secrète pour cette clé d'enregistrement, entre 1 et 37 caractères. Vous saisissez la même clé sur FMC lorsque vous ajoutez l'appareil Cisco FTD. Les paramètres de démarrage sont uniquement destinés au déploiement initial ou à la reprise sur sinistre. Pour un fonctionnement normal, vous pouvez modifier la plupart des valeurs dans la configuration de l'interface de ligne de commande de l'application.

Exemple

L'exemple suivant montre comment définir la valeur de la clé d'enregistrement :

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # create bootstrap-key-secret
REGISTRATION_KEY
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: gratuitousapples
Confirm the value: gratuitousapples
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

Commandes associées

Commande	Description
create logical-device	Crée le périphérique logique.
create mgmt-bootstrap	Crée la configuration de démarrage de l'application.
set value	Définit la valeur de cette commande.

create bootstrap-key DNS_SERVERS

Pour spécifier une liste séparée par des virgules des serveurs DNS de Défense contre les menaces, utilisez la commande **create bootstrap-key DNS_SERVERS**.

create bootstrap-key DNS_SERVERS

Modes de commande

scope ssa/create logical-device/create mgmt-bootstrap/

Commande par défaut

La valeur par défaut est « no » (non).

Historique des commandes

Version	Modification
2.4(1)	Commande ajoutée.

Instructions d'utilisation

Cisco FTD utilise DNS si vous spécifiez un nom de domaine pour FMC.

Exemple

L'exemple suivant montre comment spécifier un nom de domaine :

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.9.8.7,10.9.6.5
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

Commandes associées

Commande	Description
create logical-device	Crée le périphérique logique.
create mgmt-bootstrap	Crée la configuration de démarrage de l'application.
set value	Définit la valeur de cette commande.

create bootstrap-key FIREPOWER_MANAGER_IP

Pour spécifier l'adresse IP, le nom de domaine ou l'ID NAT de Cisco Firepower Management Center (FMC), utilisez la commande **create bootstrap-key FIREPOWER_MANAGER_IP**.

create bootstrap-key FIREPOWER_MANAGER_IP

Modes de commande

scope ssa/create logical-device/create mgmt-bootstrap/

Commande par défaut

La valeur par défaut est « no » (non).

Historique des commandes

Version	Modification
2.4(1)	Commande ajoutée.

Instructions d'utilisation

Normalement, vous avez besoin des deux adresses IP (et d'une clé d'enregistrement) à des fins de routage et d'authentification : le FMC indique l'adresse IP du périphérique et le périphérique indique l'adresse IP FMC. Toutefois, si vous ne connaissez qu'une seule des adresses IP, ce qui est le minimum requis à des fins de routage, vous devez également spécifier un ID NAT unique des deux côtés de la connexion afin d'établir la confiance pour la communication initiale et de rechercher la clé d'enregistrement correcte. Vous pouvez spécifier n'importe quelle chaîne de texte comme ID NAT (de 1 à 37 caractères). Le FMC et l'appareil utilisent la clé d'enregistrement et l'ID NAT (plutôt que les adresses IP) à des fins d'authentification et d'autorisation pour l'enregistrement initial.

Exemple

L'exemple suivant montre comment activer le mode expert à partir de SSH :

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREPOWER_MANAGER_IP
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.10.10.7
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

Commandes associées

Commande	Description
create logical-device	Crée le périphérique logique.
create mgmt-bootstrap	Crée la configuration de démarrage de l'application.
set value	Définit la valeur de cette commande.

create bootstrap-key SEARCH_DOMAINS

Pour spécifier la liste des domaines de recherche en les séparant par des virgules, utilisez la commande **create bootstrap-key SEARCH_DOMAINS**

create bootstrap-key SEARCH_DOMAINS

Modes de commande scope ssa/create logical-device/create mgmt-bootstrap/

Commande par défaut La valeur par défaut est « no » (non).

Historique des commandes

Version	Modification
2.4(1)	Commande ajoutée.

Exemple

L'exemple suivant montre comment activer le mode expert à partir de SSH :

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value cisco.com,example.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

Commandes associées

Commande	Description
create logical-device	Crée le périphérique logique.
create mgmt-bootstrap	Crée la configuration de démarrage de l'application.
set value	Définit la valeur de cette commande.

create breakout

Pour créer un port de répartition, utilisez la commande **create breakout**. Si une répartition avec les ID de logement et de port spécifiés existe déjà, la commande échoue.

Pour ajouter ou accéder à un port de répartition, utilisez la commande **enter breakout**. Si la répartition spécifiée n'existe pas, elle est créée et saisie; si le port de répartition existe, il est saisi.

Vous pouvez également utiliser la forme **scope** de cette commande pour accéder à un port de répartition existant et en afficher les propriétés.

Pour supprimer un port de répartition existant, utilisez la forme **delete** de cette commande.

create breakout *slot_ID port_ID*

Description de la syntaxe

slot_ID	Utiliser son numéro de logement pour identifier le module de port à répartir.
port_ID	Attribuer un numéro d'ID à ce port de répartition.

Modes de commande

scope cabling/scope fabric a/

Historique des commandes

Version	Modification
1.1.1	Commande ajoutée.

Instructions d'utilisation

En conjonction avec l'utilisation d'un câble de répartition, vous pouvez utiliser cette commande pour « répartir » un port Ethernet de 40 Gigabits, créant ainsi jusqu'à quatre ports de 10 Gigabits non configurés.

Les interfaces compatibles avec le contournement matériel ne peuvent pas être configurées en tant que port de répartition.

Remarque La configuration d'une répartition sur un port entraînant le redémarrage du système, nous vous recommandons de répartir tous les ports nécessaires avant de valider les modifications.

Exemple

L'exemple suivant montre comment créer quatre ports de répartition sur le logement 2 :

```
firepower# scope cabling
firepower /cabling/fabric/ # scope fabric
firepower /cabling/fabric/ # create breakout 2 1
Warning: This action will reboot the system and any existing configurations on 40G port
will be erased.!
firepower /cabling/fabric/breakout* # up
firepower /cabling/fabric/ # create breakout 2 2
Warning: This action will reboot the system and any existing configurations on 40G port
will be erased.!
firepower /cabling/fabric/breakout* # up
firepower /cabling/fabric/ # create breakout 2 3
Warning: This action will reboot the system and any existing configurations on 40G port
will be erased.!
```

```
firepower /cabling/fabric/breakout* # up
firepower /cabling/fabric/ # create breakout 2 4
Warning: This action will reboot the system and any existing configurations on 40G port
will be erased.!
firepower /cabling/fabric/breakout* # commit-buffer
firepower /cabling/fabric/breakout #
```

Commandes associées

Commande	Description
delete breakout	Supprime un port de répartition existant.
enter aggr-interface	Permet d'accéder à une interface agrégée où vous pouvez définir les paramètres.

create certreq

Pour ajouter une nouvelle demande de certificat de trousseau de clés, utilisez la commande **create certreq**. Si une demande existe déjà pour le trousseau de clés actuel, la commande échoue.

Pour modifier une demande de certificat existante, utilisez la commande **enter certreq**.

Vous pouvez également utiliser la forme **scope** de cette commande pour accéder à une demande de certificat existante afin d'affecter ou de modifier des propriétés.

Pour supprimer une demande de certificat existante, utilisez la forme **delete** de cette commande.

create certreq [**ip** | **subject-name**]

delete certreq

enter certreq
scope certreq

Description de la syntaxe

ip *ip_address*	(Facultatif) Saisissez le mot clé **ip** et l'adresse IPv4 du domaine sur lequel se trouve cet appareil. Vous devrez saisir et confirmer un mot de passe pour la demande. Ce paramètre s'applique uniquement à la forme **create certreq** de la commande.
subject-name *name*	(Facultatif) Saisissez le mot clé **subject-name** et un identifiant pour cette demande; par exemple, le nom de domaine de l'appareil. Vous devrez saisir et confirmer un mot de passe pour la demande. Ce paramètre s'applique uniquement à la forme **create certreq** de la commande.

Modes de commande

scope security/scope keyring/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Lorsque vous créez une demande de certificat de trousseau de clés, vous accédez automatiquement au mode demande de certificat (security/keyling/certreq) accompagné d'un astérisque pour indiquer que la nouvelle demande de certificat n'est pas encore définie et validée. Vous pouvez également accéder au mode demande de certificat pour un trousseau de clés existant.

Utilisez la commande **set** en mode demande de certificat pour spécifier les paramètres de demande de certificat.

Remarque Avant de créer ou de valider une demande de certificat, vous devez définir le module de clé RSA (longueur de clé SSL) à l'aide de set modulus, à la page 321.

Exemple

Cet exemple montre comment créer un trousseau de clés et sa demande de certificat :

```
firepower # scope security
firepower /security # create keyring test-ring2
firepower /security/keyring* # create certreq ip 209.165.201.20
Certificate request password:
Confirm certificate request password:
firepower /security/keyring* # scope certreq
firepower /security/keyring/certreq* #
firepower /security/keyring/certreq* # set ?
  country        Country name (2 letter code)
  dns            DNS name (subject alternative name)
  e-mail         E-mail name
  fi-a-ip        Certificate request FI A ip address
  fi-a-ipv6      Certificate request FI A ipv6 address
  fi-b-ip        Certificate request FI B ip address
  fi-b-ipv6      Certificate request FI B ipv6 address
  ip             Certificate request ip address
  ipv6           Certificate request ipv6 address
  locality       Locality name (eg, city)
  org-name       Organisation name (eg, company)
  org-unit-name  Organisational Unit Name (eg, section)
  password       Certificate request password
  state          State, province or county (full name)
  subject-name   Certificate request subject name

firepower /security/keyring/certreq* # set
```

Commandes associées

Commande	Description
delete certreq	Supprime une demande de certificat de trousseau de clés existante.
set (certreq)	Définit les informations relatives à la demande de certificat de trousseau de clés.

create class

Pour ajouter une nouvelle classe de statistiques à une politique de seuil de statistiques, utilisez la commande **create class**. Si une classe portant le nom spécifié existe déjà, la commande échoue.

Pour ajouter ou modifier une classe de statistiques, utilisez la commande **enter class**. Si la classe spécifiée n'existe pas, elle est créée et saisie. Si la classe existe, elle est saisie.

Vous pouvez également utiliser la forme **scope** de cette commande pour accéder à une classe existante afin d'affecter ou de modifier des propriétés. En général, il est plus pratique de « cibler » un objet que de le saisir, car le nom de l'objet est habituellement suffisant, tandis que la forme **enter** de la commande requiert souvent la saisie de tous ses paramètres de définition.

Pour supprimer une classe de statistiques existante, utilisez la forme **delete** de cette commande.

create class *type*
delete class *type*
enter class *type*
scope class *type*

Description de la syntaxe

type	Spécifiez la classe de statistiques souhaitée. Les classes disponibles dépendent de la politique de seuil de statistiques du mode actuel. Par exemple, en mode `eth-server/`, les classes disponibles comprennent `chassis-stats` et `ether-error-stats`. En mode `eth-uplink/`, les classes disponibles comprennent `ether-rx-stats` et `ether-rx-stats`. En mode `org/`, les classes disponibles comprennent `cpu-env-stats` et `ethernet-port-err-stats`. Utilisez la commande **create class ?** pour afficher la liste des classes disponibles pour la politique de seuil de statistiques actuelle.

Modes de commande

scope eth-server/scope stats-threshold-policy/

scope eth-uplink/scope stats-threshold-policy/

scope org/scope stats-threshold-policy/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez les classes pour définir des seuils sur des ensembles de statistiques spécifiques. Par exemple, vous pouvez définir un seuil sur un port qui déclenche une défaillance si le nombre moyen de paquets abandonnés dépasse une certaine valeur. Pour cette classe, vous créez des propriétés de seuil pour les statistiques d'erreur Ethernet.

Vous pouvez configurer plusieurs classes pour une politique de seuil de statistiques.

Utilisez la commande **set collection-interval** pour définir la fréquence de collecte des statistiques et la commande **set reporting-interval** pour définir la fréquence à laquelle ces statistiques sont présentées. Ces intervalles définissent une politique de collecte des statistiques.

Remarque Il existe une politique de seuil de statistiques par défaut pour les ports de serveur Ethernet et les ports de liaison ascendante Ethernet. Vous ne pouvez pas créer de politiques de collecte de statistiques supplémentaires, ni supprimer les politiques par défaut existantes pour ces composants. Vous pouvez uniquement modifier les politiques par défaut. Cependant, vous pouvez créer et supprimer des politiques de seuil de statistiques en mode organisation (`scope org/`).

Exemples

Cet exemple montre comment accéder à la classe de politiques de seuil de statistiques du serveur Ethernet, créer une classe de statistiques de châssis, créer une propriété de puissance d'entrée (Watts), spécifier que la puissance normale est de 8 kW, créer un seuil d'avertissement supérieur à la normale de 11 kW, puis valider la classe :

```
firepower # scope eth-server
firepower /eth-server # scope stats-threshold-policy default
firepower /eth-server/stats-threshold-policy # create class chassis-stats
firepower /eth-server/stats-threshold-policy/class* # create property input-power
firepower /eth-server/stats-threshold-policy/class/property* # set normal-value 8000.0
firepower /eth-server/stats-threshold-policy/class/property* # create threshold-value
above-normal warning
firepower /eth-server/stats-threshold-policy/class/property/threshold-value* # set escalating
 11000.0
firepower /eth-server/stats-threshold-policy/class/property/threshold-value* # commit-buffer
firepower /eth-server/stats-threshold-policy/class/property/threshold-value #
```

Cet exemple montre comment accéder au mode organisation, créer une nouvelle politique de seuil de statistiques pour les statistiques des serveurs et des composants de serveur, créer une classe de politiques de seuil pour les statistiques d'environnement du CPU, créer une propriété de température du CPU, spécifier que la température normale du CPU est de 48,5 °C, créer un seuil d'avertissement supérieur à la normale de 50 °C, puis valider la transaction complète :

```
firepower # scope org
firepower /org # create stats-threshold-policy ServStatsPolicy
firepower /org/stats-threshold-policy* # create class cpu-env-stat
firepower /org/stats-threshold-policy/class* # create property temperature
firepower /org/stats-threshold-policy/class/property* # set normal-value 48.5
firepower /org/stats-threshold-policy/class/property* # create threshold-value above-normal
 warning
firepower /org/stats-threshold-policy/class/property/threshold-value* # set escalating 50.0
firepower /org/stats-threshold-policy/class/property/threshold-value* # commit-buffer
firepower /org/stats-threshold-policy/class/property/threshold-value #
```

Commandes associées

Commande	Description
delete class	Supprime une classe de statistiques existante.
enter class	Permet d'accéder à une classe de statistiques. Si la classe n'existe pas, elle est créée.
enter property	Permet d'accéder ou crée une propriété pour une classe de statistiques.

Commande	Description
scope stats-threshold-policy	Accède au mode stats-threshold-policy vous permettant de gérer des classes de statistiques spécifiques.

create connection

Pour ajouter une nouvelle connexion IPSec, utilisez la commande **create connection**. Si une connexion portant le nom spécifié existe déjà, la commande échoue.

Pour ajouter ou modifier une connexion IPSec, utilisez la commande **enter connection**. Si la connexion spécifiée n'existe pas, elle est créée et saisie. Si la connexion existe, elle est saisie.

Vous pouvez également utiliser la forme **scope** de cette commande pour accéder à une connexion existante afin d'affecter ou de modifier des propriétés. En général, il est plus pratique de « cibler » un objet que de le saisir, car le nom de l'objet est habituellement suffisant, tandis que la forme **enter** de la commande requiert souvent la saisie de tous ses paramètres de définition.

Pour supprimer une connexion existante, utilisez la forme **delete** de cette commande.

create connection *name*
enter connection *name*
delete connection *name*
scope connection *name*

Description de la syntaxe

name	Nom de la connexion; peut comporter jusqu'à 16 caractères alphanumériques.

Modes de commande

scope security/scope ipsec/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Lorsque vous créez une connexion IPSec, vous accédez automatiquement au mode security/ipsec/connection accompagné d'un astérisque pour indiquer que la nouvelle connexion n'est pas encore validée. Vous pouvez configurer la connexion avant de la valider.

Une fois la connexion créée, son nom ne peut pas être modifié. Vous devez supprimer la connexion et en créer une nouvelle.

Exemple

Cet exemple montre comment créer et saisir une nouvelle connexion IPSec :

```
firepower # scope security
firepower /security # scope ipsec
firepower /security/ipsec # enter connection ipsec_conn2
firepower /security/ipsec/connection* #
```

Commandes associées

Commande	Description
set adminstate	Définit l'état administratif de la connexion IPSec sur activé ou désactivé.
show connection	Affiche les informations sur la connexion IPSec actuelle.

create destination

Pour ajouter une nouvelle destination Smart Call Home, utilisez la commande **create destination**. Si une destination portant le nom spécifié existe déjà, la commande échoue.

Pour ajouter ou modifier une destination Smart Call Home, utilisez la commande **enter destination**. Si la destination spécifiée n'existe pas, elle est créée et saisie; si la destination existe, elle est saisie.

Vous pouvez également utiliser la forme **scope** de cette commande pour accéder à une destination existante afin d'affecter ou de modifier des propriétés. En général, il est plus pratique de « cibler » un objet que de le saisir, car le nom de l'objet est habituellement suffisant, tandis que la forme **enter** de la commande requiert souvent la saisie de tous ses paramètres de définition.

Pour supprimer une destination existante, utilisez la forme **delete** de cette commande.

create destination *name*
delete destination *name*
enter destination *name*
scope destination *name*

Description de la syntaxe

name	Nom identifiant la destination Smart Call Home.

Modes de commande

scope monitoring/scope callhome/scope profile/

Historique des commandes

Version	Modification
1.4(1)	Commande ajoutée.

Instructions d'utilisation

Lorsque vous créez une nouvelle destination Smart Call Home, vous accédez automatiquement au mode callhome/profil (monitoring/callhome/profile) accompagné d'un astérisque pour indiquer que la nouvelle destination n'est pas encore validée. Vous pouvez définir les paramètres de destination (protocole de transport et adresse de courriel), puis valider les nouvelles informations de destination.

Remarque L'adresse de courriel est la seule adresse de destination autorisée dans un profil callhome.

Après avoir créé une destination Smart Call Home, son nom ne peut pas être modifié. Vous devez supprimer la destination et en créer une nouvelle.

Exemple

Cet exemple montre comment créer, saisir et configurer une destination Smart Call Home :

```
firepower # scope monitoring
firepower /monitoring # scope callhome
firepower /monitoring/callhome # scope profile SLProfile
firepower /monitoring/callhome/profile # enter destination TestDest
firepower /monitoring/callhome/profile/destination* # set address user1@test.com
firepower /monitoring/callhome/profile/destination* # set protocol email
firepower /monitoring/callhome/profile/destination* # commit-buffer
```

```
firepower /monitoring/callhome/profile/destination #
```

Commandes associées

Commande	Description
delete destination	Supprime une destination Smart Call Home existante.
enter destination	Permet d'accéder à une destination Smart Call Home.
set address	Définit une adresse de courriel pour une destination Smart Call Home.
set protocol	Définit le protocole de transport pour une destination Smart Call Home.

create dns

Pour créer un serveur de noms DNS dans FXOS, utilisez la commande **create dns**.

create dns

Description de la syntaxe

create dns	Cette commande permet de créer un serveur de noms DNS dans FXOS.

Modes de commande

scope system/scope services

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande crée le serveur de noms DNS dans FXOS.

Exemple

Cet exemple montre comment créer un serveur de noms DNS :

```
firepower# scope system; scope services
firepower /system /services # create dns 192.0.2.1
firepower /system /services* # commit
```

create hw-crypto

Pour créer une configuration Accélération cryptographique TLS sur une instance de contenant, utilisez la commande **create hw-crypto**. Pour plus de renseignements sur l'Accélération cryptographique TLS, consultez le *Guide de configuration de Centre de gestion*.

create hw-crypto

Modes de commande

connect module

Historique des commandes

Version	Modification
2.7.1	Cette commande a été introduite.

Instructions d'utilisation

Cette commande supprime une configuration d'Accélération cryptographique TLS pour une instance de contenant. Si l'Accélération cryptographique TLS est activée sur l'instance de contenant, la commande la désactive avant de supprimer la configuration.

Exemples

Voici un exemple de création d'une configuration Accélération cryptographique TLS :

```
scope ssa
/ssa # show app-instance

App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
 Deploy Type Turbo Mode Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- --------------- ---------------
 ----------- ---------- ------------ --------------- ------------
ftd        FTD-FDM    1          Enabled     Online           6.5.0.1159      6.5.0.1159
    Native      No                      Not Applicable  None
ftd        ftd2       2          Enabled     Online           6.5.0.1159      6.5.0.1159
    Container   No         Default-Small Not Applicable  None

/ssa # sc slot 2
/ssa/slot # scope app-instance ftd ftd2
/ssa/slot/app-instance # create hw-crypto
/ssa/slot/app-instance* # commit-buffer
```

Commandes associées

Commande	Description
delete hw-crypto	Supprimez une configuration d'Accélération cryptographique TLS pour une instance de contenant.
scope hw-crypto	Activez ou désactivez la configuration d'Accélération cryptographique TLS sur une instance de contenant.
show hw-crypto	Affichez l'état de la configuration d'Accélération cryptographique TLS sur une instance de contenant.

create ip-block

Pour ajouter un nouveau bloc d'adresses IPv4 permettant l'accès aux services, utilisez la commande **create ip-block**. Si un bloc d'adresses avec les propriétés spécifiées existe déjà, la commande échoue.

Pour ajouter ou modifier un bloc d'adresses IPv4, utilisez la commande **enter ip-block**. Si le bloc d'adresses spécifié n'existe pas, il est créé et saisi. Si le bloc d'adresses existe, il est saisi.

Vous pouvez également utiliser la forme **scope** de cette commande pour accéder à un bloc d'adresses existant afin d'affecter ou de modifier des propriétés.

Pour supprimer un bloc d'adresses existant, utilisez la forme **delete** de cette commande.

create ip-block *ip_address prefix_length* {**https** | **snmp** | **ssh**}
delete ip-block *ip_address prefix_length* {**https** | **snmp** | **ssh**}
enter ip-block *ip_address prefix_length* {**https** | **snmp** | **ssh**}
scope ip-block *ip_address prefix_length* {**https** | **snmp** | **ssh**}

Description de la syntaxe

ip_address	Adresse de début du bloc d'adresses IPv4.
prefix_length	Longueur du préfixe; détermine le nombre d'adresses du bloc. La valeur peut être comprise entre 0 et 32.
https | **snmp** | **ssh**	Service (HTTPS, SNMP ou SSH) auquel le bloc d'adresses est affecté.

Modes de commande

scope system/scope services/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour affecter un bloc d'adresses IPv4 afin de fournir un accès à un service spécifié (HTTPS, SNMP ou SSH).

Lorsque vous créez un nouveau bloc d'adresses IP, vous accédez automatiquement au mode ip-block (system/services/ip-block) accompagné d'un astérisque pour indiquer que la nouvelle affectation de bloc n'est pas encore validée.

Sur les versions FXOS 2.3.1 et antérieures, jusqu'à 25 blocs différents peuvent être configurés pour chaque service. Sur les versions FXOS 2.4.1 et ultérieures, jusqu'à 100 blocs différents peuvent être configurés pour chaque service. Une adresse 0.0.0.0 et un préfixe 0 permettent un accès sans restriction à un service. Chaque bloc d'adresses est identifié par son adresse IPv4 de début.

Exemple

L'exemple suivant montre comment créer, saisir et vérifier un bloc d'adresses IPv4 pour fournir un accès SSH :

```
firepower # scope system
firepower /system # scope services
firepower /system/services # enter ip-block 192.168.200.101 32 ssh
firepower /system/services/ip-block* # commit-buffer
```

```
firepower /system/services/ip-block # up
firepower /system/services # show ip-block

Permitted IP Block:
    IP Address      Prefix Length Protocol
    --------------- ------------- --------
    0.0.0.0                     0 https
    0.0.0.0                     0 snmp
    0.0.0.0                     0 ssh
    192.168.200.101            32 ssh
firepower /system/services #
```

Commandes associées

Commande	Description
create ipv6-block	Crée un bloc d'adresses IPv6.
delete ip-block	Supprime un bloc IPv4 existant.

create ipv6-block

Pour ajouter un nouveau bloc d'adresses IPv6 permettant l'accès aux services, utilisez la commande **create ipv6-block**. Si un bloc d'adresses avec les propriétés spécifiées existe déjà, la commande échoue.

Pour ajouter ou modifier un bloc d'adresses IPv6, utilisez la commande **enter ipv6-block**. Si le bloc d'adresses spécifié n'existe pas, il est créé et saisi. Si le bloc d'adresses existe, il est saisi.

Vous pouvez également utiliser la forme **scope** de cette commande pour accéder à un bloc d'adresses existant afin d'affecter ou de modifier des propriétés.

Pour supprimer un bloc d'adresses existant, utilisez la forme **delete** de cette commande.

create ipv6-block *ipv6_address prefix_length* {**https** | **snmp** | **ssh**}
delete ipv6-block *ipv6_address prefix_length* {**https** | **snmp** | **ssh**}
enter ipv6-block *ipv6_address prefix_length* {**https** | **snmp** | **ssh**}
scope ipv6-block *ipv6_address prefix_length* {**https** | **snmp** | **ssh**}

Description de la syntaxe

ipv6_address	Adresse de début du bloc d'adresses IPv6.
prefix_length	Longueur du préfixe; détermine le nombre d'adresses du bloc. La valeur peut être comprise entre 0 et 128.
https | **snmp** | **ssh**	Service (HTTPS, SNMP ou SSH) auquel le bloc d'adresses est affecté.

Modes de commande

scope system/scope services/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour affecter un bloc d'adresses IPv6 afin de fournir un accès à un service spécifié (HTTPS, SNMP ou SSH).

Lorsque vous créez un bloc IPv6, vous accédez automatiquement au mode ipv6-block (system/services/ipv6-block) accompagné d'un astérisque pour indiquer que la nouvelle affectation de bloc n'est pas encore validée.

Sur les versions FXOS 2.3.1 et antérieures, jusqu'à 25 blocs différents peuvent être configurés pour chaque service. Sur les versions FXOS 2.4.1 et ultérieures, jusqu'à 100 blocs différents peuvent être configurés pour chaque service. Une adresse 0:0:0:0:0:0:0:0 et un préfixe 0 permettent un accès sans restriction à un service. Chaque bloc d'adresses est identifié par son adresse IPv6 de début.

Exemple

L'exemple suivant montre comment créer, saisir et vérifier un bloc d'adresses IPv6 pour fournir un accès SSH :

```
firepower # scope system
firepower /system # scope services
firepower /system/services # create ipv6-block 2001:DB8:1::1 64 ssh
firepower /system/services/ipv6-block* # commit-buffer
```

```
firepower /system/services/ipv6-block # up
firepower /system/services # show ipv6-block

Permitted IPv6 Block:
    IPv6 Address Prefix Length Protocol
    ------------ ------------- --------
    ::                       0 https
    ::                       0 snmp
    ::                       0 ssh
    2001:DB8:1::1
                            64 ssh
firepower /system/services #
```

Commandes associées

Commande	Description
create ip-block	Crée un bloc IPv4.
delete ipv6-block	Supprime un bloc IPv6 existant.

create keyring

Pour ajouter un nouveau trousseau de clés RSA, utilisez la commande **create keyring**. Si un trousseau de clés portant le nom spécifié existe déjà, la commande échoue.

Pour modifier un trousseau de clés existant, utilisez la commande **enter keyring**.

Vous pouvez également utiliser la forme **scope** de cette commande pour accéder à un trousseau de clés existant afin d'affecter ou de modifier des propriétés.

Pour supprimer un trousseau de clés existant, utilisez la forme **delete** de cette commande.

create keyring *name*
delete keyring *name*
enter keyring *name*
scope keyring *name*

Description de la syntaxe

name	Nom identifiant le trousseau de clés; peut comporter entre 1 et 16 caractères.

Modes de commande

scope security/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Lorsque vous créez un trousseau de clés, vous accédez automatiquement au mode trousseau de clés (security/keyring) accompagné d'un astérisque pour indiquer que le nouveau trousseau de clés n'est pas encore validé. Vous pouvez créer une demande de certificat de trousseau de clés et définir des paramètres de trousseau de clés tels que le module de clé RSA et le point de confiance de l'autorité de certification, puis valider les nouvelles informations de trousseau de clés.

Exemple

Cet exemple montre comment créer et saisir un nouveau trousseau de clés RSA :

```
firepower # scope security
firepower /security # enter keyring test_keyring
firepower /security/keyring* # set ?
  cert        Keyring certificate
  modulus     RSA key modulus
  regenerate  Regenerate keyring
  trustpoint  Trustpoint CA

firepower /security/keyring* # set
```

Commandes associées

Commande	Description
delete keyring	Supprime un trousseau de clés RSA existant.

create local-user

Pour ajouter un nouveau compte d'utilisateur local, utilisez la commande **create local-user**. Si un compte d'utilisateur local portant le nom spécifié existe déjà, la commande échoue.

Pour ajouter ou modifier un compte d'utilisateur local, utilisez la commande **enter local-user**. Si le compte spécifié n'existe pas, il est créé et saisi; si le compte existe, il est saisi.

Vous pouvez également utiliser la forme **scope** de cette commande pour accéder à un compte d'utilisateur local existant afin d'affecter ou de modifier des propriétés.

Pour supprimer un compte d'utilisateur local existant, utilisez la forme **delete** de cette commande.

create local-user *nom_utilisateur*
delete local-user *nom_utilisateur*
enter local-user *nom_utilisateur*
scope local-user *nom_utilisateur*

Description de la syntaxe

user_name	ID à utiliser lors de la connexion à ce compte d'utilisateur local. Notez les lignes directrices et les restrictions suivantes lors de la saisie d'un nom d'utilisateur :
	• Le nom peut contenir entre 1 et 32 caractères, y compris les éléments suivants :
	  • Deux caractères alphabétiques
	  • Chiffre
	  • _ (trait de soulignement)
	  • - (trait d'union)
	  • . (point)
	• Le nom doit être unique.
	• Le nom doit commencer par un caractère alphabétique. Il ne peut pas commencer par un chiffre ou un caractère spécial, comme un trait de soulignement.
	• Le nom est sensible à la casse.
	• Vous ne pouvez pas créer un nom composé uniquement de chiffres.
	Après avoir créé un compte d'utilisateur, vous ne pouvez pas modifier son nom. Vous devez supprimer le compte d'utilisateur et en créer un nouveau.

Modes de commande

scope security/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous pouvez configurer jusqu'à 48 comptes d'utilisateurs locaux. Chaque compte doit avoir un nom d'utilisateur et un mot de passe uniques.

Lorsque vous créez un compte d'utilisateur, vous accédez automatiquement au mode utilisateur local (/security/local-user) accompagné d'un astérisque pour indiquer que le nouveau compte n'est pas encore validé. Vous pouvez spécifier des informations supplémentaires sur le compte d'utilisateur, comme le mot de passe, le prénom et le nom de l'utilisateur, etc., puis valider les nouvelles informations du compte.

Après avoir créé le compte d'utilisateur, son nom ne peut pas être modifié. Vous devez supprimer le compte d'utilisateur et en créer un nouveau.

Exemple

Cet exemple montre comment accéder au mode sécurité, accéder à un compte d'utilisateur local (créer simultanément le compte, car il n'existe pas), puis affecter le prénom et le nom au compte :

```
firepower # scope security
firepower /security # enter local-user test_user
firepower /security/local-user* # set firstname test
firepower /security/local-user* # set lastname user
firepower /security/local-user* # commit-buffer
firepower /security/local-user #
```

Commandes associées

Commande	Description
delete local-user	Supprime un compte d'utilisateur local existant.
set expiration	Spécifie la date d'expiration du compte d'utilisateur.
set password	Définit le mot de passe du compte d'utilisateur :

create member-port

Pour créer un port membre de canal de port, utilisez la commande **create member-port**. Si un port membre portant l'ID spécifié existe déjà, la commande échoue.

Pour ajouter ou saisir un port membre, utilisez la commande **enter member-port**. Si le port membre spécifié n'existe pas, il est créé et saisi. Si le port membre existe, il est saisi.

Vous pouvez également utiliser la forme **scope** de cette commande pour accéder à un port membre existant afin d'affecter ou de modifier des propriétés.

Pour supprimer un port membre existant, utilisez la forme **delete** de cette commande.

create member-port *interface_id*

Description de la syntaxe

interface_id	Identifiez l'interface à ajouter à ce canal de port en utilisant l'un des formats suivants : • *slot_id port_id* : emplacement du port dans le châssis en termes de numéro de logement et de port. • **Ethernet***slot_id*/*port_id* : étiquette du port Ethernet.

Modes de commande

scope eth-uplink/scope fabric a/port-channel

Historique des commandes

Version	Modification
1.1.1	Commande ajoutée.

Instructions d'utilisation

Vous devez créer ou saisir un canal de port avant de pouvoir utiliser cette commande.

Lorsque vous créez un port membre, vous accédez automatiquement au mode port membre (eth-uplink/fabric/port-channel/member-port) accompagné d'un astérisque pour indiquer que le nouveau port membre n'est pas encore validé.

Exemple

L'exemple suivant montre comment créer un canal de port, l'activer et ajouter des ports membres :

```
firepower # scope eth-uplink
firepower /eth-uplink/fabric # scope fabric a
firepower /eth-uplink/fabric # create port-channel 4
firepower /eth-uplink/fabric/port-channel* # enable
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # commit-buffer
firepower /eth-uplink/fabric/port-channel #
```

Commandes associées

Commande	Description
create port-channel	Crée un EtherChannel (port-channel).

create ntp-server

Pour créer un serveur NTP dans FXOS, utilisez la commande **create ntp-server**.

create ntp-server

Description de la syntaxe

create ntp-server	Cette commande permet de créer un serveur NTP dans FXOS.

Modes de commande

scope system/scope services/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande crée le serveur NTP dans FXOS.

Exemple

L'exemple suivant montre comment créer le serveur NTP :

```
firepower# scope system;scope services

firepower /system/services # create ntp-server 192.0.2.1
firepower /system/services # commit

firepower /system/services/ntp-server # set
  ntp-sha1-key-id     NTP SHA-1 key id   <========== [Optional] Configure NTP authentication
 key ID
  ntp-sha1-key-string  NTP SHA-1 key string  <========== [Optional] Configure NTP
authentication key string

firepower /system/services/ntp-server # commit
```

Commandes associées

Commande	Description
show ntp-server	Cette commande affiche le serveur NTP.

create policy (callhome)

Pour ajouter une nouvelle politique Smart Call Home et Smart Licensing, utilisez la commande **create policy**. Si une politique portant le nom spécifié existe déjà, la commande échoue.

Pour ajouter ou modifier une connexion IPSec, utilisez la commande **enter policy**. Si la politique spécifiée n'existe pas, elle est créée et saisie. Si la politique existe, elle est saisie.

Vous pouvez également utiliser la forme **scope** de cette commande pour accéder à une politique existante afin d'affecter ou de modifier des propriétés.

Pour supprimer une politique existante, utilisez la forme **delete** de cette commande.

create policy *event*
delete policy *event*
enter policy *event*
scope policy *event*

Description de la syntaxe

event	Défaillance ou type d'événement système. Consultez les instruction d'utilisation ci-dessous pour connaître les options d'événements.

Modes de commande

scope monitoring/scope callhome/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Lorsque vous créez une politique Smart Call Home, vous accédez automatiquement au mode callhome/policy (monitoring/callhome/policy) accompagné d'un astérisque pour indiquer que la nouvelle politique n'est pas encore validée. Vous pouvez définir des valeurs de propriété et activer/désactiver les services, puis valider la nouvelle politique.

Une fois la politique Smart Call Home créée, son nom ne peut pas être modifié. Vous devez supprimer la politique et en créer une nouvelle.

Utilisez cette commande pour créer une instance de politique pour un type existant de défaillance ou d'événement système. Les mots clés disponibles pour les types d'événements de politique Call Home sont les suivants :

- adaptor-mismatch
- arp-targets-config-error
- association-failed
- configuration-failure
- connectivity-problem
- election-failure
- equipment-degraded
- equipment-disabled

- equipment-inaccessible
- equipment-inoperable
- equipment-offline
- equipment-problem
- equipment-removed
- fru-problem
- health-led-amber
- health-led-amber-blinking
- identity-unestablishable
- inventory-failed
- license-graceperiod-expired
- limit-reached
- link-down
- management-services-failure
- management-services-unresponsive
- memory-error
- mgmtif-down
- ndisc-targets-config-error
- near-max-limit
- port-failed
- power-problem
- psu-insufficient
- psu-mixed-mode
- thermal-problem
- version-incompatible
- vif-ids-mismatch
- voltage-problem

Exemple

Cet exemple montre comment créer, saisir et activer une instance de politique Call Home pour les événements de perte de liaison :

```
firepower # scope monitoring
firepower /monitoring # scope callhome
```

```
firepower /monitoring/callhome # enter policy link-down
firepower /monitoring/callhome/policy* # set admin-state enabled
firepower /monitoring/callhome/policy* # commit-buffer
firepower /monitoring/callhome/policy #
```

Commandes associées

Commande	Description
delete policy	Supprime une politique Smart Call Home existante.
set admin-state	Active ou désactive l'état d'administration pour une politique Smart Call Home.

create policy (flow-control)

Pour ajouter une nouvelle politique de contrôle de flux nommée, utilisez la commande **create policy**. Si une politique portant le nom spécifié existe déjà, la commande échoue.

Pour ajouter ou modifier une politique de contrôle de flux nommée, utilisez la commande **enter policy**. Si la politique spécifiée n'existe pas, elle est créée et saisie. Si la politique existe, elle est saisie.

Vous pouvez également utiliser la forme **scope** de cette commande pour accéder à une politique existante afin d'affecter ou de modifier des propriétés.

Pour supprimer une politique existante, utilisez la forme **delete** de cette commande.

create policy *name*
delete policy *name*
enter policy *name*
scope policy *name*

Description de la syntaxe

name	Nom permettant d'identifier la politique de contrôle de flux. Ce nom peut comporter de 1 à 16 caractères.

Modes de commande

scope eth-uplink/scope flow-control/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Les politiques de contrôle de flux déterminent si les ports Ethernet de liaison ascendante d'un domaine d'appareil envoient et reçoivent des trames de pause IEEE 802.3x lorsque le tampon de réception d'un port atteint sa pleine capacité. Ces trames de pause demandent que le port de transmission arrête d'envoyer des données pendant quelques millisecondes jusqu'à ce que le tampon soit libéré. Pour que le contrôle de flux fonctionne entre les appareils, vous devez activer les paramètres de contrôle de flux d'envoi et de réception correspondants pour les deux appareils.

La politique par `défaut` désactive le contrôle d'envoi et de réception et définit la priorité pour la négociation automatique.

Lorsque vous créez une politique de contrôle de flux, vous accédez automatiquement au mode contrôle de flux/politique (eth-uplink/flow-control/policy) accompagné d'un astérisque pour indiquer que la nouvelle politique n'est pas encore validée. Vous pouvez définir des valeurs de propriété, puis valider la nouvelle politique.

Une fois la politique de contrôle de flux créée, son nom ne peut pas être modifié. Vous devez supprimer la politique et en créer une nouvelle.

Exemple

Cet exemple montre comment créer et saisir une politique nommée pour le contrôle de flux :

```
firepower # scope eth-uplink
firepower /eth-uplink # scope flow-control
firepower /eth-uplink/flow-control # enter policy FCpolicy1
```

```
firepower /eth-uplink/flow-control/policy* # commit-buffer
firepower /eth-uplink/flow-control/policy #
```

Commandes associées

Commande	Description
delete policy	Supprime une politique de contrôle de flux existante.
set	En mode contrôle de flux/politique, définit les propriétés de la politique de contrôle de flux.
show policy	Affiche les valeurs de propriété d'une politique de contrôle de flux.

create port-channel

Pour créer un EtherChannel (également appelé canal de port), utilisez la commande **create port-channel**. Si un canal de port portant l'ID spécifié existe déjà, la commande échoue.

Pour ajouter ou saisir un canal de port, utilisez la commande **enter port-channel**. Si le canal de port spécifié n'existe pas, il est créé et saisi. Si le canal de port existe, il est saisi.

Vous pouvez également utiliser la forme **scope** de cette commande pour accéder à un canal de port existant afin d'affecter ou de modifier des propriétés.

Pour supprimer un canal de port existant, utilisez la forme **delete** de cette commande.

create port-channel*ID*

Description de la syntaxe

ID	Attribuez un numéro d'ID à ce canal de port.

Modes de commande

scope eth-uplink/scope fabric a/

Historique des commandes

Version	Modification
1.1.1	Commande ajoutée.

Instructions d'utilisation

Lorsque vous créez un canal de port, vous accédez automatiquement au mode canal de port (eth-uplink/fabric/port-channel) accompagné d'un astérisque pour indiquer que le nouveau canal de port n'est pas encore validé. Vous pouvez définir les paramètres de canal de port, puis valider le nouveau canal de port.

Après avoir créé un canal de port, activez-le et ajoutez des ports membres.

Lorsque le châssis Firepower 4100/9300 crée un EtherChannel, celui-ci reste dans un état **Suspendu** jusqu'à ce que vous l'affectiez à un périphérique logique, même si la liaison physique est opérationnelle. L'EtherChannel sortira de l'état **Suspendu** dans les situations suivantes :

- L'EtherChannel est ajouté en tant que port de données ou de gestion pour un périphérique logique autonome.
- L'EtherChannel est ajouté en tant que port de gestion ou CCL pour un périphérique logique qui fait partie d'une grappe.
- L'EtherChannel est ajouté en tant que port de données pour un périphérique logique qui fait partie d'une grappe et au moins un module de sécurité a rejoint la grappe.

Notez que l'EtherChannel ne s'affiche pas tant que vous ne l'avez pas affecté à un périphérique logique. Si l'EtherChannel est retiré du périphérique logique ou si le périphérique logique est supprimé, l'EtherChannel repasse à l'état **Suspendu**.

Remarque Le châssis Firepower 4100/9300 prend uniquement en charge les canaux EtherChannel en mode protocole LACP (Link Aggregation Control Protocol) actif. Nous vous suggérons de régler les ports de connexion du commutateur sur le mode Active (Actif) pour une meilleure compatibilité.

Exemple

L'exemple suivant montre comment créer un canal de port, l'activer et ajouter des ports membres :

```
firepower # scope eth-uplink
firepower /eth-uplink/fabric # scope fabric a
firepower /eth-uplink/fabric # create port-channel 4
firepower /eth-uplink/fabric/port-channel* # enable
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # commit-buffer
firepower /eth-uplink/fabric/port-channel #
```

Commandes associées

Commande	Description
create member-port	Ajoute un port membre à un canal de port.
set (port-channel)	Définit ou modifie les paramètres d'un canal de port existant.

create pre-login-banner

Pour créer une bannière qui s'affiche avant l'écran de connexion, utilisez la commande **create pre-login-banner**. Si une bannière de préconnexion existe déjà, la commande échoue.

Pour ajouter ou modifier la bannière de préconnexion, utilisez la commande **enter pre-login-banner**. Si aucune bannière n'existe, elle est créée et saisie; si une bannière existe, elle est saisie.

Vous pouvez également utiliser la forme **scope** de cette commande pour accéder à une bannière de préconnexion existante afin de définir ou d'effacer le message.

Pour supprimer une bannière existante, utilisez la forme **delete** de cette commande.

create pre-login-banner

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope security/scope banner/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Lorsque vous créez une bannière de préconnexion, elle est vide et vous accédez automatiquement au mode bannière de préconnexion (security/banner/pre-login-banner) accompagné d'un astérisque pour indiquer que la bannière n'est pas encore spécifiée et validée.

Utilisez la commande **set message** pour saisir le texte de la bannière de préconnexion. Vous devez saisir `ENDOFBUF` (en majuscules) pour terminer le message de la bannière.

Si une bannière de préconnexion existe déjà lorsque vous saisissez cette commande, la commande échoue avec un message d'erreur indiquant que `l'objet géré existe déjà`.

Exemple

Cet exemple montre comment créer et spécifier une bannière de préconnexion, puis la valider et l'afficher :

```
firepower # scope security
firepower /security # scope banner
firepower /security/banner # create pre-login-banner
firepower /security/banner/pre-login-banner* # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Firepower-9300-2
>Western Data Center
>ENDOFBUF
firepower /security/banner/pre-login-banner* # commit
firepower /security/banner/pre-login-banner # show

Pre login banner:
    Message
    -------
    Firepower-9300-2
```

```
Western Data Center

firepower /security/banner/pre-login-banner #
```

Commandes associées

Commande	Description
clear message	Supprime le texte d'une bannière de préconnexion existante; l'objet de bannière en lui-même n'est pas supprimé.
set message	Spécifie les lignes de texte à afficher comme bannière de préconnexion.

create profile

Pour ajouter un nouveau profil de destination Smart Call Home et Smart Licensing, utilisez la commande **create profile**. Si un profil portant le nom spécifié existe déjà, la commande échoue.

Pour ajouter ou modifier un profil de destination, utilisez la commande **enter profile**. Si le profil spécifié n'existe pas, il est créé et saisi. Si le profil existe, il est saisi.

Vous pouvez également utiliser la forme **scope** de cette commande pour accéder à un profil existant afin d'affecter ou de modifier des propriétés. Si le profil n'existe pas, la commande échoue.

Pour supprimer un profil existant, utilisez la forme **delete** de cette commande.

create profile *name*
delete profile *name*
enter profile *name*
scope profile *name*

Description de la syntaxe

name	Nom identifiant le profil de destination.

Modes de commande

scope monitoring/scope callhome/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Lorsque vous créez un profil Smart Call Home, vous accédez automatiquement au mode callhome/profile (monitoring/callhome/profile) accompagné d'un astérisque pour indiquer que le nouveau profil n'est pas encore validé. Vous pouvez définir le profil, puis valider les nouvelles informations de profil.

Une fois le profil de destination Smart Call Home créé, son nom ne peut pas être modifié. Vous devez supprimer le profil et en créer un nouveau.

Exemple

Cet exemple montre comment créer et saisir un profil de destination Smart Call Home :

```
firepower # scope monitoring
firepower /monitoring # scope callhome
firepower /monitoring/callhome # enter profile TestProfile
firepower /monitoring/callhome/profile* # commit-buffer
firepower /monitoring/callhome/profile #
```

Commandes associées

Commande	Description
delete profile	Supprime un profil de destination Smart Call Home existant.
set	En mode monitoring/callhome, définit les propriétés du profil.

Commande	Description
show profile	Répertorie les profils de licences Smart Call Home et Smart Licensing actuellement définis; disponible en mode monitoring/callhome.

create property

Pour ajouter une nouvelle propriété à une classe de politiques de seuil de statistiques réseau, utilisez la commande **create property**. Si une propriété portant le nom spécifié existe déjà, la commande échoue.

Pour ajouter ou modifier une propriété de seuil de statistiques, utilisez la commande **enter property**. Si la propriété spécifiée n'existe pas, elle est créée et saisie; si la propriété existe, elle est saisie.

Vous pouvez également utiliser la forme **scope** de cette commande pour accéder à une propriété existante afin d'affecter ou de modifier des paramètres. En général, il est plus pratique de « cibler » un objet que de le saisir, car le nom de l'objet est habituellement suffisant, tandis que la forme **enter** de la commande requiert souvent la saisie de tous ses paramètres de définition.

Pour supprimer une propriété existante, utilisez la forme **delete** de cette commande.

create property *property-name*
delete property *property-name*
enter property *property-name*
scope property *property-name*

Description de la syntaxe

property-name	Spécifiez la propriété de statistiques souhaitée. Les propriétés disponibles dépendent du mode actuel et de la classe de statistiques définie. Par exemple, pour la classe `chassis-stats` en mode `eth-server`, les options `input-power` et `output-power` sont disponibles. Dans la classe `ether-rx-stats`, en mode `eth-uplink`, des propriétés telles que `broadcast-packets-delta` et `total-bytes-delta` sont disponibles. Utilisez la commande **create property ?** pour afficher la liste des propriétés disponibles pour la classe de statistiques actuelle.

Modes de commande

scope eth-server/scope stats-threshold-policy/scope class/

scope eth-uplink/scope stats-threshold-policy/scope class/

scope org/scope stats-threshold-policy/scope class/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez les classes pour appliquer des seuils à des ensembles de statistiques spécifiques. Utilisez les propriétés pour définir des valeurs et des seuils de statistiques particuliers pour une classe de politique. Par exemple, vous pouvez définir un seuil sur un port qui déclenche une défaillance si le nombre moyen de paquets abandonnés dépasse une certaine valeur. Pour cette classe, vous devez créer des propriétés de seuil pour la classe de statistiques d'erreur Ethernet.

Vous pouvez configurer plusieurs propriétés pour une classe de politiques.

Remarque Il existe une politique de seuil de statistiques par défaut pour les ports de serveur Ethernet et les ports de liaison ascendante Ethernet. Vous ne pouvez pas créer de politiques de collecte de statistiques supplémentaires, ni supprimer les politiques par défaut existantes pour ces composants. Vous pouvez uniquement modifier les politiques par défaut. Cependant, vous pouvez créer et supprimer des politiques de seuil de statistiques en mode organisation (`scope org/`).

Exemple

Cet exemple montre comment accéder à la politique de seuil des statistiques de liaison ascendante Ethernet par défaut, créer une classe de statistiques d'erreurs, créer une propriété de compteur d'erreurs de contrôle de redondance cyclique (CRC), spécifier que le nombre normal d'erreurs CRC par intervalle d'interrogation est de 1 000, créer un seuil d'avertissement au-dessus de la normale de 1 250, puis valider la classe :

```
firepower # scope eth-uplink
firepower /eth-uplink # scope stats-threshold-policy default
firepower /eth-uplink/stats-threshold-policy # create class ether-error-stats
firepower /eth-uplink/stats-threshold-policy/class* # create property crc-delta
firepower /eth-uplink/stats-threshold-policy/class/property* # set normal-value 1000
firepower /eth-uplink/stats-threshold-policy/class/property* # create threshold-value
above-normal warning
firepower /eth-uplink/stats-threshold-policy/class/property/threshold-value* # set escalating
 1250
firepower /eth-uplink/stats-threshold-policy/class/property/threshold-value* # commit-buffer
firepower /eth-uplink/stats-threshold-policy/class/property/threshold-value #
```

Commandes associées

Commande	Description
delete property	Supprime une propriété existante.
enter property	Permet d'accéder à une propriété de classe. Si la propriété n'existe pas, elle est créée.
enter property	Permet d'accéder ou crée une propriété pour une classe de statistiques.
scope property	Permet d'accéder au mode propriété, dans lequel vous gérez les propriétés d'une classe de statistiques.

create resource-profile

Pour ajouter un profil de ressource à utiliser avec les instances de contenant, utilisez la commande **create resource-profile**.

create resource-profile *name*

Description de la syntaxe

name	Définit le nom du profil, d'une longueur comprise entre 1 et 64 caractères. Notez que vous ne pourrez plus modifier le nom de ce profil après l'avoir ajouté.

Modes de commande

scope ssa/

Historique des commandes

Version	Modification
2.4(1)	Commande ajoutée.

Instructions d'utilisation

Pour spécifier l'utilisation des ressources par instance de conteneur, créez un ou plusieurs profils de ressource. Lorsque vous déployez l'instance d'application ou de périphérique logique, vous spécifiez le profil de ressource que vous souhaitez utiliser. Le profil de ressource définit le nombre de cœurs de CPU; la mémoire RAM est allouée de façon dynamique en fonction du nombre de cœurs et l'espace disque est défini sur 40 Go par instance.

- Le nombre minimum de cœurs est de 6.
- Compte tenu de l'architecture interne, vous ne pouvez pas spécifier 8 cœurs.
- Vous pouvez affecter un nombre pair de cœurs (6, 10, 12, 14, etc.) jusqu'au nombre maximal.
- Le nombre maximal de cœurs disponibles dépend du module de sécurité ou du modèle de châssis.

Le châssis comprend un profil de ressource par défaut appelé « Default-Small », qui comprend le nombre minimal de cœurs. Vous pouvez modifier la définition de ce profil et même le supprimer s'il n'est pas utilisé. Notez que ce profil est créé lors du rechargement du châssis et qu'aucun autre profil n'existe sur le système.

Vous ne pouvez pas modifier les paramètres du profil de ressource s'il est actuellement utilisé. Vous devez désactiver toutes les instances qui l'utilisent, puis modifier le profil de ressource et enfin réactiver l'instance. Si vous redimensionnez des instances dans une paire à haute disponibilité établie, vous devez définir une taille identique pour tous les membres dès que possible.

Si vous modifiez les paramètres du profil de ressource après avoir ajouté l'instance Défense contre les menaces au centre de gestion, mettez à jour l'inventaire de chaque unité dans la boîte de dialogue **Appareils** > **Gestion des appareils** > **Appareil** > **Système** > **Inventaire**.

Exemple

Dans l'exemple suivant, trois profils de ressource sont ajoutés.

```
firepower# scope ssa
firepower /ssa # enter resource-profile basic
firepower /ssa/resource-profile* # set description "lowest level"
```

```
firepower /ssa/resource-profile* # set cpu-core-count 6
firepower /ssa/resource-profile* # exit
firepower /ssa # enter resource-profile standard
firepower /ssa/resource-profile* # set description "middle level"
firepower /ssa/resource-profile* # set cpu-core-count 10
firepower /ssa/resource-profile* # exit
firepower /ssa # enter resource-profile advanced
firepower /ssa/resource-profile* # set description "highest level"
firepower /ssa/resource-profile* # set cpu-core-count 12
firepower /ssa/resource-profile* # commit-buffer
firepower /ssa/resource-profile #
```

Commandes associées

Commande	Description
set cpu-count	Définit le nombre de CPU pour le profil de ressource.
set resource-profile-name	Affecte le profil de ressource à l'instance d'application.
show monitor detail	Affiche l'utilisation des ressources pour le module de sécurité ou le logement de moteur.
show resource detail	Affiche l'allocation de ressources pour l'instance d'application.
show resource-profile user-defined	Affiche les affectations de profils de ressource.

create server (scope ldap)

Pour créer un objet de serveur LDAP (Lightweight Directory Access Protocol), utilisez la commande **create server** en mode security/ldap. Si un serveur portant le nom spécifié existe déjà, la commande échoue.

Pour ajouter ou modifier un serveur LDAP, utilisez la commande **enter server** en mode security/ldap. Si le serveur spécifié n'existe pas, il est créé et saisi; si le serveur existe, il est saisi.

Vous pouvez également utiliser la forme **scope** de cette commande pour accéder à un serveur existant afin d'affecter ou de modifier des propriétés.

Pour supprimer un serveur existant, utilisez la forme **delete** de cette commande.

create server *ID*

Description de la syntaxe

ID	Fournissez l'ID du serveur, en utilisant son nom de domaine, son nom de domaine complet (FQDN) ou son adresse IP (adresse IPv4 ou IPv6).

Modes de commande

scope security/scope ldap/

Historique des commandes

Version	Modification
1.1.1	Commande ajoutée.

Instructions d'utilisation

Si vous utilisez un nom de domaine ou un nom de domaine complet (FQDN) pour spécifier l'*id* du serveur, un serveur DNS doit également être configuré.

Si SSL est activé, l'*id* du serveur doit correspondre exactement à un nom commun (CN) dans le certificat de sécurité du serveur LDAP.

Lorsque vous créez un serveur LDAP, vous accédez automatiquement au mode security/ldap/server accompagné d'un astérisque pour indiquer que le nouveau serveur n'est pas encore validé. Vous pouvez configurer le serveur avant de le valider.

Remarque Le FXOS prend en charge un maximum de 16 fournisseurs LDAP.

Exemple

L'exemple suivant crée un serveur LDAP et valide la transaction :

```
firepower # scope security
firepower # scope ldap
firepower /security/ldap # create server 192.168.100.112
Warning: LDAP server name has to be DNS name in Secure LDAP connection. It has to match the
 LDAP server certificate SAN field.
firepower /security/ldap/server* # commit-buffer
firepower /security/ldap/server #
```

Commandes associées

Commande	Description
create ldap-group-rule	Crée des paramètres de règle de groupe de fournisseurs LDAP.
set	En mode security/ldap/server, définit divers paramètres liés au serveur LDAP, notamment l'activation ou la désactivation du protocole SSL.

create snmp-trap

Pour créer un hôte de déroutement SNMP (Simple Network Management Protocol), utilisez la commande **create snmp-trap**. Si un déroutement portant le nom spécifié existe déjà, la commande échoue.

Pour ajouter ou modifier un déroutement SNMP, utilisez la commande **enter snmp-trap**. Si le déroutement spécifié n'existe pas, il est créé et saisi. Si le déroutement existe, il est saisi.

Vous pouvez également utiliser la forme **scope** de cette commande pour accéder à un déroutement existant afin d'affecter ou de modifier des propriétés. En général, il est plus pratique de « cibler » un objet que de le saisir, car le nom de l'objet est habituellement suffisant, tandis que la forme **enter** de la commande requiert souvent la saisie de tous ses paramètres de définition.

Pour supprimer un déroutement existant, utilisez la forme **delete** de cette commande.

create snmp-trap *destination*

Description de la syntaxe

destination	Spécifiez le serveur de destination du déroutement, en utilisant son nom d'hôte ou son adresse IP (il peut s'agir d'une adresse IPv4 ou IPv6).

Modes de commande

scope monitoring/

Historique des commandes

Version	Modification
1.1.1	Commande ajoutée.

Instructions d'utilisation

Vous devez activer le protocole SNMP (**enable snmp**) et créer une communauté SNMP (**set snmp community**) avant de créer un déroutement SNMP.

Lorsque vous créez un déroutement SNMP, vous accédez automatiquement au mode monitoring/snmp-trap accompagné d'un astérisque pour indiquer que le nouveau déroutement n'est pas encore validé.

Remarque Vous pouvez créer jusqu'à huit déroutements SNMP.

Exemple

L'exemple suivant crée un déroutement SNMP et valide la transaction :

```
firepower # scope monitoring
firepower /monitoring/ # enable snmp
firepower /monitoring/ # create snmp-trap 192.168.100.112
firepower /monitoring/snmp-trap* # commit-buffer
firepower /monitoring/snmp-trap #
```

Commandes associées

Commande	Description
enable snmp	Active le protocole SNMP

Commande	Description
set snmp	Définit les paramètres de configuration SNMP : communauté, personne-ressource système responsable de SNMP et emplacement de l'hôte.

create snmp-user

Pour créer un utilisateur SNMPv3, utilisez la commande **create snmp-user**. Si un utilisateur portant le nom spécifié existe déjà, la commande échoue.

Pour ajouter ou modifier un utilisateur SNMP, utilisez la commande **enter snmp-user**. Si l'utilisateur spécifié n'existe pas, il est créé et saisi. Si l'utilisateur existe, il est saisi.

Vous pouvez également utiliser la forme **scope** de cette commande pour accéder à un utilisateur existant afin d'affecter ou de modifier des propriétés. En général, il est plus pratique de « cibler » un objet que de le saisir, car le nom de l'objet est habituellement suffisant, tandis que la forme **enter** de la commande requiert souvent la saisie de tous ses paramètres de définition.

Pour supprimer un utilisateur existant, utilisez la forme **delete** de cette commande.

create snmp-user *nom_utilisateur*

Description de la syntaxe

user_name	Spécifiez le nom d'utilisateur SNMPv3; peut comporter un maximum de 32 caractères alphanumériques, et un trait de soulignement (_), un point (.), un signe @ et un tiret (-).

Modes de commande

scope monitoring/

Historique des commandes

Version	Modification
1.1.1	Commande ajoutée.

Instructions d'utilisation

Vous devez activer le protocole SNMP (**enable snmp**) et créer une communauté SNMP (**set snmp community**) avant de créer un utilisateur SNMP.

Lorsque vous créez un utilisateur SNMP, vous devez créer un mot de passe pour cet utilisateur. Ce mot de passe doit comporter au moins huit caractères ; il ne s'affiche pas lors de la saisie.

Lorsque vous créez un utilisateur SNMP, vous accédez automatiquement au mode monitoring/snmp-user accompagné d'un astérisque pour indiquer que le nouvel utilisateur n'est pas encore validé.

Exemple

L'exemple suivant montre comment créer un utilisateur SNMPv3 :

```
firepower # scope monitoring
firepower /monitoring/ # enable snmp
firepower /monitoring/ # create snmp-user test1
Password:
firepower /monitoring/snmp-user* # commit-buffer
firepower /monitoring/snmp-user #
```

Commandes associées

Commande	Description
enable snmp	Active le protocole SNMP.

Commande	Description
set snmp	Définit les paramètres de configuration SNMP : communauté, personne-ressource système responsable de SNMP et emplacement de l'hôte.

create ssh-server

Pour créer une clé d'hôte SSH, utilisez la commande **create ssh-server** avec le mot clé **host-key**.

Pour supprimer la clé d'hôte SSH existante, utilisez la commande **delete ssh-server** avec le mot clé **host-key**.

create ssh-server host-key
create ssh-server host-key

Description de la syntaxe

Cette commande ne contient aucun argument supplémentaire.

Modes de commande

scope system/scope services/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez la forme **create** de cette commande pour générer une nouvelle clé d'hôte SSH.

Utilisez la forme **delete** de cette commande pour supprimer une clé d'hôte SSH existante avant d'en générer une nouvelle.

Exemples

Cet exemple montre comment générer une nouvelle clé d'hôte SSH :

```
firepower # scope system
firepower /system # scope services
firepower /system/services # create ssh-server host-key
firepower /system/services* # commit-buffer
firepower /system/services #
```

Cet exemple montre comment supprimer la clé d'hôte SSH existante et confirmer sa suppression :

```
firepower # scope system
firepower /system # scope services
firepower /system/services # delete ssh-server host-key
firepower /system/services* # commit-buffer
firepower /system/services # show ssh-server host-key
Host Key Size: 2048
Deleted: Yes
firepower /system/services #
```

Commandes associées

Commande	Description
set ssh-server	Définit la taille de la clé d'hôte du serveur SSH.
show ssh-server	Affiche les propriétés du serveur SSH.

create stats-threshold-policy

Pour créer une politique de seuil de statistiques en mode organisation, utilisez la commande **create stats-threshold-policy**. Si une politique portant le nom spécifié existe déjà, la commande échoue.

Pour ajouter ou modifier une politique de seuil en mode organisation, utilisez la commande **enter stats-threshold-policy**. Si la politique spécifiée n'existe pas, elle est créée et saisie. Si la politique existe, elle est saisie.

Vous pouvez également utiliser la forme **scope** de cette commande pour accéder à une politique de seuil de statistiques existante en mode organisation afin d'affecter ou de modifier des propriétés. En général, il est plus pratique de « cibler » un objet que de le saisir, car le nom de l'objet est habituellement suffisant, tandis que la forme **enter** de la commande requiert souvent la saisie de tous ses paramètres de définition.

Pour supprimer une politique existante, utilisez la forme **delete** de cette commande.

create stats-threshold-policy *policy-name*

Description de la syntaxe

policy-name	Nom de la nouvelle politique de seuil de statistiques. **Remarque** Vous ne pouvez pas créer ni supprimer la politique de seuil de statistiques par défaut pour les ports de serveur Ethernet (`scope eth-server/`) ou les ports de liaison ascendante Ethernet (`scope eth-uplink/`).

Modes de commande

scope org/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Une politique de seuil de statistiques surveille les statistiques relatives à certains aspects du système et génère un événement si un seuil spécifié est dépassé. Vous pouvez définir des seuils minimaux et maximaux. Par exemple, vous pouvez configurer la politique pour déclencher une alarme si la température du processeur dépasse une certaine valeur ou si un serveur est surutilisé ou sous-utilisé.

Vous pouvez créer, saisir et supprimer des politiques de seuil de statistiques supplémentaires en mode organisation uniquement. Vous ne pouvez pas créer de politiques de seuil de statistiques supplémentaires pour des ports de serveur ou de liaison ascendante Ethernet, ni supprimer les politiques par défaut existantes pour ces composants. Vous pouvez uniquement modifier les politiques par défaut.

Remarque Utilisez la commande **set collection-interval** pour définir la fréquence de collecte des statistiques et la commande **set reporting-interval** pour définir la fréquence à laquelle ces statistiques sont présentées. Ces intervalles définissent une politique de collecte des statistiques.

Exemple

Cet exemple montre comment accéder au mode organisation, créer une nouvelle politique de seuil de statistiques pour les statistiques des serveurs et des composants de serveur, créer une classe de politiques de seuil pour les statistiques d'environnement du CPU, créer une propriété de température du CPU, spécifier que la température normale du CPU est de 48,5 °C, créer un seuil d'avertissement supérieur à la normale de 50 °C, puis valider la transaction complète :

```
firepower # scope org
firepower /org # create stats-threshold-policy ServStatsPolicy
firepower /org/stats-threshold-policy* # create class cpu-env-stat
firepower /org/stats-threshold-policy/class* # create property temperature
firepower /org/stats-threshold-policy/class/property* # set normal-value 48.5
firepower /org/stats-threshold-policy/class/property* # create threshold-value above-normal
 warning
firepower /org/stats-threshold-policy/class/property/threshold-value* # set escalating 50.0
firepower /org/stats-threshold-policy/class/property/threshold-value* # commit-buffer
firepower /org/stats-threshold-policy/class/property/threshold-value #
```

Commandes associées

Commande	Description
create class	Crée une classe de statistiques.
create property	Crée une propriété pour une classe de statistiques.
create threshold-value	Spécifie un seuil supérieur ou inférieur à la normale pour une propriété de classe.
scope org	Permet d'accéder au mode organisation.

create subinterface

Pour ajouter une sous-interface à une interface physique ou EtherChannel à utiliser avec des instances de contenant, utilisez la commande **create subinterface**.

create subinterface *ID*

Description de la syntaxe

ID	Définit l'ID entre 1 et 4294967295. Cet ID sera ajouté à l'ID de l'interface parente sous le nom *interface_id.subinterface_id*. Par exemple, si vous ajoutez une sous-interface à Ethernet1/1 avec l'ID 100, l'ID de la sous-interface sera : Ethernet1/1.100. Cet ID est différent de l'ID VLAN, bien que vous puissiez définir ces ID pour des raisons de commodité.

Modes de commande

scope eth-uplink/scope fabric a/scope interface/

scope eth-uplink/scope fabric a/create port-channel/

Historique des commandes

Version	Modification
2.4(1)	Commande ajoutée.

Instructions d'utilisation

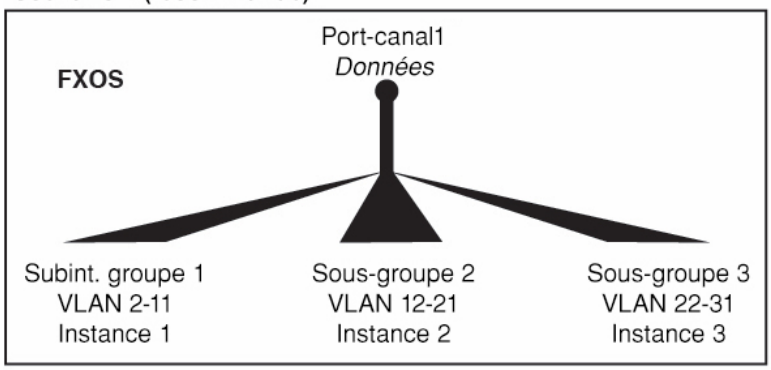
Vous pouvez ajouter jusqu'à 500 sous-interfaces à votre châssis.

Pour les instances autonomes, les ous-interfaces sont prises en charge sur les interfaces de type données ou partage de données uniquement. Pour la mise en grappe multi-instances, vous ne pouvez ajouter de sous-interfaces qu'à l'interface de type grappe; les sous-interfaces des interfaces de données ne sont pas prises en charge.

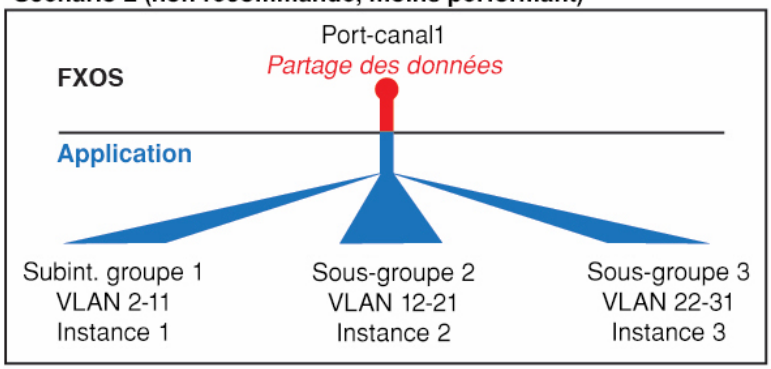
Les ID de VLAN par interface doivent être uniques et, dans une instance de conteneur, les ID de VLAN doivent être uniques pour toutes les interfaces attribuées. Vous pouvez réutiliser les ID de VLAN sur des interfaces *distinctes*, à condition qu'ils soient affectés à différentes instances de conteneur. Cependant, chaque sous-interface compte toujours dans la limite, même si elle utilise le même ID.

Pour tous les instances natives, vous pouvez créer des sous-interfaces VLAN dans l'application uniquement. Pour les instances de contenant, vous pouvez également créer des sous-interfaces VLAN à au sein de l'application sur les interfaces qui n'ont pas de sous-interfaces VLAN FXOS définies. Ces sous-interfaces ne sont pas soumises à la limite FXOS. Le choix du système d'exploitation pour la création des sous-interfaces dépend de votre déploiement réseau et de vos préférences personnelles. Par exemple, pour partager une sous-interface, vous devez créer la sous-interface dans FXOS. Un autre scénario qui favorise les sous-interfaces FXOS consiste à allouer des groupes de sous-interfaces distincts sur une seule interface à plusieurs instances. Par exemple, vous souhaitez utiliser le canal de port 1 avec le VLAN 2 à 11 sur l'instance A, le VLAN 12 à 21 sur l'instance B et le VLAN 22 à 31 sur l'instance C. Si vous créez ces sous-interfaces dans l'application, vous devrez partager l'interface parente dans FXOS, ce qui n'est peut-être pas souhaitable. Consultez l'illustration suivante qui présente les trois façons de réaliser ce scénario :

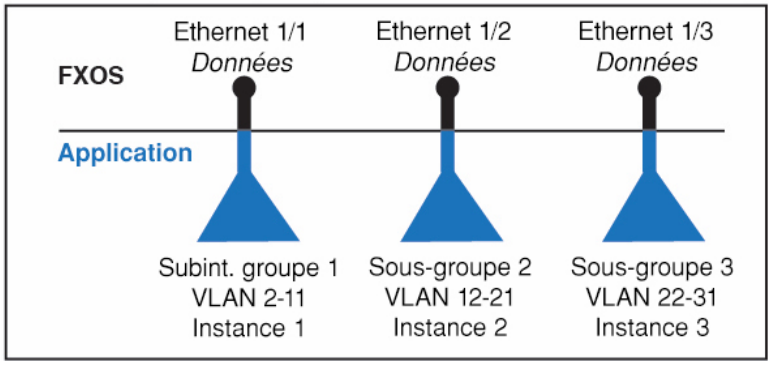
Scénario 1 (recommandé)



Scénario 2 (non recommandé, moins performant)



Scénario 3 (conseillé, mais sans redondance EtherChannel)



Vous ne pouvez pas ajouter une sous-interface à une interface physique qui est actuellement allouée à une unité logique. Si d'autres sous-interfaces du parent sont allouées, vous pouvez ajouter une nouvelle sous-interface tant que l'interface parente elle-même n'est pas allouée.

Exemple

Dans l'exemple suivant, trois sous-interfaces Ethernet 1/1 sont créées et sont définies comme interfaces de partage de données.

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # scope interface Ethernet1/1
firepower /eth-uplink/fabric/interface # create subinterface 10
```

```
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 10
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # exit
firepower /eth-uplink/fabric/interface # create subinterface 11
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 11
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # exit
firepower /eth-uplink/fabric/interface # create subinterface 12
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 12
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # commit-buffer
firepower /eth-uplink/fabric/interface/subinterface #
```

Commandes associées

Commande	Description
create port-channel	Crée un EtherChannel (canal de port).
scope interface	Permet d'accéder à l'objet d'interface physique.
set port-type	Définit le type d'interface.
set vlan	Définit l'ID de VLAN d'une sous-interface.

create theshold-value

Pour ajouter un seuil supérieur ou inférieur à la normale pour une propriété de classe, utilisez la commande **create theshold-value**. Si un seuil portant le nom spécifié existe déjà, la commande échoue.

Pour ajouter ou modifier une valeur de seuil, utilisez la commande **enter theshold-value**. Si la valeur de seuil spécifiée n'existe pas, elle est créée et saisie. Si le seuil existe, il est saisi.

Vous pouvez également utiliser la forme **scope** de cette commande pour accéder à une valeur de seuil existante afin d'affecter ou de modifier des paramètres. En général, il est plus pratique de « cibler » un objet que de le saisir, car le nom de l'objet est habituellement suffisant, tandis que la forme **enter** de la commande requiert souvent la saisie de tous ses paramètres de définition.

Pour supprimer une valeur de seuil existante, utilisez la forme **delete** de cette commande.

create theshold-value { **above-normal** | **below-normal** *event_type* }

Description de la syntaxe

above-normal | **below-normal**	Spécifiez le type de seuil : au-dessus de la normale ou en dessous de la normale. Cela détermine si l'élément *event_type* spécifié est consigné lorsque la valeur surveillée (définie séparément) augmente ou diminue suffisamment par rapport à la valeur normale associée (également définie séparément).
event_type	Spécifiez le type d'événement consigné : • `cleared` • `condition` • `critique` • `Information` • `Majeur` • `mineur` • `avertissement`

Modes de commande

scope eth-server/scope stats-threshold-policy/scope class/scope property/

scope eth-uplink/scope stats-threshold-policy/scope class/scope property/

scope org/scope stats-threshold-policy/scope class/scope property/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez les classes pour appliquer des seuils à des ensembles de statistiques spécifiques. Utilisez les propriétés pour définir des valeurs particulières, y compris les valeurs normales et les valeurs de seuil, pour une classe de politiques. Par exemple, vous pouvez définir un seuil sur un port qui déclenche une défaillance si le nombre moyen de paquets abandonnés dépasse une certaine valeur. Pour cette classe, vous créez des propriétés de seuil pour la classe de statistiques d'erreur Ethernet.

Vous pouvez configurer plusieurs propriétés pour une classe de politiques et créer plusieurs valeurs de seuil pour une propriété.

Remarque Il existe une politique de seuil de statistiques par défaut pour les ports de serveur Ethernet et les ports de liaison ascendante Ethernet. Vous ne pouvez pas créer de politiques de collecte de statistiques supplémentaires, ni supprimer les politiques par défaut existantes pour ces composants. Vous pouvez uniquement modifier les politiques par défaut. Cependant, vous pouvez créer et supprimer des politiques de seuil de statistiques en mode organisation (`scope org/`).

Exemple

Cet exemple montre comment accéder à la classe de politiques de seuil de statistiques du serveur Ethernet par défaut, créer une classe de statistiques de châssis, créer une propriété de puissance d'entrée (Watts), spécifier que le niveau de puissance normale est de 8 kW, créer un seuil d'avertissement supérieur à la normale de 11 kW, puis valider la classe :

```
firepower # scope eth-server
firepower /eth-server # scope stats-threshold-policy default
firepower /eth-server/stats-threshold-policy # create class chassis-stats
firepower /eth-server/stats-threshold-policy/class* # create property input-power
firepower /eth-server/stats-threshold-policy/class/property* # set normal-value 8000.0
firepower /eth-server/stats-threshold-policy/class/property* # create threshold-value
above-normal warning
firepower /eth-server/stats-threshold-policy/class/property/threshold-value* # set escalating
 11000.0
firepower /eth-server/stats-threshold-policy/class/property/threshold-value* # commit-buffer
firepower /eth-server/stats-threshold-policy/class/property/threshold-value #
```

Commandes associées

Commande	Description
enter class	Permet d'accéder ou crée une classe de statistiques.
enter property	Permet d'accéder ou crée une propriété pour une classe de statistiques.
scope stats-threshold-policy	Permet d'accéder au mode stats-threshold-policy vous permettant de gérer des classes de statistiques.
set normal-value	Définit la valeur normale d'une propriété de classe.

create trustpoint

Pour ajouter un nouveau point de confiance pour la validation d'un certificat lors de l'authentification IKE Internet Key Exchange), utilisez la commande **create trustpoint**. Si une connexion portant le nom spécifié existe déjà, la commande échoue.

Pour ajouter ou modifier un point de confiance, utilisez la commande **enter trustpoint**. Si le point de confiance spécifié n'existe pas, il est créé et saisi; si le point de confiance existe, il est saisi.

Vous pouvez également utiliser la forme **scope** de cette commande pour accéder à un point de confiance existant afin d'affecter ou de modifier des propriétés.

Pour supprimer un point de confiance existant, utilisez la forme **delete** de cette commande.

create trustpoint *name*
delete trustpoint *name*
enter trustpoint *name*
scope trustpoint *name*

Description de la syntaxe

name	Le nom du point de confiance peut comporter jusqu'à 32 caractères alphanumériques.

Modes de commande

scope security/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour identifier les points de confiance qui seront utilisés pour valider les certificats lors de l'authentification IKE (Internet Key Exchange).

Lorsque vous créez un point de confiance, vous accédez automatiquement au mode sécurité/point de confiance accompagné d'un astérisque pour indiquer que le nouveau point de confiance n'est pas encore validé. Après avoir créé un point de confiance, son nom ne peut pas être modifié. Vous devez supprimer le point de confiance et en créer un nouveau.

Exemple

Cet exemple montre comment créer et saisir un point de confiance :

```
firepower # scope security
firepower /security # enter trustpoint tPoint4
firepower /security/trustpoint* #
```

Commandes associées

Commande	Description
set certchain	Définit les informations sur le certificat d'un point de confiance.
show trustpoint	Affiche les informations sur le point de confiance actuel.

cycle

Pour redémarrer un module de sécurité ou un serveur, utilisez l'une des commandes **cycle**.

cycle {**cycle-immediate** | **cycle-wait**}

Description de la syntaxe

cycle-immediate	Redémarre immédiatement le module.
cycle-wait	Le système attend jusqu'à cinq minutes que l'application exécutée sur le module s'arrête avant de redémarrer celui-ci.

Modes de commande

scope service-profile/

Historique des commandes

Version	Modification
1.1(1)	Cette commande a été introduite.

Exemple

Cet exemple montre comment redémarrer un module après l'arrêt de son application en cours d'exécution :

```
firepower # scope service-profile server 1/1
firepower /org/service-profile # cycle cycle-wait
firepower /org/service-profile* # commit-buffer
firepower /org/service-profile #
```

Commandes associées

Commande	Description
set adminstate	Met un module de réseau hors ligne ou en ligne.

Commandes D – R

- decommission, à la page 121
- decommission-secure, à la page 122
- delete hw-crypto, à la page 123
- delete, à la page 124
- delete decommissioned server, à la page 126
- deregister, à la page 127
- disable (app-instance), à la page 128
- disable (export-configuration), à la page 129
- disable (interface), à la page 130
- disable (port-channel), à la page 131
- disable (modes sécurité), à la page 132
- disable reservation, à la page 133
- disable snmp, à la page 134
- discard-buffer, à la page 135
- download image, à la page 136
- enable (app-instance), à la page 138
- enable (modes sécurité CC et FIPS), à la page 139
- enable (export-configuration), à la page 141
- enable (interface), à la page 142
- enable (port-channel), à la page 143
- enable reservation, à la page 144
- enable snmp, à la page 145
- end, à la page 146
- enter, à la page 147
- erase, à la page 149
- exit, à la page 151
- export-config, à la page 152
- generate password, à la page 154
- import-config, à la page 155
- install, à la page 158
- install firmware, à la page 159
- install platform, à la page 161
- mgmt-port (connect local-mgmt), à la page 162

- ping (connect local-mgmt), à la page 163
- ping6 (connect local-mgmt), à la page 165
- power, à la page 167
- reboot, à la page 168
- reinstall, à la page 170
- register, à la page 171
- reinitialize, à la page 172
- remove server, à la page 173
- renew, à la page 174
- reset-password, à la page 175
- request universal, à la page 176
- restart, à la page 177
- return, à la page 178

decommission

Pour désactiver un serveur, utilisez la commande **decommission server**.

decommission server {*id* | *chassis_id* / *blade_id*}

Description de la syntaxe

id	Numéro d'identification du serveur. Il s'agit d'une valeur comprise entre 1 et 255.
chassis_id / *blade_id*	Numéros d'identification de châssis et de lame, au format n/n.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
2.3(1)	Commande ajoutée.

Instructions d'utilisation

Selon le type d'appareil qui héberge le module à désactiver, identifiez-le à l'aide de son ID de module (série 4100) ou de ses numéros de châssis et de module (appareils 9300).

Lorsque vous désactivez un module de sécurité, l'objet de module est supprimé de la configuration et le module n'est plus géré. Tous les périphériques logiques ou logiciels exécutés sur le module deviennent inactifs.

Exemple

Cet exemple montre comment désactiver un serveur :

```
firepower# decommission server 1/1
firepower* # commit-buffer
firepower #
```

Commandes associées

Commande	Description
delete decommissioned	Supprime un serveur désactivé.
show server decommissioned	Affiche tous les serveurs désactivés.

decommission-secure

Pour désactiver un serveur en toute sécurité, utilisez la commande **decommission-secure server**.

decommission-secure server *chassis_id/blade_id*

Description de la syntaxe

chassis_id/blade_id	Numéros d'identification de châssis et de lame, au format n/n.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
2.7(1)	Commande ajoutée.

Instructions d'utilisation

Cette commande efface en toute sécurité le module spécifié. Autrement dit, les données ne sont pas simplement supprimées : le support de stockage physique est « nettoyé » (complètement effacé). Une fois le module de sécurité effacé, il reste inactif jusqu'à ce qu'il soit confirmé (comme un module désactivé).

Exemple

Cet exemple montre comment désactiver un serveur en toute sécurité :

```
firepower# decommission-secure server 1/2
Warning:
1.Secure decommissioning of the service module may take some time. Please use the CLI command
 'show slot status [n/n] detail' to check for completion.
2.All of the application data on the service module will be lost.  Please back up the
application's configuration files before executing the commit-buffer command.
firepower* #
```

Commandes associées

Commande	Description
decommission server	Désactive un serveur : l'objet de module est supprimé de la configuration, mais le stockage physique n'est pas complètement effacé.
erase secure	Efface en toute sécurité le composant système spécifié.

delete hw-crypto

Pour supprimer une configuration d'Accélération cryptographique TLS sur une instance de contenant, utilisez la commande **delete hw-crypto**. Pour plus de renseignements sur l'Accélération cryptographique TLS, consultez le *Guide de configuration de Cisco Firepower Management Center*.

delete hw-crypto

Modes de commande

connect module

Historique des commandes

Version	Modification
2.7.1	Cette commande a été introduite.

Instructions d'utilisation

Cette commande supprime une configuration d'Accélération cryptographique TLS pour une instance de contenant. Si l'Accélération cryptographique TLS est activée sur l'instance de contenant, la commande la désactive avant de supprimer la configuration.

Exemples

Voici un exemple de suppression d'une configuration d'Accélération cryptographique TLS :

```
scope ssa
/ssa # show app-instance

App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
 Deploy Type Turbo Mode Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- --------------- ---------------
 ----------- ---------- ------------ --------------- ------------
ftd        FTD-FDM    1          Enabled     Online           6.5.0.1159      6.5.0.1159
    Native      No                      Not Applicable  None
ftd        ftd2       2          Enabled     Online           6.5.0.1159      6.5.0.1159
    Container   No         Default-Small Not Applicable  None

/ssa # sc slot 2
/ssa/slot # scope app-instance ftd ftd2
/ssa/slot/app-instance # delete hw-crypto
/ssa/slot/app-instance* # commit-buffer
```

Commandes associées

Commande	Description
create hw-crypto	Créez une configuration d'Accélération cryptographique TLS pour une instance de contenant.
scope hw-crypto	Activez ou désactivez la configuration d'Accélération cryptographique TLS sur une instance de contenant.
show hw-crypto	Affichez l'état de la configuration d'Accélération cryptographique TLS sur une instance de contenant.

delete

Pour supprimer un objet géré existant, utilisez la commande **delete** pertinente dans le mode de commande approprié.

delete *object_type name* [*parameters*]

Description de la syntaxe

object_type	Type d'objet à supprimer. Les exemples comprennent le compte d'utilisateur local et l'organisation.
name	Nom de l'objet spécifique à supprimer.
paramètres	(Facultatif) Ensemble des propriétés ou paramètres supplémentaires nécessaires pour identifier l'objet. Pour plus de renseignements, consultez la description de la commande **create** du type d'objet spécifique.

Modes de commande

Selon le type d'objet en cours de suppression; pour plus de renseignements, consultez la description de la commande **create** du type d'objet spécifique.

Historique des commandes

Pour plus de renseignements sur l'historique, consultez la description de la commande **create** du type d'objet spécifique.

Instructions d'utilisation

Les objets sont des représentations abstraites de composants physiques ou d'entités logiques qui peuvent être gérés. Par exemple, les châssis, les modules de sécurité, les modules de réseau, les ports et les processeurs sont des composants physiques représentés sous forme d'objets gérés, tandis que les licences, les rôles d'utilisateur et les politiques de plateforme sont des entités logiques représentées sous forme d'objets gérés.

FXOS fournit quatre commandes générales pour la gestion des objets : **create**, **delete**, **enter** et **scope**. Par exemple, vous pouvez créer un compte d'utilisateur local, en supprimer un, ou y accéder pour lui attribuer ou modifier des propriétés. Vous pouvez également gérer directement le compte d'utilisateur local pour lui attribuer ou modifier des propriétés.

En général, les mots clés et les options disponibles pour chacune de ces commandes de gestion d'objets sont les mêmes. Nous ne détaillons donc que la version **create** des différentes commandes d'objet. En d'autres termes, pour plus de renseignements sur la commande **delete** d'un objet particulier, reportez-vous à la description de la commande **create** de cet objet. Par exemple, reportez-vous à create local-user, à la page 83 pour des informations sur la suppression d'un compte d'utilisateur local existant.

Exemples

Cet exemple montre comment accéder au mode sécurité, puis supprimer un compte d'utilisateur local :

```
firepower # scope security
firepower /security # delete local-user test_user
firepower /security/local-user* # commit-buffer
firepower /security/local-user #
```

Cet exemple montre comment accéder à un compte d'utilisateur local, puis supprimer un rôle d'utilisateur :

```
firepower # scope security
firepower /security # enter local-user test_user
firepower /security/local-user # delete role aaa
Warning: Change of privileges will terminate active sessions (CLI and Web) of user 'test_user
firepower /security/local-user* # commit-buffer
firepower /security/local-user #
```

Commandes associées

Commande	Description
create local-user	Crée un compte d'utilisateur local.
enter local-user	Ajoute ou modifie un compte d'utilisateur local.
delete local-user	Supprime un compte d'utilisateur local existant.
scope local-user	Permet d'accéder à un compte d'utilisateur local existant.

delete decommissioned server

Pour supprimer un serveur désactivé, utilisez la commande **delete decommissioned server** .

delete decommissioned server *vendor model serial_number*

Description de la syntaxe

vendor	Nom de l'entreprise qui a fabriqué le serveur; ne doit pas dépasser 510 caractères.
model	Nom de modèle du module; ne doit pas dépasser 510 caractères.
serial_number	Numéro de série du module; ne doit pas dépasser 510 caractères.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.4(1)	Commande ajoutée.

Exemple

Cet exemple montre comment supprimer un serveur désactivé.

```
FP9300-A # delete decommissioned server Cisco Systems, Inc.
Cisco Firepower 9000 Series Security Module
FLM1949C6J1
FP9300-A* # commit-buffer
```

Commandes associées

Commande	Description
decommission server	Désactive un serveur.

deregister

Pour supprimer cet appareil Firepower 4100/9300 de votre compte de licence logicielle Cisco Smart, utilisez la commande **deregister**.

deregister

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode licence

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

L'annulation de l'enregistrement supprime l'appareil de votre compte; tous les droits de licence et certificats de l'appareil sont supprimés. Vous pouvez ainsi libérer une licence pour un nouvel appareil Firepower 4100/9300 ou supprimer l'appareil de Smart Software Manager.

Exemple

Cet exemple montre comment annuler l'enregistrement de cet appareil.

```
FP9300-A # scope license
FP9300-A /license # deregister
FP9300-A /license #
```

Commandes associées

Commande	Description
register	Enregistre un compte Smart Software Manager sur cet appareil Firepower 4100/9300.

disable (app-instance)

Pour désactiver une instance d'application existante, utilisez la commande **disable** en mode instance d'application.

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope ssa/scope slot/scope app-instance

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour désactiver une instance d'application sans la supprimer du système.

Exemple

Cet exemple montre comment afficher les instances d'application actuelles, y compris leur état, puis accéder au mode instance d'application et désactiver une instance d'application :

```
firepower # scope ssa
firepower /ssa # scope slot 2
firepower /ssa/slot # show app-instance

Application Instance:
    App Name   Identifier Admin State Oper State       Running Version Startup Version
Deploy Type Profile Name Cluster State   Cluster Role
    ---------- ---------- ----------- ---------------- --------------- ---------------
----------- ------------ --------------- ------------
    ftd1       IFT-63     Enabled     Online           6.3.0.12        6.3.0.12
Native                   In Cluster      Slave

Application Instance:
    App Name   Identifier Admin State Oper State       Running Version Startup Version
Deploy Type Profile Name Cluster State   Cluster Role
    ---------- ---------- ----------- ---------------- --------------- ---------------
----------- ------------ --------------- ------------
    ftd2       FTD-2      Enabled     Online           6.3.0.12        6.3.0.12
Container   bronze       Not Applicable  None
firepower /ssa/slot # scope app-instance ftd2 FTD-2
firepower /ssa/slot/app-instance # disable
firepower /ssa/slot/app-instance* # commit-buffer
firepower /ssa/slot/app-instance #
```

Commandes associées

Commande	Description
enable	Active une instance d'application existante.
scope app-instance	Permet d'accéder au mode application pour une instance d'application spécifique.

disable (export-configuration)

Pour désactiver un objet de configuration d'exportation existant, utilisez la commande **disable** en mode configuration d'exportation.

Pour désactiver une instance d'application existante, utilisez la commande **disable** en mode instance d'application.

Pour désactiver un objet de configuration d'exportation existant, utilisez la commande **disable** en mode configuration d'exportation.

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope system/scope export-config

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

En mode configuration d'exportation, utilisez cette commande pour désactiver un objet de configuration d'exportation existant sans le supprimer du système.

Exemple

Cet exemple montre comment cibler un objet de configuration exportée et le désactiver :

```
firepower # scope system
firepower /system # scope export-config 192.168.1.2
firepower /system/export-config #disable
firepower /system/export-config* #commit-buffer
```

Commandes associées

Commande	Description
enable	En mode de configuration d'exportation, active un objet de configuration d'exportation existant.
scope export-config	Permet d'accéder à un objet de configuration d'exportation existant.

disable (interface)

Pour désactiver l'interface actuelle, utilisez la commande **disable** en mode interface.

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope eth-uplink/scope fabric/interface

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour désactiver l'interface actuelle.

Exemple

Cet exemple montre comment désactiver une interface et confirmer son état :

```
firepower # scope eth-uplink
firepower /eth-uplink # scope fabric
firepower /eth-uplink #/fabric # scope interface Ethernet1/5
firepower /eth-uplink/fabric/interface # disable
firepower /eth-uplink/fabric/interface* # commit-buffer
firepower /eth-uplink/fabric/interface # show

Interface:
    Port Name       Port Type          Admin State Oper State       Allowed Vlan State
Reason
   --------------- ------------------ ----------- ---------------- ------------ ------------

    Ethernet1/5     Data               Disabled    Up               All
firepower /eth-uplink/fabric/interface #
```

Commandes associées

Commande	Description
enable	Active l'interface actuelle.
set	En mode interface, définit les paramètres de configuration de l'interface.
show interface	Affiche les informations de configuration et d'état de l'interface.

disable (port-channel)

Pour activer le canal de port actuel (EtherChannel), utilisez la commande **disable** en mode canal de port.

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope eth-uplink/scope fabric/port-channel

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour désactiver le canal de port actuel.

Exemple

Cet exemple montre comment désactiver un canal de port et confirmer son état :

```
firepower # scope eth-uplink
firepower /eth-uplink # scope fabric
firepower /eth-uplink #/fabric # scope port-channel 4
firepower /eth-uplink/fabric/port-channel # disable
firepower /eth-uplink/fabric/port-channel* # commit-buffer
firepower /eth-uplink/fabric/port-channel # show

Port Channel:
    Port Channel Id Name             Port Type          Admin State Oper State       Port
Channel Mode Allowed Vlan State Reason
    ---------------- ---------------- ------------------ ----------- ----------------
----------------- ------------ ------------
    4                Port-channel4    Data               Disabled    Failed           Active
            All          Admin config change
firepower /eth-uplink/fabric/port-channel #
```

Commandes associées

Commande	Description
enable	Active le canal de port actuel.
show port-channel	Affiche les informations de configuration et d'état du canal de port.

disable (modes sécurité)

Pour désactiver le mode Common Criteria ou FIPS (Federal Information Processing Standard), utilisez la commande **disable** dans security scope.

disable {**cc-mode** | **fips-mode**}

Description de la syntaxe

cc-mode	Utilisez ce mot clé pour désactiver le mode Common Criteria.
fips-mode	Utilisez ce mot clé pour désactiver le mode FIPS.

Modes de commande

scope security/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Une fois cette commande validée, le système doit être redémarré.

Exemple

Cet exemple montre comment accéder au mode sécurité et désactiver le mode FIPS :

```
firepower # scope security
firepower /security # disable fips-mode
Warning: A reboot of the system is required in order for the system to be
operating in a non-FIPS approved mode.
firepower /security* #
```

Commandes associées

Commande	Description
enable (modes sécurité)	Active le mode CC ou FIPS.
show cc-mode	Affiche les états administratif et opérationnel actuels du mode Common Criteria.
show fips-mode	Affiche les états administratif et opérationnel actuels du mode FIPS.

disable reservation

Pour désactiver la réservation de licence permanente, utilisez la commande **disable reservation**.

disable reservation

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode licence (/licence)

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Activez la réservation de licence avant de tenter d'attribuer une licence permanente à votre châssis Firepower 4100/9300.

Exemple

Cet exemple montre comment accéder au mode licence et désactiver le mode réservation :

```
FP9300-A # scope license
FP9300-A /license # disable reservation
Warning: If you have already generated the authorization code from CSSM
and have not installed it on the device, please abort this command by
issuing discard-buffer and complete the installation.
FP9300-A /license* #
```

Commandes associées

Commande	Description
enable reservation	Active la réservation de licence permanente.
show license	Affiche les informations de licences actuelles.

disable snmp

Pour désactiver le traitement du protocole SNMP (Simple Network Management Protocol) sur cet appareil, utilisez la commande **disable snmp**.

disable snmp

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope monitoring/

Historique des commandes

Version	Modification
1.1.1	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour désactiver l'agent SNMP sur cet appareil. Le paramètre de communauté SNMP actuel est ignoré, mais les autres paramètres de configuration SNMP ne sont pas supprimés.

Exemple

L'exemple suivant montre comment cibler le mode surveillance, désactiver le traitement SNMP, puis utiliser la commande **show snmp** pour confirmer sa désactivation :

```
firepower # scope monitoring
firepower /monitoring # disable snmp
firepower /monitoring* # commit-buffer
firepower /monitoring # show snmp
Name: snmp
    Admin State: Disabled
    Port: 161
    Is Community Set: No
    Sys Contact: R_Admin
    Sys Location:
firepower /monitoring #
```

Commandes associées

Commande	Description
enable snmp	Active le protocole SNMP.
set snmp	Définit les paramètres de configuration SNMP : communauté, personne-ressource système responsable de SNMP et emplacement de l'hôte.
show snmp	Affiche la configuration SNMP actuelle.

discard-buffer

Pour annuler les modifications de configuration en attente, utilisez la commande **discard-buffer**.

discard-buffer

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour annuler et ignorer toutes les modifications de configuration non validées. Si des commandes de configuration sont en attente, un astérisque (*) s'affiche avant l'invite de commande. Lorsque vous saisissez la commande **discard-buffer**, les commandes sont ignorées et l'astérisque disparaît.

Exemple

Cet exemple montre comment ignorer les modifications de configuration en attente :

```
FP9300-1# scope chassis 1
FP9300-1 /chassis # enable locator-led
FP9300-1 /chassis* # show configuration pending
 scope chassis 1
+    enable locator-led
 exit
FP9300-1 /chassis* # discard-buffer
FP9300-1 /chassis #
```

Commandes associées

Commande	Description
commit-buffer	Enregistre ou vérifie les modifications de configuration.
show configuration pending	Affiche les modifications de configuration non validées.

download image

Pour copier une image de micrologiciel FXOS sur le châssis Firepower 4100/9300, utilisez la commande **download image** en mode micrologiciel.

Pour copier une image logicielle de périphérique logique sur le châssis Firepower 4100/9300, utilisez la commande **download image** en mode logiciel d'application (/ssa/app-software).

download image {**ftp:** | **scp:** | **sftp:** | **tftp:** | **usbA:** | **usbB:** }

Description de la syntaxe

ftp://*server-ip-addr*/*path*	(Facultatif) Spécifie l'URI d'un fichier image à importer via FTP (File Transfer Protocol).
scp://*username*@ *server-ip-addr*/*path*	(Facultatif) Spécifie l'URI d'un fichier image à importer via SCP (Secure Copie Protocol).
sftp://*username*@ *server-ip-addr*/*path*	(Facultatif) Spécifie l'URI d'un fichier image à importer via SFTP (SSH File Transfer Protocol ou Secure File Transfer Protocol).
tftp://*username*@ *server-ip-addr***:***port-num*/*path*	(Facultatif) Spécifie l'URI d'un fichier image à importer via TFTP (Trivial File Transfer Protocol). **Remarque** Le protocole TFTP présente une limite de taille de fichier de 32 Mo. Les offres groupées de micrologiciels pouvant être beaucoup plus volumineuses, nous vous recommandons de ne pas utiliser le protocole TFTP pour télécharger des micrologiciels.
usbA:/*path*	(Facultatif) Spécifie le chemin d'accès à un fichier image à importer à partir d'un périphérique USB de type A connecté.
usbB:/*path*	(Facultatif) Spécifie le chemin d'accès à un fichier image à importer à partir d'un périphérique USB de type B connecté.

Modes de commande

scope firmware/

scope ssa/scope app-software/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Assurez-vous de disposer de l'adresse d'emplacement et des informations d'authentification pour l'accès au fichier image, ainsi que du nom complet du fichier.

FXOS stocke les images de micrologiciel dans la mémoire flash de démarrage sur l'interconnexion de structures.

En mode micrologiciel, vous pouvez utiliser la commande **show package** *image_name* **detail** pour surveiller le processus de téléchargement de l'image. L'affichage de la sortie ne s'actualise pas automatiquement et vous pouvez être amené à saisir plusieurs fois la commande jusqu'à ce que l'état de la tâche indique « Téléchargé ».

En mode micrologiciel et en mode logiciel d'application, vous pouvez utiliser la commande **show download-task** pour surveiller le processus de téléchargement de l'image. L'affichage de la sortie n'actualise pas automatiquement et vous pouvez être amené à saisir plusieurs fois la commande.

Exemples

Cet exemple montre comment télécharger un fichier image de micrologiciel à l'aide du protocole SCP et surveiller la progression du téléchargement :

```
FP9300-A# scope firmware
FP9300-A /firmware # download image scp://user@192.168.1.1/images/fxos-k9.1.1.1.119.SPA
FP9300-A /firmware # show package fxos-k9.1.1.1.119.SPA detail
Download task:
File Name: fxos-k9.1.1.1.119.SPA
Protocol: scp
Server: 192.168.1.1
Userid:
Path:
Downloaded Image Size (KB): 5120
State: Downloading
Current Task: downloading image fxos-k9.1.1.1.119.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Cet exemple montre comment télécharger un fichier image de logiciel à l'aide du protocole SCP et surveiller la progression du téléchargement :

```
firepower# scope ssa
firepower /ssa # scope app-software
firepower /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
firepower /ssa/app-software # show download-task
Downloads for Application Software:
    File Name                      Protocol   Server               Userid          State
    ------------------------------ ---------- -------------------- --------------- -----
    cisco-asa.9.4.1.65.csp         Scp        192.168.1.1          user            Downloaded
```

Commandes associées

Commande	Description
show download-task	Affiche la progression du téléchargement du fichier image.
show package	Affiche la progression du téléchargement du fichier de micrologiciel.
verify platform-pack	Vérifie une image de plateforme FXOS spécifiée.

enable (app-instance)

Pour activer une instance d'application existante, utilisez la commande **enable** en mode instance d'application.

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope ssa/scope slot/scope app-instance

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour réactiver une instance d'application précédemment désactivée.

Exemple

Cet exemple montre comment afficher les instances d'application actuelles, y compris leur état, puis accéder au mode instance d'application et activer une application désactivée :

```
firepower # scope ssa
firepower /ssa # scope slot 2
firepower /ssa/slot # show app-instance

Application Instance:
    App Name   Identifier Admin State Oper State       Running Version Startup Version
Deploy Type Profile Name Cluster State   Cluster Role
    ---------- ---------- ----------- ---------------- --------------- ---------------
----------- ------------ --------------- ------------
    ftd1       IFT-63     Enabled     Online           6.3.0.12        6.3.0.12
Native                    In Cluster      Slave

Application Instance:
    App Name   Identifier Admin State Oper State       Running Version Startup Version
Deploy Type Profile Name Cluster State   Cluster Role
    ---------- ---------- ----------- ---------------- --------------- ---------------
----------- ------------ --------------- ------------
    ftd2       FTD-2      Disabled    Online           6.3.0.12        6.3.0.12
Container   bronze       Not Applicable  None
firepower /ssa/slot # scope app-instance ftd2 FTD-2
firepower /ssa/slot/app-instance # enable
firepower /ssa/slot/app-instance* # commit-buffer
firepower /ssa/slot/app-instance #
```

Commandes associées

Commande	Description
disable	En mode instance d'application, désactive une instance d'application existante.
scope app-instance	Permet d'accéder au mode application pour une instance d'application spécifique.

enable (modes sécurité CC et FIPS)

Pour activer le mode Common Criteria ou FIPS (Federal Information Processing Standard), utilisez la commande **enable** dans security scope.

enable { **cc-mode** | **fips-mode** }

Description de la syntaxe

cc-mode	Utilisez ce mot clé pour activer le mode Common Criteria.
fips-mode	Utilisez ce mot clé pour activer le mode FIPS.

Modes de commande

scope security/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

La connectivité à un ou plusieurs services peut être refusée lorsque cette commande est validée. De plus, un redémarrage du système est nécessaire.

Important Dans les versions FXOS antérieures à la version 2.0.1, la clé d'hôte SSH existante créée lors de la première configuration d'un appareil était codée en dur sur 1024 bits. Afin de respecter les exigences de certification FIPS et Common Criteria, vous devez supprimer cette ancienne clé d'hôte et en générer une nouvelle (pour plus de renseignements sur la création et la suppressions de clés d'hôte SSH, consultez create ssh-server, à la page 109). Si vous n'effectuez pas ces étapes supplémentaires, vous ne pourrez pas vous connecter au superviseur à l'aide de SSH après le redémarrage du périphérique et le mode Common Criteria activé. Si vous avez effectué la configuration initiale en utilisant FXOS 2.0.1 ou une version ultérieure, vous n'avez pas besoin de générer une nouvelle clé d'hôte.

Exemple

Cet exemple montre comment accéder au mode sécurité et activer le mode FIPS :

```
firepower # scope security
firepower /security # enable fips-mode
Warning: Connectivity to one or more services may be denied when committed.
Please consult the product's FIPS Security Policy documentation.
WARNING: A reboot of the system is required in order for the system to be operating in a
FIPS approved mode.

firepower /security* #
```

Commandes associées

Commande	Description
disable (modes sécurité)	Désactive le mode CC ou FIPS.
show cc-mode	Affiche les états administratif et opérationnel actuels du mode Common Criteria.

Commande	Description
show fips-mode	Affiche les états administratif et opérationnel actuels du mode FIPS.

enable (export-configuration)

Pour réactiver un objet de configuration d'exportation existant, utilisez la commande **enable** en mode configuration d'exportation.

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope system/scope export-config

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour réactiver un objet de configuration d'exportation précédemment sauvegardé, avant d'exporter à nouveau la configuration. La configuration système actuelle est exportée en fonction des paramètres d'objet lorsque vous exécutez la commande **commit-buffer**.

Exemple

Cet exemple montre comment accéder à un objet de configuration précédemment exporté, l'activer, lancer la sauvegarde de la configuration, puis confirmer que l'exportation est en cours :

```
firepower # scope system
firepower /system # scope export-config 192.168.1.2
firepower /system/export-config #enable
firepower /system/export-config* #commit-buffer
firepower /system/export-config #show

Export Configuration Task:
    Hostname   User       Protocol Admin State Status    Description
    ---------- ---------- -------- ----------- --------- -----------
    192.168.1.2
               user1      Scp      Enabled     Exporting
```

Commandes associées

Commande	Description
disable	Désactive un objet de configuration d'exportation existant.
scope export-config	Permet d'accéder à un objet de configuration d'exportation existant.

enable (interface)

Pour activer l'interface actuelle, utilisez la commande **enable** en mode interface.

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope eth-uplink/scope fabric/interface

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour activer ou réactiver une interface.

Exemple

Cet exemple montre comment activer une interface et confirmer son état :

```
firepower # scope eth-uplink
firepower /eth-uplink # scope fabric
firepower /eth-uplink #/fabric # scope interface Ethernet1/5
firepower /eth-uplink/fabric/interface # enable
firepower /eth-uplink/fabric/interface* # commit-buffer
firepower /eth-uplink/fabric/interface # show

Interface:
    Port Name       Port Type          Admin State Oper State       Allowed Vlan State
Reason
    --------------- ------------------ ----------- ---------------- ------------ ------------

    Ethernet1/5     Data               Enabled     Up               All
firepower /eth-uplink/fabric/interface #
```

Commandes associées

Commande	Description
disable	Désactive l'interface actuelle.
set	En mode interface, définit les paramètres de configuration de l'interface.
show interface	Affiche les informations de configuration et d'état de l'interface.

enable (port-channel)

Pour activer le canal de port actuel (EtherChannel), utilisez la commande **enable** en mode canal de port.

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope eth-uplink/scope fabric/port-channel

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour activer ou réactiver un canal de port.

Exemple

L'exemple suivant montre comment créer un canal de port, l'activer et ajouter des ports membres :

```
firepower # scope eth-uplink
firepower /eth-uplink/fabric # scope fabric a
firepower /eth-uplink/fabric # create port-channel 4
firepower /eth-uplink/fabric/port-channel* # enable
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # commit-buffer
firepower /eth-uplink/fabric/port-channel #
```

Commandes associées

Commande	Description
create member-port	Ajoute un port membre à un canal de port.
disable	Désactive le canal de port actuel.
set (port-channel)	Définit ou modifie les paramètres d'un canal de port existant.
show port-channel	Affiche les informations de configuration et d'état du canal de port.

enable reservation

Pour activer la réservation de licence permanente, utilisez la commande **enable reservation**.

enable reservation

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode licence (/licence)

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Activez la réservation de licence avant de tenter d'attribuer une licence permanente à votre châssis Firepower 4100/9300.

Exemple

Cet exemple montre comment accéder au mode licence et activer le mode réservation :

```
FP9300-A # scope license
FP9300-A /license # enable reservation
FP9300-A /license #
```

Commandes associées

Commande	Description
disable reservation	Désactive la réservation de licence permanente.
show license	Affiche les informations de licences actuelles.

enable snmp

Pour activer le traitement du protocole SNMP (Simple Network Management Protocol) sur cet appareil, utilisez la commande **enable snmp**.

enable snmp

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope monitoring/

Historique des commandes

Version	Modification
1.1.1	Commande ajoutée.

Instructions d'utilisation

Après avoir utilisé cette commande pour activer l'agent SNMP sur cet appareil, vous pouvez créer une communauté SNMP et créer des utilisateurs, ainsi que des déroutements SNMP.

Exemple

L'exemple suivant montre comment cibler le mode surveillance et activer le traitement de SNMP :

```
firepower # scope monitoring
firepower /monitoring # enable snmp
firepower /monitoring* # commit-buffer
firepower /monitoring #
```

Commandes associées

Commande	Description
disable snmp	Désactive le protocole SNMP.
set snmp	Définit les paramètres de configuration SNMP : communauté, personne-ressource système responsable de SNMP et emplacement de l'hôte.
show snmp	Affiche la configuration SNMP actuelle.

end

Pour revenir au mode EXEC (niveau supérieur) de l'interface de ligne de commande, utilisez la commande **end**.

end

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment revenir au mode profil de service le plus élevé de l'interface de ligne de commande.

```
FP9300-A # scope org Test
FP9300-A /org # scope service-profile Sample
FP9300-A /org/service-profile # end
FP9300-A #
```

Commandes associées

Commande	Description
top	Permet d'accéder au mode de niveau supérieur à partir de n'importe quel mode.

enter

Pour saisir un objet géré, utilisez la commande **enter** pertinente dans le mode de commande approprié. En règle générale, si l'objet spécifié n'existe pas, il est créé.

enter *object_type name* [*parameters*]

Description de la syntaxe

object_type	Type d'objet à saisir. Les exemples comprennent le compte d'utilisateur local et l'organisation.
name	Nom de l'objet spécifique à saisir.
paramètres	(Facultatif) Ensemble des propriétés ou paramètres supplémentaires nécessaires pour identifier l'objet. Pour plus de renseignements, consultez la description de la commande **create** du type d'objet spécifique.

Modes de commande

Selon le type d'objet en cours de saisie; pour plus de renseignements, consultez la description de la commande **create** du type d'objet spécifique.

Historique des commandes

Pour plus de renseignements sur l'historique, consultez la description de la commande **create** du type d'objet spécifique.

Instructions d'utilisation

Les objets sont des représentations abstraites de composants physiques ou d'entités logiques qui peuvent être gérés. Par exemple, les châssis, les modules de sécurité, les modules de réseau, les ports et les processeurs sont des composants physiques représentés sous forme d'objets gérés, tandis que les licences, les rôles d'utilisateur et les politiques de plateforme sont des entités logiques représentées sous forme d'objets gérés.

FXOS fournit quatre commandes générales pour la gestion des objets : **create**, **delete**, **enter** et **scope**. Par exemple, vous pouvez créer un compte d'utilisateur local, en supprimer un, ou y accéder pour lui attribuer ou modifier des propriétés. Vous pouvez également gérer directement le compte d'utilisateur local pour lui attribuer ou modifier des propriétés.

En général, les mots clés et les options disponibles pour chacune de ces commandes de gestion d'objets sont les mêmes. Nous ne détaillons donc que la version **create** des différentes commandes d'objet. En d'autres termes, pour plus de renseignements sur la commande **delete** d'un objet particulier, reportez-vous à la description de la commande **create** de cet objet. Par exemple, reportez-vous à create local-user, à la page 83 pour des informations sur l'accès à un compte d'utilisateur local existant.

Exemple

Cet exemple montre comment accéder au mode sécurité, accéder à un compte d'utilisateur local et afficher les détails correspondants :

```
firepower # scope security
firepower /security # enter local-user test_user
firepower /security/local-user # show detail
Local User test_user:
    First Name: test
    Last Name: user
    Email: test_user@testuser.com
    Phone:
```

```
    Expiration: Never
    Password: ****
    User lock status: Not Locked
    Account status: Active
    User Roles:
        Name: admin
        Name: read-only
    User SSH public key:
firepower /security/local-user #
```

Commandes associées

Commande	Description
create local-user	Crée un compte d'utilisateur local.
enter local-user	Ajoute ou modifie un compte d'utilisateur local.
delete local-user	Supprime un compte d'utilisateur local existant.
scope local-user	Permet d'accéder à un compte d'utilisateur local existant.

erase

Pour effacer toute la configuration utilisateur de l'application ou effacer des éléments de l'application en toute sécurité, utilisez la commande **erase**.

erase { **configuration** | **secure** { **chassis** | **security_modulesupervisor** } }

Description de la syntaxe

configuration	Utilisez ce mot clé pour effacer toutes les informations de configuration utilisateur sur le châssis et rétablir sa configuration d'usine par défaut.
secure	Utilisez cette option pour effacer en toute sécurité le composant d'appareil spécifié : • **chassis** : utilisez ce mot clé pour effacer le châssis en toute sécurité. • **security_module** *module_id* : utilisez cette option pour effacer le module spécifié en toute sécurité. • **supervisor** : utilisez ce mot clé pour effacer le superviseur de châssis en toute sécurité.

Modes de commande

connect local-mgmt/

Historique des commandes

Version	Modification
2.0.1	Commande ajoutée.
2.7(1)	Option **secure** ajoutée.

Instructions d'utilisation

La commande **erase configuration** supprime toutes les informations de configuration utilisateur du châssis et rétablit sa configuration d'usine par défaut.

La commande **erase secure** efface en toute sécurité le composant d'appareil spécifié. Autrement dit, les données ne sont pas simplement supprimées : le support de stockage physique est « nettoyé » (complètement effacé). Cela est important lorsque l'appareil est transféré ou retourné, car ses composants de stockage physique ne conservent pas de données ou d'éléments résiduels.

Remarque L'appareil redémarre pendant l'effacement sécurisé, ce qui signifie que les connexions SSH sont interrompues. Par conséquent, nous recommandons d'effectuer l'effacement sécurisé via une connexion au port console série.

Exemples

Cet exemple montre comment effacer toutes les informations de configuration utilisateur sur le châssis et rétablir sa configuration d'usine par défaut.

```
firepower# connect local-mgmt
firepower(local-mgmt)# erase configuration
```

```
All configurations will be erased and system will reboot. Are you sure? (yes/no):
```

Cet exemple montre comment effacer le module de sécurité 2 de manière sécurisée :

```
firepower# connect local-mgmt
firepower# erase secure security_module 2
The physical storages in security module will be securely erased.
ALL DATA AND IMAGES WILL BE LOST AND CANNOT BE RECOVERED!
After the erase the module will reboot and need to be re-initialized.
DO NOT POWER OFF THE DEVICE IF YOU DECIDE TO PERFORM THIS TASK!
Are you sure? (yes/no):
```

Commandes associées

Commande	Description
decommission-secure	Efface en toute sécurité le module spécifié.

exit

Pour quitter la session d'interface de ligne de commande actuelle et se déconnecter de l'appareil, ou pour quitter un mode d'objet connecté et revenir au niveau EXEC, utilisez la commande **exit**.

exit

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment quitter la session d'interface de ligne de commande de niveau supérieur actuelle et se déconnecter de cet appareil.

```
FP9300-A # exit
```

Cet exemple montre comment établir et quitter une connexion de gestion locale.

```
FP9300-A # connect local-mgmt
FP9300-A(local-mgmt) # exit
FP9300-A #
```

Commandes associées

Commande	Description
connect	Se connecte à un autre objet géré.
end	Revient au mode de niveau supérieur de l'interface de ligne de commande.

export-config

Pour exporter la configuration système actuelle vers un serveur distant en tant que fichier XML, utilisez la commande **export-config** .

export-config { *URL* **disabled** | **enabled** }

Description de la syntaxe

URL	Indiquez le chemin complet vers le système distant, y compris le nom du compte d'utilisateur, le protocole de transport et le nom de fichier, pour le fichier d'image XML exporté. Les protocoles de transport suivants peuvent être utilisés : • **ftp:***//username@hostname/path/image_name* • **scp:***//username@hostname/path/image_name* • **sftp:***//username@hostname/path/image_name* • **tftp:***//username@hostname/path/image_name*
disabled	Désactive l'état administratif de la politique; le fichier de configuration n'est pas exporté.
enabled	Active l'état administratif de la politique; le fichier de configuration est immédiatement exporté.

Modes de commande

scope system/

Historique des commandes

Version	Modification
1.1.3	Commande ajoutée.

Instructions d'utilisation

Utilisez la fonctionnalité d'exportation de configuration pour exporter un fichier XML contenant les paramètres de configuration des périphériques logiques et de la plateforme pour votre châssis Firepower 4100/9300. Vous pouvez importer ce fichier de configuration ultérieurement pour appliquer rapidement les paramètres de configuration à votre châssis Firepower 4100/9300 afin de retrouver une configuration stable ou de récupérer suite à une défaillance système.

Veuillez noter les points suivants :

- À partir de FXOS 2.6.1, vous devez spécifier une clé à utiliser lors du chiffrement d'informations sensibles telles que les mots de passe et autres clés secrètes durant l'exportation de la configuration, et vous devez l'avoir spécifiée avant de tenter d'exporter la configuration.

  De plus, la même clé utilisée lors de l'exportation doit être définie sur le système cible lorsque vous importez une configuration exportée, sauf si le fichier a été exporté à partir d'une version FXOS antérieure à la version 2.6.1, auquel cas le système cible ne vérifie pas la clé de chiffrement et autorise l'importation.

- Ne modifiez pas le contenu du fichier de configuration. Si un fichier de configuration est modifié, l'importation de la configuration à l'aide de ce fichier peut échouer.

- Les paramètres de configuration spécifiques à l'application ne sont pas contenus dans le fichier de configuration. Vous devez utiliser les outils de sauvegarde de configuration fournis par l'application pour gérer les paramètres et les configurations spécifiques à l'application.
- Pour éviter d'écraser les fichiers de sauvegarde existants, modifiez le nom du fichier lors de l'opération de sauvegarde ou copiez le fichier existant à un autre emplacement.

Selon le protocole de transport et la configuration du serveur distant, vous devrez peut-être saisir le mot de passe de l'utilisateur à des fins de connexion.

Lorsque vous exportez un nouveau fichier de configuration, vous accédez automatiquement au mode configuration d'exportation (system/export-config) accompagné d'un astérisque pour indiquer que le nouveau fichier n'a pas encore été exporté; saisissez **commit-buffer** pour commencer le processus.

Exemple

Cet exemple montre comment exporter un fichier XML contenant les paramètres de configuration du périphérique logique et de la plateforme vers un serveur distant :

```
firepower # scope system
firepower /system # export-config scp://user1@192.168.1.2:/export/cfg-backup.xml enabled
Password:
firepower /system/export-config* # commit-buffer
firepower /system/export-config #
```

Commandes associées

Commande	Description
cfg-export-policy	Configure une politique d'exportation de configuration.
import-config	Copie un fichier de configuration XML précédemment exporté vers cet appareil.
set password-encryption-key	Spécifie une clé utilisée pour le chiffrement des informations sensibles lors de l'exportation de la configuration.

generate password

Pour générer un mot de passe aléatoire de longueur fixe avec ou sans caractères spéciaux, utilisez la commande **generate password** .

generate password *password*

Description de la syntaxe

password	Mot de passe de l'utilisateur lors de la connexion.

Modes de commande

scope security

Historique des commandes

Version	Modification
2.10(1)	Commande ajoutée.

Instructions d'utilisation

Vous pouvez générer un mot de passe aléatoire de longueur fixe avec ou sans caractères spéciaux.

Exemple

Cet exemple montre comment accéder au mode sécurité et générer un mot de passe aléatoire de longueur fixe avec ou sans caractères spéciaux :

```
firepower # scope security
firepower # create local-user admin2
firepower /security/local-user #

firepower /security/local-user # generate password
  8-127  Password length

firepower /security/local-user # generate password 10 with
  with-special-char     With Special Char
  without-special-char  Without Special Char

firepower /security/local-user # generate password 10 with-special-char
@!D4%vlwCN
```

Commandes associées

Commande	Description
set password	Définit le mot de passe du compte d'utilisateur :

import-config

Pour importer un fichier de configuration XML précédemment exporté, utilisez la commande **import-config**.

import-config { *URL* **disabled** | **enabled** }

Description de la syntaxe

URL	Indiquez le chemin complet vers le système distant, y compris le protocole de transport et le nom du fichier, pour le fichier image XML à importer. Les protocoles de transport suivants peuvent être utilisés : • **ftp:***//username@hostname/path/image_name* • **scp:***//username@hostname/path/image_name* • **sftp:***//username@hostname/path/image_name* • **tftp:***//username@hostname/path/image_name*
disabled	Désactive l'état administratif de la politique; le fichier de configuration n'est pas importé.
enabled	Active l'état administratif de la politique; le fichier de configuration est immédiatement importé.

Modes de commande

scope system/

Historique des commandes

Version	Modification
2.0.1	Commande ajoutée.

Instructions d'utilisation

Utilisez la fonctionnalité d'exportation de configuration pour exporter un fichier XML contenant les paramètres de configuration des périphériques logiques et de la plateforme pour votre châssis Firepower 4100/9300. Vous pouvez importer ce fichier de configuration ultérieurement pour appliquer rapidement les paramètres de configuration à votre châssis Firepower 4100/9300 afin de retrouver une configuration stable ou de récupérer suite à une défaillance système.

Veuillez noter les points suivants :

- À partir de FXOS 2.6.1, vous devez spécifier une clé à utiliser lors du chiffrement d'informations sensibles telles que les mots de passe et autres clés secrètes durant l'exportation de la configuration, et vous devez l'avoir spécifiée avant de tenter d'exporter la configuration.

  De plus, la même clé utilisée lors de l'exportation doit être définie sur le système cible lorsque vous importez une configuration exportée, sauf si le fichier a été exporté à partir d'une version FXOS antérieure à la version 2.6.1, auquel cas le système cible ne vérifie pas la clé de chiffrement et autorise l'importation.

- Ne modifiez pas le contenu du fichier de configuration. Si un fichier de configuration est modifié, l'importation de la configuration à l'aide de ce fichier peut échouer.

- Les paramètres de configuration spécifiques à l'application ne sont pas contenus dans le fichier de configuration. Vous devez utiliser les outils de sauvegarde de configuration fournis par l'application pour gérer les paramètres et les configurations spécifiques à l'application.

- Lorsque vous importez une configuration sur un châssis Firepower 4100/9300, toutes les configurations existantes sur le châssis (y compris les périphériques logiques) sont supprimées et complètement remplacées par la configuration contenue dans le fichier d'importation.
- Nous vous recommandons d'importer uniquement un fichier de configuration sur le même châssis Firepower 4100/9300 à partir duquel la configuration a été exportée.
- La version logicielle de la plateforme du châssis Firepower 4100/9300 vers lequel vous importez doit être la même que lorsque l'exportation a eu lieu. Sinon, la réussite de l'opération d'importation n'est pas garantie. Nous vous recommandons d'exporter une configuration de sauvegarde chaque fois que le châssis Firepower 4100/9300 est mis à niveau ou rétrogradé.
- Les mêmes modules de réseau doivent être installés dans les mêmes logements sur le châssis Firepower 4100/9300 vers lequel vous importez qu'au moment de l'exportation.
- Les bonnes images d'applications logicielles doivent être installées sur le châssis Firepower 4100/9300 vers lequel vous importez le périphérique logique défini dans le fichier d'exportation que vous importez.
- Si le fichier de configuration importé contient un périphérique logique dont l'application est assortie d'un contrat de licence d'utilisateur final (CLUF), vous devez accepter le CLUF pour cette application sur le châssis Firepower 4100/9300 avant d'importer la configuration, sinon l'opération échoue.

Selon le protocole de transport et la configuration du serveur distant, vous devrez peut-être saisir le mot de passe de l'utilisateur distant à des fins de connexion.

Vous pouvez vérifier l'état de l'importation et suivre sa progression en saisissant la commande **show fsm status**; consultez l'exemple suivant. Vous devrez peut-être saisir la commande plusieurs fois à mesure que la tâche progresse.

Exemple

Cet exemple montre comment importer un fichier XML contenant les paramètres de configuration du périphérique logique et de la plateforme à partir d'un serveur distant :

```
firepower # scope system
firepower /system # import-config scp://user1@192.168.1.2:/export/cfg-backup.xml enabled
Password:
Warning: After configuration import any changes on the breakout port configuration will
cause the system to reboot
firepower /system* # commit-buffer
firepower /system # show fsm status

Hostname: 192.168.1.2

    FSM 1:
        Remote Result: Not Applicable
        Remote Error Code: None
        Remote Error Description:
        Status: Import Wait For Switch
        Previous Status: Import Config Breakout
        Timestamp: 2016-01-03T15:45:03.963
        Try: 0
        Progress (%): 97
        Current Task: updating breakout port
configuration(FSM-STAGE:sam:dme:MgmtImporterImport:configBreakout)
```

Commandes associées

Commande	Description
cfg-export-policy	Configure une politique d'exportation.
export-config	Exporte la configuration système actuelle vers un serveur distant en tant que fichier XML.
set password-encryption-key	Spécifie une clé utilisée pour le chiffrement des informations sensibles lors de l'exportation de la configuration.

install

Pour installer un code d'autorisation de réservation, utilisez la commande **install**.

install *Code*

Description de la syntaxe

Code	Code d'autorisation de réservation obtenu à partir de Smart Software Manager.

Modes de commande

Mode réservation (/license/reservation)

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Si vous avez déjà généré le code d'autorisation, vous devez l'installer.

Exemple

Cet exemple montre comment installer un code d'autorisation de réservation :

```
FP9300-A# scope license
FP9300-A /license # scope reservation
FP9300-A /license/reservation # install <code>
FP9300-A /license/reservation* #
```

Commandes associées

Commande	Description
request universal	Génère un code de demande de réservation.
show license	Affiche les informations de licences actuelles.

install firmware

Pour installer un package de mise à niveau de micrologiciel téléchargé précédemment, utilisez la commande **install firmware**.

install firmware pack-version *version_number*

Description de la syntaxe

pack-version *version_number*	Spécifie la version du package de micrologiciel à installer. **Remarque** L'élément *version_number* du package n'est pas le nom du fichier image (bien qu'il fasse généralement partie du nom du fichier). Vous pouvez utiliser la commande **show** pour déterminer l'élément *version_number* du package.

Modes de commande

Mode installation de micrologiciel

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous devez disposer de privilèges d'administrateur pour utiliser cette commande. Le processus d'installation de la mise à niveau prend généralement entre 20 et 30 minutes. Le système redémarre au cours de ce processus.

Avant de lancer l'installation, passez en revue les défaillances critiques ou majeures et sauvegardez la configuration actuelle.

La mise à niveau est un processus à deux étapes : vérification du package, suivie de l'installation. Au début de chaque étape, il vous est demandé si vous souhaitez continuer. Si vous saisissez **non** à l'une ou l'autre de ces invites, le processus prend fin.

Vous pouvez utiliser la commande **show detail** pour surveiller le processus d'installation.

Exemple

Cet exemple montre comment installer un package de mise à niveau du micrologiciel téléchargé précédemment :

```
FP9300-A# scope firmware
FP9300-A /firmware # scope firmware-install
FP9300-A /firmware/firmware-install # install firmware pack-version 1.0.16
Verifying FXOS firmware package 1.0.16. Verification could take several minutes.
Do you want to proceed? (yes/no):yes

FXOS SUP ROMMON: Upgrade from 1.0.10 to 1.0.10
FXOS SUP FPGA : Upgrade from 1.04 to 1.05
This operation upgrades SUP firmware on Security Platform.
Here is the checklist of things that are recommended before starting the install operation
(1) Review current critical/major faults
(2) Initiate a configuration backup
Attention:
   The system will be reboot to upgrade the SUP firmware.
   The upgrade operation will take several minutes to complete.
   PLEASE DO NOT POWER RECYCLE DURING THE UPGRADE.
```

```
Do you want to proceed? (yes/no):yes
Upgrading FXOS SUP firmware software package version 1.0.10
command executed
```

Commandes associées

Commande	Description
scope firmware-install	Permet d´accéder au mode installation de micrologiciel.
show download-task	Affiche des information sur les téléchargements de package de micrologiciel.
show (firmware-install)	En mode installation de micrologiciel, affiche les informations sur le package de micrologiciel.
install firmware pack-version *version_number* **verify-only**	Vérifie le package de micrologiciel. **Remarque** Vous pouvez utiliser cette commande pour vérifier au préalable le package de micrologiciel avant de procéder à son installation.

install platform

Pour mettre à niveau le micrologiciel et le logiciel sur les composants de la plateforme de sécurité, utilisez la commande **install platform**.

install platform platform-vers *version_number*

Description de la syntaxe

platform-vers *version_number*	Spécifie la version du package de plateforme à installer.

Modes de commande

Mode installation automatique (/firmware/auto-install)

Historique des commandes

Version	Modification
1.4(1)	Commande ajoutée.

Instructions d'utilisation

Vous devez disposer de privilèges d'administrateur pour utiliser cette commande. Le processus de mise à niveau prend généralement entre 20 et 30 minutes.

Avant de lancer l'installation, passez en revue les défaillances critiques ou majeures et sauvegardez la configuration actuelle.

Vous pouvez utiliser la commande **show fsm status expand** en mode installation automatique pour surveiller le processus d'installation.

Pour terminer le processus d'installation de la mise à niveau, vous devez confirmer le redémarrage en attente de l'interconnexion de structures principale.

Exemple

Cet exemple montre comment installer un package de mise à niveau de plateforme :

```
FP9300-A# scope firmware
FP9300-A /firmware # scope auto-install
FP9300-A /firmware/auto-install # install platform platform-vers 2.3(1.51)
The currently installed FXOS platform software package is 2.2(2.19)

INFO: There is no service impact to install this FXOS platform software 2.3(1.51)

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup
Do you want to proceed? (yes/no):
```

Commandes associées

Commande	Description
download image	Télécharge une image logicielle FXOS sur le châssis Firepower 4100/9300.
show validate-task	Affiche l'état du processus de vérification d'image.

mgmt-port (connect local-mgmt)

Pour afficher et configurer l'état administratif des informations sur le port de gestion, utilisez la commande **mgmt-port** .

mgmt-port

Description de la syntaxe

mgmt-port	Affiche les informations sur le port de gestion.

Modes de commande

connect local-mgmt

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande affiche les informations sur le port de gestion.

Exemple

Cet exemple montre comment afficher les informations sur le port de gestion :

```
firepower#
firepower# connect local-mgmt...

firepower(local-mgmt)#mgmt-port
  <CR>
  no-shut  Management port up  <====== Administratively enable the chassis management
interface.
  shut     Management port down <====== Administratively disable/shutdown the chassis
management interface.
```

ping (connect local-mgmt)

Pour tester la connectivité du réseau de base en envoyant un message ping à un autre appareil sur le réseau avec son adresse IPv4, utilisez la commande **ping**.

ping {*hostname* | *IPv4_address*} [**count** *number_packets*] | [**deadline** *seconds*] | [**interval** *seconds*] | [**packet-size** *bytes*]

Description de la syntaxe

hostname	*IPv4_address*	Nom de domaine ou adresse IP de l'appareil à contacter. Le nombre maximal de caractères autorisé pour le nom de domaine est de 510.
count *number_packets*	(Facultatif) Nombre de paquets ping à envoyer. La plage est comprise entre 1 et 2 147 483 647 paquets.
deadline *seconds*	(Facultatif) Durée maximale pendant laquelle l'envoi de paquets se poursuit en l'absence de paquets de réponse; le ping prend alors fin. La plage est comprise entre 1 et 3 600 secondes.
interval *seconds*	(Facultatif) Intervalle en secondes entre les paquets ping. La plage est comprise entre 1 et 60 secondes; la valeur par défaut est de 1 seconde.
packet-size *bytes*	(Facultatif) Nombre d'octets de données à ajouter au paquet ping. La plage est comprise entre 32 et 65 500 octets. La valeur par défaut est de 56 octets, ce qui donne un paquet de 64 octets lorsqu'il est ajouté à l'en-tête ICMP de 8 octets.

Modes de commande

connect local-mgmt

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour tester la connectivité IP de base de l'interface de gestion du châssis vers un réseau externe en envoyant des paquets de demande d'écho ICMP à un hôte spécifié.

Exemple

Cet exemple montre comment se connecter au shell de gestion locale, puis envoyer douze pings à un autre appareil du réseau :

```
firepower# connect local-mgmt
firepower(local-mgmt)# ping 198.51.100.10 count 12
PING 198.51.100.10 (198.51.100.10) from 203.0.113.5 eth0: 56(84) bytes of data.
64 bytes from 198.51.100.10: icmp_seq=1 ttl=61 time=0.264 ms
64 bytes from 198.51.100.10: icmp_seq=2 ttl=61 time=0.219 ms
64 bytes from 198.51.100.10: icmp_seq=3 ttl=61 time=0.234 ms
64 bytes from 198.51.100.10: icmp_seq=4 ttl=61 time=0.205 ms
64 bytes from 198.51.100.10: icmp_seq=5 ttl=61 time=0.216 ms
64 bytes from 198.51.100.10: icmp_seq=6 ttl=61 time=0.251 ms
64 bytes from 198.51.100.10: icmp_seq=7 ttl=61 time=0.223 ms
64 bytes from 198.51.100.10: icmp_seq=8 ttl=61 time=0.221 ms
```

```
64 bytes from 198.51.100.10: icmp_seq=9 ttl=61 time=0.227 ms
64 bytes from 198.51.100.10: icmp_seq=10 ttl=61 time=0.224 ms
64 bytes from 198.51.100.10: icmp_seq=11 ttl=61 time=0.261 ms
64 bytes from 198.51.100.10: icmp_seq=12 ttl=61 time=0.261 ms

--- 198.51.100.10 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11104ms
rtt min/avg/max/mdev = 51.005/51.062/51.164/0.064 ms
firepower(local-mgmt)#
```

Commandes associées

Commande	Description
ping6	Teste la connectivité du réseau de base en envoyant un message ping à un autre appareil sur le réseau avec son adresse IPv6.
traceroute	Trace la route vers une destination spécifiée (adresse IPv4).

ping6 (connect local-mgmt)

Pour envoyer un message ping à un autre appareil sur le réseau en utilisant son adresse IPv6, utilisez la commande **ping6**.

ping6 {*hostname* | *IPv6_address*} [**count** *number_packets*] | [**deadline** *seconds*] | [**interval** *seconds*] | [**mtu-hint** {**do** | **dont** | **want**}] | [**packet-size** *bytes*]

Description de la syntaxe

hostname	*IPv6_address*	Nom de domaine ou adresse IP de l'appareil à contacter. Le nombre maximal de caractères autorisé pour le nom de domaine est de 510.
count *number_packets*	(Facultatif) Nombre de paquets ping à envoyer. La plage est comprise entre 1 et 2 147 483 647 paquets.
deadline *seconds*	(Facultatif) Durée maximale pendant laquelle l'envoi de paquets se poursuit en l'absence de paquets de réponse; le ping prend alors fin. La plage est comprise entre 1 et 3 600 secondes.
interval *seconds*	(Facultatif) Intervalle en secondes entre les paquets ping. La plage est comprise entre 1 et 60 secondes; la valeur par défaut est de 1 seconde.
mtu-hint {**do** | **dont** | **want**}	(Facultatif) Politique de découverte du chemin MTU; Un indice peut être : • **do** : interdit la fragmentation, même pour les paquets locaux; définit un indicateur de non-fragmentation (DF). • **dont** : interdit la fragmentation; ne définit pas d'indicateur DF. • **want** : effectue la découverte PMTU, fragmente localement lorsque la taille des paquets est importante.
packet-size *octets*	(Facultatif) Nombre d'octets de données à ajouter au paquet ping. La plage est comprise entre 32 et 65 500 octets. La valeur par défaut est de 56 octets, ce qui donne un paquet de 64 octets lorsqu'il est ajouté à l'en-tête ICMP de 8 octets.

Modes de commande

connect local-mgmt

Historique des commandes

Version	Modification
1.1(4)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour tester la connectivité IPv6 de base de l'interface de gestion du châssis vers un réseau externe en envoyant des paquets de demande d'écho ICMP à un hôte spécifié.

Exemple

Cet exemple montre comment se connecter au shell de gestion locale, puis envoyer douze pings à un autre appareil du réseau :

```
firepower# connect local-mgmt
firepower(local-mgmt)# ping6 2001:DB8:0:ABCD::1 count 12
PING 2001:DB8:0:ABCD::1 (2001:DB8:0:ABCD::1) from 2001:DB8:1::1 eth0: 56(84) bytes of data.
64 bytes from 2001:DB8:0:ABCD::1: icmp_seq=1 ttl=61 time=0.264 ms
64 bytes from 2001:DB8:0:ABCD::1: icmp_seq=2 ttl=61 time=0.219 ms
64 bytes from 2001:DB8:0:ABCD::1: icmp_seq=3 ttl=61 time=0.234 ms
64 bytes from 2001:DB8:0:ABCD::1: icmp_seq=4 ttl=61 time=0.205 ms
64 bytes from 2001:DB8:0:ABCD::1: icmp_seq=5 ttl=61 time=0.216 ms
64 bytes from 2001:DB8:0:ABCD::1: icmp_seq=6 ttl=61 time=0.251 ms
64 bytes from 2001:DB8:0:ABCD::1: icmp_seq=7 ttl=61 time=0.223 ms
64 bytes from 2001:DB8:0:ABCD::1: icmp_seq=8 ttl=61 time=0.221 ms
64 bytes from 2001:DB8:0:ABCD::1: icmp_seq=9 ttl=61 time=0.227 ms
64 bytes from 2001:DB8:0:ABCD::1: icmp_seq=10 ttl=61 time=0.224 ms
64 bytes from 2001:DB8:0:ABCD::1: icmp_seq=11 ttl=61 time=0.261 ms
64 bytes from 2001:DB8:0:ABCD::1: icmp_seq=12 ttl=61 time=0.261 ms

--- 2001:DB8:0:ABCD::1 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11104ms
rtt min/avg/max/mdev = 51.005/51.062/51.164/0.064 ms
firepower(local-mgmt)#
```

Commandes associées

Commande	Description
ping	Teste la connectivité du réseau de base en envoyant un message ping à un autre appareil sur le réseau avec son adresse IPv4.
traceroute6	Trace la route vers une destination spécifiée (adresse IPv6).

power

Pour mettre sous tension ou hors tension un module, utilisez la commande **power**.

power { **down** [**soft-followed-by-hard** | **soft-shut-down**] | **up** }

Description de la syntaxe

soft-followed-by-hard	(Facultatif) Vous pouvez utiliser ce mot clé mettre « progressivement » le module hors tension, en attendant jusqu'à 45 minutes que le système d'exploitation SSP s'arrête. Passé ce délai, le module est mis hors tension quel que soit l'état d'arrêt du système d'exploitation.
soft-shut-down	(Facultatif) Vous pouvez utiliser ce mot clé pour mettre « progressivement » le module hors tension, le système attendant indéfiniment l'arrêt du système d'exploitation SSP. Le module est mis hors tension uniquement après l'arrêt effectif du système d'exploitation SSP.

Modes de commande

Mode profil de service

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Si vous n'incluez pas l'un des mots clés facultatifs avec la commande **power down**, le module immédiatement mis hors tension, sans arrêt progressif de son système d'exploitation.

Nous vous recommandons de sauvegarder la configuration du module avant de le mettre hors tension.

Exemple

Cet exemple montre comment accéder au mode profil de service, puis mettre progressivement hors tension le module :

```
FP9300-A # scope service-profile server 1/1
FP9300-A /org/service-profile # power down soft-shut-down
FP9300-A /org/service-profile* # commit-buffer
FP9300-A /org/service-profile #
```

Commandes associées

Commande	Description
shutdown	Met l'appareil hors tension.

reboot

Pour redémarrer le châssis ou l'interconnexion de structure, utilisez la commande **reboot**.

```
(local-mgmt)# reboot
```

```
/chassis # reboot [no-prompt|reason]
```

Description de la syntaxe

	En mode gestion locale, cette commande ne contient aucun argument ou mot clé.
no-prompt	(Facultatif) En mode châssis, vous pouvez utiliser ce mot clé pour lancer le redémarrage immédiatement. Sinon, une commande **commit-buffer** est requise pour lancer le redémarrage.
reason	(Facultatif) En mode châssis, vous pouvez saisir une chaîne de texte à ajouter au journal de redémarrage; peut comporter jusqu'à 510 caractères.

Modes de commande

Mode châssis

Mode gestion locale

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Nous vous recommandons de sauvegarder la configuration système avant le redémarrage.

En mode gestion locale, cette commande ne contient aucun mot clé ou aucun option.

Remarque Nous vous recommandons d'utiliser cette commande en mode châssis, car elle permet un arrêt et un redémarrage « progressifs » du système.

Exemples

Cet exemple montre comment accéder à un shell de gestion locale et redémarrer le système :

```
FP9300-A # connect local-mgmt
FP9300-A (local-mgmt)# reboot
Before rebooting, please take a configuration backup.
Do you still want to reboot? (yes/no)::yes
nohup: ignoring input and appending output to `nohup.out'

Broadcast message from root (Fri Apr 13 17:12:49 2018):

All shells being terminated due to system /sbin/reboot
```

Cet exemple montre comment accéder au mode châssis et redémarrer le système :

```
FP9300-A # scope chassis 1
FP9300-A /chassis # reboot
This command will reboot the chassis when committed
FP9300-A /chassis* # commit-buffer
Starting chassis shutdown. Monitor progress with the command "show fsm status"
System is safe to power off after "System halted." message is seen
FP9300-A /chassis #
Broadcast message from root@DOC-FP9300-A (Fri Apr 13 16:27:04 2018):

All shells being terminated due to system /sbin/shutdown
```

Commandes associées

Commande	Description
shutdown	Met l'appareil hors tension.

reinstall

Pour modifier les paramètres de démarrage d'un périphérique logique, réinstallez l'instance d'application à l'aide de la commande **reinstall**.

reinstall

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope slot/scope app/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous pouvez modifier les paramètres de démarrage d'un périphérique logique. Vous pouvez réinstaller l'instance d'application en utilisant ces nouveaux paramètres ou enregistrer les modifications et la réinstaller ultérieurement.

Exemple

Cet exemple montre comment accéder au mode licence/licdebug et renouveler manuellement le certificat d'ID de logiciel Smart et les droits de licence.

```
FP9300-A # scope slot 2
FP9300-A /slot # scope app-instance asa cluster1
FP9300-A /slot/app-instance # reinstall app
FP9300-A /slot/app-instance # Do you want to reinstall the app now [Y/N]? Y
…
```

Commandes associées

Commande	Description
register	Modifie les paramètres de démarrage d'un périphérique logique pour redémarrer l'instance d'application.

register

Pour enregistrer un compte Smart Software Manager sur cet appareil Firepower 4100/9300, utilisez la commande **register**.

register idtoken *id_token*

Description de la syntaxe

id_token	Jeton d'enregistrement obtenur à partir de Smart Software Manager Satellite.

Modes de commande

Mode licence (/licence)

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Demandez et copiez le jeton d'enregistrement à partir de Smart Software Manager ou Smart Software Manager Satellite. Pour plus de renseignements, consultez le *Guide de l'utilisateur Cisco Smart Software Manager* .

Exemple

Cet exemple montre comment enregistrer cet appareil.

```
FP9300-A # scope license
FP9300-A /license # register idtoken ZGFmNWM5NjgtYmNjYS00ZWI3L
WE3NGItMWJkOGExZjIxNGQ0LTE0NjI2NDYx%0AMDIzNT
V8N3R0dXM1Z0NjWkdpR214eFZhMldBOS9CVnNEYnVKM1
FP9300-A /license #
```

Commandes associées

Commande	Description
deregister	La désinscription supprime l'appareil de votre compte; tous les droits de licence et certificats de l'appareil sont supprimés.

reinitialize

Pour reformater intégralement un module, utilisez la commande **reinitialize**.

reinitialize

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode logement

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

La réinitialisation d'un module efface complètement toutes les données d'application stockées. Sauvegardez tous les fichiers de configuration en cours d'exécution avant d'exécuter la commande **commit-buffer**.

Exemple

Cet exemple montre comment réinitialiser le module dans le logement 2.

```
FP9300-A # scope ssa
FP9300-A /ssa # scope slot 2
FP9300-A /ssa/slot # reinitialize
Warning: Reinitializing blade takes a few minutes. All the application data on blade will
get lost. Please backup application running config files before commit-buffer.
FP9300-A /ssa/slot* #
```

Commandes associées

Commande	Description
decommission	Désactive un serveur.

remove server

Pour supprimer un serveur précédemment désactivé de l'inventaire des périphériques, utilisez la commande **remove server**.

remove server {*id* | *chassis_id* / *blade_id*}

Description de la syntaxe

ID	Numéro de logement La plage valide est comprise entre 1 et 255.
chassis_id / *blade_id*	Numéros de châssis et de lame de serveur, au format n/n. **Remarque** Le numéro de châssis est toujours **1**.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Lorsque vous utilisez cette commande en mode châssis, vous devez spécifier le numéro d'ID de logement uniquement.

Exemple

Cet exemple montre comment supprimer un serveur désactivé :

```
FP9300-A# remove server 1/1
FP9300-A* # commit-buffer
FP9300-A#
```

Commandes associées

Commande	Description
decommission server	Désactive un serveur.
show server decommissioned	Affiche le(s) serveur(s) désactivé(s).

renew

Pour renouveler manuellement le certificat d'enregistrement du logiciel Smart et mettre à jour les droits sur tous les modules de sécurité, utilisez la commande **renew**.

renew

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode débogage de licence (/licence/licdebug)

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, le certificat d'ID est automatiquement renouvelé tous les six mois et le droit de licence tous les 30 jours. Vous pouvez renouveler manuellement l'enregistrement de l'un de ces éléments si votre accès à Internet est limité, par exemple, ou si vous apportez des modifications de licence dans Smart Software Manager, par exemple.

Exemple

Cet exemple montre comment accéder au mode licence/licdebug et renouveler manuellement le certificat d'ID de logiciel Smart et les droits de licence.

```
FP9300-A # scope license
FP9300-A /license # scope licdebug
FP9300-A /license/licdebug # renew
FP9300-A /license/licdebug #
```

Commandes associées

Commande	Description
register	Enregistre un compte Smart Software Manager sur cet appareil Firepower 4100/9300.

reset-password

Pour forcer l'utilisateur à modifier son mot de passe d'utilisateur, utilisez la commande **reset-password** .

reset-password *password*

Description de la syntaxe

password	Mot de passe de l'utilisateur lors de la connexion.

Modes de commande

scope security

Historique des commandes

Version	Modification
2.10(1)	Commande ajoutée.

Instructions d'utilisation

Vous pouvez forcer l'utilisateur à modifier son mot de passe lors de sa prochaine connexion.

Exemple

Cet exemple montre comment accéder au mode sécurité, puis réinitialiser le mot de passe :

```
firepower# scope security
firepower# create local-user admin2
firepower /security/local-user # set
  account-status  Account status
  email           Email
  expiration      User account expiration
  firstname       FirstName
  lastname        LastName
  password        Password
  phone           Phone
  reset-password  Change password at next login

firepower /security/local-user # set reset-password
  no   No
  yes  Yes
```

Commandes associées

Commande	Description
set password	Définit le mot de passe du compte d'utilisateur :
generate password	Génère un mot de passe pour le compte d'utilisateur :

request universal

Pour générer un code de demande de réservation, utilisez la commande **request universal**.

request universal

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode réservation (/license/reservation)

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Avant de commencer, vous devez acheter des licences permanentes pour qu'elles soient disponibles dans Smart Software Manager. Tous les comptes ne sont pas approuvés pour la réservation de licence permanente. Assurez-vous d'avoir l'approbation de Cisco pour cette fonctionnalité avant de tenter de la configurer.

Activez la réservation de licence avant de tenter d'attribuer une licence permanente à votre châssis Firepower 4100/9300.

Après avoir exécuté cette commande, utilisez **show license resvcode** pour afficher la demande de réservation, l'autorisation et les codes de retour générés.

Exemple

Cet exemple montre comment générer un code de demande de réservation et afficher les codes générés :

```
FP9300-A# scope license
FP9300-A /license # scope reservation
FP9300-A /license/reservation # request universal
FP9300-A /license/reservation # show license resvcode
Warning : generating the reservation code takes a few seconds.
Please run the 'show license resvcode' again if the code is not available.
Reservation request code :
<empty>
Reservation authorization code :
<empty>
Reservation return code :
<empty>
```

Commandes associées

Commande	Description
enable reservation	Active la réservation de licence permanente.
show license	Affiche les informations de licences actuelles.

restart

Pour modifier les paramètres de démarrage d'un périphérique logique, redémarrez l'instance d'application à l'aide de la commande **restart**.

restart

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope slot/scope app/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous pouvez modifier les paramètres de démarrage d'un périphérique logique. Vous pouvez ensuite redémarrer immédiatement l'instance d'application en utilisant ces nouveaux paramètres ou enregistrer les modifications et la redémarrer ultérieurement.

Cet exemple montre comment redémarrer une application :

```
FP9300-A # scope slot 2
FP9300-A /slot # scope app-instance asa cluster1
FP9300-A /slot /app-instance # restart app
FP9300-A /slot /app-instance # Do you want to restart now [Y/N]? Y
```

Commandes associées

Commande	Description
reinstall	Réinstalle l'instance d'application.

return

Pour générer un code de retour de licence permanente, utilisez la commande **return**.

return [*Code*]

Description de la syntaxe

Code	(Facultatif) Code de licence obtenu depuis Smart Software Manager.

Modes de commande

Mode réservation (/license/reservation)

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Si vous n'avez plus besoin d'une licence permanente, vous devez officiellement la retourner à Smart Software Manager. À défaut, la licence reste à l'état « en cours d'utilisation » et ne peut pas être réutilisée ailleurs.

Lorsque vous saisissez cette commande, le châssis Firepower 4100/9300 n'est plus sous licence et passe à l'état d'évaluation.

Pour terminer le retour, rendez-vous sur https://software.cisco.com/#SmartLicensing-Inventory, localisez votre châssis Firepower 4100/9300 à l'aide de son identifiant universel d'appareil (UDI), puis supprimez l'instance de produit.

Exemple

Cet exemple montre comment retourner une licence permanente :

```
FP9300-A# scope license
FP9300-A /license # scope reservation
FP9300-A /license/reservation # return
FP9300-A /license/reservation #
```

Commandes associées

Commande	Description
show license udi	Affiche l'identifiant universel d'appareil (UDI) FXOS pour vous permettre de trouver votre instance FXOS dans Smart Software Manager.

PARTIE II

Commandes S

- Commandes scope, à la page 181
- Commandes set, à la page 253
- Commandes sh, à la page 391

Commandes scope

- scope, à la page 183
- scope adapter, à la page 185
- scope app-software, à la page 186
- scope auto-install, à la page 187
- scope auto-macpool, à la page 188
- scope banner, à la page 190
- scope cabling, à la page 191
- scope callhome, à la page 192
- scope card, à la page 193
- scope cfg-export-policy, à la page 194
- scope cfg-export-reminder, à la page 195
- scope chassis, à la page 196
- scope cimc, à la page 197
- scope cloud-connector, à la page 198
- scope default-auth, à la page 199
- scope environment-features, à la page 200
- scope eth-uplink, à la page 201
- scope eth-server, à la page 202
- scope export-config, à la page 203
- scope fabric, à la page 204
- scope fabric-interconnect, à la page 206
- scope fan-module, à la page 207
- scope faulty-policy, à la page 208
- scope firmware, à la page 209
- scope firmware-install, à la page 210
- scope flow-control, à la page 211
- scope health monitoring policy, à la page 212
- scope hw-crypto, à la page 214
- scope import-config, à la page 216
- scope info-policy, à la page 217
- scope interface, à la page 218
- scope ipsec, à la page 220
- scope ipv6-config, à la page 221

- scope ldap, à la page 222
- scope licdebug, à la page 223
- scope license, à la page 224
- scope mem-leak-logging, à la page 225
- scope monitoring, à la page 226
- scope network-features, à la page 227
- scope org, à la page 228
- scope packet-capture, à la page 229
- scope password-profile, à la page 230
- scope profile, à la page 231
- scope qos, à la page 232
- scope radius, à la page 233
- scope reservation, à la page 234
- scope security, à la page 235
- scope server, à la page 236
- scope server-features, à la page 237
- scope service-profile, à la page 238
- scope services, à la page 239
- scope slot, à la page 240
- scope ssa, à la page 241
- scope stats-collection-policy, à la page 242
- scope stats-threshold-policy, à la page 244
- scope storage-features, à la page 247
- scope system, à la page 248
- scope tacacs, à la page 249
- scope telemetry, à la page 250
- scope vnic, à la page 251
- sub scopes (scope fabric-interconnect), à la page 252

scope

Pour accéder à un objet géré existant, utilisez la commande **scope** pertinente dans le mode de commande approprié.

scope *object_type* *name* [*parameters*]

Description de la syntaxe

object_type	Type d'objet à saisir. Les exemples comprennent le compte d'utilisateur local et l'organisation.
name	Nom de l'objet spécifique à saisir.
paramètres	(Facultatif) Ensemble des propriétés ou paramètres supplémentaires nécessaires pour identifier l'objet. Avec cette commande, le *nom* est généralement suffisant pour identifier un objet. Pour plus de renseignements, consultez la description de la commande **create** du type d'objet spécifique.

Modes de commande

Selon le type d'objet ciblé; pour plus de renseignements, consultez la description de la commande **create** du type d'objet spécifique.

Historique des commandes

Pour plus de renseignements sur l'historique, consultez la description de la commande **create** du type d'objet spécifique.

Instructions d'utilisation

Les objets sont des représentations abstraites de composants physiques ou d'entités logiques qui peuvent être gérés. Par exemple, les châssis, les modules de sécurité, les modules de réseau, les ports et les processeurs sont des composants physiques représentés sous forme d'objets gérés, tandis que les licences, les rôles d'utilisateur et les politiques de plateforme sont des entités logiques représentées sous forme d'objets gérés.

FXOS fournit quatre commandes générales pour la gestion des objets : **create**, **delete**, **enter** et **scope**. Par exemple, vous pouvez créer un compte d'utilisateur local, en supprimer un, ou y accéder pour lui attribuer ou modifier des propriétés. Vous pouvez également gérer directement le compte d'utilisateur local pour lui attribuer ou modifier des propriétés.

En général, les mots clés et les options disponibles pour chacune de ces commandes de gestion d'objets sont les mêmes. Nous ne détaillons donc que la version **create** des différentes commandes d'objet. En d'autres termes, pour plus de renseignements sur la commande **delete** d'un objet particulier, reportez-vous à la description de la commande **create** de cet objet. Par exemple, reportez-vous à create local-user, à la page 83 pour des informations sur le ciblage d'un compte d'utilisateur local existant.

Exemple

Cet exemple montre comment accéder au mode sécurité, accéder à un compte d'utilisateur local et afficher les détails correspondants :

```
firepower # scope security
firepower /security # scope local-user test_user
firepower /security/local-user # show detail
Local User test_user:
    First Name: test
    Last Name: user
    Email: test_user@testuser.com
```

```
    Phone:
    Expiration: Never
    Password: ****
    User lock status: Not Locked
    Account status: Active
    User Roles:
        Name: admin
        Name: read-only
    User SSH public key:
firepower /security/local-user #
```

Commandes associées

Commande	Description
create local-user	Crée un compte d'utilisateur local.
enter local-user	Ajoute ou modifie un compte d'utilisateur local.
delete local-user	Supprime un compte d'utilisateur local existant.

scope adapter

Pour accéder au mode adaptateur, utilisez la commande **scope adapter**.

scope adapter {*rack_server* / *id* | *chassis* / *server* / *id*}

Description de la syntaxe

rack_server / *id*	Emplacement de l'adaptateur spécifié à l'aide des ID du serveur rack et de l'adaptateur saisis au format n/n.
chassis / *server* / *id*	Emplacement de l'adaptateur spécifié à l'aide des ID du châssis, du serveur et de l'adaptateur saisis au format n/n/n. **Remarque** L'ID de châssis est toujours **1**.

Modes de commande

Mode EXEC

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

En mode adaptateur, vous pouvez activer ou mettre à jour une version de micrologiciel, afficher diverses données spécifiques à l'adaptateur et explorer les interfaces Ethernet hôtes et externes.

Exemple

Cet exemple montre comment accéder au mode adaptateur à l'aide des ID du châssis, du serveur et de l'adaptateur :

```
firepower# scope adapter 1/1/1
firepower /chassis/server/adapter #
```

Commandes associées

Commande	Description
connect adapter	Se connecte au shell de commande d'un adaptateur spécifique.
scope chassis	Permet d'accéder au mode châssis.

scope app-software

Pour accéder au mode logiciel d'application, utilisez la commande **scope app-software**.

scope app-software

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope ssa/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous pouvez utiliser la commande **download image** en mode logiciel d'application pour copier une image logicielle de périphérique logique sur le châssis Firepower 4100/9300.

Exemple

Cet exemple montre comment accéder au mode logiciel d'application :

```
firepower# scope ssa
firepower /ssa # scope app-software
firepower /ssa/app-software #
```

Commandes associées

Commande	Description
download image	Copie une image logicielle de périphérique logique sur le châssis Firepower 4100/9300
show download-task	Affiche la progression du téléchargement du fichier image.

scope auto-install

Pour accéder au mode installation automatique des mises à jour d'infrastructure, utilisez la commande **scope auto-install**.

scope auto-install

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode micrologiciel (/firmware)

Historique des commandes

Version	Modification
1.4(1)	Commande ajoutée.

Instructions d'utilisation

Aucune

Exemple

Cet exemple montre comment accéder au mode micrologiciel, puis au mode installation automatique :

```
FP9300-A# scope firmware
FP9300-A /firmware # scope auto-install
FP9300-A /firmware/auto-install #
```

Commandes associées

Commande	Description
install platform	Met à niveau les composants d'infrastructure UCS (UCSM, FI et IOM) vers la version d'infrastructure spécifiée.

scope auto-macpool

Pour gérer l'ensemble d'adresses MAC de l'interface d'instance de contenant, utilisez la commande **scope auto-macpool**.

scope auto-macpool

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope ssa/

Historique des commandes

Version	Modification
2.4(1)	Commande ajoutée.

Instructions d'utilisation

Le châssis FXOS génère automatiquement les adresses MAC pour les interfaces d'instance et garantit qu'une interface partagée dans chaque instance utilise une adresse MAC unique.

Si vous attribuez manuellement une adresse MAC à une interface partagée dans l'application, l'adresse MAC attribuée manuellement est utilisée. Si vous supprimez ultérieurement l'adresse MAC manuelle, l'adresse générée automatiquement est utilisée. Dans les rares cas où l'adresse MAC générée entre en conflit avec une autre adresse MAC privée de votre réseau, nous vous suggérons de définir manuellement l'adresse MAC pour l'interface dans l'application.

Étant donné que les adresses générées automatiquement commencent par A2, vous ne devez pas commencer les adresses MAC manuelles par A2 en raison du risque de chevauchement d'adresses.

Remarque Même si vous ne partagez pas une sous-interface, si vous configurez manuellement des adresses MAC, veillez à utiliser des adresses MAC uniques pour toutes les sous-interfaces sur la même interface parente afin de garantir une classification correcte.

Le châssis FXOS génère l'adresse MAC en utilisant le format suivant :

A2*xx*.*yyzz*.*zzzz*

Où *xx*.*yy* est un préfixe défini par l'utilisateur ou un préfixe défini par le système, et *zz*.*zzzz* est un compteur interne généré par le châssis. Le préfixe défini par le système correspond aux 2 octets inférieurs de la première adresse MAC dans l'ensemble d'adresses MAC gravées qui est programmée dans la mémoire IDPROM. Utilisez **connect fxos**, puis **show module** pour afficher l'ensemble des adresses MAC. Par exemple, si la plage d'adresses MAC affichée pour le module 1 va de b0aa.772f.f0b0 à b0aa.772f.f0bf, le préfixe du système sera f0b0.

Le préfixe défini par l'utilisateur est un entier qui est converti en hexadécimal. Pour donner un exemple de la façon dont le préfixe défini par l'utilisateur est utilisé, si vous définissez un préfixe de 77, le châssis convertit 77 dans la valeur hexadécimale 004D (*yyxx*). Lorsqu'il est utilisé dans l'adresse MAC, le préfixe est inversé (*xxyy*) pour correspondre à la forme native du châssis :

A2**4D**.**00***zz*.*zzzz*

Pour un préfixe 1009 (03F1), l'adresse MAC est :

A2**F1**.**03***zz*.*zzzz*

Exemple

Cet exemple montre comment accéder au mode mac-pool :

```
firepower# scope ssa
firepower /ssa # scope auto-macpool
firepower /ssa/auto-macpool #
```

Commandes associées

Commande	Description
scope ssa	Permet d'accéder au mode ssa.
set prefix	Définit le préfixe de l'adresse MAC.
show mac-address	Affiche les adresses MAC attribuées.

scope banner

Pour accéder au mode gestion de bannière, utilisez la commande **scope banner**.

scope banner

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope security/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Ce mode vous permet de gérer la bannière présentée par l'appareil avant la connexion de l'utilisateur.

Exemple

Cet exemple montre comment accéder au mode bannière et afficher la bannière de préconnexion actuelle :

```
firepower # scope security
firepower /security # scope banner
firepower /security/banner # show pre-login-banner

Pre login banner:
    Message
    -------
    Firepower-9300-2
Western Data Center

firepower /security/banner #
```

Commandes associées

Commande	Description
clear message	Supprime le texte d'une bannière de préconnexion existante; l'objet de bannière en lui-même n'est pas supprimé.
create pre-login-banner	Crée une bannière à présenter avant l'écran de connexion; l'objet de bannière est initialement vide.
set message	Ajoute ou remplace les lignes de texte présentées comme bannière de préconnexion.

scope cabling

Pour accéder au mode câblage, utilisez la commande **scope cabling**.

scope cabling

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode EXEC

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous pouvez accéder au mode structure à partir du mode câblage, où vous pouvez afficher et gérer les répartitions de ports.

Exemple

Cet exemple montre comment accéder au mode câblage :

```
FP9300-A # scope cabling
FP9300-A /cabling #
```

Commandes associées

Commande	Description
scope fabric-interconnect	Accéder au mode interconnexion de structure.

scope callhome

Pour accéder au mode Callhome, utilisez la commande **scope callhome**.

scope callhome

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode surveillance

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous n'avez pas besoin d'accéder à ce mode avec un objet géré.

Exemple

Cet exemple montre comment accéder au mode Callhome à partir du mode surveillance :

```
FP9300-A#scope monitoring
FP9300-A /monitoring # scope callhome
FP9300-A /monitoring/callhome #
```

Commandes associées

Commande	Description
show callhome	Affiche des informations de configuration et d'état sur Call Home.

scope card

Pour accéder au mode administratif pour une carte de structure spécifique, utilisez la commande **scope card**.

scope card *card_ID*

Description de la syntaxe

card_ID	Identifiant numérique de la carte de structure.

Modes de commande

scope fabric-interconnect/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

En mode carte, vous pouvez utiliser la carte de structure hors ligne ou en ligne.

Exemple

Cet exemple montre comment accéder au mode carte et afficher les commandes disponibles :

```
firepower# scope fabric-interconnect
firepower /fabric-interconnect # scope card 2
firepower /fabric-interconnect/card # ?
  acknowledge  Acknowledge
  scope        Changes the current mode
  set          Set property values
  show         Show system information

firepower /fabric-interconnect/card #
```

Commande	Description
set adminstate	Met une carte de structure hors ligne ou en ligne.

scope cfg-export-policy

Pour accéder à la politique d'exportation de la configuration, utilisez la commande **scope cfg-export-policy**.

scope cfg-export-policy*name*

Description de la syntaxe

name	Nom de la politique d'exportation de la configuration à saisir. Vous ne pouvez pas créer ou supprimer de politique d'exportation de configuration. Vous pouvez uniquement configurer la politique par défaut existante; saisissez **default** comme nom de politique.

Modes de commande

scope org/

Historique des commandes

Version	Modification
2.0.1	Commande ajoutée.

Instructions d'utilisation

Vous ne pouvez pas créer ou supprimer de politique d'exportation de configuration; vous pouvez uniquement configurer la politique par défaut existante.

Exemple

Cet exemple montre comment accéder à la politique d'exportation de configuration et afficher les détails sur ses paramètres actuels :

```
firepower # scope org
firepower /org # scope cfg-export-policy default
firepower /org/cfg-export-policy # show detail
Config Export policy:
    Name: default
    Description: Configuration Export Policy
    Admin State: Enable
    Protocol: Ftp
    Hostname: 192.168.1.2
    User: user1
    Remote File: /export/cfg-backup.xml
    Schedule: Daily
    Port: Default
    Current Task:
firepower /org/cfg-export-policy #
```

Commandes associées

Commande	Description
export-config	Exporte la configuration système actuelle vers un serveur distant en tant que fichier XML; crée un objet de configuration d'exportation.
import-config	Copie un fichier de configuration XML précédemment exporté vers cet appareil.
set password-encryption-key	Spécifie une clé utilisée pour le chiffrement des informations sensibles lors de l'exportation de la configuration.

scope cfg-export-reminder

Pour accéder à l'objet de rappel d'exportation de configuration, utilisez la commande **scope cfg-export-reminder**.

scope cfg-export-reminder

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope org/

Historique des commandes

Version	Modification
2.0.1	Commande ajoutée.

Instructions d'utilisation

Vous ne pouvez pas créer ou supprimer un objet de rappel d'exportation de configuration; vous pouvez uniquement configurer l'objet de rappel existant.

Exemple

Cet exemple montre comment accéder à l'objet de rappel d'exportation de configuration et afficher ses paramètres actuels :

```
firepower # scope org
firepower /org # scope cfg-export-reminder
firepower /org/cfg-export-reminder # show

Config Export Reminder:
    Config Export Reminder (Days): 30
    AdminState: Enable
firepower /org/cfg-export-reminder #
```

Commandes associées

Commande	Description
import-config	Copie un fichier de configuration XML précédemment exporté vers cet appareil.
scope cfg-export-policy	Permet d'accéder à la politique d'exportation de la configuration.
set password-encryption-key	Spécifie une clé utilisée pour le chiffrement des informations sensibles lors de l'exportation de la configuration.

scope chassis

Pour accéder au mode châssis, utilisez la commande **scope chassis**.

scope chassis *chassis_id*

Description de la syntaxe

chassis_id	Numéro d'identification du châssis. Cette valeur est toujours **1**.

Modes de commande

Mode EXEC

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment accéder au mode châssis :

```
firepower# scope chassis 1
firepower /chassis #
```

Commandes associées

Commande	Description
show chassis	Affiche les informations sur le châssis.

scope cimc

Pour accéder au mode cimc, utilisez la commande **scope cimc**.

scope cimc

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope chassis, scope server.

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Vous n'avez pas besoin d'accéder à ce mode avec un objet géré.

Exemple

Cet exemple montre comment accéder au mode cimc :

```
tb-03# scope chassisss
tb-03 /chassis # scope server
tb-03 /chassis/server # scope cimc
tb-03 /chassis/server/cimc #
```

Commandes associées

Commande	Description
Acknowledge	Confirmation
Activate	Activer le composant avec la version d'image spécifiée.
Create	Créer des objets gérés.
Delete	Supprimer des objets gérés.
Enter	Accéder à un objet géré.
Reset	Réinitialiser des objets gérés.
Scope	Modifie le mode actuel.
Show	Afficher les données système.
Update	Mettre à jour le micrologiciel de sauvegarde avec la version d'image spécifiée.

scope cloud-connector

Pour accéder au mode connecteur infonuagique, utilisez la commande **scope cloud-connector**.

scope cloud-connector

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode EXEC

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment accéder au mode connecteur infonuagique :

```
FP9300-A # scope cloud-connector
FP9300-A /cloud-connector #
```

Commandes associées

Commande	Description
show cloud-connector	Affiche des informations sur la configuration du connecteur infonuagique.

scope default-auth

Pour accéder au mode d'authentification par défaut, utilisez la commande **scope default-auth**.

scope default-auth

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode sécurité

Domaine d'authentification (/security/auth-domain)

Historique des commandes

Version	Modification
1.4(1)	Commande ajoutée.

Instructions d'utilisation

Dans ce mode, utilisez les commandes **set** pour configurer les paramètres d'authentification par défaut tels que les valeurs de service d'authentification et de délai d'expiration de session.

Un domaine d'authentification doit être créé avant d'utiliser cette commande pour accéder au mode d'authentification par défaut d'un domaine.

Exemple

Cet exemple montre comment accéder au mode sécurité, puis en mode d'authentification par défaut :

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth #
```

Commandes associées

Commande	Description
set realm	Définit le service d'authentification par défaut.
show	Affiche les paramètres d'authentification par défaut.

scope environment-features

Pour accéder aux fonctionnalités d'environnement en mode configuration, utilisez la commande **scope environment-features**.

scope environment-features

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Scope system

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Vous n'avez pas besoin d'accéder à ce mode avec un objet géré.

Exemple

Cet exemple montre comment accéder au mode fonctionnalités d'environnement :

```
firepower # scope system
firepower /system # scope environment-features
firepower /system/environment-features # show
```

Commandes associées

Commande	Description
show	Affiche les informations sur les fonctionnalités d'environnement du domaine.

scope eth-uplink

Pour accéder au mode liaison ascendante Ethernet, utilisez la commande **scope eth-uplink**.

scope eth-uplink

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode EXEC

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous n'avez pas besoin d'accéder à ce mode avec un objet géré.

Exemple

Cet exemple montre comment accéder au mode liaison ascendante Ethernet :

```
firepower#scope eth-uplink
firepower /eth-uplink #
```

Commandes associées

Commande	Description
show	Affiche les informations sur la liaison ascendante Ethernet.

scope eth-server

Pour accéder au mode serveur Ethernet, utilisez la commande **scope eth-server**.

scope eth-server

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode EXEC

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Vous n'avez pas besoin d'accéder à ce mode avec un objet géré.

Exemple

Cet exemple montre comment accéder au mode serveur Ethernet :

```
firepower#scope eth-server
firepower /eth-server #
```

Commandes associées

Commande	Description
show	Affiche les informations sur le serveur Ethernet.

scope export-config

Pour accéder à un objet de configuration d'exportation existant, utilisez la commande **scope export-config**.

scope export-config*nom d'hôte*

Description de la syntaxe

nom d'hôte	Identifiant de l'objet de configuration d'exportation; il s'agit du nom ou de l'adresse IP du serveur distant sur lequel la configuration a été sauvegardée.

Modes de commande

scope system/

Historique des commandes

Version	Modification
1.1.(1)	Commande ajoutée.

Instructions d'utilisation

Un objet de configuration d'exportation est créé lorsque vous exécutez une commande **export-config** pour sauvegarder la configuration actuelle du périphérique logique et de la plateforme, et que la commande **scope export-config** est utilisée pour accéder à l'objet et modifier ses paramètres. Aucune commande **create** ou **enter** n'est associée aux objets de configuration d'exportation. Une commande **delete** vous permet supprimer un objet de configuration d'exportation.

Exemple

Cet exemple montre comment accéder à un objet de configuration précédemment exporté :

```
firepower # scope system
firepower /system # scope export-config 192.168.1.2
firepower /system/export-config #
```

Commandes associées

Commande	Description
cfg-export-policy	Configure une politique d'exportation de configuration.
delete export-config	Supprime un objet de configuration d'exportation existant.
export-config	Exporte la configuration système actuelle vers un serveur distant en tant que fichier XML; crée un objet de configuration d'exportation.

scope fabric

Pour accéder au mode structure, utilisez la commande **scope fabric**.

scope fabric [**a**]

Description de la syntaxe

a	Spécifie la structure A. Il n'existe qu'une structure sur les appareils Firepower. L'utilisation de ce mot clé est facultative.

Modes de commande

scope eth-uplink, scope eth-server

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

En mode structure, vous pouvez gérer les interfaces, les canaux de ports, les interfaces agrégées et les VLAN.

Exemple

Cet exemple montre comment accéder au mode structure :

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric #
```

```
firepower# scope eth-server
firepower /eth-server # scope fabric
firepower /eth-server/fabric #
```

Commandes associées

Commande	Description
show interface	En mode structure, répertorie les informations pour toutes les interfaces de l'appareil.
show port-channel	En mode structure, répertorie les informations et l'état de tous les canaux de ports.
show fabric-port-channel	En mode structure, répertorie les informations et l'état de tous les canaux de ports.
show fault	En mode structure, répertorie toutes les défaillances.
show detail	Affiche des informations sur la structure.
show event	Affiche des informations sur les événements FSM.
show expand	Affiche des informations développées sur la structure. Le mot clé de détail est disponible avec cette option.

Commande	Description
show fsm	Affiche des informations sur le FSM pour l'application actuelle selon le mot clé spécifié. État : affiche des informations sur l'état du FSM. Tâche : affiche des informations sur la tâche du FSM
show interface	Affiche l'état de l'interface Ethernet.

scope fabric-interconnect

Pour accéder au mode interconnexion de structure, utilisez la commande **scope fabric-interconnect** .

scope fabric-interconnect a

Description de la syntaxe

a	Spécifie la structure A. Il n'existe qu'une structure sur les appareils Firepower.

Modes de commande

Mode EXEC

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment accéder au mode interconnexion de structure :

```
firepower# scope fabric-interconnect a
firepower /fabric-interconnect #
```

Commandes associées

Commande	Description
show fabric-interconnect	Affiche les informations sur l'interconnexion de structures.

scope fan-module

Pour accéder à un module de ventilation spécifique, utilisez la commande **scope fan-module** en mode châssis.

scope fan-module {**1** *module_id*}

Description de la syntaxe

tray_id	L'élément *tray_id* est toujours **1**.
module_id	Identifie le module de ventilation spécifique auquel accéder; la valeur peut être comprise entre 1 et 8.

Modes de commande

scope chassis/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment accéder au mode module de ventilation :

```
firepower# scope chassis
firepower /chassis # scope fan-module 1 2
firepower /chassis/fan-module #
```

Commandes associées

Commande	Description
scope fan	Cible un ventilateur spécifique.

scope faulty-policy

Pour accéder à la politique en matière de défaillances pour l'une des zones fonctionnelles du système, utilisez la commande **scope faulty policy**.

scope faulty policy

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope monitoring

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Vous n'avez pas besoin d'accéder à ce mode avec un objet géré.

Commandes associées

Commande	Description
Show detail	Affiche des informations détaillées sur la politique en matière de défaillances du système.
Set Ack-action	Spécifie l'action de confirmation.
Set Clear-action	Spécifie l'action d'effacement.
Set Clear-interval	Spécifie l'intervalle d'effacement.
Set Flap-interval	Spécifie l'intervalle d'oscillation.
Set Retention-interval	Spécifie l'intervalle de rétention. (jj:hh:mm:ss)

scope firmware

Pour accéder au mode micrologiciel, utilisez la commande **scope firmware**.

scope firmware

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode EXEC

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous n'avez pas besoin d'accéder à ce mode avec un objet géré.

Exemple

Cet exemple montre comment accéder au mode micrologiciel :

```
firepower# scope firmware
firepower /firmware #
```

Commandes associées

Commande	Description
show server firmware	Affiche les informations sur le micrologiciel du serveur.
show server version	Affiche la version du micrologiciel du serveur.

scope firmware-install

Pour accéder au mode installation de micrologiciel, utilisez la commande **scope firmware-install**.

scope firmware-install

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode micrologiciel

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette portée pour mettre à jour le micrologiciel du système avec un package de micrologiciel précédemment téléchargé.

Exemple

Cet exemple montre comment accéder au mode installation de micrologiciel :

```
FP9300-A# scope firmware
FP9300-A /firmware # scope firmware-install
FP9300-A /firmware-install #
```

Commandes associées

Commande	Description
download image	Télécharge un ensemble de micrologiciels.
install firmware	Installe un ensemble de micrologiciels.

scope flow-control

Pour accéder au mode contrôle de flux, utilisez la commande **scope flow-control**.

scope flow-control

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope eth-uplink/

Historique des commandes

Version	Modification
1.1.1	Commande ajoutée.

Instructions d'utilisation

Les politiques de contrôle de flux déterminent si les ports Ethernet envoient et reçoivent des trames de pause IEEE 802.3x lorsque le tampon de réception d'un port atteint sa pleine capacité. Ces trames de pause demandent que le port de transmission arrête d'envoyer des données pendant quelques millisecondes jusqu'à ce que le tampon soit libéré. Pour que le contrôle de flux fonctionne entre les appareils, vous devez activer les paramètres de contrôle de flux d''envoi et de réception correspondants pour les deux appareils.

La politique par `défaut` désactive le contrôle d'envoi et de réception et définit la priorité pour la négociation automatique.

Exemple

L'exemple suivant montre comment accéder au mode contrôle de flux et afficher les informations sur la politique actuelle :

```
firepower # scope eth-uplink
firepower /eth-uplink # scope flow-control
firepower /eth-uplink/flow-control # show policy detail
Flowctrl policy:
    Name: default
    receive: Off
    send: Off
    Prio: Auto
firepower /eth-uplink/flow-control #
```

Commandes associées

Commande	Description
create policy	Ajoute une nouvelle politique de contrôle de flux nommée.
set	En mode contrôle de flux/politique, définit les propriétés de la politique de contrôle de flux.
show policy	Affiche les valeurs de propriété d'une politique de contrôle de flux.

scope health monitoring policy

Mesures d'utilisation de la mémoire

La collecte des statistiques de mémoire peut être activée ou désactivée à l'aide de l'interface de ligne de commande, sous **scope** « stats-collection-memory ». Par défaut, elle est activée.

Un seuil de défaillance peut également être défini pour toutes les défaillances de surveillance de la mémoire. La valeur de seuil peut être comprise entre 50 et 99. Par défaut, elle est définie sur 95 %.

scope health-monitoring-policy
scope stats-collection-memory
enable | disable
set fault-threshold <threshold-value>

Modes de commande

Mode surveillance

Historique des commandes

Version	Modification
2.11.1	Cette commande a été introduite.

Instructions d'utilisation

Cette commande active ou désactive la surveillance de la mémoire et modifie également la valeur du seuil de défaillance de toutes les défaillances de surveillance de la mémoire.

Exemple

```
firepower# scope monitoring
firepower /monitoring # scope health-monitoring-policy
firepower /monitoring/health-monitoring-policy # scope stats-collection-memory
firepower /monitoring/health-monitoring-policy/stats-collection-memory # set fault-threshold
 75
firepower /monitoring/health-monitoring-policy/stats-collection-memory # disable
firepower /monitoring/health-monitoring-policy/stats-collection-memory* # commit-buffer
firepower /monitoring/health-monitoring-policy/stats-collection-memory # show
Memory stats collection policy:
Admin State Fault-Threshold (%)
-----------
Disabled 75
firepower /monitoring/health-monitoring-policy/stats-collection-memory # show detail
Admin State: Disabled
Fault Threshold (%): 75
```

Mesure d'utilisation du processeur

La collecte des statistiques de processeur peut être activée ou désactivée à l'aide de l'interface de ligne de commande, sous scope « stats-collection-cpu ». Par défaut, elle est activée.

Un seuil de défaillance peut également être défini pour toutes les défaillances de surveillance du processeur. La valeur de seuil peut être comprise entre 50 et 99. Par défaut, elle est définie sur 90 %.

scope health-monitoring-policy
scope stats-collection-cpu

enable | disable
set fault-threshold <threshold-value>

Modes de commande

Mode surveillance

Historique des commandes

Version	Modification
2.11.1	Cette commande a été introduite.

Instructions d'utilisation

Cette commande active ou désactive la surveillance du processeur et modifie également la valeur du seuil de défaillance de toutes les défaillances de surveillance du processeur.

Exemple

```
firepower# scope monitoring
firepower /monitoring # scope health-monitoring-policy
firepower /monitoring/health-monitoring-policy # scope stats-collection-cpu
firepower /monitoring/health-monitoring-policy/stats-collection-cpu # set fault-threshold
85
firepower /monitoring/health-monitoring-policy/stats-collection-cpu # enable
firepower /monitoring/health-monitoring-policy/stats-collection-cpu * # commit-buffer
firepower /monitoring/health-monitoring-policy/stats-collection-cpu # show
Cpu stats collection policy:
Admin State Fault-Threshold (%)
-----------
Enabled 85
firepower /monitoring/health-monitoring-policy/stats-collection-cpu # show detail
Admin State: Enabled
Fault Threshold (%): 85
```

scope hw-crypto

Pour activer ou désactiver Accélération cryptographique TLS sur une instance de contenant, utilisez la commande **scope hw-crypto**. Pour plus de renseignements sur l'Accélération cryptographique TLS, consultez le *Guide de configuration de Centre de gestion*.

scope hw-crypto

Modes de commande

connect module

Historique des commandes

Version	Modification
2.7.1	Cette commande a été introduite.

Instructions d'utilisation

Cette commande active ou désactive Accélération cryptographique TLS sur une instance de contenant.

Exemples

Voici un exemple d'activation de Accélération cryptographique TLS sur une instance de contenant :

```
scope ssa
/ssa # show app-instance

App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
 Deploy Type Turbo Mode Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- --------------- --------------- ---------------
 ----------- ---------- ------------ --------------- -------------
ftd        FTD-FDM    1          Enabled     Online          6.5.0.1159      6.5.0.1159
    Native      No                      Not Applicable  None
ftd        ftd2       2          Enabled     Online          6.5.0.1159      6.5.0.1159
    Container   No         Default-Small Not Applicable  None

/ssa # sc slot 2
/ssa/slot # scope app-instance ftd ftd2
/ssa/slot/app-instance # scope hw-crypto
/ssa/slot/app-instance/hw-crypto # set admin-state enabled
 /ssa/slot/app-instance/hw-crypto* # commit-buffer
```

Voici un exemple de désactivation de Accélération cryptographique TLS sur une instance de contenant :

```
scope ssa
/ssa # show app-instance

App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
 Deploy Type Turbo Mode Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- --------------- --------------- ---------------
 ----------- ---------- ------------ --------------- -------------
ftd        FTD-FDM    1          Enabled     Online          6.5.0.1159      6.5.0.1159
    Native      No                      Not Applicable  None
ftd        ftd2       2          Enabled     Online          6.5.0.1159      6.5.0.1159
    Container   No         Default-Small Not Applicable  None

/ssa # sc slot 2
/ssa/slot # scope app-instance ftd ftd2
 /ssa/slot/app-instance # scope hw-crypto
```

```
/ssa/slot/app-instance/hw-crypto # set admin-state disbled
/ssa/slot/app-instance/hw-crypto* # commit-buffer
```

Commandes associées

Commande	Description
create hw-crypto	Créer une configuration d'Accélération cryptographique TLS pour une instance de contenant.
delete hw-crypto	Supprimez une configuration d'Accélération cryptographique TLS pour une instance de contenant.
show hw-crypto	Affiche l'état de la configuration Accélération cryptographique TLS sur une instance de contenant.

scope import-config

Pour accéder à un objet de configuration d'importation existant, utilisez la commande **scope import-config**.

scope import-config *hostname*

Description de la syntaxe

hostname	Identifiant de l'objet de configuration d'importation; il s'agit du nom ou de l'adresse IP du serveur distant sur lequel se trouve la configuration.

Historique des commandes

Version	Modification
1.1.(1)	Commande ajoutée.

Instructions d'utilisation

Un objet de configuration d'exportation est créé lorsque vous exécutez une commande **export-config** pour sauvegarder la configuration actuelle du périphérique logique et de la plateforme; la commande **import-config** est utilisée pour importer un fichier de configuration précédemment exporté, tout en créant simultanément un objet de configuration d'importation.

Vous pouvez utiliser **scope import-config** pour accéder à un objet de configuration d'importation existant et modifier ses paramètres. Aucune commande **create** ou **enter** n'est associée aux objets de configuration d'importation. Une commande **delete** vous permet de supprimer un objet de configuration d'importation.

Exemple

Cet exemple montre comment accéder à un objet de configuration d'importation existant :

```
firepower # scope system
firepower /system # scope import-config 192.168.1.2
firepower /system/import-config #
```

Commandes associées

Commande	Description
cfg-export-policy	Configure une politique d'exportation de configuration.
delete import-config	Supprime un objet d'importation de configuration existant.
import-config	Importe la configuration système précédemment exportée à partir d'un serveur distant; crée un objet de configuration d'importation.

scope info-policy

Pour accéder aux politiques d'informations système en mode configuration, utilisez la commande **scope info-policy**.

scope info-policy

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Scope system

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Vous n'avez pas besoin d'accéder à ce mode avec un objet géré.

Exemple

Cet exemple montre comment accéder au mode des politiques d'informations :

```
firepower # scope system
firepower /system # scope info-policy
firepower /system/info-policy #
```

Commandes associées

Commande	Description
Afficher	Affiche les informations sur les politiques d'informations.

scope interface

Pour accéder au mode configuration d'une interface spécifique, utilisez la commande **scope interface**.

scope interface {**Ethernet***slot_id*/*port_id* | *slot_num*}

Description de la syntaxe

Ethernet*slot_id*/*port_id*	Nom du port Ethernet.
slot_num	Numéro de logement d'interface

Modes de commande

scope eth-uplink/scope fabric a/

Historique des commandes

Version	Modification
1.1.1	Commande ajoutée.

Exemple

Cet exemple montre comment cibler le mode configuration d'une interface spécifique et afficher sa configuration actuelle :

```
firepower # scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # scope interface Ethernet1/5
firepower /eth-uplink/fabric/interface # show detail

Interface:
    Port Name: Ethernet1/5
    User Label:
    Port Type: Data
    Admin State: Enabled
    Oper State: Up
    State Reason:
    flow control policy: default
    Auto negotiation: No
    Admin Speed: 1 Gbps
    Oper Speed: 1 Gbps
    Admin Duplex: Full Duplex
    Oper Duplex: Full Duplex
    Ethernet Link Profile name: default
    Oper Ethernet Link Profile name: fabric/lan/eth-link-prof-default
    Udld Oper State: Admin Disabled
    Inline Pair Admin State: Enabled
    Inline Pair Peer Port Name:
    Allowed Vlan: All
    Network Control Policy: default
    Current Task:
firepower /eth-uplink/fabric/interface #
```

Commandes associées

Commande	Description
disable	Désactive l'interface actuelle.

Commande	Description
enable	Active l'interface actuelle.
set	En mode interface, définit les paramètres de configuration de l'interface.
show interface	Affiche les informations de configuration et d'état de l'interface.

scope ipsec

Pour accéder au mode IPSec, utilisez la commande **scope ipsec**.

scope ipsec

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode sécurité

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous n'avez pas besoin d'accéder à ce mode avec un objet géré.

Exemple

Cet exemple montre comment accéder au mode IPSec :

```
FP9300-A# scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec #
```

Commandes associées

Commande	Description
show connection	Affiche des informations sur la connexion IPSec.

scope ipv6-config

Pour accéder au mode configuration IPv6 vous permettant de configurer l'interface de gestion IPv6 de la structure, utilisez la commande **scope ipv6-config** en mode interconnexion de structure.

scope ipv6-config

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode interconnexion de structure

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous n'avez pas besoin d'accéder à ce mode avec un objet géré.

Exemple

Cet exemple montre comment accéder au mode configuration IPv6 :

```
FP9300-A# scope fabric-interconnect a
FP9300-A /fabric-interconnect # scope ipv6-config
FP9300-A /fabric-interconnect/ipv6-config #
```

Commandes associées

Commande	Description
show ipv6-if	Affiche les informations sur l'interface de gestion IPv6.

scope ldap

Pour accéder au mode configuration LDAP (Lightweight Directory Access Protocol), utilisez la commande **scope ldap**.

scope ldap

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope security/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous n'avez pas besoin d'accéder à ce mode avec un objet géré.

Exemple

Cet exemple montre comment accéder au mode LDAP :

```
firepower# scope security
firepower /security # scope ldap
firepower /security/ldap #
```

Commandes associées

Commande	Description
create ldap-group-rule	Crée des paramètres de règle de groupe de fournisseurs LDAP.
create server	En mode security/ldap, crée un serveur LDAP.
set	En mode security/ldap/server, définit divers paramètres liés au serveur LDAP, notamment l'activation ou la désactivation du protocole SSL.

scope licdebug

Pour accéder au mode débogage de licence à partir du mode licence, utilisez la commande **scope licdebug**.

scope licdebug

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode licence

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment accéder au mode débogage de licence à partir du mode licence :

```
FP9300-A # scope license
FP9300-A /license # scope licdebug
FP9300-A /license/licdebug #
```

Commandes associées

Commande	Description
scope license	Permet d'accéder au mode licence.

scope license

Pour accéder au mode licence, utilisez la commande **scope license**.

scope license

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment accéder au mode licence à partir du niveau EXEC :

```
FP9300-A# scope license
FP9300-A /license #
```

Commandes associées

Commande	Description
show license	Affiche l'utilisation de tout ou partie des ensembles de licences.

scope mem-leak-logging

Pour activer l'état de trace de pile afin de détecter la fuite de mémoire de chaque processus UCSM, utilisez la commande **scope mem-leak-logging**.

scope mem-leak-logging *set*

Description de la syntaxe		
	set	Définir la journalisation des fuites de mémoire pour le bouton.

Modes de commande

scope monitoring/scope sysdebug

Instructions d'utilisation

Utilisez cette commande pour activer la fonctionnalité de fuite de mémoire afin de déboguer les problèmes de fuite de mémoire pour le processus spécifié et activer la trace de pile.

Exemple

Cet exemple montre comment définir l'état du bouton et activer le mode trace de pile :

```
Firepower#scope monitoring
Firepower /monitoring# scope sysdebug
Firepower /monitoring/sysdebug#  scope mem-leak-logging
Firepower /monitoring/sysdebug/mem-leak-logging # set  ?
  appag-log               Memory Leak Logging for appAG
  bladeag-log            Memory Leak Logging for bladeAG
  dcosag-log             Memory Leak Logging for dcosAG
  dme-log                 Memory Leak Logging for dme
  extvmmag-log       Memory Leak Logging for extvmmAG
  hostagentag-log     Memory Leak Logging for hostagentAG
  licenseag-log         Memory Leak Logging for licenseAG
  nicag-log               Memory Leak Logging for nicAG
  portag-log              Memory Leak Logging for portAG
  rsdag-log                Memory Leak Logging for rsdAG
  serviceorchag-log   Memory Leak Logging for serviceOrchAG
  sessionmgrag-log   Memory Leak Logging for sessionmgrAG
  statsag-log              Memory Leak Logging for statsAG
  svcmonag-log        Memory Leak Logging for svcmonAG
Firepower /monitoring/sysdebug/mem-leak-logging # set statsag-log enable ?
  <CR>
  stacktrace  Stacktrace for Memory Leak Report
Firepower /monitoring/sysdebug/mem-leak-logging # set statsag-log enable stacktrace ?
  off  Off
  on   On
```

scope monitoring

Pour accéder au mode surveillance du système, utilisez la commande **scope monitoring**.

scope monitoring

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous n'avez pas besoin d'accéder à ce mode avec un objet géré.

Exemple

Cet exemple montre comment accéder au mode surveillance :

```
FP9300-A#scope monitoring
FP9300-A /monitoring #
```

Commandes associées

Commande	Description
show server status	Affiche les informations sur l'état d'un serveur.

scope network-features

Pour accéder aux fonctionnalités du réseau en mode configuration, utilisez la commande **scope network-features**.

scope network-features

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Scope system

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Vous n'avez pas besoin d'accéder à ce mode avec un objet géré.

Exemple

Cet exemple montre comment accéder au mode fonctionnalités du réseau :

```
firepower # scope system
firepower /system # scope network-features
firepower /system/network-features* # show
```

Commandes associées

Commande	Description
show	Affiche les informations sur les fonctionnalités du réseau de domaine.

scope org

Pour accéder au mode organisation, utilisez la commande **scope org**.

scope org [*org_name*]

Description de la syntaxe

org_name	(Facultatif) Nom de l'organisation.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment accéder au mode organisation :

```
FP9300-A# scope org org100
FP9300-A /org #
```

Commandes associées

Commande	Description
show org	Répertorie les organisations actuellement définies.

scope packet-capture

Pour accéder au mode capture de paquets, utilisez la commande **scope packet-capture**.

scope packet-capture

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous n'avez pas besoin d'accéder à ce mode avec un objet géré.

Exemple

Cet exemple montre comment accéder au mode capture de paquets :

```
FP9300-A#scope packet-capture
FP9300-A /monitoring #
```

Commandes associées

Commande	Description
traceroute	Trace la route vers un autre appareil du réseau.

scope password-profile

Pour accéder au mode profil de mot de passe, utilisez la commande **scope password-profile**.

scope password-profile

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode sécurité

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment accéder au mode sécurité de profil de mot de passe :

```
FP9300-A # scope security
FP9300-A /security # scope password-profile
FP9300-A /security/password-profile #
```

Commandes associées

Commande	Description
show password-profile	Affiche les informations sur le profil de mot de passe.

scope profile

Pour accéder au mode profil de destination Smart Call Home et Licences Smart, utilisez la commande **scope profile**.

scope profile *profile_name*

Description de la syntaxe

profile_name	Nom du profil de destination; entre 1 et 16 caractères.

Modes de commande

Mode Callhome (/monitoring/callhome/)

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment accéder au mode profil, puis afficher la destination configurée pour le profil :

```
FP9300-A /monitoring/callhome # scope profile SLProfile
FP9300-A /monitoring/callhome/profile # show destination

Destination:
    Name       Transport Protocol Email or HTTP/HTTPS URL Address
    ---------- ------------------ ------------------------------
    SLDest     Https
https://tools.cisco.com/its/service/oddce/services/DDCEService
FP9300-A /monitoring/callhome/profile #
```

Commandes associées

Commande	Description
show profile	Répertorie les profils de licences Smart Call Home et Smart actuellement définis; disponible en mode surveillance/callhome.

scope qos

Pour accéder au mode QoS, utilisez la commande **scope qos**.

scope qos

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope eth-server

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

En mode QoS, vous pouvez distinguer le trafic et mettre en file d'attente la bande passante pour chaque paquet, indépendamment du paquet ou de sa taille.

Exemple

Cet exemple montre comment accéder au mode QoS.

```
Firepower# scope eth-server
Firepower /eth-server # scope qos
Firepower /eth-server/qos #
```

Commandes associées

Commande	Description
show eth-best-effort	Affiche les informations détaillées d'une classe Ethernet de type meilleur effort
show eth-classified	Affiche les informations détaillées d'une classe Ethernet classifiée.
show fc	Affiche les informations de classe fc disponibles sur le système.
Show event	Affiche les informations sur les événements FSM.
show fsm	Affiche des informations sur le FSM pour l'application actuelle selon le mot clé spécifié. État : affiche les informations sur l'état du FSM. Tâche : affiche les informations sur la tâche du FSM

scope radius

Pour accéder au mode RADIUS (Remote Authentication Dial-in User Service), utilisez la commande **scope radius**.

scope radius

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope security

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Vous n'avez pas besoin d'accéder à ce mode avec un objet géré.

Exemple

Cet exemple montre comment accéder au mode RADIUS :

```
firepower # scope security
firepower /security # scope radius
firepower /security/radius #
```

scope reservation

Pour accéder au mode réservation de licence, utilisez la commande **scope reservation**.

scope reservation

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode licence

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment accéder au mode réservation à partir du mode licence :

```
FP9300-A# scope license
FP9300-A /license # scope reservation
FP9300-A /license/reservation #
```

Commandes associées

Commande	Description
request universal	Génère un code de demande de réservation.
show license	Affiche l'utilisation de tout ou partie des ensembles de licences.

scope security

Pour accéder au mode sécurité, utilisez la commande **scope security**.

scope security

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous n'avez pas besoin d'accéder à ce mode avec un objet géré.

Exemple

Cet exemple montre comment accéder au mode sécurité :

```
firepower# scope security
firepower /security #
```

Commandes associées

Commande	Description
show security	En mode EXEC, affiche les informations sur les politiques de sécurité actuelles.

scope server

Pour accéder au mode serveur, utilisez la commande **scope server**.

scope server {*id* | *dynamic_uuid* | *chassis_id* / *blade_id*}

Description de la syntaxe

ID	ID du serveur; entier compris entre 1 et 255.
dynamic_uid	Identifiant unique universel (UUID) dynamique du serveur.
chassis_id / *blade_id*	Serveur spécifié à l'aide des ID de châssis et de lame; doit être saisi au format n/n. **Remarque** L'ID de châssis est toujours **1**.

Modes de commande

Mode EXEC

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment accéder au mode serveur :

```
FP9300-A# scope server 1/1
FP9300-A /chassis/server #
```

Commandes associées

Commande	Description
show server adapter	Affiche les informations sur les adaptateurs réseau d'un serveur.
show server identity	Affiche les informations d'identité sur un serveur.

scope server-features

Pour accéder aux fonctionnalités du serveur en mode configuration, utilisez la commande **scope server-features**.

scope server-features

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Scope system

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Vous n'avez pas besoin d'accéder à ce mode avec un objet géré.

Exemple

Cet exemple montre comment accéder au mode fonctionnalités du serveur :

```
firepower # scope system
firepower /system # scope server-features
firepower /system/server-features* # show
```

Commandes associées

Commande	Description
afficher	Affiche des informations sur les fonctionnalités du serveur de domaine.

scope service-profile

Pour accéder au mode profil de service, utilisez la commande **scope service-profile**.

scope service-profile {*dynamic_uuid* | *org* | *server*}

Description de la syntaxe

dynamic_uuid	UUID dynamique du profil de service.
org	Nom de l'organisation pour laquelle le profil de service a été créé; entre 1 et 16 caractères.
serveur	ID du serveur pour lequel le profil de service a été créé.

Modes de commande

Mode EXEC

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Pour utiliser cette commande avec l'option *org*, une organisation et un profil de service associé à cette organisation doivent déjà exister.

Pour utiliser cette commande avec l'option *server*, le serveur peut être spécifié avec son ID de serveur ou l'ID de châssis et l'ID de lame (format n/n). L'ID de châssis est toujours **1**.

Exemple

Cet exemple montre comment accéder au mode profil de service :

```
firepower # scope service-profile server 1/1
firepower /org/service-profile #
```

Commandes associées

Commande	Description
show service-profile	Affiche les informations sur le profil de service.

scope services

Pour accéder aux services système en mode configuration, utilisez la commande **scope services**.

scope services

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Scope system

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Vous n'avez pas besoin d'accéder à ce mode avec un objet géré.

Exemple

Cet exemple montre comment accéder au mode services :

```
firepower # scope system
firepower /system # scope services
firepower /system/services #
```

Commandes associées

Commande	Description
show	Affiche des informations sur les services.

scope slot

Pour accéder au mode logement d'un module SSP spécifique, utilisez la commande **scope slot**.

scope slot *slot_ID*

Description de la syntaxe

slot_ID / id	Identifie le logement du module. Pour le FP9300, cette valeur peut être 1, 2 ou 3; pour le FP4100, cette valeur est 1.

Modes de commande

scope ssa/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

En mode logement, vous pouvez mettre à jour l'image d'application sur le périphérique logique.

Exemple

Cet exemple montre comment accéder au mode logement :

```
firepower# scope ssa
firepower /ssa # scope slot 2
firepower /ssa/slot #
```

Commandes associées

Commande	Description
show security	Affiche les informations relatives à la sécurité.

scope ssa

Pour accéder au mode services de sécurité (ssa), utilisez la commande **scope ssa**.

scope ssa

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode EXEC

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous n'avez pas besoin d'accéder à ce mode avec un objet géré.

Exemple

Cet exemple montre comment accéder au mode ssa :

```
FP9300-A# scope ssa
FP9300-A /ssa #
```

Commandes associées

Commande	Description
show security	Affiche les informations relatives à la sécurité.

scope stats-collection-policy

Pour accéder à la politique de collecte de statistiques pour l'un des domaines fonctionnels de votre système, utilisez la commande **scope stats-collection-policy**.

scope stats-collection-policy *policy-area*

Description de la syntaxe

policy-area	Domaine spécifique de la politique de collecte : • `Adapter` : statistiques relatives aux adaptateurs. • `Chassis` : statistiques relatives au châssis du serveur lame. • `FEX` : statistiques relatives aux dispositifs d'extension de structure. • `Host` : cette politique est un espace réservé pour une future prise en charge. • `Port` : statistiques relatives aux ports, y compris les ports de serveur, les ports de liaison ascendante Ethernet et Fibre Channel. • `Server` : statistiques relatives aux serveurs.

Modes de commande

scope monitoring/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Les statistiques peuvent être collectées et présentées pour plusieurs domaines fonctionnels de votre système.

Utilisez la commande **set collection-interval** pour définir la fréquence de collecte des statistiques et la commande **set reporting-interval** pour définir la fréquence à laquelle ces statistiques sont présentées. Ces intervalles définissent une politique de collecte des statistiques.

Les intervalles de production de rapports sont plus longs que les intervalles de collecte, de sorte que plusieurs points de données statistiques peuvent être collectés au cours de l'intervalle de production de rapports, fournissant ainsi des données suffisantes pour calculer et communiquer les valeurs minimales, maximales et moyennes.

Remarque Il existe une politique de collecte de statistiques par défaut pour chacun de ces domaines fonctionnels. Vous ne pouvez pas créer de politiques de collecte de statistiques supplémentaires, ni supprimer les politiques par défaut existantes. Vous pouvez uniquement modifier les politiques par défaut.

Exemple

Cet exemple montre comment accéder à la politique de collecte de statistiques pour les ports, définir l'intervalle de collecte sur une minute, définir l'intervalle de production de rapports sur 30 minutes, puis valider la transaction :

```
firepower # scope monitoring
firepower /monitoring # scope stats-collection-policy port
firepower /monitoring/stats-collection-policy # set collection-interval 1minute
firepower /monitoring/stats-collection-policy* # set reporting-interval 30minute
firepower /monitoring/stats-collection-policy* # commit-buffer
firepower /monitoring/stats-collection-policy #
```

Commandes associées

Commande	Description
set collection-interval	Spécifie la fréquence à laquelle les statistiques sont collectées.
set reporting-interval	Spécifie la fréquence à laquelle les statistiques sont présentées.

scope stats-threshold-policy

Pour accéder à la politique de seuil de statistiques pour l'un des composants de votre système, utilisez la commande **scope stats-threshold-policy**.

scope stats-threshold-policy *policy-name*

Description de la syntaxe

policy-name	Nom de la politique de seuil spécifique à saisir. Vous ne pouvez pas créer ni supprimer de politique de seuil de statistiques pour les ports de serveur Ethernet ou les ports de liaison ascendante Ethernet. Vous ne pouvez configurer que la politique par défaut existante. Par conséquent, pour ces politiques, saisissez **default** pour *policy-name*.

Modes de commande

scope eth-server/

scope eth-uplink/

scope org/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Une politique de seuil de statistiques surveille les statistiques relatives à certains aspects du système et génère un événement si un seuil spécifié est dépassé. Vous pouvez définir des seuils minimaux et maximaux. Par exemple, vous pouvez configurer la politique pour déclencher une alarme si la température du processeur dépasse une certaine valeur ou si un serveur est surutilisé ou sous-utilisé.

Il existe une politique de seuil de statistiques par défaut pour les ports de serveur Ethernet et les ports de liaison ascendante Ethernet. Vous ne pouvez pas créer de politiques de seuil de statistiques supplémentaires, ni supprimer les politiques par défaut existantes pour ces composants. Vous pouvez uniquement modifier les politiques par défaut.

Cependant, vous pouvez créer et supprimer des politiques de seuil de statistiques en mode organisation (`scope org/`). Pour plus de renseignements, consultez la commande **create stats-threshold-policy**.

Remarque Utilisez la commande **set collection-interval** pour définir la fréquence de collecte des statistiques et la commande **set reporting-interval** pour définir la fréquence à laquelle ces statistiques sont présentées. Ces intervalles définissent une politique de collecte des statistiques.

Exemples

Cet exemple montre comment accéder à la politique de seuil des statistiques de liaison ascendante Ethernet par défaut, créer une classe de statistiques d'erreurs, créer une propriété de compteur d'erreurs de contrôle de redondance cyclique (CRC), spécifier que le nombre normal d'erreurs CRC par intervalle d'interrogation est de 1 000, créer un seuil d'avertissement au-dessus de la normale de 1 250, puis valider la classe :

```
firepower # scope eth-uplink
firepower /eth-uplink # scope stats-threshold-policy default
firepower /eth-uplink/stats-threshold-policy # create class ether-error-stats
firepower /eth-uplink/stats-threshold-policy/class* # create property crc-delta
firepower /eth-uplink/stats-threshold-policy/class/property* # set normal-value 1000
firepower /eth-uplink/stats-threshold-policy/class/property* # create threshold-value
above-normal warning
firepower /eth-uplink/stats-threshold-policy/class/property/threshold-value* # set escalating
 1250
firepower /eth-uplink/stats-threshold-policy/class/property/threshold-value* # commit-buffer
firepower /eth-uplink/stats-threshold-policy/class/property/threshold-value #
```

Cet exemple montre comment accéder au mode organisation, créer une nouvelle politique de seuil de statistiques pour les statistiques des serveurs et des composants de serveur, créer une classe de politiques de seuil pour les statistiques d'environnement du CPU, créer une propriété de température du CPU, spécifier que la température normale du CPU est de 48,5 °C, créer un seuil d'avertissement supérieur à la normale de 50 °C, puis valider la transaction complète :

```
firepower # scope org
firepower /org # create stats-threshold-policy ServStatsPolicy
firepower /org/stats-threshold-policy* # create class cpu-env-stat
firepower /org/stats-threshold-policy/class* # create property temperature
firepower /org/stats-threshold-policy/class/property* # set normal-value 48.5
firepower /org/stats-threshold-policy/class/property* # create threshold-value above-normal
 warning
firepower /org/stats-threshold-policy/class/property/threshold-value* # set escalating 50.0
firepower /org/stats-threshold-policy/class/property/threshold-value* # commit-buffer
firepower /org/stats-threshold-policy/class/property/threshold-value #
```

Cet exemple montre comment cibler la politique de seuil de statistiques du serveur Ethernet par défaut.

```
Firepower# scope eth-server
Firepower /eth-server # scope stats-threshold-policy default
Firepower /eth-server/stats-threshold-policy #
```

Commandes associées

Commande	Description
create class	Crée une classe de statistiques.
create property	Crée une propriété pour une classe de statistiques.
create threshold-value	Spécifie un seuil supérieur ou inférieur à la normale pour une propriété de classe.
scope stats-collection-policy	Permet d'accéder au mode stats-collection-policy dans lequel vous gérez les intervalles de collecte de statistiques et de création de rapports.
create	Objets gérés créés
delete	Supprimer des objets gérés
enter	Accéder à un objet géré
scope	Modifier le mode actuel

Commande	Description
set	Définir les valeurs de propriété.
show	Afficher les informations système

scope storage-features

Pour accéder aux fonctionnalités de stockage en mode configuration, utilisez la commande **scope storage-features**.

scope storage-features

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Scope system

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Vous n'avez pas besoin d'accéder à ce mode avec un objet géré.

Exemple

Cet exemple montre comment accéder au mode fonctionnalités de stockage :

```
firepower # scope system
firepower /system # scope environment-features
firepower /system/environment-features # show
```

Commandes associées

Commande	Description
show	Affiche les informations sur les fonctionnalités de stockage de domaine.

scope system

Pour accéder au mode gestion du système, utilisez la commande **scope system**.

scope system

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode EXEC

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Ce mode vous permet de gérer la configuration système, notamment l'exportation et l'importation d'un fichier de configuration.

Exemple

Cet exemple montre comment accéder au mode gestion du système :

```
firepower# scope system
firepower /system #
```

Commandes associées

Commande	Description
show system	Affiche les informations sur les systèmes configurés sur cet appareil.

scope tacacs

Pour accéder au mode configuration TACACS (Terminal Access Controller Access Control System), utilisez la commande **scope tacacs**.

scope tacacs

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope security

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Vous n'avez pas besoin d'accéder à ce mode avec un objet géré.

Exemple

Cet exemple montre comment accéder au mode TACACS :

```
firepower # scope security
firepower /security # scope tacacs
firepower /security/tacacs #
```

scope telemetry

Pour accéder au mode télémétrie, utilisez la commande **scope telemetry**.

scope telemetry

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope system, scope services

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Vous pouvez utiliser les commandes enable, disable et show.

Commandes associées

Commande	Description
show detail	Affiche les informations de télémétrie du système.

scope vnic

Pour accéder au mode carte réseau virtuelle, utilisez la commande **scope vnic**.

scope vnic *dynamic_mac*

Description de la syntaxe

dynamic_mac	Adresse MAC dynamique de la carte réseau virtuelle.

Modes de commande

Mode EXEC

Mode profil de service

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment accéder au mode carte réseau virtuelle en mode organisation :

```
FP9300-A # scope org org10
FP9300-A /org # scope service-profile sp10
FP9300-A /org/service-profile # scope vnic vNIC10
FP9300-A /org/service-profile/vnic #
```

Commandes associées

Commande	Description
show server adapter	Affiche des informations sur les adaptateurs réseau disponibles.

sub scopes (scope fabric-interconnect)

Pour accéder au mode liaison ascendante de commutateur, utilisez la commande **scope sw-uplink** dans scope fabric interconnect.

scope sw-uplink

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode EXEC

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Vous n'avez pas besoin d'accéder à ce mode avec un objet géré.

Exemple

Cet exemple montre comment accéder au mode sw-uplink :

```
firepower# scope fabric-interconnect
firepower /fabric-interconnect # scope sw-uplink
firepower /fabric-interconnect/sw-uplink #
```

Commandes associées

Commande	Description
show	Affiche les informations sur sw-uplink.

Commandes set

- set absolute-session-timeout, à la page 256
- set account-status, à la page 257
- set address, à la page 258
- set admin-state, à la page 259
- set auth-server-group, à la page 260
- set authentication, à la page 261
- set auto-negotiation, à la page 262
- set cert, à la page 263
- set certchain, à la page 265
- set (certreq), à la page 267
- set (cfg-export-policy), à la page 269
- set (cfg-export-reminder), à la page 272
- set cli , à la page 273
- set clock , à la page 275
- set cluster-control-link network, à la page 276
- set collection-interval, à la page 277
- set con-absolute-session-timeout, à la page 279
- set con-session-timeout, à la page 280
- set cpu-core-count, à la page 281
- set deploy-type, à la page 283
- set descr, à la page 285
- set duplex, à la page 286
- set email, à la page 287
- set enforce-strong-password, à la page 288
- set expiration, à la page 290
- set (configuration d'exportation), à la page 291
- set firstname, à la page 293
- set flow-control-policy, à la page 294
- set (politique de contrôle de flux), à la page 295
- set frequency, à la page 297
- set http-proxy-server-enable, à la page 298
- set http-proxy-server-port, à la page 299
- set http-proxy-server-url, à la page 300

- set https, à la page 301
- set (interface), à la page 304
- set ipv6, à la page 307
- set ipv6-auto eui64, à la page 308
- set ipv6-auto stablesec, à la page 309
- set ipv6-ready, à la page 310
- set keyring-name, à la page 311
- set lastname, à la page 312
- set link-state-sync, à la page 313
- set local-address, à la page 314
- set log-level, à la page 315
- set max-login-attempts, à la page 316
- set message, à la page 317
- set min-password-length, à la page 319
- set mode, à la page 320
- set modulus, à la page 321
- set nd, à la page 322
- set out-of-band, à la page 323
- set password, à la page 325
- set password-encryption-key, à la page 326
- set (password-profile), à la page 328
- set phone, à la page 330
- set (port-channel), à la page 331
- set port-channel-mode, à la page 335
- set port-type, à la page 337
- set port-type (aggr-interface), à la page 341
- set prefix, à la page 345
- set protocol, à la page 347
- set realm, à la page 349
- set refresh-period, à la page 350
- set regenerate, à la page 351
- set remote-address, à la page 352
- set remote-ike-ident, à la page 353
- set remote-subnet, à la page 354
- set remote-user, à la page 355
- set reporting-interval, à la page 356
- set resource-profile-name, à la page 358
- set session-timeout, à la page 360
- set snmp-adminappinstance, à la page 361
- set snmp, à la page 363
- set (snmp-trap), à la page 365
- set (snmp-user), à la page 368
- set speed, à la page 370
- set speed (aggr-interface), à la page 372
- set ssh-server, à la page 375
- set sshkey, à la page 376

- set startup-version, à la page 377
- set timezone, à la page 378
- set trustpoint, à la page 380
- set use-2-factor, à la page 381
- set user-account-unlock-time, à la page 382
- set user-label, à la page 383
- set value (create bootstrap-key FIREWALL_MODE), à la page 385
- set value (create bootstrap-key MANAGEMENT_TYPE), à la page 386
- set value (create bootstrap-key PERMIT_EXPERT_MODE), à la page 387
- set vlan, à la page 388

set absolute-session-timeout

Pour définir le délai d'expiration absolu de session, utilisez la commande **set absolute-session-timeout**.

set absolute-session-timeout *seconds*

Description de la syntaxe

seconds	Délai d'expiration absolu des sessions Web, SSH et Telnet; la valeur peut être comprise entre 0 et 3 600 secondes. Pour désactiver ce délai d'expiration, définissez la valeur sur 0.

Modes de commande

Mode d'authentification par défaut (/security/default-auth)

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Le délai d'expiration absolu de session ferme les sessions utilisateur après la période d'expiration spécifiée, quelle qu'en soit l'utilisation. Ce délai d'expiration absolu porte sur toutes les formes d'accès, y compris la console de série, SSH et HTTPS.

Exemple

Cet exemple montre comment accéder au mode d'authentification par défaut, puis définir le délai d'expiration absolu de toutes les sessions sur quatre minutes :

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set absolute-session-timeout 240
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

Commandes associées

Commande	Description
set refresh-period	Définit la période d'actualisation de session Web.
show detail	Affiche les paramètres de session actuelle et de délai d'expiration de session absolu.

set account-status

Pour indiquer si un compte d'utilisateur local est actif ou inactif, utilisez la commande **set account-status**.

set account-status {**active** | **inactive**}

Description de la syntaxe

active	Indique que le compte d'utilisateur local est activé.
inactive	Indique que le compte d'utilisateur local est actif.

Modes de commande

Mode utilisateur local (/security/local-user)

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Seuls les utilisateurs dotés de privilèges d'administrateur ou AAA peuvent utiliser cette commande.

Le compte administrateur est toujours actif. Il ne peut pas être modifié.

Exemple

Cet exemple montre comment accéder au mode utilisateur local et désactiver un compte d'utilisateur local :

```
FP9300-A # scope security
FP9300-A /security # scope local-user test_user
FP9300-A /security/local-user # set account-status inactive
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

Commandes associées

Commande	Description
set expiration	Spécifie la date d'expiration du compte d'utilisateur.

set address

Pour définir une adresse de courriel ou une adresse URL pour une destination Smart Call Home ou Smart Licensing, utilisez la commande **set address**.

set address *address*

Description de la syntaxe

address	Adresse de courriel ou URL de la destination Smart Call Home ou Smart Licensing.

Modes de commande

scope monitoring/scope callhome/scope profile/scope destination/

Historique des commandes

Version	Modification
1.4(1)	Commande ajoutée.

Instructions d'utilisation

Chaque châssis Firepower 4100/9300 doit être enregistré auprès de l'autorité de licence Smart Call Home ou du serveur satellite de licences Smart. Utilisez cette commande pour définir une adresse courriel ou une adresse URL HTTP/HTTPS comme destination de la licence.

Exemple d'autorité de licence : `https://tools.cisco.com/its/service/oddce/services/DDCEService`

Exemple de serveur satellite : `https://ip_address/Transportgateway/services/DeviceRequestHandler`

Exemple

Cet exemple montre comment créer et saisir une destination Smart Call Home :

```
firepower # scope monitoring
firepower /monitoring # scope callhome
firepower /monitoring/callhome # scope profile SLProfile
firepower /monitoring/callhome/profile # scope destination SLDest
firepower /monitoring/callhome/profile/destination # set address
https://tools.cisco.com/its/service/oddce/services/DDCEService
firepower /monitoring/callhome/profile/destination* # commit-buffer
firepower /monitoring/callhome/profile/destination #
```

Commandes associées

Commande	Description
create destination	Création d'une destination Smart Call Home.
delete destination	Supprime une destination Smart Call Home existante.
set protocol	Définit le protocole de transport pour une destination Smart Call Home.

set admin-state

Pour activer ou désactiver l'état administratif d'une politique Smart Call Home, utilisez la commande **set admin-state**.

set admin-state { **disabled** | **enabled** }

Description de la syntaxe

disabled	Désactive l'état administratif de la politique.
enabled	Active l'état administratif de la politique.

Modes de commande

scope monitoring/scope callhome/policy/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour activer ou désactiver la politique Call Home lorsqu'une défaillance ou un événement système correspondant à la cause associée survient.

Exemple

Cet exemple montre comment accéder et activer une instance de politique Call Home pour les événements de perte de liaison :

```
firepower /monitoring/callhome # enter policy link-down
firepower /monitoring/callhome/policy* # set admin-state enabled
firepower /monitoring/callhome/policy* # commit-buffer
firepower /monitoring/callhome/policy #
```

Commandes associées

Commande	Description
enter policy	Permet d'accéder à une politique Smart Call Home.
delete policy	Supprime une politique Smart Call Home existante.
scope policy	Cible une politique Smart Call Home.
show	Affiche les informations de configuration ou de politique Call Home.

set auth-server-group

Pour définir un groupe de serveurs d'authentification par défaut, utilisez la commande **set auth-server-group**.

set auth-server-group *admin*

Description de la syntaxe

admin	Nom du groupe de serveurs d'authentification.

Modes de commande

Mode d'authentification par défaut

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment spécifier le groupe de serveurs d'authentification par défaut :

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set auth-server-group admin_server
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

Commandes associées

Commande	Description
set realm	Spécifie le service d'authentification par défaut.

set authentication

Pour définir la méthode d'authentification par défaut de l'utilisateur lors de la connexion et de l'accès à l'interface de ligne de commande FXOS via le port de console, utilisez la commande **set authentication** .

set authentication

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope security

Historique des commandes

Version	Modification
2.10(1)	Commande ajoutée.

Instructions d'utilisation

Vous pouvez définir la méthode par défaut selon laquelle un utilisateur est authentifié lors de la connexion et de l'accès à l'interface de ligne de commande FXOS via le port de console.

Exemple

Cet exemple montre comment accéder au mode sécurité et définir la méthode d'authentification par défaut :

```
firepower# scope security
firepower /security # set authentication
  console  Console authentication
  default  Default authentication
```

Commandes associées

Commande	Description
show authentication	Affiche le service d'authentification existant.

set auto-negotiation

Pour activer ou désactiver la négociation automatique d'une interface, utilisez la commande **set auto-negotiation**.

set auto-negotiation {**on** | **off**}

Description de la syntaxe

on	(Facultatif) La négociation automatique est activée.
off	(Facultatif) La négociation automatique est désactivée.

Modes de commande

scope eth-uplink/scope fabric a/scope interface/

Historique des commandes

Version	Modification
2.1.1	Commande ajoutée.

Instructions d'utilisation

Cette commande fonctionne uniquement sur des types de ports spécifiques.

Exemple

Cet exemple montre comment activer ou désactiver la négociation automatique :

```
Firepower-9300 # scope eth-uplink
Firepower-9300 /eth-uplink # scope fabric a
Firepower-9300 /eth-uplink #/fabric # scope interface Ethernet2/1
Firepower-9300 /eth-uplink/fabric/interface* # set auto-negotiation on
Firepower-9300 /eth-uplink/fabric/interface* # commit-buffer
Firepower-9300 /eth-uplink/fabric/interface #
```

Commandes associées

Commande	Description
scope interface	Affiche des informations sur l'interface Ethernet de l'interface.

set cert

Pour ajouter un certificat RSA à un trousseau de clés, utilisez la commande **set cert**.

set cert

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode trousseau de clés

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Après avoir saisi la commande , vous êtes invité à saisir le texte du certificat, qui doit se terminer par **ENDOFBUF**.

Exemple

Cet exemple montre comment saisir le texte de certificat pour un trousseau de clés :

```
FP9300-A /security/keyring # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
>-----BEGIN CERTIFICATE-----
MIIFqDCCA5CgAwIBAgIBBDANBgkqhkiG9w0BAQsFADBwMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCQ0ExDDAKBgNVBAcMA1NKQzEOMAwGA1UECgwFQ2lzY28xDTALBgNV
BAsMBFNUQlUxCzAJBgNVBAMMAkNBMRowGAYJKoZIhvcNAQkBFgtzc3BAc3NwLm5l
dDAeFw0xNjEyMTUyMTM0NTRaFw>0yNjEyMTMyMTM0NTRaMHwxCzAJBgNVBAYTAlVT
MQswCQYDVQQIDAJDQTEPMA0GA1UECgwGbmV3c3RnMRAwDgYDVQQLDAduZXdzdGJ1
MRMwEQYDVQQDDAppbnRlcm0xLWNhMSgwJgYJKoZIhvcNAQkBFhlpbnRlcm0xLWNh
QGludGVybTEtY2EubmV0MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA
wLpNnyEx5I4P8uDoW>KWF3IZsegjhLANsodxuAUmhmwKekd0OpZZxHMw1wSO4IBX5
4itJS0xyXFzPmeptG3OXvNqCcsT+4BXl3DoGgPMULccc4NesHeg2z8+q3SPA6uZh
iseWNvKfnUjixbQEBtcrWBiSKnZuOz1cpuBn34gtgeFFoCEXN+EZVpPESiancDVh
8pCPlipc/08ZJ3o9GW2j0eHJN84sguIEDL812ROejQvpmfqGUq11stkIIuh+wB+V
VRhUBVG7p>V57I6DHeeRp6cDMLXaM3iMTelhdShyo5YUaRJMak/t8kCqhtGXfuLlI
E2AkxKXeeveR9n6cpQd5JiNzCT/t9IQL/T/CCqMICRXLFpLCS9o5S5O2B6QFgcTZ
yKR6hsmwe22wpK8QI7/5oWNXlolb96hHJ7RPbG7RXYqmcLiXY/d2j9/RuNoPJawI
hLkfhoIdPA28xlnfIB1azCmMmdPcBO6cbUQfCj5hSmk3StVQKgJCjaujz55TGGd1
G>jnxDMX9twwz7Ee51895Xmtr24qqaCXJoW/dPhcIIXRdJPMsTJ4yPG0BieuRwd0p
i8w/rFwbHzv4C9Fthw1JrRxH1yeHJHrLlZgJ5txSaVUIgrgVCJaf6/jrRRWoRJwt
AzvnzYql2dZPCcEAYgP7JcaQpvdpuDgq++NgBtygiqECAwEAAaNBMD8wDAYDVR0T
BAUwAwEB/zAvBgNVHR8EKDAmMCSgIqAghh5odHRwOi8vMTkyLjE2OC40LjI5>L2lu
dGVybS5jcmwwDQYJKoZIhvcNAQELBQADggIBAG/XujJh5G5UWo+cwTSitAezWbJA
h1dAiXZ/OYWZSxkFRliErKdupLqL0ThjnX/wRFfEXbrBQwm5kWAUUDr97D1Uz+2A
8LC5I8SWKXmyf0jUtsnEQbDZb33oVL7yXJk/A0SF0jihpPheMA+YRazalT9xj9KH
PE7nHCJMbb2ptrHUyvBrKSYrSeEqOpQU2+otnFyV3rS9aelgV>juaWyaWOc3lZ1Oi
CC2tJvY3NnM56j5iesxUCeY/SZ2/ECXN7RRBViLHmA3gFKmWf3xeNiKkxmJCxOaa
UWPC1x2V66I8DG9uUzlWyd79O2dy52aAphAHC6hqlzb6v+gw1Tld7UxaqVd8CD5W
ATjNs+ifkJS1h5ERxHjgcurZXOpR+NWpwF+UDzbMXxx+KAAXCI6ltCd8Pb3wOUC3
PKvwEXaIcCcxGx71eRLpWPZFyEoi4N2NGE9OXRjz0>K/KERZgNhsIW3bQMjcw3aX6
OXskEuKgsayctnWyxVqNnqvpuz06kqyubh4+ZgGKZ5LNEXYmGNz3oED1rUN636Tw
SjGAPHgeROzyTFDixCei6aROlGdP/Hwvb0/+uThIe89g8WZ0djTKFUM8uBO3f+II
/cbuyBO1+JrDMq8NkAjxKlJlp1c3WbfCue/qcwtcfUBYZ4i53a56UNF5Ef0rpy/8
```

```
B/+07Me/p2y9Luqa
-----END CERTIFICATE-----
ENDOFBUF
FP9300-A /security/keyring* #
```

Commandes associées

Commande	Description
set modulus	Spécifie le module de clé RSA (longueur de clé SSL) en bits.
set regenerate	Renouvelle les clés RSA du trousseau de clés par défaut.
set trustpoint	Spécifie si le certificat de trousseau de clés peut être renouvelé.

set certchain

Pour accéder à la liste (ou chaîne) de certificats du point de confiance actuel, utilisez la commande **set certchain**.

set certchain [*cert_chain*]

Description de la syntaxe

cert_chain	(Facultatif) Chaîne de certificats obtenue auprès d'une autorité de certification. Si cette variable est omise, vous êtes invité à saisir les informations de certificat manuellement.

Modes de commande

Mode point de confiance

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Les certificats doivent être au format X.509 codés en Base64 (CER).

Si vous ne spécifiez pas la chaîne de certificats dans la commande, vous êtes invité à saisir un certificat ou une liste de points de confiance définissant un chemin de certification vers l'autorité de certification (CA) racine. Saisissez `ENDOFBUF` pour finaliser l'entrée.

Pour plus de renseignements sur l'obtention d'un certificat de confiance, consultez la section « Certificats, trousseaux de clés et points de confiance » dans le *Guide de configuration de l'interface de ligne de commande Cisco FXOS*.

Exemple

Cet exemple montre comment créer et saisir un point de confiance, puis coller une chaîne de certificats dans ce point de confiance :

```
FP9300-A # scope security
FP9300-A /security # enter trustpoint tPoint4
FP9300-A /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3nO4MIGeBgNVHSMEgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> C1NhbnRhIENsYXJhMRswGQYDVQQKExJOdW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
```

```
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
FP9300-A /security/trustpoint* # commit-buffer
FP9300-A /security/trustpoint #
```

Commandes associées

Commande	Description
enter trustpoint	Permet d'accéder à un point de confiance.
show trustpoint	Affiche les informations sur le point de confiance actuel.

set (certreq)

Pour spécifier les paramètres d'une demande de certificat de trousseau de clés, utilisez la commande **set** en mode demande de certificat.

set {*country* | *dns* | *e-mail* | *fi-a-ip* | *fi-a-ipv6* | *fi-b-ip* | *fi-b-ipv6* | *ip* | *ipv6* | *locality* | *org-name* | *org-unit-name* | *password* | *state* | *subject-name* }

Description de la syntaxe

country	(Facultatif) Spécifiez un code de pays à deux lettres pour la demande; les lettres doivent être en majuscules.
dns	(Facultatif) Spécifiez le nom de domaine attribué au réseau; commun à tous les noms de domaine. Il s'agit d'une alternative à *subject-name*.
e-mail	(Facultatif) Spécifiez l'adresse de courriel associée à la demande.
fi-a-ip	Pas utilisée.
fi-a-ipv6	Pas utilisée.
fi-b-ip	Pas utilisée; il n'existe pas d'interconnexion de structures B.
fi-b-ipv6	Pas utilisée; il n'existe pas d'interconnexion de structures B.
ip	(Facultatif) Spécifiez l'adresse IPv4 du domaine de l'appareil.
IPv6	(Facultatif) Spécifiez l'adresse IPv6 du domaine de l'appareil.
locality	(Facultatif) Spécifiez la ville dans laquelle se trouve le siège social de l'entreprise qui demande le certificat. Saisissez jusqu'à 64 caractères. Vous pouvez utiliser des lettres, des chiffres, des espaces et les caractères spéciaux suivants : , (virgule), . (point), @ (arobase), ^ (accent circonflexe), ((parenthèse ouvrante),) (parenthèse fermante), - (tiret), _ (trait de soulignement), + (signe plus), : (deux-points), / (barre oblique).
org-name	(Facultatif) Spécifiez le nom de l'organisation qui demande le certificat. Saisissez jusqu'à 64 caractères. Vous pouvez utiliser des lettres, des chiffres, des espaces et les caractères spéciaux suivants : , (virgule), . (point), @ (arobase), ^ (accent circonflexe), ((parenthèse ouvrante),) (parenthèse fermante), - (tiret), _ (trait de soulignement), + (signe plus), : (deux-points), / (barre oblique).
org-unit-name	(Facultatif) Spécifiez le nom de l'unité au sein de l'organisation. Saisissez jusqu'à 64 caractères. Vous pouvez utiliser des lettres, des chiffres, des espaces et les caractères spéciaux suivants : , (virgule), . (point), @ (arobase), ^ (accent circonflexe), ((parenthèse ouvrante),) (parenthèse fermante), - (tiret), _ (trait de soulignement), + (signe plus), : (deux-points), / (barre oblique).

password	(Facultatif) Vous êtes invité à saisir puis à confirmer le mot de passe de la demande.
state	(Facultatif) Spécifiez l'État ou la province dans lequel se trouve le siège social de l'entreprise qui demande le certificat. Saisissez jusqu'à 64 caractères. Vous pouvez utiliser des lettres, des chiffres, des espaces et les caractères spéciaux suivants : , (virgule), . (point), @ (arobase), ^ (accent circonflexe), ((parenthèse ouvrante),) (parenthèse fermante), - (tiret), _ (trait de soulignement), + (signe plus), : (deux-points), / (barre oblique).
subject-name	(Facultatif) Spécifiez le nom de domaine complet de l'interconnexion de structures locale.

Modes de commande

scope security/enter keyring/scope certreq/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Après avoir créé ou saisi une demande de certificat, utilisez ces options pour spécifier les informations relatives à cette demande.

Exemple

Cet exemple montre comment spécifier des informations sur une demande de certificat :

```
firepower /security/keyring # enter certreq
firepower /security/keyring/certreq # set subject-name FP9300-1.testnet.com
firepower /security/keyring/certreq* # set password
Certificate request password:
Confirm certificate request password:
firepower /security/keyring/certreq* #
```

Commandes associées

Commande	Description
create certreq	Crée une demande de certificat de trousseau de clés.
delete certreq	Supprime une demande de certificat de trousseau de clés existante.
enter certreq	Permet d'accéder à une demande de certificat de trousseau de clés.
set (keyring)	Définissez les informations relatives au trousseau de clés, y compris le module et le point de confiance.

set (cfg-export-policy)

Pour spécifier ou modifier les paramètres d'une politique d'exportation de configuration existante, utilisez la commande **set** en mode politique d'exportation de configuration.

set { **adminstate** | **descr** | **hostname** | **password** | **port** | **protocol** | **remote-file** | **schedule** | **user** }

Description de la syntaxe

adminstate { **disable** | **enable**	Active ou désactive l'administration des politiques. Lorsque cette option est désactivée, les sauvegardes de configuration ne sont pas exportées selon le calendrier des politiques.
descr *description*	(Facultatif) Vous pouvez ajouter une description à l'objet de configuration; la description peut comporter entre 1 et 256 caractères. La plupart des caractères alphanumériques sont autorisés, de même que les tirets et les traits de soulignement. La chaîne peut se terminer par des signes de ponctuation comme un point-virgule, un point et un point d'exclamation, mais vous ne pouvez pas intégrer ces caractères dans la description.
hostname *host_ID*	(Facultatif) Spécifiez l'adresse IP ou le nom de domaine du serveur distant vers lequel la sauvegarde de la configuration est exportée. Il peut s'agir d'un serveur, d'une baie de stockage, d'un lecteur local ou de tout support en lecture/écriture accessible sur le réseau. **Remarque** Pour utiliser un nom de domaine réel, un serveur DNS configuré doit être disponible.
password	(Facultatif) Spécifiez le mot de passe utilisé pour la connexion au serveur distant; vous êtes invité à saisir, puis à confirmer le mot de passe.
port { *number* | **default** }	(Facultatif) Vous pouvez modifier le port sur lequel les communications avec le serveur distant interviennent; si cette option n'est pas spécifiée, le port par défaut du protocole est utilisé. Les options correspondent à un numéro d'ID de port compris entre zéro et 4294967295, ou **default** pour le port par défaut du protocole actuel.
protocol *name*	(Facultatif) Spécifiez le protocole de transfert de fichiers à utiliser. Les options disponibles sont les suivantes : • **ftp** • **scp** • **sftp** • **tftp**
remote-file *name*	(Facultatif) Spécifiez le chemin complet, y compris un nom de fichier, pour la configuration exportée ; peut comporter entre 1 et 128 caractères.

schedule {**bi-weekly** | **daily** | **weekly**}	(Facultatif) Spécifiez la fréquence à laquelle la configuration est automatiquement exportée : • **bi-weekly** : l'exportation a lieu toutes les deux semaines. • **daily** : l'exportation a lieu tous les jours. • **weekly** : l'exportation a lieu une fois par semaine.
user *name*	(Facultatif) Spécifiez le nom du compte d'utilisateur utilisé pour se connecter à l'hôte distant; peut comporter de zéro à 510 caractères.

Modes de commande

scope org/scope cfg-export-policy/

Historique des commandes

Version	Modification
1.1.1	Commande ajoutée.

Instructions d'utilisation

Remplacer `set adminstate` par `enable`, puis exécuter une commande `commit-buffer` déclenche immédiatement une exportation de configuration.

Exemple

Cet exemple montre comment configurer la politique d'exportation de configuration par défaut, puis en vérifier les paramètres :

```
firepower # scope org
firepower /org # scope cfg-export-policy default
firepower /org/cfg-export-policy # set protocol scp
firepower /org/cfg-export-policy* # set hostname 192.168.1.2
firepower /org/cfg-export-policy* # set remote-file /export/cfg-backup.xml
firepower /org/cfg-export-policy* # set user user1
firepower /org/cfg-export-policy* # set password
Enter a password:
Confirm the password:
firepower /org/cfg-export-policy* # set schedule weekly
firepower /org/cfg-export-policy* # set adminstate enable
firepower /org/cfg-export-policy* # commit-buffer
firepower /org/cfg-export-policy # show detail
Config Export policy:
    Name: default
    Description: Configuration Export Policy
    Admin State: Enable
    Protocol: Scp
    Hostname: 192.168.1.2
    User: user1
    Remote File: /export/cfg-backup.xml
    Schedule: Weekly
    Port: Default
    Current Task:
firepower /org/cfg-export-policy #
```

Commandes associées

Commande	Description
export-config	Exporte la configuration système actuelle vers un serveur distant en tant que fichier XML; crée un objet de configuration d'exportation.
import-config	Copie un fichier de configuration XML précédemment exporté vers cet appareil.
set password-encryption-key	Spécifie une clé utilisée pour le chiffrement des informations sensibles lors de l'exportation de la configuration.

set (cfg-export-reminder)

Pour spécifier ou modifier les paramètres de l'objet de rappel d'exportation de configuration, utilisez la commande **set** en mode rappel d'exportation de configuration.

set { **adminstate** | **frequency** }

Description de la syntaxe

adminstate { **disable** | **enable**	Activer ou désactiver le rappel d'exportation. Lorsqu'il est activé, les alertes de rappel de sauvegarde de la configuration ne sont pas générées.
frequency *number_of_days*	Spécifier le nombre de jours qui peuvent s'écouler sans sauvegarde de configuration. Après cette période, le système génère une alerte de rappel. Cette valeur peut être comprise entre un et 365 jours.

Modes de commande

scope org/scope cfg-export-reminder/

Historique des commandes

Version	Modification
1.1.3	Commande ajoutée.

Instructions d'utilisation

Lorsque le rappel est activé, le système génère une alerte lorsqu'une exportation de configuration n'a pas été exécutée pendant le nombre de jours spécifié.

Exemple

Cet exemple montre comment accéder à l'objet de rappel d'exportation, l'activer, spécifier la fréquence des sauvegardes, puis afficher les paramètres :

```
firepower # scope org
firepower /org # scope cfg-export-reminder
firepower /org/cfg-export-reminder # set adminstate enable
firepower /org/cfg-export-reminder* # set frequency 30
firepower /org/cfg-export-policy* # commit-buffer
firepower /org/cfg-export-reminder # show

Config Export Reminder:
    Config Export Reminder (Days): 30
    AdminState: Enable
firepower /org/cfg-export-reminder #
```

Commandes associées

Commande	Description
scope cfg-export-policy	Permet d'accéder à la politique d'exportation de la configuration.
show	En mode rappel d'exportation de configuration, affiche la configuration de l'objet de rappel actuelle.

set cli

Pour spécifier si les lignes de sortie des commandes doivent être renvoyées à la ligne ou tronquées pour s'adapter à la largeur de la fenêtre de terminal, si les en-têtes de tableau sont affichés et si des virgules ou des espaces sont utilisés pour séparer les champs dans les tableaux de sortie des commandes, utilisez la commande **set cli**.

set cli { **suppress-field-spillover** { **off** | **on** } | **suppress-headers** { **off** | **on** } | **table-field-delimiter** { **comma** | **none** } }

Description de la syntaxe

suppress-field-spillover { **off** | **on** }	Utilisez **off** pour retourner à la ligne automatiquement dans la fenêtre du terminal. Utilisez **on** pour tronquer les lignes de sortie à la fin de la fenêtre de terminal.
suppress-headers { **off** | **on** }	Utilisez **off** pour afficher les en-têtes de tableau. Utilisez **on** pour ne pas afficher les en-têtes de tableau.
table-field-delimiter { **comma** | **none** }	Utilisez **comma** pour séparer les champs des tableaux de sortie des commandes par des virgules. Utilisez **none** pour séparer les champs des tableaux de sortie des commandes par des espaces.

Commande par défaut

Les lignes de sortie des commandes retournent à la ligne automatiquement dans la fenêtre du terminal.

Les en-têtes de tableau s'affichent.

Les espaces sont utilisés pour séparer les champs dans les tableaux de sortie des commandes.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour spécifier si les lignes de sortie des commandes doivent être renvoyées à la ligne ou tronquées pour s'adapter à la largeur de la fenêtre de terminal, si les en-têtes de tableau sont affichés et si des virgules ou des espaces sont utilisés pour séparer les champs dans les tableaux de sortie des commandes

Exemple

Cet exemple montre comment spécifier la troncation des lignes de sortie des commandes, puis comment rétablir le retour à la ligne automatique :

```
FP9300-A# set cli suppress-field-spillover on
FP9300-A# show fault
Severity  Code     Last Transition Time     ID       Description
--------- -------- ----------------------- -------- -----------
Warning   F16520   2010-01-21T18:33:22.065   5785755 [FSM:STAGE:RETRY:]: detect
mezz cards in 1/6(FSM-STAGE:sam:dme:ComputeBladeDiscover:NicPresence)
Condition F77960   2010-01-21T18:32:31.255   1089623 [FSM:STAGE:REMOTE-ERROR]: R
```

```
esult: end-point-unavailable Code: unspecified Message: sendSamDmeAdapterInfo: i
dentify failed

FP9300-A# set cli suppress-field-spillover off
FP9300-A# show fault
Severity  Code     Last Transition Time     ID       Description
--------- -------- ----------------------- -------- -----------
Warning   F16520   2010-01-21T18:33:22.065   5785755 [FSM:STAGE:RETRY:]: detect
Condition F77960   2010-01-21T18:32:31.255   1089623 [FSM:STAGE:REMOTE-ERROR]: R

FP9300-A#
```

Commandes associées

Commande	Description
show cli	Affiche les paramètres d'interface de ligne de commande actuels.
terminal	Définit le nombre et la largeur des lignes affichées dans la fenêtre de terminal.

set clock

Pour définir manuellement l'horloge dans FXOS, utilisez la commande **set clock** .

set clock

Description de la syntaxe		
	set clock	Utilisez **set clock** pour définir manuellement l'horloge dans FXOS.

Modes de commande

scope system/scope services

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Lorsque vous modifiez l'heure sur le châssis de plus de deux heures, vous devez redémarrer l'appareil dès que possible, par exemple dans une fenêtre de maintenance, pour éviter tout dysfonctionnement.

Exemple

Cet exemple montre comment définir l'horloge dans FXOS :

```
firepower# scope system
firepower /system# scope services
firepower /system/services # set clock aug 23 2021 12 00 00
firepower /system/services* # commit
firepower /system/services # show clock
Tue Aug 24 12:00:02 UTC 2021
```

set cluster-control-link network

Pour définir le réseau IP de liaison de commande de grappe dans la configuration de démarrage de grappe pour Défense contre les menaces et ASA, utilisez la commande **set cluster-control-link network**.

set cluster-control-link network *a*.*b*.**0.0**

Description de la syntaxe

a.*b*.**0.0**	Spécifie toute adresse réseau /16, à l'exception des adresses de boucle avec retour (127.0.0.0/8) et de multidiffusion (224.0.0.0/4). Si vous définissez la valeur à 0.0.0.0, le réseau par défaut est utilisé : 127.2.0.0.

Commande par défaut

Le réseau par défaut est 127.2.0.0.

Modes de commande

scope ssa/create logical-device/create cluster-bootstrap/

Historique des commandes

Version	Modification
2.4(1)	Commande ajoutée.

Instructions d'utilisation

Le châssis génère automatiquement l'adresse IP de l'interface de liaison de commande de grappe pour chaque unité en fonction de l'ID du châssis et de l'ID de logement : *a.b.chassis_id.slot_id*.

Les paramètres de démarrage sont uniquement destinés au déploiement initial ou à la reprise sur sinistre. Pour un fonctionnement normal, vous pouvez modifier la plupart des valeurs dans la configuration de l'interface de ligne de commande de l'application.

Exemple

L'exemple suivant montre comment définir le mode sur le mode routé :

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 clustered
Firepower /ssa/logical-device* # create cluster-bootstrap
firepower /ssa/logical-device/cluster-bootstrap* # set cluster-control-link network 10.10.0.0
firepower /ssa/logical-device/cluster-bootstrap* #
```

Commandes associées

Commande	Description
create logical-device	Crée le périphérique logique.
create cluster-bootstrap	Crée la configuration de démarrage de grappe de l'application.

set collection-interval

Pour définir la fréquence de collecte des statistiques de supervision, utilisez la commande **set collection-interval**.

set collection-interval *interval*

Description de la syntaxe

interval	Durée définissant l'intervalle de collecte des statistiques; les valeurs disponibles sont les suivantes : • `1minute` : intervalles d'une minute • `2minutes` : intervalles de deux minutes • `30seconds` : intervalles de 30 secondes • `5minutes` : intervalles de cinq minutes

Modes de commande

scope monitoring/scope stats-collection-policy/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez la commande **set collection-interval** pour définir la fréquence de collecte des statistiques et la commande **set reporting-interval** pour définir la fréquence à laquelle ces statistiques sont présentées. Ces intervalles définissent une politique de collecte des statistiques.

Les intervalles de production de rapports sont plus longs que les intervalles de collecte, de sorte que plusieurs points de données statistiques peuvent être collectés au cours de l'‘intervalle de production de rapports, fournissant ainsi des données suffisantes pour calculer et communiquer les valeurs minimales, maximales et moyennes.

Des statistiques peuvent être collectées et présentées pour chacun des domaines fonctionnels suivantes de votre système Firepower. Utilisez la commande **scope stats-collection-policy** pour accéder à une politique de collecte spécifique :

- `Adapter` : statistiques relatives aux adaptateurs.
- `Chassis` : statistiques relatives au châssis du serveur lame.
- `FEX` : statistiques relatives aux dispositifs d'extension de structure.
- `Host` : cette politique est un espace réservé pour une future prise en charge.
- `Port` : statistiques relatives aux ports, y compris les ports de serveur, les ports de liaison ascendante Ethernet et Fibre Channel.
- `Server` : statistiques relatives aux serveurs.

Remarque Il existe une politique de collecte de statistiques par défaut pour chacun de ces domaines fonctionnels. Vous ne pouvez pas créer de politiques de collecte de statistiques supplémentaires, ni supprimer les politiques par défaut existantes. Vous pouvez uniquement modifier les politiques par défaut.

Exemple

Cet exemple montre comment accéder à la politique de collecte de statistiques pour les ports, définir l'intervalle de collecte sur une minute, définir l'intervalle de production de rapports sur 30 minutes, puis valider la transaction :

```
firepower # scope monitoring
firepower /monitoring # scope stats-collection-policy port
firepower /monitoring/stats-collection-policy # set collection-interval 1minute
firepower /monitoring/stats-collection-policy* # set reporting-interval 30minute
firepower /monitoring/stats-collection-policy* # commit-buffer
firepower /monitoring/stats-collection-policy #
```

Commandes associées

Commande	Description
scope stats-collection-policy	Permet d'accéder au mode stats-collection-policy dans lequel vous gérez les intervalles de collecte de statistiques et de création de rapports.
set reporting-interval	Spécifie la fréquence à laquelle les statistiques sont présentées.

set con-absolute-session-timeout

Pour définir le délai d'expiration de session absolue de la console série, utilisez la commande **set con-absolute-session-timeout**.

set con-absolute-session-timeout *seconds*

Description de la syntaxe

seconds	Délai d'expiration de session absolue de la console de série; la valeur peut être comprise entre 0 et 3 600 secondes. Pour désactiver ce délai d'expiration, définissez la valeur sur 0.

Modes de commande

Mode d'authentification par défaut

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous pouvez configurer séparément le délai d'expiration absolu de la session pour les sessions de console de série. Vous pouvez en effet désactiver le délai d'expiration absolu de la session de la console de série à des fins de débogage, tout en maintenant le délai d'expiration absolu pour les autres formes d'accès.

Exemple

Cet exemple montre comment accéder au mode d'authentification par défaut, puis définir le délai d'expiration absolu de la console de série sur quatre minutes :

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set con-absolute-session-timeout 240
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

Commandes associées

Commande	Description
set refresh-period	Définit la période d'actualisation de session Web.
show detail	Affiche les paramètres de session actuelle et de délai d'expiration de session absolu.

set con-session-timeout

Pour définir le délai d'expiration de session inactive de la console série, utilisez la commande **set con-session-timeout**.

set con-session-timeout *seconds*

Description de la syntaxe

seconds	Délai d'expiration de session inactive de la console série; la valeur peut être comprise entre 0 et 3 600 secondes. Pour désactiver ce délai d'expiration, définissez la valeur sur 0.

Modes de commande

Mode d'authentification par défaut

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour spécifier le délai d'expiration de session inactive des sessions de console série.

Exemple

Cet exemple montre comment accéder au mode d'authentification par défaut, puis définir le délai d'expiration de session inactive de la console série sur quatre minutes :

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set con-session-timeout 240
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

Commandes associées

Commande	Description
set refresh-period	Définit la période d'actualisation de session Web.
show detail	Affiche les paramètres de session actuelle et de délai d'expiration de session absolu.

set cpu-core-count

Pour définir les cœurs de CPU pour un profil de ressource à utiliser avec des instances de contenant, utilisez la commande **set cpu-core-count**.

set cpu-core-count *cores*

Description de la syntaxe

cores	Spécifie un nombre pair de cœurs pour le profil, entre 6 et le maximum, selon votre châssis. Vous *ne pouvez pas* indiquer 8 cœurs.

Modes de commande

scope ssa/create resource-profile/

Historique des commandes

Version	Modification
2.4(1)	Commande ajoutée.

Instructions d'utilisation

Pour spécifier l'utilisation des ressources par instance de conteneur, créez un ou plusieurs profils de ressource. Lorsque vous déployez l'instance d'application ou de périphérique logique, vous spécifiez le profil de ressource que vous souhaitez utiliser. Le profil de ressource définit le nombre de cœurs de CPU; la mémoire RAM est allouée de façon dynamique en fonction du nombre de cœurs et l'espace disque est défini sur 40 Go par instance.

- Le nombre minimum de cœurs est de 6.
- Compte tenu de l'architecture interne, vous ne pouvez pas spécifier 8 cœurs.
- Vous pouvez affecter un nombre pair de cœurs (6, 10, 12, 14, etc.) jusqu'au nombre maximal.
- Le nombre maximal de cœurs disponibles dépend du module de sécurité ou du modèle de châssis.

Le châssis comprend un profil de ressource par défaut appelé « Default-Small », qui comprend le nombre minimal de cœurs. Vous pouvez modifier la définition de ce profil et même le supprimer s'il n'est pas utilisé. Notez que ce profil est créé lors du rechargement du châssis et qu'aucun autre profil n'existe sur le système.

Vous ne pouvez pas modifier les paramètres du profil de ressource s'il est actuellement utilisé. Vous devez désactiver toutes les instances qui l'utilisent, puis modifier le profil de ressource et enfin réactiver l'instance. Si vous redimensionnez des instances dans une paire à haute disponibilité établie, vous devez définir une taille identique pour tous les membres dès que possible.

Si vous modifiez les paramètres du profil de ressource après avoir ajouté l'instance Défense contre les menaces au centre de gestion, mettez à jour l'inventaire de chaque unité dans la boîte de dialogue **Appareils** > **Gestion des appareils** > **Appareil** > **Système** > **Inventaire**.

Exemple

Dans l'exemple suivant, trois profils de ressource sont ajoutés.

```
firepower# scope ssa
firepower /ssa # enter resource-profile basic
firepower /ssa/resource-profile* # set description "lowest level"
firepower /ssa/resource-profile* # set cpu-core-count 6
```

```
firepower /ssa/resource-profile* # exit
firepower /ssa # enter resource-profile standard
firepower /ssa/resource-profile* # set description "middle level"
firepower /ssa/resource-profile* # set cpu-core-count 10
firepower /ssa/resource-profile* # exit
firepower /ssa # enter resource-profile advanced
firepower /ssa/resource-profile* # set description "highest level"
firepower /ssa/resource-profile* # set cpu-core-count 12
firepower /ssa/resource-profile* # commit-buffer
firepower /ssa/resource-profile #
```

Commandes associées

Commande	Description
create resource-profile	Ajoute un profil de ressource à utiliser avec les instances de contenant.
set resource-profile-name	Affecte le profil de ressource à l'instance d'application.
show monitor detail	Affiche l'utilisation des ressources pour le module de sécurité ou le logement de moteur.
show resource detail	Affiche l'affectation de ressources pour l'instance d'application.
show resource-profile user-defined	Affiche les affectations de profils de ressource.

set deploy-type

Pour définir le type de déploiement d'une instance d'application, native ou de contenant, utilisez la commande **set deploy-type**.

set deploy-type {**native** | **container**}

Description de la syntaxe

container	Définit l'instance d'application sur le type de contenant.
native	Définit l'instance d'application sur le type natif.

Commande par défaut Le type par défaut est natif.

Modes de commande scope ssa/scope slot/create app-instance/

Historique des commandes

Version	Modification
2.4(1)	Commande ajoutée pour Défense contre les menaces.

Instructions d'utilisation

Les instances d'application du périphérique logique s'exécutent dans les types de déploiement suivants :

- Instance native : une instance native utilise toutes les ressources (CPU, RAM et espace disque) du module/moteur de sécurité, de sorte que vous ne pouvez installer qu'une seule instance native.
- Instance de conteneur : une instance de conteneur utilise un sous-ensemble de ressources du module/moteur de sécurité, de sorte que vous pouvez installer plusieurs instances de conteneur. La capacité multi-instances n'est prise en charge que pour Défense contre les menaces; elle n'est pas prise en charge par l'ASA.

Remarque La capacité multi-instance est similaire au mode à contexte multiple ASA, bien que son implémentation soit différente. Le mode contexte multiple partitionne une seule instance d'application, tandis que la capacité multi-instance permet des instances de conteneur indépendantes. Les instances de conteneur permettent la séparation des ressources matérielles, la gestion distincte de la configuration, des rechargements distincts, des mises à jour logicielles distinctes et la prise en charge complète de la fonctionnalité Défense contre les menaces. Le mode contexte multiple, en raison des ressources partagées, prend en charge plus de contextes sur une plateforme donnée. Le mode contexte multiple n'est pas disponible sur Défense contre les menaces.

Pour le Firepower 9300, vous pouvez utiliser une instance native sur certains modules et des instances de conteneurs sur le(s) autre(s) module(s).

Exemple

L'exemple suivant ajoute une instance d'application Défense contre les menaces et la définit pour le type de contenant :

```
Firepower# scope ssa
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd MyDevice1
Firepower /ssa/slot/app-instance* # set deploy-type container
Firepower /ssa/slot/app-instance* # set resource-profile-name silver 1
Firepower /ssa/slot/app-instance* # set startup-version 6.3.0.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

Commandes associées

Commande	Description
show app-attri	Affiche les attributs de l'application actuelle.
create resource-profile	Crée un profil de ressource à utiliser avec les instances de contenant.
show resource-profile-name	Affiche les profils de ressources disponibles.

set descr

Pour définir une description du canal de port, utilisez la commande **set descr**.

set descr *description*

Description de la syntaxe

description	(Facultatif) Description. Saisissez jusqu'à 256 caractères.

Modes de commande

scope eth-uplink/scope fabric a/port-channel/

Historique des commandes

Version	Modification
2.0.1	Commande ajoutée.

Instructions d'utilisation

Si votre description comprend des espaces, des caractères spéciaux ou des ponctuations, vous devez la délimiter par des guillemets. Les guillemets n'apparaissent pas dans le champ de description d'une sortie de commande Ethernet.

Exemple

Cet exemple montre comment définir la description :

```
firepower-9300 # scope eth-uplink
firepower-9300 /eth-uplink # scope fabric a
firepower-9300 /eth-uplink/fabric # create port-channel id
firepower-9300 /eth-uplink/fabric/port-channel* # enable
firepower-9300 /eth-uplink/fabric/port-channel* # set descr "link"
firepower-9300 /eth-uplink/fabric/port-channel* # commit-buffer
firepower-9300 /eth-uplink/fabric/port-channel #
```

Commandes associées

Commande	Description
show interface	Affiche les informations sur l'interface, notamment le paramètre de duplex.

set duplex

Pour définir le mode duplex pour tous les membres du canal de port, utilisez la commande **set duplex**.

set duplex {**fullduplex** | **halfduplex**}

Description de la syntaxe

fullduplex	(Facultatif) Définit le mode duplex sur intégral.
halfduplex	(Facultatif) Définit le mode duplex sur semi-duplex.

Modes de commande

scope eth-uplink/scope fabric a/port-channel/

Historique des commandes

Version	Modification
2.0.1	Commande ajoutée.

Instructions d'utilisation

Vous devez définir la vitesse avant de définir le mode duplex. Si vous définissez une vitesse de 10 ou 100 Mbit/s, le port est automatiquement configuré pour utiliser le mode semi-duplex, mais vous pouvez indiquer le mode duplex intégral. Gigabit Ethernet n'est proposé qu'en mode duplex intégral. Vous ne pouvez pas modifier le mode duplex sur les ports Gigabit Ethernet ou sur un port de 10/100/1000 Mbit/s défini pour Gigabit Ethernet.

Exemple

Cet exemple montre comment définir le mode duplex de l'interface :

```
firepower-9300# scope eth-uplink
firepower-9300 /eth-uplink # scope fabric a
firepower-9300 /eth-uplink/fabric # create port-channel id
firepower-9300 /eth-uplink/fabric/port-channel* # enable
firepower-9300 /eth-uplink/fabric/port-channel* # set duplex halfduplex
firepower-9300 /eth-uplink/fabric/port-channel* # commit-buffer
firepower-9300 /eth-uplink/fabric/port-channel #
```

Commandes associées

Commande	Description
show interface	Affiche des informations sur l'interface, notamment le paramètre duplex.

set email

Pour définir une adresse de courriel de contact pour un compte d'utilisateur, utilisez la commande **set email**.

set email *email_address*

Description de la syntaxe

email_address	Adresse de courriel pour le compte d'utilisateur. Spécifiez l'adresse de courriel au format : *nom_utilisateur@nom_domaine*.

Modes de commande

Mode Callhome (/monitoring/callhome) : pour spécifier une adresse de courriel de contact principale à inclure dans les messages Call Home.

Mode utilisateur local (/security/local-user) : – pour spécifier une adresse de courriel de contact pour l'utilisateur local actuel.

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Si l'adresse de courriel contient des caractères spéciaux, tels que # (dièse), des espaces ou & (esperluette), le serveur de messagerie peut ne pas être en mesure d'acheminer les courriels à cette adresse. Cisco recommande d'utiliser des adresses de courriel conformes aux RFC2821 et RFC2822, et contenant uniquement des caractères ASCII 7 bits.

En mode Callhome, vous pouvez utiliser un maximum de 2 083 caractères pour l'adresse de courriel.

En mode utilisateur local, vous pouvez utiliser un maximum de 510 caractères pour l'adresse de courriel.

Exemple

Cet exemple montre comment spécifier une adresse de courriel pour l'utilisateur local actuel :

```
FP9300-A /security/local-user # set email admin@example.com
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

Commandes associées

Commande	Description
create local-user	Crée un compte d'utilisateur local.
set phone-contact	Spécifie un numéro de téléphone pour un compte Smart Call Home.

set enforce-strong-password

Pour activer et désactiver l'application de mots de passe forts, utilisez la commande **set enforce-strong-password**.

set enforce-strong-password {**no** | **yes**}

Description de la syntaxe

no	Désactive l'application de mots de passe forts.
yes	Active l'application de mots de passe forts.

Modes de commande

Mode sécurité

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Un mot de passe est requis pour chaque compte d'utilisateur authentifié localement. Un utilisateur avec des privilèges d'administrateur ou AAA peut configurer le système pour effectuer une vérification de la force des mots de passe de tous les utilisateurs. Si la vérification de la force des mots de passe est activée, chaque utilisateur doit disposer d'un mot de passe fort.

Nous vous recommandons d'utiliser des mots de passe robustes pour chaque utilisateur. Si la vérification de la force des mots de passe est activée pour les utilisateurs authentifiés localement, FXOS rejette tout mot de passe qui ne répond pas aux exigences suivantes :

- Doit contenir un minimum de 8 caractères et un maximum de 80 caractères. (La commande set min-password-length, à la page 319 peut être utilisée pour spécifier le nombre minimal de caractères requis.)
- Doit contenir au moins un caractère alphabétique majuscule.
- Doit contenir au moins un caractère alphabétique minuscule.
- Doit inclure au moins un caractère non alphanumérique (spécial).
- Ne doit pas contenir un caractère répété plus de trois fois consécutives, comme aaabbb.
- Ne doit pas contenir trois chiffres ou lettres consécutifs dans n'importe quel ordre, comme motdepasseABC ou motdepasse321.
- Ne doit pas être identique au nom d'utilisateur ou à l'inverse du nom d'utilisateur.
- Doit passer une vérification effectuée à l'aide d'un dictionnaire de mots de passe. Par exemple, le mot de passe ne doit pas être basé sur un mot du dictionnaire standard.
- Ne doit pas contenir les symboles suivants : $ (signe de dollar), ? (point d'interrogation) et = (signe d'égalité).
- Ne doit pas être vide pour les comptes d'utilisateurs et d'administrateurs locaux.

Exemple

Cet exemple montre comment accéder au mode sécurité et activer l'application de mots de passe forts :

```
FP9300-A# scope security
FP9300-A /security # set enforce-strong-password yes
FP9300-A /security* # commit-buffer
FP9300-A /security #
```

Commandes associées

Commande	Description
set min-password-length	Spécifie une longueur de mot de passe minimale.

set expiration

Pour définir une date d'expiration pour un compte d'utilisateur local, utilisez la commande **set expiration**.

set expiration { { **apr** | **aug** | **dec** | **feb** | **jan** | **jul** | **jun** | **mar** | **may** | **nov** | **oct** | **sep** } *day* *year* }

Description de la syntaxe

{ **apr** | **aug** | **dec** | **feb** | **jan** | **jul** | **jun** | **mar** | **may** | **nov** | **oct** | **sep** }	Abréviation du mois en trois lettres.
day	Jour numérique du mois; les valeurs valides sont comprises entre 1 et 31.
year	Année numérique d'expiration; la valeur maximale est 2037.

Modes de commande

Mode utilisateur local : pour spécifier une date d'expiration pour l'utilisateur local actuel.

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Après avoir configuré un compte d'utilisateur avec une date d'expiration, vous ne pouvez pas reconfigurer le compte pour qu'il n'expire pas. Vous pouvez cependant configurer le compte avec la dernière date d'expiration disponible.

Exemple

Cet exemple montre comment accéder au mode sécurité, créer un nouveau compte d'utilisateur local et spécifier une date d'expiration pour ce compte :

```
FP9300-A# scope security
FP9300-A /security # create local-user test_user
FP9300-A /security/local-user* # set expiration dec 31 2019
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

Commandes associées

Commande	Description
create local-user	Crée un nouveau compte d'utilisateur local.
set password	Spécifie un mot de passe pour un compte d'utilisateur.

set (configuration d'exportation)

Pour modifier les paramètres d'un objet de configuration d'exportation existant, utilisez la commande **set** en mode configuration d'exportation.

set {**descr** | **password** | **port** | **protocol** | **remote-file** | **user**}

Description de la syntaxe

descr *description*	(Facultatif) Vous pouvez ajouter une description à l'objet de configuration; peut comporter de 1 à 256 caractères. La plupart des caractères alphanumériques sont autorisés, de même que les tirets et les traits de soulignement. La chaîne peut se terminer par des signes de ponctuation comme un point-virgule, un point et un point d'exclamation, mais vous ne pouvez pas intégrer ces caractères dans la description.
password	(Facultatif) Vous pouvez modifier le mot de passe utilisé pour se connecter au serveur distant; vous êtes invité à saisir, puis à confirmer le mot de passe.
port {*number* | **default**}	(Facultatif) Vous pouvez modifier le port sur lequel les communications avec le serveur distant ont lieu. Les options correspondent à un numéro d'ID de port compris entre zéro et 4294967295, ou **default** pour le port par défaut du protocole actuel.
protocol *name*	(Facultatif) Vous pouvez modifier le protocole de transfert de fichiers utilisé pour transmettre la sauvegarde de configuration au serveur distant. Les options disponibles sont les suivantes : • **ftp** • **scp** • **sftp** • **tftp**
remote-file *name*	(Facultatif) Vous pouvez modifier le nom du fichier de configuration de sauvegarde; peut comporter de 1 à 128 caractères.
user *name*	(Facultatif) Vous pouvez modifier le nom du compte d'utilisateur utilisé pour se connecter à l'hôte distant; peut comporter de zéro à 510 caractères.

Modes de commande

scope system/scope export-config/

Historique des commandes

Version	Modification
1.1.3	Commande ajoutée.

Instructions d'utilisation

Utilisez ces options pour modifier les options de sauvegarde d'un objet de configuration d'exportation existant.

Un objet de configuration d'exportation est créé lorsque vous exécutez une commande **export-config** pour sauvegarder la configuration actuelle du périphérique logique et de la plateforme, et que la commande **scope export-config** est utilisée pour accéder à l'objet et modifier ses paramètres.

Veuillez noter les points suivants :

- À partir de FXOS 2.6.1, vous devez spécifier une clé à utiliser lors du chiffrement d'informations sensibles telles que les mots de passe et autres clés secrètes durant l'exportation de la configuration, et vous devez l'avoir spécifiée avant de tenter d'exporter la configuration.

  De plus, la même clé utilisée lors de l'exportation doit être définie sur le système cible lorsque vous importez une configuration exportée, sauf si le fichier a été exporté à partir d'une version FXOS antérieure à la version 2.6.1, auquel cas le système cible ne vérifie pas la clé de chiffrement et autorise l'importation.

- Ne modifiez pas le contenu du fichier de configuration. Si un fichier de configuration est modifié, l'importation de la configuration à l'aide de ce fichier peut échouer.

- Pour éviter d'écraser les fichiers de sauvegarde existants, veillez à modifier le nom du fichier lors de l'opération d'exportation ou copiez le fichier existant à un autre emplacement.

Exemple

Cet exemple montre comment ajouter une description à un objet de configuration d'exportation existant :

```
firepower # scope system
firepower /system # scope export-config 192.168.1.2
firepower /system/export-config # set descr one-time_back-up_be_sure_to_change_file_name
firepower /system/export-config* # commit-buffer
firepower /system/export-config #
```

Commandes associées

Commande	Description
cfg-export-policy	Configure une politique d'exportation de configuration.
export-config	Exporte la configuration système actuelle vers un serveur distant en tant que fichier XML; crée un objet de configuration d'exportation.
import-config	Copie un fichier de configuration XML précédemment exporté vers cet appareil.
set password-encryption-key	Spécifie une clé utilisée pour le chiffrement des informations sensibles lors de l'exportation de la configuration.

set firstname

Pour spécifier le prénom d'un utilisateur local, utilisez la commande **set firstname**.

set firstname *name*

Description de la syntaxe

name	Prénom de l'utilisateur; peut comporter de 0 à 32 caractères.

Modes de commande

Mode utilisateur local

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment accéder au mode sécurité, créer un nouveau compte d'utilisateur local et spécifier le nom et le prénom de cet utilisateur :

```
FP9300-A# scope security
FP9300-A /security # create local-user test_user
FP9300-A /security/local-user* # set firstname john
FP9300-A /security/local-user* # set lastname doe
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

Commande	Description
create local-user	Crée un compte d'utilisateur local.
set lastname	Spécifie le nom d'un compte d'utilisateur local.

set flow-control-policy

Pour affecter une politique de contrôle de flux à une interface ou à un canal de port, utilisez la commande **set flow-control-policy**.

set flow-control-policy *name*

Description de la syntaxe

name	Nom de la politique de contrôle de flux; 16 caractères maximum.

Modes de commande

scope eth-uplink/scope fabric a/scope interface/

scope eth-uplink/scope fabric a/scope port-channel/

Historique des commandes

Version	Modification
2.0.1	Commande ajoutée.

Instructions d'utilisation

Lorsque vous créez une politique de contrôle de flux, vous accédez automatiquement au mode contrôle de flux/politique (eth-uplink/flow-control/policy) accompagné d'un astérisque pour indiquer que la nouvelle politique n'est pas encore validée. Vous pouvez définir des valeurs de propriété, puis valider la nouvelle politique. Une fois la politique de contrôle de flux créée, son nom ne peut pas être modifié. Vous devez supprimer la politique et en créer une nouvelle.

Exemple

Cet exemple montre comment affecter une politique de contrôle de flux à une interface :

```
firepower-9300 # scope eth-uplink
firepower-9300 /eth-uplink # scope fabric
firepower-9300 /eth-uplink #/fabric # scope interface Ethernet1/8
firepower-9300 /eth-uplink/fabric/interface* # set flow-control-policy eth1-8flowcontrol
firepower-9300 /eth-uplink/fabric/interface* # commit-buffer
firepower-9300 /eth-uplink/fabric/interface #
```

Commandes associées

Commande	Description
create policy (flow control)	Crée une politique de contrôle de flux.
show interface	Affiche l'état de l'interface, qui comprend les paramètres de vitesse.
show port-channel	Affiche les informations sur un canal de port.

set (politique de contrôle de flux)

Pour spécifier ou modifier les paramètres d'une politique de contrôle de flux existante, utilisez la commande **set** en mode contrôle de flux/politique.

set {**prio** | **receive** | **send**}

Description de la syntaxe

prio {**auto** | **on**	Définit l'option de priorité de contrôle de flux : • **auto** : cet appareil et le réseau négocient si le protocole PPP (Point-to-Point Protocol) est utilisé sur cette structure. • **on** : le protocole PPP est activé sur cette structure.
receive off	Spécifie si les demandes de pause provenant du réseau sont ignorées et le flux de trafic se poursuit normalement.
send off | **on**	Définit le paramètre d'envoi de contrôle de flux : • **off** : le trafic circule normalement, quelle que soit la charge de paquets. • **on** : cet appareil envoie une demande de pause au réseau si le tampon de paquets entrants est saturé. La mise en pause est effective pendant quelques millisecondes, jusqu'à ce que le trafic revienne à des niveaux normaux.

Modes de commande

scope eth-uplink/scope flow-control/policy/

Historique des commandes

Version	Modification
1.1.1	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour spécifier les options de réception de contrôle de flux. En cas de désactivation, les demandes de pause provenant du réseau sont ignorées et le flux de trafic se poursuit normalement. En cas d'activation, les demandes de pause sont honorées et tout le trafic est arrêté sur ce port de liaison ascendante jusqu'à ce que le réseau annule la demande de pause.

Utilisez cette commande pour spécifier les options d'envoi de contrôle de flux. Lorsque vous spécifiez **off**, le trafic sur le port circule normalement, quelle que soit la charge de paquets. Lorsque vous spécifiez **on**, FXOS envoie une demande de pause au réseau si le débit de paquets entrants devient trop élevé. La pause demeure active pendant quelques millisecondes avant que le trafic ne soit réinitialisé à des niveaux normaux.

Exemple

Cet exemple montre comment créer et saisir une politique nommée pour le contrôle de flux, puis définir les paramètres de cette politique :

```
firepower # scope eth-uplink
firepower /eth-uplink # scope flow-control
firepower /eth-uplink/flow-control # enter policy FCpolicy1
firepower /eth-uplink/flow-control/policy* # set prio auto
firepower /eth-uplink/flow-control/policy* # set send on
```

```
firepower /eth-uplink/flow-control/policy* # commit-buffer
firepower /eth-uplink/flow-control/policy #
```

Commandes associées

Commande	Description
show policy	En mode contrôle de flux/politique, affiche les valeurs de propriété de la politique de contrôle de flux actuelle. En mode contrôle de flux, affiche les valeurs de propriété de toutes les politiques de contrôle de flux actuellement définies.

set frequency

Pour générer une défaillance lorsqu'une exportation de configuration n'a pas été exécutée depuis un certain nombre de jours, utilisez la commande **set frequency**.

set frequency *days*

Description de la syntaxe

days	Rappel d'exportation de la configuration (jours).

Modes de commande

scope org/scope cfg-export-reminder/

Historique des commandes

Version	Modification
2.0.1	Commande ajoutée.

Exemple

Cet exemple montre comment définir les jours de fréquence de configuration pour le rappel d'exportation :

```
firepower-9300* # scope org
firepower-9300 /org* # scope cfg-export-reminder
firepower-9300 /org/scope cfg-export-reminder* # set frequency 2
firepower-9300 /org/scope cfg-export-reminder* # commit-buffer
firepower-9300 /org/scope cfg-export-reminder* # show detail
Config Export Reminder:
Config Export Reminder (Days): 10
AdminState: Enable
```

Commandes associées

Commande	Description
set adminstate	Spécifie l'état d'administration pour le rappel d'exportation.

set http-proxy-server-enable

Pour activer ou désactiver un proxy HTTP/HTTPS pour les licences logicielles Smart et Smart Call Home, utilisez la commande **set http-proxy-server-enable**.

set http-proxy-server-enable { **off** | **on** }

Description de la syntaxe

off	Désactive le proxy HTTP/HTTPS Smart Call Home.
on	Active le proxy HTTP/HTTPS Smart Call Home.

Commande par défaut Le proxy HTTP/HTTPS est désactivé par défaut.

Modes de commande Mode Callhome

Instructions d'utilisation

Si votre réseau utilise un proxy HTTP pour l'accès Internet, vous devez activer ce proxy et configurer son adresse pour les licences logicielles Smart. Ce mandataire est également utilisé pour Smart Call Home en général.

Exemple

Cet exemple montre comment activer un proxy HTTP :

```
FP9300-A# scope monitoring
FP9300-A /monitoring # scope callhome
FP9300-A /monitoring/callhome # set http-proxy-server-enable on
FP9300-A /monitoring/callhome #
```

Commandes associées

Commande	Description
set http-proxy-server-url	Définit l'adresse HTTP ou HTTPS du serveur proxy.
set http-proxy-server-port	Définit le port de communication pour le serveur proxy.

set http-proxy-server-port

Pour définir le port du serveur proxy HTTP/HTTPS pour la gestion des licences logicielles Smart et Smart Call Home, utilisez la commande **set http-proxy-server-port**.

set http-proxy-server-port *port_number*

Description de la syntaxe

port_number	Port du serveur proxy HTTP ou HTTPS; la plage se situe entre 1 et 65 535.

Commande par défaut

Le proxy HTTP/HTTPS est désactivé par défaut. Le proxy doit être activé avant de saisir l'adresse du serveur et le numéro du port.

Modes de commande

Mode Callhome

Instructions d'utilisation

Si votre réseau utilise un proxy HTTP pour l'accès Internet, vous devez activer ce proxy et configurer son adresse pour les licences logicielles Smart. Ce mandataire est également utilisé pour Smart Call Home en général.

Exemple

Cet exemple montre comment saisir un numéro de port de serveur proxy HTTP/HTTPS :

```
FP9300-A# scope monitoring
FP9300-A /monitoring # scope callhome
FP9300-A /monitoring/callhome # set http-proxy-server-port 443
FP9300-A /monitoring/callhome #
```

Commandes associées

Commande	Description
set http-proxy-server-enable	Active ou désactive le proxy HTTP/HTTPS pour les licences logicielles Smart et Smart Call Home.
set http-proxy-server-url	Définit l'adresse HTTP/HTTPS du serveur proxy.

set http-proxy-server-url

Pour définir l'adresse du serveur proxy HTTP/HTTPS pour la gestion des licences logicielles Smart et Smart Call Home, utilisez la commande **set http-proxy-server-url**.

set http-proxy-server-url *URL*

Description de la syntaxe

URL	Adresse HTTP ou HTTPS du serveur proxy; peut comporter un maximum de 2 083 caractères.

Commande par défaut Le proxy HTTP/HTTPS est désactivé par défaut. Le proxy doit être activé avant de saisir l'adresse du serveur.

Modes de commande Mode Callhome

Instructions d'utilisation Si votre réseau utilise un proxy HTTP pour l'accès Internet, vous devez activer ce proxy et configurer son adresse pour les licences logicielles Smart. Ce mandataire est également utilisé pour Smart Call Home en général.

Exemple

Cet exemple montre comment accéder à une adresse de serveur proxy HTTPS :

```
FP9300-A# scope monitoring
FP9300-A /monitoring # scope callhome
FP9300-A /monitoring/callhome # set http-proxy-server-url https://209.165.201.10
FP9300-A /monitoring/callhome #
```

Commandes associées

Commande	Description
set http-proxy-server-enable	Active ou désactive le proxy HTTP/HTTPS pour les licences logicielles Smart et Smart Call Home.
set http-proxy-server-port	Définit le port de communication pour le serveur proxy.

set https

Pour spécifier les paramètres de service HTTPS, utilisez la commande **set https**.

set https {**auth-type** {**cert-auth** | **cred-auth**} | **cipher-suite** *cipher_string* | **cipher-suite-mode** {**custom** | **high-strength** | **low-strength** | **medium-strength**} | **crl-mode** {**relaxed** | **strict**} | **keyring** *keyring_name* | **port** *port_number*}

Description de la syntaxe

auth-type {**cert-auth** | **cred-auth**}	(Facultatif) Spécifie le type d'authentification à utiliser pour l'accès HTTPS : • **cert-auth** : permet au système d'utiliser un certificat client conjointement avec LDAP afin d'authentifier les utilisateurs pour l'accès HTTPS. • **cred-auth** : permet au système d'utiliser l'authentification d'utilisateur basée sur les identifiants pour l'accès HTTPS.
cipher-suite *cipher_string*	(Facultatif) Spécifie la chaîne de définition de la suite de chiffrement à utiliser avec la commande personnalisée **cipher-suite-mode**. La chaîne de spécification peut contenir jusqu'à 256 caractères et doit être conforme aux spécifications de la suite de chiffrement OpenSSL. Vous ne pouvez pas utiliser d'espaces ni de caractères spéciaux, à l'exception des suivants : ! (point d'exclamation), + (signe plus), - (trait d'union) et : (deux-points). Voir http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite pour de plus amples informations. **Remarque** Cette chaîne est ignorée si **cipher-suite-mode** est défini sur une autre valeur que **custom**.

cipher-suite-mode {**custom** | **high-strength** | **low-strength**	(Facultatif) Définit le niveau de sécurité de la suite de chiffrement utilisé : • **custom** : permet de définir une chaîne de spécification de sécurité personnalisée pour la suite de chiffrement à l'aide de l'option **cipher-suite**. • **high-strength**—ALL:!EDH-RSA-DES-CBC3-SHA: !EDH-DSS-DES-CBC3-SHA: !DES-CBC3-SHA:!ADH:!3DES: !EXPORT40:!EXPORT56:!LOW:!MEDIUM:!eNULL:!RC4:!MD5: !IDEA:+HIGH:+EXP • **low-strength**—ALL:!EDH-RSA-DES-CBC3-SHA: !EDH-DSS-DES-CBC3-SHA: !DES-CBC3-SHA:!ADH:!3DES: !EXPORT40:!EXPORT56:RC4+RSA: !IDEA:+HIGH:+MEDIUM:+LOW:+EXP:+eNULL • **medium-strength**—ALL:!EDH-RSA-DES-CBC3-SHA: !EDH-DSS-DES-CBC3-SHA: !DES-CBC3-SHA:!ADH:!3DES:!EXPORT40:!EXPORT56: !LOW:!RC4:!MD5:!IDEA:+HIGH:+MEDIUM:+EXP:+eNULL En général, la force d'un chiffrement est globalement basée sur les bits de sécurité (ou taille de clé symétrique), « faible » signifie moins de 128 bits de sécurité, « moyen » est égal à 128 bits et « élevé » signifie plus de 128 bits de sécurité.
crl-mode {**relaxed** | **strict**}	(Facultatif) Définit le niveau de vérification des listes de révocation de certificats (CRL) pour les connexions HTTPS : • **relaxed** : les certificats trouvés sur une CRL peuvent être utilisés pour permettre l'authentification HTTPS, selon la raison de leur inscription; un message d'avertissement est enregistré chaque fois que cela se produit. Désactive principalement la vérification de la CRL. • **strict** : l'authentification de la connexion échoue pour tout certificat figurant sur une CRL; un message d'avertissement est enregistré chaque fois que cela se produit. La CRL doit également être à jour.
keyring *keyring_name*	(Facultatif) Spécifie le nom du trousseau de clés RSA à utiliser pour les connexions HTTPS.
port *port_number*	(Facultatif) Spécifie le port à utiliser pour les connexions HTTPS; peut être compris entre 1 et 65535. La valeur par défaut est 443.

Commande par défaut

Sur le châssis Firepower 4100/9300, la configuration d'authentification par défaut est basée sur les informations d'authentification.

Le niveau de sécurité par défaut de la suite de chiffrement est moyen.

Modes de commande

Mode service

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Si l'authentification par certificat est activée, est constituera la seule forme d'authentification autorisée pour le protocole HTTPS.

Le certificat client doit respecter les exigences suivantes pour utiliser cette fonctionnalité :

- Le nom d'utilisateur doit être inclus dans l'attribut X509 Autre nom de l'objet - Courriel.
- Le certificat client doit être signé par une autorité de certification racine dont le certificat a été importé dans un point de confiance sur le superviseur.

Mise en garde Lorsque vous appliquez la plupart de ces paramètres de configuration (notamment le trousseau de clés, le port, la suite de chiffrement et le mode de suite de chiffrement personnalisé), toutes les sessions HTTP et HTTPS actives sont fermées sans avertissement pour l'utilisateur

Exemple

Cet exemple montre comment activer l'authentification par certificat pour l'accès HTTPS :

```
FP9300-A# scope system
FP9300-A /system # scope services
FP9300-A /system/services # set https auth-type cert-auth
FP9300-A /system/services* # commit-buffer
FP9300-A /system/services #
```

Commandes associées

Commande	Description
enable https	Active le service HTTPS.
show https	Affiche la configuration actuelle du service HTTPS.

set (interface)

Pour spécifier ou modifier les paramètres d'une interface, utilisez la commande **set** en mode interface.

set
{**admin-duplex** | **admin-speed** | **auto-negotiation** | **descr** | **eth-link-profile** | **flow-control-policy** | **nw-ctrl-policy** | **port-type** | **user-label** }

Description de la syntaxe

admin-duplex {**fullduplex** | **halfduplex** }	Définit le mode duplex pour l'interface : • **fullduplex** : spécifie les communications bidirectionnelles simultanées. • **halfduplex** : spécifie les communications unidirectionnelles alternées.
admin-speed {**100gbps** | **100mbps** | **10gbps** | **10mbps** | **1gbps** | **40gbps** }	Spécifiez la vitesse de transfert des données de l'interface : • **100gbps** : cent gigabits par seconde. • **100mbps** : cent mégabits par seconde. • **10gbps** : dix gigabits par seconde. • **10mbps** : dix mégabits par seconde. • **1gbps** : un gigabit par seconde. • **40gbps** : quarante gigabits par seconde.
auto-negotiation {**no** | **yes** }	Active ou désactive la négociation automatique des paramètres de transmission communs tels que la vitesse, les conditions de duplex et le contrôle de flux. • **no** : désactive la négociation automatique. • **yes** : active la négociation automatique.
descr *description*	Vous pouvez ajouter une description à l'interface; la description peut comporter entre zéro et 256 caractères. La plupart des caractères alphanumériques sont autorisés, de même que les tirets et les traits de soulignement. Les espaces ne sont pas autorisés. La chaîne peut se terminer par des signes de ponctuation comme un point-virgule, un point et un point d'exclamation, mais vous ne pouvez pas intégrer ces caractères dans la description.
eth-link-profile *name*	Vous pouvez affecter un profil de liaison Ethernet à l'interface, ce qui configure automatiquement l'interface en fonction des paramètres de profil. Indiquez le nom du profil; peut comporter jusqu'à 16 caractères alphanumériques.
flow-control-policy *name*	Vous pouvez affecter une politique de contrôle de flux à l'interface; indiquez le nom de la politique, qui peut comporter jusqu'à 16 caractères alphanumériques.
nw-ctrl-policy *name*	Vous pouvez affecter une politique de contrôle de réseau à l'interface; indiquez le nom de la politique, qui peut comporter jusqu'à 16 caractères alphanumériques.

port-type {**cluster** | **data** | **data-sharing** | **firepower-eventing** | **mgmt** }	Spécifiez le type ou la fonction de l'interface : • **cluster** : spécifiez **cluster** uniquement si vous souhaitez utiliser cette interface comme liaison de commande de grappe. • **data** : permet la transmission régulière de données. Il s'agit du type par défaut. • **data-sharing** – Utiliser pour des données régulières; uniquement pris en charge avec les instances de conteneur. • **firepower-eventing** : utilisez cette interface en tant qu'interface de gestion secondaire pour les appareils Défense contre les menaces. L'interface firepower-eventing est utiliser pour acheminer tout le trafic des événements (comme les événements Web). • **mgmt** : permet de gérer les instances d'application. Vous ne pouvez affecter qu'une seule interface de gestion par périphérique logique. Consultez set port-type, à la page 337 pour plus d'informations sur cette commande.
user-label *étiquette*	Vous pouvez appliquer une étiquette de description à cette interface; peut comporter entre zéro et 16 caractères alphanumériques.

Modes de commande

scope eth-uplink/scope fabric a/interface/

Historique des commandes

Version	Modification
2.4(1)	Nous avons ajouté le type **data-sharing**.
1.1(4)	Nous avons ajouté le type **firepower-eventing**.
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Le type `cluster` est un type d'interface spécial utilisé pour un périphérique logique en grappe. Ce type est automatiquement attribué au lien de contrôle de grappe pour les communications inter-unités de grappe. Par défaut, la liaison de commande de grappe est automatiquement créée sur le canal de port 48.

Les interfaces de données ne peuvent pas être partagées entre les périphériques logiques.

Le type `data-sharing` est uniquement pris en charge avec les instances de conteneur. Ces interfaces de données peuvent être partagées par un ou plusieurs périphériques logiques/instances de conteneur (Défense contre les menaces uniquement). Chaque instance de contenant peut communiquer sur le fond de panier avec toutes les autres instances qui partagent cette interface. Les interfaces partagées peuvent avoir une incidence sur le nombre d'instances de conteneur que vous pouvez déployer. Les interfaces partagées ne sont pas prises en charge pour les interfaces de membre de groupe de ponts (en mode transparent ou en mode routage), les ensembles en ligne, les interfaces passives ou les liaisons de basculement.

Une interface `firepower-eventing` est une interface de gestion secondaire pour les appareils Défense contre les menaces. Pour utiliser cette interface, vous devez configurer son adresse IP et d'autres paramètres à l'aide de l'interface de ligne de commande Défense contre les menaces. Par exemple, vous pouvez séparer le trafic de gestion des événements (comme les événements Web). Consultez la section « Interfaces de gestion » dans le chapitre *Configuration système* du guide de configuration Centre de gestion. Les interfaces pour événements

Firepower peuvent être partagées par un ou plusieurs périphériques logiques pour accéder à des hôtes externes; les périphériques logiques ne peuvent pas communiquer sur cette interface avec d'autres périphériques logiques qui partagent l'interface.

Utilisez les interfaces `mgmt` pour gérer les instances d'application. Elles peuvent être partagées par un ou plusieurs périphériques logiques pour accéder à des hôtes externes; les périphériques logiques ne peuvent pas communiquer sur cette interface avec d'autres périphériques logiques qui partagent l'interface. Vous ne pouvez affecter qu'une seule interface de gestion par périphérique logique.

La vitesse d'interface que vous définissez peut avoir une incidence sur le mode duplex utilisé pour une interface. Vous devez donc définir la vitesse avant de définir le mode duplex. Si vous définissez une vitesse de 10 ou 100 Mbit/s, le port est automatiquement configuré pour utiliser le mode semi-duplex, mais vous pouvez spécifier le mode duplex intégral à la place. Si vous définissez une vitesse de 1 000 Mbit/s (1 Gbit/s) ou plus, le mode duplex intégral est automatiquement utilisé.

Si vous avez modifié la politique de contrôle de flux par défaut, elle est déjà appliquée aux interfaces. Si vous avez créé une politique, vous pouvez l'appliquer à l'interface.

Exemple

Cet exemple montre comment définir la vitesse de l'interface sur 10 Gbit/s et le type de port sur les données :

```
firepower # scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # enter interface Ethernet1/8
firepower /eth-uplink/fabric/interface # enable
firepower /eth-uplink/fabric/interface* # set admin-speed 10gbps
firepower /eth-uplink/fabric/interface* # set port-type data
firepower /eth-uplink/fabric/interface* # commit-buffer
firepower /eth-uplink/fabric/interface
```

Commandes associées

Commande	Description
enter interface	Permet d'accéder à une interface pour vous permettre de configurer et de gérer ses paramètres.
scope interface	Cible une interface pour vous permettre de configurer et de gérer ses paramètres.
show interface	Affiche les informations de configuration et d'état de l'interface.

set ipv6

Pour activer ou désactiver la prise en charge d'IPv6 sur l'appareil Firepower, utilisez la commande **set ipv6** en mode interconnexion de structure.

set ipv6 [**enable** | **disable**]

Description de la syntaxe

enable/disable	Active ou désactive la prise en charge d'IPv6 sur l'appareil Firepower.

Modes de commande

scope fabric-interconnect/scope ipv6-config

Historique des commandes

Version	Modification
2.13(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, IPv6 n'est pas défini. Utilisez cette commande pour activer ou désactiver IPv6.

Exemple

Cet exemple montre comment activer IPv6 sur un appareil Firepower :

```
firepower # scope fabric-interconnect
firepower /fabric-interconnect # scope ipv6-config
firepower /fabric-interconnect/ipv6-config # set ipv6 enable
firepower /fabric-interconnect/ipv6-config* # commit-buffer
```

set ipv6-auto eui64

Pour générer une adresse IPv6 basée sur la méthode eui64, utilisez la commande **set ipv6-auto eui64** en mode interconnexion de structure. Les 64 bits inférieurs proviennent de l'identifiant d'adresse matérielle, comme l'adresse MAC

set ipv6 auto eui64

Description de la syntaxe

auto eui64	Génère l'adresse IPv6 à partir des identifiants matériels.

Modes de commande

scope fabric-interconnect/scope ipv6-config

Historique des commandes

Version	Modification
2.13(1)	Commande ajoutée.

Instructions d'utilisation

Vous devez disposer d'une adresse globale valide sur l'interface de gestion pour définir ipv6-auto eui64.

Exemple

Cet exemple montre comment définir ipv6-auto eui64 :

```
firepower # scope fabric-interconnect
firepower /fabric-interconnect # scope ipv6-config
firepower /fabric-interconnect/ipv6-config # set ipv6-auto eui64
firepower /fabric-interconnect/ipv6-config* # commit-buffer
```

set ipv6-auto stablesec

Pour générer une adresse IPv6 basée sur le mécanisme de semence secrète stable, utilisez la commande **set ipv6-auto stablesec** en mode interconnexion de structure.

set ipv6 auto stablesec

Description de la syntaxe

auto stablesec	Génère l'adresse IPv6 en fonction des valeurs de semence secrète stable.

Modes de commande

scope fabric-interconnect/scope ipv6-config

Historique des commandes

Version	Modification
2.13(1)	Commande ajoutée.

Exemple

Cet exemple montre comment utiliser la commande set ipv6-auto stablesec :

```
firepower # scope fabric-interconnect
firepower /fabric-interconnect # scope ipv6-config
firepower /fabric-interconnect/ipv6-config # set ipv6-auto stablesec
Warning: Setting ipv6readycfg to stablesec will require reboot
firepower /fabric-interconnect/ipv6-config* # commit-buffer
```

set ipv6-ready

Pour définir l'adresse IPv6 basée sur la méthode eui64 ou la méthode de démarrage secret stable basée sur l'adresse IPv6 d'entrée, utilisez la commande **set ipv6-ready** en mode interconnexion de structure.

set ipv6-ready [**ipv6-addr** *address* **ipv6-readyconfig-eui64 ipv6-readyprefix** *prefix* | **ipv6-addr** *address* **ipv6-readyconfig stablesec ipv6-readyprefix** *prefix*]

Description de la syntaxe

ipv6-addr <address>	Adresse IPv6 d'entrée
ipv6-readyconfig eui64	Méthode eui64 pour générer l'adresse ipv6 basée sur l'adresse d'entrée
ipv6-readyconfig stablesec	Méthode stablesec pour générer l'adresse ipv6 basée sur l'adresse d'entrée
ipv6-readyprefix <prefix>	Préfixe IPv6

Modes de commande

scope fabric-interconnect/scope ipv6-config

Historique des commandes

Version	Modification
2.13(1)	Commande ajoutée.

Exemple

Cet exemple montre comment définir l'adresse ipv6 basée sur la méthode eui64 :

```
firepower # scope fabric-interconnect
firepower /fabric-interconnect # scope ipv6-config
firepower /fabric-interconnect/ipv6-config # set ipv6-ready ipv6-addr 2003::12
ipv6-readyconfig eui64 ipv6-readyprefix 64
firepower /fabric-interconnect/ipv6-config* # commit-buffer
```

Cet exemple montre comment définir l'adresse ipv6 basée sur la méthode stablesec :

```
firepower # scope fabric-interconnect
firepower /fabric-interconnect # scope ipv6-config
firepower /fabric-interconnect/ipv6-config # set ipv6-ready ipv6-addr
e2ca:83a7:eb48:8f6f:da04:949b:b701:1049 ipv6-readyconfig stablesec ipv6-readyprefix 64
Warning: Setting ipv6readycfg to stablesec will require reboot
firepower /fabric-interconnect/ipv6-config* # commit-buffer
```

set keyring-name

Pour affecter un trousseau de clés à une connexion IPSec, utilisez la commande **set keyring-name**.

set keyring-name *name*

Description de la syntaxe

name	Nom d'un trousseau de clés à affecter à la connexion IPSec; 16 caractères maximum.

Modes de commande

Mode connexion (/security/ipsec/connection)

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour ajouter un trousseau de clés à une connexion IPSec.

Exemple

Cet exemple montre comment ajouter un trousseau de clés à la connexion IPSec actuelle :

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # enter connection testconn
FP9300-A /security/ipsec/connection # set keyring-name kr22
FP9300-A /security/ipsec/connection* # commit-buffer
FP9300-A /security/ipsec/connection #
```

Commande	Description
create connection	Crée une connexion IPSec.
set keyring-passwd	Spécifie la phrase secrète pour un trousseau de clés affectée à une connexion IPSec.

set lastname

Pour spécifier le nom d'un utilisateur local, utilisez la commande **set lastname**.

set lastname *name*

Description de la syntaxe

name	Nom de l'utilisateur; peut comporter de 0 à 32 caractères.

Modes de commande

Mode utilisateur local

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment accéder au mode sécurité, créer un compte d'utilisateur local et spécifier le nom et le prénom de cet utilisateur :

```
FP9300-A# scope security
FP9300-A /security # create local-user test_user
FP9300-A /security/local-user* # set firstname john
FP9300-A /security/local-user* # set lastname doe
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

Commande	Description
create local-user	Crée un compte d'utilisateur local.
set firstname	Spécifie le prénom d'un compte d'utilisateur local.

set link-state-sync

Pour synchroniser l'état de la liaison opérationnelle avec l'état de la liaison physique pour les interfaces de données à l'aide d'un état de service, utilisez la commande **set link-state-sync** .

set link-state-sync

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope ssa

Historique des commandes

Version	Modification
2.9(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour synchroniser l'état de la liaison opérationnelle Cisco FTD avec l'état de la liaison physique pour les interfaces de données.

Exemple

Cet exemple montre comment accéder au mode scope ssa, puis set link-state-sync.

```
firepower# scope ssa
firepower /ssa # scope logical-device <logical device identifier>
firepower /ssa/logical-device # set link-state-sync ?
  disabled  Disabled
  enabled   Enabled
```

set local-address

Pour spécifier l'adresse IP locale d'une connexion IPSec, utilisez la commande **set local-address**.

set local-address *ip_address*

Description de la syntaxe

ip_address	Fournissez une adresse de passerelle locale IPv4 ou IPv6 d'une connexion IPSec; 510 caractères maximum.

Modes de commande

Mode connexion

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande et la commande **set remote-address** pour définir les terminaux d'une connexion IPSec.

Exemple

Cet exemple montre comment définir l'adresse locale d'une connexion IPSec :

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # enter connection testconn
FP9300-A /security/ipsec/connection # set local-address 209.165.201.12
FP9300-A /security/ipsec/connection* # commit-buffer
FP9300-A /security/ipsec/connection #
```

Commande	Description
create connection	Crée une connexion IPSec.
set remote-addr	Définit l'adresse IP distante d'une connexion IPSec.

set log-level

Pour spécifier le niveau de journalisation IPSec, utilisez la commande **set log-level**.

set log-level *log_level*

Description de la syntaxe

log_level	Saisissez une valeur comprise entre 0 et 4 pour spécifier la verbosité des journaux IPSec; la valeur par défaut est 1. **0** : informations d'audit de base; par exemple, SA activé/désactivé. **1** : informations générales sur le flux de contrôle, avec erreurs. **2** : informations plus détaillées sur le flux de contrôle; comprend des informations de débogage. **3** : comprend les vidages de données brutes (hexadécimal). **4** : comprend des informations sensibles dans les vidages de données; par exemple, des clés SA.

Modes de commande

Mode IPSec

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez la commande **show ipsec-log** pour afficher les journaux.

Exemple

Cet exemple montre comment définir le niveau de journalisation IPSec sur 2 :

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # set log-level 2
FP9300-A /security/ipsec* # commit-buffer
FP9300-A /security/ipsec #
```

Commandes associées

Commande	Description
show ipsec-log	Affiche le fichier journal IPSec.

set max-login-attempts

Pour spécifier le nombre maximal de tentatives de connexion infructueuses, utilisez la commande **set max-login-attempts**.

set max-login-attempts *max_attempts*

Description de la syntaxe

max_attempts	Nombre maximal de tentatives de connexion infructueuses avant qu'un utilisateur ne soit bloqué du système. La valeur peut être comprise entre 0 et 10; la valeur par défaut est 0.

Modes de commande

Mode sécurité

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Si un utilisateur (utilisateur administrateur compris) dépasse ce nombre maximal de tentatives de connexion, il est bloqué du système et doit attendre le temps spécifié avant de pouvoir se reconnecter. Aucune notification ne s'affiche pour indiquer que l'utilisateur est verrouillé.

Exemple

Cet exemple montre comment accéder au mode sécurité et spécifier un nombre maximal de tentatives de connexion :

```
FP9300-A# scope security
FP9300-A /security # set max-login-attempts 4
FP9300-A /security* # commit-buffer
FP9300-A /security #
```

Commandes associées

Commande	Description
clear lock-status	Déverrouille le blocage d'un utilisateur.
set user-account-unlock-time	Spécifie la durée pendant laquelle l'utilisateur reste bloqué du système après avoir atteint le nombre maximal de tentatives de connexion.

set message

Pour ajouter ou remplacer les lignes de texte présentées comme bannière de préconnexion, utilisez la commande **set message**.

set message

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope security/scope banner/scope pre-login-banner/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Après avoir saisi la commande, vous êtes invité à saisir les lignes de texte de la bannière. Vous devez saisir `ENDOFBUF` (en majuscules) pour terminer le texte de la bannière.

Remarque L'objet de bannière de préconnexion doit déjà exister; voir create pre-login-banner, à la page 95.

Exemple

Cet exemple vous montre comment créer et spécifier une bannière de préconnexion, puis la valider et l'afficher :

```
firepower # scope security
firepower /security # scope banner
firepower /security/banner # create pre-login-banner
firepower /security/banner/pre-login-banner* # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Firepower-9300-2
>Western Data Center
>ENDOFBUF
firepower /security/banner/pre-login-banner* # commit
firepower /security/banner/pre-login-banner # show

Pre login banner:
    Message
    -------
    Firepower-9300-2
Western Data Center

firepower /security/banner/pre-login-banner #
```

Commandes associées

Commande	Description
clear message	Supprime le texte d'une bannière de préconnexion existante; l'objet de bannière en lui-même n'est pas supprimé.
create pre-login-banner	Crée une bannière à présenter avant l'écran de connexion; l'objet de bannière est initialement vide.

set min-password-length

Pour spécifier la longueur minimale des mots de passe des utilisateurs, utilisez la commande **set min-password-length**.

set min-password-length *num_chars*

Description de la syntaxe

num_chars	Nombre minimum de caractères requis pour les mots de passe des utilisateurs; la valeur peut être comprise entre 8 et 80.

Modes de commande

Mode sécurité

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Si cette option est activée, les utilisateurs doivent créer des mots de passe avec le nombre minimum de caractères spécifié ou plus. Par exemple, si *num_chars* est défini sur 15, les mots de passe doivent comporter au moins 15 caractères.

Exemple

Cet exemple montre comment accéder au mode sécurité et spécifier une longueur de mot de passe minimum de 15 caractères :

```
FP9300-A# scope security
FP9300-A /security # set min-password-length 15
FP9300-A /security* # commit-buffer
FP9300-A /security #
```

Commandes associées

Commande	Description
set enforce-strong-password	Active et désactive l'application de mots de passe forts.

set mode

Pour spécifier le mode connexion IPSec, utilisez la commande **set mode**.

set mode {**transport** | **tunnel**}

Description de la syntaxe

transport	Définit le mode connexion sur **transport**.
tunnel	Définit le mode connexion sur **tunnel**.

Modes de commande

Mode connexion

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

En mode transport, seule la charge utile d'un paquet IP est chiffrée; en mode tunnel, le paquet est entièrement chiffré. Le mode transport est généralement utilisé pour les sessions de bout en bout, et le mode tunnel pour tous les autres types de connexions (entre passerelles, par exemple).

Exemple

Cet exemple montre comment définir le mode connexion IPSec sur tunnel :

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # enter connection testconn
FP9300-A /security/ipsec/connection # set mode tunnel
FP9300-A /security/ipsec/connection* # commit-buffer
FP9300-A /security/ipsec/connection #
```

Commande	Description
create connection	Crée une connexion IPSec.
set local-addr	Définit l'adresse IP locale d'une connexion IPSec.
set remote-addr	Définit l'adresse IP distante d'une connexion IPSec.

set modulus

Pour spécifier le module de clé RSA (longueur de clé SSL) en bits, utilisez la commande **set modulus**.

set modulus {**mod1536** | **mod2048** | **mod2560** | **mod3072** | **mod3584** | **mod4096**}

Description de la syntaxe

Module de clé RSA (longueur de clé SSL) en bits	Les options valides sont les suivantes : • **mod1536** : le module est de 1 536 bits • **mod2048** : le module est de 2 048 bits • **mod2560** : le module est de 2 560 bits • **mod3072** : le module est de 3 072 bits • **mod3584** : le module est de 3 584 bits • **mod4096** : le module est de 4 096 bits

Modes de commande

Mode trousseau de clés

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour spécifier la longueur de clé pour un trousseau de clés.

Exemple

Cet exemple montre comment spécifier une longueur de clé de 2 048 bits pour un trousseau de clés :

```
FP9300-A# scope security
FP9300-A /security # scope keyring test-ring
FP9300-A /security/keyring # set modulus 2048
FP9300-A /security/keyring* # commit-buffer
switch-A /security/keyring #
```

Commandes associées

Commande	Description
set cert	Permet d'accéder à un certificat RSA pour un trousseau de clés.
set regenerate	Renouvelle les clés RSA du trousseau de clés par défaut.
set trustpoint	Spécifie si le certificat de trousseau de clés peut être renouvelé.

set nd

Pour activer ou désactiver la prise en charge de ND IPv6 sur l'appareil Firepower, utilisez la commande **set nd** en mode interconnexion de structure.

set nd [**enable** | **disable**]

Description de la syntaxe

enable	Permet d'exécuter rdnssd (démon de découverte du serveur dns récursif ipv6), une fois qu'il est activé.
disable	Désactive le démon rdnsd sur l'appareil Firepower.

Modes de commande

scope fabric-interconnect/scope ipv6-config

Historique des commandes

Version	Modification
2.13(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, ND n'est pas défini. Utilisez cette commande pour activer ou désactiver IPv6.

Exemple

Cet exemple montre comment activer ND sur un appareil Firepower :

```
firepower # scope fabric-interconnect
firepower /fabric-interconnect # scope ipv6-config
firepower /fabric-interconnect/ipv6-config # set nd enable
firepower /fabric-interconnect/ipv6-config* # commit-buffer
```

set out-of-band

Pour modifier l'adresse IP de gestion de l'appareil, utilisez la commande **set out-of-band**.

Pour une adresse IPv4 :

set out-of-band {**gw** *gateway_address* | **ip** *ip_address* | **netmask** *network_mask*}

Pour une adresse IPv6 :

set out-of-band {**ipv6** *ipv6_address* | **ipv6-gw** *ipv6_gateway* | **ipv6-prefix** *ipv6_prefix*}

Description de la syntaxe

gw *gateway_address*	Indiquer une adresse de passerelle IPv4.
ip *ip_address*	Indiquer une adresse IPv4 pour l'accès à la gestion des appareils.
netmask *network_mask*	Indiquer un masque réseau pour l'adresse IPv4.
ipv6 *ipv6_address*	Indiquer une adresse IPv6 pour l'accès à la gestion des appareils.
ipv6-gw *ipv6_gateway*	Indiquer une adresse de passerelle IPv6.
prefix *ipv6_prefix*	Indiquer une longueur de préfixe pour l'adresse IPv6. **Remarque** Seules les adresses IPv6 Global Unicast sont prises en charge comme adresse de gestion IPv6 du châssis.

Modes de commande

Adresse IPv4 : mode interconnexion structure

Adresse IPv6 : mode configuration IPv6 (fabric-interconnect/ipv6-config)

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Après avoir modifié l'adresse IP de gestion, vous devez rétablir toutes les connexions existante en utilisant la nouvelle adresse.

Vous pouvez saisir les trois mots clés et variables, quel que soit le type d'adresse IP, dans n'importe quel ordre sur une seule ligne de commande. Consultez les exemples suivants.

Remarque Seules les adresses IPv6 Global Unicast sont prises en charge comme adresse de gestion IPv6 du châssis.

Exemples

Cet exemple montre comment afficher l'interface de gestion IPv4 actuelle et les adresses de passerelle, puis spécifier de nouvelles adresses :

```
FP9300-A # scope fabric-interconnect a
FP9300-A /fabric-interconnect # show
```

```
Fabric Interconnect:
ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
Prefix Operability
---- --------------- --------------- --------------- ---------------- ----------------
------ -----------
A    192.0.2.112     192.0.2.1       255.255.255.0   ::               ::               64
    Operable
FP9300-A /fabric-interconnect # set out-of-band ip 192.0.2.111 netmask 255.255.255.0 gw
192.0.2.1
Warning: When committed, this change may disconnect the current CLI session
FP9300-A /fabric-interconnect* # commit-buffer
FP9300-A /fabric-interconnect #
```

Cet exemple montre comment afficher l'interface de gestion IPv6 actuelle et les adresses de passerelle, puis spécifier de nouvelles adresses :

```
FP9300-A # scope fabric-interconnect a
FP9300-A /fabric-interconnect # scope ipv6-config
FP9300-A /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
IPv6 Address                          Prefix     IPv6 Gateway
------------------------------------ ---------- ------------
2001::8998                            64         2001::1
FP9300-A /fabric-interconnect/ipv6-config # set out-of-band ipv6 2001::8999 ipv6-prefix 64
 ipv6-gw 2001::1
FP9300-A /fabric-interconnect/ipv6-config* # commit-buffer
FP9300-A /fabric-interconnect/ipv6-config #
```

Commande	Description
show	Affiche les adresses IP de gestion des appareils actuelles.
show ipv6-if	Affiche l'adresse IPv6 actuelle de gestion des appareils.

set password

Pour spécifier le mot de passe d'un compte d'utilisateur, utilisez la commande **set password**.

set password

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

`scope security/` : pour modifier le mot de passe de l'utilisateur actuellement connecté

`scope security/scope local-user/` : pour spécifier un mot de passe pour l'utilisateur local actuel

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Après avoir saisi la commande **set password**, vous êtes invité à saisir et à confirmer le mot de passe. Pour des raisons de sécurité, le mot de passe que vous saisissez n'apparaît pas dans la fenêtre de l'interface de ligne de commande.

Ce mot de passe doit contenir entre 8 et 80 caractères. Utilisez set min-password-length, à la page 319 pour définir un nombre minimum de caractères. Utilisez set enforce-strong-password, à la page 288 pour exiger l'utilisation de mots de passe « forts ».

Exemple

Cet exemple montre comment accéder au mode sécurité, créer un compte d'utilisateur local et spécifier un mot de passe pour cet utilisateur :

```
firepower# scope security
firepower /security # create local-user test_user
firepower /security/local-user* # set password
Enter a password:
Confirm the password:
firepower /security/local-user* # commit-buffer
firepower /security/local-user #
```

Commande	Description
create local-user	Crée un compte d'utilisateur local.
set expiration	Spécifie la date d'expiration du compte d'utilisateur.

set password-encryption-key

Pour indiquer une clé à utiliser lors du chiffrement d'informations sensibles durant l'exportation de la configuration, utilisez la commande **set password-encryption-key** .

set password-encryption-key

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé. Après avoir saisi la commande, vous êtes invité à saisir et à confirmer une clé de chiffrement.

La clé peut comporter entre quatre et quarante caractères. La clé que vous saisissez est ensuite utilisée pour générer une valeur de hachage MD5 de 128 bits.

Modes de commande

scope security/

Historique des commandes

Version	Modification
2.6.1	Commande ajoutée.

Instructions d'utilisation

Utilisez la fonctionnalité d'exportation de configuration pour exporter un fichier XML contenant les paramètres de configuration des périphériques logiques et de la plateforme pour votre châssis Firepower 4100/9300. Vous pouvez importer ce fichier de configuration ultérieurement pour appliquer rapidement les paramètres de configuration à votre châssis Firepower 4100/9300 afin de retrouver une configuration stable ou de récupérer suite à une défaillance système.

À partir de FXOS 2.6.1, vous devez indiquer une clé à utiliser lors du chiffrement d'informations sensibles telles que les mots de passe et autres clés secrètes durant l'exportation de la configuration, et vous devez l'avoir indiquée avant de tenter d'exporter la configuration.

De plus, la même clé utilisée lors de l'exportation doit être définie sur le système cible lorsque vous importez une configuration exportée, sauf si le fichier a été exporté à partir d'une version FXOS antérieure à la version 2.6.1, auquel cas le système cible autorise l'importation.

Après avoir été définie, une clé de chiffrement de mot de passe ne peut pas être modifiée ou supprimée, sauf si vous effectuez une réinitialisation d'usine ou une récupération du mot de passe. La réinitialisation d'usine ou la récupération du mot de passe efface la clé comme si elle n'avait jamais été définie.

Exemple

Cet exemple montre comment indiquer une clé de chiffrement de mot de passe avant d'exporter la configuration actuelle :

```
firepower # scope security
firepower /security # set password-encryption-key
Enter a key:
Confirm the key:
Warning: Please make note of the encryption key configured. If you change the key, importing
 configurations that were exported with the previous key will fail, because Import and
Export requires the same encryption key on the system.
firepower /security* # commit-buffer
firepower /security #
```

Commandes associées

Commande	Description
cfg-export-policy	Configure une politique d'exportation.
export-config	Exporte la configuration système actuelle vers un serveur distant en tant que fichier XML.
import-config	Copie un fichier de configuration XML précédemment exporté vers cet appareil.

set (password-profile)

Pour spécifier ou modifier les paramètres de profil de mot de passe de l'utilisateur local, utilisez la commande **set** en mode profil de mot de passe.

set { **change-count** | **change-during-interval** | **change-interval** | **history-count** | **no-change-interval** }

Description de la syntaxe

change-count *count*	Nombre maximum de fois où un utilisateur peut modifier son mot de passe (au cours de la période spécifiée par **set change-interval**); la valeur peut être comprise entre 0 et 10.
change-during-interval { **disable** | **enable** }	Activer ou désactiver les restrictions sur le nombre de modifications de mot de passe qu'un utilisateur authentifié localement peut effectuer : • `disable` : désactive les restrictions sur le nombre de modifications de mot de passe. • `enable` : active les restrictions sur le nombre de modifications de mot de passe. Cette option doit être activée pour vous permettre de spécifier le nombre maximum de fois qu'un utilisateur authentifié localement peut modifier son mot de passe et le nombre d'heures pendant lesquelles ce nombre de modifications de mot de passe peut être effectué.
change-interval *interval*	Intervalle sur lequel les modifications de mot de passe d'un utilisateur sont comptées pour s'assurer qu'elles ne dépassent pas le nombre maximum spécifié à l'aide de la commande **set change-count**; le nombre d'heures peut être compris entre 1 et 745. L'option **set change-during-interval** doit être activée pour vous permettre de spécifier cet intervalle.
history-count *count*	Nombre de mots de passe uniques qu'un utilisateur authentifié localement doit créer avant de pouvoir réutiliser un mot de passe précédemment utilisé; la valeur peut être comprise entre 0 et 15. Par défaut, la valeur *count* est zéro, ce qui désactive l'historique des mots de passe. Les utilisateurs peuvent alors réutiliser des mots de passe déjà employés à tout moment.
no-change-interval *hours*	Durée en heures pendant laquelle un utilisateur ne peut plus modifier son mot de passe; la valeur peut être comprise entre 1 et 745. L'option **set change-during-interval** doit être désactivée avant de définir cette période, sinon cette valeur est ignorée.

Modes de commande

scope security/scope password-profile/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

L'option **set change-during-interval** doit être activée pour vous permettre de spécifier le nombre maximum de fois qu'un utilisateur authentifié localement peut modifier son mot de passe et le nombre d'heures pendant lesquelles ce nombre de modifications de mot de passe peut être effectué.

Par défaut, la valeur **set history-count** est zéro, ce qui désactive l'historique des mots de passe. Les utilisateurs peuvent alors réutiliser des mots de passe déjà employés à tout moment.

Exemples

Cet exemple montre comment accéder au mode profil de mot de passe, activer les restrictions de modification de mot de passe, spécifier qu'un utilisateur ne peut modifier son mot de passe que deux fois par période de 48 heures, puis afficher les paramètres actuels :

```
firepower # scope security
firepower /security # scope password-profile
firepower /security/password-profile # set change-during-interval enable
firepower /security/password-profile* # set change-count 2
firepower /security/password-profile* # set change-interval 48
firepower /security/password-profile* # commit-buffer
firepower /security/password-profile # show detail

Password profile:
    Password history count: 5
    No password changes allowed (in Hours): 24
    Password change during interval: Enable
    Password change interval (in Hours): 48
    Password change count: 2
firepower /security/password-profile #
```

Commandes associées

Commande	Description
show detail	Affiche les paramètres de profil de mot de passe actuels.

set phone

Pour définir un numéro de téléphone pour un compte d'utilisateur, utilisez la commande **set phone**.

set phone *tel_number*

Description de la syntaxe

tel_number	Numéro de téléphone du compte d'utilisateur; 20 caractères maximum.

Modes de commande

Mode utilisateur local

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment spécifier un numéro de téléphone pour l'utilisateur local actuel :

```
FP9300-A /security/local-user # set phone +1-408-555-1212
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

Commandes associées

Commande	Description
create local-user	Crée un compte d'utilisateur local.
set phone-contact	Spécifie un numéro de téléphone pour un compte Smart Call Home.

set (port-channel)

Pour spécifier ou modifier les paramètres d'un canal de port existant, utilisez la commande **set** en mode canal de port.

set { **auto-negotiation** | **descr** | **duplex** | **flow-control-policy** | **lacp-policy-name** | **nw-ctrl-policy** | **port-channel-mode** | **port-type** | **speed** }

Description de la syntaxe

auto-negotiation { **no** | **yes** }	Active ou désactive la négociation automatique des paramètres de transmission communs tels que la vitesse, les conditions de duplex et le contrôle de flux. • **no** : désactive la négociation automatique. • **yes** : active la négociation automatique.
descr *description*	Vous pouvez ajouter une description au canal de port; la description peut comporter entre zéro et 256 caractères. La plupart des caractères alphanumériques sont autorisés, de même que les tirets et les traits de soulignement. Les espaces ne sont pas autorisés. La chaîne peut se terminer par des signes de ponctuation comme un point-virgule, un point et un point d'exclamation, mais vous ne pouvez pas intégrer ces caractères dans la description.
duplex { **fullduplex** | **halfduplex** }	Définit le mode duplex pour le canal de port : • **fullduplex** : spécifie les communications bidirectionnelles simultanées. • **halfduplex** : spécifie les communications unidirectionnelles alternées.
flow-control-policy *name*	Vous pouvez attribuer une politique de contrôle de flux au canal de port; indiquez le nom de la politique, qui peut comporter jusqu'à 16 caractères alphanumériques.
lacp-policy-name *name*	Vous pouvez attribuer une politique LACP au canal de port; indiquez le nom de la politique, qui peut comporter jusqu'à 16 caractères alphanumériques.
nw-ctrl-policy *name*	Vous pouvez attribuer une politique de contrôle de réseau au canal de port; indiquez le nom de la politique, qui peut comporter jusqu'à 16 caractères alphanumériques.

port-channel-mode {**active** | **on**}	Définissez le mode pour les interfaces de données physiques ou de partage de données du canal de port : • **active** : envoie et reçoit les mises à jour du protocole LACP. Un canal de port actif peut établir une connectivité avec un canal de port actif ou passif. Vous devez utiliser le mode actif, sauf si vous devez réduire au minimum le trafic LACP. Il s'agit du paramètre par défaut. • **on** : le canal de port est toujours activé et le protocole LACP n'est pas utilisé. Un canal de port actif peut uniquement établir une connexion avec un autre canal de port actif. Les interfaces sans données ne prennent en charge que le mode actif.
port-type {**cluster** | **data** | **data-sharing** | **firepower-eventing** | **mgmt**}	Spécifiez le type ou la fonction de canal de port : • **cluster** : spécifier **cluster** uniquement si vous souhaitez utiliser ce canal de port comme liaison de commande de grappe. • **data** : permet la transmission régulière de données. Il s'agit du type par défaut. • **data-sharing** : à utiliser pour les données régulières; uniquement pris en charge avec les instances de contenant. • **firepower-eventing** : utilisez ce canal de port comme interface de gestion secondaire pour les appareils Défense contre les menaces. Le canal de port firepower-eventing est utilisé pour acheminer tout le trafic des événements (comme les événements Web). • **mgmt** : permet de gérer les instances d'application. Vous ne pouvez affecter qu'une seule interface de gestion par périphérique logique. Consultez set port-type, à la page 337 pour plus d'informations sur cette commande.
speed {**100gbps** | **100mbps** | **10gbps** | **10mbps** | **1gbps** | **40gbps**}	Spécifiez la vitesse de transfert des données du port : • **100gbps** : cent gigabits par seconde. • **100mbps** : cent mégabits par seconde. • **10gbps** : dix gigabits par seconde. • **10mbps** : dix mégabits par seconde. • **1gbps** : un gigabit par seconde. • **40gbps** : quarante gigabits par seconde.

Modes de commande

scope eth-uplink/scope fabric a/port-channel/

Historique des commandes

Version	Modification
2.4(1)	Nous avons ajouté le type **data-sharing**.

Version	Modification
1.1(4)	Nous avons ajouté le type **firepower-eventing**.
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Affectez des interfaces membres au canal de port avant d'utiliser cette commande pour définir les paramètres.

Le mode canal de port LACP s'applique aux données et aux interfaces de partage de données. Pour les interfaces sans données et sans partage de données, le mode est toujours `actif`.

Le type `cluster` est un type d'interface spécial utilisé pour un périphérique logique en grappe. Ce type est automatiquement attribué au lien de commande de grappe pour les communications inter-unités de grappe. Par défaut, la liaison de commande de grappe est automatiquement créée sur le canal de port 48.

Les interfaces de données ne peuvent pas être partagées entre les périphériques logiques.

Le type `data-sharing` est uniquement pris en charge avec les instances de conteneur. Ces interfaces de données peuvent être partagées par un ou plusieurs périphériques logiques/instances de conteneur (Défense contre les menaces uniquement). Chaque instance de contenant peut communiquer sur le fond de panier avec toutes les autres instances qui partagent cette interface. Les interfaces partagées peuvent avoir une incidence sur le nombre d'instances de conteneur que vous pouvez déployer. Les interfaces partagées ne sont pas prises en charge pour les interfaces de membre de groupe de ponts (en mode transparent ou en mode routage), les ensembles en ligne, les interfaces passives ou les liaisons de basculement.

Une interface `firepower-eventing` est une interface de gestion secondaire pour les appareils Défense contre les menaces. Pour utiliser cette interface, vous devez configurer son adresse IP et d'autres paramètres à l'aide de l'interface de ligne de commande Défense contre les menaces. Par exemple, vous pouvez séparer le trafic de gestion des événements (comme les événements Web). Consultez la section « Interfaces de gestion » dans le chapitre *Configuration système* du guide de configuration Centre de gestion. Les interfaces pour événements Firepower peuvent être partagées par un ou plusieurs périphériques logiques pour accéder à des hôtes externes; les périphériques logiques ne peuvent pas communiquer sur cette interface avec d'autres périphériques logiques qui partagent l'interface.

Utilisez les interfaces `mgmt` pour gérer les instances d'application. Elles peuvent être partagées par un ou plusieurs périphériques logiques pour accéder à des hôtes externes; les périphériques logiques ne peuvent pas communiquer sur cette interface avec d'autres périphériques logiques qui partagent l'interface. Vous ne pouvez affecter qu'une seule interface de gestion par périphérique logique.

La vitesse d'interface que vous définissez peut avoir une incidence sur le mode duplex utilisé pour une interface. Vous devez donc définir la vitesse avant de définir le mode duplex. Si vous définissez une vitesse de 10 ou 100 Mbit/s, le port est automatiquement configuré pour utiliser le mode semi-duplex, mais vous pouvez spécifier le mode duplex intégral. Si vous définissez une vitesse de 1 000 Mbit/s (1 Gbit/s) ou plus, le mode duplex intégral est automatiquement utilisé.

Si vous avez modifié la politique de contrôle de flux par défaut, elle est déjà appliquée aux interfaces. Si vous avez créé une politique, vous pouvez l'appliquer au canal de port.

Exemple

L'exemple suivant crée le canal de port 1 avec quatre interfaces membres, définit le type de données, ainsi que le mode EtherChannel sur le mode Activé.

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # create port-channel 1
```

```
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # set port-type data
firepower /eth-uplink/fabric/port-channel* # set port-channel-mode on
firepower /eth-uplink/fabric/port-channel* # commit-buffer
firepower /eth-uplink/fabric/port-channel #
```

Commandes associées

Commande	Description
create port-channel	Ajoute une interface EtherChannel.
scope interface	Permet d'accéder à une interface physique pour vous permettre de configurer et de gérer les paramètres d'interface.

set port-channel-mode

Pour définir le mode canal de port pour un EtherChannel, utilisez la commande **set port-channel-mode**.

set port-channel-mode {**active** | **on**}

Description de la syntaxe

active	Active l'interface dans un EtherChannel.
on	Active l'interface dans un EtherChannel. Uniquement pris en charge par les interfaces de données ou de partage de données.

Commande par défaut Le mode par défaut est le mode Actif.

Modes de commande scope eth-uplink/scope fabric a/create port-channel/

Historique des commandes

Version	Modification
2.4(1)	Commande ajoutée.

Instructions d'utilisation

Vous pouvez configurer chaque interface physique de données ou de partage de données dans un EtherChannel pour qu'elle soit :

- Actif : envoie et reçoit les mises à jour du protocole LACP. Un EtherChannel actif peut établir une connectivité avec un EtherChannel actif ou passif. Vous devez utiliser le mode actif, sauf si vous devez réduire au minimum le trafic LACP.
- Activé : l'EtherChannel est toujours activé et le protocole LACP n'est pas utilisé. Un EtherChannel « activé » ne peut établir une connexion qu'avec un autre EtherChannel « activé ».

Les interfaces sans données ne prennent en charge que le mode actif.

Exemple

L'exemple suivant ajoute le canal de port 1 avec 4 interfaces membres, définit le type de données et active le mode EtherChannel.

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # create port-channel 1
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # set port-type data
firepower /eth-uplink/fabric/port-channel* # set port-channel-mode on
```

Commandes associées

Commande	Description
create port-channel	Ajoute une interface EtherChannel.
create member-port	Affecte un membre à l'EtherChannel.
set port-type	Définit le type d'interface.

set port-type

Pour définir le type de port d'une interface, utilisez la commande **set port-type**.

set port-type { **cluster** | **data** | **data-sharing** | **firepower-eventing** | **mgmt** }

Description de la syntaxe

cluster	Type d'interface spéciale utilisé pour un périphérique logique en grappe. Ce type est automatiquement attribué au lien de contrôle de grappe pour les communications inter-unités de grappe. Par défaut, la liaison de commande de grappe est automatiquement créée sur le canal de port 48. Pour la mise en grappe multi-instances, vous ne pouvez pas partager une interface de type grappe sur plusieurs appareils. Vous pouvez ajouter des sous-interfaces VLAN à la grappe EtherChannel pour fournir des liaisons de commande de grappe distinctes par grappe. Si vous ajoutez des sous-interfaces à une interface Cluster, vous ne pouvez pas utiliser cette interface pour une grappe native. gestionnaire d'appareil ne prend pas en charge la mise en grappe.
data	Les interfaces de données ne peuvent pas être partagées entre les périphériques logiques.
data-sharing	Uniquement prises en charge avec les instances de contenant, ces interfaces de données peuvent être partagées par un ou plusieurs périphériques logiques/instances de contenant (Défense contre les menaces uniquement). Chaque instance de contenant peut communiquer sur le fond de panier avec toutes les autres instances qui partagent cette interface. Les interfaces partagées peuvent avoir une incidence sur le nombre d'instances de conteneur que vous pouvez déployer. Les interfaces partagées ne sont pas prises en charge pour les interfaces de membre de groupe de ponts (en mode transparent ou en mode routage), les ensembles en ligne, les interfaces passives, les grappes ou les liaisons de basculement.
firepower-eventing	Cette interface est une interface de gestion secondaire pour les périphériques Défense contre les menaces. Pour utiliser cette interface, vous devez configurer son adresse IP et d'autres paramètres à l'aide de l'interface de ligne de commande Défense contre les menaces. Par exemple, vous pouvez séparer le trafic de gestion des événements (comme les événements Web). Consultez la section « Interfaces de gestion » dans le chapitre *Configuration système* du guide de configuration Centre de gestion. Les interfaces pour événements Firepower peuvent être partagées par un ou plusieurs périphériques logiques pour accéder à des hôtes externes; les périphériques logiques ne peuvent pas communiquer sur cette interface avec d'autres périphériques logiques qui partagent l'interface.
mgmt	Utilisez les interfaces de gestion pour gérer les instances d'application. Elles peuvent être partagées par un ou plusieurs périphériques logiques pour accéder à des hôtes externes; les périphériques logiques ne peuvent pas communiquer sur cette interface avec d'autres périphériques logiques qui partagent l'interface. Vous ne pouvez affecter qu'une seule interface de gestion par périphérique logique.

Commande par défaut Le type par défaut est Données.

Modes de commande

scope eth-uplink/scope fabric a/scope interface/

scope eth-uplink/scope fabric a/scope interface/create subinterface/

scope eth-uplink/scope fabric a/create port-channel/

scope eth-uplink/scope fabric a/create port-channel/create subinterface/

Historique des commandes

Version	Modification
2.8(1)	Vous pouvez définir le type **cluster** sur une sous-interface VLAN à des fins d'utilisation avec la mise en grappe multi-instances.
2.4(1)	Nous avons ajouté le type **data-sharing**.
1.1(4)	Nous avons ajouté le type **firepower-eventing**.
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Les instances de contenant peuvent partager des interfaces de type partage de données. Cette fonctionnalité vous permet d'économiser l'utilisation de l'interface physique et de prendre en charge des déploiements réseau flexibles. Lorsque vous partagez une interface, le châssis utilise des adresses MAC uniques pour transférer le trafic vers la bonne instance. Cependant, les interfaces partagées peuvent faire grossir la table de transfert en raison de la nécessité d'une topologie de maillage complet dans le châssis (chaque instance doit pouvoir communiquer avec toutes les autres instances qui partagent la même interface). Par conséquent, il y a des limites au nombre d'interfaces que vous pouvez partager.

En plus du tableau de transfert, le châssis gère un tableau de groupes VLAN pour le transfert de la sous-interface VLAN. Selon le nombre d'interfaces parentes et d'autres décisions de déploiement, vous pouvez créer jusqu'à 500 sous-interfaces VLAN.

Consultez les limites suivantes pour l'attribution d'interface partagée :

- Maximum de 14 instances par interface partagée. Par exemple, vous pouvez allouer Ethernet1/1 aux Instance1 à Instance14.
- Maximum de 10 interfaces partagées par instance. Par exemple, vous pouvez allouer Ethernet1/1.1 à Ethernet1/1.10 à l'Instance 1.

Consultez le tableau suivant pour de l'information sur la prise en charge des types d'interface pour les applications FTD et ASA dans les déploiements autonomes et en grappe.

Tableau 4 : Prise en charge des types d'interface

Application		Données	Données : sous-interface	Partage de données	Partage de données : sous-interface	Gestion	Événements Firepower	Grappe (EtherChannel uniquement)	Grappe : sous-interface
FTD	Instance native autonome	**Oui**	—	—	—	**Oui**	**Oui**	—	—
	Instance de conteneur autonome	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	—	—
	Instance native de grappe	**Oui** (EtherChannel uniquement pour la grappe inter-châssis)	—	—	—	**Oui**	**Oui**	**Oui**	—
	Instance de conteneur de grappe	**Oui** (EtherChannel uniquement pour la grappe inter-châssis)	—	—	—	**Oui**	**Oui**	**Oui**	**Oui**
ASA	Instance native autonome	**Oui**	—	—	—	**Oui**	—	**Oui**	—
	Instance native de grappe	**Oui** (EtherChannel uniquement pour la grappe inter-châssis)	—	—	—	**Oui**	—	**Oui**	—

Exemples

L'exemple suivant ajoute le canal de port 1 avec 4 interfaces membres, définit le type de données et active le mode EtherChannel.

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # create port-channel 1
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
firepower /eth-uplink/fabric/port-channel/member-port* # exit
```

```
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # set port-type data
firepower /eth-uplink/fabric/port-channel* # set port-channel-mode on
```

L'exemple suivant ajoute trois sous-interfaces et définit le type de port sur le partage de données.

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # enter interface Ethernet1/1
firepower /eth-uplink/fabric/interface # enter subinterface 10
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 10
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # exit
firepower /eth-uplink/fabric/interface # enter subinterface 11
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 11
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # exit
firepower /eth-uplink/fabric/interface # enter subinterface 12
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 12
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # commit-buffer
firepower /eth-uplink/fabric/interface/subinterface #
```

Commandes associées

Commande	Description
create port-channel	Ajoute une interface EtherChannel.
scope interface	Permet d'accéder à une interface physique pour vous permettre de configurer et de gérer les paramètres d'interface.

set port-type (aggr-interface)

Pour configurer le type de port de l'interface, utilisez la commande **set port-type**.

set port-type { *data* | *data-sharing* | *mgmt* | *firepower-eventing* | *cluster* }

Description de la syntaxe

data	(Facultatif) Les interfaces de données ne peuvent pas être partagées entre les périphériques logiques.
data-sharing	(Facultatif) Pris en charge uniquement avec les instances de contenant, ces interfaces de données peuvent être partagées par un ou plusieurs périphériques logiques/instances de contenant (Cisco FTD uniquement). Chaque instance de contenant peut communiquer sur le fond de panier avec toutes les autres instances qui partagent cette interface. Les interfaces partagées peuvent avoir une incidence sur le nombre d'instances de conteneur que vous pouvez déployer. Les interfaces partagées ne sont pas prises en charge pour les interfaces de membre de groupe de ponts (en mode transparent ou en mode routage), les ensembles en ligne, les interfaces passives ou les liaisons de basculement.
mgmt	(Facultatif) Utilisez les interfaces de gestion pour gérer les instances d'application. Elles peuvent être partagées par un ou plusieurs périphériques logiques pour accéder à des hôtes externes; les périphériques logiques ne peuvent pas communiquer sur cette interface avec d'autres périphériques logiques qui partagent l'interface. Vous ne pouvez affecter qu'une seule interface de gestion par périphérique logique.
firepower-eventing	(Facultatif) Cette interface est une interface de gestion secondaire pour les appareils Cisco FTD. Pour utiliser cette interface, vous devez configurer son adresse IP et d'autres paramètres à l'aide de l'interface de ligne de commande Cisco FTD. Par exemple, vous pouvez séparer le trafic de gestion des événements (comme les événements Web). Consultez la section « Interfaces de gestion » dans le chapitre Configuration système du guide de configuration Centre de gestion. Les interfaces pour événements Firepower peuvent être partagées par un ou plusieurs périphériques logiques pour accéder à des hôtes externes; les périphériques logiques ne peuvent pas communiquer sur cette interface avec d'autres périphériques logiques qui partagent l'interface.
cluster	(Facultatif) Type d'interface spéciale utilisé pour un périphérique logique en grappe. Ce type est automatiquement attribué au lien de contrôle de grappe pour les communications inter-unités de grappe. Par défaut, la liaison de commande de grappe est automatiquement créée sur le canal de port 48.

Modes de commande

scope cabling/scope fabric a/

Historique des commandes

Version	Modification
2.4(1)	Ajout du type **data-sharing**.
1.1(4)	Ajout du type **firepower-eventing**.

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Les instances de contenant peuvent partager des interfaces de type partage de données. Cette fonctionnalité vous permet d'économiser l'utilisation de l'interface physique et de prendre en charge des déploiements réseau flexibles. Lorsque vous partagez une interface, le châssis utilise des adresses MAC uniques pour transférer le trafic vers la bonne instance. Cependant, les interfaces partagées peuvent faire grossir la table de transfert en raison de la nécessité d'une topologie de maillage complet dans le châssis (chaque instance doit pouvoir communiquer avec toutes les autres instances qui partagent la même interface). Par conséquent, il y a des limites au nombre d'interfaces que vous pouvez partager.

Exemple

L'exemple suivant montre comment configurer le type de port de l'interface, puis répertorier les commandes disponibles :

```
firepower-9300* # scope cabling
firepower-9300 /cabling* # scope fabric a
firepower-9300 /cabling/fabric* # create breakout port breakout 2 1
firepower-9300 /cabling/fabric* # show config
 scope fabric a
+    enter breakout 2 3
+    exit
 exit
firepower-9300 /cabling/fabric* # exit
firepower-9300 /cabling* # exit
```

Le système redémarre après l'utilisation de la commande `commit-buffer`.

```
firepower-9300* # scope eth-uplink
firepower-9300 /eth-uplink* # scope fabric a
firepower-9300 /eth-uplink/fabric* # show

Fabric:
    Fabric ID
    ---------
    Afirepower-9300 /eth-uplink/fabric* # show
  <CR>
  >               Redirect it to a file
  >>              Redirect it to a file in append mode
  aggr-interface  Aggregate Interface
  detail          Detail
  event           Event Management
  expand          Expand
  fault           Fault
  fsm             Fsm
  interface       Interface
  port-channel    Port Channel
  stats           statistics
  |               Pipe command output to filter

firepower-9300 /eth-uplink/fabric* # show aggr-interface expand
firepower-9300 /eth-uplink/fabric* # show aggr-interface
  1-4     Slot
  <CR>
  >       Redirect it to a file
  >>      Redirect it to a file in append mode
```

```
  detail  Detail
  expand  Expand
  n/n     Ethernet<Slot Id>/<Aggregate Port Id>
  |       Pipe command output to filter
firepower-9300 /eth-uplink/fabric* # show aggr-interface expand
firepower-9300 /eth-uplink/fabric* #
  acknowledge  Acknowledge
  create       Create managed objects
  delete       Delete managed objects
  enter        Enters a managed object
  scope        Changes the current mode
  show         Show system information

firepower-9300 /eth-uplink/fabric* # scope aggr-interface
  1-4  Slot
  n/n  Ethernet<Slot Id>/<Aggregate Port Id>

firepower-9300 /eth-uplink/fabric* # scope port-channel 2
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface* # create member-port
Ethernet2/1/1
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface/member-port* # show config
+enter member-port 2 1
+exit
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface/member-port* #
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface/member-port* # exit
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface* # exit
firepower-9300 /eth-uplink/fabric/port-channel* # show config
 enter port-channel 2
     enable
+    enter aggr-interface 2 1
+        enter member-port 2 1
+        exit
+    exit
     enter member-port 1 6
         enable
     exit
     set auto-negotiation no
     set descr ""
     set duplex fullduplex
     set flow-control-policy default
     set lacp-policy-name default
     set nw-ctrl-policy default
     set port-channel-mode active
     set port-type data
     set speed 1gbps
 exit

firepower-9300 /eth-uplink/fabric/port-channel* # set port-type
  cluster             Cluster
  data                Data
  data-sharing        Data Sharing
  firepower-eventing  Firepower Eventing
  mgmt                Mgmt

firepower-9300 /eth-uplink/fabric/port-channel* # set port-type cluster
firepower-9300 /eth-uplink/fabric/port-channel* commit-buffer
firepower-9300 /eth-uplink/fabric/port-channel #
```

Commandes associées

Commande	Description
create port-channel	Ajoute une interface EthernetChannel.

Commande	Description
scope interface	Modifie une interface physique.

set prefix

Pour définir le préfixe d'adresse MAC à utiliser lors de la génération automatique des adresses MAC pour les interfaces d'instance de contenant, utilisez la commande **set prefix**.

set prefix *prefix*

Description de la syntaxe

prefix	Spécifie une valeur décimale comprise entre 0 et 65 535. Ce préfixe est converti en nombre hexadécimal à quatre chiffres et utilisé dans l'adresse MAC.

Modes de commande

scope ssa/scope auto-macpool/

Historique des commandes

Version	Modification
2.4(1)	Commande ajoutée.

Instructions d'utilisation

Le châssis FXOS génère automatiquement les adresses MAC pour les interfaces d'instance et garantit qu'une interface partagée dans chaque instance utilise une adresse MAC unique.

Si vous attribuez manuellement une adresse MAC à une interface partagée dans l'application, l'adresse MAC attribuée manuellement est utilisée. Si vous supprimez ultérieurement l'adresse MAC manuelle, l'adresse générée automatiquement est utilisée. Dans les rares cas où l'adresse MAC générée entre en conflit avec une autre adresse MAC privée de votre réseau, nous vous suggérons de définir manuellement l'adresse MAC pour l'interface dans l'application.

Étant donné que les adresses générées automatiquement commencent par A2, vous ne devez pas commencer les adresses MAC manuelles par A2 en raison du risque de chevauchement d'adresses.

Remarque Même si vous ne partagez pas une sous-interface, si vous configurez manuellement des adresses MAC, veillez à utiliser des adresses MAC uniques pour toutes les sous-interfaces sur la même interface parente afin de garantir une classification correcte.

Le châssis FXOS génère l'adresse MAC en utilisant le format suivant :

A2*xx.yyzz.zzzz*

Où *xx.yy* est un préfixe défini par l'utilisateur ou un préfixe défini par le système, et *zz.zzzz* est un compteur interne généré par le châssis. Le préfixe défini par le système correspond aux 2 octets inférieurs de la première adresse MAC dans l'ensemble d'adresses MAC gravées qui est programmée dans la mémoire IDPROM. Utilisez **connect fxos**, puis **show module** pour afficher l'ensemble des adresses MAC. Par exemple, si la plage d'adresses MAC affichée pour le module 1 va de b0aa.772f.f0b0 à b0aa.772f.f0bf, le préfixe du système sera f0b0.

Le préfixe défini par l'utilisateur est un entier qui est converti en hexadécimal. Pour donner un exemple de la façon dont le préfixe défini par l'utilisateur est utilisé, si vous définissez un préfixe de 77, le châssis convertit 77 dans la valeur hexadécimale 004D (*yyxx*). Lorsqu'il est utilisé dans l'adresse MAC, le préfixe est inversé (*xxyy*) pour correspondre à la forme native du châssis :

A2**4D**.**00***zz.zzzz*

Pour un préfixe 1009 (03F1), l'adresse MAC est :

A2**F1**.**03***zz*.*zzzz*

Exemple

L'exemple suivant définit le préfixe MAC sur 33.

```
firepower# scope ssa
firepower /ssa # scope auto-macpool
firepower /ssa/auto-macpool # set prefix 33
firepower /ssa/auto-macpool* # commit-buffer
firepower /ssa/auto-macpool
```

Commandes associées

Commande	Description
scope ssa	Permet d'accéder au mode ssa.
scope auto-macpool	Permet d'accéder au mode auto-macpool.
show mac-address	Affiche les adresses MAC attribuées.

set protocol

Pour spécifier le protocole à utiliser lors de la communication avec le serveur distant pour la politique d'exportation, utilisez la commande **set protocol** .

set protocol { **ftp** | **scp** | **sftp** | **tfp** }

Description de la syntaxe

ftp	Spécifie le protocole FTP (File Transfer Protocol) pour le transfert de fichiers.
scp	Spécifie le protocole SCP (Secure Copy Protocol) pour le transfert de fichiers.
sftp	Spécifie le protocole SFTP (Secure File Transfer Protocol) pour le transfert de fichiers.
tfp	Spécifie le protocole TFTP (Trivial File Transfer Protocol) pour le transfert de fichiers.

Modes de commande

Politique d'exportation de la configuration (/org/cfg-export-policy)

Historique des commandes

Version	Modification
2.0.1	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour spécifier un protocole de transfert de fichiers.

Exemple

Cet exemple montre comment définir le numéro de port de la politique d'exportation :

```
firepower-9300* # scope org
firepower-9300 /org* # scope cfg-export-policy default
firepower-9300 /org/cfg-export-policy* # set protocol scp
firepower-9300 /org/cfg-export-policy* # commit-buffer
firepower-9300 /org/cfg-export-policy #
```

Commandes associées

Commande	Description
set adminstate (/org)	Active la politique d'exportation.
set hostname (/org)	Spécifie l'emplacement du nom de domaine où le fichier de sauvegarde doit être stocké.
set password (/org)	Spécifie le mot de passe pour le nom d'utilisateur du serveur distant.
set port (/org)	Spécifie le numéro de port.
set protocol (/org)	Spécifie le protocole à utiliser lors de la communication avec le serveur distant.
set remote-file (/org)	Spécifie le chemin d'accès complet vers l'endroit où vous souhaitez exporter le fichier de configuration, y compris le nom du fichier.

Commande	Description
set schedule (/org)	Spécifie la fréquence à laquelle vous souhaitez que la configuration soit exportée automatiquement.
set user (/org)	Spécifie le nom d'utilisateur que le système doit utiliser pour se connecter au serveur distant.

set realm

Pour spécifier le service d'authentification par défaut, utilisez la commande **set realm**.

set realm {**ldap** | **local** | **none** | **radius** | **tacacs**}

Description de la syntaxe

ldap	Spécifie l'authentification LDAP.
local	Spécifie l'authentification locale.
none	Permet aux utilisateurs locaux de se connecter sans spécifier de mot de passe.
radius	Spécifie l'authentification RADIUS.
tacacs	Spécifie l'authentification TACACS+.

Modes de commande

Mode d'authentification par défaut

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment accéder au mode sécurité/authentification par défaut et le service d'authentification par défaut sur Radius :

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set realm radius
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

Commandes associées

Commande	Description
set auth-server-group	Spécifie un groupe de fournisseurs d'authentification associé.
set use-2-factor	Définit la méthode d'authentification sur l'authentification à deux facteurs pour un domaine Radius ou TACACS+.

set refresh-period

Pour définir la période d'actualisation de session Web (durée maximale autorisée entre les demandes d'actualisation pour un utilisateur de ce domaine), utilisez la commande **set refresh-period**.

set refresh-period *seconds*

Description de la syntaxe

seconds	Nombre de secondes après lesquelles une session Web est considérée comme inactive. La valeur peut être comprise entre 0 et 3 600 secondes; la valeur par défaut est de 600 secondes.

Modes de commande

Mode d'authentification par défaut

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Si cette durée est dépassée, FXOS considère la session Web comme inactive, sans y mettre fin.

Exemple

Cet exemple montre comment accéder au mode d'authentification par défaut et définir l'intervalle d'actualisation de session :

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set refresh-period 800
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

Commandes associées

Commande	Description
set timeout values	Les commandes **set absolute-session-timeout**, **set con-absolute-session-timeout**, **set con-session-timeout** et **set session-timeout** permettent de définir diverses valeurs de délai d'expiration.

set regenerate

Pour régénérer les clés dans le trousseau de clés par défaut, utilisez la commande **set regenerate**.

set regenerate {**no** | **yes**}

Description de la syntaxe

no	Ne pas régénérer les clés.
yes	Régénérer les clés.

Modes de commande

Mode trousseau de clés

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour régénérer les clés RSA dans le trousseau de clés par défaut. Cette commande est uniquement acceptée dans le trousseau de clés par défaut.

Exemple

Cet exemple montre comment renouveler les clés dans le trousseau de clés par défaut :

```
FP9300-A# scope security
FP9300-A /security # scope keyring default
FP9300-A /security/keyring # set regenerate yes
FP9300-A /security/keyring* # commit-buffer
switch-A /security/keyring #
```

Commandes associées

Commande	Description
set cert	Permet d'accéder à un certificat RSA pour un trousseau de clés.
set modulus	Spécifie le module de clé RSA (longueur de clé SSL) en bits.
set trustpoint	Spécifie si le certificat de trousseau de clés peut être renouvelé.

set remote-address

Pour spécifier l'adresse IP distante d'une connexion IPSec, utilisez la commande **set remote-address**.

set remote-address *ip_address*

Description de la syntaxe

ip_address	Fournissez une adresse de passerelle distante IPv4 ou IPv6 d'une connexion IPSec; 510 caractères maximum.

Modes de commande

Mode connexion (/security/ipsec/connection)

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande et la commande **set local-address** pour définir les terminaux d'une connexion IPSec.

Exemple

Cet exemple montre comment définir l'adresse distante d'une connexion IPSec :

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # enter connection testconn
FP9300-A /security/ipsec/connection # set local-address 209.165.202.129
FP9300-A /security/ipsec/connection* # commit-buffer
FP9300-A /security/ipsec/connection #
```

Commande	Description
create connection	Crée une connexion IPSec.
set local-addr	Définit l'adresse IP locale d'une connexion IPSec.

set remote-ike-ident

Pour spécifier l'identité IKE de l'homologue distant pour une connexion de tunnel IPSec, utilisez la commande **set remote-ike-ident**.

set remote-ike-ident *remote_ID*

Description de la syntaxe

remote_ID	Identification IKE de l'homologue distant; 510 caractères maximum.

Modes de commande

Mode connexion (/security/ipsec/connection)

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour spécifier l'ID IKE de l'homologue distant pour une connexion IPSec. Cette identification est utilisée pour la validation des homologues lors des négociations IKE.

Exemple

Cet exemple montre comment spécifier l'ID IKE distant pour une connexion IPSec :

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # enter connection testconn
FP9300-A /security/ipsec/connection # set remote-ike-ident 203.0.113.12
FP9300-A /security/ipsec/connection* # commit-buffer
FP9300-A /security/ipsec/connection #
```

Commande	Description
create connection	Crée une connexion IPSec.
set remote-addr	Définit l'adresse IP distante d'une connexion IPSec.

set remote-subnet

Pour spécifier le sous-réseau distant d'une connexion de tunnel IPSec, utilisez la commande **set remote-subnet**.

set remote-subnet *ip_address/mask_bits*

Description de la syntaxe

ip_address/mask_bits	Fournissez une adresse/un masque de sous-réseau distant IPv4 ou IPv6 pour la connexion IPSec; 510 caractères maximum.

Modes de commande

Mode connexion (/security/ipsec/connection)

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour spécifier l'adresse IP/le masque du sous-réseau distant d'une connexion IPSec.

Exemple

Cet exemple montre comment définir le sous-réseau distant d'une connexion IPSec :

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # enter connection testconn
FP9300-A /security/ipsec/connection # set remote-subnet 209.165.202.128/27
FP9300-A /security/ipsec/connection* # commit-buffer
FP9300-A /security/ipsec/connection #
```

Commande	Description
create connection	Crée une connexion IPSec.
set remote-addr	Définit l'adresse IP distante d'une connexion IPSec.

set remote-user

Pour restreindre l'accès aux utilisateurs correspondant à un rôle d'utilisateur établi, utilisez la commande **set remote-user**.

set remote-user default-role { **assign-default-role** | **no-login** }

Description de la syntaxe

assign-default-role	Lorsqu'un utilisateur tente de se connecter et que le fournisseur d'authentification distant ne fournit pas de rôle d'utilisateur avec les informations d'authentification de l'utilisateur, ce dernier est autorisé à se connecter avec un rôle d'utilisateur en lecture seule.
no-login	Lorsqu'un utilisateur tente de se connecter et que le fournisseur d'authentification distant ne fournit pas de rôle d'utilisateur avec les informations d'authentification de l'utilisateur, l'accès est refusé.

Modes de commande

Mode sécurité

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

assign-default-role correspond au comportement par défaut.

Exemple

Cet exemple montre comment accéder au mode sécurité et refuser l'accès aux utilisateurs sans rôle d'utilisateur :

```
FP9300-A# scope security
FP9300-A /security # set remote-user default-role no-login
FP9300-A /security* # commit-buffer
FP9300-A /security #
```

Commandes associées

Commande	Description
set authentication	Spécifie le service d'authentification par défaut.

set reporting-interval

Pour définir la fréquence de rapport des statistiques surveillées, utilisez la commande **set reporting-interval**.

set reporting-interval *interval*

Description de la syntaxe

interval	Durée définissant l'intervalle de rapport des statistiques ; les valeurs disponibles sont les suivantes : • `15minutes` : intervalles de 15 minutes • `2hours` : intervalles de deux heures (120 minutes) • `2minutes` : intervalles de deux minutes • `30minutes` : intervalles de 30 minutes • `4hours` : intervalles de quatre heures (240 minutes) • `60minutes` : intervalles de 60 minutes (une heure) • `8hours` : intervalles de huit heures (480 minutes)

Modes de commande

scope monitoring/scope stats-collection-policy/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez la commande **set collection-interval** pour définir la fréquence de collecte des statistiques et la commande **set reporting-interval** pour définir la fréquence à laquelle ces statistiques sont présentées. Ces intervalles définissent une politique de collecte des statistiques.

Les intervalles de production de rapports sont plus longs que les intervalles de collecte, de sorte que plusieurs points de données statistiques peuvent être collectés au cours de l'‘intervalle de production de rapports, fournissant ainsi des données suffisantes pour calculer et communiquer les valeurs minimales, maximales et moyennes.

Des statistiques peuvent être collectées et présentées pour chacun des domaines fonctionnels suivantes de votre système Firepower. Utilisez la commande **scope stats-collection-policy** pour accéder à une politique de collecte spécifique :

- `Adapter` : statistiques relatives aux adaptateurs.
- `Chassis` : statistiques relatives au châssis du serveur lame.
- `FEX` : statistiques relatives aux dispositifs d'extension de structure.
- `Host` : cette politique est un espace réservé pour une future prise en charge.
- `Port` : statistiques relatives aux ports, y compris les ports de serveur, les ports de liaison ascendante Ethernet et Fibre Channel.
- `Server` : statistiques relatives aux serveurs.

Remarque Il existe une politique de collecte de statistiques par défaut pour chacun de ces domaines fonctionnels. Vous ne pouvez pas créer de politiques de collecte de statistiques supplémentaires, ni supprimer les politiques par défaut existantes. Vous pouvez uniquement modifier les politiques par défaut.

Exemple

Cet exemple montre comment accéder à la politique de collecte de statistiques pour les ports, définir l'intervalle de collecte sur une minute, définir l'intervalle de production de rapports sur 30 minutes, puis valider la transaction :

```
firepower # scope monitoring
firepower /monitoring # scope stats-collection-policy port
firepower /monitoring/stats-collection-policy # set collection-interval 1minute
firepower /monitoring/stats-collection-policy* # set reporting-interval 30minute
firepower /monitoring/stats-collection-policy* # commit-buffer
firepower /monitoring/stats-collection-policy #
```

Commandes associées

Commande	Description
scope stats-collection-policy	Permet d'accéder au mode stats-collection-policy dans lequel vous gérez les intervalles de collecte de statistiques et de création de rapports.
set collection-interval	Spécifie la fréquence à laquelle les statistiques sont collectées.

set resource-profile-name

Pour définir le profil de ressource d'une instance d'application, utilisez la commande **set resource-profile-name**.

set resource-profile-name *profile_name*

Description de la syntaxe

profile_name	Définit le nom du profil de ressource pour cette instance d'application.

Modes de commande

scope ssa/scope slot/create app-instance/

Historique des commandes

Version	Modification
2.4(1)	Peut désormais être utilisée pour les instances de contenant.
1.1(1)	Commande ajoutée pour une utilisation avec vDP.

Instructions d'utilisation

Pour vDP, les profils de ressources sont précréés dans la configuration FXOS lorsque vous téléchargez l'image vDP. Pour les instances de contenant, créez des profils de ressource à l'aide de la commande **create resource-profile**. Utilisez la commande **show resource-profile system** pour afficher les profils disponibles.

Si vous modifiez le profil de ressource d'une instance d'application en cours d'exécution, l'instance redémarre.

Exemple

L'exemple suivant montre comment définir le profil de ressource d'une instance d'application vDP :

```
firepower# scope ssa
firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is Default App

    ---------- --------------- ---------- ---------------------- ----------- --------------

    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
    vdp        8.13.01.09-2    radware    Vm                     Application Yes

firepower /ssa # show resource-profile system
Profile Name       App Name   App Version  Is In Use  Security Model  CPU Logical Core Count
 RAM Size (MB)  Default Profile Profile Type Description
------------------ ---------- ------------ ---------- --------------- ----------------------
 -------------- ---------------- ------------ -----------
DEFAULT-4110-RESOURCE
                    vdp        8.13.01.09-2 No         FPR4K-SM-12
 4          16384 Yes             System
DEFAULT-RESOURCE   vdp        8.13.01.09-2 No        FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36,
 FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

 6          24576 Yes             System
VDP-10-CORES       vdp        8.13.01.09-2 No        FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36,
 FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

10          40960 No              System
VDP-2-CORES        vdp        8.13.01.09-2 No         all
```

```
 2           8192 No              System
VDP-4-CORES        vdp        8.13.01.09-2 No         all
 4          16384 No              System
VDP-8-CORES        vdp        8.13.01.09-2 No         FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36,
 FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

 8          32768 No              System
firepower /ssa/app # exit
firepower /ssa # scope slot 1
firepower /ssa/slot # create app-instance vdp VDP1
firepower /ssa/slot/app-instance* # set resource-profile-name VDP-10-CORES
firepower /ssa/slot/app-instance* #
```

Exemple

L'exemple suivant montre comment définir le profil de ressource d'une instance de contenant Défense contre les menaces :

```
firepower# scope ssa
firepower /ssa # show resource-profile

Profile Name       App Name   App Version  Is In Use  Security Model  CPU Logical Core Count
 RAM Size (MB)  Default Profile Profile Type Description
------------------ ---------- ------------ ---------- --------------- ----------------------
 -------------- --------------- ------------ -----------
bronze              N/A        N/A          No         all
 6            N/A No              Custom       low end device
silver              N/A        N/A          No         all
 8            N/A No              Custom       mid-level

firepower /ssa # scope slot 1
firepower /ssa/slot # create app-instance ftd FTD1
firepower /ssa/slot/app-instance* # set resource-profile-name silver
firepower /ssa/slot/app-instance* #
```

Commandes associées

Commande	Description
show app-attri	Affiche les attributs de l'application actuelle.
create resource-profile	Crée un profil de ressource à utiliser avec les instances de contenant.
show resource-profile-name	Affiche les profils de ressources disponibles.

set session-timeout

Pour définir le délai d'expiration de session inactive pour les sessions Web, SSH et Telnet, utilisez la commande **set session-timeout**.

set session-timeout *seconds*

Description de la syntaxe

seconds	Délai d'expiration de session inactive pour les sessions Web, SSH et Telnet; la valeur peut être comprise entre 0 et 3 600 secondes.

Modes de commande

Mode d'authentification par défaut

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour spécifier le délai d'expiration de session inactive pour les sessions Web, SSH et Telnet.

Exemple

Cet exemple montre comment accéder au mode d'authentification par défaut, puis définir le délai d'expiration de session inactive sur quatre minutes :

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set session-timeout 240
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

Commandes associées

Commande	Description
set refresh-period	Définit la période d'actualisation de session Web.
show detail	Affiche les paramètres de session actuelle et de délai d'expiration de session absolu.

set snmp-adminappinstance

Pour définir les paramètres de configuration de l'instance d'application du protocole SNMP (Simple Network Management Protocol), utilisez la commande **set snmp adminappinstance**.

set snmp adminappinstance { **slot | appname | id | enable | yes/no** }

Description de la syntaxe

slot	Sélection de logement entre 1 et 3
appname	Affiche le nom de l'application
id	Affiche le nom de l'identifiant
enable	Sélectionnez **Oui/Non** pour activer ou désactiver

Modes de commande

scope monitoring

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Cisco vous recommande d'activer uniquement les services de communication nécessaires pour interagir avec d'autres applications réseau. Vous devez donc activer l'agent SNMP (**enable snmp**).

Il s'agit d'une sous-commande de la commande **show** dans scope monitoring.

Exemple

Cet exemple montre comment afficher les informations du protocole SNMP :

```
Firepower /monitoring # set snmp adminappinstance
  slot  Slot
Firepower /monitoring # set snmp adminappinstance slot
  1-3  Admin App Slot
Firepower /monitoring # set snmp adminappinstance slot 1
  appname  AppName
Firepower /monitoring # set snmp adminappinstance slot 1 appname
  WORD  Admin App Name (Min size 0, Max size 510)
Firepower /monitoring # set snmp adminappinstance slot 1 appname ftd
  id  Id
Firepower /monitoring # set snmp adminappinstance slot 1 appname ftd id
  WORD  Admin App Id (Min size 0, Max size 510)
Firepower /monitoring # set snmp adminappinstance slot 1 appname ftd id FTD
  enable  Enable
Firepower /monitoring # set snmp adminappinstance slot 1 appname ftd id FTD enable
  no   No
  yes  Yes
Firepower /monitoring # set snmp adminappinstance slot 1 appname ftd id FTD enable yes
Firepower /monitoring* # commit-buffer

Firepower /monitoring #
Firepower /monitoring # show snmp
Name: snmp
    Admin State: Enabled
```

```
Port: 161
Is Community Set: No
Sys Contact:
Sys Location:
Admin App Enable: Yes
    Admin App Slot: 1
    Admin App Name: ftd
    Admin App Id: FTD
```

set snmp

Pour définir les paramètres de configuration du protocole SNMP (Simple Network Management Protocol), utilisez la commande **set snmp**.

set snmp {**community** | **syscontact** | **syslocation**}

Description de la syntaxe

community	Après avoir saisi cette commande, vous êtes invité à saisir un nom de communauté SNMP, qui peut comporter entre 1 et 32 caractères alphanumériques. Le nom de la communauté ne s'affiche pas lorsque vous le saisissez. Cependant, après avoir appuyé sur **Entrée**, l'invite du système s'affiche avec un astérisque pour indiquer que vous devez valider le tampon.
syscontact *name*	Saisissez le nom de la personne à contacter au sujet de SNMP sur ce système; il peut comporter de 0 à 255 caractères alphanumériques.
syslocation *location*	Saisissez un emplacement pour ce système; il peut comporter de 0 à 510 caractères alphanumériques.

Modes de commande

scope monitoring/

Historique des commandes

Version	Modification
1.1.1	Commande ajoutée.

Instructions d'utilisation

Cisco vous recommande d'activer uniquement les services de communication nécessaires pour interagir avec d'autres applications réseau.

Vous devez activer l'agent SNMP (**enable snmp**) avant de configurer SNMP sur ce système.

Utilisez **set snmp community** pour spécifier la chaîne d'accès de communauté utilisée afin d'autoriser l'accès à la destination de déroutement SNMP. Si SNMPv1 ou v2c est défini comme version SNMP, l'argument de communauté est utilisé comme identifiant de communauté. Si SNMPv3 est configuré, il est utilisé comme nom d'utilisateur SNMP pour l'envoi des messages de déroutement.

Lorsque vous spécifiez un nom de communauté SNMP, vous activez automatiquement les versions SNMP 1 et 2c pour interroger les demandes du gestionnaire à distance SNMP.

Remarque Sachez que les versions SNMP 1 et 2c présentent d'important problèmes de sécurité : elles transmettent toutes les informations sans chiffrement, y compris l'identifiant de communauté, qui constitue la seule forme d'authentification dans ces versions.

Il ne peut y avoir qu'un seul nom de communauté; cependant, vous pouvez utiliser **set snmp community** pour remplacer le nom existant. Pour supprimer un nom de communauté existant, saisissez **set snmp community**, mais n'entrez pas d'identifiant de communauté; appuyez simplement une nouvelle fois sur **Entrée**. Une fois le tampon validé, la sortie **show snmp** inclut la ligne `Is Community Set: No`.

Exemple

L'exemple suivant montre comment accéder au mode surveillance, activer le traitement SNMP, définir l'identifiant de communauté SNMP et un contact système, valider les modifications et utiliser la commande **show snmp** pour confirmer les modifications :

```
firepower # scope monitoring
firepower /monitoring # enable snmp
firepower /monitoring* # set snmp community
Enter a snmp community:
firepower /monitoring* # set snmp syscontact R_Admin
firepower /monitoring* # commit-buffer
firepower /monitoring # show snmp
Name: snmp
    Admin State: Enabled
    Port: 161
    Is Community Set: Yes
    Sys Contact: R_Admin
    Sys Location:
firepower /monitoring #
```

Commandes associées

Commande	Description
disable snmp	Désactive le protocole SNMP.
enable snmp	Active le protocole SNMP
show snmp	Affiche la configuration SNMP actuelle.

set (snmp-trap)

Pour spécifier les paramètres de déroutement SNMP (Simple Network Management Protocol), utilisez la commande **set** en mode snmp-trap.

set { **community** | **notificationtype** | **port** | **v3privilege** | **version** }

Description de la syntaxe

community	Spécifie l'identifiant de communauté SNMPv1/v2c ou le nom d'utilisateur SNMPv3 pour autoriser l'accès à la destination du déroutement. Après avoir saisi cette commande, le nom de la communauté vous est demandé. Ce nom peut comporter jusqu'à 32 caractères sans espace; il ne s'affiche pas lors de la saisie.
notificationtype { **informs** | **traps** }	Spécifie le type de notification SNMP produite par cet agent : • **informs** : notifications spontanées, envoyées pour informer le gestionnaire d'événements locaux importants. Ces messages donnent lieu à une confirmation. Cette option peut uniquement être utilisée si **version** est définie sur **vc2**. • **traps** : notifications spontanées, envoyées pour informer le gestionnaire d'événements locaux importants. Ces messages ne donnent pas lieu à une confirmation.
port *port_num*	Utilisez cette commande pour modifier le port sur lequel l'agent reçoit les requêtes SNMP; le port par défaut est 161.
v3privilege { **auth** | **noauth** | **priv** }	Utilisez cette commande pour spécifier le niveau de sécurité du protocole SNMPv3 (Simple Network Management Protocol, version 3) pour les déroutements SNMP transmis. • **auth** : spécifie l'authentification par hachage avec clé, sans chiffrement. • **noauth** : ne spécifie ni authentification ni chiffrement. Notez que bien que vous puissiez le spécifier, FXOS ne prend pas en charge ce niveau de sécurité avec SNMPv3. • **priv** : spécifie l'authentification par hachage et le chiffrement des données (confidentialité).

version {**v1** | **v2c** | **v3**}	Utilisez cette commande pour spécifier le modèle de sécurité SNMP utilisé lors de l'envoi de notifications de déroutement : • **v1** : spécifie la version 1 du protocole SNMP. • **v2c** : spécifie la version 2c de SNMP. • **v3** : spécifie la version 3 du protocole SNMP. **Remarque** Sachez que les versions SNMP 1 et 2c présentent d'important problèmes de sécurité : elles transmettent toutes les informations sans chiffrement, y compris l'identifiant de communauté, qui constitue la seule forme d'authentification dans ces versions.

Modes de commande

scope monitoring/snmp-trap

Historique des commandes

Version	Modification
1.1.1	Commande ajoutée.

Instructions d'utilisation

Vous devez activer le protocole SNMP (**enable snmp**) et créer une communauté SNMP (**set snmp community**) avant de créer un déroutement SNMP et de définir ces paramètres.

Lorsque vous créez un déroutement SNMP, vous accédez automatiquement au mode monitoring/snmp-trap accompagné d'un astérisque pour indiquer que le nouveau déroutement n'est pas encore validé.

Remarque Vous pouvez créer jusqu'à huit déroutements SNMP.

Si SNMPv1 ou v2c est configuré avec **set version**, l'argument **set community** est utilisé comme identifiant de communauté. Si SNMPv3 est configuré, il est utilisé comme nom d'utilisateur pour la transmission des notifications.

Avec SNMPv3, le paramètre **v3privilege** du déroutement doit être compatible avec le niveau de sécurité de l'utilisateur SNMPv3 associé; à savoir, la configuration de sécurité de l'utilisateur associé doit être au moins aussi sécurisée que celle du déroutement. Par exemple, si l'authentification est activée pour l'utilisateur SNMPv3 (authentification, mais pas de chiffrement de confidentialité), le mot de passe PRIV de l'utilisateur ne sera pas défini. Cela étant, pour envoyer des notifications avec la confidentialité activée (à savoir, authentifier et chiffrer la confidentialité), le mot de passe PRIV de l'utilisateur sera défini. Le mot de passe associé à l'utilisateur SNMPv3 est utilisé pour authentifier l'utilisateur lors de l'envoi d'un déroutement ou d'une information.

Exemple

L'exemple suivant active SNMP, crée un déroutement SNMP à l'aide d'une adresse IPv4, définit la version sur v3, définit le niveau de privilège v3 sur confidentialité, puis valide la transaction :

```
firepower # scope monitoring
firepower /monitoring/ # enable snmp
firepower /monitoring/ # create snmp-trap 192.168.100.112
firepower /monitoring/snmp-trap* # set notificationtype traps
```

```
firepower /monitoring/snmp-trap* # set version v3
firepower /monitoring/snmp-trap* # set v3privilege priv
firepower /monitoring/snmp-trap* # commit-buffer
firepower /monitoring/snmp-trap #
```

Commandes associées

Commande	Description
create snmp-trap	Crée une destination de déroutement SNMP.
enable snmp	Active le protocole SNMP.

set (snmp-user)

Pour spécifier les paramètres d'un utilisateur SNMP (Simple Network Management Protocol) v3 existant, utilisez la commande **set** en mode `snmp-user`.

set {**aes-128** | **auth** | **password** | **priv-password**}

Description de la syntaxe

aes-128 {**no** | **yes**}	Désactiver ou activer l'utilisation du chiffrement AES-128 (Advanced Encryption Standard) : saisissez `no` ou `yes`. Par défaut, le chiffrement AES-128 est désactivé.
auth sha	Active l'authentification pour les utilisateurs SNMPv3 basée sur l'algorithme de hachage sécurisé (SHA) HMAC.
password	Spécifiez un mot de passe pour cet utilisateur; vous êtes invité à saisir le mot de passe et à le confirmer après avoir saisi cette commande.
priv-password	Spécifiez un mot de passe de confidentialité de l'utilisateur; vous êtes invité à saisir le mot de passe et à le confirmer après avoir saisi cette commande. Le mot de passe de confidentialité AES doit comporter au moins huit caractères.

Modes de commande

scope monitoring/snmp-user

Historique des commandes

Version	Modification
1.1.1	Commande ajoutée.

Instructions d'utilisation

Vous devez activer SNMP (**enable snmp** avant de créer un utilisateur SNMP et de définir ces paramètres.

Lorsque vous créez un utilisateur SNMP, vous accédez automatiquement au mode monitoring/snmp-user accompagné d'un astérisque pour indiquer que le nouvel utilisateur n'est pas encore validé.

Le mot de passe de confidentialité, ou option priv, offre un choix de chiffrement DES ou AES-128 pour le chiffrement de sécurité SNMP. Si vous activez la configuration AES-128 et incluez un mot de passe de confidentialité pour un utilisateur SNMPv3, le châssis Firepower utilise le mot de passe de confidentialité pour générer une clé AES de 128 bits.

Exemple

L'exemple suivant crée un utilisateur SNMPv3 nommé `snmp-user14`, active le chiffrement AES-128, définit un mot de passe de confidentialité et valide la transaction :

```
firepower # scope monitoring
firepower /monitoring/ # enable snmp
firepower /monitoring/ # create snmp-user snmp-user14
Password:
firepower /monitoring/snmp-user* # set aes-128 yes
firepower /monitoring/snmp-user* # set priv-password
Enter a password:
Confirm the password:
firepower /monitoring/snmp-user* # commit-buffer
```

```
firepower /monitoring/snmp-user #
```

Commandes associées

Commande	Description
create snmp-user	Crée un utilisateur SNMPv3.
enable snmp	Active le protocole SNMP.

set speed

Pour définir la vitesse de l'interface, utilisez la commande **set speed**.

Remarque Cette commande est uniquement disponible dans port-channel scope.

set speed { **10mbps** | **100mbps** | **1gbps** | **10gbps** | **40gbps** | **100gbps** }

Description de la syntaxe

10mbps	(Facultatif) Définit la vitesse sur 10 Mbit/s.
100mbps	(Facultatif) Définit la vitesse sur 100 Mbit/s.
1gbps	(Facultatif) Définit la vitesse sur 1 Gbit/s.
10gbps	(Facultatif) Définit la vitesse sur 10 Gbit/s.
40gbps	(Facultatif) Définit la vitesse sur 40 Gbit/s.
100gbps	(Facultatif) Définit la vitesse sur 100 Gbit/s.

Modes de commande

scope eth-uplink/scope fabric a/port-channel/

Historique des commandes

Version	Modification
2.4.1(1)	Commande ajoutée.

Instructions d'utilisation

La vitesse d'interface que vous définissez peut avoir une incidence sur le mode duplex utilisé pour une interface. Vous devez donc définir la vitesse avant de définir le mode duplex. Si vous définissez une vitesse de 10 ou 100 Mbit/s, le port est automatiquement configuré pour utiliser le mode semi-duplex, mais vous pouvez spécifier le mode duplex intégral à la place. Si vous définissez une vitesse de 1 000 Mbit/s (1 Gbit/s) ou plus, le mode duplex intégral est automatiquement utilisé.

Exemple

Cet exemple montre comment définir la vitesse de l'interface :

```
firepower-9300 # scope eth-uplink
firepower-9300 /eth-uplink # scope fabric a
firepower-9300 /eth-uplink/fabric # create port-channel id
firepower-9300 /eth-uplink/fabric/port-channel* # enable
firepower-9300 /eth-uplink/fabric/port-channel* # set speed
firepower-9300 /eth-uplink/fabric/port-channel* # set speed 1gbps
firepower-9300 /eth-uplink/fabric/port-channel* # commit-buffer
firepower-9300 /eth-uplink/fabric/port-channel #
```

Commandes associées

Commande	Description
duplex	Spécifie le mode duplex intégral ou semi-duplex.

Commande	Description
show interface	Affiche l'état de l'interface, qui comprend les paramètres de vitesse.

set speed (aggr-interface)

Pour définir la vitesse de l'interface, utilisez la commande **set speed**.

set speed {**10mbps** | **100mbps** | **1gbps** | **10gbps** | **40gbps** | **100gbps**}

Description de la syntaxe

10mbps	(Facultatif) Définit la vitesse sur 10 Mbit/s.
100mbps	(Facultatif) Définit la vitesse sur 100 Mbit/s.
1gbps	(Facultatif) Définit la vitesse sur 1 Gbit/s.
10gbps	(Facultatif) Définit la vitesse sur 10 Gbit/s.
40gbps	(Facultatif) Définit la vitesse sur 40 Gbit/s.
100gbps	(Facultatif) Définit la vitesse sur 100 Gbit/s.

Modes de commande

scope eth-uplink/scope fabric a/port-channel/

Historique des commandes

Version	Modification
2.4.1(1)	Commande ajoutée.

Instructions d'utilisation

La vitesse d'interface que vous définissez peut avoir une incidence sur le mode duplex utilisé pour une interface. Vous devez donc définir la vitesse avant de définir le mode duplex. Si vous définissez une vitesse de 10 ou 100 Mbit/s, le port est automatiquement configuré pour utiliser le mode semi-duplex, mais vous pouvez spécifier le mode duplex intégral à la place. Si vous définissez une vitesse de 1 000 Mbit/s (1 Gbit/s) ou plus, le mode duplex intégral est automatiquement utilisé.

Cet exemple montre comment définir la vitesse de l'interface :

```
firepower-9300* # scope cabling
firepower-9300 /cabling* # scope fabric a
firepower-9300 /cabling/fabric* # create breakout port breakout 2 1
firepower-9300 /cabling/fabric* # show config
 scope fabric a
+    enter breakout 2 3
+    exit
 exit
firepower-9300 /cabling/fabric* # exit
firepower-9300 /cabling* # exit
firepower-9300* # scope eth-uplink
firepower-9300 /eth-uplink* # scope fabric a
firepower-9300 /eth-uplink/fabric* # show

Fabric:
    Fabric ID
    ---------
    A
firepower-9300 /eth-uplink/fabric* # show
  <CR>
  >               Redirect it to a file
```

```
  >>              Redirect it to a file in append mode
  aggr-interface  Aggregate Interface
  detail          Detail
  event           Event Management
  expand          Expand
  fault           Fault
  fsm             Fsm
  interface       Interface
  port-channel    Port Channel
  stats           statistics
  |               Pipe command output to filter

firepower-9300 /eth-uplink/fabric* # show aggr-interface expand
firepower-9300 /eth-uplink/fabric* # show aggr-interface
  1-4     Slot
  <CR>
  >       Redirect it to a file
  >>      Redirect it to a file in append mode
  detail  Detail
  expand  Expand
  n/n     Ethernet<Slot Id>/<Aggregate Port Id>
  |       Pipe command output to filter
firepower-9300 /eth-uplink/fabric* # show aggr-interface expand
firepower-9300 /eth-uplink/fabric* #
  acknowledge  Acknowledge
  create       Create managed objects
  delete       Delete managed objects
  enter        Enters a managed object
  scope        Changes the current mode
  show         Show system information

firepower-9300 /eth-uplink/fabric* # scope aggr-interface
  1-4  Slot
  n/n  Ethernet<Slot Id>/<Aggregate Port Id>

firepower-9300 /eth-uplink/fabric* # scope port-channel 2
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface* # create member-port
Ethernet2/1/1
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface/member-port* # show config
+enter member-port 2 1
+exit
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface/member-port* # exit
firepower-9300 /eth-uplink/fabric/port-channel/aggr-interface* # exit
firepower-9300 /eth-uplink/fabric/port-channel* # show config
 enter port-channel 2
     enable
+    enter aggr-interface 2 1
+        enter member-port 2 1
+        exit
+    exit
     enter member-port 1 6
         enable
     exit
     set auto-negotiation no
     set descr ""
     set duplex fullduplex
     set flow-control-policy default
     set lacp-policy-name default
     set nw-ctrl-policy default
     set port-channel-mode active
     set port-type data
     set speed 1gbps
 exit
firepower-9300 /eth-uplink/fabric/port-channel* # set speed
```

```
  100gbps  100 Gbps
  100mbps  100 Mbps
  10gbps   10 Gbps
  10mbps   10 Mbps
  1gbps    1 Gbps
  40gbps   40 Gbps

firepower-9300 /eth-uplink/fabric/port-channel* # set speed 1gbps
firepower-9300 /eth-uplink/fabric/port-channel* commit-buffer
firepower-9300 /eth-uplink/fabric/port-channel #
```

Commandes associées

Commande	Description
duplex	Spécifie le mode duplex intégral ou semi-duplex.
show interface	Affiche l'état de l'interface, qui comprend les paramètres de vitesse.

set ssh-server

Pour définir la taille de clé d'hôte SSH, utilisez la commande **set ssh-server**.

set ssh-server host-key rsa *key_size*

Description de la syntaxe

rsa	Indique le type de clé d'hôte.
key-size	Taille de clé d'hôte.

Modes de commande

Mode de service

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour définir la taille de clé d'hôte SSH.

Exemple

Cet exemple montre comment définir la taille de clé d'hôte SSH sur 2 048 bits :

```
FP9300-A # scope system
FP9300-A /system # scope services
FP9300-A /system/services # set ssh-server host-key rsa 2048
FP9300-A /system/services* # commit-buffer
FP9300-A /system/services #
```

Commandes associées

Commande	Description
create ssh-server	Crée une clé d'hôte de serveur SSH.
delete ssh-server	Supprime la clé d'hôte SSH existante.
show ssh-server	Affiche la taille de clé d'hôte.

set sshkey

Pour définir une clé SSH permettant un accès sans mot de passe, utilisez la commande **set sshkey**.

set sshkey [**none** | *user_ssh_key*]

Description de la syntaxe

none	(Facultatif) Saisir le mot clé **none** pour effacer la clé publique SSH de l'utilisateur.
user_ssh_key	(Facultatif) Saisir ou coller la clé SSH publique de l'utilisateur.

Modes de commande

Mode utilisateur local

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Si vous appuyez sur **Entrée** après avoir saisi **set sshkey**, vous êtes invité à fournir la clé SSH, une ligne à la fois. Saisissez ENDOFBUF pour terminer. Appuyez sur Ctrl-C pour abandonner.

Exemple

Cet exemple montre comment spécifier une clé SSH publique pour l'utilisateur local actuel :

```
FP9300-A /security/local-user # set sshkey
"ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAuo9VQ2CmWBI9/S1f30klCWjnV3lgdXMzO0WUl5iPw85lkdQqap+NFuNmHcb4K
iaQB8X/PDdmtlxQQcawclj+k8f4VcOelBxlsGk5luq5ls1ob1VOIEwcKEL/h5lrdbNlI8y3SS9I/gGiBZ9ARlop9LDpD
 m8HPh2LOgyH7Ei1MI8="
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

Commandes associées

Commande	Description
create local-user	Crée un compte d'utilisateur local.
set password	Spécifie un mot de passe pour un compte d'utilisateur.

set startup-version

Pour spécifier la version de démarrage d'une application, utilisez la commande **set startup-version** .

set startup-version

Description de la syntaxe

startup-version	Version du logiciel de démarrage d'une instance d'application

Modes de commande

scope ssa

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Si vous appuyez sur **Entrée** après **scope app-instance ftd ftd1** , vous êtes invité à définir la version de démarrage.

Exemple

Cet exemple montre comment définir la version de démarrage d'une application Cisco FTD :

```
FPR# scope ssa
FPR /ssa # scope slot 1
FPR /ssa/slot # scope app-instance ftd ftd1
FPR /ssa/slot/app-instance # set startup-version 6.6.1.91
Warning: Upgrade of ftd through FXOS is not supported. The specified version of ftd will
be installed. Please reinitialize or reinstall ftd.
```

set timezone

Pour définir le fuseau horaire dans FXOS, utilisez la commande **set timezone** .

set timezone

Description de la syntaxe

set timezone	Utilisez la commande set timezone pour définir le fuseau horaire dans FXOS.

Modes de commande

scope system/scope services

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour définir le fuseau horaire dans FXOS.

Exemple

Cet exemple montre comment définir le fuseau horaire dans FXOS :

```
firepower# scope system
firepower /system# scope services
firepower /system/services # set timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa            4) Arctic Ocean     7) Australia       10) Pacific Ocean
2) Americas          5) Asia             8) Europe
3) Antarctica        6) Atlantic Ocean   9) Indian Ocean


#? 8 <====== Europe


Please select a country.
 1) Aaland Islands        18) Greece               35) Norway
 2) Albania               19) Guernsey             36) Poland
 3) Andorra               20) Hungary              37) Portugal
 4) Austria               21) Ireland              38) Romania
 5) Belarus               22) Isle of Man          39) Russia
 6) Belgium               23) Italy                40) San Marino
 7) Bosnia & Herzegovina  24) Jersey               41) Serbia
 8) Britain (UK)          25) Latvia               42) Slovakia
 9) Bulgaria              26) Liechtenstein        43) Slovenia
10) Croatia               27) Lithuania            44) Spain
11) Czech Republic        28) Luxembourg           45) Sweden
12) Denmark               29) Macedonia            46) Switzerland
13) Estonia               30) Malta                47) Turkey
14) Finland               31) Moldova              48) Ukraine
15) France                32) Monaco               49) Vatican City
16) Germany               33) Montenegro
17) Gibraltar             34) Netherlands

#? 36 <======Poland

The following information has been given:
```

```
        Poland

Therefore timezone 'Europe/Warsaw' will be set.
Local time is now:      Sun Oct 24 08:51:04 CEST 2021.
Universal Time is now:  Sun Oct 24 06:51:04 UTC 2021.
Is the above information OK?
1) Yes
2) No


#? 1 <======== Yes

firepower /system/services* # commit
firepower /system/services # show timezone
Timezone: Europe/Warsaw <======= Timezone is set

To set the timezone to UTC:

firepower /system/services* # set timezone UTC
firepower /system/services* # commit
```

set trustpoint

Pour définir le point de confiance de certificat pour un trousseau de clés, utilisez la commande **set trustpoint**.

set trustpoint *trustpoint_name*

Description de la syntaxe

trustpoint_name	Nom d'un point de confiance défini. Ce nom peut comporter entre 1 et 32 caractères alphanumériques. Vous ne pouvez pas utiliser des espaces ni de caractères spéciaux autres que - (tiret), _ (trait de soulignement), : (deux-points) et . (point), et vous ne pouvez pas modifier ce nom après l'enregistrement de l'objet.

Modes de commande

scope security/scope keyring/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour spécifier le point de confiance qui a signé le certificat de ce trousseau de clés.

Exemple

Cet exemple montre comment renouveler les clés dans le trousseau de clés par défaut :

```
firepower# scope security
firepower /security # scope keyring test-ring
firepower /security/keyring # set trustpoint CiscoCA5
firepower /security/keyring* # commit-buffer
firepower /security/keyring #
```

Commande	Description
set cert	Permet d'accéder à un certificat RSA pour un trousseau de clés.
set modulus	Spécifie le module de clé RSA (longueur de clé SSL) en bits.
set regenerate	Renouvelle les clés RSA du trousseau de clés par défaut.

set use-2-factor

Pour activer et désactiver l'authentification à deux facteurs dans le domaine d'authentification, utilisez la commande **set use-2-factor**.

Remarque L'authentification à deux facteurs s'applique uniquement aux domaines RADIUS et TACACS+.

set use-2-factor {**no** | **yes**}

Description de la syntaxe

no	Désactive l'authentification à deux facteurs pour le domaine.
yes	Active l'authentification à deux facteurs pour le domaine.

Modes de commande

Mode d'authentification par défaut

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Si vous définissez l'authentification à deux facteurs pour un domaine RADIUS ou TACACS+, envisagez d'augmenter les périodes d'actualisation et d'expiration des sessions afin que les utilisateurs distants n'aient pas à se réauthentifier trop fréquemment.

Exemple

Cet exemple montre comment accéder au mode d'authentification par défaut et activer l'authentification à deux facteurs :

```
FP9300-A# scope security
FP9300-A /security # scope default-auth
FP9300-A /security/default-auth # set use-2-factor yes
FP9300-A /security/default-auth* # commit-buffer
FP9300-A /security/default-auth #
```

Commandes associées

Commande	Description
set authentication	Spécifie le service d'authentification par défaut.
set timeout values	Les commandes **set absolute-session-timeout**, **set con-absolute-session-timeout**, **set con-session-timeout** et **set session-timeout** permettent de définir diverses valeurs de délai d'expiration.

set user-account-unlock-time

Pour spécifier la durée pendant laquelle l'utilisateur reste bloqué du système après avoir atteint le nombre maximal de tentatives de connexion, utilisez la commande **set user-account-unlock-time**.

set user-account-unlock-time *unlock_time*

Description de la syntaxe

unlock_time	Durée en secondes pendant laquelle un utilisateur reste bloqué du système. La valeur peut varier de 600 à 36 000; la valeur par défaut est de 1 800 secondes (30 minutes).

Modes de commande

Mode sécurité

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Si un utilisateur (utilisateur administrateur compris) dépasse le nombre maximal de tentatives de connexion spécifié, il est bloqué du système et doit attendre le temps défini avant de pouvoir se reconnecter. Aucune notification ne s'affiche pour indiquer que l'utilisateur est verrouillé.

Exemple

Cet exemple montre comment accéder au mode sécurité et définir le temps qui doit s'écouler avant qu'un utilisateur déconnecté puisse se reconnecter :

```
FP9300-A # scope security
FP9300-A /security # set user-account-unlock-time 900
FP9300-A /security* # commit-buffer
FP9300-A /security #
```

Commandes associées

Commande	Description
clear lock-status	Déverrouille le blocage d'un utilisateur.
set max-login-attempts	Spécifie le nombre maximal de tentatives de connexion infructueuses avant qu'un utilisateur ne soit bloqué du système.

set user-label

Pour attribuer un identifiant défini par l'utilisateur au châssis de l'appareil, utilisez la commande **set user-label** en mode `chassis/`.

Pour attribuer un identifiant défini par l'utilisateur à l'un des serveurs installés, utilisez la commande **set user-label** en mode `server/`.

set user-label *user_label*

Description de la syntaxe

user_label	Étiquette que vous souhaitez affecter à l'appareil ou au serveur; 32 caractères maximum.

Modes de commande

scope chassis/

scope chassis/scope server

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous pouvez utiliser la commande **show detail** en mode `chassis/` pour afficher l'étiquette d'utilisateur actuellement affectée au châssis.

Vous pouvez utiliser la commande **show detail** en mode `chassis/server/` pour afficher l'étiquette d'utilisateur actuellement affectée au serveur connecté.

Exemple

Cet exemple montre comment affecter une étiquette définie par l'utilisateur au châssis de l'appareil :

```
firepower # scope chassis 1
firepower /chassis # set user-label FP9300-4
firepower /chassis* # commit-buffer
firepower /chassis # show detail

Chassis:
    Chassis: 1
    User Label: FP9300-4
    Overall Status: Operable
    Oper qualifier: N/A
    Operability: Operable
    Conf State: Ok
    Admin State: Acknowledged
    Conn Path: A
    Conn Status: A
    Managing Instance: A
    Product Name: Cisco Firepower 9300 Security Appliance AC
    PID: FPR-C9300-AC
    VID: V02
    Part Number: 68-100280-04
    Vendor: Cisco Systems Inc
    Model: FPR-C9300-AC
    Serial (SN): JMX1950196H
    HW Revision: 0
```

```
    Mfg Date: 2015-12-16T00:00:00.000
    Power State: Ok
    Thermal Status: Ok
    SEEPROM operability status: Operable
    Dynamic Reallocation: Chassis
    Reserved Power Budget (W): 600
    PSU Capacity (W): 0
    PSU Line Mode: High Line
    PSU State: Ok
    Current Task:
firepower /chassis #
```

Commandes associées

Commande	Description
show detail	En mode `chassis/`, affiche des informations détaillées sur le châssis, notamment l'étiquette d'utilisateur actuelle du châssis. En mode `chassis/server/`, affiche des informations détaillées sur le serveur, notamment l'étiquette d'utilisateur du serveur connecté.

set value (create bootstrap-key FIREWALL_MODE)

Pour définir le mode pare-feu routé ou transparent dans la configuration de démarrage de Défense contre les menaces et ASA, utilisez la commande **set value**.

set value {**routed** | **transparent**}

Description de la syntaxe

routed	Définit le mode pare-feu sur le mode pare-feu routé.
transparent	Définit le mode pare-feu sur pare-feu transparent :

Modes de commande

scope ssa/create logical-device/create mgmt-bootstrap/create bootstrap-key FIREWALL_MODE/

Commande par défaut

Le mode par défaut est le mode routé.

Historique des commandes

Version	Modification
2.4(1)	Ajout de prise en charge pour ASA.
1.1(4)	Commande ajoutée pour Cisco FTD.

Instructions d'utilisation

Les paramètres de démarrage sont uniquement destinés au déploiement initial ou à la reprise sur sinistre. Pour un fonctionnement normal, vous pouvez modifier la plupart des valeurs dans la configuration de l'interface de ligne de commande de l'application.

Exemple

L'exemple suivant montre comment définir le mode sur le mode routé :

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
firepower /ssa/logical-device/mgmt-bootstrap* #
```

Commandes associées

Commande	Description
create bootstrap-key FIREWALL_MODE	Définit le mode pare-feu pour l'application.
create logical-device	Crée le périphérique logique.
create mgmt-bootstrap	Crée la configuration de démarrage de l'application.

set value (create bootstrap-key MANAGEMENT_TYPE)

Pour spécifier le gestionnaire, FMC ou FDM, dans la configuration de démarrage de Défense contre les menaces, utilisez la commande **set value**.

set value {**FMC** | **LOCALLY_MANAGED**}

Description de la syntaxe

FMC	Configure le gestionnaire sur FDM.
LOCALLY_MANAGED	Configure le gestionnaire sur FMC.

Modes de commande

scope ssa/create logical-device/create mgmt-bootstrap/create bootstrap-key LOCALLY_MANAGED/

Commande par défaut

Le gestionnaire par défaut est FMC.

Historique des commandes

Version	Modification
2.7(1)	Commande ajoutée pour Cisco FTD.

Instructions d'utilisation

Les paramètres de démarrage sont uniquement destinés au déploiement initial ou à la reprise sur sinistre. Pour un fonctionnement normal, vous pouvez modifier la plupart des valeurs dans la configuration de l'interface de ligne de commande de l'application.

Exemple

L'exemple suivant montre comment définir le gestionnaire sur FDM :

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key MANAGEMENT_TYPE
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value LOCALLY_MANAGED
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
firepower /ssa/logical-device/mgmt-bootstrap* #
```

Commandes associées

Commande	Description
create bootstrap-key FIREWALL_MODE	Définit le mode pare-feu pour l'application.
create logical-device	Crée le périphérique logique.
create mgmt-bootstrap	Crée la configuration de démarrage de l'application.

set value (create bootstrap-key PERMIT_EXPERT_MODE)

Pour autoriser le mode expert des sessions FTD SSH pour Défense contre les menaces, utilisez la commande **set value**.

set value {**yes** | **no**}

Description de la syntaxe

no	Interdit le mode expert depuis une session SSH vers Défense contre les menaces.
yes	Autorise le mode expert depuis une session SSH vers Défense contre les menaces.

Modes de commande

scope ssa/create logical-device/create mgmt-bootstrap/create bootstrap-key PERMIT_EXPERT_MODE/

Commande par défaut

La valeur par défaut est « no » (non).

Historique des commandes

Version	Modification
2.4(1)	Commande ajoutée.

Instructions d'utilisation

Le mode expert fournit à Cisco FTD un accès au shell pour un dépannage avancé. Par défaut, pour les instances de contenant, le mode expert n'est disponible que pour les utilisateurs qui accèdent à l'interface de ligne de commande Cisco FTD à partir de l'interface de ligne de commande FXOS. Cette limitation est uniquement appliquée aux instances de conteneur pour augmenter l'isolement entre les instances. Utilisez le mode expert uniquement si une procédure documentée vous indique que c'est nécessaire ou si le Centre d'assistance technique (TAC) de Cisco vous demande de l'utiliser. Pour accéder à ce mode, utilisez la commande expert dans l'interface de ligne de commande Cisco FTD.

Exemple

L'exemple suivant montre comment activer le mode expert à partir de SSH :

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key PERMIT_EXPERT_MODE
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value yes
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
firepower /ssa/logical-device/mgmt-bootstrap* #
```

Commandes associées

Commande	Description
create bootstrap-key FIREWALL_MODE	Définit le mode pare-feu pour l'application.
create logical-device	Crée le périphérique logique.
create mgmt-bootstrap	Crée la configuration de démarrage de l'application.

set vlan

Pour définir l'ID de VLAN d'une sous-interface à utiliser avec les instances de contenant, utilisez la commande **set vlan**.

set vlan *ID*

Description de la syntaxe

ID	Définit l'ID de VLAN entre 1 et 4095.

Modes de commande

scope eth-uplink/scope fabric a/scope interface/create subinterface/

scope eth-uplink/scope fabric a/create port-channel/create subinterface/

Historique des commandes

Version	Modification
2.4(1)	Commande ajoutée.

Instructions d'utilisation

Vous pouvez ajouter entre 250 et 500 sous-interfaces VLAN au châssis, selon votre déploiement réseau.

Les ID de VLAN par interface doivent être uniques et, dans une instance de conteneur, les ID de VLAN doivent être uniques pour toutes les interfaces attribuées. Vous pouvez réutiliser les ID de VLAN sur des interfaces *distinctes*, à condition qu'ils soient affectés à différentes instances de conteneur. Cependant, chaque sous-interface compte toujours dans la limite, même si elle utilise le même ID.

Exemple

Dans l'exemple suivant, trois sous-interfaces Ethernet 1/1 sont créées et sont définies comme interfaces de partage de données.

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # scope interface Ethernet1/1
firepower /eth-uplink/fabric/interface # create subinterface 10
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 10
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # exit
firepower /eth-uplink/fabric/interface # create subinterface 11
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 11
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # exit
firepower /eth-uplink/fabric/interface # create subinterface 12
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 12
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # commit-buffer
firepower /eth-uplink/fabric/interface/subinterface #
```

Commandes associées

Commande	Description
create port-channel	Crée un EtherChannel (canal de port).
create subinterface	Ajoute une sous-interface.

Commande	Description
scope interface	Permet d'accéder à l'objet d'interface physique.
set port-type	Définit le type d'interface.

Commandes sh

- show, à la page 395
- show aggr-interface expand, à la page 396
- show app, à la page 400
- show (app-instance), à la page 406
- show audit-logs, à la page 409
- show auth-domain, à la page 410
- show auth-realm fsm status, à la page 411
- show authentication, à la page 413
- show breakout, à la page 414
- show callhome, à la page 415
- show (card), à la page 416
- show card detail, à la page 418
- show cc-mode, à la page 421
- show certreq, à la page 422
- show cfg-export-policy, à la page 424
- show chassis, à la page 426
- show cli, à la page 428
- show clock, à la page 429
- show cloud-connector, à la page 430
- show configuration, à la page 431
- show connection, à la page 432
- show console-auth, à la page 433
- show controller fsm status, à la page 434
- show core-export-target, à la page 436
- show cores-detail, à la page 438
- show cpu, à la page 439
- show default-auth detail, à la page 441
- show domain-env-feature, à la page 442
- show domain-name, à la page 444
- show domain-nw-feature, à la page 445
- show domain-server-feature, à la page 446
- show domain-storage-feature, à la page 447
- show dns, à la page 448

- show download-task, à la page 449
- show enforce-strong-password, à la page 451
- show environment, à la page 452
- show eth-uplink, à la page 488
- show event, à la page 490
- show export-config detail, à la page 491
- show fabric, à la page 492
- show fabric-interconnect, à la page 493
- show fan-module, à la page 495
- show fault, à la page 497
- show fc, à la page 499
- show fips-mode, à la page 501
- show firmware, à la page 502
- show (firmware-install), à la page 504
- show filter expand detail, à la page 506
- show flexflash-controller, à la page 508
- show fsm status, à la page 509
- show fw-infra-pack, à la page 511
- show hardware-bypass-ports, à la page 513
- show health-led, à la page 514
- show https, à la page 515
- show hw-crypto, à la page 516
- show image, à la page 517
- show image detail, à la page 520
- show import-config detail, à la page 521
- show identity, à la page 522
- show interface (afficher l'interface), à la page 526
- show interface counter errors (connect fxos), à la page 529
- show interface transceiver (connect fxos), à la page 536
- show interface brief (connect fxos), à la page 537
- show inventory, à la page 549
- show inventory (connect fxos), à la page 553
- show ip-block, à la page 554
- show ip-pool, à la page 556
- show ipsec-log, à la page 558
- show ipv6-block, à la page 560
- show ipv6-if, à la page 562
- show keyring, à la page 563
- show lacp (connect fxos), à la page 565
- show license, à la page 570
- show load-stats, à la page 572
- show local-user, à la page 573
- show local-user tech-support, à la page 574
- show logical-device, à la page 575
- show logical-device-template, à la page 577
- show mac-address, à la page 579

- show mgmt-iface in-band expand detail, à la page 581
- show member-port, à la page 582
- show mac-pool, à la page 584
- show memory, à la page 586
- show (management interface), à la page 589
- show mgmt-port, à la page 590
- show monitor, à la page 591
- show nfs-mount-def, à la page 593
- show nm-fpga-version, à la page 595
- show ntp-overall-status, à la page 596
- show ntp server, à la page 597
- show nw-ctrl-policy, à la page 598
- show org, à la page 600
- show package, à la page 601
- show password-profile, à la page 603
- show pki fsm status, à la page 604
- show pmon state, à la page 606
- show post, à la page 607
- show pre-login-banner, à la page 608
- show provider-load-stats, à la page 609
- show port-channel (connect fxos), à la page 611
- show port-channel (scope fabric), à la page 614
- show power-control-policy, à la page 616
- show psu, à la page 618
- show psu-policy, à la page 620
- show registry-repository, à la page 621
- show remote-user, à la page 622
- show resource, à la page 623
- show resource-profile, à la page 625
- show role, à la page 627
- show (scope fabric), à la page 628
- show schedule infra-fw, à la page 629
- show security, à la page 631
- show sel, à la page 632
- show server actual-boot-order, à la page 633
- show server adapter, à la page 634
- show server assoc, à la page 636
- show server bios, à la page 637
- show server boot-order, à la page 639
- show server cpu, à la page 641
- show server decommissioned, à la page 642
- show server detail, à la page 643
- show server environment, à la page 647
- show server firmware, à la page 649
- show server fsm status, à la page 651
- show server identity, à la page 653

- show server inventory, à la page 655
- show server memory, à la page 657
- show server status, à la page 659
- show server storage, à la page 660
- show server version, à la page 662
- show service-profile, à la page 664
- show session expand detail, à la page 670
- show shell-session-limits, à la page 671
- show (slot), à la page 672
- show slot, à la page 674
- show snmp (connect fxos), à la page 678
- show snmp (monitoring), à la page 682
- show snmp-trap, à la page 683
- show snmp-user, à la page 685
- show ssh-server, à la page 687
- show stats, à la page 688
- show storage, à la page 690
- show subinterface, à la page 691
- show sup, à la page 693
- show system, à la page 694
- show system reset-reason, à la page 696
- show stats system-stats, à la page 697
- show system uptime (connect fxos), à la page 699
- show tech-support, à la page 700
- show timezone, à la page 705
- show trustpoint, à la page 706
- show user-sessions, à la page 708
- show validate-task, à la page 710
- show version, à la page 712
- shutdown, à la page 715
- show web-session-limits, à la page 716

show

Pour afficher des informations sur les opérations et la configuration actuelle dans différents modes de commande, utilisez la commande **show**.

La plupart des modes de commande FXOS CLI fournissent une commande générale **show** qui affiche diverses informations pertinentes pour le mode de commande actuel. Par exemple, utilisez la commande **show** en mode logement (scope ssa/scope slot) pour afficher les informations SSP actuelles.

Nombre de ces commandes ne sont pas explicitement documentées dans ce guide. Utilisez **show ?** pour afficher les options **show** disponibles pour le mode de commande actuel.

show aggr-interface expand

Pour afficher des informations détaillées sur aggr-interface, utilisez la commande **show aggr-interface detail**.

show aggr-interface [**detail** | **expand**]

Description de la syntaxe

detail	Affiche les informations détaillées sur la configuration d'exportation.
expand	(Facultatif) Affiche des informations développées pour aggr-interface

Modes de commande

scope eth-uplink/fabric a

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope eth-uplink/ fabric a.

Exemple

Cet exemple affiche des informations sur aggr-interface.

```
Firepower# scope eth-uplink
Firepower /eth-uplink # scope fabric a
Firepower /eth-uplink/fabric # show aggr-interface expand detail
Aggregate Interface:
    Port Name: Ethernet2/1
    Config State: Disabled

    Interface:
        Port Name: Ethernet2/1/1
        User Label:
        Port Type: Data
        Admin State: Disabled
        Oper State: Sfp Not Present
        State Reason: Unknown
        flow control policy: default
        Admin Speed: 10 Gbps
        Oper Speed: 10 Gbps
        Ethernet Link Profile name: default
        Oper Ethernet Link Profile name: fabric/lan/eth-link-prof-default
        Udld Oper State: Unknown
        Inline Pair Admin State: Enabled
        Inline Pair Peer Port Name:
        Service State: Enabled
        Last Service State Down Reason: None
        Allowed Vlan: All
        Network Control Policy: default
        Current Task:

        Port Name: Ethernet2/1/2
        User Label:
        Port Type: Data
        Admin State: Disabled
        Oper State: Sfp Not Present
```

```
        State Reason: Unknown
        flow control policy: default
        Admin Speed: 10 Gbps
        Oper Speed: 10 Gbps
        Ethernet Link Profile name: default
        Oper Ethernet Link Profile name: fabric/lan/eth-link-prof-default
        Udld Oper State: Unknown
        Inline Pair Admin State: Enabled
        Inline Pair Peer Port Name:
        Service State: Enabled
        Last Service State Down Reason: None
        Allowed Vlan: All
        Network Control Policy: default
        Current Task:

        Port Name: Ethernet2/1/3
        User Label:
        Port Type: Data
        Admin State: Disabled
        Oper State: Sfp Not Present
        State Reason: Unknown
        flow control policy: default
        Admin Speed: 10 Gbps
        Oper Speed: 10 Gbps
        Ethernet Link Profile name: default
        Oper Ethernet Link Profile name: fabric/lan/eth-link-prof-default
        Udld Oper State: Unknown
        Inline Pair Admin State: Enabled
        Inline Pair Peer Port Name:
        Service State: Enabled
        Last Service State Down Reason: None
        Allowed Vlan: All
        Network Control Policy: default
        Current Task:

        Port Name: Ethernet2/1/4
        User Label:
        Port Type: Data
        Admin State: Disabled
        Oper State: Sfp Not Present
        State Reason: Unknown
        flow control policy: default
        Admin Speed: 10 Gbps
        Oper Speed: 10 Gbps
        Ethernet Link Profile name: default
        Oper Ethernet Link Profile name: fabric/lan/eth-link-prof-default
        Udld Oper State: Unknown
        Inline Pair Admin State: Enabled
        Inline Pair Peer Port Name:
        Service State: Enabled
        Last Service State Down Reason: None
        Allowed Vlan: All
        Network Control Policy: default
        Current Task:

Port Name: Ethernet2/3
Config State: Disabled

Interface:
        Port Name: Ethernet2/3/1
        User Label:
        Port Type: Data
        Admin State: Disabled
        Oper State: Admin Down
```

```
State Reason: Administratively down
flow control policy: default
Admin Speed: 10 Gbps
Oper Speed: 10 Gbps
Ethernet Link Profile name: default
Oper Ethernet Link Profile name: fabric/lan/eth-link-prof-default
Udld Oper State: Admin Disabled
Inline Pair Admin State: Enabled
Inline Pair Peer Port Name:
Service State: Enabled
Last Service State Down Reason: None
Allowed Vlan: All
Network Control Policy: default
Current Task:

Port Name: Ethernet2/3/2
User Label:
Port Type: Data
Admin State: Disabled
Oper State: Admin Down
State Reason: Administratively down
flow control policy: default
Admin Speed: 10 Gbps
Oper Speed: 10 Gbps
Ethernet Link Profile name: default
Oper Ethernet Link Profile name: fabric/lan/eth-link-prof-default
Udld Oper State: Admin Disabled
Inline Pair Admin State: Enabled
Inline Pair Peer Port Name:
Service State: Enabled
Last Service State Down Reason: None
Allowed Vlan: All
Network Control Policy: default
Current Task:

Port Name: Ethernet2/3/3
User Label:
Port Type: Data
Admin State: Disabled
Oper State: Admin Down
State Reason: Administratively down
flow control policy: default
Admin Speed: 10 Gbps
Oper Speed: 10 Gbps
Ethernet Link Profile name: default
Oper Ethernet Link Profile name: fabric/lan/eth-link-prof-default
Udld Oper State: Admin Disabled
Inline Pair Admin State: Enabled
Inline Pair Peer Port Name:
Service State: Enabled
Last Service State Down Reason: None
Allowed Vlan: All
Network Control Policy: default
Current Task:

Port Name: Ethernet2/3/4
User Label:
Port Type: Data
Admin State: Disabled
Oper State: Admin Down
State Reason: Administratively down
flow control policy: default
Admin Speed: 10 Gbps
Oper Speed: 10 Gbps
```

```
Ethernet Link Profile name: default
Oper Ethernet Link Profile name: fabric/lan/eth-link-prof-default
Udld Oper State: Admin Disabled
Inline Pair Admin State: Enabled
Inline Pair Peer Port Name:
Service State: Enabled
Last Service State Down Reason: None
Allowed Vlan: All
Network Control Policy: default
Current Task:
```

Utilisez la commande suivante pour configurer le type de port de l'interface.

```
Firepower# scope cabling
Firepower /cabling # scope fabric a
Firepower /cabling/fabric # create breakout 2 3
Warning: This action will reboot the system and any existing configurations on 40G port
will be erased.!
Firepower /cabling/fabric/breakout* # commit-buffer
Firepower /cabling/fabric/breakout # connect local-mgmt
Firepower(local-mgmt)# reboot
```

show app

Pour afficher la liste des applications de démarrage disponibles sur le système, comme ASA et Cisco FTD, utilisez la commande **show app**.

.

show app [**detail**]

Description de la syntaxe

Detail	Affiche la liste des informations détaillées sur les applications.

Modes de commande

scope ssa

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope ssa.

Exemple

Cet exemple montre comment afficher des informations sur toutes les applications de démarrage :

```
Firepower /fabric-interconnect # scope ssa
Firepower /ssa # show app

  Name       Version         Author     Supported Deploy Types CSP Type    Is
Default App
    ---------- --------------- ---------- ---------------------- ----------- ---
-----------
    asa        99.18.20.36     cisco      Native           Application Yes
    ftd        7.2.0.1784      cisco      Native, Container  Application  No
    ftd        7.2.0.83      cisco      Native, Container  Application No
    ftd        7.3.0.1258      cisco      Native, Container  Application No
    ftd        7.3.0.1402      cisco      Native, Container  Application Yes
                   In Cluster      Data Node
```

Exemple

Cet exemple montre comment afficher des informations sur toutes les applications disponibles :

```
firepower /ssa # show app detail
        Application:
Name: asa
    Version: 99.18.20.36
    Author: cisco
    Supported Deploy Types: Native
    Is Default App: Yes
    CSP Type: Application
    Is Decorator: No
    Has License Agreement: No
    License Agreement has been Accepted: No
    Time Stamp: 2012-01-27T11:34:37.000
```

```
Validation State: None
Validation Time Stamp: Never
Application Information:
    Deploy Type: Native
    Description: N/A
    Build Date: 12/16/2021
    Min OS: 92.12.0.122
    Data VNIC NR: 0
    Mgmt VNIC NR: 0
    Security Control: No
    Support Aggregated VNIC: No
    Can Upgrade: Yes
    Full Install: Yes
    Can Downgrade: Yes
    Is Secondary Data Disk Supported: No
    Installation Timeout (sec): 240
    Uninstallation Timeout (sec): 240
    Upgrade Timeout (sec): 360
    Recommended Data Disk (MB): 20481
    Recommended Cpu Cores: 0
    Recommended Ram (MB): 0
    Minimum Required Data Disk (MB): 20481
    Minimum Required Cpu Logical Cores: 16
    Minimum Required Ram (MB): 24576
    Required Binary Disk (MB): 171
    Net Management Bootstrap Type: Appagent
    Is App Agent Supported: Yes
    Is Clustering Supported: Yes
    Is Turbo Mode Supported: No
    Aggregator: Full
    Incompatible Apps: ftd
    Support Customized CCL IP Subnet: Yes
    Max Application Instance Count: 1
    Reboot Module On App Restart: Yes
    Hardware Crypto Version: Unsupported
Name: ftd
Version: 7.2.0.1784
Author: cisco
Supported Deploy Types: Native,Container
Is Default App: No
CSP Type: Application
Is Decorator: No
Has License Agreement: Yes
License Agreement has been Accepted: No
Time Stamp: 2012-01-26T11:16:15.000
Validation State: None
Validation Time Stamp: Never
Application Information:
    Deploy Type: Native
    Description: N/A
    Build Date: 02/28/2022
    Min OS: 92.12.0.122
    Data VNIC NR: 0
    Mgmt VNIC NR: 0
    Security Control: No
    Support Aggregated VNIC: No
    Can Upgrade: No
    Full Install: Yes
    Can Downgrade: No
    Is Secondary Data Disk Supported: Yes
    Installation Timeout (sec): 1800
    Uninstallation Timeout (sec): 600
    Upgrade Timeout (sec): 1800
    Recommended Data Disk (MB): 195313
```

```
        Recommended Secondary Disk (MB): 0
        Recommended Cpu Cores: 0
        Recommended Ram (MB): 0
        Minimum Required Data Disk (MB): 39063
        Minimum Required Secondary Disk (MB): 0
        Minimum Required Cpu Logical Cores: 4
        Minimum Required Ram (MB): 10
        Required Binary Disk (MB): 3907
        Net Management Bootstrap Type: Appagent
        Is App Agent Supported: Yes
        Is Clustering Supported: Yes
        Is Turbo Mode Supported: No
        Aggregator: Full
        Incompatible Apps: asa
        Support Customized CCL IP Subnet: Yes
        Max Application Instance Count: 1
        Reboot Module On App Restart: Yes
        Hardware Crypto Version: Unsupported
        Deploy Type: Container
        Description: N/A
        Build Date: 02/28/2022
        Min OS: 92.12.0.122
        Data VNIC NR: 0
        Mgmt VNIC NR: 0
        Security Control: No
        Support Aggregated VNIC: No
        Can Upgrade: No
        Full Install: Yes
        Can Downgrade: No
        Is Secondary Data Disk Supported: Yes
        Installation Timeout (sec): 1800
        Uninstallation Timeout (sec): 600
        Upgrade Timeout (sec): 1800
        Recommended Data Disk (MB): 40960
        Recommended Secondary Disk (MB): 102400
        Recommended Cpu Cores: 10
        Recommended Ram (MB): 32768
        Minimum Required Data Disk (MB): 40960
        Minimum Required Secondary Disk (MB): 0
        Minimum Required Cpu Logical Cores: 6
        Minimum Required Ram (MB): 10
        Required Binary Disk (MB): 3907
        Net Management Bootstrap Type: Appagent
        Is App Agent Supported: Yes
        Is Clustering Supported: Yes
        Is Turbo Mode Supported: No
        Aggregator: Full
        Incompatible Apps: asa
        Support Customized CCL IP Subnet: No
        Max Application Instance Count: 0
        Reboot Module On App Restart: No
        Hardware Crypto Version: 2
    Name: ftd
    Version: 7.2.0.83
    Author: cisco
    Supported Deploy Types: Native,Container
    Is Default App: No
    CSP Type: Application
    Is Decorator: No
    Has License Agreement: Yes
    License Agreement has been Accepted: No
    Time Stamp: 2012-01-22T07:04:58.000
    Validation State: None
    Validation Time Stamp: Never
```

Exemple

Cet exemple montre comment afficher des informations détaillées sur toutes les applications disponibles :

```
Firepower /ssa # show app expand detail
 Application:
    Application:

    Name: asa
    Version: 99.18.20.36
    Author: cisco
    Supported Deploy Types: Native
    Is Default App: Yes
    CSP Type: Application
    Is Decorator: No
    Has License Agreement: No
    License Agreement has been Accepted: No
    Time Stamp: 2012-01-27T11:34:37.000
    Validation State: None
    Validation Time Stamp: Never
    Application Information:
        Deploy Type: Native
        Description: N/A
        Build Date: 12/16/2021
        Min OS: 92.12.0.122
        Data VNIC NR: 0
        Mgmt VNIC NR: 0
        Security Control: No
        Support Aggregated VNIC: No
        Can Upgrade: Yes
        Full Install: Yes
        Can Downgrade: Yes
        Is Secondary Data Disk Supported: No
        Installation Timeout (sec): 240
        Uninstallation Timeout (sec): 240
        Upgrade Timeout (sec): 360
        Recommended Data Disk (MB): 20481
        Recommended Cpu Cores: 0
        Recommended Ram (MB): 0
        Minimum Required Data Disk (MB): 20481
        Minimum Required Cpu Logical Cores: 16
        Minimum Required Ram (MB): 24576
        Required Binary Disk (MB): 171
        Net Management Bootstrap Type: Appagent
        Is App Agent Supported: Yes
        Is Clustering Supported: Yes
        Is Turbo Mode Supported: No
        Aggregator: Full
        Incompatible Apps: ftd
        Support Customized CCL IP Subnet: Yes
        Max Application Instance Count: 1
        Reboot Module On App Restart: Yes
        Hardware Crypto Version: Unsupported
        App Attribute Key for the Application:
            App Attribute Key: cluster-role
            Description: This is the role of the blade in the cluster
            App Attribute Key: mgmt-ip
            Description: This is the IP for the management interface
            App Attribute Key: mgmt-ip-virtual
            Description: This is the Virtual IP for cluster only
            App Attribute Key: mgmt-ipv6
            Description: This is the IPv6 for the management interface
```

```
            App Attribute Key: mgmt-ipv6-virtual
            Description: This is the Virtual IPv6 for cluster only
            App Attribute Key: mgmt-url
            Description: This is the management URL for this application
            App Attribute Key: mgmt-url-ipv6
            Description: This is the management IPv6 URL for this application
        Net Mgmt Bootstrap Key for the Application:
            Bootstrap Key: FIREWALL_MODE
            Key Data Type: enum:(routed, transparent)
            Mandatory: No
            Is the Key Secret: No
            Description: This is the mode to set the firewall (transparent routed)
            Key scope: Global
            Bootstrap Key: PASSWORD
            Key Data Type: string
            Mandatory: No
            Is the Key Secret: Yes
            Description: The admin user password.
            Key scope: Global
        Port Requirement for the Application:
            Port Type: Data
            Max Ports: 120
            Min Ports: 1
            Interchassis Supported Port Types: PORT_CHANNEL
            Port Type: Mgmt
            Max Ports: 1
            Min Ports: 0
            Interchassis Supported Port Types:
            Port Type: Cluster
            Max Ports: 1
            Min Ports: 0
            Interchassis Supported Port Types:

    Name: ftd
    Version: 7.3.0.1258
    Author: cisco
    Supported Deploy Types: Native,Container
    Is Default App: No
    CSP Type: Application
    Is Decorator: No
    Has License Agreement: Yes
    License Agreement has been Accepted: No
    Time Stamp: 2012-03-18T13:06:33.000
    Validation State: None
    Validation Time Stamp: Never
    Application Information:
        Deploy Type: Native
        Description: N/A
        Build Date: 04/19/2022
        Min OS: 92.13.0.100
        Data VNIC NR: 0
        Mgmt VNIC NR: 0
        Security Control: No
        Support Aggregated VNIC: No
        Can Upgrade: No
        Full Install: Yes
        Can Downgrade: No
        Is Secondary Data Disk Supported: Yes
        Installation Timeout (sec): 1800
        Uninstallation Timeout (sec): 600
        Upgrade Timeout (sec): 1800
        Recommended Data Disk (MB): 195313
        Recommended Secondary Disk (MB): 0
        Recommended Cpu Cores: 0
```

```
        Recommended Ram (MB): 0
        Minimum Required Data Disk (MB): 39063
        Minimum Required Secondary Disk (MB): 0
        Minimum Required Cpu Logical Cores: 4
        Minimum Required Ram (MB): 10
        Required Binary Disk (MB): 3907
        Net Management Bootstrap Type: Appagent
        Is App Agent Supported: Yes
        Is Clustering Supported: Yes
        Is Turbo Mode Supported: No
        Aggregator: Full
        Incompatible Apps: asa
        Support Customized CCL IP Subnet: Yes
        Max Application Instance Count: 1
        Reboot Module On App Restart: Yes
        Hardware Crypto Version: Unsupported
        App Attribute Key for the Application:
            App Attribute Key: cluster-role
            Description: This is the cluster role for this application instance
            App Attribute Key: firepower-mgmt-ip
            Description: This is the IP address used to initialize a tunnel with
 Firepower Management Center
            App Attribute Key: firepower-mgmt-ipv6
            Description: This is the IPv6 address used to initialize a tunnel wi
th Firepower Management Center
            App Attribute Key: mgmt-url
            Description: This is the management URL for Firepower Management Cen
ter
            App Attribute Key: NAT_ID
            Description: This is the token used to associate with Firepower Mana
gement Center
        Net Mgmt Bootstrap Key for the Application:
            Bootstrap Key: DNS_SERVERS
            Key Data Type: string
            Mandatory: No
            Is the Key Secret: No
            Description: Comma-separated DNS servers for the application
            Key scope: Global
            Bootstrap Key: FIREPOWER_MANAGER_IP
            Key Data Type: string
            Mandatory: No
            Is the Key Secret: No
            Description: The IP address of Cisco Firepower Management Center
            Key scope: Global
```

show (app-instance)

Pour afficher les informations actuelles sur l'application, utilisez la commande **show** en mode instance d'application.

show [**app** | **app-attri** | **detail** | **event** | **expand** | **fault** | **fsm** | **heartbeat** | **hotfix** | **resource**]

Description de la syntaxe

app	(Facultatif) Affiche la liste des packages d'applications, tels que ASA ou Cisco FTD, disponibles pour l'installation (lame).
app-attri	(Facultatif) Affiche les attributs d'application actuels.
detail	(Facultatif) Affiche les informations détaillées sur l'instance d'application actuelle. Ce mot clé est également disponible avec de nombreuses autres options de commande pour afficher les informations détaillées sur l'option spécifiée.
event	(Facultatif) Affiche les informations sur la gestion des événements pour l'application.
expand	(Facultatif) Affiche les informations développées pour l'instance d'application actuelle. Ce mot clé est également disponible avec de nombreuses autres options de commande pour afficher les informations développées sur l'option spécifiée.
fault	(Facultatif) Affiche les informations sur les défaillances qui se sont produites dans cette instance d'application. Les options suivantes sont également disponibles : • *fault_ID* : affiche les informations pour la défaillance spécifiée. • **cause** : affiche les informations pour le type de cause spécifié uniquement. • **detail** : affiche les informations détaillées sur la défaillance. • **severity** : affiche les informations pour le niveau de gravité spécifié uniquement. • **suppressed** : répertorie les défaillances supprimées. Les mots clés **cause**, **detail** et **severity** sont disponibles avec cette option.
fsm { **status** | **task** }	(Facultatif) Affiche les informations sur la machine à états finis (FSM) de l'application actuelle, selon le mot clé spécifié : • **status** : affiche les informations sur l'état du FSM. • **task** : affiche les informations sur les tâches du FSM.
heartbeat	(Facultatif) Affiche les informations sur la dernière pulsation reçue.

hotfix	(Facultatif) Affiche les informations sur les correctifs appliqués. Les options suivantes sont également disponibles avec ce mot clé : **detail**, **expand** et *version* que vous pouvez utiliser pour afficher les informations sur un correctif spécifique.
resource	(Facultatif) Affiche les informations sur les allocations de ressources actuelles.

Modes de commande

scope ssa/scope slot

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.
2.13(0)	Le rôle de grappe est passé de maître/esclave à nœud de contrôle/nœud de données.

Instructions d'utilisation

Par défaut, cette commande affiche les informations générales sur la configuration de l'instance d'application.

Exemple

Cet exemple montre comment afficher les informations générales sur l'instance d'application :

```
firepower# scope ssa
firepower /ssa # scope slot 2
firepower /ssa/slot # scope app-instance asa cluster1
firepower /ssa/slot/app-instance # show

Application Instance:
    App Name   Identifier Admin State Oper State       Running Version Startup Version
Deploy Type Profile Name Cluster State   Cluster Role
    ---------- ---------- ----------- ---------------- --------------- ---------------
----------- ------------ --------------- ------------
    asa        cluster1   Enabled     Online           201.2.1.125     201.2.1.125
Native                    In Cluster      Data Node
```

Exemple

Cet exemple montre comment afficher les informations générales sur les applications disponibles pour l'installation :

```
firepower# scope ssa
firepower# show app
firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is Default App

    ---------- --------------- ---------- ---------------------- ----------- --------------

    asa        9.12.3.12       cisco      Native                 Application No
    asa        9.12.3.140      cisco      Native                 Application No
    asa        9.12.3.9        cisco      Native                 Application No
    asa        9.14.1.150      cisco      Native                 Application No
    asa        9.16.2.3        cisco      Native                 Application Yes
    asa        9.9.2           cisco      Native                 Application No
    ftd        6.4.0.102       cisco      Native,Container       Application No
    ftd        6.5.0.115       cisco      Native,Container       Application No
```

```
ftd         6.6.1.91         cisco      Native,Container       Application No
ftd         6.6.4.59         cisco      Native,Container       Application Yes
ftd         6.7.0.65         cisco      Native,Container       Application No
ftd         7.0.0.94         cisco      Native,Container       Application No
```

Commandes associées

Commande	Description
scope app-instance	Permet d'accéder au mode instance d'application pour une application spécifique.
show slot	Affiche les informations de configuration générales pour un module SSP spécifique.

show audit-logs

Pour afficher les journaux d'audit des utilisateurs, utilisez la commande **show audit-logs** .

show audit-logs

Modes de commande

scope security

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande affiche les informations sur les journaux d'audit des utilisateurs.

Exemple

Cet exemple affiche les informations sur les journaux d'audit des utilisateurs :

```
firepower# scope security
firepower # /security # show audit-logs
Audit trail logs:
    Creation Time        User       ID       Action           Description
    -------------------- ---------- -------- ---------------- -----------
    2021-10-11T21:42:30.885
                         admin      18405523 Creation         PreLoginBanner created
    2021-10-11T21:41:07.340
                         admin      18405498 Deletion         PreLoginBanner deleted
    2021-10-11T21:40:48.222
                         internal   18405486 Deletion         Web A: user admin terminated
 session id web_34771_A
    2021-10-11T21:39:52.703
                         internal   18405463 Creation         Fabric A: remote user test1
logged in from 192.0.2.1
    2021-10-11T21:39:44.351
                        internal   18405450 Deletion        Fabric A: user test1 terminated
 session id pts_1_1_5725
firepower# /security # show audit-logs 18405523 detail
Audit trail logs:
    Creation Time: 2021-10-11T21:42:30.885
    User: admin
    Session ID: pts_0_1_24360
    ID: 18405523
    Action: Creation
    Description: PreLoginBanner created
    Affected Object: sys/user-ext/pre-login-banner
    Trigger: Admin
    Modified Properties: message:TEST
, policyOwner:local
```

show auth-domain

Pour afficher les informations actuelles sur le domaine d'authentification, utilisez la commande **show auth-domain** en mode sécurité.

show auth-domain [**detail** | *domain_name*]

Description de la syntaxe

detail	(Facultatif) Affiche les informations détaillées sur tous les domaines d'authentification actuels.
domain_name	(Facultatif) Affiche les informations sur le domaine spécifié uniquement. Le mot clé **detail** est disponible avec cette option.

Modes de commande

scope security/

Historique des commandes

Version	Modification
1.4(1)	Commande ajoutée.

Instructions d'utilisation

Les domaines d'authentification sont créés à l'aide des commandes **create auth-domain** ou **enter auth-domain**.

Exemple

Cet exemple montre comment afficher les informations détaillées sur le domaine d'authentification pour un domaine spécifique :

```
firepower# scope security
firepower /security # show auth-domain test_domain detail

Authentication domain:
    Authentication domain name: test_domain
    Web session refresh period(in secs): 600
    Idle Session timeout(in secs) for web, ssh, telnet sessions: 600
    Absolute Session timeout(in secs) for web, ssh, telnet sessions: 3600
    Serial Console Idle Session timeout(in secs): 600
    Serial Console Absolute Session timeout(in secs): 3600
    Default Realm: Local
    Authentication server group:
    Use of 2nd factor: No
firepower /security #
```

Commande	Description
create auth-domain	Crée un domaine d'authentification.
scope auth-domain	Permet d'accéder au mode auth-domain pour un domaine d'authentification spécifique.

show auth-realm fsm status

Pour afficher les informations sur l'état du FSM disponible sur le système, utilisez la commande **show-auth fsm status**.

show auth-realm fsm status [**detail**]

Description de la syntaxe

detail	(Facultatif) Affiche les informations développées pour l'instance d'application actuelle. Ce mot clé est également disponible avec de nombreuses autres options de commande pour afficher les informations développées sur l'option spécifiée.

Modes de commande

scope security

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope security.

Exemple

Cet exemple montre comment afficher les informations sur l'état du FSM.

```
Firepower # scope security
Firepower /security # show auth-realm fsm status

FSM 1:
        Status: Nop
        Previous Status: Update Realm Success
        Timestamp: 2012-07-05T23:47:54.643
        Try: 0
        Progress (%): 100
        Current Task:
```

Cet exemple montre comment afficher les informations développées sur l'état du FSM :

```
Firepower # show auth-realm fsm status expand detail

    FSM Status:

        Affected Object: sys/auth-realm/fsm
        Current FSM: update Realm
        Status: Success
        Completion Time: 2012-07-05T23:47:54.643
        Progress (%): 100
        Description:
        Remote Result: Not Applicable
        Error Code: None
        Error Description:

        FSM Stage:

            Order: 1
            Stage Name: updateRealmSetRealmLocal
            Status: Success
            Try: 2
```

```
            Last Update Time: 2012-07-05T23:47:54.642
            Stage Description: realm configuration to primary (FSM-STAGE: Sam: dme:
AaaRealmUpdateRealm: SetRealmLocal)

            Order: 2
            Stage Name: updateRealmSetRealmPeer
            Status: Skip
            Try: 0
            Last Update Time: 2012-07-05T23:47:54.643
            Stage Description: realm configuration to secondary (FSM-STAGE: sam:dm e:
AaaRealmUpdateRealm: SetRealmPeer)
```

show authentication

Pour afficher la configuration administrative existante et l'état opérationnel de la console et l'authentification par défaut, utilisez la commande **show authentication** .

show authentication

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope security

Historique des commandes

Version	Modification
2.10(1)	Commande ajoutée.

Instructions d'utilisation

Vous pouvez afficher la configuration administrative existante et l'état opérationnel de la console et de l'authentification par défaut.

Exemple

Cet exemple montre comment accéder au mode sécurité et afficher la méthode d'authentification par défaut :

```
firepower# scope security
firepower /security # show authentication
Console authentication: Local
Operational Console authentication: Local
Default authentication: Local
Operational Default authentication: Local
Role Policy For Remote Users: Assign Default Role
```

Commandes associées

Commande	Description
set authentication	Définit le service d'authentification par défaut.

show breakout

Pour afficher des informations sur les configurations de répartition de port d'interface, utilisez la commande **show breakout** en mode structure.

show breakout [*slot_id port_id* | **detail** | **expand**]

Description de la syntaxe

slot_id port_id	(Facultatif) Affiche les informations de répartition pour un port spécifique. Les mots clés **expand** et **expand** sont disponibles avec cette option.
detail	(Facultatif) Affiche les informations détaillées sur les répartitions de port. Le mot clé **expand** est disponible avec cette option.
expand	(Facultatif) Affiche des informations développées sur les répartitions de port. Le mot clé **detail** est disponible avec cette option.

Modes de commande

scope cabling/scope fabric a/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande affiche les informations de répartition pour tous les ports.

Exemple

Cet exemple montre comment afficher les informations de câblage développées :

```
firepower# scope cabling
firepower /cabling # scope fabric a
firepower /cabling/fabric # show breakout

port breakout:
    Slot ID    Port ID    breakout type
    ---------- ---------- -------------
             3          1 10g 4x
             3          2 10g 4x
firepower /cabling/fabric #
```

Commandes associées

Commande	Description
create breakout	Crée une répartition d'interface.

show callhome

Pour afficher les informations de configuration et d'état de Call Home, utilisez la commande **show callhome**.

show callhome [**detail** | **expand** | **fsm status**]

Description de la syntaxe

detail	(Facultatif) Affiche les informations détaillées sur Call Home.
expand	(Facultatif) Affiche les informations développées sur Call Home.
fsm status	(Facultatif) Affiche les informations sur Call Home et l'état de la machine à états finis (FSM).

Modes de commande

Mode surveillance

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment afficher les informations sur Call Home :

```
FP9300-A /monitoring # show callhome

Callhome:
    Admin State: Off
    Throttling State: On
    Contact Information: admin
    Customer Contact Email:
    From Email:
    Reply To Email:
    Phone Contact e.g., +1-011-408-555-1212:
    Street Address:
    Contract Id:
    Customer Id:
    Site Id:
    Switch Priority: Debugging
    Enable/Disable HTTP/HTTPS Proxy: Off
    HTTP/HTTPS Proxy Server Address:
    HTTP/HTTPS Proxy Server Port: 80
    SMTP Server Address:
    SMTP Server Port: 25

DOC-FP9300-A /monitoring #
```

Commandes associées

Commande	Description
scope callhome	Permet d'accéder au mode configuration Call Home.

show (card)

Pour afficher les informations sur la carte de structure actuelle, utilisez la commande **show** en mode carte.

show [**beacon-led** | **detail** | **event** | **expand** | **fault** | **fsm task** | **port**]

Description de la syntaxe

beacon-led	(Facultatif) Affiche des informations sur les voyants DEL de balise de la carte. Les options suivantes sont également disponibles : • **detail** : affiche les informations détaillées sur les voyants DEL. Le mot clé **expand** est disponible avec cette option. • **expand** : affiche les informations développées sur les voyants DEL. Le mot clé **detail** est disponible avec cette option. • **fsm status** : affiche les informations sur l'état de la machine à états finis (FSM). Le mot clé **expand** est disponible avec cette option.
detail	(Facultatif) Affiche les informations détaillées sur la carte de structure. Le mot clé **expand** est disponible avec cette option.
event [*event_ID* | **detail** | **expand**]	(Facultatif) Affiche les informations sur les événements pour la carte de structure. Vous pouvez saisir un ID d'événement numérique pour afficher les informations sur cet événement uniquement. Les mots clés **detail** et **expand** sont disponibles avec cette option.
expand	(Facultatif) Affiche les informations développées pour la carte de structure. Le mot clé **detail** est disponible avec cette option.
fault	(Facultatif) Affiche les informations sur les défaillances qui se sont produites sur la carte de structure. Les options suivantes sont également disponibles avec ce mot clé : • *fault_ID* : affiche les informations pour la défaillance spécifiée. • **cause** : affiche les informations pour le type de cause spécifié uniquement. • **detail** : affiche les informations détaillées sur la défaillance. • **severity** : affiche les informations pour le niveau de gravité spécifié uniquement. • **suppressed** : répertorie les défaillances supprimées. Les mots clés **cause**, **detail** et **severity** sont disponibles avec cette option.
fsm task	(Facultatif) Affiche les informations sur la tâche FSM pour la carte. Le mot clé **detail** est disponible avec cette option.
port	(Facultatif) Répertorie les informations sur le port pour la carte.

Modes de commande

scope fabric-interconnect/scope card

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande affiche l'état de base de la carte.

Exemple

Cet exemple montre comment afficher les informations sur le port d'une carte de structure spécifique :

```
firepower# scope fabric-interconnect
firepower /fabric-interconnect # scope card 1
firepower /fabric-interconnect/card # show port

Ether Port:

Slot  Aggr Port  Port  Oper State       Mac                 Role    Xcvr
----- ---------- ----- ---------------- ------------------- ------- ----
    1          0     1 Up               B0:AA:77:2F:F0:B0   Network 1000BASE T
    1          0     2 Up               B0:AA:77:2F:F0:B1   Network 1000BASE T
    1          0     3 Up               B0:AA:77:2F:F0:B2   Network 1000BASE T
    1          0     4 Up               B0:AA:77:2F:F0:B3   Network 1000BASE T
    1          0     5 Up               B0:AA:77:2F:F0:B4   Network 1000BASE T
    1          0     6 Up               B0:AA:77:2F:F0:B5   Network 1000BASE T
    1          0     7 Failed           B0:AA:77:2F:F0:B6   Network 1000BASE T
    1          0     8 Sfp Not Present  B0:AA:77:2F:F0:B7   Network N/A

firepower /fabric-interconnect/card #
```

Commandes associées

Commande	Description
scope card	Permet d'accéder au mode administratif pour une carte de structure spécifique.

show card detail

Pour afficher les informations sur la carte, utilisez la commande **show card detail**.

show card [**detail** | **event** | **expand** | **card-config**]

Description de la syntaxe

detail	Affiche les informations pour la carte de structure.
expand	(Facultatif) Affiche les informations développées pour la carte de structure.
card-config	(Facultatif) Affiche des informations sur la configuration actuelle de la carte.

Modes de commande

scope fabric-interconnect a

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope fabric-interconnect a.

Exemple

Cet exemple montre comment afficher les informations pour une carte de structure spécifique :

```
Firepower# scope fabric-interconnect a
Firepower /fabric-interconnect # show card

Fabric Card:
    Id         State
    ---------- -----
             1 Online
             2 Online
             3 Online
```

Cet exemple montre comment afficher les informations détaillées pour une carte de structure spécifique :

```
Firepower /fabric-interconnect # show card detail

Fabric Card:
    Id: 1
    Description: Firepower 9300 Supervisor
    Number of Ports: 8
    State: Online
    Vendor: Cisco Systems, Inc.
    Model: FPR9K-SUP
    HW Revision: 0
    Serial (SN): JSJ18250001
    Perf: N/A
    Admin State: Online
    Power State: Online
    Presence: Equipped
    Thermal Status: N/A
    Voltage Status: N/A

    Id: 2
```

```
    Description: Firepower 8x10G SFP+ NM
    Number of Ports: 8
    State: Online
    Vendor: Cisco Systems, Inc.
    Model: FPR-NM-8X10G
    HW Revision: 0
    Serial (SN): JAD19510ALL
    Perf: N/A
    Admin State: Online
    Power State: Online
    Presence: Equipped
    Thermal Status: N/A
    Voltage Status: N/A

    Id: 3
    Description: Firepower 4x40G QSFP NM
    Number of Ports: 16
    State: Online
    Vendor: Cisco Systems, Inc.
    Model: FPR-NM-4X40G
    HW Revision: 0
    Serial (SN): JAD21040C9U
    Perf: N/A
    Admin State: Online
    Power State: Online
    Presence: Equipped
    Thermal Status: N/A
    Voltage Status: N/A
```

Cet exemple montre comment afficher les informations développées de la carte de structure actuelle :

```
Firepower# scope fabric-interconnect a
Firepower /fabric-interconnect # show card detail expand

Fabric Card:
    Id: 1
    Description: Firepower 9300 Supervisor
    Number of Ports: 8
    State: Online
    Vendor: Cisco Systems, Inc.
    Model: FPR9K-SUP
    HW Revision: 0
    Serial (SN): JSJ18250001
    Perf: N/A
    Admin State: Online
    Power State: Online
    Presence: Equipped
    Thermal Status: N/A
    Voltage Status: N/A

    Id: 2
    Description: Firepower 8x10G SFP+ NM
    Number of Ports: 8
    State: Online
    Vendor: Cisco Systems, Inc.
    Model: FPR-NM-8X10G
    HW Revision: 0
    Serial (SN): JAD19510ALL
    Perf: N/A
    Admin State: Online
    Power State: Online
    Presence: Equipped
    Thermal Status: N/A
    Voltage Status: N/A
```

```
    Id: 3
    Description: Firepower 4x40G QSFP NM
    Number of Ports: 16
    State: Online
    Vendor: Cisco Systems, Inc.
    Model: FPR-NM-4X40G
    HW Revision: 0
    Serial (SN): JAD21040C9U
    Perf: N/A
    Admin State: Online
    Power State: Online
    Presence: Equipped
    Thermal Status: N/A
    Voltage Status: N/A
```

Cet exemple montre comment afficher les informations sur la configuration de la carte actuelle :

```
Firepower# scope fabric-interconnect a
Firepower /fabric-interconnect # show card-config

Card Config:

Slot     Model            OperState    Presence ConfigState
-------- ---------------- ------------ -------- -----------
       1 FPR9K-SUP        Online       Yes      Ok
       2 FPR-NM-8X10G     Online       Yes      Ok
       3 FPR-NM-4X40G     Online       Yes      Ok
```

show cc-mode

Pour afficher des informations sur l'état actuel du mode Common Criteria, utilisez la commande **show cc-mode**.

show cc-mode

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode sécurité

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

L'activation de la conformité de certification sur un châssis Firepower 4100/9300 ne propage pas automatiquement la conformité à l'un de ses périphériques logiques connectés.

Exemple

Cet exemple montre comment accéder au mode sécurité et afficher des informations sur l'état actuel du mode Common Criteria :

```
FP9300-A # scope security
FP9300-A /security # show cc-mode
Common Criteria Mode Admin State: Disabled
Common Criteria Mode Operational State: Disabled
FP9300-A /security #
```

Commandes associées

Commande	Description
disable cc-mode	Désactive le mode Common Criteria.
enable cc-mode	Active le mode Common Criteria.

show certreq

Pour afficher la demande de certificat pour un trousseau de clés RSA spécifique, utilisez la commande **show certreq**.

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode trousseau de clés

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour afficher la demande de certificat pour le trousseau de clés actuel, que vous pouvez ensuite copier et envoyer à une ancre d'approbation ou une autorité de certification.

Exemple

Cet exemple montre comment accéder à un trousseau de clés existant et afficher sa demande de certificat :

```
FP9300-A # scope security
FP9300-A # scope keyring test-ring
FP9300-A /security/keyring # show certreq
Certificate request subject name: SSP
Certificate request ip address: 198.168.0.111
Certificate request FI A ip address: 0.0.0.0
Certificate request FI B ip address: 0.0.0.0
Certificate request e-mail name:
Certificate request ipv6 address: ::
Certificate request FI A ipv6 address: ::
Certificate request FI B ipv6 address: ::
Certificate request country name:
State, province or county (full name): CA
Locality name (eg, city): SJC
Organisation name (eg, company): Cisco
Organisational Unit Name (eg, section): Sec
DNS name (subject alternative name):
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIDEzCCAbsCAQAwEDEOMAwGA1UEAwwFdGVzdDEwggFiMA0GCSqGSIb3DQEBAQUA
A4IBTwAwggFKAoIBQQCDnam/ZTgX8SYXeaYIMeVPeMLvOO7EemP7kEAHPpAqX9d6
3V5NIOLNnCfr7SL8gmLDFORanzZIYb9uxD7/z98xlrS3LdIB3GWCYw+IN1Hz5do/
uClI56thmN5nWgjEWGDwTnu+CD0tFn3qPg8wOpynutE+f43B4fyhWRpU5VO6I3Ma
SRrR4Cp9CKju6U9lttqiNkt5VH3+peM+3AgF6suFF96tN2G+caIlwwf3h6EpFJ1e
NE6CHUIQAdrKPtJVcmMYIYEmEogMYD1O0RXY+ionucK7id4JFAKLVFXPrzHGA3g7
n+xInFC84/2kM1TtapWHrMAOYcTiQ5UR6BJOpLT1V6yXTJrv/FrknJkZJUFKvOBX
9fvZ82UH9o+gWMD8rRBvsz94zGbjBm3SpKh1MLvXjR9af3koaiWMR45BSob0XwID
AQABoD4wEwYJKoZIhvcNAQkHMQYMBHRlc3QwJwYJKoZIhvcNAQkOMRowGDAWBgNV
HREEDzANggV0ZXN0MYcEAQEBATANBgkqhkiG9w0BAQsFAAOCAUEAClVpnjwB8KjD
Okw6k9PaBde07a1eSWwmMd99rR3F9SmnWQMvFXj07m3dEgNRoTCMyxZXH3diDd6/
0e9Ss91/FxORTI3ux+lXhKAOKjOJ5Urz1YLLjomHGrhGNpITQCm71r/fXIjPfUHx
fwaN5lbgImiLI6copKMPY+XMPSFNvIuM4dTAZLHhn5PG0jRAztMNBogw+Fb659BH
vad0QYrz2SHAiH7xETZXp3CTBX4jGhoCad8ffS4YdGQd73/jpu8Zy1nnd1jv7mEj
H9GkSm8sQQfTwQX8RgbzegZGHu3/LxLO6XQDIRj9bTo1aa6zTuhwPyPs4MtdYbpv
```

```
mGdEB8QAMHUChdPZdPC44XRPhjPyseig91j+Q1HUmFCMvzNGXksbY1rWj3T4G8gn
z/g7x+OXX/31dLJA2yLx9osUsshmqjs=
-----END CERTIFICATE REQUEST-----

FP9300-A /security/keyring #
```

Commandes associées

Commande	Description
create certreq	Crée une demande de certificat de trousseau de clés.
create keyring	Crée un trousseau de clés RSA.
delete certreq	Supprime une demande de certificat de trousseau de clés existante.
enter certreq	Permet d'accéder à une demande de certificat de trousseau de clés.

show cfg-export-policy

Pour afficher la liste des politiques d'exportation configurées, utilisez la commande **show cfg-export-policy**.

Description de la syntaxe

detail	Affiche les informations détaillées sur les politiques d'exportation configurées.

Modes de commande

scope org

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope org.

Exemple

Cet exemple montre comment afficher les informations sur les politiques d'exportation configurées avec une planification :

```
Firepower /fabric-interconnect # scope org
Firepower /org # show cfg-export-policy
Config Export policy:
    Name                 Description Admin State
    -------------------- ----------- -----------
    default              Configuration Export Policy
                                     Disable
```

Exemple

Cet exemple montre comment afficher les informations détaillées de toutes les politiques d'exportation configurées disponibles

```
Firepower /org # show cfg-export-policy detail
Config Export policy:
    Name: default
    Description: Configuration Export Policy
    Admin State: Disable
    Protocol: Ftp
    Hostname:
    User:
    Remote File:
    Schedule: Daily
    Port: Default
    Current Task:
```

Exemple

Cet exemple montre comment afficher les informations détaillées de l'état fsm de toutes les politiques d'exportation configurées disponibles :

```
Firepower /org # show cfg-export-policy fsm status
Name: default
```

```
FSM 1:
    Status: Nop
    Previous Status: Nop
    Timestamp: Never
    Try: 0
    Progress (%): 100
    Current Task:
```

show chassis

Pour afficher les informations sur le châssis, utilisez la commande **show chassis**.

show chassis [**1**] [**decommissioned** | **detail** | **environment** | **fabric** | **fi-iom** | **firmware** | **fsm status** | **inventory** | **iom** | **psu** | **version**]

Description de la syntaxe

1	(Facultatif) ID de châssis. En présence d'un seul châssis, la saisie de cet ID est facultative.
decommissioned	(Facultatif) Affiche les informations sur un châssis désactivé.
detail	(Facultatif) Affiche les informations détaillées sur le châssis.
environment	(Facultatif) Affiche les informations sur l'environnement. Les mots clés **detail**, **expand**, **fan**, **iom**, **psu** et **server** sont également disponibles.
fabric	(Facultatif) Affiche les informations sur la structure. Le mot clé **detail** est également disponible.
fi-iom	(Facultatif) Affiche les informations sur le module I/I d'interconnexion de structures. Le mot clé **detail** est également disponible.
firmware	(Facultatif) Affiche les informations sur le micrologiciel. Le mot clé **detail** est également disponible.
fsm status	(Facultatif) Affiche les informations sur la machine à états finis (FSM). Le mot clé **expand** est également disponible.
inventory	(Facultatif) Affiche les informations sur le fournisseur et l'identification du châssis. Les mots clés **detail**, **expand**, **fabric**, **fan**, **fi-iom**, **iom**, **psu**, **server** et **unspecified** sont également disponibles.
iom	(Facultatif) Affiche des informations sur le module d'entrée/de sortie. Le mot clé **detail** est également disponible.
psu	(Facultatif) Affiche l'état du bloc d'alimentation. Le mot clé **detail** est également disponible.
version	(Facultatif) Affiche les numéros de version de tous les appareils du châssis. Le mot clé **detail** est également disponible.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous pouvez utiliser la commande **show chassis** sans arguments ni mots clés pour afficher les informations de base sur le châssis.

Exemple

Cet exemple montre comment afficher les informations de base sur le châssis :

```
FP9300-A# show chassis 1
Chassis:
Chassis    Overall Status           Admin State
---------- ------------------------ -----------
         1 Accessibility Problem    Acknowledged
FP9300-A#
```

Commandes associées

Commande	Description
show server environment	Affiche les informations sur le matériel du serveur.

show cli

Pour afficher les informations sur l'interface de ligne de commande, utilisez la commande **show cli**.

show cli { **command-status** | **history** | **mode-info** | **session-config** | **shell-type** }

Description de la syntaxe

command-status	(Facultatif) Affiche l'état de la commande la plus récente. Le mot clé facultatif **detail** fournit des détails supplémentaires sur la commande saisie précédemment.
history	(Facultatif) Affiche la liste des commandes saisies lors de la session en cours.
mode-info	(Facultatif) Affiche des informations sur le mode d'interface de ligne de commande actuel.
session-config	(Facultatif) Affiche des informations sur la configuration de la session actuelle.
shell-type	(Facultatif) Affiche des informations sur le type de shell de commande actuel.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Cette commande ne nécessite pas de licence.

Exemple

Cet exemple montre comment afficher les informations sur la configuration de la session actuelle :

```
FP9300-A# show cli session-config
Suppress Headers: off
Suppress Field Spillover: off
Table Field Delimiter: none
Terminal Width: 61
Terminal Length: 31
Session Absolute Timeout: 3600 seconds
Session Timeout: 600 seconds

FP9300-A#
```

Commandes associées

Commande	Description
set cli	Spécifie si les lignes de sortie des commandes doivent être renvoyées à la ligne ou tronquées pour s'adapter à la largeur de la fenêtre de terminal, si les en-têtes de tableau sont affichés et si des virgules ou des espaces sont utilisés pour séparer les champs dans les tableaux de sortie des commandes.

show clock

Pour afficher la date et l'heure actuelles du système, utilisez la commande **show clock**.

show clock [**detail**]

Description de la syntaxe

detail	(Facultatif) Affiche les informations détaillées sous forme de liste.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment afficher la date et l'heure actuelles du système :

```
FP9300-A# show clock
Tue Apr 20 13:24:33 PDT 2010
FP9300-A#
```

Commandes associées

Commande	Description
set clock	Définit manuellement la date et l'heure.
show timezone	Affiche le fuseau horaire actuellement défini.

show cloud-connector

Pour afficher l'état et les informations de configuration du connecteur infonuagique, utilisez la commande **show cloud-connector**.

show cloud-connector [**detail** | **expand** | **fsm**]

Description de la syntaxe

detail	(Facultatif) Affiche des détails supplémentaires sur le connecteur infonuagique.
expand	(Facultatif) Affiche des informations développées sur le connecteur infonuagique.
fsm status	(Facultatif) Affiche des informations sur l'état actuel de la machine à états finis (FSM).

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
2.2(2)	Commande ajoutée.

Exemple

Cet exemple montre comment afficher des informations d'état pour le FSM du connecteur infonuagique :

```
FP9300-A# show cloud-connector fsm status

    FSM 1:
        Remote Result: Not Applicable
        Remote Error Code: None
        Remote Error Description:
        Status: Nop
        Previous Status: Nop
        Timestamp: Never
        Try: 0
        Progress (%): 100
        Current Task:
FP9300-A #
```

Commandes associées

Commande	Description
scope cloud-connector	Permet d'accéder au mode connecteur infonuagique.

show configuration

Pour afficher les informations de configuration système, utilisez la commande **show configuration**.

show configuration [**all** | **no-diff-markers** | **no-pending** | **pending**]

Description de la syntaxe

all	(Facultatif) Affiche toutes les informations sur la configuration actuelle.
no-diff-markers	(Facultatif) N'inclut pas de marqueurs de différence dans les informations de configuration affichées.
no-pending	(Facultatif) N'inclut pas de commandes de configuration en attente (non validées).
pending	(Facultatif) Affiche toutes les commandes de configuration en attente uniquement.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment afficher des informations sur les commandes de configuration en attente (non validées) :

```
FP9300-A# show configuration pending
 scope services
+    create ntp-server 192.168.200.101
 exit
FP9300-A#
```

Commandes associées

Commande	Description
show cli	Affiche des informations sur l'état de l'interface de ligne de commande.

show connection

Pour afficher les informations de configuration pour les connexions IPSec actuelles ou pour une connexion unique, utilisez la commande **show connection**.

show connection [**detail** | *name*]

Description de la syntaxe

detail	(Facultatif) Affichez les informations détaillées sur la connexion IPSec.
name	(Facultatif) Nom de connexion spécifique; peut comporter jusqu'à 16 caractères alphanumériques.

Modes de commande

Mode IPSec

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour afficher les informations de connexion IPSec actuelles.

Exemple

Cet exemple montre comment afficher les informations de connexion IPSec :

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # show connection

IPSec Connection:
    Name       Admin State Local Address Remote Address ESP Mode  Keyring Name
    ---------- ----------- ------------- -------------- --------- ------------
    TEST       Disabled                                 Transport

FP9300-A /security/ipsec #
```

Commandes associées

Commande	Description
show ipsec-log	Affiche les journaux de connexion IPSec.
show stats	Affiche les statistiques.

show console-auth

Pour afficher les détails d'authentification de la console, utilisez la commande **show console-auth**.

show console-auth [**detail**]

Description de la syntaxe

detail	Informations détaillées sur l'authentification de la console.

Modes de commande

scope security

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope security.

Exemple

Cet exemple montre comment afficher les informations d'authentification de console :

```
Firepower # scope security
Firepower /security # show console-auth

Console authentication:
    Admin Realm                 Admin Authentication server group Use of 2nd factor
    --------------------------- --------------------------------- -------------
----
    Local                                                         No
```

show controller fsm status

Pour afficher la liste des états du FSM des contrôleurs disponibles sur le système, utilisez la commande **show controller fsm status**.

show controller fsm status [**expand**]

Description de la syntaxe

expand	(Facultatif) Affiche les informations développées pour l'instance d'application actuelle. Ce mot clé est également disponible avec de nombreuses autres options de commande pour afficher les informations développées sur l'option spécifiée.

Modes de commande

scope system

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope system.

Exemple

Cet exemple montre comment afficher des informations sur l'état du FSM du contrôleur :

```
Firepower # scope system
QP1 /system # show controller fsm status


    FSM 1:
        Remote Result: Not Applicable
        Remote Error Code: None
        Remote Error Description:
        Status: Nop
        Previous Status: Nop
        Timestamp: Never
        Try: 0
        Flags: 0
        Progress (%): 100
        Current Task:


    FSM 1:
        Remote Result: Not Applicable
        Remote Error Code: None
        Remote Error Description:
        Status: Nop
        Previous Status: Nop
        Timestamp: Never
        Try: 0
        Flags: 0
        Progress (%): 100
        Current Task:
Firepower /system # show controller fsm status expand


    FSM Status:
```

```
        Affected Object: sys/chassis-1/blade-1/adaptor-1/mgmt/fsm
        Current FSM: nop
        Status: Nop
        Completion Time:
        Progress (%): 100

        FSM Stage:


    FSM Status:
Affected Object: sys/chassis-1/blade-1/board Controller/mgmt/fsm
        Current FSM: nop
        Status: Nop
        Completion Time:
        Progress (%): 100

        FSM Stage:


    FSM Status:

        Affected Object: sys/chassis-1/blade-1/mgmt/fsm
        Current FSM: ExtMgmtIfConfig
        Status: Success
        Completion Time: 2012-07-27T00:42:51.248
        Progress (%): 100

        FSM Stage:

        Order Stage Name                                Status       Try
        ------ ---------------------------------------- ------------ ---
        1      ExtMgmtIfConfigPrimary                   Success      1
        2      ExtMgmtIfConfigSecondary                 Skip         0

    FSM Status:

        Affected Object: sys/chassis-1/sw-slot-1/mgmt/fsm
        Current FSM: nop
        Status: Nop
        Completion Time:
        Progress (%): 100
                                                        No
```

show core-export-target

Pour afficher des informations sur la cible d'exportation principale disponible sur le système, utilisez la commande **show core-export-target**.

show connection [**detail** | **FSM**]

Description de la syntaxe

detail	Répertorie des informations détaillées sur la cible d'exportation principale.
fsm	Affiche les informations de la machine à états finis (FSM) sur l'application actuelle selon le mot clé spécifié : État : affiche les informations sur l'état du FSM.

Modes de commande

Scope monitoring et scope sysdebug

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope monitoring et scope sysdebug.

Exemple

Cet exemple montre comment afficher les informations sur la cible d'exportation principale de tous les systèmes :

```
Firepower # scope monitoring
Firepower /monitoring # scope sysdebug
Firepower /monitoring/sysdebug # show core-export-target

Core Export Target:
    Server Name Port       Path       Admin State
    ----------- ---------- ---------- -----------
                69                    Disabled
Firepower /monitoring/sysdebug # show core-export-target detail

Core Export Target:
Server Name:
    Port: 69
    Path:
    Admin State: Disabled
    Description:
    Current Task:
Firepower /monitoring/sysdebug # show core-export-target fsm status

Server Name:
Port: 69
Path:
Admin State: Disabled

    FSM 1:
        Remote Result: Not Applicable
        Remote Error Code: None
        Remote Error Description:
```

```
Status: Nop
Previous Status: Configure Success
Timestamp: 2012-08-04T12:24:44.253
Try: 0
Progress (%): 100
Current Task:
```

show cores-detail

Pour afficher les informations sur les fichiers principaux disponibles sur le système, utilisez la commande **show cores-detail**.

show cores detail

Description de la syntaxe

detail	Répertorie les informations détaillées sur les fichiers principaux.

Modes de commande

Scope monitoring et scope sysdebug

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope monitoring et scope sysdebug.

Exemple

Cet exemple montre comment afficher les informations de la cible d'exportation principale du système :

```
Firepower # scope monitoring
Firepower /monitoring # scope sysdebug
Firepower /monitoring/sysdebug # show cores detail

Core Files:
    Name: 1339202710_SAM_QP1_svc_sam_portAG_log.10885.tar.gz
    Fabric ID: A
    Description: SAM/Fabric Interconnect Core Dump
    Size: 9928624
    Timestamp: 2012-06-09T00:45:23.000
    URI: corefile/1339202710_SAM_QP1_svc_sam_portAG_log.10885.tar.gz
    Current Task:

    Name: 1339202451_SAM_QP1_svc_sam_portAG_log.6740.tar.gz
    Fabric ID: A
    Description: SAM/Fabric Interconnect Core Dump
    Size: 9928180
    Timestamp: 2012-06-09T00:41:14.000
    URI: corefile/1339202451_SAM_QP1_svc_sam_portAG_log.6740.tar.gz
    Current Task:
```

show cpu

Pour afficher les détails d'un processeur, utilisez la commande **show cpu**.

show cpu [**detail**]

Description de la syntaxe

detail	Affiche les informations détaillées sur la version.

Modes de commande

scope chassis/scope server

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope server 1 sous scope chassis 1.

Exemple

Cet exemple montre comment afficher les informations du processeur sur un serveur particulier :

```
Firepower # KSEC-FPR4115-3# scope chassis 1
Firepower /chassis # scope server 1
Firepower /chassis/server # show cpu
CPU:
    ID  Presence             Architecture      Socket Cores       Speed (GHz)
    --- -------------------- ----------------- ------ ----------- -----------
      1 Equipped             Xeon              CPU1   12          2.100000
       2 Equipped             Xeon              CPU2   12          2.100000
Firepower /chassis/server #
```

Exemple

Cet exemple montre comment afficher les informations détaillées du processeur sur un serveur particulier :

```
Firepower# scope chassis 1
Firepower /chassis # scope server 1
Firepower /chassis/server # show cpu detail

CPU:
    ID: 1
    Presence: Equipped
    Architecture: Xeon
    Socket: CPU1
    Cores: 12
    Cores Enabled: 12
    Speed (GHz): 2.100000
    Stepping: 4
    Vendor: Intel(R) Corporation
    HW Revision: 0
    Thermal Status: OK
    Overall Status: Operable
    Operability: Operable
```

```
    ID: 2
    Presence: Equipped
    Architecture: Xeon
    Socket: CPU2
    Cores: 12
    Cores Enabled: 12
    Speed (GHz): 2.100000
    Stepping: 4
    Vendor: Intel(R) Corporation
    HW Revision: 0
    Thermal Status: OK
    Overall Status: Operable
    Operability: Operable
Firepower /chassis/server #
```

show default-auth detail

Pour afficher la configuration administrative existante, l'état de l'authentification opérationnelle de la console et l'authentification par défaut, utilisez la commande **show default-auth detail**.

show default-auth [**detail**]

Description de la syntaxe

Detail	Affiche les détails de l'authentification par défaut.

Modes de commande

scope security

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope system.

Exemple

Cet exemple affiche les informations d'authentification par défaut.

```
Firepower# scope security
Firepower /security # show default-auth detail
Default authentication:
    Admin Realm: Local
    Operational Realm: Local
    Web session refresh period(in secs): 0
    Idle Session timeout(in secs) for web, ssh, telnet sessions: 0
    Absolute Session timeout(in secs) for web, ssh, telnet sessions: 3600
    Serial Console Idle Session timeout(in secs): 0
    Serial Console Absolute Session timeout(in secs): 3600
    Admin Authentication server group:
    Operational Authentication server group:
    Use of 2nd factor: No
Firepower /security #
```

show domain-env-feature

Pour afficher la fonctionnalité d'environnement de domaine, utilisez la commande **show domain-env-feature** .

show domain-env-feature [**detail**]

Description de la syntaxe

detail dns	Affiche des informations détaillées sur la fonctionnalité d'environnement de domaine.

Modes de commande

scope system (scope environment-feature)

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope system, scope environment-feature.

Exemple

Cet exemple montre comment afficher les informations sur la fonctionnalité d'environnement de domaine :

```
Firepower /fabric-interconnect # scope system
Firepower /system/ # scope environment-feature
Firepower /system/environment-feature/ show domain-env-feature
Domain Environment Feature:
    Name                                Functional State
    ----------------------------------- ----------------
    DC_POWER_GROUP_FEATURE              Disabled
    ESTIMATE_IMPACT_ON_RECONNECT        Enabled
    HEALTH_REPORTING_FEATURE            Disabled
    POWER_GROUP_FEATURE                 Enabled
    REMOTE_OPERATION_FEATURE            Enabled
    UCS_REGISTRATION_FEATURE            Enabled
```

Exemple

```
Firepower /system/environment-feature # show domain-env-feature detail
Domain Environment Feature:
    Name: DC_POWER_GROUP_FEATURE
    Feature Type: Major
    Functional State: Disabled

    Name: ESTIMATE_IMPACT_ON_RECONNECT
    Feature Type: Major
    Functional State: Enabled

    Name: HEALTH_REPORTING_FEATURE
    Feature Type: Major
    Functional State: Disabled

    Name: POWER_GROUP_FEATURE
```

```
Feature Type: Major
Functional State: Enabled

Name: REMOTE_OPERATION_FEATURE
Feature Type: Major
Functional State: Enabled

Name: UCS_REGISTRATION_FEATURE
Feature Type: Major
Functional State: Enabled
```

show domain-name

Pour afficher le nom de domaine, utilisez la commande **show domain-name** .

show domain-name

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

scope system/services

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope system/services.

Exemple

Cet exemple affiche les informations sur le nom de domaine.

```
Firepower# scope system
Firepower /system # scope services
Firepower /system/services # show domain-name
Domain: <any configured domain name>
Note: Domain name can be configured based on user requirements as shown below.
Firepower /system/services # set domain-name cisco
Firepower /system/services* # commit-buffer
Firepower /system/services # show domain-name
Domain: cisco
```

show domain-nw-feature

Pour afficher des informations sur les fonctionnalités du réseau disponibles sur le système, utilisez la commande **show domain-nw-feature** .

show domain-nw-feature [**detail**]

Description de la syntaxe

detail dns	Affiche des informations détaillées sur les fonctionnalités du réseau.

Modes de commande

scope system, scope network-features

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope system, scope network-features.

Exemple

Cet exemple montre comment afficher les informations sur les fonctionnalités du réseau du système :

```
Firepower /fabric-interconnect # scope system
Firepower /system/ # scope environment-feature
Firepower /system/environment-feature/ show domain-nw-feature
Domain Environment Feature:
    Domain Network Feature:
    Name: NETFLOW_FEATURE
    Feature Type: Major
    Functional State: Disabled
```

show domain-server-feature

Pour afficher des informations sur les fonctionnalités du serveur disponibles sur le système, utilisez la commande **show domain-server-feature**.

show domain-server-feature [**detail**]

Description de la syntaxe

detail	Affiche des informations détaillées sur les fonctionnalités du réseau.

Modes de commande

Scope system, scope server-features

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope system, scope server-features.

Exemple

Cet exemple affiche les informations pour toutes les fonctionnalités du serveur du système :

```
Firepower # scope system
Firepower /system # scope server-features
Firepower /system/server-features # show domain-server-feature detail
Domain Server Feature:
    Name: GLOBAL_SP_FEATURE
    Feature Type: Major
    Functional State: Enabled

    Name: HEALTH_POLICY_FEATURE
    Feature Type: Major
    Functional State: Disabled

    Name: IN_BAND_MGMT_FEATURE
    Feature Type: Major
    Functional State: Enabled

    Name: POLICY_MAP_FEATURE
    Feature Type: Major
    Functional State: Enabled
```

show domain-storage-feature

Pour afficher la fonctionnalité de stockage de domaine système, utilisez la commande **show show domain-storage-feature**.

show domain-storage-feature [**detail** | **Name**]

Description de la syntaxe

detail dns	Affiche des informations détaillées sur la fonctionnalité de stockage de domaine.
Name	Affiche des informations sur le stockage de domaine spécifique. Les mots clés de détails sont également disponibles avec cette option.

Modes de commande

scope system/scope storage feature

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope system, scope storage feature.

Exemple

Cet exemple montre comment afficher des informations sur la politique de fonctionnalité de stockage de domaine :

```
Firepower /fabric-interconnect # scope system
Firepower /system # scope storage-feature
Firepower /system/storage-feature # show domain-storage-feature
Domain Storage Feature:
    Name                                Functional State
    ----------------------------------- ----------------
    FC_ZONING_FEATURE                   Enabled
    ISCSI_IPV6_FEATURE                  Enabled
```

Exemple

Cet exemple montre comment afficher des informations détaillées sur la fonctionnalité de stockage de domaine disponible :

```
Firepower /system/storage-feature # show domain-storage-feature detail
Domain Storage Feature:
    Name: FC_ZONING_FEATURE
    Feature Type: Major
    Functional State: Enabled

    Name: ISCSI_IPV6_FEATURE
    Feature Type: Major
    Functional State: Enabled
  Firepower /system/storage-features # show domain-storage-feature FC_ZONING_FEATURE
Domain Storage Feature:
Name Functional State
---------------------------------- ----------------
FC_ZONING_FEATURE Enabled
```

show dns

Pour afficher les serveurs de noms DNS dans FXOS, utilisez la commande **show dns** .

show dns

Description de la syntaxe

show dns	Cette commande permet d'afficher un serveur de noms DNS dans FXOS.

Modes de commande

scope system/scope services

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande affiche le serveur de noms DNS.

Exemple

L'exemple suivant montre comment afficher un serveur de noms DNS.

```
firepower# scope system; scope services
firepower /system /services # show dns
Domain Name Servers:
IP Address: 192.0.2.1
```

show download-task

Pour afficher des informations sur les opérations de téléchargement de l'ensemble de micrologiciels, utilisez la commande **show download-task** en mode micrologiciel.

Pour afficher les informations sur les opérations de téléchargement d'image logicielle de périphérique logique, utilisez la commande **show download-task** en mode logiciel d'application (/ssa/app-software).

show download-task [**detail** | **fsm** | *file_name*]

Description de la syntaxe

detail	(Facultatif) Utilisez ce mot clé pour afficher la liste détaillée de tous les téléchargements, ou si *file_name* est fourni, des informations détaillées sur le téléchargement du fichier spécifié.
fsm status | **fsm task**	(Facultatif) Utilisez ce mot clé pour répertorier les informations relatives à la machine à états finis (FSM) pour tous les téléchargements, ou si *file_name* est fourni, les informations relatives au FSM pour le fichier spécifié uniquement. **Remarque** En mode micrologiciel, ce mot clé est **fsm status**. En mode logiciel d'application (/ssa/app-software), ce mot clé est **fsm task**.
file_name	(Facultatif) Pour afficher les informations sur le téléchargement d'un fichier spécifique, indiquez le nom de ce fichier.

Modes de commande

scope firmware/

scope ssa/scope app-software

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Si vous n'indiquez pas de *nom de fichier* spécifique, tous les téléchargements sont répertoriés.

Exemples

Cet exemple montre comment afficher les informations détaillées sur la tâche de téléchargement de micrologiciels pour un ensemble spécifique :

```
firepower# scope firmware
firepower /firmware # show download-task fxos-k9-fpr9k-firmware.1.0.16.SPA detail

Download task:
    File Name: fxos-k9-fpr9k-firmware.1.0.16.SPA
    Protocol: Scp
    Server: 172.23.32.21
    Port: 0
    Userid: admin2
    Path: /auto/sspdev/bios/MIO_Firmware/release_images/fpr9k/1.0.16
    Downloaded Image Size (KB): 2118
    Time stamp: 2018-05-14T09:30:01.047
```

```
    State: Downloaded
    Status: Successful unpack the image
    Transfer Rate (KB/s): 192.545456
    Current Task:
firepower /firmware #
```

Cet exemple montre comment répertorier les fichiers images de logiciels téléchargés :

```
firepower# scope ssa
firepower /ssa # scope app-software
firepower /ssa/app-software # show download-task
Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State
    ----------------------------- ---------- -------------------- --------------- -----
    cisco-asa.9.4.1.65.csp        Scp        192.168.1.1          user            Downloaded
```

Commandes associées

Commande	Description
download image	Copie une image de micrologiciel ou une image logicielle de périphérique logique sur l'appareil.
install firmware	Installe un package de micrologiciel.
show firmware	Affiche des informations sur le micrologiciel du système.

show enforce-strong-password

Pour afficher la vérification de la force du mot de passe, utilisez la commande **show enforce-strong-password**.

show enforce-strong-password

Description de la syntaxe

Enforce-strong-password	Affiche la vérification de la force du mot de passe (oui/non).

Modes de commande

scope security

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope security.

Exemple

Cet exemple montre comment afficher la vérification de la force du mot de passe :

```
firepower# scope security
firepower /security # show enforce-strong-password
Password Strength Check: No
```

show environment

Pour afficher des informations sur l'état environnemental du châssis, utilisez la commande **show environment** en mode châssis, fxos ou gestion locale.

show environment [**detail** | **expand** | **fan** | **iom** | **psu** | **server** | **summary** | **verbose** | **tech**]

Description de la syntaxe

detail	(Facultatif) Utilisez ce mot clé pour afficher des informations détaillées sur l'environnement du châssis.
expand	(Facultatif) Utilisez ce mot clé pour afficher des informations sur l'état de chaque composant du châssis.
fan	(Facultatif) Affiche des informations d'état détaillées pour chaque ventilateur de chaque module de ventilation. Les mots clés **detail**, **iom**, **psu** et **server** sont également disponibles.
iom	(Facultatif) Affiche des informations sur le module d'entrée/de sortie. Les mots clés **detail**, **fan**, **psu** et **server** sont également disponibles.
psu	(Facultatif) Affiche l'état du bloc d'alimentation. Les mots clés **detail**, **fan**, **iom** et **server** sont également disponibles.
server	(Facultatif) Répertorie les informations sur l'état d'extension pour chaque composant matériel de chaque serveur. Les mots clés **detail**, **fan**, **iom** et **psu** sont également disponibles.
summary	(Facultatif) Affiche un résumé de l'état de chaque composant matériel. Le mot clé **detail** est également disponible.
verbose | **tech**	(Facultatif) Utilisez ce mot clé pour afficher des informations de débogage détaillées pour chaque composant de l'environnement.

Modes de commande

scope chassis/connect fxos/connect local-mgmt

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous pouvez utiliser cette commande sans arguments ni mots clés pour afficher les informations de base sur l'environnement du châssis.

Exemple

Cet exemple montre comment afficher un résumé de l'environnement du châssis :

```
firepower# scope chassis
firepower /chassis # show environment summary

Chassis INFO :
    Total Power Consumption: 726.000000
    Inlet Temperature (C): 35.000000
    CPU Temperature (C): 46.000000
    Last updated Time: 2018-12-18T21:19:22.353

    PSU 1:
        Type: AC
        Input Feed Status: Ok
        12v Output Status: Ok
        Overall Status: Operable
    PSU 2:
        Type: AC
        Input Feed Status: Ok
        12v Output Status: Ok
        Overall Status: N/A

    FAN 1
        Fan Speed RPM (RPM): 4268
        Speed Status: Ok
        Overall Status: Operable
    FAN 2
        Fan Speed RPM (RPM): 4312
        Speed Status: Ok
        Overall Status: Operable
    FAN 3
        Fan Speed RPM (RPM): 4180
        Speed Status: Ok
        Overall Status: Operable
    FAN 4
        Fan Speed RPM (RPM): 4092
        Speed Status: Ok
        Overall Status: Operable

    BLADE 1:
        Total Power Consumption: 258.000000
        Processor Temperature (C): 61.000000
    BLADE 2:
        Total Power Consumption: 270.000000
        Processor Temperature (C): 65.500000

firepower /chassis #
```

Exemple

Cet exemple montre comment afficher les informations sur l'environnement du châssis :

```
firepower# scope chassis
firepower /chassis # show environment expand

Chassis 1:
    Overall Status: Thermal Problem
    Operability: Operable
    Power State: Ok
    Thermal Status: Upper Critical   <<<---!!!

             CPU 1:
                Threshold Status: N/A
```

```
        Overall Status: Operable
        Operability: Operable
        Power State: N/A
        Thermal Status: OK
        Voltage Status: N/A

    CPU 2:
        Threshold Status: N/A
        Overall Status: Operable
        Operability: Operable
        Power State: N/A
        Thermal Status: UC   <<<---!!!
        Voltage Status: N/A
```

Remarque Si l'état thermique indique UC (Upper Critical), l'appareil fonctionne bien sans aucune perte de performance. Tandis que, si l'état thermique indique UNR (Upper Non-Recoverable), lesles performances de l'appareil sont dégradées.

Exemple

Cet exemple montre comment afficher les informations de débogage détaillées :

```
firepower# connect fxos
firepower (fxos) # show environment verbose
***************  Chassis Temps  ***************
AD7416_INLET_TEMP is 34 degrees Celsius
AD7416_OUTLET_TEMP_1 is 31 degrees Celsius

***************  CPU Data  ***************
Core Temperature 0 is 46 degrees Celsius
Core Temperature 1 is 46 degrees Celsius
Core Temperature 2 is 46 degrees Celsius
Core Temperature 3 is 46 degrees Celsius
Core Temperature 4 is 46 degrees Celsius
Core Temperature 5 is 46 degrees Celsius
Core Temperature 6 is 46 degrees Celsius
Core Temperature 7 is 46 degrees Celsius
Core Temperature 8 is 46 degrees Celsius
Core Temperature 9 is 46 degrees Celsius
Core Temperature 10 is 46 degrees Celsius
Core Temperature 11 is 46 degrees Celsius
Core Temperature 12 is 46 degrees Celsius
Core Temperature 13 is 46 degrees Celsius
Core Temperature 14 is 46 degrees Celsius
Core Temperature 15 is 46 degrees Celsius

***************  Power Supplies  ***************
PSU 1 input is okay
PSU 1 output is okay


-- Power Supply 1
  Voltage In         : 0xf9ab Raw Hex
  Current In         : 0xc878 Raw Hex
  Power In           : 0x00c0 Raw Hex
  Temperature 1      : 0x0022 Raw Hex
  Temperature 2      : 0x0026 Raw Hex
```

```
  Temperature 3      : 0x001f Raw Hex
  Fan Speed          : 0x28c4 Raw Hex
  Fan Status         : 0x00 Raw Hex
  Voltage Out        : 0x0078 Raw Hex
  Current Out        : 0x008f Raw Hex
  Power Out          : 0x00ab Raw Hex

No detected PSU in PSU Slot 2


***************  PSEQ Data  ***************
  12V         Voltage Output     :  12.22 Volts
  3.3V        Voltage Output     :   3.37 Volts
  1.2V_FPGA   Voltage Output     :   1.23 Volts
  2.5V_FPGA   Voltage Output     :   2.56 Volts
  0.85V_KC    Voltage Output     :   0.87 Volts
  0.9V_KC     Voltage Output     :   0.93 Volts
  1.8V_KC     Voltage Output     :   1.85 Volts
  1.2V_KC     Voltage Output     :   1.23 Volts
  1.8V_SW     Voltage Output     :   1.84 Volts
  1.0V_SW     Voltage Output     :   1.01 Volts
  SW_CORE     Voltage Output     :   1.01 Volts
  1.8V_NIC    Voltage Output     :   1.84 Volts
  0.9V_CORE_NIC Voltage Output     :   0.93 Volts
  1.0V_NIC    Voltage Output     :   1.03 Volts
  VDD_18_S5   Voltage Output     :   1.84 Volts
  VDDCR_SOC_S5 Voltage Output     :   0.92 Volts
  VDD_18      Voltage Output     :   1.84 Volts
  VDD_33      Voltage Output     :   3.45 Volts
  VPP_CD      Voltage Output     :   2.55 Volts
  VPP_GH      Voltage Output     :   2.55 Volts
  VDDIO_MEM_CD Voltage Output     :   1.23 Volts
  VDDIO_MEM_GH Voltage Output     :   1.23 Volts
  1.2V_MGTAVTT_KC Voltage Output     :   1.23 Volts
  0.9V_NTX_EN Voltage Output     :   0.00 Volts
  1.5V_NTX_EN Voltage Output     :   0.00 Volts
  1.8V_PHY_EN Voltage Output     :   0.00 Volts
  1.0V_PHY_EN Voltage Output     :   0.00 Volts
  VDDCR_SOC_EN Voltage Output     :   0.00 Volts
  VDDCR_CPU_EN Voltage Output     :   0.00 Volts
  VDD_3.3_S5_EN Voltage Output     :   0.00 Volts
  3.3_NIC_EN  Voltage Output     :   0.00 Volts
  5V_EN       Voltage Output     :   0.00 Volts

 PSEQ log

Fault Info Reg (0xb5):
12 9a 00 00 4f a9 33 48 7f ff ff ff ff ff ff ff 7f ff

Fault Rails Warning Reg (0xb6):
20 00 00 00 00 00 00 00 7f ff ff ff ff ff ff ff
7f ff ff ff ff ff ff ff 7f ff ff ff ff ff ff ff


Rails Value Reg (0xb7) page 0:
07 00 d0 2f 00 00 00

Rails Value Reg (0xb7) page 1:
07 00 45 34 00 00 00

Rails Value Reg (0xb7) page 2:
07 00 54 4c 00 00 00

Rails Value Reg (0xb7) page 3:
```

```
07 00 7d 4f 00 00 00

Rails Value Reg (0xb7) page 4:
07 00 10 36 00 00 00

Rails Value Reg (0xb7) page 5:
07 00 6c 39 00 00 00

Rails Value Reg (0xb7) page 6:
07 00 44 39 00 00 00

Rails Value Reg (0xb7) page 7:
07 00 18 4c 00 00 00

Rails Value Reg (0xb7) page 8:
07 00 22 39 00 00 00

Rails Value Reg (0xb7) page 9:
07 00 80 3e 00 00 00

Rails Value Reg (0xb7) page 10:
07 00 80 3e 00 00 00

Rails Value Reg (0xb7) page 11:
07 00 12 39 00 00 00

Rails Value Reg (0xb7) page 12:
07 00 a0 39 00 00 00

Rails Value Reg (0xb7) page 13:
07 00 b8 3f 00 00 00

Rails Value Reg (0xb7) page 14:
07 00 36 39 00 00 00

Rails Value Reg (0xb7) page 15:
07 00 3c 39 00 00 00

Rails Value Reg (0xb7) page 16:
07 00 22 39 00 00 00

Rails Value Reg (0xb7) page 17:
07 00 74 35 00 00 00

Rails Value Reg (0xb7) page 18:
07 00 3e 4f 00 00 00

Rails Value Reg (0xb7) page 19:
07 00 37 4f 00 00 00

Rails Value Reg (0xb7) page 20:
07 00 7c 4c 00 00 00

Rails Value Reg (0xb7) page 21:
07 00 7c 4c 00 00 00

Rails Value Reg (0xb7) page 22:
07 00 74 4c 00 00 00

Rails Value Reg (0xb7) page 23:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 24:
07 00 00 00 00 00 00
```

```
Rails Value Reg (0xb7) page 25:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 26:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 27:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 28:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 29:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 30:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 31:
07 00 01 00 00 00 00

Logged Fault Reg (0xea):
25 03 00 00 08 02 82 00 7f ff ff ff ff ff ff ff
7f ff ff ff ff ff ff ff 7f ff ff ff ff ff ff ff
00 00 00 00 00

Fault Details Index Reg (0xeb):
00 64

Fault Details Reg (0xec) index 0:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 1:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 2:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 3:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 4:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 5:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 6:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 7:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 8:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 9:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 10:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 11:
```

```
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 12:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 13:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 14:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 15:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 16:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 17:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 18:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 19:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 20:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 21:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 22:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 23:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 24:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 25:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 26:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 27:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 28:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 29:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 30:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 31:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 32:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff
```

```
Fault Details Reg (0xec) index 33:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 34:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 35:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 36:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 37:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 38:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 39:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 40:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 41:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 42:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 43:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 44:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 45:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 46:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 47:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 48:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 49:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 50:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 51:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 52:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 53:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff
```

```
Fault Details Reg (0xec) index 54:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 55:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 56:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 57:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 58:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 59:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 60:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 61:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 62:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 63:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 64:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 65:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 66:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 67:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 68:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 69:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 70:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 71:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 72:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 73:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 74:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 75:
```

```
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 76:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 77:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 78:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 79:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 80:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 81:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 82:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 83:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 84:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 85:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 86:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 87:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 88:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 89:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 90:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 91:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 92:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 93:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 94:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 95:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 96:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff
```

```
Fault Details Reg (0xec) index 97:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 98:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 99:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Logged Page Peaks Reg (0xed) page 0:
05 00 4b 31 00

Logged Page Peaks Reg (0xed) page 1:
05 00 fa 35 00

Logged Page Peaks Reg (0xed) page 2:
05 00 08 4f 00

Logged Page Peaks Reg (0xed) page 3:
05 00 25 52 00

Logged Page Peaks Reg (0xed) page 4:
05 00 fc 37 00

Logged Page Peaks Reg (0xed) page 5:
05 00 58 3b 00

Logged Page Peaks Reg (0xed) page 6:
05 00 24 3b 00

Logged Page Peaks Reg (0xed) page 7:
05 00 e8 4e 00

Logged Page Peaks Reg (0xed) page 8:
05 00 06 3b 00

Logged Page Peaks Reg (0xed) page 9:
05 00 c8 41 00

Logged Page Peaks Reg (0xed) page 10:
05 00 c8 41 00

Logged Page Peaks Reg (0xed) page 11:
05 00 16 3b 00

Logged Page Peaks Reg (0xed) page 12:
05 00 d8 3b 00

Logged Page Peaks Reg (0xed) page 13:
05 00 dc 41 00

Logged Page Peaks Reg (0xed) page 14:
05 00 10 3b 00

Logged Page Peaks Reg (0xed) page 15:
05 00 1c 3b 00

Logged Page Peaks Reg (0xed) page 16:
05 00 2a 3b 00

Logged Page Peaks Reg (0xed) page 17:
05 00 3e 37 00
```

```
Logged Page Peaks Reg (0xed) page 18:
05 00 ce 51 00

Logged Page Peaks Reg (0xed) page 19:
05 00 ce 51 00

Logged Page Peaks Reg (0xed) page 20:
05 00 4c 4f 00

Logged Page Peaks Reg (0xed) page 21:
05 00 58 4f 00

Logged Page Peaks Reg (0xed) page 22:
05 00 44 4f 00

Logged Page Peaks Reg (0xed) page 23:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 24:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 25:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 26:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 27:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 28:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 29:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 30:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 31:
05 00 00 00 00

Fault Detail Enable Reg (0xef):
25 ff ff ff f7 fd 07 07 7f ff ff ff ff ff ff ff
7f ff ff ff ff ff ff ff 7f ff ff ff ff ff ff ff
00 00 00 00 00


*************** EPM Data ***************
EPM0 is present
EPM0 Card power is okay
EPM0 Card is ready
EPM0 temperature is 32 degrees Celsius

***************  Fans  ***************
FanMod 1 Fan 1 rotating
FanMod 1 Fan 1 RPM = 21720
FanMod 1 Fan 2 rotating
FanMod 1 Fan 2 RPM = 19380
FanMod 1 Fan 3 rotating
FanMod 1 Fan 3 RPM = 21900
FanMod 1 Fan 4 rotating
FanMod 1 Fan 4 RPM = 19320
FanMod 2 Fan 1 rotating
```

```
FanMod 2 Fan 1 RPM = 21720
FanMod 2 Fan 2 rotating
FanMod 2 Fan 2 RPM = 19200
FanMod 2 Fan 3 rotating
FanMod 2 Fan 3 RPM = 21540
FanMod 2 Fan 4 rotating
FanMod 2 Fan 4 RPM = 19440
Fan Controller Speed = automatic
```

Exemple

Cet exemple montre comment afficher les informations de débogage :

```
firepower# connect fxos
firepower (fxos) # show environment tech
***************  Chassis Temps  ***************
AD7416_INLET_TEMP is 34 degrees Celsius
AD7416_OUTLET_TEMP_1 is 31 degrees Celsius

***************  CPU Data  ***************
Core Temperature 0 is 45 degrees Celsius
Core Temperature 1 is 45 degrees Celsius
Core Temperature 2 is 45 degrees Celsius
Core Temperature 3 is 45 degrees Celsius
Core Temperature 4 is 45 degrees Celsius
Core Temperature 5 is 45 degrees Celsius
Core Temperature 6 is 45 degrees Celsius
Core Temperature 7 is 45 degrees Celsius
Core Temperature 8 is 45 degrees Celsius
Core Temperature 9 is 45 degrees Celsius
Core Temperature 10 is 45 degrees Celsius
Core Temperature 11 is 45 degrees Celsius
Core Temperature 12 is 45 degrees Celsius
Core Temperature 13 is 45 degrees Celsius
Core Temperature 14 is 45 degrees Celsius
Core Temperature 15 is 45 degrees Celsius
Tdie is 45
Tctl is 45
Tccd3 is 45
Tccd5 is 38

***************  Power Supplies  ***************
PSU 1 input is okay
PSU 1 output is okay


-- Power Supply 1
  Voltage In         : 0xf9ab Raw Hex
  Current In         : 0xc878 Raw Hex
  Power In           : 0x00c0 Raw Hex
  Temperature 1      : 0x0022 Raw Hex
  Temperature 2      : 0x0026 Raw Hex
  Temperature 3      : 0x001f Raw Hex
  Fan Speed          : 0x28c5 Raw Hex
  Fan Status         : 0x00 Raw Hex
  Voltage Out        : 0x0078 Raw Hex
  Current Out        : 0x0091 Raw Hex
  Power Out          : 0x00ac Raw Hex

No detected PSU in PSU Slot 2
```

```
***************  PSEQ Data  ***************

Common PSEQ Regs
  CAPABILITY                     : 0xb0 Raw Hex
  STATUS_BYTE                    : 0x03 Raw Hex
  STATUS_WORD                    : 0x1003 Raw Hex
  Communication status           : 0x40 Raw Hex
  MFR_ID                         :  31 37 2d 31 30 32 30 7f ff ff ff ff ff ff ff 80 Raw Hex

  PMBus revision                 : 0x12 Raw Hex
  MFR_MODEL                      :  46 50 52 2d 33 31 30 7f ff ff ff ff ff ff ff 80 Raw Hex

  MFR_REVISION                   :  56 31 2e 35 a3 ff ff 7f ff ff ff ff ff ff ff 80 Raw Hex

  MFR_LOCATION                   :  43 69 73 63 6f 6e ff 7f ff ff ff ff ff ff ff 80 Raw Hex

  MFR_DATE                       :  30 35 32 31 32 31 db 7f ff ff ff ff ff ff ff 80 Raw Hex

  MFR_SERIAL                     :  55 31 36 36 c5 ff ff 7f ff ff ff ff ff ff ff 80 Raw Hex

  Silicon device ID              :  55 43 44 39 30 33 32 7f ff ff ff ff ff ff ff 80 Raw Hex

  Silicon device revision        :  2e 30 2e 30 2e 33 30 7f ff ff ff ff ff ff ff 80 Raw Hex


  12V         Voltage Output     :  12.24 Volts
  Page                           : 0x00 Raw Hex
  OPERATION                      : 0x00 Raw Hex
  On Off Config                  : 0x14 Raw Hex
  VOUT mode                      : 0x16 Raw Hex
  VOUT command                   : 0x3000 Raw Hex
  VOUT margin hi                 : 0x3266 Raw Hex
  VOUT margin lo                 : 0x2d9a Raw Hex
  VOUT scale                     : 0xa2a8 Raw Hex
  VOUT OV fault limit            : 0x3733 Raw Hex
  VOUT OV warn limit             : 0x34cd Raw Hex
  VOUT UV warn limit             : 0x2b33 Raw Hex
  VOUT UV fault limit            : 0x28cd Raw Hex
  IOUT OC fault limit            : 0x8000 Raw Hex
  IOUT OC warn limit             : 0x8000 Raw Hex
  Power good on                  : 0x2b33 Raw Hex
  Power good off                 : 0x28cd Raw Hex
  On delay                       : 0xba00 Raw Hex
  On time limit                  : 0x8000 Raw Hex
  Off delay                      : 0xba00 Raw Hex
  Off time limit                 : 0x8000 Raw Hex
  STATUS_VOUT                    : 0x00 Raw Hex
  STATUS_IOUT                    : 0x00 Raw Hex
  Output voltage                 : 0x30e5 Raw Hex
  Output current                 : 0x8000 Raw Hex

  3.3V        Voltage Output     :   3.37 Volts
  Page                           : 0x01 Raw Hex
  OPERATION                      : 0x00 Raw Hex
  On Off Config                  : 0x14 Raw Hex
  VOUT mode                      : 0x14 Raw Hex
  VOUT command                   : 0x34cd Raw Hex
  VOUT margin hi                 : 0x3771 Raw Hex
  VOUT margin lo                 : 0x3229 Raw Hex
  VOUT scale                     : 0xb26d Raw Hex
  VOUT OV fault limit            : 0x3cb8 Raw Hex
  VOUT OV warn limit             : 0x3a14 Raw Hex
```

```
VOUT UV warn limit            : 0x2f85 Raw Hex
VOUT UV fault limit           : 0x2ce1 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x2f85 Raw Hex
Power good off                : 0x2ce1 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
Output voltage                : 0x35ea Raw Hex
Output current                : 0x8000 Raw Hex

1.2V_FPGA   Voltage Output    :   1.23 Volts
Page                          : 0x02 Raw Hex
OPERATION                     : 0x00 Raw Hex
On Off Config                 : 0x14 Raw Hex
VOUT mode                     : 0x12 Raw Hex
VOUT command                  : 0x4ccd Raw Hex
VOUT margin hi                : 0x50a4 Raw Hex
VOUT margin lo                : 0x48f6 Raw Hex
VOUT scale                    : 0xba00 Raw Hex
VOUT OV fault limit           : 0x5852 Raw Hex
VOUT OV warn limit            : 0x547b Raw Hex
VOUT UV warn limit            : 0x451f Raw Hex
VOUT UV fault limit           : 0x4148 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x451f Raw Hex
Power good off                : 0x4148 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
Output voltage                : 0x4ec0 Raw Hex
Output current                : 0x8000 Raw Hex

2.5V_FPGA   Voltage Output    :   2.56 Volts
Page                          : 0x03 Raw Hex
OPERATION                     : 0x00 Raw Hex
On Off Config                 : 0x14 Raw Hex
VOUT mode                     : 0x13 Raw Hex
VOUT command                  : 0x5000 Raw Hex
VOUT margin hi                : 0x5400 Raw Hex
VOUT margin lo                : 0x4c00 Raw Hex
VOUT scale                    : 0xb333 Raw Hex
VOUT OV fault limit           : 0x5c00 Raw Hex
VOUT OV warn limit            : 0x5800 Raw Hex
VOUT UV warn limit            : 0x4800 Raw Hex
VOUT UV fault limit           : 0x4400 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x4800 Raw Hex
Power good off                : 0x4400 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
```

```
Output voltage                : 0x5207 Raw Hex
Output current                : 0x8000 Raw Hex

0.85V_KC    Voltage Output    :   0.87 Volts
Page                          : 0x04 Raw Hex
OPERATION                     : 0x00 Raw Hex
On Off Config                 : 0x14 Raw Hex
VOUT mode                     : 0x12 Raw Hex
VOUT command                  : 0x3666 Raw Hex
VOUT margin hi                : 0x3927 Raw Hex
VOUT margin lo                : 0x33b6 Raw Hex
VOUT scale                    : 0xba00 Raw Hex
VOUT OV fault limit           : 0x3e87 Raw Hex
VOUT OV warn limit            : 0x3bd7 Raw Hex
VOUT UV warn limit            : 0x30f6 Raw Hex
VOUT UV fault limit           : 0x2e35 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x30f6 Raw Hex
Power good off                : 0x2e35 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
Output voltage                : 0x37c8 Raw Hex
Output current                : 0x8000 Raw Hex

0.9V_KC     Voltage Output    :   0.93 Volts
Page                          : 0x05 Raw Hex
OPERATION                     : 0x00 Raw Hex
On Off Config                 : 0x14 Raw Hex
VOUT mode                     : 0x12 Raw Hex
VOUT command                  : 0x399a Raw Hex
VOUT margin hi                : 0x3c7b Raw Hex
VOUT margin lo                : 0x36b8 Raw Hex
VOUT scale                    : 0xba00 Raw Hex
VOUT OV fault limit           : 0x423d Raw Hex
VOUT OV warn limit            : 0x3f5c Raw Hex
VOUT UV warn limit            : 0x33d7 Raw Hex
VOUT UV fault limit           : 0x30f6 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x33d7 Raw Hex
Power good off                : 0x30f6 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
Output voltage                : 0x3b38 Raw Hex
Output current                : 0x8000 Raw Hex

1.8V_KC     Voltage Output    :   1.85 Volts
Page                          : 0x06 Raw Hex
OPERATION                     : 0x00 Raw Hex
On Off Config                 : 0x14 Raw Hex
VOUT mode                     : 0x13 Raw Hex
VOUT command                  : 0x399a Raw Hex
VOUT margin hi                : 0x3c7b Raw Hex
VOUT margin lo                : 0x36b8 Raw Hex
VOUT scale                    : 0xba00 Raw Hex
```

```
VOUT OV fault limit           : 0x423d Raw Hex
VOUT OV warn limit            : 0x3f5c Raw Hex
VOUT UV warn limit            : 0x33d7 Raw Hex
VOUT UV fault limit           : 0x30f6 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x33d7 Raw Hex
Power good off                : 0x30f6 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
Output voltage                : 0x3b1a Raw Hex
Output current                : 0x8000 Raw Hex

1.2V_KC     Voltage Output    :   1.23 Volts
Page                          : 0x07 Raw Hex
OPERATION                     : 0x00 Raw Hex
On Off Config                 : 0x14 Raw Hex
VOUT mode                     : 0x12 Raw Hex
VOUT command                  : 0x4ccd Raw Hex
VOUT margin hi                : 0x50a4 Raw Hex
VOUT margin lo                : 0x48f6 Raw Hex
VOUT scale                    : 0xba00 Raw Hex
VOUT OV fault limit           : 0x5852 Raw Hex
VOUT OV warn limit            : 0x547b Raw Hex
VOUT UV warn limit            : 0x451f Raw Hex
VOUT UV fault limit           : 0x4148 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x451f Raw Hex
Power good off                : 0x4148 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
Output voltage                : 0x4e84 Raw Hex
Output current                : 0x8000 Raw Hex

1.8V_SW     Voltage Output    :   1.84 Volts
Page                          : 0x08 Raw Hex
OPERATION                     : 0x00 Raw Hex
On Off Config                 : 0x14 Raw Hex
VOUT mode                     : 0x13 Raw Hex
VOUT command                  : 0x399a Raw Hex
VOUT margin hi                : 0x3c7b Raw Hex
VOUT margin lo                : 0x36b8 Raw Hex
VOUT scale                    : 0xba00 Raw Hex
VOUT OV fault limit           : 0x423d Raw Hex
VOUT OV warn limit            : 0x3f5c Raw Hex
VOUT UV warn limit            : 0x33d7 Raw Hex
VOUT UV fault limit           : 0x30f6 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x33d7 Raw Hex
Power good off                : 0x30f6 Raw Hex
On delay                      : 0xeb20 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
```

```
STATUS_VOUT                    : 0x00 Raw Hex
STATUS_IOUT                    : 0x00 Raw Hex
Output voltage                 : 0x3af2 Raw Hex
Output current                 : 0x8000 Raw Hex

1.0V_SW     Voltage Output     :   1.01 Volts
Page                           : 0x09 Raw Hex
OPERATION                      : 0x00 Raw Hex
On Off Config                  : 0x14 Raw Hex
VOUT mode                      : 0x12 Raw Hex
VOUT command                   : 0x4000 Raw Hex
VOUT margin hi                 : 0x4333 Raw Hex
VOUT margin lo                 : 0x3ccd Raw Hex
VOUT scale                     : 0xba00 Raw Hex
VOUT OV fault limit            : 0x499a Raw Hex
VOUT OV warn limit             : 0x4666 Raw Hex
VOUT UV warn limit             : 0x399a Raw Hex
VOUT UV fault limit            : 0x3666 Raw Hex
IOUT OC fault limit            : 0x8000 Raw Hex
IOUT OC warn limit             : 0x8000 Raw Hex
Power good on                  : 0x399a Raw Hex
Power good off                 : 0x3666 Raw Hex
On delay                       : 0xba00 Raw Hex
On time limit                  : 0xda80 Raw Hex
Off delay                      : 0xba00 Raw Hex
Off time limit                 : 0x8000 Raw Hex
STATUS_VOUT                    : 0x00 Raw Hex
STATUS_IOUT                    : 0x00 Raw Hex
Output voltage                 : 0x409c Raw Hex
Output current                 : 0x8000 Raw Hex

SW_CORE     Voltage Output     :   1.01 Volts
Page                           : 0x0a Raw Hex
OPERATION                      : 0x00 Raw Hex
On Off Config                  : 0x14 Raw Hex
VOUT mode                      : 0x12 Raw Hex
VOUT command                   : 0x4000 Raw Hex
VOUT margin hi                 : 0x4333 Raw Hex
VOUT margin lo                 : 0x3ccd Raw Hex
VOUT scale                     : 0xba00 Raw Hex
VOUT OV fault limit            : 0x499a Raw Hex
VOUT OV warn limit             : 0x4666 Raw Hex
VOUT UV warn limit             : 0x399a Raw Hex
VOUT UV fault limit            : 0x3666 Raw Hex
IOUT OC fault limit            : 0x8000 Raw Hex
IOUT OC warn limit             : 0x8000 Raw Hex
Power good on                  : 0x399a Raw Hex
Power good off                 : 0x3666 Raw Hex
On delay                       : 0xca80 Raw Hex
On time limit                  : 0xda80 Raw Hex
Off delay                      : 0xba00 Raw Hex
Off time limit                 : 0x8000 Raw Hex
STATUS_VOUT                    : 0x00 Raw Hex
STATUS_IOUT                    : 0x00 Raw Hex
Output voltage                 : 0x4094 Raw Hex
Output current                 : 0x8000 Raw Hex

1.8V_NIC    Voltage Output     :   1.84 Volts
Page                           : 0x0b Raw Hex
OPERATION                      : 0x00 Raw Hex
On Off Config                  : 0x14 Raw Hex
VOUT mode                      : 0x13 Raw Hex
VOUT command                   : 0x399a Raw Hex
VOUT margin hi                 : 0x3c7b Raw Hex
```

```
VOUT margin lo                : 0x36b8 Raw Hex
VOUT scale                    : 0xba00 Raw Hex
VOUT OV fault limit           : 0x423d Raw Hex
VOUT OV warn limit            : 0x3f5c Raw Hex
VOUT UV warn limit            : 0x33d7 Raw Hex
VOUT UV fault limit           : 0x30f6 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x33d7 Raw Hex
Power good off                : 0x30f6 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
Output voltage                : 0x3ae8 Raw Hex
Output current                : 0x8000 Raw Hex

0.9V_CORE_NIC Voltage Output     :   0.93 Volts
Page                          : 0x0c Raw Hex
OPERATION                     : 0x00 Raw Hex
On Off Config                 : 0x14 Raw Hex
VOUT mode                     : 0x12 Raw Hex
VOUT command                  : 0x399a Raw Hex
VOUT margin hi                : 0x3c7b Raw Hex
VOUT margin lo                : 0x36b8 Raw Hex
VOUT scale                    : 0xba00 Raw Hex
VOUT OV fault limit           : 0x423d Raw Hex
VOUT OV warn limit            : 0x3f5c Raw Hex
VOUT UV warn limit            : 0x33d7 Raw Hex
VOUT UV fault limit           : 0x30f6 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x33d7 Raw Hex
Power good off                : 0x30f6 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
Output voltage                : 0x3bc4 Raw Hex
Output current                : 0x8000 Raw Hex

1.0V_NIC    Voltage Output     :   1.03 Volts
Page                          : 0x0d Raw Hex
OPERATION                     : 0x00 Raw Hex
On Off Config                 : 0x14 Raw Hex
VOUT mode                     : 0x12 Raw Hex
VOUT command                  : 0x4000 Raw Hex
VOUT margin hi                : 0x4333 Raw Hex
VOUT margin lo                : 0x3ccd Raw Hex
VOUT scale                    : 0xba00 Raw Hex
VOUT OV fault limit           : 0x499a Raw Hex
VOUT OV warn limit            : 0x4666 Raw Hex
VOUT UV warn limit            : 0x399a Raw Hex
VOUT UV fault limit           : 0x3666 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x399a Raw Hex
Power good off                : 0x3666 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
```

```
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
Output voltage                : 0x41a0 Raw Hex
Output current                : 0x8000 Raw Hex

VDD_18_S5   Voltage Output    :   1.84 Volts
Page                          : 0x0e Raw Hex
OPERATION                     : 0x00 Raw Hex
On Off Config                 : 0x14 Raw Hex
VOUT mode                     : 0x13 Raw Hex
VOUT command                  : 0x399a Raw Hex
VOUT margin hi                : 0x3c7b Raw Hex
VOUT margin lo                : 0x36b8 Raw Hex
VOUT scale                    : 0xba00 Raw Hex
VOUT OV fault limit           : 0x423d Raw Hex
VOUT OV warn limit            : 0x3f5c Raw Hex
VOUT UV warn limit            : 0x33d7 Raw Hex
VOUT UV fault limit           : 0x30f6 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x33d7 Raw Hex
Power good off                : 0x30f6 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
Output voltage                : 0x3b02 Raw Hex
Output current                : 0x8000 Raw Hex

VDDCR_SOC_S5 Voltage Output    :   0.92 Volts
Page                          : 0x0f Raw Hex
OPERATION                     : 0x00 Raw Hex
On Off Config                 : 0x14 Raw Hex
VOUT mode                     : 0x12 Raw Hex
VOUT command                  : 0x399a Raw Hex
VOUT margin hi                : 0x3c7b Raw Hex
VOUT margin lo                : 0x36b8 Raw Hex
VOUT scale                    : 0xba00 Raw Hex
VOUT OV fault limit           : 0x423d Raw Hex
VOUT OV warn limit            : 0x3f5c Raw Hex
VOUT UV warn limit            : 0x33d7 Raw Hex
VOUT UV fault limit           : 0x30f6 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x33d7 Raw Hex
Power good off                : 0x30f6 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
Output voltage                : 0x3b08 Raw Hex
Output current                : 0x8000 Raw Hex

VDD_18      Voltage Output    :   1.84 Volts
Page                          : 0x10 Raw Hex
OPERATION                     : 0x00 Raw Hex
On Off Config                 : 0x14 Raw Hex
VOUT mode                     : 0x13 Raw Hex
```

```
VOUT command                    : 0x399a Raw Hex
VOUT margin hi                  : 0x3c7b Raw Hex
VOUT margin lo                  : 0x36b8 Raw Hex
VOUT scale                      : 0xba00 Raw Hex
VOUT OV fault limit             : 0x423d Raw Hex
VOUT OV warn limit              : 0x3f5c Raw Hex
VOUT UV warn limit              : 0x33d7 Raw Hex
VOUT UV fault limit             : 0x30f6 Raw Hex
IOUT OC fault limit             : 0x8000 Raw Hex
IOUT OC warn limit              : 0x8000 Raw Hex
Power good on                   : 0x33d7 Raw Hex
Power good off                  : 0x30f6 Raw Hex
On delay                        : 0xb39a Raw Hex
On time limit                   : 0xda80 Raw Hex
Off delay                       : 0xba00 Raw Hex
Off time limit                  : 0x8000 Raw Hex
STATUS_VOUT                     : 0x00 Raw Hex
STATUS_IOUT                     : 0x00 Raw Hex
Output voltage                  : 0x3aee Raw Hex
Output current                  : 0x8000 Raw Hex

VDD_33      Voltage Output      :   3.45 Volts
Page                            : 0x11 Raw Hex
OPERATION                       : 0x00 Raw Hex
On Off Config                   : 0x14 Raw Hex
VOUT mode                       : 0x14 Raw Hex
VOUT command                    : 0x34cd Raw Hex
VOUT margin hi                  : 0x3771 Raw Hex
VOUT margin lo                  : 0x3229 Raw Hex
VOUT scale                      : 0xb266 Raw Hex
VOUT OV fault limit             : 0x3cb8 Raw Hex
VOUT OV warn limit              : 0x3a14 Raw Hex
VOUT UV warn limit              : 0x2f85 Raw Hex
VOUT UV fault limit             : 0x2ce1 Raw Hex
IOUT OC fault limit             : 0x8000 Raw Hex
IOUT OC warn limit              : 0x8000 Raw Hex
Power good on                   : 0x2f85 Raw Hex
Power good off                  : 0x2ce1 Raw Hex
On delay                        : 0xba00 Raw Hex
On time limit                   : 0xda80 Raw Hex
Off delay                       : 0xba00 Raw Hex
Off time limit                  : 0x8000 Raw Hex
STATUS_VOUT                     : 0x00 Raw Hex
STATUS_IOUT                     : 0x00 Raw Hex
Output voltage                  : 0x372a Raw Hex
Output current                  : 0x8000 Raw Hex

VPP_CD      Voltage Output      :   2.55 Volts
Page                            : 0x12 Raw Hex
OPERATION                       : 0x00 Raw Hex
On Off Config                   : 0x14 Raw Hex
VOUT mode                       : 0x13 Raw Hex
VOUT command                    : 0x5000 Raw Hex
VOUT margin hi                  : 0x5400 Raw Hex
VOUT margin lo                  : 0x4c00 Raw Hex
VOUT scale                      : 0xb333 Raw Hex
VOUT OV fault limit             : 0x5c00 Raw Hex
VOUT OV warn limit              : 0x5800 Raw Hex
VOUT UV warn limit              : 0x4800 Raw Hex
VOUT UV fault limit             : 0x4400 Raw Hex
IOUT OC fault limit             : 0x8000 Raw Hex
IOUT OC warn limit              : 0x8000 Raw Hex
Power good on                   : 0x4800 Raw Hex
Power good off                  : 0x4400 Raw Hex
```

```
On delay                        : 0xba00 Raw Hex
On time limit                   : 0xda80 Raw Hex
Off delay                       : 0xba00 Raw Hex
Off time limit                  : 0x8000 Raw Hex
STATUS_VOUT                     : 0x00 Raw Hex
STATUS_IOUT                     : 0x00 Raw Hex
Output voltage                  : 0x51c1 Raw Hex
Output current                  : 0x8000 Raw Hex

VPP_GH      Voltage Output      :   2.55 Volts
Page                            : 0x13 Raw Hex
OPERATION                       : 0x00 Raw Hex
On Off Config                   : 0x14 Raw Hex
VOUT mode                       : 0x13 Raw Hex
VOUT command                    : 0x5000 Raw Hex
VOUT margin hi                  : 0x5400 Raw Hex
VOUT margin lo                  : 0x4c00 Raw Hex
VOUT scale                      : 0xb333 Raw Hex
VOUT OV fault limit             : 0x5c00 Raw Hex
VOUT OV warn limit              : 0x5800 Raw Hex
VOUT UV warn limit              : 0x4800 Raw Hex
VOUT UV fault limit             : 0x4400 Raw Hex
IOUT OC fault limit             : 0x8000 Raw Hex
IOUT OC warn limit              : 0x8000 Raw Hex
Power good on                   : 0x4800 Raw Hex
Power good off                  : 0x4400 Raw Hex
On delay                        : 0xba00 Raw Hex
On time limit                   : 0xda80 Raw Hex
Off delay                       : 0xba00 Raw Hex
Off time limit                  : 0x8000 Raw Hex
STATUS_VOUT                     : 0x00 Raw Hex
STATUS_IOUT                     : 0x00 Raw Hex
Output voltage                  : 0x51bc Raw Hex
Output current                  : 0x8000 Raw Hex

VDDIO_MEM_CD Voltage Output     :   1.23 Volts
Page                            : 0x14 Raw Hex
OPERATION                       : 0x00 Raw Hex
On Off Config                   : 0x14 Raw Hex
VOUT mode                       : 0x12 Raw Hex
VOUT command                    : 0x4ccd Raw Hex
VOUT margin hi                  : 0x50a4 Raw Hex
VOUT margin lo                  : 0x48f6 Raw Hex
VOUT scale                      : 0xba00 Raw Hex
VOUT OV fault limit             : 0x5852 Raw Hex
VOUT OV warn limit              : 0x547b Raw Hex
VOUT UV warn limit              : 0x451f Raw Hex
VOUT UV fault limit             : 0x4148 Raw Hex
IOUT OC fault limit             : 0x8000 Raw Hex
IOUT OC warn limit              : 0x8000 Raw Hex
Power good on                   : 0x451f Raw Hex
Power good off                  : 0x4148 Raw Hex
On delay                        : 0xba00 Raw Hex
On time limit                   : 0xda80 Raw Hex
Off delay                       : 0xba00 Raw Hex
Off time limit                  : 0x8000 Raw Hex
STATUS_VOUT                     : 0x00 Raw Hex
STATUS_IOUT                     : 0x00 Raw Hex
Output voltage                  : 0x4ef4 Raw Hex
Output current                  : 0x8000 Raw Hex

VDDIO_MEM_GH Voltage Output     :   1.23 Volts
Page                            : 0x15 Raw Hex
OPERATION                       : 0x00 Raw Hex
```

```
On Off Config                  : 0x14 Raw Hex
VOUT mode                      : 0x12 Raw Hex
VOUT command                   : 0x4ccd Raw Hex
VOUT margin hi                 : 0x50a4 Raw Hex
VOUT margin lo                 : 0x48f6 Raw Hex
VOUT scale                     : 0xba00 Raw Hex
VOUT OV fault limit            : 0x5852 Raw Hex
VOUT OV warn limit             : 0x547b Raw Hex
VOUT UV warn limit             : 0x451f Raw Hex
VOUT UV fault limit            : 0x4148 Raw Hex
IOUT OC fault limit            : 0x8000 Raw Hex
IOUT OC warn limit             : 0x8000 Raw Hex
Power good on                  : 0x451f Raw Hex
Power good off                 : 0x4148 Raw Hex
On delay                       : 0xba00 Raw Hex
On time limit                  : 0xda80 Raw Hex
Off delay                      : 0xba00 Raw Hex
Off time limit                 : 0x8000 Raw Hex
STATUS_VOUT                    : 0x00 Raw Hex
STATUS_IOUT                    : 0x00 Raw Hex
Output voltage                 : 0x4ef4 Raw Hex
Output current                 : 0x8000 Raw Hex

1.2V_MGTAVTT_KC Voltage Output     :   1.23 Volts
Page                           : 0x16 Raw Hex
OPERATION                      : 0x00 Raw Hex
On Off Config                  : 0x14 Raw Hex
VOUT mode                      : 0x12 Raw Hex
VOUT command                   : 0x4ccd Raw Hex
VOUT margin hi                 : 0x50a4 Raw Hex
VOUT margin lo                 : 0x48f6 Raw Hex
VOUT scale                     : 0xba00 Raw Hex
VOUT OV fault limit            : 0x5852 Raw Hex
VOUT OV warn limit             : 0x547b Raw Hex
VOUT UV warn limit             : 0x451f Raw Hex
VOUT UV fault limit            : 0x4148 Raw Hex
IOUT OC fault limit            : 0x8000 Raw Hex
IOUT OC warn limit             : 0x8000 Raw Hex
Power good on                  : 0x451f Raw Hex
Power good off                 : 0x4148 Raw Hex
On delay                       : 0xba00 Raw Hex
On time limit                  : 0xda80 Raw Hex
Off delay                      : 0xba00 Raw Hex
Off time limit                 : 0x8000 Raw Hex
STATUS_VOUT                    : 0x00 Raw Hex
STATUS_IOUT                    : 0x00 Raw Hex
Output voltage                 : 0x4ee0 Raw Hex
Output current                 : 0x8000 Raw Hex

0.9V_NTX_EN Voltage Output     :   0.00 Volts
Page                           : 0x17 Raw Hex
OPERATION                      : 0x00 Raw Hex
On Off Config                  : 0x14 Raw Hex
VOUT mode                      : 0x14 Raw Hex
VOUT command                   : 0x0000 Raw Hex
VOUT margin hi                 : 0x0000 Raw Hex
VOUT margin lo                 : 0x0000 Raw Hex
VOUT scale                     : 0xba00 Raw Hex
VOUT OV fault limit            : 0x0000 Raw Hex
VOUT OV warn limit             : 0x0000 Raw Hex
VOUT UV warn limit             : 0x0000 Raw Hex
VOUT UV fault limit            : 0x0000 Raw Hex
IOUT OC fault limit            : 0x8000 Raw Hex
IOUT OC warn limit             : 0x8000 Raw Hex
```

```
Power good on                 : 0x0000 Raw Hex
Power good off                : 0x0000 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
Output voltage                : 0x0000 Raw Hex
Output current                : 0x8000 Raw Hex

1.5V_NTX_EN Voltage Output    :   0.00 Volts
Page                          : 0x18 Raw Hex
OPERATION                     : 0x00 Raw Hex
On Off Config                 : 0x14 Raw Hex
VOUT mode                     : 0x14 Raw Hex
VOUT command                  : 0x0000 Raw Hex
VOUT margin hi                : 0x0000 Raw Hex
VOUT margin lo                : 0x0000 Raw Hex
VOUT scale                    : 0xba00 Raw Hex
VOUT OV fault limit           : 0x0000 Raw Hex
VOUT OV warn limit            : 0x0000 Raw Hex
VOUT UV warn limit            : 0x0000 Raw Hex
VOUT UV fault limit           : 0x0000 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x0000 Raw Hex
Power good off                : 0x0000 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
Output voltage                : 0x0000 Raw Hex
Output current                : 0x8000 Raw Hex

1.8V_PHY_EN Voltage Output    :   0.00 Volts
Page                          : 0x19 Raw Hex
OPERATION                     : 0x00 Raw Hex
On Off Config                 : 0x14 Raw Hex
VOUT mode                     : 0x14 Raw Hex
VOUT command                  : 0x0000 Raw Hex
VOUT margin hi                : 0x0000 Raw Hex
VOUT margin lo                : 0x0000 Raw Hex
VOUT scale                    : 0xba00 Raw Hex
VOUT OV fault limit           : 0x0000 Raw Hex
VOUT OV warn limit            : 0x0000 Raw Hex
VOUT UV warn limit            : 0x0000 Raw Hex
VOUT UV fault limit           : 0x0000 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x0000 Raw Hex
Power good off                : 0x0000 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
Output voltage                : 0x0000 Raw Hex
Output current                : 0x8000 Raw Hex

1.0V_PHY_EN Voltage Output    :   0.00 Volts
```

```
Page                            : 0x1a Raw Hex
OPERATION                       : 0x00 Raw Hex
On Off Config                   : 0x14 Raw Hex
VOUT mode                       : 0x14 Raw Hex
VOUT command                    : 0x0000 Raw Hex
VOUT margin hi                  : 0x0000 Raw Hex
VOUT margin lo                  : 0x0000 Raw Hex
VOUT scale                      : 0xba00 Raw Hex
VOUT OV fault limit             : 0x0000 Raw Hex
VOUT OV warn limit              : 0x0000 Raw Hex
VOUT UV warn limit              : 0x0000 Raw Hex
VOUT UV fault limit             : 0x0000 Raw Hex
IOUT OC fault limit             : 0x8000 Raw Hex
IOUT OC warn limit              : 0x8000 Raw Hex
Power good on                   : 0x0000 Raw Hex
Power good off                  : 0x0000 Raw Hex
On delay                        : 0xba00 Raw Hex
On time limit                   : 0xda80 Raw Hex
Off delay                       : 0xba00 Raw Hex
Off time limit                  : 0x8000 Raw Hex
STATUS_VOUT                     : 0x00 Raw Hex
STATUS_IOUT                     : 0x00 Raw Hex
Output voltage                  : 0x0000 Raw Hex
Output current                  : 0x8000 Raw Hex

VDDCR_SOC_EN Voltage Output     :   0.00 Volts
Page                            : 0x1b Raw Hex
OPERATION                       : 0x00 Raw Hex
On Off Config                   : 0x14 Raw Hex
VOUT mode                       : 0x14 Raw Hex
VOUT command                    : 0x0000 Raw Hex
VOUT margin hi                  : 0x0000 Raw Hex
VOUT margin lo                  : 0x0000 Raw Hex
VOUT scale                      : 0xba00 Raw Hex
VOUT OV fault limit             : 0x0000 Raw Hex
VOUT OV warn limit              : 0x0000 Raw Hex
VOUT UV warn limit              : 0x0000 Raw Hex
VOUT UV fault limit             : 0x0000 Raw Hex
IOUT OC fault limit             : 0x8000 Raw Hex
IOUT OC warn limit              : 0x8000 Raw Hex
Power good on                   : 0x0000 Raw Hex
Power good off                  : 0x0000 Raw Hex
On delay                        : 0xba00 Raw Hex
On time limit                   : 0xda80 Raw Hex
Off delay                       : 0xba00 Raw Hex
Off time limit                  : 0x8000 Raw Hex
STATUS_VOUT                     : 0x00 Raw Hex
STATUS_IOUT                     : 0x00 Raw Hex
Output voltage                  : 0x0000 Raw Hex
Output current                  : 0x8000 Raw Hex

VDDCR_CPU_EN Voltage Output     :   0.00 Volts
Page                            : 0x1c Raw Hex
OPERATION                       : 0x00 Raw Hex
On Off Config                   : 0x14 Raw Hex
VOUT mode                       : 0x14 Raw Hex
VOUT command                    : 0x0000 Raw Hex
VOUT margin hi                  : 0x0000 Raw Hex
VOUT margin lo                  : 0x0000 Raw Hex
VOUT scale                      : 0xba00 Raw Hex
VOUT OV fault limit             : 0x0000 Raw Hex
VOUT OV warn limit              : 0x0000 Raw Hex
VOUT UV warn limit              : 0x0000 Raw Hex
VOUT UV fault limit             : 0x0000 Raw Hex
```

```
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x0000 Raw Hex
Power good off                : 0x0000 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
Output voltage                : 0x0000 Raw Hex
Output current                : 0x8000 Raw Hex

VDD_3.3_S5_EN Voltage Output     :   0.00 Volts
Page                          : 0x1d Raw Hex
OPERATION                     : 0x00 Raw Hex
On Off Config                 : 0x14 Raw Hex
VOUT mode                     : 0x14 Raw Hex
VOUT command                  : 0x0000 Raw Hex
VOUT margin hi                : 0x0000 Raw Hex
VOUT margin lo                : 0x0000 Raw Hex
VOUT scale                    : 0xba00 Raw Hex
VOUT OV fault limit           : 0x0000 Raw Hex
VOUT OV warn limit            : 0x0000 Raw Hex
VOUT UV warn limit            : 0x0000 Raw Hex
VOUT UV fault limit           : 0x0000 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x0000 Raw Hex
Power good off                : 0x0000 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
Output voltage                : 0x0000 Raw Hex
Output current                : 0x8000 Raw Hex

3.3_NIC_EN  Voltage Output    :   0.00 Volts
Page                          : 0x1e Raw Hex
OPERATION                     : 0x00 Raw Hex
On Off Config                 : 0x14 Raw Hex
VOUT mode                     : 0x14 Raw Hex
VOUT command                  : 0x0000 Raw Hex
VOUT margin hi                : 0x0000 Raw Hex
VOUT margin lo                : 0x0000 Raw Hex
VOUT scale                    : 0xba00 Raw Hex
VOUT OV fault limit           : 0x0000 Raw Hex
VOUT OV warn limit            : 0x0000 Raw Hex
VOUT UV warn limit            : 0x0000 Raw Hex
VOUT UV fault limit           : 0x0000 Raw Hex
IOUT OC fault limit           : 0x8000 Raw Hex
IOUT OC warn limit            : 0x8000 Raw Hex
Power good on                 : 0x0000 Raw Hex
Power good off                : 0x0000 Raw Hex
On delay                      : 0xba00 Raw Hex
On time limit                 : 0xda80 Raw Hex
Off delay                     : 0xba00 Raw Hex
Off time limit                : 0x8000 Raw Hex
STATUS_VOUT                   : 0x00 Raw Hex
STATUS_IOUT                   : 0x00 Raw Hex
Output voltage                : 0x0000 Raw Hex
Output current                : 0x8000 Raw Hex
```

```
  5V_EN       Voltage Output     :   0.00 Volts
  Page                           : 0x1f Raw Hex
  OPERATION                      : 0x00 Raw Hex
  On Off Config                  : 0x14 Raw Hex
  VOUT mode                      : 0x14 Raw Hex
  VOUT command                   : 0x0000 Raw Hex
  VOUT margin hi                 : 0x0000 Raw Hex
  VOUT margin lo                 : 0x0000 Raw Hex
  VOUT scale                     : 0xba00 Raw Hex
  VOUT OV fault limit            : 0x0000 Raw Hex
  VOUT OV warn limit             : 0x0000 Raw Hex
  VOUT UV warn limit             : 0x0000 Raw Hex
  VOUT UV fault limit            : 0x0000 Raw Hex
  IOUT OC fault limit            : 0x8000 Raw Hex
  IOUT OC warn limit             : 0x8000 Raw Hex
  Power good on                  : 0x0000 Raw Hex
  Power good off                 : 0x0000 Raw Hex
  On delay                       : 0xba00 Raw Hex
  On time limit                  : 0xda80 Raw Hex
  Off delay                      : 0xba00 Raw Hex
  Off time limit                 : 0x8000 Raw Hex
  STATUS_VOUT                    : 0x00 Raw Hex
  STATUS_IOUT                    : 0x00 Raw Hex
  Output voltage                 : 0x0001 Raw Hex
  Output current                 : 0x8000 Raw Hex


 PSEQ log

Fault Info Reg (0xb5):
12 9a 00 00 4f a9 33 48 7f ff ff ff ff ff ff ff 7f ff

Fault Rails Warning Reg (0xb6):
20 00 00 00 00 00 00 00 7f ff ff ff ff ff ff ff
7f ff ff ff ff ff ff ff 7f ff ff ff ff ff ff ff


Rails Value Reg (0xb7) page 0:
07 00 d0 2f 00 00 00

Rails Value Reg (0xb7) page 1:
07 00 45 34 00 00 00

Rails Value Reg (0xb7) page 2:
07 00 54 4c 00 00 00

Rails Value Reg (0xb7) page 3:
07 00 7d 4f 00 00 00

Rails Value Reg (0xb7) page 4:
07 00 10 36 00 00 00

Rails Value Reg (0xb7) page 5:
07 00 6c 39 00 00 00

Rails Value Reg (0xb7) page 6:
07 00 44 39 00 00 00

Rails Value Reg (0xb7) page 7:
07 00 18 4c 00 00 00

Rails Value Reg (0xb7) page 8:
07 00 22 39 00 00 00
```

```
Rails Value Reg (0xb7) page 9:
07 00 80 3e 00 00 00

Rails Value Reg (0xb7) page 10:
07 00 80 3e 00 00 00

Rails Value Reg (0xb7) page 11:
07 00 12 39 00 00 00

Rails Value Reg (0xb7) page 12:
07 00 a0 39 00 00 00

Rails Value Reg (0xb7) page 13:
07 00 b8 3f 00 00 00

Rails Value Reg (0xb7) page 14:
07 00 36 39 00 00 00

Rails Value Reg (0xb7) page 15:
07 00 3c 39 00 00 00

Rails Value Reg (0xb7) page 16:
07 00 22 39 00 00 00

Rails Value Reg (0xb7) page 17:
07 00 74 35 00 00 00

Rails Value Reg (0xb7) page 18:
07 00 3e 4f 00 00 00

Rails Value Reg (0xb7) page 19:
07 00 37 4f 00 00 00

Rails Value Reg (0xb7) page 20:
07 00 7c 4c 00 00 00

Rails Value Reg (0xb7) page 21:
07 00 7c 4c 00 00 00

Rails Value Reg (0xb7) page 22:
07 00 74 4c 00 00 00

Rails Value Reg (0xb7) page 23:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 24:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 25:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 26:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 27:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 28:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 29:
07 00 00 00 00 00 00
```

```
Rails Value Reg (0xb7) page 30:
07 00 00 00 00 00 00

Rails Value Reg (0xb7) page 31:
07 00 01 00 00 00 00

Logged Fault Reg (0xea):
25 03 00 00 08 02 82 00 7f ff ff ff ff ff ff ff
7f ff ff ff ff ff ff ff 7f ff ff ff ff ff ff ff
00 00 00 00 00

Fault Details Index Reg (0xeb):
00 64

Fault Details Reg (0xec) index 0:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 1:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 2:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 3:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 4:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 5:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 6:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 7:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 8:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 9:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 10:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 11:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 12:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 13:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 14:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 15:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 16:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff
```

```
Fault Details Reg (0xec) index 17:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 18:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 19:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 20:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 21:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 22:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 23:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 24:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 25:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 26:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 27:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 28:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 29:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 30:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 31:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 32:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 33:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 34:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 35:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 36:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 37:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff
```

```
Fault Details Reg (0xec) index 38:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 39:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 40:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 41:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 42:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 43:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 44:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 45:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 46:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 47:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 48:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 49:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 50:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 51:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 52:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 53:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 54:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 55:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 56:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 57:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 58:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 59:
```

```
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 60:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 61:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 62:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 63:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 64:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 65:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 66:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 67:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 68:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 69:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 70:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 71:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 72:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 73:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 74:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 75:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 76:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 77:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 78:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 79:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 80:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff
```

```
Fault Details Reg (0xec) index 81:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 82:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 83:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 84:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 85:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 86:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 87:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 88:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 89:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 90:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 91:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 92:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 93:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 94:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 95:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 96:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 97:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 98:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Fault Details Reg (0xec) index 99:
0c 02 66 2c 4e 88 04 e9 7f ff ff ff

Logged Page Peaks Reg (0xed) page 0:
05 00 4b 31 00

Logged Page Peaks Reg (0xed) page 1:
05 00 fa 35 00
```

```
Logged Page Peaks Reg (0xed) page 2:
05 00 08 4f 00

Logged Page Peaks Reg (0xed) page 3:
05 00 25 52 00

Logged Page Peaks Reg (0xed) page 4:
05 00 fc 37 00

Logged Page Peaks Reg (0xed) page 5:
05 00 58 3b 00

Logged Page Peaks Reg (0xed) page 6:
05 00 24 3b 00

Logged Page Peaks Reg (0xed) page 7:
05 00 e8 4e 00

Logged Page Peaks Reg (0xed) page 8:
05 00 06 3b 00

Logged Page Peaks Reg (0xed) page 9:
05 00 c8 41 00

Logged Page Peaks Reg (0xed) page 10:
05 00 c8 41 00

Logged Page Peaks Reg (0xed) page 11:
05 00 16 3b 00

Logged Page Peaks Reg (0xed) page 12:
05 00 d8 3b 00

Logged Page Peaks Reg (0xed) page 13:
05 00 dc 41 00

Logged Page Peaks Reg (0xed) page 14:
05 00 10 3b 00

Logged Page Peaks Reg (0xed) page 15:
05 00 1c 3b 00

Logged Page Peaks Reg (0xed) page 16:
05 00 2a 3b 00

Logged Page Peaks Reg (0xed) page 17:
05 00 3e 37 00

Logged Page Peaks Reg (0xed) page 18:
05 00 ce 51 00

Logged Page Peaks Reg (0xed) page 19:
05 00 ce 51 00

Logged Page Peaks Reg (0xed) page 20:
05 00 4c 4f 00

Logged Page Peaks Reg (0xed) page 21:
05 00 58 4f 00

Logged Page Peaks Reg (0xed) page 22:
05 00 44 4f 00

Logged Page Peaks Reg (0xed) page 23:
```

```
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 24:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 25:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 26:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 27:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 28:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 29:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 30:
05 00 00 00 00

Logged Page Peaks Reg (0xed) page 31:
05 00 00 00 00

Fault Detail Enable Reg (0xef):
25 ff ff ff f7 fd 07 07 7f ff ff ff ff ff ff ff
7f ff ff ff ff ff ff ff 7f ff ff ff ff ff ff ff
00 00 00 00 00


*************** EPM Data ***************
EPM0 is present
EPM0 Card power is okay
EPM0 Card is ready
EPM0 temperature is 32 degrees Celsius

***************  Fans  ***************
FanMod 1 Fan 1 rotating
FanMod 1 Fan 1 RPM = 21720
FanMod 1 Fan 2 rotating
FanMod 1 Fan 2 RPM = 19380
FanMod 1 Fan 3 rotating
FanMod 1 Fan 3 RPM = 21900
FanMod 1 Fan 4 rotating
FanMod 1 Fan 4 RPM = 19320
FanMod 2 Fan 1 rotating
FanMod 2 Fan 1 RPM = 21720
FanMod 2 Fan 2 rotating
FanMod 2 Fan 2 RPM = 19260
FanMod 2 Fan 3 rotating
FanMod 2 Fan 3 RPM = 21540
FanMod 2 Fan 4 rotating
FanMod 2 Fan 4 RPM = 19440

Environmental Fan FPGA Control   : 0x00000107
Environmental Fan Status         : 0x00000003
Environmental Fan Enable Control : 0x00110700
Fanmod1 PWM Slope                : 0x00000108
Fanmod1 Speed                    : 0x000003e8
Fanmod1 Smartfan Control         : 0x00000000
Fanmod1 Smartfan Status          : 0x00540000
Fanmod1 Smartfan PWM             : 0x000000f0
```

```
Fanmod1 Smartfan Debug           : 0x00003aee
Fanmod2 PWM Slope                : 0x00000108
Fanmod2 Speed                    : 0x000003e8
Fanmod2 Smartfan Control         : 0x00000000
Fanmod2 Smartfan Status          : 0x00540000
Fanmod2 Smartfan PWM             : 0x000000f0
Fanmod2 Smartfan Debug           : 0x00003b14
T2/T1 Temp                       : 0x0088007c
T4/T3 Temp                       : 0x0098008c
T6/T5 Temp                       : 0x00a8009c
T8/T7 Temp                       : 0x00b800ac
Level 1 Speed                    : 0x000004b0
Level 2 Speed                    : 0x00000550
Level 3 Speed                    : 0x000005b4
Level 4 Speed                    : 0x00000640
Level 5 Speed                    : 0x000007d0
Minimal Speed Threshold          : 0x00000054
Fan Controller Speed = automatic

***************  Disks  ***************

***************  SSD Data  ***************
```

Commandes associées

Commande	Description
show server environment	Affiche les informations sur le matériel du serveur.

show eth-uplink

Pour afficher les informations sur la liaison ascendante Ethernet, utilisez la commande **show eth-uplink**.

show eth-uplink [**detail** | **expand** | **fsm**]

Description de la syntaxe

detail	(Facultatif) Affiche les détails sur la liaison ascendante Ethernet.
expand	(Facultatif) Affiche les informations développées sur la liaison ascendante Ethernet.
fsm status	(Facultatif) Affiche l'état de la machine à états finis (FSM).

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

FXOS ne prend pas en charge la détection de liaison unidirectionnelle (UDLD); ignorer toute référence à UDLD.

Exemple

Cet exemple montre comment afficher les informations développées sur liaison ascendante Ethernet :

```
firepower# show eth-uplink expand

Ethernet Uplink:
    Mode          MAC Table Aging Time (dd:hh:mm:ss) VLAN Port Count Optimization
    ------------- ---------------------------------- ----------------------------
    Security Node 00:04:01:40                        Disabled
firepower# show eth-uplink expand

Ethernet Uplink:
    Mode: Security Node
    MAC Table Aging Time (dd:hh:mm:ss): 00:04:01:40
    VLAN Port Count Optimization: Disabled

    Ethernet Link Profile:
        Name       UDLD link policy name Oper UDLD link policy name
        ---------- --------------------- --------------------------
        default    default               fabric/lan/udld-link-pol-default

    Fabric:
        Fabric ID: A

        Interface:
            Port Name: Ethernet1/1
            Port Type: Mgmt
            Admin State: Enabled
            Oper State: Link Down
            State Reason: Link failure or not-connected

    <--- intevening lines removed for brevity --->
```

```
            Port Name: Ethernet2/6
            Port Type: Data
            Admin State: Disabled
            Oper State: Admin Down
            State Reason: Administratively down

            Port Name: Ethernet2/7
            Port Type: Data
            Admin State: Disabled
            Oper State: Sfp Not Present
            State Reason: Unknown

            Port Name: Ethernet2/8
            Port Type: Data
            Admin State: Disabled
            Oper State: Sfp Not Present
            State Reason: Unknown

        Port Channel:
            Port Channel Id: 48
            Name: Port-channel48
            Port Type: Cluster
            Admin State: Enabled
            Oper State: Failed
            State Reason: No operational members

            Member Port:
                Port Name       Membership         Oper State       State Reason
                --------------- ------------------ ---------------- ------------
                Ethernet1/5     Down               Link Down        Link failure or
not-connected
                Ethernet1/6     Down               Link Down        Link failure or
not-connected

    Stats Threshold Policy:
        Name: default
        Full Name: fabric/lan/thr-policy-default
        Policy Owner: Local

    UDLD link policy:
        Name       Admin State UDLD mode
        ---------- ----------- ---------
        default    Disabled    Normal
firepower#
```

Commandes associées

Commande	Description
scope eth-uplink	Permet d'accéder au mode liaison ascendante Ethernet.

show event

Pour afficher des informations sur les événements du FSM, utilisez la commande **show event**.

show event [*event_id* | **detail**]

Description de la syntaxe

event_id	(Facultatif) Affiche des informations sur un événement spécifique.
detail	(Facultatif) Affiche des informations détaillées sur tous les événements.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous pouvez utiliser la commande **show event** sans arguments ni mots clés pour afficher une liste d'événements.

Exemple

Cet exemple montre comment afficher une liste d'événements :

```
FP9300-A# show event
Creation Time            ID       Code     Description
------------------------ -------- -------- -----------
2025-12-23T04:17:00.678    176144 E4195253 [FSM:STAGE:SKIP]: keyring configuration on
secondary(FSM-STAGE:sam:dme:PkiEpUpdateEp:SetKeyRingPeer)
2025-12-23T04:17:00.678    176145 E4195253 [FSM:STAGE:END]: keyring configuration on
secondary(FSM-STAGE:sam:dme:PkiEpUpdateEp:SetKeyRingPeer)
2025-12-23T04:17:00.678    176146 E4197130 [FSM:STAGE:SKIP]: post processing after keyring
 configration on primary(FSM-STAGE:sam:dme:PkiEpUpdateEp:PostSetKeyRingLocal)
2025-12-23T04:17:00.678    176147 E4197130 [FSM:STAGE:END]: post processing after keyring
configration on primary(FSM-STAGE:sam:dme:PkiEpUpdateEp:PostSetKeyRingLocal)
2025-12-23T04:17:00.678    176148 E4197131 [FSM:STAGE:SKIP]: post processing after keyring
 configuration on secondary(FSM-STAGE:sam:dme:PkiEpUpdateEp:PostSetKeyRingPeer)
2025-12-23T04:17:00.678    176149 E4197131 [FSM:STAGE:END]: post processing after keyring
configuration on secondary(FSM-STAGE:sam:dme:PkiEpUpdateEp:PostSetKeyRingPeer)
2025-12-23T04:17:00.678    176150 E4195525 [FSM:END]: keyring
configuration(FSM:sam:dme:PkiEpUpdateEp)
2025-12-23T04:17:00.677   176142 E4195252 [FSM:STAGE:STALE-SUCCESS]: keyring configuration
 on primary(FSM-STAGE:sam:dme:PkiEpUpdateEp:SetKeyRingLocal)

    <--- remaining lines removed for brevity --->

FP9300-A#
```

Commandes associées

Commande	Description
show sel	Affiche le contenu du journal des événements système (SEL) d'un serveur.

show export-config detail

Pour afficher les configurations d'exportation en détail, utilisez la commande **show export-config detail**.

show export-config [**detail**]

Description de la syntaxe

Detail	Affiche les informations détaillées sur la configuration d'exportation.

Modes de commande

scope system

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope system.

Exemple

Cet exemple montre les informations de configuration d'exportation.

```
Firepower # scope system
Firepower /system #
Firepower /system # export-config
scp://<user>@10.196.154.20:/auto/stg_03/ssp/92.14.2/92.14.2.4/final/<config
.txt> enabled
Password:
Firepower /system/export-config* # commit-buffer
Firepower /system/export-config # exit
Firepower /system # show export-config detail
Export Configuration Task:
Hostname: 10.196.154.20
Remote File: :/auto/stg_03/ssp/92.14.2/92.14.2.4/final/<config.txt>
User: user
Protocol: Scp
Admin State: Disabled
Status: Pass
Description:
Port: Default
Current Task: internal system backup(FSM-
STAGE:sam:dme:MgmtBackupBackup:upload)
Note: Any issue/errors regarding keys while committing the buffer. Please
set the encryption key as shown below.
```

Définition d'une clé de chiffrement pour l'importation et l'exportation de la configuration

```
Firepower# scope security
Firepower /security # set password-encryption-key
Enter a key:
Confirm the key:
Warning: Please make note of the encryption key configured.
If you change the key, importing configurations that were exported with the previous key
will fail, because Import and Export requires the same encryption key on
the system.
Firepower /security* # commit-buffer
```

show fabric

Pour afficher les renseignements sur le câblage de la structure, utilisez la commande **show fabric** en mode câblage.

show fabric [**breakout** | **detail** | **expand**]

Description de la syntaxe

a	(Facultatif) Affiche les informations de câblage spécifiques à la structure A. **Remarque** Il n'existe pas de structure B.
detail	(Facultatif) Affiche des informations détaillées sur le câblage. Le mot clé **expand** est disponible avec cette option.
expand	(Facultatif) Affiche des informations développées sur le câblage y compris les répartitions de port. Le mot clé **detail** est disponible avec cette option.

Modes de commande

scope cabling/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande affiche des informations générales sur le câblage de la structure.

Exemple

Cet exemple montre comment afficher les informations de câblage développées :

```
firepower# scope cabling
firepower /cabling # show fabric expand

cabling on switch:
    Id: A

    port breakout:
        Slot ID    Port ID    breakout type
        ---------- ---------- -------------
                 3          1 10g 4x
                 3          2 10g 4x
firepower /cabling #
```

Commandes associées

Commande	Description
create breakout	Crée une répartition d'interface.

show fabric-interconnect

Pour afficher les informations sur l'interconnexion de structures, utilisez la commande **show fabric-interconnect**.

show fabric-interconnect [**a** | **b** | **detail** | **environment** | **firmware** | **fsm** | **inventory** | **mac-aging** | **mode** | **version**]

Description de la syntaxe

a	(Facultatif) Affiche les informations sur interconnexion de structures pour la structure A. Utilisez le mot clé facultatif **detail** pour afficher les informations détaillées sur la structure. **Remarque** Il n'existe qu'une seule structure étiquetée par A. Il n'est donc pas nécessaire de saisir ce mot clé.
b	(Facultatif) Ne pas utiliser : il n'existe pas de structure B.
detail	(Facultatif) Affiche les informations détaillées sur l'interconnexion de structures.
environment	(Facultatif) Affiche les informations sur les cartes de structure installées. Ces mots clés facultatifs sont disponibles : • **a** : affiche les informations sur la structure A. Il n'existe qu'une seule structure et ce mot clé est donc facultatif. • **b** : ne pas utiliser, il n'existe pas de structure B. • **detail** : affiche les informations détaillées sur l'environnement. • **expand** : affiche les informations développées sur l'environnement. Le mot clé **detail** est disponible avec cette option. • **fan** : affiche les informations propres au ventilateur. Les mots clés **detail** et **psu**sont disponibles avec cette option. • **psu** : affiche les informations propres au bloc d'alimentation. Les mots clés **detail** et **fan**sont disponibles avec cette option.
firmware	(Facultatif) Affiche les informations sur le micrologiciel.
fsm status	(Facultatif) Affiche les informations sur l'état de la machine à états finis (FSM).
inventory	(Facultatif) Affiche les informations matérielles de base sur la structure. Les mots clés **detail**, **expand** et **id** sont disponibles avec cette option.
mac-aging	(Facultatif) Affiche la durée de vie du tableau MAC.
mode	(Facultatif) Affiche les informations sur le mode interconnexion de structure.
version	(Facultatif) Affiche les informations sur la version du micrologiciel.

Modes de commande Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation Cette commande ne nécessite pas de licence.

Exemple

Cet exemple montre comment afficher les informations sur l'interconnexion de structures de base :

```
FP9300-A# show fabric-interconnect

Fabric Interconnect:
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
 Prefix Operability
    ---- --------------- --------------- --------------- ---------------- ----------------
 ------ -----------
    A    10.201.153.14   10.201.153.1    255.255.255.0   ::               ::
 64     Operable
FP9300-A#
```

Commandes associées

Commande	Description
scope fabric-interconnect	Permet d'accéder au mode interconnexion de structure.

show fan-module

Pour afficher les informations sur les modules de ventilation installés, utilisez la commande **show fan-module** en mode châssis.

show fan-module [[**1** *module_id*] | **detail** | **expand**]

Description de la syntaxe

tray_id module_id	(Facultatif) Pour afficher les informations sur un module spécifique, utilisez *tray_id module_id* pour identifier le module. *tray_id* correspond toujours à 1; *module_id* peut être compris entre 1 et 8.
detail	(Facultatif) Utilisez ce mot clé pour afficher les informations détaillées sur l'état de chaque module de ventilation.
expand	(Facultatif) Utilisez ce mot clé pour afficher les informations sur l'état global de chaque module de ventilation.

Modes de commande

scope chassis/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous pouvez utiliser cette commande sans arguments ni mots clés pour afficher les informations de base sur le module de ventilation.

Exemple

Cet exemple montre comment afficher les informations détaillées sur un module de ventilation spécifique :

```
firepower# scope chassis
firepower /chassis # show fan-module 1 2 detail

Fan Module:
    Tray: 1
    Module: 2
    Overall Status: Operable
    Operability: Operable
    Threshold Status: OK
    Power State: On
    Presence: Equipped
    Thermal Status: OK
    Product Name: Cisco Firepower 9000 Series Fan
    PID: FPR9K-FAN
    VID: 01
    Part Number: 73-17509-01
    Vendor: Cisco Systems Inc
    Serial (SN): NWG194500D8
    HW Revision: 0
    Mfg Date: 2015-11-07T00:00:00.000
firepower /chassis #
```

Commandes associées

Commande	Description
scope fan	Cible un ventilateur spécifique.

show fault

Pour afficher les informations sur les défaillances, utilisez la commande **show fault**.

show fault [*ID* | **cause** | **detail** | **severity** | **suppressed**]

Description de la syntaxe

ID	(Facultatif) Affiche les informations sur la défaillance indiquée uniquement.
cause *label*	(Facultatif) Affiche les défaillances avec l'étiquette de cause spécifiée; par exemple, `set-user-local-failed`.
detail	(Facultatif) Affiche des informations détaillées sur chaque défaillance.
severity {**cleared** | **condition** | **critical** | **info** | **major** | **minor** | **warning**}	(Facultatif) Affiche toutes les défaillances de la gravité spécifiée : • **cleared** • **condition** • **critical** • **info** • **major** • **minor** • **warning**
suppressed	(Facultatif) Affiche toutes les défaillances supprimées. Vous pouvez également ajouter le mot clé **cause** , **detail** ou **severity** .

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.0(1)	Cette commande a été introduite.

Exemple

Cet exemple montre comment afficher la liste de défaillances :

```
FP9300-A# show fault
Severity  Code     Last Transition Time     ID       Description
--------- -------- ----------------------- -------- -----------
Major     F0276    2025-12-16T07:08:08.542     52605 ether port 1/1 on fabric interconnect
 A oper state: link-down, reason: Link failure or not-connected
Major     F0276    2025-12-16T07:08:08.542     78300 ether port 1/5 on fabric interconnect
 A oper state: link-down, reason: Link failure or not-connected
Major     F0276    2025-12-16T07:08:08.542     78301 ether port 1/6 on fabric interconnect
 A oper state: link-down, reason: Link failure or not-connected
Warning   F16683   2025-12-16T07:08:00.670     78430 [FSM:STAGE:FAILED]: internal system
backup(FSM-STAGE:sam:dme:MgmtBackupBackup:upload)
```

```
Warning   F78123   2025-12-16T07:08:00.670     78428 [FSM:STAGE:REMOTE-ERROR]: Result:
end-point-failed Code: unspecified
Message: End point timed out. Check for IP, port, password, disk space or network access
related issues.#(sam:dme:MgmtBackupBackup:upload)

    <--- remaining lines removed for brevity --->

FP9300-A#
```

Commandes associées

Commande	Description
show server status	Affiche les informations sur l'état d'un serveur.

show fc

Pour afficher les informations de classe fc disponibles sur le système, utilisez la commande **show fc**.

show fc [**detail**]

Description de la syntaxe

detail	Répertorie les informations détaillées de classe fc.

Modes de commande

scope eth-server, scope qos

Historique des commandes

Version	Modification
2.3.1	Cette commande a été introduite.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope eth-server, scope qos.

Exemple

Cet exemple montre comment tpo affiche les informations de classe fc de système :

```
Firepower # scope eth-server
Firepower /eth-server # scope qos
Firepower /eth-server/qos # show fc

FC Class:
    Priority: Fc
    Cos: 3
    Weight: 5
    Bw Percent: 50
    Drop: No Drop
    Mtu: Fc
    Admin State: Enabled
```

Cet exemple montre comment afficher les informations détaillées d'une classe Ethernet classifiée :

```
Firepower /eth-server/qos # show eth-classified

Ethernet Classified Class:
    Priority: Platinum
    CoS: 5
    Weight: 10
    BW Percent: Not Applicable
    Drop: No Drop
    MTU: Normal
    Multicast Optimize: No
    Admin State: Disabled

    Priority: Gold
    CoS: 4
    Weight: 9
    BW Percent: Not Applicable
    Drop: Drop
    MTU: Normal
    Multicast Optimize: No
    Admin State: Disabled
```

```
    Priority: Silver
    CoS: 2
    Weight: 8
    BW Percent: Not Applicable
    Drop: Drop
    MTU: Normal
    Multicast Optimize: No
    Admin State: Disabled
```

Cet exemple montre comment afficher les informations détaillées d'une classe Ethernet de type meilleur effort :

```
Firepower /eth-server/qos # show eth-best-effort

Ethernet Best-Effort Class:
    Priority: Best Effort
    Cos: Any
    Weight: 5
    Bw Percent: 50
    Drop: Drop
    Mtu: 9198
    Multicast Optimize: No
    Admin State: Enabled
```

Cet exemple montre comment afficher les informations détaillées d'une classe Ethernet de type meilleur effort :

```
Firepower /eth-server/qos # show eth-best-effort detail

Ethernet Best-Effort Class:
    Priority: Best Effort
    Cos: Any
    Weight: 5
    Bw Percent: 50
    Drop: Drop
    Mtu: 9198
    Multicast Optimize: No
    Admin State: Enabled
```

show fips-mode

Pour afficher les informations sur l'état du mode FIPS (Federal Information Processing Standard), utilisez la commande **show fips-mode**.

show fips-mode

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode sécurité

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

L'activation de la conformité de certification sur un châssis Firepower 4100/9300 ne propage pas automatiquement la conformité à l'un de ses périphériques logiques connectés.

Exemple

Cet exemple montre comment accéder au mode sécurité et afficher les informations sur l'état actuel du mode FIPS :

```
FP9300-A # scope security
FP9300-A /security # show fips-mode
FIPS Mode Admin State: Disabled
FIPS Mode Operational State: Disabled
FP9300-A /security #
```

Commandes associées

Commande	Description
disable fips-mode	Désactive le mode FIPS.
enable fips-mode	Active le mode FIPS.

show firmware

Pour afficher les informations sur le micrologiciel du système, utilisez la commande **show firmware**.

show firmware [**detail** | **expand** | **monitor** | **package-version**]

Description de la syntaxe

detail	(Facultatif) Utilisez ce mot clé pour afficher les versions actuelles du micrologiciel et du démarrage de l'appareil, ainsi que la version en cours d'exécution, son état d'activation et la version de démarrage du gestionnaire de service.
expand	(Facultatif) Utilisez ce mot clé pour répertorier de manière exhaustive les informations sur la version et l'état des divers composants du système.
monitor	(Facultatif) Utilisez ce mot clé pour afficher la version actuelle du package et l'état de mise à niveau du gestionnaire d'appareils, de l'interconnexion de structures et des serveurs de châssis.
package-version	(Facultatif) Utilisez ce mot clé pour afficher la version actuelle du package pour le gestionnaire d'appareils.

Modes de commande

Mode système

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous pouvez utiliser **show firmware monitor** à plusieurs reprises pour surveiller l'état du téléchargement et de l'activation d'une mise à niveau du micrologiciel.

Exemple

Cet exemple montre comment surveiller la version du micrologiciel et l'état de la mise à niveau :

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.4(1.52)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.4(1.52)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.4(1.52)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.4(1.52)
        Upgrade-Status: Ready
```

```
FP9300-A /system #
```

Commandes associées

Commande	Description
activate firmware	Active un package de micrologiciel.
show server firmware	Affiche les versions du micrologiciel et les informations d'état actuelles du serveur.

show (firmware-install)

Pour afficher les informations sur le package de micrologiciel actuel, utilisez la commande **show** en mode installation de micrologiciel.

show [**detail** | **event** | **fsm**]

Description de la syntaxe

detail	(Facultatif) Utilisez ce mot clé pour afficher des informations détaillées sur le package de micrologiciel.
event [*event_ID* | **detail**]	(Facultatif) Utilisez ce mot clé pour afficher les événements consignés lors de la mise à niveau du micrologiciel; le mot clé **detail** est disponible. Fournissez un *event_ID* spécifique pour afficher les informations sur cet événement uniquement.
fsm {**status** | **task**}	(Facultatif) Utilisez ces mots clés pour afficher les informations relatives à la mise à niveau du micrologiciel sur l'état ou les tâches de la machine à états finis (FSM).

Modes de commande

Mode installation de micrologiciel

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande affiche des informations sur le package de micrologiciel le plus récemment installé.

Exemple

Cet exemple montre comment afficher des informations détaillées sur le package de micrologiciel installé :

```
FP9300-A# scope firmware
FP9300-A /firmware # scope firmware-install
FP9300-A /firmware-install # show detail

Firmware Pack Install:
    Upgrade Package Version: 1.0.16
    Oper State: Ready
    Upgrade Status: Upgrade Complete Successful
    Current Task:
FP9300-A /firmware-install #
```

Commandes associées

Commande	Description
install firmware	Installe un package de micrologiciel.
show download-task	Affiche des informations sur les opérations de téléchargement du package de micrologiciel.

Commande	Description
show firmware	Affiche des informations sur le micrologiciel du système.

show filter expand detail

Pour afficher les détails du filtre pour la capture de paquets, utilisez la commande **show filter expand detail**.

show filter expand detail

Description de la syntaxe

show filter expand detail	Affiche les détails du filtre configuré pour la capture de paquets.

Modes de commande

scope packet-capture

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Cette commande **show** se trouve dans scope packet-capture. Reportez-vous au tableau suivant pour obtenir des informations sur les propriétés de filtre prises en charge.

ivlan	Identifiant du réseau VLAN interne (vlan du paquet dans le port d'entrée)
ovlan	ID de VLAN externe (VLAN ajouté par le châssis Firepower 4100/9300)
srcip	Adresse IP de la source (IPv4)
destip	Adresse IP de destination (IPv4)
srcport	Numéro du port de la source
destport	Numéro du port de destination
protocol	Protocole IP [valeurs du protocole défini par IANA en format décimal]
ethertype	Type de protocole Ethernet [valeur de type de protocole Ethernet définie par IANA en format décimal. Par exemple, IPv4 = 2048, IPv6 = 34525, ARP = 2054, SGT = 35081]
srcmac	Adresse MAC de source
destmac	Adresse Mac de destination

Exemple

Cet exemple montre comment afficher les détails du filtre configuré :

```
Firepower# scope packet-capture
Firepower /packet-capture # create filter check
Firepower /packet-capture/filter* # set destip 10.126.12.45
Firepower /packet-capture/filter* # commit-buffer
```

```
Firepower /packet-capture/filter # exit
Firepower /packet-capture # show filter expand detail

Configure a filter for packet capture:
    Name: check
    Protocol: 0
    Ivlan: 0
    Ovlan: 0
    Src Ip: 0.0.0.0
    Dest Ip: 10.126.12.45
    Src MAC: 00:00:00:00:00:00
    Dest MAC: 00:00:00:00:00:00
    Src Port: 0
    Dest Port: 0
    Ethertype: 0
    Src Ipv6: ::
    Dest Ipv6: ::
```

show flexflash-controller

Pour afficher les détails du contrôleur FlexFlash, utilisez la commande **show flexflash-controller detail expand**

show flexflash-controller detail expand

Description de la syntaxe

detail	Affiche les informations détaillées sur le contrôleur Flexflash
expand	(Facultatif) Affiche des informations développées pour le contrôleur FlexFlash, y compris la définition de la configuration du disque local

Modes de commande

scope fabric-interconnect a, scope server 1/1

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Cette commande **show** se trouve dans scope fabric-interconnect et inner scope server.

Exemple

Cet exemple montre l'état d'intégrité du module de sécurité.

```
Firepower# scope fabric-interconnect a
Firepower /fabric-interconnect # scope server 1/1
Firepower /chassis/server # show flexflash-controller detail expand

FlexFlash Controller:
    ID: 1
    Type: SD
    FlexFlash Type: FX3S
    Vendor: Cypress
    Model: FX3S
    Serial: NA
    Firmware Version: 1.3.2 build 173
    Controller State: Other Failure(s)
    Controller Health: OK
    RAID State: Disabled
    RAID Health: Not Reporting
    Physical Drive Count: 0
    Virtual Drive Count: 0
    RAID Sync Support: Supported
    Operability: Operable
    Oper Qualifier Reason:
    Presence: Equipped
    Current Task:

    Local Disk Config Definition:
        Mode: Any Configuration
        Description:
        Protect Configuration: Yes
```

show fsm status

Pour afficher le contenu des détails fsm disponibles sur le système, utilisez la commande **show fsm status**.

show fsm status [**expand**]

Description de la syntaxe

expand	Affiche des informations développées sur l'état du FSM. Le mot clé expand est disponible avec cette option.

Modes de commande

scope fabric-interconnect a

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope fabric-interconnect a.

Exemple

Cet exemple montre comment afficher des informations sur l'état du FSM :

```
Firepower # scope fabric-interconnect a
QP1 /fabric-interconnect # show fsm status

ID: A

    FSM 1:
        Remote Result: Not Applicable
        Remote Error Code: None
        Remote Error Description:
        Status: Nop
        Previous Status: Update Switch Success
        Timestamp: 2012-07-05T23:47:10.032
        Try: 0
        Flags: 0
        Progress (%): 100
        Current Task:

    FSM 2:
        Status: Nop
        Previous Status: SW Mgmt Oob Ipv6 If Config Success
        Timestamp: 2012-07-05T23:47:10.017
        Try: 0
        Progress (%): 100
        Current Task:

    FSM 3:
        Status:
        Previous Status:
        Timestamp:
        Try:
        Progress (%):
        Current Task:
```

Cet exemple montre comment afficher des informations détaillées sur l'état du FSM :

```
Firepower /fabric-interconnect # show fsm status expand detail

ID: A

    FSM Status:

        Affected Object: sys/switch-A/mgmt/fsm
        Current FSM: Update Switch
        Status: Success
        Completion Time: 2012-07-05T23:47:10.033
        Progress (%): 100
        Description:
        Remote Result: Not Applicable
        Error Code: None
        Error Description:

        FSM Stage:

            Order: 1
            Stage Name: UpdateSwitchCopyToLocal
            Status: Skip
            Try: 0
            Last Update Time: 2012-07-05T23:46:54.941
            Stage Description: copying image from external repository to local repository
(FSM-STAGE: sam: dme: MgmtControllerUpdateSwitch: copyToLocal)

            Order: 2
            Stage Name: UpdateSwitchCopyToPeer
            Status: Skip
            Try: 0
            Last Update Time: 2012-07-05T23:46:54.942
            Stage Description: copying image from external repository to local repository
of peer (FSM-STAGE: sam: dme: MgmtControllerUpdateSwitch: copyToPeer

            Order: 3
            Stage Name: UpdateSwitchUpdateLocal
            Status: Success
            Try: 1
            Last Update Time: 2012-07-05T23:47:10.016
            Stage Description: updating local fabric interconnect (FSM-STAGE: sam:
dme: MgmtControllerUpdateSwitch: update Local)

            Order: 4
            Stage Name: UpdateSwitchVerifyLocal
            Status: Success
            Try: 1
            Last Update Time: 2012-07-05T23:47:10.027
```

show fw-infra-pack

Pour afficher la liste de l'ensemble d'infrastructure de micrologiciels disponibles sur le système, utilisez la commande **show fw-infra-pack**.

show fw-infra-pack [**detail**]

Description de la syntaxe

detail	Répertorie les informations détaillées sur l'infrastructure de l'ensemble de micrologiciels.

Modes de commande

scope org

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope org.

Exemple

Cet exemple montre comment afficher les informations sur tous les paquets d'infrastructure de micrologiciels du système :

```
Firepower /fabric-interconnect # scope org
Firepower /org # show fw-infra-pack
Infra Pack:
    Name                 Description Infrastructure Bundle Version
    -------------------- ----------- ------------------------------
    default              Infrastructure Pack
                                     92.14(0.0808g_libtirpc)
```

Exemple

Cet exemple montre comment afficher les informations détaillées sur tous les paquets d'infrastructure de micrologiciels du système disponibles :

```
Firepower /org # show fw-infra-pack expand detail
Infra Pack:
    Name: default
    Description: Infrastructure Pack
    Infrastructure Bundle Version: 92.14(0.0808g_libtirpc)

    Pack Image:
HW Vendor: Cisco Systems
        HW Model: FPR-Manager
        Type: System
        Version: 92.13(0.0808g)
        Presence: Present

        HW Vendor: Cisco Systems
        HW Model: MGMTEXT
        Type: 17
```

```
Version: 92.13(0.107g)
Presence: Present

HW Vendor: Cisco Systems, Inc.
HW Model: F9K-C9300-SUP-K9
Type: Fabric Interconnect Kernel
Version: 5.0(3)N2(92.130.0808g)
Presence: Present

HW Vendor: Cisco Systems, Inc.
HW Model: F9K-C9300-SUP-K9
Type: Fabric Interconnect System
Version: 5.0(3)N2(92.130.0808g)
Presence: Present

HW Vendor: Cisco Systems, Inc.
HW Model: FPR-4110-SUP
Type: Fabric Interconnect Kernel
Version: 5.0(3)N2(92.130.0808g)
Presence: Present

HW Vendor: Cisco Systems, Inc.
HW Model: FPR-4110-SUP
Type: Fabric Interconnect System
Version: 5.0(3)N2(92.130.0808g)
Presence: Present

HW Vendor: Cisco Systems, Inc.
HW Model: FPR-4112-SUP
Type: Fabric Interconnect Kernel
Version: 5.0(3)N2(92.130.0808g)
Presence: Present

HW Vendor: Cisco Systems, Inc.
HW Model: FPR-4112-SUP
Type: Fabric Interconnect System
Version: 5.0(3)N2(92.130.0808g)
Presence: Present

HW Vendor: Cisco Systems, Inc.
HW Model: FPR-4115-SUP
Type: Fabric Interconnect Kernel
Version: 5.0(3)N2(92.130.0808g)
Presence: Present
```

show hardware-bypass-ports

Pour afficher les informations sur les ports de contournement matériel, utilisez la commande **show hardware-bypass-ports** .

show hardware-bypass-ports

Description de la syntaxe

show hardware-bypass-ports	(Facultatif) Affiche les informations sur le contournement matériel.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
2.6(1)	Commande ajoutée.

Instructions d'utilisation

Cette commande ne nécessite pas de licence.

Exemple

Cet exemple montre comment afficher les informations sur les paires de ports de contournement :

```
FPR # scope fabric-interconnect
FPR /fabric-interconnect # show hardware-bypass-ports

hardware-bypass port pairs:

Port1                Port2                Mode              Oper Mode      WDT      WDT Val
---------------- ---------------- ---------------- ---------------- -------- -------
Ethernet2/1      Ethernet2/2      Standby          Standby          Enabled  1000 <-------Pair
 Ethernet 2/1-2 is in standby mode
Ethernet2/3      Ethernet2/4      Disabled         Disabled         Disabled 0
Ethernet2/5      Ethernet2/6      Disabled         Disabled         Disabled 0
Ethernet2/7      Ethernet2/8      Disabled         Disabled         Disabled 0
Ethernet3/1      Ethernet3/2      Disabled         Disabled         Disabled 0
Ethernet3/3      Ethernet3/4      Switch Bypass    Switch Bypass    Enabled  1000
<-------Pair Ethernet 3/3-4 is in bypass mode (bypass is active)
Ethernet3/5      Ethernet3/6      Switch Bypass    Switch Bypass    Enabled  1000 <-------Pair
 Ethernet 3/5-6 is in bypass mode (bypass is active)
```

Commandes associées

Commande	Description
scope fabric-interconnect	Permet d'accéder au mode interconnexion de structures.

show health-led

Pour afficher l'état d'intégrité du module de sécurité, utilisez la commande **show health-led expand detail**.

show health-led expand detail

Description de la syntaxe

show health-led expand detail	Affiche les détails sur l'intégrité du module de sécurité. • Désactivé : hors tension. • Vert : fonctionnement normal. • Ambre : erreur mineure. • Ambre, clignotant : erreur critique.

Modes de commande

scope fabric-interconnect a, scope server 1/1

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Cette commande **show** se trouve dans scope fabric-interconnect et inner scope server.

Exemple

Cet exemple affiche l'état d'intégrité du module de sécurité.

```
Firepower# scope fabric-interconnect a
Firepower /fabric-interconnect # scope server 1/1
Firepower /chassis/server # show health-led expand detail
Health LED:
    Severity: Normal
    Reason:
    Color: Green
    Oper State: On
```

show https

Pour afficher la configuration du service HTTPS actuelle, utilisez la commande **show https**.

show https

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode de service

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment afficher la configuration du service HTTPS actuelle :

```
FP9300-A# scope system
FP9300-A /system # scope services
FP9300-A /system/services # show https
Name: https
    Admin State: Enabled
    Port: 443
    Operational port: 443
    Key Ring: default
    Cipher suite mode: Medium Strength
    Cipher suite: ALL:!EDH-RSA-DES-CBC3-SHA:!EDH-DSS-DES-CBC3-SHA:!DES-CBC3-SHA:
    !ADH:!3DES:!EXPORT40:!EXPORT56:!LOW:!RC4:!MD5:!IDEA:+HIGH:+MEDIUM:+EXP:+eNULL
    Https authentication type: Cred Auth
    Crl mode: Relaxed
FP9300-A /system/services #
```

Commandes associées

Commande	Description
set https auth-type	Spécifie le type d'authentification pour l'accès HTTPS.

show hw-crypto

Pour afficher l'état de l'Accélération cryptographique TLS, utilisez la commande **show hw-crypto**. Pour plus de renseignements sur l'Accélération cryptographique TLS, consultez le *Guide de configuration de Centre de gestion*.

show hw-crypto

Modes de commande

connect module

Historique des commandes

Version	Modification
2.7.1	Cette commande a été introduite.

Instructions d'utilisation

Cette commande affiche l'état de l'Accélération cryptographique TLS pour une instance de contenant.

Exemples

Voici un exemple d'affichage de l'état de l'Accélération cryptographique TLS :

```
scope ssa
/ssa # show app-instance

App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
 Deploy Type Turbo Mode Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- --------------- ---------------
 ----------- ---------- ------------ ---------------- ------------
ftd        FTD-FDM    1          Enabled     Online           6.5.0.1159      6.5.0.1159
    Native      No                      Not Applicable  None
ftd        ftd2       2          Enabled     Online           6.5.0.1159      6.5.0.1159
    Container   No         Default-Small Not Applicable  None

/ssa # sc slot 2
/ssa/slot # scope app-instance ftd ftd2
/ssa/slot/app-instance # show hw-crypto

Hardware Crypto:
    Admin State Hardware Crypto Size Hardware Crypto Version
    ----------- -------------------- ----------------------
    Enabled     13%                  2
```

Commandes associées

Commande	Description
create hw-crypto	Créer une configuration d'Accélération cryptographique TLS pour une instance de contenant.
delete hw-crypto	Supprimez une configuration d'Accélération cryptographique TLS pour une instance de contenant.
scope hw-crypto	Activez ou désactivez la configuration d'Accélération cryptographique TLS sur une instance de contenant.

show image

Pour afficher la liste des images de démarrage et système disponibles sur le système, utilisez la commande **show image**.

show image [**detail** | **type** | **version**]

Description de la syntaxe

detail	Répertorie les informations détaillées sur les images.
type	(Facultatif) Affiche les informations sur le type d'image actuel.
version	(Facultatif) Affiche les informations sur la version du micrologiciel.

Modes de commande

scope firmware

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope firmware.

Exemple

Cet exemple montre les informations de toutes les images système :

```
Firepower # scope firmware
Firepower /firmware# show image

Name                                        Type                Version
------------------------------------------- ------------------- -------
fxos-b200-m5-brdprog.11.0.bin               Board Controller    11.0
fxos-b200-m5-brdprog.5.0.bin                Board Controller    5.0
fxos-k9-compatibility.2.10.1. 1102.json      FXOS CSP Compatibility
                                                                2.10(1.1102)
fxos-k9-compatibility.2.10.1. 159.json       FXOS CSP Compatibility
                                                                2.10(1.159)
fxos-k9-compatibility.2.10.1.175_r. json     FXOS CSP Compatibility
                                                                2.10(1.175_r)
fxos-k9-compatibility.2.10.1. 177.json       FXOS CSP Compatibility
                                                                2.10(1.177)
fxos-k9-compatibility.2.10.1. 179.json       FXOS CSP Compatibility
                                                                2.10(1.179)
fxos-k9-compatibility.2.10.1.192_fix. json   FXOS CSP Compatibility
                                                                2.10(1.192_fi
x)
fxos-k9-compatibility.2.10.1. 193.json       FXOS CSP Compatibility
                                                                2.10(1.193)
fxos-k9-compatibility.2.10.1.198_rf. json    FXOS CSP Compatibility
                                                                2.10(1.198_rf
)
fxos-k9-compatibility.2.10.1. 199.json       FXOS CSP Compatibility
                                                                2.10(1.199)
fxos-k9-compatibility.2.10.1. 207.json       FXOS CSP Compatibility
                                                                2.10(1.207)
fxos-k9-compatibility.2.11.1. 156.json       FXOS CSP Compatibility
```

```
                                                                    2.11(1.156)
fxos-k9-compatibility.2.11.1.1922f_dpipev. json
                                            FXOS CSP Compatibility
                                                                    2.11(1.1922f_
dpipev)
fxos-k9-compatibility.2.11.1.2022f_cpio. json FXOS CSP Compatibility
                                                                    2.11(1.2022f_
cpio)
fxos-k9-compatibility.2.11.1.2022f_modsec. json
                                            FXOS CSP Compatibility
```

Cet exemple montre les informations détaillées des images :

```
Firepower/firmware# show image detail

Image fxos-b200-m5-brdprog.11.0.bin:
    Type: Board Controller
    Version: 11.0
    Size: 1391730
    Supported Models:
        Vendor: Cisco Systems Inc
        Model: FPR4K-SM-12S

        Vendor: Cisco Systems Inc
        Model: FPR4K-SM-24S

        Vendor: Cisco Systems Inc
        Model: FPR4K-SM-32S

        Vendor: Cisco Systems Inc
        Model: FPR4K-SM-44S

        Vendor: Cisco Systems Inc
        Model: FPR9K-SM-40

        Vendor: Cisco Systems Inc
        Model: FPR9K-SM-48

        Vendor: Cisco Systems Inc
```

Cet exemple montre comment afficher les informations de toutes les images de démarrage et système :

```
Firepower#
Firepower# scope fabric-interconnect a
Firepower /fabric-interconnect #
Firepower /fabric-interconnect # show image
Name                                       Type                 Version
------------------------------------------ -------------------- -------
fxos-k9-kickstart.5.0.3.N2.4.101.555.SSA   Fabric Interconnect Kernel
                                                                5.0(3)N2(4.10
1.555)
fxos-k9-kickstart.5.0.3.N2.4.101.777.SSA   Fabric Interconnect Kernel
                                                                5.0(3)N2(4.10
1.777)
fxos-k9-kickstart.5.0.3.N2.4.101.95.SPA    Fabric Interconnect Kernel
                                                                5.0(3)N2(4.10
1.95)
fxos-k9-kickstart.5.0.3.N2.4.111.111.SSA   Fabric Interconnect Kernel
                                                                5.0(3)N2(4.11
1.111)
fxos-k9-kickstart.5.0.3.N2.4.111.333.SSA   Fabric Interconnect Kernel
                                                                5.0(3)N2(4.11
1.333)
fxos-k9-kickstart.5.0.3.N2.4.111.85.SPA    Fabric Interconnect Kernel
```

```
                                                                    5.0(3)N2(4.11
1.85)
fxos-k9-kickstart.5.0.3.N2.4.120.6.SPA        Fabric Interconnect Kernel
                                                                    5.0(3)N2(4.12
0.6)
fxos-k9-kickstart.5.0.3.N2.4.130.10.SPA       Fabric Interconnect Kernel
                                                                    5.0(3)N2(4.13
0.10)
fxos-k9-kickstart.5.0.3.N2.4.131.983.SSA      Fabric Interconnect Kernel
                                                                    5.0(3)N2(4.13
1.983)
fxos-k9-kickstart.5.0.3.N2.4.61.235.SPA       Fabric Interconnect Kernel
                                                                    5.0(3)N2(4.61
.235)
fxos-k9-kickstart.5.0.3.N2.4.81.0812.SSA      Fabric Interconnect Kernel
                                                                    5.0(3)N2(4.81
.0812)
fxos-k9-kickstart.5.0.3.N2.4.81.306.SPA       Fabric Interconnect Kernel
                                                                    5.0(3)N2(4.81
.306)
fxos-k9-kickstart.5.0.3.N2.4.81.789.SSA       Fabric Interconnect Kernel
                                                                    5.0(3)N2(4.81
.789)
fxos-k9-kickstart.5.0.3.N2.4.91.1182.SPA      Fabric Interconnect Kernel
                                                                    5.0(3)N2(4.91
.1182)
fxos-k9-kickstart.5.0.3.N2.4.91.222.SSB       Fabric Interconnect Kernel
                                                                    5.0(3)N2(4.91
.222)
```

show image detail

Pour afficher la liste des images de démarrage et système disponibles sur le système, utilisez la commande **show image**.

show image detail

Description de la syntaxe

detail	Répertorie les informations détaillées sur les images.

Modes de commande

scope fabric-interconnect

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** en mode scope fabric-interconnect.

Exemple

Cet exemple affiche les informations de toutes les images de démarrage et système :

```
firepower# /system/services # scope fabric-interconnect
firepower# /fabric-interconnect # show image
Name                                        Type                 Version
------------------------------------------- -------------------- -------
fxos-k9-kickstart.5.0.3.N2.4.111.85.SPA     Fabric Interconnect Kernel
                                                                 5.0(3)N2(4.11
1.85)
fxos-k9-kickstart.5.0.3.N2.92.130.257g.gSSB Fabric Interconnect Kernel
                                                                 5.0(3)N2(92.1
30.257g)
fxos-k9-system.5.0.3.N2.4.111.85.SPA        Fabric Interconnect System
                                                                 5.0(3)N2(4.11
1.85)
fxos-k9-system.5.0.3.N2.92.130.257g.gSSB    Fabric Interconnect System
                                                                 5.0(3)N2(92.1
30.257g)
Mahendra-QPD /fabric-interconnect #
```

show import-config detail

Pour afficher les configurations d'importation en détail, utilisez la commande **show import-config detail**.

Show import-config [**detail**]

Description de la syntaxe		
	Detail	Affiche les informations détaillées sur la configuration d'importation.

Modes de commande **scope system**

Historique des commandes		
	Version	**Modification**
	2.3.1	Commande ajoutée.

Instructions d'utilisation Il s'agit d'une sous-commande de la commande **show** dans scope system.

Exemple

Cet exemple montre comment afficher les informations de configuration d'importation.

```
Firepower # scope system
Firepower /system #
Firepower /system # import-config
scp://<user>@<hostname>:/auto/stg_03/ssp/92.14.2/92.14.2.4/final/<config.txt> enabled
Password:
Warning: After configuration import any changes on the breakout port configuration will
cause the system to reboot
Firepower /system/import-config* # commit-buffer
Firepower /system/import-config # exit
Firepower /system # show import-config detail
Import Configuration Task:
    Hostname: <hostname>
    Remote File: /auto/stg_03/ssp/92.14.2/92.14.2.4/final/<config.txt>
    User: <user>
    Protocol: Scp
    Admin State: Disabled
    Status: Failed
    Description:
    Port: Default
    Error Msg:
```

show identity

Pour afficher diverses informations sur le système, utilisez la commande **show identity**.

show identity {**ip-addr** | **ipv6-addr** | **iqn** | **mac-addr** | **uuid** | **wwn**}

Description de la syntaxe

ip-addr	(Facultatif) Répertorie les informations de toutes les adresses IP disponibles. Les mots clés facultatifs suivants sont disponibles : • *IPv4_address* : affiche les informations d'identité de l'adresse IPv4 spécifiée. • **detail** : affiche les informations d'identité détaillées de l'adresse IPv4. • **pool-info** : affiche les informations d'adresse IPv4 pour l'ensemble. Le mot clé **detail** est également disponible. • **profile-info** : affiche les informations d'adresse IPv4 pour le profil. Le mot clé **detail** est également disponible.
ipv6-addr	(Facultatif) Répertorie les informations de toutes les adresses IPv6 disponibles. Les mots clés facultatifs suivants sont disponibles : • **detail** : affiche les informations d'identité détaillées de l'adresse IPv6. • **pool-info** : affiche les informations d'adresse IPv6 pour l'ensemble. Le mot clé **detail** est également disponible. • **profile-info** : affiche les informations d'adresse IPv6 pour le profil. Le mot clé **detail** est également disponible. • *IPv6_address* : affiche les informations d'identité de l'adresse IPv6 spécifiée.

iqn	(Facultatif) Affiche les informations sur les identités IQN (iSCSI Qualified Name) d'un système. Les mots clés facultatifs suivants sont également disponibles : • **detail** : affiche les détails sur les informations d'identité sous forme de liste. • **pool-info** : affiche les informations d'identité IQN pour l'ensemble. Le mot clé **detail** est également disponible. • **profile-info** : affiche les informations d'identité IQN pour le profil. Le mot clé **detail** est également disponible. • *prefix* : affiche les informations pour le préfixe IQN spécifié. • *name* : affiche les informations pour l'identité IQN nommée; peut comporter un maximum de 510 caractères. Par défaut, cette commande répertorie les informations sur toutes les identités IQN configurées pour un ensemble IQN.
mac-addr	(Facultatif) Affiche les informations d'identité des adresses MAC pour un système. Les mots clés facultatifs suivants sont également disponibles : • *id* : affiche les informations d'identité pour une adresse MAC spécifique. Spécifier une adresse MAC au format AA:BB:CC:DD:EE:FF. • **detail** : affiche les détails sur les informations d'identité sous forme de liste. • **pool-info** : affiche les informations d'identité d'adresse MAC pour l'ensemble. Le mot clé **detail** est également disponible. • **profile-info** : affiche les informations d'identité d'adresse MAC pour le profil. Le mot clé **detail** est également disponible.

uuid	(Facultatif) Affiche les informations d'identité de l'identifiant unique universel (UUID) pour un système. Les mots clés facultatifs suivants sont également disponibles : • **derived** *id* : affiche les informations d'identité dérivées pour l'UUID spécifié; saisi au format `FFFF-FFFFFFFFFFFF`. • **detail** — Affiche les informations détaillées d'identité UUID. • *uuid_prefix* : affiche les informations d'identité pour le préfixe UUID spécifié; saisi au format `FFFFFFFF-FFFF-FFFF`. • *uuid* : affiche les informations d'identité pour l'UUID spécifié; saisi au format `FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF`. • **pool-info** : affiche les informations d'identité UUID pour l'ensemble. Le mot clé **detail** est également disponible. • **profile-info** : affiche les informations d'identité UUID pour le profil. Le mot clé **detail** est également disponible.
wwn	(Facultatif) Affiche les informations sur le nom universel (WWN) d'un système. Les mots clés facultatifs suivants sont également disponibles : • **detail** : affiche les détails sur les informations d'identité sous forme de liste. • *id* : affiche les informations d'identité pour un WWN donné; fournir un identifiant WWN unique au format `FF:FF:FF:FF:FF:FF:FF:FF`. • **pool-info** : affiche les informations d'identité pour le pool. Le mot clé **detail** est également disponible. • **profile-info** : affiche les informations d'identité pour le profil. Le mot clé **detail** est également disponible.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Les ensembles et préfixes IQN doivent être configurés pour pouvoir utiliser la commande **show identity iqn**.

Exemple

Cet exemple montre comment afficher les informations d'identité détaillées des adresses IPv4 de l'appareil :

```
FP9300-A# show identity ip-addr detail
IP Address: 192.0.2.9
    Assigned: No
    Assigned Service Profile:
```

```
    Owner: Pool
IP Address: 192.0.2.10
    Assigned: No
    Assigned Service Profile:
    Owner: Pool
IP Address: 192.0.2.11
    Assigned: No
    Assigned Service Profile:
    Owner: Pool
IP Address: 192.0.2.12
    Assigned: No
    Assigned Service Profile:
    Owner: Pool

    <--- remaining lines removed for brevity --->

FP9300-A#
```

Commandes associées

Commande	Description
show server identity	Affiche les informations d'identité des serveurs, adaptateurs et interfaces.

show interface (afficher l'interface)

Pour afficher l'état de l'interface Ethernet, utilisez la commande **show interface**.

show interface [**detail** | **expand** | **fsm status** | *interface_id*]

Description de la syntaxe

detail	Affiche les informations détaillées sur l'interface.
expand	Affiche des informations sur les interfaces dans une vue non tabulaire, ainsi que des informations sur les sous-interfaces.
fsm status	Affiche l'état de la machine à états finis (FSM).
interface_id	Affiche des informations sur une interface Ethernet particulière, par exemple, Ethernet1/4.

Modes de commande

scope eth-uplink/scope fabric a/

Historique des commandes

Version	Modification
2.4(1)	Des champs supplémentaires ont été ajoutés pour les sous-interfaces VLAN.
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Cette commande s'applique uniquement aux interfaces Ethernet. Pour les EtherChannels, consultez la commande **show port-channel**. Pour les sous-interfaces, consultez la commande **show subinterface**.

Remarque FXOS ne prend pas en charge la détection de liaison unidirectionnelle (UDLD); ignorer toute référence à UDLD.

Exemple

Voici un exemple de sortie de la commande **show interface**.

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # show interface

Interface:
    Port Name       Port Type          Admin State Oper State       Allowed Vlan State
Reason
    --------------- ------------------ ----------- ---------------- ------------ ------------

    Ethernet1/2     Data               Enabled     Up               All
    Ethernet1/4     Mgmt               Enabled     Up               All
    Ethernet1/5     Data               Enabled     Up               Untagged
    Ethernet1/7     Firepower Eventing Enabled     Up               All
    Ethernet1/8     Data               Disabled    Sfp Not Present  All          Unknown
    Ethernet2/1     Data               Disabled    Sfp Not Present  All          Unknown
```

```
    Ethernet2/2     Data               Disabled    Sfp Not Present  All          Unknown
    Ethernet2/3     Data               Disabled    Sfp Not Present  All          Unknown
    Ethernet2/4     Data               Disabled    Sfp Not Present  All          Unknown
    Ethernet2/5     Data               Disabled    Sfp Not Present  All          Unknown
    Ethernet2/6     Data               Disabled    Sfp Not Present  All          Unknown
    Ethernet2/7     Data               Disabled    Sfp Not Present  All          Unknown
    Ethernet2/8     Data               Disabled    Sfp Not Present  All          Unknown
```

Voici un exemple de sortie de la commande **show interface detail**.

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # show interface detail

Interface:
    Port Name: Ethernet1/2
    User Label:
    Port Type: Data
    Admin State: Enabled
    Oper State: Up
    State Reason:
    flow control policy: default
    Auto negotiation: No
    Admin Speed: 1 Gbps
    Oper Speed: 1 Gbps
    Admin Duplex: Full Duplex
    Oper Duplex: Full Duplex
    Ethernet Link Profile name: default
    Oper Ethernet Link Profile name: fabric/lan/eth-link-prof-default
    Udld Oper State: Admin Disabled
    Inline Pair Admin State: Enabled
    Inline Pair Peer Port Name:
    Allowed Vlan: All
    Network Control Policy: default
    Current Task:

    Port Name: Ethernet1/4
    User Label:
    Port Type: Mgmt
    Admin State: Enabled
    Oper State: Up
    State Reason:
    flow control policy: default
    Auto negotiation: No
    Admin Speed: 1 Gbps
    Oper Speed: 1 Gbps
    Admin Duplex: Full Duplex
    Oper Duplex: Full Duplex
    Ethernet Link Profile name: default
    Oper Ethernet Link Profile name: fabric/lan/eth-link-prof-default
    Udld Oper State: Admin Disabled
    Inline Pair Admin State: Enabled
    Inline Pair Peer Port Name:
    Allowed Vlan: All
    Network Control Policy: default
    Current Task:

[...]
```

Voici un exemple de sortie de la commande **show interface expand**.

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # show interface expand

Interface:
    Port Name: Ethernet1/2
    Port Type: Data
    Admin State: Enabled
    Oper State: Up
    Allowed Vlan: All
    State Reason:

    Port Name: Ethernet1/4
    Port Type: Mgmt
    Admin State: Enabled
    Oper State: Up
    Allowed Vlan: All
    State Reason:

    Port Name: Ethernet1/5
    Port Type: Data
    Admin State: Enabled
    Oper State: Up
    Allowed Vlan: Untagged
    State Reason:

    Sub Interface:
        Sub-If Id  Sub-Interface Name VLAN        Port Type
        ---------- ------------------ ----------- ---------
               100 Ethernet1/5.100    500         Data Sharing
```

Commandes associées

Commande	Description
show port-channel	Affiche l'état de l'interface EtherChannel.
show subinterface	Affiche l'état de la sous-interface.

show interface counter errors (connect fxos)

Pour afficher les erreurs des compteurs d'interfaces, utilisez la commande **show interface counter errors**.

show interface counter errors

Description de la syntaxe

Align-Err	Les erreurs d'alignement correspondent au nombre de trames reçues qui ne se terminent pas par un nombre pair d'octets et présentent un contrôle de redondance cyclique (CRC) erroné. Causes courantes : les erreurs d'alignement résultent généralement d'une incompatibilité des conditions de duplex ou d'un problème physique (câblage, port ou carte réseau défectueux, par exemple). Lorsque le câble est connecté au port pour la première fois, certaines de ces erreurs peuvent survenir. De plus, si un concentrateur est connecté au port, les collisions entre d'autres périphériques sur le concentrateur peuvent entraîner ces erreurs.
FCS-Err	Nombre de trames de taille valide présentant des erreurs de séquence de contrôle de trame (FCS) mais sans erreurs de tramage. Causes courantes : il s'agit généralement d'un problème physique (câblage, port ou carte réseau défectueux, par exemple), voire d'une incompatibilité des conditions de duplex.
Xmit-Err	Cela indique que le tampon d'envoi interne (Tx) est saturé. Causes courantes : une cause courante de Xmit-Err peut être liée au trafic provenant d'une liaison à haut débit commuté vers une liaison à faible débit, ou le trafic de plusieurs liaisons entrantes commuté vers une seule liaison sortante. Par exemple, si un volume important de trafic en rafales transite par une interface gigabit et est commuté vers une interface de 100 Mbit/s, cela peut entraîner l'incrémentation des erreurs Xmit-Err sur cette interface. En effet, le tampon de sortie de l'interface est submergé par le trafic excédentaire en raison d'une incompatibilité de vitesse entre les bandes passantes entrantes et sortantes.
Rcv-Err	Une erreur de réception (à savoir, Rcv-Err) se produit lorsqu'un port se heurte à débordements de tampon. La congestion sur le fond de panier d'un commutateur peut entraîner le remplissage du tampon de réception d'un port, les trames attendant alors d'accéder au fond de panier du commutateur. Cependant, très probablement, un Rcv-Err indique une incompatibilité des conditions de duplex.
Undersize	Trames reçues inférieures à la taille de trame IEEE 802.3 minimale de 64 octets (ce qui exclut les bits de trame, mais inclut les octets FCS) et, par ailleurs, bien formées. Causes courantes : vérifiez l'appareil qui envoie ces trames.
Out-Discard	Nombre de paquets sortants à supprimer même si aucune erreur n'a été détectée. Causes courantes : une raison possible de supprimer un tel paquet peut être de libérer de l'espace tampon.

Single-Col	Nombre de fois où une seule collision s'est produite avant que l'interface ne parvienne à transmette une trame au support. Causes courantes : les collisions sont normales pour les interfaces configurées en semi-duplex, mais ne doivent en aucun cas être observées sur les interfaces en duplex intégral. Si les collisions augmentent considérablement, cela indique une liaison fortement sollicitée, voire une incompatibilité de mode duplex avec l'appareil connecté.
Multi-Col	Nombre de fois où plusieurs collisions se sont produites avant que l'interface ne parvienne à transmette une trame au support. Causes courantes : les collisions sont normales pour les interfaces configurées en semi-duplex, mais ne doivent en aucun cas être observées sur les interfaces en duplex intégral. Si les collisions augmentent considérablement, cela indique une liaison fortement sollicitée, voire une incompatibilité de mode duplex avec l'appareil connecté.
Late-Col	Nombre de fois où une collision est détectée sur une interface donnée tardivement dans le processus de transmission. Pour un port à 10 Mbit/s, cela se produit plus tard que 512 temps-bits après le début de la transmission d'un paquet. Cinq cent douze temps-bits correspondent à 51,2 microsecondes sur un système à 10 Mbit/s. Causes courantes : cette erreur peut indiquer notamment indiquer une incompatibilité des conditions de duplex. Dans un scénario d'incompatibilité des conditions de duplex, la collision tardive est observée du côté du mode semi-duplex. Lorsque le côté semi-duplex assure une transmission, le côté duplex intégral n'attend pas son tour et procède à une transmission simultanée, ce qui provoque une collision tardive. Des collisions tardives peuvent également indiquer qu'un câble ou segment Ethernet est trop long. Aucune collision ne doit être observée sur les interfaces configurées en duplex intégral.
Excess-Col	Nombre de trames pour lesquelles la transmission sur une interface particulière échoue en raison de collisions excessives. Une collision excessive se produit lorsqu'un paquet se heurte à une collision 16 fois de suite. Le paquet est alors abandonné. Causes courantes : Des collisions excessives indiquent généralement que la charge sur le segment doit être répartie sur plusieurs segments. Elle peuvent également indiquer une incompatibilité des conditions de duplex avec l'appareil connecté. Aucune collision ne doit être observée sur les interfaces configurées en duplex intégral.
Carri-Sen	Le compteur Carri-Sen (Carrier Sense) est incrémenté chaque fois qu'un contrôleur Ethernet tente d'envoyer des données sur une connexion semi-duplex. Le contrôleur détecte le câble et vérifie s'il n'est pas occupé préalablement à la transmission. Causes courantes : cette situation est normale sur un segment Ethernet en semi-duplex.

Runts	Les trames reçues sont inférieures à la taille de trame IEEE 802.3 minimale (64 octets pour Ethernet) et présentent un CRC incorrect. Causes courantes : cela peut être dû à une incompatibilité des conditions de duplex et des problèmes physiques, câblage, port ou carte réseau défectueux, par exemple, sur l'appareil connecté. Exceptions de plateforme : gamme Catalyst 4000 exécutant une version de Cisco IOS antérieure à la version logicielle 12.1(19)EW, un « runt » = sous-dimensionnement. Sous-dimensionnement = trame inférieure à 64 octets. Le compteur de « runts » ne s'incrémentait que lors de la réception d'une trame inférieure à 64 octets. Après la version 12.1(19)EW, un « runt » = un fragment. Un fragment est une trame inférieure à 64 octets, mais présentant un CRC incorrect. En conséquence, le compteur de « runts » s'incrémente maintenant dans show interfaces, de même que le compteur de fragments dans show interfaces counters errors, lors de la réception d'une trame de 64 octets présentant un CRC incorrect. Commutateurs de la gamme Cisco Catalyst 3750 Dans les versions antérieures à Cisco IOS 12.1(19)EA1, lorsque dot1q est utilisé sur l'interface de liaison du commutateur Catalyst 3750, des « runts » peuvent être observés sur la sortie show interfaces en raison de paquets encapsulés dot1q valides, comprenant de 61 à 64 octets, avec la balise q-bal, sont comptabilisés par Catalyst 3750 en tant que trames sous-dimensionnées, même si ces paquets sont correctement transférés. En outre, ces paquets ne sont pas signalés dans la catégorie appropriée (monodiffusion, multidiffusion ou diffusion) dans les statistiques de réception. Ce problème a été résolu dans les versions 12.1(19)EA1 ou 12.2(18)SE de Cisco IOS ou ultérieures.
Giants	Trames reçues dont la taille dépasse la taille de trame IEEE 802.3 maximale (1 518 octets pour Ethernet non jumbo) et dont la séquence de contrôle de trame (FCS) est incorrecte. Causes courantes : dans de nombreux cas, il s'agit du résultat d'une carte réseau incorrecte. Essayez de localiser l'appareil incriminé et supprimez-le du réseau. Exceptions de plateforme : sur les appareils de la gamme Catalyst 4000 exécutant une version de Cisco IOS antérieure à la version logicielle 12.1(19)EW, le compteur de trames géantes s'incrémentait pour les trames > 1 518 octets. Dans les versions postérieures à 12.1(19)EW, une trame géante est comptabilisée dans les données de sortie de la commande show interfaces lors de la réception d'une trame > 1 518 octets accompagnée d'une séquence FCS incorrecte.
IntMacTx-Er	Interface mac TX : erreur de transmission
IntMacRx-Er	Interface mac RX : erreur de réception
Symbol-Err	L'erreur symbol-err s'affiche lorsque Mac observe des symboles « non valides ». Dans la plupart des cas, il s'agit d'un problème physique (Gbits, fibre optique, etc.). Ces erreurs sont également incrémentées lorsque la liaison n'est pas active, car Mac n'est pas synchronisé et reçoit du bruit. De petites quantités d'erreurs de symboles peuvent être ignorées. De grandes quantités d'erreurs de symboles peuvent indiquer un problème d'appareil, de câble ou de matériel.

Deferred-tx	Le compteur « Deferred-tx » s'incrémente chaque seconde. Il représente le nombre de premières tentatives de transmission retardées car le support était occupé.
SQETest-Err	SQE signifie « Signal Quality Error » (erreur de qualité de signal, SQE) et peut aussi être appelé « pulsation » Ethernet. Avec les premières cartes Ethernet qui nécessitaient des émetteurs-récepteurs, l'émetteur-récepteur renvoyait une erreur de qualité de signal à la carte Ethernet après chaque transmission de trame, afin de s'assurer du bon fonctionnement du circuit de détection de collision. Avec les cartes réseau modernes, ce test SQE peut faire croire aux cartes qu'une véritable collision s'est produite, et une collision est alors signalée sur le réseau lorsqu'un test SQE est détecté. Cela peut considérablement dégrader les performances du réseau, car chaque trame transmise avec succès est suivie d'une collision causée par le test SQE. Cause 1 : les erreurs de test SQE peuvent être dues à un émetteur-récepteur dont le commutateur DIP « SQE test » est activé (celui-ci devrait être désactivé). Vérifiez les paramètres du commutateur sur tous les émetteurs-récepteurs du segment. Cause 2 : les erreurs de test SQE peuvent être dues à émetteurs-récepteurs défectueux. Vérifiez la présence d'émetteurs-récepteurs défectueux sur le segment.

Modes de commande

connect fxos

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Cette commande affiche les erreurs du compteur de l'interface.

Exemple

Cet exemple montre comment afficher les informations sur les erreurs des compteurs de l'interface :

```
firepower#
firepower# connect fxos
...
firepower(fxos)# show interface counters errors
-------------------------------------------------------------------------------
Port          Align-Err    FCS-Err   Xmit-Err    Rcv-Err  UnderSize OutDiscards
-------------------------------------------------------------------------------
Eth1/1                0          0          0          0          0           0
Eth1/2                0          0          0          0          0           0
Eth1/3                0          0          0          0          0           0
Eth1/4                0          0          0          0          0           0
Eth1/5                0          0          0          0          0           0
Eth1/6                0          0          0          0          0           0
Eth1/7                0          0          0          0          0           0
Eth1/8                0          0          0          0          0           0
Eth1/9                0 1378344622          0 1384807633          0           0
Eth1/10               0          0          0          0          0           0
Eth1/11               0          0          0          0          0           0
Eth1/12               0          0          0          0          0           0
Eth2/1                0          0          0          0          0           0
Eth2/2                0          0          0          0          0           0
Eth2/3                0          0          0          0          0           0
Eth2/4                0          0          0          0          0           0
```

Eth2/5	0	0	0	0	0	0
Eth2/6	0	0	0	0	0	0
Eth2/7	0	0	0	0	0	0
Eth2/8	0	0	0	0	0	0
Po1	0	0	0	0	0	0
Po48	0	0	0	0	0	0
Veth687	--	--	--	--	--	0
Veth688	--	--	--	--	--	0
Veth689	--	--	--	--	--	0
Veth690	--	--	--	--	--	0
Veth691	--	--	--	--	--	0
Veth692	--	--	--	--	--	0
Veth693	--	--	--	--	--	0
Veth694	--	--	--	--	--	0
Veth695	--	--	--	--	--	0
Veth696	--	--	--	--	--	0
Veth697	--	--	--	--	--	0
Veth698	--	--	--	--	--	0
Veth718	--	--	--	--	--	0
Veth736	--	--	--	--	--	0
Veth737	--	--	--	--	--	0
Veth772	--	--	--	--	--	0
Veth773	--	--	--	--	--	0
Veth774	--	--	--	--	--	0
Veth775	--	--	--	--	--	0
Veth776	--	--	--	--	--	0
Veth777	--	--	--	--	--	0
Veth855	--	--	--	--	--	0
Veth856	--	--	--	--	--	0
Veth857	--	--	--	--	--	0
Veth858	--	--	--	--	--	0
Veth859	--	--	--	--	--	0
Veth860	--	--	--	--	--	0
Veth861	--	--	--	--	--	0
Veth862	--	--	--	--	--	0

Port	Single-Col	Multi-Col	Late-Col	Exces-Col	Carri-Sen	Runts
Eth1/1	0	0	0	0	0	0
Eth1/2	0	0	0	0	0	0
Eth1/3	0	0	0	0	0	0
Eth1/4	0	0	0	0	0	0
Eth1/5	0	0	0	0	0	0
Eth1/6	0	0	0	0	0	0
Eth1/7	0	0	0	0	0	0
Eth1/8	0	0	0	0	0	0
Eth1/9	0	0	0	0	0	0
Eth1/10	0	0	0	0	0	0
Eth1/11	0	0	0	0	0	0
Eth1/12	0	0	0	0	0	0
Eth2/1	0	0	0	0	0	0
Eth2/2	0	0	0	0	0	0
Eth2/3	0	0	0	0	0	0
Eth2/4	0	0	0	0	0	0
Eth2/5	0	0	0	0	0	0
Eth2/6	0	0	0	0	0	0
Eth2/7	0	0	0	0	0	0
Eth2/8	0	0	0	0	0	0
Po1	0	0	0	0	0	0
Po48	0	0	0	0	0	0
Veth687	--	--	--	--	--	--
Veth688	--	--	--	--	--	--
Veth689	--	--	--	--	--	--

```
Veth690             --         --         --         --         --         --
Veth691             --         --         --         --         --         --
Veth692             --         --         --         --         --         --
Veth693             --         --         --         --         --         --
Veth694             --         --         --         --         --         --
Veth695             --         --         --         --         --         --
Veth696             --         --         --         --         --         --
Veth697             --         --         --         --         --         --
Veth698             --         --         --         --         --         --
Veth718             --         --         --         --         --         --
Veth736             --         --         --         --         --         --
Veth737             --         --         --         --         --         --
Veth772             --         --         --         --         --         --
Veth773             --         --         --         --         --         --
Veth774             --         --         --         --         --         --
Veth775             --         --         --         --         --         --
Veth776             --         --         --         --         --         --
Veth777             --         --         --         --         --         --
Veth855             --         --         --         --         --         --
Veth856             --         --         --         --         --         --
Veth857             --         --         --         --         --         --
Veth858             --         --         --         --         --         --
Veth859             --         --         --         --         --         --
Veth860             --         --         --         --         --         --
Veth861             --         --         --         --         --         --
Veth862             --         --         --         --         --         --

--------------------------------------------------------------------------------
Port          Giants SQETest-Err Deferred-Tx IntMacTx-Er IntMacRx-Er Symbol-Err
--------------------------------------------------------------------------------
Eth1/1             0         --           0          0          0          0
Eth1/2             0         --           0          0          0          0
Eth1/3             0         --           0          0          0          0
Eth1/4             0         --           0          0          0          0
Eth1/5             0         --           0          0          0          0
Eth1/6             0         --           0          0          0          0
Eth1/7             0         --           0          0          0          0
Eth1/8             0         --           0          0          0          0
Eth1/9             0         --           0    6463011          0          0
Eth1/10            0         --           0          0          0          0
Eth1/11            0         --           0          0          0          0
Eth1/12            0         --           0          0          0          0
Eth2/1             0         --           0          0          0          0
Eth2/2             0         --           0          0          0          0
Eth2/3             0         --           0          0          0          0
Eth2/4             0         --           0          0          0          0
Eth2/5             0         --           0          0          0          0
Eth2/6             0         --           0          0          0          0
Eth2/7             0         --           0          0          0          0
Eth2/8             0         --           0          0          0          0
Po1                0         --           0          0          0          0
Po48               0         --           0          0          0          0
Veth687           --         --          --         --         --         --
Veth688           --         --          --         --         --         --
Veth689           --         --          --         --         --         --
Veth690           --         --          --         --         --         --
Veth691           --         --          --         --         --         --
Veth692           --         --          --         --         --         --
Veth693           --         --          --         --         --         --
Veth694           --         --          --         --         --         --
Veth695           --         --          --         --         --         --
Veth696           --         --          --         --         --         --
Veth697           --         --          --         --         --         --
Veth698           --         --          --         --         --         --
```

```
Veth718           --         --         --         --         --         --
Veth736           --         --         --         --         --         --
Veth737           --         --         --         --         --         --
Veth772           --         --         --         --         --         --
Veth773           --         --         --         --         --         --
Veth774           --         --         --         --         --         --
Veth775           --         --         --         --         --         --
Veth776           --         --         --         --         --         --
Veth777           --         --         --         --         --         --
Veth855           --         --         --         --         --         --
Veth856           --         --         --         --         --         --
Veth857           --         --         --         --         --         --
Veth858           --         --         --         --         --         --
Veth859           --         --         --         --         --         --
Veth860           --         --         --         --         --         --
Veth861           --         --         --         --         --         --
Veth862           --         --         --         --         --         --
firepower(fxos)#
```

show interface transceiver (connect fxos)

Pour afficher les détails et les étalonnages de l'émetteur-récepteur, utilisez la commande **show interface transceiver**.

show interface transceiver | **details** | **calibrations**

Description de la syntaxe

details	Affiche les informations détaillées sur l'émetteur-récepteur d'interface.
calibrations	Affiche les informations détaillées sur les étalonnages.

Modes de commande

connect fxos

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Cette commande est une sous-commande de la commande **show interface** dans le shell **connect fxos** .

Exemple

Cet exemple montre comment afficher un bref ensemble d'informations relatives à l'émetteur-récepteur d'interface :

```
firepower#
firepower# connect fxos
...
firepower(fxos)# show interface transceiver calibrations
Ethernet1/1
    transceiver is present
    type is 1000base-T
    name is CISCO-METHODE
    part number is SP7041-R
    revision is
    serial number is ABCD1234
    nominal bitrate is 1300 MBit/sec
    Link length supported for copper is 100 m
    cisco id is --
    cisco extended id number is 4

firepower(fxos)# show interface transceiver details
Ethernet1/1
    transceiver is present
    type is 1000base-T
    name is CISCO-METHODE
    part number is SP7041-R
    revision is
    serial number is ABCD1234
    nominal bitrate is 1300 MBit/sec
    Link length supported for copper is 100 m
    cisco id is --
    cisco extended id number is 4

DOM is not supported
```

show interface brief (connect fxos)

Pour afficher ou enregistrer un ensemble réduit d'informations sur l'état des interfaces et d'autres données, utilisez la commande **show interface brief**.

show interface brief

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

connect fxos/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Cette commande est une sous-commande de la commande **show interface** dans le shell **connect fxos**.

Exemple

Cet exemple montre comment afficher un bref ensemble d'informations relatives à l'interface :

```
firepower # connect fxos
firepower(fxos)# show interface brief

--------------------------------------------------------------------------------
Ethernet      VLAN   Type Mode   Status  Reason                   Speed     Port
Interface                                                                  Ch #
--------------------------------------------------------------------------------
Eth1/1        1       eth  1qtunl up      none                      1000(D) 48
Eth1/2        1       eth  1qtunl up      none                      1000(D) --
Eth1/3        1       eth  1qtunl down    suspended(no LACP PDU)    1000(D) 1
Eth1/4        1       eth  1qtunl up      none                      1000(D) --
Eth1/5        1       eth  1qtunl up      none                      1000(D) --
Eth1/6        1       eth  1qtunl up      none                      1000(D) 2
Eth1/7        1       eth  1qtunl up      none                      1000(D) --
Eth1/8        1       eth  1qtunl down    SFP not inserted           10G(D) --
Eth1/9        1       eth  vntag  up      none                       40G(D) --
Eth1/10       1       eth  vntag  up      none                       40G(D) --
Eth1/11       1       eth  vntag  up      none                       40G(D) --
Eth1/12       1       eth  vntag  up      none                       40G(D) --
Eth1/13       1       eth  access down    Administratively down      40G(D) --
Eth1/14       1       eth  access down    Administratively down      40G(D) --
Eth1/15       1       eth  access down    Administratively down     1000(D) --
Eth1/16       1       eth  access down    Administratively down     1000(D) --
Eth2/1        1       eth  1qtunl down    SFP not inserted           10G(D) --
Eth2/2        1       eth  1qtunl down    SFP not inserted           10G(D) --
Eth2/3        1       eth  1qtunl down    SFP not inserted          1000(D) --
Eth2/4        1       eth  1qtunl down    SFP not inserted          1000(D) --
Eth2/5        1       eth  1qtunl down    SFP not inserted           10G(D) --
Eth2/6        1       eth  1qtunl down    SFP not inserted           10G(D) --
Eth2/7        1       eth  1qtunl down    SFP not inserted           10G(D) --
Eth2/8        1       eth  1qtunl down    SFP not inserted           10G(D) --

--------------------------------------------------------------------------------
Port-channel VLAN    Type Mode   Status  Reason                   Speed   Protocol
```

```
Interface
--------------------------------------------------------------------------------
Po1          1       eth  1qtunl down    No operational members      1000(D)  lacp
Po2          1       eth  1qtunl up      none                       a-1000(D)  lacp
Po48         1       eth  1qtunl up      none                       a-1000(D)  lacp

--------------------------------------------------------------------------------
Port   VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0  --           down   --                                      --       1500

--------------------------------------------------------------------------------
Vethernet     VLAN   Type Mode   Status  Reason                     Speed
--------------------------------------------------------------------------------
Veth721       4047   virt trunk  up      none                       auto
Veth722       1      virt trunk  up      none                       auto
Veth723       1      virt trunk  up      none                       auto
Veth724       1      virt trunk  up      none                       auto
Veth725       1      virt trunk  up      none                       auto
Veth726       4047   virt trunk  up      none                       auto
Veth727       4047   virt trunk  up      none                       auto
Veth728       4047   virt trunk  up      none                       auto
Veth736       1      virt trunk  up      none                       auto
Veth737       1      virt trunk  down    Administratively down      auto
Veth738       1      virt trunk  down    Administratively down      auto
Veth739       4047   virt trunk  up      none                       auto
Veth740       4047   virt trunk  up      none                       auto
Veth741       4047   virt trunk  up      none                       auto
Veth757       4047   virt trunk  up      none                       auto
Veth758       1      virt trunk  up      none                       auto
Veth759       1      virt trunk  up      none                       auto
Veth760       1      virt trunk  up      none                       auto
Veth761       1      virt trunk  up      none                       auto
Veth762       4047   virt trunk  up      none                       auto
Veth763       4047   virt trunk  up      none                       auto
Veth764       4047   virt trunk  up      none                       auto
Veth772       1      virt trunk  down    Administratively down      auto
Veth773       1      virt trunk  down    Administratively down      auto
Veth774       1      virt trunk  down    Administratively down      auto
Veth775       4047   virt trunk  up      none                       auto
Veth776       4047   virt trunk  up      none                       auto
Veth777       4047   virt trunk  up      none                       auto
Veth792       1      virt trunk  up      none                       auto
Veth793       1      virt trunk  up      none                       auto
Veth794       1      virt trunk  up      none                       auto
Veth797       1      virt trunk  up      none                       auto
Veth798       1      virt trunk  up      none                       auto
Veth800       1      virt trunk  up      none                       auto
Veth801       1      virt trunk  up      none                       auto
Veth802       1      virt trunk  up      none                       auto
Veth805       1      virt trunk  up      none                       auto
Veth806       1      virt trunk  up      none                       auto
Veth2182      1      virt trunk  up      none                       auto
Veth2328      1      virt trunk  up      none                       auto
Veth2482      1      virt trunk  up      none                       auto
Veth2502      1      virt trunk  up      none                       auto
Veth2503      1      virt trunk  down    nonParticipating           auto
Veth2504      1      virt trunk  up      none                       auto
Veth2636      1      virt trunk  up      none                       auto
Veth2637      1      virt trunk  up      none                       auto
Veth2638      1      virt trunk  down    nonParticipating           auto
Veth2639      1      virt trunk  up      none                       auto
Veth2640      1      virt trunk  up      none                       auto
Veth2660      1      virt trunk  up      none                       auto
```

```
Veth2661      1      virt trunk  down    nonParticipating         auto
Veth2662      1      virt trunk  up      none                     auto
Veth2788      1      virt trunk  up      none                     auto
Veth2789      1      virt trunk  down    nonParticipating         auto
Veth2790      1      virt trunk  up      none                     auto
Veth2791      1      virt trunk  up      none                     auto
firepower(fxos)#
```

Le tableau suivant décrit les colonnes affichées par la commande `show interface brief`.

Tableau 5 : Champs show interface brief

Champ	Description
Identifiant de l'interface	*Identifiant de l'interface ou du port*
VLAN	*Identifiant de VLAN*
Type	**Type d'interface :** `eth` : interface Ethernet dédiée `virt` : interface virtuelle
Mode	**Mode de fonctionnement du port :** `layer3` : interface de couche 3 `access` : port d'accès `trunk` : port de ligne principale `pvlan` : VLAN privé `fabric` : port de structure (F_port) `1qtunl` : port 1q-tunnel (802.1Q tunnel) `f-path` : chemin de structure
État	**État de l'interface :** `up` : le port est opérationnel `down` : le port n'est pas opérationnel `testing` : l'interface est en mode test; aucun paquet opérationnel ne peut être transmis `trunking` : les solutions de liaisons sont activées `link up` : la liaison est active, mais le port n'est pas encore entièrement opérationnel pour le trafic vers le plan de données, bien qu'il le soit pour les protocoles de contrôle

Champ	Description
Motif	

Champ	Description
	Raison détaillée de l'état de l'interface : Initialisation de l'émetteur-récepteur Autre Aucun Défaillance matérielle Échec du diagnostic Erreur désactivée Défaillance logicielle du port Échec de la liaison ou absence de connexion hors ligne Non-participation Initialisation en cours... Inactif Administrativement en panne Admin canal arrêté Suspension (interface) Suspension (port) Mise à jour de l'appartenance au canal en cours RCF en cours Isolement dû à une défaillance ELP Isolement dû à une défaillance ESC Isolement dû à un chevauchement de domaines Isolement dû à un échec d'affectation d'ID de domaine Isolement dû à l'isolement de l'ePort du domaine distant Isolement dû à une reconfiguration de structure non valide Isolement dû à la désactivation du gestionnaire de domaine Isolement dû à une défaillance de fusion de zones Isolement dû à un vsan non configuré sur l'homologue Administrateur de l'interface parente arrêté Interface src de port de tunnel non associée Interface supprimée SFP absent Erreur, désactivation due à un fournisseur SFP non pris en charge

Champ	Description
	Erreur, désactivation due à un mode de port d'administration incompatible
	Erreur, désactivation due à une vitesse de port d'administration incompatible
	Suspension due à un mode incompatible
	Suspension due à une vitesse incompatible
	Suspension due à un WWN de commutateur distant incompatible
	Isolement dû à l'absence de réponse du gestionnaire de domaine de l'autre côté
	Erreur, désactivation due à une défaillance EPP
	Isolement dû à une incompatibilité de vsan de port
	Isolement dû à un bouclage de port vers le même commutateur
	Mise à niveau de carte de ligne en cours
	Erreur, désactivation due à un port d'administration incompatible rxbbcredit
	Erreur, désactivation due à un port d'administration incompatible rxbufsize
	Aucun membre opérationnel
	Isolement dû à l'absence de réponse d'un serveur de zone distant
	Erreur, désactivation car la première interface de ce groupe est E
	Erreur, désactivation car d'autres interfaces de ce groupe ne sont pas arrêtées
	Connexion TCP fermée par l'homologue
	Connexion TCP réinitialisée par l'homologue
	Nombre maximal de retransmissions TCP atteint
	Expiration du minuteur de maintien d'activité TCP
	Expiration du minuteur de persistance TCP
	Liaison Ethernet parente hors service
	Ethernet parent hors service
	Modification de la configuration par l'administrateur
	Port source du tunnel supprimé
	Module source du tunnel hors ligne
	Mauvaise configuration possible du canal de port
	Isolement dû à une défaillance de sécurité du port
	Isolement dû à une défaillance de liaison de la structure
	Isolement dû à l'absence de VSAN commun avec l'homologue sur la ligne réseau
	VSAN Ficon désactivé
	Connexion non valide : Ficon non configuré sur l'homologue

Champ	Description
	Port bloqué en raison de Ficon
	Erreur, désactivation due à des des tampons de performances rxbbcredit incompatibles du port d'administration
	Suspension en raison d'un nombre excessif de flogis non valides
	Suspension en raison de la sécurité du port
	Isolement dû à une défaillance ELP, incompatibilité de révision
	Isolement dû à une défaillance ELP, erreur de paramètre de classe F
	Isolement dû à une défaillance ELP, erreur de paramètre de classe N
	Isolement dû à une défaillance ELP, code de contrôle de flux non valide
	Isolement dû à un paramètre de contrôle de flux non valide de défaillance ELP
	Isolement dû à une défaillance ELP, nom de port non valide
	Isolement dû à une défaillance ELP, nom de commutateur non valide
	Isolement dû à une défaillance ELP, incompatibilité R_A_TOV ou E_D_TOV
	Isolement dû à une défaillance ELP, boucle avec retour détectée
	Isolement dû à une défaillance ELP, crédit B2B de transmission non valide
	Isolement dû à une défaillance ELP, taille de charge utile non valide
	Erreur, désactivation due à une mauvaise configuration du canal de port
	Défaillance de liaison, port inutilisable
	Défaillance de liaison, perte de signal
	Défaillance de liaison, perte de synchronisation
	Défaillance de liaison, NOS reçu
	Défaillance de liaison, OLS reçu
	Défaillance de liaison, échec de renégociation
	Défaillance de liaison, réinitialisation de liaison en échec, file d'attente de réception non vide
	Défaillance de liaison, indications de perte de crédit excessives
	Défaillance de liaison, débordement de la file d'attente de réception
	Erreur, désactivation due à des interruptions de port excessives
	Défaillance de liaison, initialisation de boucle en échec, file d'attente de réception non vide
	Défaillance de liaison, réinitialisation de liaison en échec, file d'attente non vide
	Défaillance de liaison, délai d'expiration OPny alors que la file d'attente de réception n'est pas vide

Champ	Description
	Défaillance de liaison, OPny renvoyé alors que la file d'attente de réception n'est pas vide
	Défaillance de liaison, réinitialisation de liaison en échec, file d'attente non vide
	Défaillance de liaison ou absence de connexion
	Isolement dû à une défaillance FCSP
	Erreur de somme de contrôle SFP
	Suspension due à une défaillance de diagnostic de boucle avec retour externe
	Échange de liaison de structure non valide
	Isolement dû à une incompatibilité TOV
	Erreur, désactivation due à ficon non activé
	Erreur, désactivation due à l'absence de numéro de port ficon pour l'interface logique
	Ficon en cours d'activation
	Port inactif car un masque d'interdiction est configuré pour le port E/TE
	Arrêt progressif
	Tous les VSAN ne sont pas actifs sur la ligne réseau
	Isolement dû à la liaison de structure, WWN commutateur homologue introuvable
	Isolement dû à la liaison de structure, incompatibilité de domaine homologue
	Isolement dû à la liaison de structure, incompatibilité de base de données
	Isolement dû à la liaison de structure, absence de réponde de l'homologue
	Suspension due à une suspension dynamique vsan
	Suspension due à un vsan dynamique introuvable
	Tous les ports suivis sont inactifs
	Suspension en tant que mode de crédit étendu non autorisé pour les ports de boucle
	Isolement dû à une mauvaise configuration du canal de port
	L'appareil homologue ne prend pas en charge les canaux de ports
	Isolement lors du démarrage du port
	Isolement dû à un domaine non autorisé
	Isolement dû à un chevauchement de domaines IVR virtuels
	Hors service
	Échec de l'authentification
	Détection de liaison unidirectionnelle

Champ	Description
	Remarque FXOS ne prend pas en charge la détection de liaison unidirectionnelle (UDLD); ignorer toute référence à UDLD. Boucle Tx Rx UDLD Incompatibilité de voisin UDLD Écho vide UDLD UDLD a détecté une défaillance de liaison en mode dynamique Erreur de type de connecteur de port Erreur, désactivation due à une limite de réinitialisation atteinte Numéro de port en double dans VSAN RCF interne en cours WWN en double Autre demande EPP non valide reçue Isolement dû à une raison inconnue Configuration de tunnel incomplète. Échec de programmation du matériel Aucune route vers l'adresse de destination du tunnel Module supprimé Échec d'allocation MTU Tous les paramètres n'ont pas été configurés SFP non inséré Émetteur-récepteur non inséré SFP non certifié Cisco Émetteur-récepteur non certifié Cisco Seuil de taux d'erreurs binaires dépassé Défaillance de liaison, réinitialisation de liaison Défaillance de liaison, initialisation du port en échec Défaillance ELP, WWN homologue entièrement nul reçu Isolement dû à un chemin préféré Isolement de redirection FC Licence d'activité de port non disponible Isolement SDM Échec d'allocation FCID Désactivation externe

Champ	Description
	Autorisation en attente
	Offre groupée en veille à chaud
	Erreur de canal désactivé
	Fonctionnalités de port inconnues
	Incompatibilité entre le VRF source et le VRF de transport
	VRF de transport avec référence en amont
	La configuration identique de deux interfaces de tunnel n'est pas autorisée
	Trop de liaisons intermittente dans un court intervalle
	VLAN principal inactif
	VRF inutilisable
	Échec d'établissement de liaison interne
	Désactivation de l'erreur déclenchée par BPDUGuard
	Le port est désactivé
	Erreur, désactivation due à une violation de sécurité
	L'interface de tunnel est inactive car le mode n'est pas configuré
	L'interface de tunnel est inactive car la source n'est pas configurée
	L'interface de tunnel est inactive car la destination n'est pas configurée
	L'interface de tunnel est inactive en raison de l'adresse IP non résolue associée à l'interface source de tunnel
	L'interface de tunnel est inactive en raison de l'adresse IP non résolue associée à la destination de tunnel
	L'interface de tunnel est inactive car le VRF configuré sur celle-ci est inactif
	L'interface est désactivée en erreur en raison d'une incohérence STP sur la liaison homologue VPC
	Interface désactivée en erreur en raison d'un échec de définition d'état de port STP
	Le canal de port est inactif en raison d'une suspension par vpc
	La configuration vpc est en cours
	La liaison homologue vpc est inactive
	Vpc inactif en l'absence de réponse de l'homologue
	Vpc inactif en raison de l'échec de la vérification de la compatibilité
	Pas assez d'entrées libres dans la banque TCAM
	L'interface de tunnel est inactive car l'interface source de tunnel est inactive
	Erreur, désactivation en raison d'un conflit d'adresses IP
	Le port de structure épinglé est inactif

Champ	Description
	Port de structure non valide
	SFP de structure FEX non valide
	Délai d'expiration SDP/Incompatibilité SFP
	Incompatibilité d'identité FEX
	ID FEX non configuré sur le port de structure
	Erreur, désactivation en raison d'une défaillance d'application de la politique IP QoS
	Échec d'allocation d'adresse MAC au routeur
	Le VLAN/BD n'existe pas
	Le VLAN/BD est inactif
	Le type de VLAN n'est pas valide
	Multiples ID MSAP DCX reçus pour le port
	DCX a reçu 100 PDU sans accusé de réception
	Échec de vérification de compatibilité IP QOS DCBXP
	Suspension due à des min-links
	Interface parente inactive
	Inactif - port M1 non autorisé dans le VLAN de mode FabricPath
	La vitesse prise en charge par l'émetteur-récepteur ne correspond pas à la vitesse configurée sur le port
	Échec d'authentification de l'émetteur-récepteur sur le port
	Échec d'activation de la liaison de l'homologue vPC+, ID de commutateur FabricPath non configuré
	Échec d'activation de la liaison de l'homologue vPC+, le port n'est pas configuré comme port FabricPath.
	L'émetteur-récepteur ne respecte pas la conformité Ethernet
	La configuration de Speed-Group ne correspond pas au type d'émetteur-récepteur
	Suspension due à l'absence de réception de PDU LACP de l'homologue

Champ	Description
Vitesse	**Vitesse de l'interface :** `Auto` : négociation automatique `10` : 10 Mbit/s `100` : 100 Mbit/s `Auto110` : négociation automatique entre 10 et 100 Mbit/s `1000` : 1 Gbit/s `10G` : 10 Gbit/s `a-10` : négociation automatique, 16 Mbit/s `a-100` : négociation automatique, 106 Mbit/s `a-1000` : négociation automatique, 1 006 Mbit/s `a-10G` : négociation automatique, 10 006 Mbit/s `40G` : 40 000 Mbit/s `100G` : 100 000 Mbit/s `a-40G` : négociation automatique, 40 006 Mbit/s `a-100G` : négociation automatique, 100 006 Mbit/s **Remarque** Une entrée de vitesse accompagnée de `(D)` indique une interface dédiée, tandis qu'une entrée de vitesse accompagnée d'un `(S)` indique qu'elle est partagée.
Numéro de canal de port	Numéro d'identification du canal de port auquel l'interface est affectée, le cas échéant.
Protocole	**Protocole de canal de port :** `none` : le protocole LCAP (Link Aggregation Control Protocol) n'est pas activé `lcap` : le protocole LCAP est activé
VRF	Nom de l'instance de routage et transfert virtuels (VRF) à laquelle le port est affecté, le cas échéant.
Adresse IP	Adresse IP du port
MTU	Taille de l'unité de transfert maximale (MTU) du port

Commandes associées

Commande	Description
show port	En mode connect fxos, affiche les informations sur le port.
show vlan	En mode connect fxos, affiche les informations sur le VLAN.

show inventory

Pour afficher des informations sur le châssis et ses modules installés, utilisez la commande **show inventory** en mode châssis.

show inventory [**detail** | **expand** | **fabric** | **fan** | **fi-iom** | **iom** | **psu** | **server** | **unspecified**]

Description de la syntaxe

detail	(Facultatif) Utilisez ce mot clé pour afficher des informations détaillées sur le châssis lui-même.
expand	(Facultatif) Utilisez ce mot clé pour afficher des informations développées sur chaque composant du châssis.
fabric	(Facultatif) Utilisez ce mot clé pour afficher les informations sur le transport de structures. Le mot clé **detail** est également disponible.
fan	(Facultatif) Affiche des informations sur chaque module de ventilation du châssis. Le mot clé **detail** est également disponible.
fi-iom	(Facultatif) Affiche des informations sur les modules I/O du commutateur d'interconnexion de structure. Le mot clé **detail** est également disponible.
iom	(Facultatif) Affiche des informations sur les modules d'entrée et de sortie du châssis. Le mot clé **detail** est également disponible.
psu	(Facultatif) Affiche des informations sur les blocs d'alimentation installés. Le mot clé **detail** est également disponible.
server	(Facultatif) Répertorie les informations sur chaque composant du serveur. Le mot clé **detail** est également disponible.
unspecified	(Facultatif) Répertorie les informations sur le composant du châssis. Le mot clé **detail** est également disponible.

Modes de commande

scope chassis/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous pouvez utiliser cette commande sans arguments ni mots clés pour afficher les informations de base sur le châssis.

Exemple

Cet exemple montre comment afficher l'inventaire matériel développée du châssis :

```
firepower# scope chassis
firepower /chassis # show inventory expand
Chassis 1:
    Servers:
        Server 1/1:
            Equipped Product Name: Cisco Firepower 9000 Series Security Module
            Equipped PID: FPR9K-SM-24
            Equipped VID: V01
            Equipped Serial (SN): FCH19057S0L
            Slot Status: Equipped
            Acknowledged Product Name: Cisco Firepower 9000 Series Security Module
            Acknowledged PID: FPR9K-SM-24
            Acknowledged VID: V01
            Acknowledged Serial (SN): FCH19057S0L
            Acknowledged Memory (MB): 262144
            Acknowledged Effective Memory (MB): 262144
            Acknowledged Cores: 24
            Acknowledged Adapters: 2

        Server 1/2:
            Equipped Product Name: Cisco Firepower 9000 Series Security Module
            Equipped PID: FPR9K-SM-24
            Equipped VID: V01
            Equipped Serial (SN): FCH19057RTY
            Slot Status: Equipped
            Acknowledged Product Name: Cisco Firepower 9000 Series Security Module
            Acknowledged PID: FPR9K-SM-24
            Acknowledged VID: V01
            Acknowledged Serial (SN): FCH19057RTY
            Acknowledged Memory (MB): 262144
            Acknowledged Effective Memory (MB): 262144
            Acknowledged Cores: 24
            Acknowledged Adapters: 2

        Server 1/3:
            Equipped Product Name:
            Equipped PID:
            Equipped VID:
            Equipped Serial (SN):
            Slot Status: Empty
            Acknowledged Product Name:
            Acknowledged PID:
            Acknowledged VID:
            Acknowledged Serial (SN):
            Acknowledged Memory (MB):
            Acknowledged Effective Memory (MB):
            Acknowledged Cores:
            Acknowledged Adapters:

    PSU 1:
        Presence: Equipped
        Product Name: Cisco Firepower 9000 Series  AC Power Supply
        PID: FPR9K-PS-AC
        VID: V00
        Vendor: Cisco Systems Inc
        Serial (SN): DTM190705G3
        HW Revision: 0

    PSU 2:
```

```
        Presence: Equipped
        Product Name: Cisco Firepower 9000 Series  AC Power Supply
        PID: FPR9K-PS-AC
        VID: V00
        Vendor: Cisco Systems Inc
        Serial (SN): DTM190705J8
        HW Revision: 0

    Fan Modules:
        Tray 1 Module 1:
            Presence: Equipped
            ID         PID          Vendor          Serial (SN) HW Revision
            ---------- ------------ --------------- ----------- -----------
                     1 FPR9K-FAN    Cisco Systems I NWG190200LD 0
                     2 FPR9K-FAN    Cisco Systems I NWG190200LD 0

        Tray 1 Module 2:
            Presence: Equipped
            ID         PID          Vendor          Serial (SN) HW Revision
            ---------- ------------ --------------- ----------- -----------
                     1 FPR9K-FAN    Cisco Systems I NWG190200ML 0
                     2 FPR9K-FAN    Cisco Systems I NWG190200ML 0

        Tray 1 Module 3:
            Presence: Equipped
            ID         PID          Vendor          Serial (SN) HW Revision
            ---------- ------------ --------------- ----------- -----------
                     1 FPR9K-FAN    Cisco Systems I NWG190200KZ 0
                     2 FPR9K-FAN    Cisco Systems I NWG190200KZ 0

        Tray 1 Module 4:
            Presence: Equipped
            ID         PID          Vendor          Serial (SN) HW Revision
            ---------- ------------ --------------- ----------- -----------
                     1 FPR9K-FAN    Cisco Systems I NWG190200L8 0
                     2 FPR9K-FAN    Cisco Systems I NWG190200L8 0

    Switch IOCard 1:
        Side: Left
        Fabric ID: A
        Product Name: Cisco FPR9K-SUP
        PID: FPR9K-SUP
        VID: V01
        Vendor: Cisco Systems, Inc.
        Serial (SN): JAD190800VU
        HW Revision: 0

Fabric Card 1:
    Description: Firepower 9300 Supervisor
    Number of Ports: 8
    State: Online
    Vendor: Cisco Systems, Inc.
    Model: FPR9K-SUP
    HW Revision: 0
    Serial (SN): JAD190800VU
    Perf: N/A
    Power State: Online
    Presence: Equipped
    Thermal Status: N/A
    Voltage Status: N/A


Fabric Card 2:
    Description: Firepower 4x100G QSFP28 NM
```

```
    Number of Ports: 4
    State: Online
    Vendor: Cisco Systems, Inc.
    Model: FPR-NM-4X100G
    HW Revision: 0
    Serial (SN): JAD2151037Z
    Perf: N/A
    Power State: Online
    Presence: Equipped
    Thermal Status: N/A
    Voltage Status: N/A


Fabric Card 3:
    Description: Firepower 4x40G QSFP NM
    Number of Ports: 16
    State: Online
    Vendor: Cisco Systems, Inc.
    Model: FPR9K-NM-4X40G
    HW Revision: 0
    Serial (SN): JAD191601DK
    Perf: N/A
    Power State: Online
    Presence: Equipped
    Thermal Status: N/A
    Voltage Status: N/A


firepower /chassis #
```

Commandes associées

Commande	Description
show environment	Affiche les informations sur l'état du matériel du châssis.

show inventory (connect fxos)

Pour afficher des informations sur l'inventaire du châssis, y compris le nom, la description, le PID et le numéro de série des modules superviseur et réseau, utilisez la commande **show inventory** en mode connect fxos.

show inventory

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

connect fxos

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous pouvez utiliser cette commande sans arguments ni mots clés pour afficher les informations sur le châssis ou les modules.

Exemple

Cet exemple montre comment afficher les informations sur l'inventaire du châssis ou les modules :

```
firepower#
firepower# connect fxos
...
firepower(fxos)# show inventory
NAME: "Chassis", DESCR: "Cisco Firepower 9300 Security Appliance"
PID: FPR9K-SUP         , VID: V08 , SN: ABCD123456

NAME: "Module 1", DESCR: "Firepower 9300 Supervisor"
PID: FPR9K-SUP         , VID: V08 , SN: CBDA123456

NAME: "Module 2", DESCR: "Firepower 4x40G QSFP NM"
PID: FPR-NM-4X40G      , VID: V01 , SN: CBDA654321
```

show ip-block

Pour afficher la liste des blocs d'adresses IPv4 actuellement définis pour l'accès au service, utilisez la commande **show ip-block**.

show ip-block [[*ip_address prefix_length* { **https** | **snmp** | **ssh** }] | **detail**]

Description de la syntaxe

ip_address prefix_length { **https** | **snmp** | **ssh** }	(Facultatif) Pour afficher un bloc d'adresses IPv4 spécifique, saisissez ces informations d'adresse : • Adresse de début du bloc d'adresses IPv4. • Longueur du préfixe; détermine le nombre d'adresses du bloc. La valeur peut être comprise entre 0 et 32. • Service (HTTPS, SNMP ou SSH) auquel le bloc d'adresses est affecté.
detail	(Facultatif) L'ajout du mot clé **detail** affiche l'adresse, le préfixe et le service de chaque bloc IPv4 sur des lignes distinctes.

Modes de commande

Mode de service

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour répertorier les blocs d'adresses IPv4 actuellement autorisés. Jusqu'à 25 blocs différents peuvent être configurés pour chaque service.

Exemple

Cet exemple montre comment afficher des informations détaillées sur le bloc d'adresses IPv4 :

```
FP9300-A # scope system
FP9300-A /system # scope services
FP9300-A /system/services # show ip-block detail

    IP Address: 209.165.201.1
    Prefix Length: 24
    Protocol: https

Permitted IP Block:
    IP Address: 0.0.0.0
    Prefix Length: 0
    Protocol: snmp

    IP Address: 209.165.202.129
    Prefix Length: 24
    Protocol: ssh
FP9300-A /system/services #
```

Commandes associées

Commande	Description
create ip-block	Crée un bloc IPv4.
delete ip-block	Supprime un bloc IPv4 existant.

show ip-pool

Pour afficher la liste des ensembles d'adresses IP disponibles sur le système, utilisez la commande **show ip-pool**.

show ip-pool [*detail* | *expand* | *name*]

Description de la syntaxe

detail	(Facultatif) Affiche les informations sur les ensembles d'adresses IP d'un ensemble spécifique. Les mots clés **expand** et **expand** sont disponibles avec cette option.
expand	(Facultatif) Affiche les informations développées sur l'ensemble d'adresses IP. Le mot clé **detail** est disponible avec cette option.
name	Répertorie les informations détaillées sur l'ensemble d'adresses IP.

Modes de commande

scope org

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope org.

Exemple

Cet exemple montre comment afficher les informations sur un ensemble d'adresses IP :

```
Firepower /fabric-interconnect # scope org
Firepower /org # show ip-pool
IP Pool:
    Name                  Size       Assigned   Management mode
    -------------------- ---------- ---------- ---------------
    ext-mgmt                     0          0 Internal
    iscsi-initiator-pool         0          0 Internal
    ssp-ippool-app-ccl         126          0 Internal
    ssp-ippool-inter-mgmt
                               117          0 Internal
```

Exemple

Cet exemple montre comment afficher les informations détaillées de tous les ensembles d'adresses IP disponibles :

```
Firepower /org # show ip-pool expand detail

IP Pool:
    Name: ext-mgmt
    Size: 0
    Assigned: 0
    IPv4 Size: 0
```

```
IPv4 Assigned: 0
IPv6 Size: 0
IPv6 Assigned: 0
Descr:
Assignment Order: Default
Management mode: Internal
Guid: 00000000-0000-0000-0000-000000000000
Net bios enabled or disabled: Not Active
DHCP enaled or disabled: Not Supported
Name: iscsi-initiator-pool
Size: 0
Assigned: 0
IPv4 Size: 0
IPv4 Assigned: 0
IPv6 Size: 0
IPv6 Assigned: 0
Descr:
Assignment Order: Default
Management mode: Internal
Guid: 00000000-0000-0000-0000-000000000000
Net bios enabled or disabled: Not Active
DHCP enaled or disabled: Not Supported
Name: ssp-ippool-app-ccl
Size: 126
Assigned: 0
IPv4 Size: 126
IPv4 Assigned: 0
IPv6 Size: 0
IPv6 Assigned: 0
Descr: SSP service profile IP Pool for app ccl vlan
Assignment Order: Default
Management mode: Internal
Guid: 00000000-0000-0000-0000-000000000000
Net bios enabled or disabled: Not Active
DHCP enaled or disabled: Not Supported
```

show ipsec-log

Pour afficher les journaux de connexion IPSec, utilisez la commande **show ipsec-log**.

show ipsec-log

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Mode IPSec

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez la commande **set log-level** pour modifier la quantité d'informations affichées par ces journaux.

Exemple

Cet exemple montre comment afficher le contenu du fichier journal IPSec :

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # show ipsec-log
Feb 10 23:40:02 15[CFG] <test-connection|69>   using trusted ca certificate "C=US, ST=CA,
L=SJC, O=Cisco, OU=STBU, CN=CA, E=ssp@ssp.net"
Feb 10 23:40:02 15[CFG] <test-connection|69>   reached self-signed root ca with a path
length of 0
Feb 10 23:40:02 15[CFG] <test-connection|69>   crl correctly signed by "C=US, ST=CA, O=CA1,
 OU=ca1, CN=InterCA1, E=ca1@ca.net"
Feb 10 23:40:02 15[CFG] <test-connection|69>   crl is valid: until Mar 12 22:30:51 2017
Feb 10 23:40:02 15[CFG] <test-connection|69>   using cached crl
Feb 10 23:40:02 15[CFG] <test-connection|69> certificate status is good
Feb 10 23:40:02 15[CFG] <test-connection|69>   using trusted ca certificate "C=US, ST=CA,
L=SJC, O=Cisco, OU=STBU, CN=CA, E=ssp@ssp.net"
Feb 10 23:40:02 15[CFG] <test-connection|69> checking certificate status of "C=US, ST=CA,
O=CA1, OU=ca1, CN=InterCA1, E=ca1@ca.net"
Feb 10 23:40:02 15[CFG] <test-connection|69>   fetching crl from
'file:///opt/certstore/ssp2-tp.crl' ...
Feb 10 23:40:02 15[CFG] <test-connection|69> issuer of fetched CRL 'C=US, ST=CA, O=CA1,
OU=ca1, CN=InterCA1, E=ca1@ca.net' does not match CRL issuer
'56:71:f1:d9:b1:62:fd:c3:2b:4d:cb:6b:01:85:ea:75:e5:0e:99:0d'
Feb 10 23:40:02 15[CFG] <test-connection|69>   fetching crl from
'http://192.168.0.81/interca_inuse.crl.pem' ...
Feb 10 23:40:02 15[CFG] <test-connection|69>   using trusted certificate "C=US, ST=CA,
L=SJC, O=Cisco, OU=STBU, CN=CA, E=ssp@ssp.net"
Feb 10 23:40:02 15[CFG] <test-connection|69>   crl correctly signed by "C=US, ST=CA, L=SJC,
 O=Cisco, OU=STBU, CN=CA, E=ssp@ssp.net"
Feb 10 23:40:02 15[CFG] <test-connection|69>   crl is valid: until Mar 12 22:30:49 2017
Feb 10 23:40:02 15[CFG] <test-connection|69> certificate status is good
Feb 10 23:40:02 15[CFG] <test-connection|69>   reached self-signed root ca with a path
length of 1
Feb 10 23:40:02 15[IKE] <test-connection|69> authentication of 'C=US, ST=CA, O=Cisco,
OU=STBU, CN=SSP, E=ssp@ssp.net' with RSA signature successful
Feb 10 23:40:02 15[IKE] <test-connection|69> IKE_SA test-connection[69] established between
 192.168.0.174[C=US, ST=CA, O=Cisco, OU=STBU, CN=SSP]
```

```
FP9300-A /security/ipsec #
```

Commandes associées

Commande	Description
set log-level	Définit la verbosité du journal IPSec.

show ipv6-block

Pour afficher la liste des blocs d'adresses IPv6 actuellement définis pour l'accès au service, utilisez la commande **show ipv6-block**.

show ipv6-block [[*ipv6_address prefix_length* { **https** | **snmp** | **ssh** }] | **detail**]

Description de la syntaxe

ipv6_address prefix_length { **https** | **snmp** | **ssh** }	(Facultatif) Pour afficher un bloc d'adresses IPv6 spécifique, saisissez ces informations d'adresse : • Adresse de début du bloc d'adresses IPv6. • Longueur du préfixe; détermine le nombre d'adresses du bloc. La valeur peut être comprise entre 0 et 128. • Service (HTTPS, SNMP ou SSH) auquel le bloc d'adresses est affecté.
detail	(Facultatif) L'ajout du mot clé **detail** affiche l'adresse, le préfixe et le service de chaque bloc IPv6 sur des lignes distinctes.

Modes de commande

Mode de service

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour répertorier les blocs d'adresses IPv6 actuellement autorisés. Jusqu'à 25 blocs différents peuvent être configurés pour chaque service.

Exemple

Cet exemple montre comment afficher des informations détaillées sur le bloc d'adresses IPv4 :

```
FP9300-A # scope system
FP9300-A /system # scope services
FP9300-A /system/services # show ip-block detail

    IP Address: 2001:DB8:1::1
    Prefix Length: 64
    Protocol: https

Permitted IP Block:
    IP Address: 0:0:0:0:0:0:0:0
    Prefix Length: 0
    Protocol: snmp

    IP Address: 2001:DB8:0:ABCD::1
    Prefix Length: 64
    Protocol: ssh
FP9300-A /system/services #
```

Commandes associées

Commande	Description
create ipv6-block	Crée un bloc IPv6.
delete ipv6-block	Supprime un bloc IPv6 existant.

show ipv6-if

Pour afficher les informations actuelles sur l'interface de gestion IPv6, utilisez la commande **show ipv6-if**.

Description de la syntaxe

detail	Répertorie les informations détaillées sur l'interface de gestion IPv6.
fsm status	Répertorie les informations sur l'état de la machine à états finis (FSM) liées à l'interface de gestion IPv6.

Modes de commande

Mode de configuration IPv6 (fabric-interconnect/ipv6-config)

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande affiche uniquement les informations sur l'interface de gestion IPv6.

Exemple

Cet exemple montre comment afficher les informations sur l'interface de gestion IPv6 :

```
FP9300-A# scope fabric-interconnect
FP9300-A# scope ipv6-config
FP9300-A /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
IPv6 Address                       Prefix     IPv6 Gateway
---------------------------------- ---------- ------------
2001::8998                         64         2001::1
FP9300-A /fabric-interconnect/ipv6-config #


FP9300-A# scope fabric-interconnect
FP9300-A# scope ipv6-config
FP9300-A /fabric-interconnect/ipv6-config # show ipv6-if
Management IPv6 Interface:
    IPv6 Address                              Prefix     IPv6 Gateway
       AutoCfg-method  ReadyCfg-method IPv6 state      ND state
    ------------------------------------- ----------
---------------------------------------- --------------- --------------- ---------------
--------
    ::                                        64         2008::1
       Stablesec       Notset          Enable          Enable
```

Commandes associées

Commande	Description
scope fabric-interconnect	Permet d'accéder au mode interconnexion de structure.
scope ipv6-config	Permet d'accéder au mode configuration IPv6.

show keyring

Pour afficher les informations sur les certificats importés, utilisez la commande **show keyring**.

show keyring [**detail** | **name**]

Description de la syntaxe

detail	Affiche les informations sur les certificats importés.
name	(Facultatif) Affiche le contenu du certificat importé spécifié.

Modes de commande

scope security

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

show keyring est une sous-commande de la commande **show** dans scope security.

Exemple

Cet exemple montre comment afficher les certificats importés et vérifier la valeur d'état de ces certificats :

```
Firepower# scope security
Firepower# show keyring
Name            Key pair type   RSA key modulus Elliptic Curve TrustpointCA
--------------- --------------- --------------- --------------- -------------
default         Rsa             Mod2048         Ec         invalid
```

Cet exemple montre comment afficher le contenu des certificats importés.

```
Firepower /security # show keyring detail
Keyring default:
    RSA key modulus: Mod2048
    Trustpoint CA:
    Certificate status: Self Signed Certificate
    Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            6f:fe:83:56:a2:60:da:fd:66:f9:50:75:47:bd:48:da:86:dc:81:81
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = MOIO-2
        Validity
            Not Before: May 26 12:14:42 2012 GMT
            Not After : May 26 12:14:42 2014 GMT
        Subject: CN = MOIO-2
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:d0:78:39:a6:c3:b7:dd:f3:c8:8c:90:5e:6c:43:
                    9b:a0:d3:40:15:06:c9:cc:3b:d8:6c:f1:51:fc:5a:
                    09:2c:7c:eb:f7:74:25:aa:1d:94:5c:d7:6e:95:61:
                    6b:8d:d7:52:23:c8:6c:c7:86:ef:a9:cf:f4:41:65:
                    2a:7f:9d:f9:b5:d3:1e:15:91:6e:b5:3d:4a:a7:49:
```

```
                    d5:a0:cb:4e:8e:1a:e7:55:f3:aa:f9:f3:2a:e8:36:
                    b6:e8:a8:15:ad:54:b2:8a:f8:f3:b1:2f:ab:8f:df:
                    c8:28:a6:1d:08:df:25:bd:58:8c:e0:8e:8f:ce:db:
                    5a:68:68:ce:9a:37:37:66:a8:fa:8c:50:4f:54:0e:
                    e8:cf:10:a3:70:6a:f9:08:c5:45:5d:38:4f:70:2f:
                    7a:85:ca:37:e6:67:bf:63:77:c1:24:89:8f:d0:7f:
                    1d:a2:db:08:ad:33:33:53:ee:95:a9:2f:a3:d6:c1:
                    bf:d7:de:cd:ac:60:e6:db:2c:1f:20:81:14:c8:f5:
                    ce:3b:ea:aa:ed:c6:d9:c3:32:5f:f7:e7:36:ce:79:
                    31:19:18:43:42:62:4a:fa:f6:77:36:85:04:49:e2:
                    e7:40:0e:f6:9f:a9:a3:9c:c5:23:5e:c8:bc:50:fd:
                    f6:36:7f:e0:46:59:70:3d:82:84:45:a7:59:23:35:
                    80:bd
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                DNS:MOIO-2, IP Address:10.0.0.6
    Signature Algorithm: sha256WithRSAEncryption
         cb:b6:f5:2a:96:4d:b9:a9:18:9f:00:fa:b6:e0:c0:0e:50:51:
         79:74:ca:21:25:e5:ae:e1:fe:03:dc:0b:9b:f7:c0:02:d2:72:
         e7:da:fd:f2:76:25:12:27:5f:bc:38:14:80:31:8c:e1:8b:5f:
         f8:7b:14:28:7a:be:2a:22:b8:b5:ea:90:1d:69:af:38:1b:ae:
         5e:c3:3c:95:f3:9b:32:0b:af:cb:2a:0b:5d:d7:57:77:25:df:
         26:ef:5b:ec:fb:09:6e:87:60:fb:3a:14:de:09:5e:13:f6:a8:
         10:70:50:e0:dd:cf:6d:78:4f:5e:27:d0:ad:92:db:65:fe:d7:
         81:cf:fb:93:d3:1f:21:e1:3f:20:50:62:5b:d3:7d:80:49:82:
         99:fc:74:9a:c3:d8:29:bf:2a:cb:a5:33:4d:dd:04:d2:fe:2c:
         1d:81:27:cc:56:70:9d:3e:f0:5c:ef:3a:86:ef:21:0a:6b:da:
         6c:7a:aa:1a:43:86:8c:f0:89:92:38:71:83:d9:8a:6c:47:22:
         03:4d:84:05:69:57:e9:a4:e5:2b:e2:3c:de:63:a9:10:3c:19:
         f2:2e:55:de:04:3a:6f:f1:e4:20:1b:2f:2f:38:b6:96:9f:7a:
         6b:18:09:f5:89:cd:8a:bc:95:59:b0:91:e9:61:46:7f:6e:6a:
         7c:0e:95:d7
-----BEGIN CERTIFICATE-----
MIICyzCCAbOgAwIBAgIUb/6DVqJg2v1m+VB1R71I2obcgYEwDQYJKoZIhvcNAQEL
BQAwETEPMA0GA1UEAwwGTU9JTy0yMB4XDTEyMDUyNjEyMTQ0MloXDTE0MDUyNjEy
MTQ0MlowETEPMA0GA1UEAwwGTU9JTy0yMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA0Hg5psO33fPIjJBebEOboNNAFQbJzDvYbPFR/FoJLHzr93Qlqh2U
XNdulWFrjddSI8hsx4bvqc/0QWUqf535tdMeFZFutT1Kp0nVoMtOjhrnVfOq+fMq
6Da26KgVrVSyivjzsS+rj9/IKKYdCN8lvViM4I6PzttaaGjOmjc3Zqj6jFBPVA7o
zxCjcGr5CMVFXThPcC96hco35me/Y3fBJImP0H8dotsIrTMzU+6VqS+j1sG/197N
rGDm2ywfIIEUyPXOO+qq7cbZwzJf9+c2znkxGRhDQmJK+vZ3NoUESeLnQA72n6mj
nMUjXsi8UP32Nn/gRllwPYKERadZIzWAvQIDAQABoxswGTAXBgNVHREEEDAOggZN
T0lPLTKHBAoAAAYwDQYJKoZIhvcNAQELBQADggEBAMu29SqWTbmpGJ8A+rbgwA5Q
UXl0yiEl5a7h/gPcC5v3wALScufa/fJ2JRInX7w4FIAxjOGLX/h7FCh6vioiuLXq
kB1przgbrl7DPJXzmzILr8sqC13XV3cl3ybvW+z7CW6HYPs6FN4JXhP2qBBwUODd
z214T14n0K2S22X+14HP+5PTHyHhPyBQYlvTfYBJgpn8dJrD2Cm/KsulM03dBNL+
LB2BJ8xWcJ0+8FzvOobvIQpr2mx6qhpDhozwiZI4cYPZimxHIgNNhAVpV+mk5Svi
PN5jqRA8GfIuVd4EOm/x5CAbLy84tpafemsYCfWJzYq8lVmwkelhRn9uanwOldc=
-----END CERTIFICATE-----

    Zeroized: No
```

show lacp (connect fxos)

Pour afficher des informations sur le protocole LACP (Link Aggregation Control Protocol), utilisez la commande **show lacp**.

show lacp { **counters** | **interface** | **internal** | **issu-impact** | **neighbor** [**port-channel**] | **system-identifier** }

Description de la syntaxe

counters [**interface port-channel** *number*]	Affiche les statistiques de trafic LACP. (Facultatif) Vous pouvez spécifier un canal de port particulier pour afficher les statistiques sur ce canal de port uniquement; les numéros de canal de port valides sont compris entre 1 et 4096.
interface [**br-ethernet** *slot/chassis_num* | **ethernet** *slot/chassis_num*]	Affiche les informations LACP pour les interfaces Ethernet. (Facultatif) Vous pouvez spécifier une interface Ethernet de répartition ou une interface Ethernet pour afficher des informations sur l'interface en question.

internal { **debug** **buffer** | **event-history** | **info** | **mem-stats** }

Affiche les informations et les statistiques LCAP internes, selon le mot clé fourni :

- **debug buffer** : affiche les informations de débogage LACP.
- **event-history** : affiche les journaux des événements LACP; l'un des mots clés de type d'événement suivants est requis :
  - **errors** : affiche les journaux d'erreurs LCP.
  - **global** : affiche les transactions d'événements globales.
  - **ifindex** *index_ID* : affiche les journaux d'interface LACP pour l'index d'interface spécifié; les valeurs valides sont comprises entre 0 et 2147483647.
  - **interface** { **br-ethernet** *slot/chassis_num* | **ethernet** *slot/chassis_num* } : affiche les événements LACP pour l'interface Ethernet spécifiée.
  - **lock** : affiche les journaux de verrouillage LACP.
  - **msgs** : affiche les journaux des messages d'événements LACP.
- **info** : affiche les informations générales internes LACP. Les mots clés facultatifs suivants sont disponibles pour spécifier des types d'informations précis :
  - **all** : affiche toutes les informations LACP internes.
  - **global** : affiche les informations LACP globales.
  - **ifindex** *index_ID* : affiche les statistiques LACP pour l'index d'interface spécifié; les valeurs valides sont comprises entre 0 et 2147483647.
  - **interface** { **br-ethernet** *slot/chassis_num* | **ethernet** *slot/chassis_num* } : affiche les informations LACP pour l'interface Ethernet spécifiée.
  - **log** : affiche les journaux d'informations LACP.
  - **pc-db interface port-channel** *number* : affiche l'état de la base de données de canaux de ports virtuels (2lvpc) pour le canal de port spécifié.
  - **pss** : affiche les informations globales du service

de stockage persistant (PSS).

- **mem-stats** : affiche les statistiques d'allocation de la mémoire LACP.

issu-impact	L'option de mise à niveau logicielle pendant que l'appareil fonctionne (ISSU) ne s'applique pas à FXOS.
neighbor [**interface port-channel** *number*]	Affiche des informations sur les voisins LACP. (Facultatif) Vous pouvez spécifier un canal de port particulier pour afficher les informations sur ce canal de port uniquement; les numéros de canal de port valides sont compris entre 1 et 4096.
port-channel [**interface port-channel** *number*]	Affiche des informations sur tous les canaux de ports. (Facultatif) Vous pouvez spécifier un canal de port particulier pour afficher les informations sur ce canal de port uniquement; les numéros de canal de port valides sont compris entre 1 et 4096.
system-identifier	Affiche l'identification du système LACP. Il s'agit d'une combinaison de la priorité de port et de l'adresse MAC de l'appareil.

Modes de commande

connect fxos/

Historique des commandes

Version	Modification
1.1.1	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour résoudre les problèmes liés à LACP dans un réseau.

Remarque Lorsque vous vous connectez au shell de commande FXOS, l'invite de ligne de commande passe de votre invite par défaut, qui correspond au nom que vous avez attribué à l'appareil, à l'invite par défaut à laquelle est ajouté (fxos); consultez l'exemple suivant.

Exemples

Cet exemple montre comment afficher les compteurs LACP :

```
firepower# connect fxos
firepower(fxos)# show lacp counters                    LACPDUs         Marker      Marker
Response    LACPDUs
Port              Sent   Recv     Sent   Recv     Sent   Recv      Pkts Err
--------------------------------------------------------------------------
port-channel1
Ethernet1/3        20552782218005  0      0        0      0         0
```

```
port-channel2
Ethernet1/6        671621 724750   0      0        0      0        0

port-channel48
Ethernet1/1        23974772587653  0      0        0      0        0

firepower(fxos)#
```

Cet exemple montre comment afficher les informations LACP pour un canal de port particulier :

```
firepower# connect fxos
firepower(fxos)# show lacp port-channel interface port-channel 48
port-channel48
  System Mac=b0-aa-77-2f-f0-af
  Local System Identifier=0x8000,b0-aa-77-2f-f0-af
  Admin key=0x2f
  Operational key=0x2f
  Partner System Identifier=0x8000,78-ba-f9-e2-60-c0
  Operational key=0x30
  Max delay=0
  Aggregate or individual=1
  Member Port List=
firepower(fxos)#
```

Commandes associées

Commande	Description
clear lacp counters	Efface les compteurs LACP.

show license

Pour afficher l'utilisation de tout ou partie des ensembles de licences, utilisez la commande **show license**.

show license { **all** | **resvcode** | **status** | **summary** | **techsupport** | **udi** | **usage** }

Description de la syntaxe

all	Affiche l'état des licences Smart et des informations sur l'utilisation de toutes les licences.
resvcode	Affiche des informations sur le code de réservation généré.
status	Affiche des informations sur l'état des licences Smart.
summary	Affiche des informations récapitulatives sur les licences Smart.
techsupport	Affiche un ensemble complet d'informations sur les licences Smart à des fins de transmission au centre d'assistance technique (TAC) de Cisco.
udi	Affiche l'identifiant universel d'appareil (UDI) FXOS.
usage	Affiche l'utilisation actuelle des licences.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous devez acheter des licences permanentes pour qu'elles soient disponibles dans Smart Software Manager. Tous les comptes ne sont pas approuvés pour la réservation de licence permanente.

Exemple

Cet exemple montre comment afficher l'état actuel et l'utilisation de tous les ensembles de licences :

```
FP9300-A# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Cisco SVS temp
  Virtual Account: Escalations
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Feb 10 18:55:08 2016 CST
  Last Renewal Attempt: SUCCEEDED on Jun 27 06:11:11 2017 CDT
  Next Renewal Attempt: Jul 28 03:02:49 2017 CDT
  Registration Expires: Jun 27 06:05:09 2018 CDT

License Authorization:
```

```
  Status: AUTHORIZED on Jul 05 18:19:38 2017 CDT
  Last Communication Attempt: SUCCESS on Jul 05 18:19:38 2017
CDT
  Next Communication Attempt: Aug 08 14:50:41 2017 CDT

    <--- remaining lines removed for brevity --->

FP9300-A#
```

Commandes associées

Commande	Description
scope license	Permet d'accéder au mode licence.

show load-stats

Pour afficher la liste des fonctionnalités de statistiques de charge disponibles sur le système, utilisez la commande **show load-stats** .

show load-stats detail

Description de la syntaxe

detail	Répertorie les informations sur les fonctionnalités des statistiques de charge.

Modes de commande

scope system, scope capability

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope system, scope capability.

Exemple

Cet exemple montre comment afficher les fonctionnalités des statistiques de charge :

```
Firepower # scope system
Firepower /system # scope capability
Firepower /system/capability # show load-stats

Capability:
    Load Errors: 0
    Load Warnings: 4
    Providers Loaded: 128
    Provider Load Failures: 0
    Files Parsed: 17
    File Parse Failures: 0

Firepower /system/capability # show load-stats detail
Capability:
    Load Errors: 0
    Load Warnings: 4
    Providers Loaded: 126
    Provider Load Failures: 0
    Files Parsed: 17
    File Parse Failures: 0
```

show local-user

Pour afficher des informations sur un utilisateur spécifique ou tous les utilisateurs locaux, utilisez la commande **show local-user**.

show local-user [**detail** | *user_name*]

Description de la syntaxe

detail	(Facultatif) Affiche des informations détaillées sur l'utilisateur local.
user_name	(Facultatif) Affiche des informations sur l'utilisateur local spécifié.

Modes de commande

Mode sécurité

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

En mode sécurité, les informations sur tous les utilisateurs locaux sont répertoriées par défaut, sauf si vous saisissez un *nom d'utilisateur* spécifique.

En mode utilisateur local, utilisez la commande **show** pour afficher des informations sur l'utilisateur connecté.

Exemple

Cet exemple montre comment afficher des informations détaillées sur un utilisateur local spécifique :

```
FP9300-A /security # show local-user test_user detail
Local User test_user:
    First Name: test
    Last Name: user
    Email: test_user@testuser.com
    Phone:
    Expiration: Never
    Password: ****
    User lock status: Not Locked
    Account status: Active
    User Roles:
        Name: admin
        Name: read-only
    User SSH public key:
FP9300-A /security #
```

Commandes associées

Commande	Description
create local-user	Crée un compte d'utilisateur local.
delete local-user	Supprime un compte d'utilisateur local existant.
enter local-user	Permet d'accéder à un compte d'utilisateur local existant.

show local-user tech-support

Pour afficher l'utilisateur local administrateur, utilisez la commande **show local-user tech-support**.

show local-user tech-support detail

Description de la syntaxe

detail	Informations détaillées sur l'assistance technique locale.

Modes de commande

scope security

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope security.

Exemple

Cet exemple montre comment afficher les informations sur l'utilisateur local administrateur :

```
Firepower # scope security
Firepower /security # show local-user-tech support

Local User admin:
    Expiration: Never
    Password: ****
    User lock status: Not Locked
    Account status: Active
    User Roles:
        Name: admin
        Name: read-only
    User SSH public key:
```

show logical-device

Pour afficher des informations sur les périphériques logiques disponibles sur le système, utilisez la commande **show logical-device**.

show logical-device [**expand**] [**detail**] [**fsm**]

Description de la syntaxe

detail	Affiche des informations détaillées sur les fonctionnalités du réseau.
expand	(Facultatif) Affiche les informations développées pour l'instance d'application actuelle. Ce mot clé est également disponible avec de nombreuses autres options de commande pour afficher les informations développées sur l'option spécifiée.
fsm	Affiche les informations sur l'état du FSM.

Modes de commande

Scope ssa

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope ssa :

Exemple

Cet exemple affiche des informations sur tous les périphériques logiques disponibles :

```
firepower # scope ssa
firepower /ssa # show logical-device

Logical Device:
    Name       Description Slot ID    Mode       Oper State                Template Name
    ---------- ----------- ---------- ---------- ------------------------- -------------
    ftd                    1          Standalone Incomplete Configuration ftd
```

Cet exemple affiche des informations détaillées sur les périphériques logiques :

```
firepower /ssa # show logical-device detail
Logical Device:
    Name: ftd
    Description:
    Slot ID: 1
    Mode: Standalone
    Oper State: Incomplete Configuration
    Template Name: ftd
    Error Msg: Missing bootstrap keys MANAGEMENT_TYPE in ftd mgmt bootstrap
    Switch Configuration Status: Ok
    Current Task:
```

Cet exemple montre les informations développées sur les périphériques logiques :

```
firepower /ssa # show logical-device expand detail

Logical Device:
    Name: ftd
    Description:
    Slot ID: 1
    Mode: Standalone
    Oper State: Incomplete Configuration
    Template Name: ftd
    Error Msg: Missing bootstrap keys MANAGEMENT_TYPE in ftd mgmt bootstrap
    Switch Configuration Status: Ok
    Current Task:

    External-Port Link:
        Name: Ethernet11_ftd
        Port or Port Channel Name: Ethernet1/1
        Port Type: Mgmt
        App Name: ftd
        Description:
        Link Decorator:

         Name: Ethernet21_asa
        Port or Port Channel Name: Ethernet2/1
        Port Type: Data
        App Name: asa
        Description:
        Link Decorator:

        System MAC address:
            Mac Address: F8:0F:6F:A1:93:BB

    Management Configuration:
        App Name: asa

        IP v4:
            Slot ID: 2
            Management Sub Type: Default
            IP Address: 10.62.148.241
            Netmask: 255.255.255.128
            Gateway: 10.62.148.129
            Last Updated Timestamp: 2021-12-01T22:42:22.722
```

show logical-device-template

Pour afficher le modèle de périphériques logiques comme ASA et Cisco FTD disponibles sur le système, utilisez la commande **show logical-device-template**.

show logical-device-template [**detail** | *expand* | *name*]

Description de la syntaxe

detail	Affiche la liste des informations détaillées sur le modèle de périphérique logique.
name	Affiche les informations sur le modèle de périphérique logique d'un périphérique logique spécifique. Les mots clés expand et expand sont disponibles avec cette option.
expand	(Facultatif) Affiche les informations développées sur le modèle de périphérique logique.

Modes de commande

scope ssa

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope ssa.

Exemple

Cet exemple montre comment afficher les informations sur le modèle de tous les périphériques logiques :

```
Firepower /fabric-interconnect # scope ssa
Firepower /ssa # show logical-device-template

Logical Device Template:
    Name       Version    Description
    ---------- ---------- -----------
    asa        1
    ftd        1
Firepower /ssa # show logical
```

Exemple

Cet exemple montre comment afficher les informations détaillées sur le modèle de tous les périphériques logiques disponibles sur le système :

```
Firepower /ssa # show logical-device-template detail
 Logical Device Template:
    Name: asa
    Version: 1
    Description:
    Name: ftd
```

```
    Version: 1
    Description:
```

Exemple

Cet exemple montre comment afficher les informations détaillées du modèle pour tous les périphériques logiques disponibles dans le système :

```
Firepower /ssa # show logical-device-template expand detail
   QP1 /ssa # show logical-device-template expand detail
Logical Device Template:
    Name: asa
    Version: 1
    Description:
    Template Applications:
        App Name: asa
        Application can be a decorator: No
    Name: ftd
    Version: 1
    Description:
    Template Applications:
        App Name: ftd
        Application can be a decorator: No
```

show mac-address

Pour afficher les affectations d'adresses MAC pour les interfaces d'instance de contenant, utilisez la commande **show mac-address**.

show mac-address [**detail** | *mac_address*]

Description de la syntaxe

detail	Affiche les adresses MAC dans un format non tabulaire.
mac_address	Affiche les informations sur une adresse MAC spécifique.

Modes de commande

scope ssa/scope auto-macpool/

Historique des commandes

Version	Modification
2.4(1)	Commande ajoutée.

Instructions d'utilisation

Cette commande s'applique uniquement aux interfaces d'instance de contenant et n'affiche pas les adresses MAC pour les instances natives.

Exemple

Voici un exemple de sortie de la commande **show mac-address**.

```
firepower# scope ssa
firepower /ssa # scope auto-macpool
firepower /ssa/auto-macpool # show mac-address
Mac Address Item:
    Mac Address          Owner Profile            Owner Name
    -------------------- ------------------------ ----------
    A2:46:C4:00:00:1E    ftd13                    Port-channel14
    A2:46:C4:00:00:20    ftd14                    Port-channel15
    A2:46:C4:00:01:7B    ftd1                     Ethernet1/3
    A2:46:C4:00:01:7C    ftd12                    Port-channel11
    A2:46:C4:00:01:7D    ftd13                    Port-channel14
    A2:46:C4:00:01:7E    ftd14                    Port-channel15
    A2:46:C4:00:01:7F    ftd1                     Ethernet1/2
    A2:46:C4:00:01:80    ftd12                    Ethernet1/2
    A2:46:C4:00:01:81    ftd13                    Ethernet1/2
    A2:46:C4:00:01:82    ftd14                    Ethernet1/2
    A2:46:C4:00:01:83    ftd2                     Ethernet3/1/4
    A2:46:C4:00:01:84    ftd2                     Ethernet3/1/1
    A2:46:C4:00:01:85    ftd2                     Ethernet3/1/3
    A2:46:C4:00:01:86    ftd2                     Ethernet3/1/2
    A2:46:C4:00:01:87    ftd2                     Ethernet1/2
    A2:46:C4:00:01:88    ftd1                     Port-channel21
    A2:46:C4:00:01:89    ftd1                     Ethernet1/8
```

Voici un exemple de sortie de la commande **show mac-address detail**.

```
firepower# scope ssa
firepower /ssa # scope auto-macpool
```

```
firepower /ssa/auto-macpool #  show mac-address detail

Mac Address Item:
    Mac Address: A2:F0:B0:00:00:16
    Owner Profile: ftd1
    Owner Name: Ethernet1/5

    Mac Address: A2:F0:B0:00:00:17
    Owner Profile: ftd1
    Owner Name: Port-channel1

    Mac Address: A2:F0:B0:00:00:18
    Owner Profile: ftd1
    Owner Name: Ethernet1/4

    Mac Address: A2:F0:B0:00:00:19
    Owner Profile: ftd1
    Owner Name: Ethernet1/4
```

Commandes associées

Commande	Description
create port-channel	Crée un EtherChannel (canal de port).
create subinterface	Ajoute une sous-interface.
scope interface	Permet d'accéder à l'objet d'interface physique.
set port-type	Définit le type d'interface.

show mgmt-iface in-band expand detail

Pour afficher les détails de l'interface de gestion externe dans la bande, utilisez la commande **show mgmt-iface in-band expand detail**.

```
show mgmt-iface in-band expand detail
```

Description de la syntaxe

Show mgmt-iface in-band expand detail	Affiche les détails de l'interface de gestion externe dans la bande

Modes de commande

scope fabric-interconnect a, scope server 1/1, scope cimc

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

La commande show se trouve dans scope fabric-interconnect et sub scope cimc

Exemple

Cet exemple montre les détails de l'interface de gestion externe dans la bande

```
Firepower# scope fabric-interconnect a
Firepower /fabric-interconnect # scope server 1/1
Firepower /chassis/server # scope cimc
Firepower /chassis/server/cimc # enter mgmt-iface in-band
Firepower /chassis/server/cimc/mgmt-iface* #
Firepower /chassis/server/cimc/mgmt-iface* # commit-buffer
Firepower /chassis/server/cimc/mgmt-iface # exit
Firepower /chassis/server/cimc # show mgmt-iface in-band expand detail

External Management Interface:
    Mode: In Band
    Ip V4 State: None
    Ip V6 State: None
    Is Derived from Inband Profile: No
Firepower /chassis/server/cimc #
```

show member-port

Pour afficher les informations sur l'état des ports membres du canal de port, utilisez la commande **show member-port**.

show member-port [*slot_id port_id* | **detail** | **Ethernet***slot_id*/*port_id* | **expand** | **fsm status**]

Description de la syntaxe

slot_id port_id	(Facultatif) Vous pouvez afficher les informations sur l'état d'un seul port membre en spécifiant son logement et son numéro. Les mots clés **detail** et **expand** sont disponibles avec cette option.
detail	(Facultatif) Utilisez ce mot clé pour afficher les informations détaillées sur tous les ports membres. Le mot clé **expand** est disponible avec cette option.
Ethernet*slot_id*/*port_id*	(Facultatif) Vous pouvez afficher les informations sur l'état d'un seul port membre en spécifiant son étiquette de port Ethernet. Le mot clé **detail** est disponible avec cette option.
expand	(Facultatif) Utilisez ce mot clé pour afficher la liste développée des informations sur tous les ports membres. Le mot clé **detail** est disponible avec cette option.
fsm status	(Facultatif) Utilisez ce mot clé pour afficher les informations sur l'état de la machine à états finis (FSM) pour les ports membres. Vous pouvez ajouter un logement et un numéro de port (*slot_id port_id*) pour limiter l'affichage des informations au port membre spécifié. Le mot clé **expand** est disponible avec cette option.

Modes de commande

scope eth-uplink/scope fabric a/port-channel

Historique des commandes

Version	Modification
1.1.1	Commande ajoutée.

Instructions d'utilisation

Vous devez créer ou saisir un canal de port avant de pouvoir utiliser cette commande.

Il s'agit d'une sous-commande de la commande **show** en mode scope eth-uplink/scope fabric/port-channel.

Exemple

Cet exemple affiche les informations développées sur le port membre d'un un canal de port spécifique :

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # enter port-channel 3
firepower /eth-uplink/fabric/port-channel # show member-port expand

Member Port:
    Port Name       Membership         Oper State       State Reason
    --------------- ------------------ ---------------- ------------
    Ethernet1/1     Up                 Up
    Ethernet2/3     Suspended          Failed           Suspended
```

```
    Ethernet2/4     Down               Sfp Not Present  Unknown
firepower /eth-uplink/fabric/port-channel #
```

Commandes associées

Commande	Description
create member-port	Crée un port membre de canal de port.
create port-channel	Crée un canal de port.

show mac-pool

Pour afficher la liste des ensembles d'adresses MAC disponibles sur le système, utilisez la commande **show mac-pool**.

show mac-pool [**detail** | **expand** | **name**]

Description de la syntaxe

detail	Répertorie les informations détaillées sur les ensembles d'adresses MAC.
expand	(Facultatif) Affiche les informations sur les ensembles d'adresses MAC pour un ensemble spécifique. Les mots clés **expand** et **expand** sont disponibles avec cette option.
name	(Facultatif) Affiche les informations développées sur l'ensemble d'adresses MAC. Le mot clé **detail** est disponible avec cette option.

Modes de commande

scope org

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope org.

Exemple

Cet exemple montre comment afficher les informations sur l'ensemble d'adresses MAC disponibles :

```
Firepower /fabric-interconnect # scope org
Firepower /org # show mac-pool

MAC Pool:
    Name                  Size       Assigned
    -------------------- ---------- --------
    default                          0          0
    ssp-macpool-ccl                200          0
    ssp-macpool-inter-vnics
                                   300         81
    ssp-macpool-mio-external-ports

                                  76          3
```

Exemple

Cet exemple montre comment afficher des informations détaillées sur la commande mac pool expand detail :

```
Firepower /org # show mac-pool expand detail

MAC Pool:
    Name: default
```

```
Size: 0
Assigned: 0
Descr:
Assignment Order: Default

Name: ssp-macpool-ccl
Size: 200
Assigned: 0
Descr: SSP service profile MAC Pool for ccl
Assignment Order: Default

Block of MAC Addresses:
    From: 00:15:C5:00:00:00
    To: 00:15:C5:00:00:C7

Pooled:
    Id: 00:15:C5:00:00:00
    Assigned: No
Assigned To Dn:
    Poolable Dn: mac/00:15:C5:00:00:00/pool-31022
    Prev Assigned To Dn:

    Id: 00:15:C5:00:00:01
    Assigned: No
    Assigned To Dn:
    Poolable Dn: mac/00:15:C5:00:00:01/pool-31025
    Prev Assigned To Dn:

    Id: 00:15:C5:00:00:02
    Assigned: No
    Assigned To Dn:
    Poolable Dn: mac/00:15:C5:00:00:02/pool-31028
    Prev Assigned To Dn:
```

show memory

Pour afficher les informations d'un module de mémoire, utilisez la commande **show memory**.

show memory [*details*]

Description de la syntaxe

detail	Vous pouvez afficher les informations détaillées sur la version.

Modes de commande

scope chassis/scope server

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope server 1 sous scope chassis 1.

Exemple

Cet exemple montre comment afficher les informations sur le module de mémoire disponibles sur un serveur spécifique :

```
firepower# scope chassis 1
firepower /chassis # scope server 1
firepower /chassis/server # show memory
DIMM Location   Presence         Overall Status           Type         Capacity (MB) Clock
---- ---------- ---------------- ------------------------ ------------ ------------- -----
   1 DIMM_A1    Equipped         Operable                  DDR4         16384         2666
   2 DIMM_A2    Missing          Removed                  Undisc       Unknown       Unknown

   3 DIMM_B1    Equipped         Operable                  DDR4         16384         2666
   4 DIMM_B2    Missing          Removed                  Undisc       Unknown       Unknown

   5 DIMM_C1    Equipped         Operable                  DDR4         16384         2666
   6 DIMM_C2    Missing          Removed                  Undisc       Unknown       Unknown

   7 DIMM_D1    Equipped         Operable                  DDR4         16384         2666
   8 DIMM_D2    Missing          Removed                  Undisc       Unknown       Unknown

   9 DIMM_E1    Equipped         Operable                  DDR4         16384         2666
  10 DIMM_E2    Missing          Removed                  Undisc       Unknown       Unknown

  11 DIMM_F1    Equipped         Operable                  DDR4         16384         2666
  12 DIMM_F2    Missing          Removed                  Undisc       Unknown       Unknown

  13 DIMM_G1    Equipped         Operable                  DDR4         16384         2666
  14 DIMM_G2    Missing          Removed                  Undisc       Unknown       Unknown

  15 DIMM_H1    Equipped         Operable                  DDR4         16384         2666
  16 DIMM_H2    Missing          Removed                  Undisc       Unknown       Unknown

  17 DIMM_J1    Equipped         Operable                  DDR4         16384         2666
  18 DIMM_J2    Missing          Removed                  Undisc       Unknown       Unknown

  19 DIMM_K1    Equipped         Operable                  DDR4         16384         2666
  20 DIMM_K2    Missing          Removed                  Undisc       Unknown       Unknown
```

```
  21 DIMM_L1    Equipped         Operable                DDR4         16384         2666
  22 DIMM_L2    Missing          Removed                 Undisc       Unknown       Unknown

  23 DIMM_M1    Equipped         Operable                DDR4         16384         2666
  24 DIMM_M2    Missing          Removed                 Undisc       Unknown       Unknown
firepower /chassis/server #
```

Exemple

Cet exemple montre comment afficher les informations détaillées de tous les modules de mémoire disponibles sur un serveur spécifique :

```
firepower# scope chassis 1
KSEC-FPR4115-3 /chassis # scope server 1
KSEC-FPR4115-3 /chassis/server # show memory detail
ID 1:
    Location: DIMM_A1
Presence: Equipped
    Overall Status: Operable
    Visibility: Yes
    Vendor: 0x2C00
    Vendor Part Number: 18ASF2G72PDZ-2G6E1
    Vendor Serial (SN): 43585030
    HW Revision: 0
    Form Factor: DIMM
    Type: DDR4
    Capacity (MB): 16384
    Clock: 2666
    Latency: 0.400000
    Width: 64
ID 2:
    Location: DIMM_A2
    Presence: Missing
    Overall Status: Removed
    Visibility: No
    Vendor:
    Vendor Part Number:
    Vendor Serial (SN):
    HW Revision: 0
    Form Factor: Undisc
    Type: Undisc
    Capacity (MB): Unknown
    Clock: Unknown
    Latency: Unknown
    Width: Unknown
ID 3:
    Location: DIMM_B1
    Presence: Equipped
    Overall Status: Operable
    Visibility: Yes
    Vendor: 0x2C00
    Vendor Part Number: 18ASF2G72PDZ-2G6E1
    Vendor Serial (SN): 4358534D
    HW Revision: 0
    Form Factor: DIMM
    Type: DDR4
    Capacity (MB): 16384
    Clock: 2666
    Latency: 0.400000
    Width: 64
          ..................................
```

```
                .....
                .....
firepower /chassis/server #
```

show (management interface)

Pour afficher des informations sur l'interface de gestion actuelle, utilisez la commande **show** en mode interconnexion de structure.

show

Description de la syntaxe

En mode interconnexion de structure, cette commande comporte un certain nombre de mots clés, mais la saisie de **show** sans modificateurs affiche des informations sur l'interface de gestion de structures actuelle.

Modes de commande

scope fabric-interconnect/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande affiche des informations sur l'interface de gestion IPv4 et IPv6. L'ajout du mot clé **detail** affiche ces informations d'interface, ainsi que d'autres informations propres à la structure.

Exemple

Cet exemple montre comment afficher des informations sur l'interface de gestion :

```
firepower# scope fabric-interconnect
firepower /fabric-interconnect # show

Fabric Interconnect:
ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
Prefix Operability
---- --------------- --------------- --------------- ---------------- ----------------
------ -----------
A    192.0.2.112     192.0.2.1       255.255.255.0   ::               ::               64
    Operable
firepower /fabric-interconnect #
```

Commandes associées

Commande	Description
scope fabric-interconnect	Permet d'accéder au mode interconnexion de structure.
show ipv6-if	Affiche l'adresse IPv6 actuelle de gestion des appareils.

show mgmt-port

Pour afficher les informations d'état du port de gestion des appareils, utilisez la commande **show mgmt-port**.

```
(local-mgmt)# show mgmt-port
```

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

connect local-mgmt

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour afficher les informations sur la configuration et l'état de l'interface de gestion des appareils.

Exemple

Cet exemple montre comment afficher les informations sur le port de gestion :

```
firepower # connect local-mgmt
firepower(local-mgmt)# show mgmt-port
eth0      Link encap:Ethernet  HWaddr b0:aa:77:2f:f0:a9
          inet addr:10.89.5.14  Bcast:10.89.5.63  Mask:255.255.255.192
          inet6 addr: fe80::b2aa:77ff:fe2f:f0a9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:174151 errors:0 dropped:0 overruns:0 frame:0
          TX packets:101268 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15273492 (14.5 MiB)  TX bytes:80246582 (76.5 MiB)

firepower(local-mgmt)#
```

Commandes associées

Commande	Description
show open-network-ports	Affiche tous les ports réseau ouverts.

show monitor

Pour afficher les informations et les ressources par module de sécurité, utilisez la commande **show monitor**.

show monitor [**detail** | **expand**]

Description de la syntaxe

detail	Affiche l'utilisation détaillée des ressources pour le module.
expand	Affiche les informations détaillées sur le système de fichiers du disque.

Modes de commande

scope ssa/scope slot/

Historique des commandes

Version	Modification
2.4(1)	Des champs supplémentaires ont été ajoutés pour afficher les cœurs de CPU, la mémoire et l'utilisation du disque.
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous pouvez afficher des informations sur le module de sécurité, notamment la version du système d'exploitation, la mémoire et le temps de disponibilité. Cette commande est utile pour les instances de conteneur afin de suivre la disponibilité des ressources.

Exemple

Voici un exemple de sortie de la commande **show monitor**.

```
firepower# scope ssa
firepower /ssa # scope slot 1
firepower /ssa/slot # show monitor

Monitor:
    OS Version Memory Total (MB) Memory Free (MB) Memory Used (MB) CPU Cores Available Blade
 Uptime Last Updated Timestamp
    ---------- ----------------- ---------------- ---------------- -------------------
------------ ----------------------
    2.4(1.101)             251844           222089            29755                  22 up
 19 days,  2:06

          2018-11-27T18:11:34.155
```

Voici un exemple de sortie de la commande **show monitor detail**.

```
firepower# scope ssa
firepower /ssa # scope slot 1
firepower /ssa/slot # show monitor detail

Monitor:
    OS Version: 2.4(1.101)
    CPU Total Load 1 min Avg: 4.790000
    CPU Total Load 5 min Avg: 4.790000
    CPU Total Load 15 min Avg: 4.780000
```

```
    Memory Total (MB): 251844
    Memory Free (MB): 222084
    Memory Used (MB): 29760
    CPU Cores Total: 48
    CPU Cores Available: 22
    Memory App Total (MB): 226886
    Memory App Available (MB): 108514
    Data Disk Total (MB): 699651
    Data Disk Available (MB): 535811
    Secondary Disk Total (MB): 0
    Secondary Disk Available (MB): 0
    Disk File System Count: 5
    Blade Uptime: up 19 days,  1:55
    Last Updated Timestamp: 2018-11-27T18:00:04.560
```

Voici un exemple de sortie de la commande **show monitor expand**.

```
firepower# scope ssa
firepower /ssa # scope slot 1
firepower /ssa/slot # show monitor expand
Monitor:
    OS Version: 2.4(1.101)
    Memory Total (MB): 251844
    Memory Free (MB): 222089
    Memory Used (MB): 29755
    CPU Cores Available: 22
    Blade Uptime: up 19 days,  2:06
    Last Updated Timestamp: 2018-11-27T18:11:34.155

    Disk File System:
        File System Mount Point Disk Total (MB) Disk Free (MB) Disk Used (MB)
        ----------- ----------- --------------- -------------- --------------
        /dev/sda1   /mnt/boot              7614           7451            163
        /dev/sda2   /opt/cisco/config
                                           1846           1707             43
        /dev/sda3   /opt/cisco/platform/logs
                                           4565           4278             49
        /dev/sda5   /var/data/cores
                                          46807          44368             54
        /dev/sda6   /opt/cisco/csp
                                         699651         653295          46356
```

Commandes associées

Commande	Description
show resource	Affiche l'utilisation des ressources.

show nfs-mount-def

Pour afficher les informations sur mount def disponibles sur le système, utilisez la commande **show nfs-mount-def**.

show [**detail**]

Description de la syntaxe

detail	Répertorie les informations détaillées sur mount def.

Modes de commande

Scope monitoring

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope monitoring :

Exemple

Cet exemple montre les informations pour toutes les commandes mount def disponibles :

```
firepower # scope monitoring
firepower /monitoring # show nfs-mount-def
Mount Def:
    Name: external Backup Repository
    Admin State: Disabled
    Local dir: /boot flash/externalcfg
    policy owner: Local
    Purpose: Backup
    Remote dir:
    server:

    Name: external Image Repository
    Admin State: Disabled
    Local dir: /boot flash/external
    policy owner: Local
    Purpose: Image
    Remote dir:
    server:
```

Cet exemple montre les informations détaillées sur mount def :

```
firepower /monitoring # show nfs-mount-def detail
Mount Def:
    Admin State: Disabled
    Name: external Backup Repository
    Local dir: /boot flash/externalcfg
    policy owner: Local
    Purpose: Backup
    Remote dir:
    server:
    Current Task:

    Admin State: Disabled
    Name: external Image Repository
    Local dir: /boot flash/externalrep
```

```
    policy owner: Local
    Purpose: Image
    Remote dir:
    server:
    Current Task:
```

Cet exemple montre les informations détaillées de l'état mount def :

```
firepower /monitoring # show nfs-mount-def fsm status

    FSM 1:
        Remote Result: Not Applicable
        Remote Error Code: None
        Remote Error Description:
        Status: Nop
        Previous Status: Nop
        Timestamp: Never
        Try: 0
        Progress (%): 100
        Current Task:


    FSM 1:
        Remote Result: Not Applicable
        Remote Error Code: None
        Remote Error Description:
        Status: Nop
        Previous Status: Nop
        Timestamp: Never
        Try: 0
        Progress (%): 100
        Current Task:
```

show nm-fpga-version

Pour afficher une version FPGA de l'adaptateur réseau, utilisez la commande **show nm-fpga-version**.

show nm-fpga-version [**detail**]

Description de la syntaxe

detail	Informations détaillées sur la version.

Modes de commande

scope chassis 1

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Sous-commande de la commande **show** dans scope chassis 1.

Exemple

Cet exemple montre les informations sur la version FPGA du module de réseau :

```
firepower/fabric-interconnect # scope chassis 1
firepower /chassis # show nm-fpga-version

Network Module Version:
    Network Module Slot: 2
    Running-Vers: 0.6.0
    Package-Vers: 0.0
    Activate-Status: Ready
firepower/chassis #
```

show ntp-overall-status

Pour afficher l'état général de synchronisation du protocole Network Time Protocol pour le système, utilisez la commande **show ntp-overall-status**.

show ntp-overall-status

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment afficher l'état actuel de la synchronisation de l'horloge pour le châssis et tous les périphériques logiques installés sur celui-ci :

```
FP9300-A# show ntp-overall-status

    NTP Overall Time-Sync Status: Time Synchronized
FP9300-A#
```

Commandes associées

Commande	Description
show clock	Affiche l'horloge système.

show ntp server

Pour afficher le serveur NTP, utilisez la commande **show ntp-server** .

show ntp-server

Description de la syntaxe

show ntp-server	Cette commande affiche le serveur NTP dans FXOS.

Modes de commande

scope system/scope services/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande affiche le serveur NTP.

Exemple

Cet exemple montre comment afficher le serveur NTP :

```
firepower# scope system;scope services

firepower /system/services # show ntp-server

NTP server hostname:
    Name                                                                Time Sync Status
    ------------------------------------------------------------------- ----------------
    192.0.2.1                                                           Time Synchronized

firepower /system/services # show ntp-server expand detail

NTP server hostname:
    Name: 192.0.2.1
    Time Sync Status: Time Synchronized
    NTP SHA-1 key id: 0
    Error Msg:
```

show nw-ctrl-policy

Pour afficher les détails de la politique de transmission LLDP, de réception LLDP, d'action en cas de défaillance de la liaison ascendante et d'enregistrement des adresses MAC des adaptateurs, utilisez la commande **show nw-ctrl-policy** .

show nw-ctrl-policy [*detail* | *expand*]

Description de la syntaxe

Detail	Affiche les informations détaillées sur la politique de réseau.
Diversification	Affiche les informations développées sur l'instance d'application actuelle. Ce mot clé est également disponible avec de nombreuses autres options de commande pour afficher les informations développées sur l'option spécifiée.

Modes de commande

scope org

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope org.

Exemple

Cet exemple montre comment afficher les informations de la politique réseau dans le système :

```
Firepower# scope org
Firepower /org # show nw-ctrl-policy
Network Control Policy:
    Name       CDP      LLDP Transmit LLDP Receive Uplink fail action Adapter MA
C Address Registration
    ---------- -------- ------------- ------------ ------------------ ----------
----------------------
    default    Disabled Disabled      Disabled     Link Down          Only Nativ
e Vlan
```

Cet exemple montre comment afficher les informations de la politique réseau en détail dans le système :

```
Firepower /org # show nw-ctrl-policy detail
Network Control Policy:
    Name: default
    CDP: Disabled
    LLDP Transmit: Disabled
    LLDP Receive: Disabled
    Uplink fail action: Link Down
    Adapter MAC Address Registration: Only Native Vlan
    Policy Owner: Local
    Description:
```

Cet exemple montre des informations développées sur la politique réseau dans le système :

```
Firepower /org # show nw-ctrl-policy detail expand
Network Control Policy:
    Name: default
```

```
CDP: Disabled
LLDP Transmit: Disabled
LLDP Receive: Disabled
Uplink fail action: Link Down
Adapter MAC Address Registration: Only Native Vlan
Policy Owner: Local
Description:
```

show org

Pour afficher les informations sur l'organisation actuelle, utilisez la commande **show org**.

show org [**detail** | *name*]

Description de la syntaxe

detail	(Facultatif) Affiche les détails de toutes les organisations actuellement définies.
nom	(Facultatif) Affiche les informations sur l'organisation spécifiée; maximum de 16 caractères pour cet identifiant.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment afficher les informations sur l'organisation actuelle :

```
FP9300-A# show org

Organizations:
    Name: / (root)
FP9300-A#
```

Commandes associées

Commande	Description
scope org	Permet d'accéder au mode organisation (/org).

show package

Pour afficher les informations sur le paquet téléchargé, utilisez la commande **show package**.

show package [**detail** | **expand** | **type** *endpoint_type* | *name*]

Description de la syntaxe

detail	(Facultatif) Affiche les informations détaillées sur le package, y compris le numéro de version et les horodatages.
expand	(Facultatif) Répertorie les images regroupées dans chaque package. Le mot clé **detail** est également disponible.
type *endpoint_type*	(Facultatif) Affiche les informations sur le type de terminal du package spécifié : • **b-series-bundle** : répertorie les informations sur les offres groupées de la série B disponibles. • **c-series-bundle** : répertorie les informations sur les offres groupées de la série C disponibles. • **catalog** : répertorie les informations du catalogue d'images FXOS, qui est une liste d'images et de packages. • **firmware-fpr4k-bundle** : répertorie les informations sur les offres groupées de micrologiciels de la série FP4100 disponibles. • **firmware-fpr9k-bundle** : répertorie les informations sur les offres groupées de micrologiciels de la série FP9300 disponibles. • **image** : répertorie les images de micrologiciel disponibles. • **full-bundle** : répertorie les informations sur les offres groupées complètes téléchargées. • **infrastructure-bundle** : répertorie les informations sur les offres groupées d'infrastructure téléchargées. • **platform-bundle** : répertorie les informations sur les offres groupées de plateforme téléchargées. • **unknown** : répertorie les informations sur les offres groupées de type inconnu téléchargées. Les mots clés **detail** et **expand** sont disponibles avec cette option.
name	(Facultatif) Affiche les informations sur le package spécifié. Les mots clés **detail**, **expand** et **type** sont également disponibles avec cette option.

Modes de commande

Mode micrologiciel

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Si vous n'incluez pas de *nom*, la commande **show package** répertorie les informations pour chaque package de micrologiciel sur l'appareil.

Exemple

Cet exemple montre comment répertorier des informations détaillées et développées sur un package de micrologiciel spécifique :

```
FP9300-A# scope firmware
FP9300-A /firmware # show package fxos-k9.2.3.1.51.SPA detail
Firmware Package fxos-k9.2.3.1.51.SPA:
    Version: 2.3(1.51)
    Type: Platform Bundle
    State: Active
Time Stamp: 2017-10-25T16:53:30.000
Build Date: 2017-10-21 09:10:36 UTC
FP9300-A /firmware # show package fxos-k9.2.3.1.51.SPA expand
Package fxos-k9.2.3.1.51.SPA:
    Images:
        fxos-k9-bundle-infra.2.3.1.51.SPA
        fxos-k9-bundle-server.2.3.1.51.SPA
FP9300-A /firmware #
```

Commandes associées

Commande	Description
show server firmware	Affiche les versions du micrologiciel et les informations d'état actuelles du serveur.
verify platform-pack	Vérifie une image de plateforme FXOS spécifiée.

show password-profile

Pour afficher les informations sur le profil de mot de passe, utilisez la commande **show password-profile**.

show password-profile [**detail**]

Description de la syntaxe

detail	(Facultatif) Affiche les informations détaillées sur le profil de mot de passe.

Modes de commande

Mode sécurité

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande répertorie les informations pour le profil de mot de passe de sécurité actuel.

Exemple

Cet exemple montre comment afficher les informations détaillées sur le profil de mot de passe :

```
FP9300-A# scope security
FP9300-A /security # show password-profile detail

Password profile:
    Password history count: 5
    No password changes allowed (in Hours): 24
    Password change during interval: Enable
    Password change interval (in Hours): 48
    Password change count: 2
FP9300-A#
```

Commandes associées

Commande	Description
scope password-profile	Permet d'accéder au mode profil de mot de passe.

show pki fsm status

Pour afficher des informations sur le FSM, utilisez la commande **show pki fsm status**.

show pki fsm status [**expand** | **detail**]

Description de la syntaxe

expand	Affiche l'état du FSM.
Détails	Affiche le contenu détaillé de l'état du FSM.

Modes de commande

scope security

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Par défaut, il s'agit d'une sous-commande de la commande **show** dans scope security.

Exemple

Cet exemple montre comment afficher l'état du FSM :

```
Firepower# scope security
Firepower # show pki fsm status expand detail
    FSM Status:
        Affected Object: sys/pki-ext/fsm
        Current FSM: updateEp
        Status: Success
        Completion Time: 2022-08-23T05:14:02.628
        Progress (%): 100
        Description:
        Remote Result: Not Applicable
        Error Code: None
        Error Description:

        FSM Stage:

            Order: 1
            Stage Name: updateEpSetKeyRingLocal
            Status: Success
            Try: 1
            Last Update Time: 2022-08-23T05:14:02.626
            Stage Description: keyring configuration on
primary(FSM-STAGE:sam:dme:PkiEpUpdateEp:SetKeyRingLocal)

            Order: 2
            Stage Name: updateEpSetKeyRingPeer
            Status: Skip
            Try: 0
            Last Update Time: 2022-08-23T05:14:02.626
            Stage Description: keyring configuration on
secondary(FSM-STAGE:sam:dme:PkiEpUpdateEp:SetKeyRingPeer)

            Order: 3
            Stage Name: updateEpPostSetKeyRingLocal
```

```
            Status: Skip
            Try: 0
            Last Update Time: 2022-08-23T05:14:02.627
            Stage Description: post processing after keyring configration on
primary(FSM-STAGE:sam:dme:PkiEpUpdateEp:PostSetKeyRingLocal)

            Order: 4
            Stage Name: updateEpPostSetKeyRingPeer
            Status: Skip
            Try: 0
            Last Update Time: 2022-08-23T05:14:02.628
condary(FSM-STAGE:sam:dme:PkiEpUpdateEp:PostSetKeyRingPeer)g configuration on se--More—
```

show pmon state

Pour afficher l'état des processus en mode gestion locale, utilisez la commande **show pmon state**.

show pmon state

Description de la syntaxe		
	show pmon state	Affiche l'état des processus en mode gestion locale.

Modes de commande connect local-mgmt

Historique des commandes	Version	Modification
	1.1(1)	Commande ajoutée.

Instructions d'utilisation Par défaut, cette commande répertorie l'état des processus en mode gestion locale.

Exemple

Cet exemple montre comment afficher l'état des informations sur les processus en mode gestion locale :

```
firepower#
firepower# connect local-mgmt
...
firepower(local-mgmt)#(local-mgmt)# show pmon state

SERVICE NAME             STATE     RETRY(MAX)    EXITCODE    SIGNAL    CORE
------------             -----     ----------    --------    ------    ----
svc_sam_controller     running           0(4)           0         0      no
smConLogger            running           0(4)           0         0      no
svc_sam_dme            running           0(4)           0         0      no
svc_sam_dcosAG         running           0(4)           0         0      no
svc_sam_bladeAG        running           0(4)           0         0      no
svc_sam_portAG         running           0(4)           0         0      no
svc_sam_statsAG        running           0(4)           0         0      no
svc_sam_hostagentAG    running           0(4)           0         0      no
svc_sam_nicAG          running           0(4)           0         0      no
svc_sam_licenseAG      running           0(4)           0         0      no
svc_sam_extvmmAG       running           0(4)           0         0      no
httpd.sh               running           0(4)           0         0      no
...
```

show post

Pour afficher les erreurs qui se sont produites lors de l'autotest de mise sous tension (POST) du BIOS le plus récent, utilisez la commande **show post**.

show post [*ID* | **detail** | **expand** | **no-errors**]

Description de la syntaxe

id	(Facultatif) Afficher les informations POST pour un serveur spécifique; les valeurs valides sont comprises entre 0 et 42949667295.
detail	(Facultatif) Afficher les détails POST supplémentaires.
expand	(Facultatif) Afficher toutes les informations POST.
no-errors	(Facultatif) Afficher les informations POST sans erreur.

Modes de commande

Tout mode de commande; plus pertinent en mode serveur (/chassis/server).

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande en mode serveur.

Exemple

Cet exemple montre comment afficher les informations POST :

```
FP9300-A# scope server 1/1
FP9300-A /chassis/server # show post

POST:
    Global ID Code     Severity  Affected Object        Description
    --------- -------- --------- ---------------------- ------------
    608       Post 608 Info      sys/chassis-1/blade-1  Invalid DIMM Configuration
```

Commandes associées

Commande	Description
show server bios	Affiche les informations sur le micrologiciel BIOS du serveur.

show pre-login-banner

Pour afficher la bannière de préconnexion, utilisez la commande **show pre-login-banner** .

show pre-login-banner

Modes de commande

scope security

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande affiche les informations sur la bannière de préconnexion.

Exemple

Cet exemple affiche les informations sur la bannière préconnexion :

```
firepower# scope security
firepower /security # scope banner
firepower /security/banner # show pre-login-banner

Pre login banner:
    Message
    -------
    TEST
```

show provider-load-stats

Pour afficher les informations sur les fonctionnalités du fournisseur disponibles sur le système, utilisez la commande **show provider-load-stats** .

show provider-load-stats

Modes de commande

scope system, scope capability

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope system, scope capability.

Exemple

Cet exemple montre comment afficher les informations sur les fonctionnalités du fournisseur :

```
Firepower # scope system
Firepower/system # scope capability
Firepower /system/capability # show provider-load-stats

Provider: capabilities/bundle-type-cap
    Vendor:
    Model:
    Load Errors: 0
    Load Warnings: 0
    Elements Loaded: 8
    Element Load Failures: 0

Provider: capabilities/manufacturer-Cisco Systems Inc-model-CHORLEYWOOD-revision
-0
    Vendor: Cisco Systems Inc
    Model: CHORLEYWOOD
    Load Errors: 0
    Load Warnings: 1
    Elements Loaded: 5
    Element Load Failures: 0

Provider: capabilities/manufacturer-Cisco Systems Inc-model-F9K-C9300-revision-0
    Vendor: Cisco Systems Inc
    Model: F9K-C9300
    Load Errors: 0
    Load Warnings: 0
    Elements Loaded: 5
    Element Load Failures: 0

    TEST
```

Cet exemple montre comment afficher les informations détaillées sur les fonctionnalités du fournisseur :

```
Firepower /system/capability # show provider-load-stats detail

Provider: capabilities/bundle-type-cap
    Vendor:
```

```
    Model:
    Load Errors: 0
    Load Warnings: 0
    Elements Loaded: 8
    Element Load Failures: 0

Provider: capabilities/manufacturer-Cisco Systems Inc-model-CHORLEYWOOD-revision
-0
    Vendor: Cisco Systems Inc
    Model: CHORLEYWOOD
    Load Errors: 0
    Load Warnings: 1
    Elements Loaded: 5
    Element Load Failures: 0

Provider: capabilities/manufacturer-Cisco Systems Inc-model-F9K-C9300-revision-0
    Vendor: Cisco Systems Inc
    Model: F9K-C9300
    Load Errors: 0
    Load Warnings: 0
    Elements Loaded: 5
    Element Load Failures: 0

Provider: capabilities/manufacturer-Cisco Systems Inc-model-FPR-4110-K9-revision
-0
    Vendor: Cisco Systems Inc
    Model: FPR-4110-K9
    Load Errors: 0
    Load Warnings: 0
    Elements Loaded: 5
    Element Load Failures: 0
```

show port-channel (connect fxos)

Pour afficher des informations sur les canaux de ports configurés, utilisez la commande **show port-channel**.

show port-channel { **capacity** | **compatibility-parameters** | **database** | **internal** | **load-balance** | **summary** | **traffic** | **usage** }

Description de la syntaxe

capacity	Affiche des informations sur la capacité du canal de port de l'appareil, y compris le total disponible et le total utilisé.
compatibility-parameters	Répertorie les exigences et l'état de compatibilité de l'interface de canal de port.
database [**interface port-channel** *number*]	Répertorie les informations de configuration et d'état du canal de port, y compris le premier port opérationnel et l'ancienneté du canal de port. (Facultatif) Vous pouvez spécifier un canal de port particulier pour afficher les informations sur ce canal de port uniquement; les numéros de canal de port valides sont compris entre 1 et 4096. Vous pouvez spécifier une sous-interface en ajoutant un point et le numéro de sous-interface (**.** *subinterface_num*) après le numéro de canal de port. Vous pouvez également spécifier une plage de canaux de ports ou plusieurs plages à afficher : • Pour spécifier une plage unique, saisissez *start_num* **-** *end_num* • Pour spécifier plusieurs plages, saisissez *start_num* **-** *end_num* **,** *start_num* **-** *end_num* **,** , etc.
internal { **event-history** | **info** | **max-channels** | **mem-stat** | **sdb** }	Affichez les informations de canal de port pour diverses statistiques internes à l'aide d'un des mots clés suivants : • **event-history** : vous pouvez afficher les journaux pour divers types d'événements de canal de port. • **info** : vous pouvez afficher toutes les informations globales sur les canaux de ports internes ou les informations sur les canaux de ports propres à l'interface. • **max-channels** : affiche le nombre maximal de canaux de ports autorisés sur cet appareil. • **mem-stats** : affiche les statistiques d'allocation de mémoire privée. Le mot clé facultatif **detail** permet d'afficher des statistiques détaillées. • **sdb** : extrait les informations d'état interne du canal de port. La plupart des options disposent d'options et de mots clés supplémentaires; utilisez la commande **show port-channel internal** *keyword* **?** pour afficher les options.
load-balance	Configurez l'équilibrage de charge du canal de port.

summary [**interface port-channel** *number*]	Affichez un résumé du canal de port. (Facultatif) Vous pouvez définir un canal de port particulier pour afficher les informations sur ce canal de port uniquement; les numéros de canal de port valides sont compris entre 1 et 4096. Vous pouvez définir une sous-interface en ajoutant un point et le numéro de sous-interface (**.** *subinterface_num*) après le numéro de canal de port.
traffic [**interface port-channel** *number*]	Affichez les statistiques de trafic des canaux de ports. (Facultatif) Vous pouvez définir un canal de port particulier pour afficher les informations sur ce canal de port uniquement; les numéros de canal de port valides sont compris entre 1 et 4096. Vous pouvez définir une sous-interface en ajoutant un point et le numéro de sous-interface (**.** *subinterface_num*) après le numéro de canal de port.
usage	Répertorie les numéros d'ID de canal de port utilisés et inutilisés.

Modes de commande

connect fxos/

Historique des commandes

Version	Modification
1.1.1	Commande ajoutée.

Instructions d'utilisation

Cette commande est une sous-commande de la commande **show** dans le shell **connect fxos**.

Remarque Lorsque vous vous connectez au shell de commande FXOS, l'invite de ligne de commande passe de votre invite par défaut, qui correspond au nom que vous avez attribué à l'appareil, à l'invite par défaut à laquelle est ajouté (fxos) ; consultez les exemples suivants.

Exemples

Cet exemple présente des informations sur le résumé du canal de port :

```
firepower # connect fxos
firepower(fxos)# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        S - Switched    R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------------
1     Po1(SU)     Eth      LACP      Eth1/3(P)
2     Po2(SU)     Eth      LACP      Eth1/6(P)
48    Po48(SU)    Eth      LACP      Eth1/1(P)
firepower(fxos)#
```

Cet exemple présente des informations sur le trafic du canal de port :

```
firepower # connect fxos
firepower(fxos)# show port-channel traffic
ChanId      Port Rx-Ucst Tx-Ucst Rx-Mcst Tx-Mcst Rx-Bcst Tx-Bcst
------ --------- ------- ------- ------- ------- ------- -------
     1    Eth1/3    0.0%    0.0% 100.00% 100.00%    0.0%    0.0%
------ --------- ------- ------- ------- ------- ------- -------
     2    Eth1/6    0.0%    0.0% 100.00% 100.00%    0.0%    0.0%
------ --------- ------- ------- ------- ------- ------- -------
    48    Eth1/1    0.0%    0.0% 100.00% 100.00%    0.0% 100.00%
firepower(fxos)#
```

Commandes associées

Commande	Description
enter member-port	Permet d'accéder à un port membre existant ou le crée s'il n'existe pas.
enter port-channel	Permet d'accéder à un canal de port existant ou le crée s'il n'existe pas.

show port-channel (scope fabric)

Pour afficher la liste des canaux de ports actuels avec les informations d'état, utilisez la commande **show port-channel**.

show port-channel [**detail** | **expand** | *port_channel_num*]

Description de la syntaxe

detail	Répertorier les informations détaillées sur le canal de port. Le mot clé **expand** est disponible avec cette option.
expand	Répertorier les informations développées sur le canal de port. Le mot clé **detail** est disponible avec cette option.
port_channel_num	Afficher les informations d'état pour le canal de port spécifié uniquement. Les mots clés **detail** et **expand** sont disponibles avec cette option.

Modes de commande

scope eth-uplink/scope fabric/

Historique des commandes

Version	Modification
1.1.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans le mode scope eth-uplink/scope fabric.

Si vous ne spécifiez pas de numéro de canal de port, les informations de tous les canaux de ports sont répertoriées.

Exemple

Cet exemple affiche les informations détaillées sur un canal de port spécifique :

```
firepower /eth-uplink/fabric # show port-channel 48 detail

Port Channel:
    Port Channel Id: 48
    Name: Port-channel48
    Port Type: Cluster
    Description:
    Admin State: Enabled
    Oper State: Up
    Port Channel Mode: Active
    Port Channel Mode State: Enabled
    Auto negotiation: No
    Speed: 1 Gbps
    Duplex: Full Duplex
    Oper Speed: 1 Gbps
    Band Width (Gbps): 1
    State Reason:
    flow control policy: default
    LACP policy name: default
    Oper Lacp Policy Name: org-root/lacp-default
    Inline Pair Admin State: Enabled
    Inline Pair Peer Port Name:
    Allowed Vlan: All
```

```
    Network Control Policy: default
firepower /eth-uplink/fabric #
```

Commandes associées

Commande	Description
create port-channel	Crée un canal de port.
scope port-channel	Cible un canal de port existant pour vous permettre de le configurer et le gérer.

show power-control-policy

Pour afficher la liste des politiques d'alimentation disponibles sur le système, utilisez la commande **show power-control-policy**.

show power-control-policy [**detail** | **expand**]

Description de la syntaxe

detail	Répertorie les informations détaillées sur les politiques de contrôle de l'alimentation.
expand	(Facultatif) Affiche les informations développées pour l'instance d'application actuelle.

Modes de commande

scope org

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope org.

Exemple

Cet exemple affiche les informations de toutes les politiques d'alimentation :

```
QP1 # scope org
QPD /org # show power-control-policy

Power Policy:
    Name
    ----
    default
    ssp-default

QP1 /org # show power-control-policy detail

Power Policy:
    Name: default
    Admin Priority: 5
    Oper Priority: 5
    Description:
    Policy Owner: Local

    Name: ssp-default
    Admin Priority: No Cap
    Oper Priority: No Cap
    Description: ssp default power policy
    Policy Owner: Local

QP1 /org # show power-control-policy detail expand

Power Policy:
    Name: default
    Admin Priority: 5
    Oper Priority: 5
```

```
Description:
Policy Owner: Local

Name: ssp-default
Admin Priority: No Cap
Oper Priority: No Cap
Description: ssp default power policy
Policy Owner: Local
```

show psu

Pour afficher des informations sur les unités d'alimentation installées, utilisez la commande **show psu** en mode châssis.

show psu [*unit_id* | **detail** | **expand**]

Description de la syntaxe

unit_id	(Facultatif) Saisissez un numéro d'unité d'alimentation pour répertorier les informations sur cette unité.
detail	(Facultatif) Utilisez ce mot clé pour répertorier les informations détaillées sur chaque unité d'alimentation installée.
expand	(Facultatif) Utilisez ce mot clé pour afficher les informations développées sur l'alimentation.

Modes de commande

scope chassis/

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Vous pouvez utiliser cette commande sans arguments ni mots clés pour afficher les informations de base sur l'unité d'alimentation.

Exemple

Cet exemple montre comment afficher les informations détaillées sur l'unité d'alimentation :

```
firepower# scope chassis
firepower /chassis # show psu detail

PSU:
    PSU: 1
    Overall Status: N/A
    Operability: N/A
    Threshold Status: N/A
    Power State: Off
    Presence: Equipped
    Thermal Status: OK
    Voltage Status: N/A
    Product Name: Cisco Firepower 9000 Series  AC Power Supply
    PID: FPR9K-PS-AC
    VID: V00
    Part Number: 341-0723-01
    Vendor: Cisco Systems Inc
    Serial (SN): DTM190705G3
    HW Revision: 0
    Firmware Version: N/A
    Type: DV
    Wattage (W): 0
    Input Source: Unknown

    PSU: 2
```

```
    Overall Status: Operable
    Operability: Operable
    Threshold Status: OK
    Power State: On
    Presence: Equipped
    Thermal Status: OK
    Voltage Status: OK
    Product Name: Cisco Firepower 9000 Series  AC Power Supply
    PID: FPR9K-PS-AC
    VID: V00
    Part Number: 341-0723-01
    Vendor: Cisco Systems Inc
    Serial (SN): DTM190705J8
    HW Revision: 0
    Firmware Version: N/A
    Type: DV
    Wattage (W): 2500
    Input Source: 210AC 50 380DC

firepower /chassis #
```

Commandes associées

Commande	Description
show inventory	Affiche des informations sur le châssis et les modules installés.

show psu-policy

Pour afficher le contenu des politiques d'alimentation disponibles sur le système, utilisez la commande **show psu-policy**.

show psu-policy [**detail**]

Description de la syntaxe

detail	Répertorie les informations détaillées sur les politiques d'alimentation.

Modes de commande

scope org

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope org.

Exemple

Cet exemple montre comment afficher les informations sur les politiques d'alimentation :

```
firepower# scope org
firepower /chassis # show psu-policy

PSU Policy:
    Redundancy Description
    ---------- -----------
    NonRedund



QP1 /org # show psu-policy detail

PSU Policy:
    Redundancy: NonRedund
    Description:
```

show registry-repository

Pour afficher les informations sur le registre de services, utilisez la commande **show registry-repository**.

show registry-repository

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment afficher les informations sur le registre de services :

```
FP9300-A# show registry-repository

Service Registry:

    Name:
    ID: 1000
    IP: 0.0.0.0
    Type: Service Reg
    Version:
    Capability: Unspecified
FP9300-A#
```

Commandes associées

Commande	Description
show service-profile	Affiche des informations sur le profil de service.

show remote-user

Pour afficher les détails de l'utilisateur distant, utilisez la commande **show remote-user** .

show remote-user

Modes de commande

scope security

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande affiche les informations sur l'utilisateur distant.

Exemple

Cet exemple affiche les informations sur l'utilisateur distant :

```
firepower# scope security
firepower /ssa # show remote-user
User Name
---------
test1

firepower /security # show remote-user test1 detail
Remote User test1:
    Description:
    User Roles:
        Name: read-only
firepower /security # show remote-user detail
Remote User test1:
    Description:
    User Roles:
        Name: read-only
```

show resource

Pour afficher l'allocation de ressources pour l'instance d'application, utilisez la commande **show resource**.

show resource [**detail**]

Description de la syntaxe

detail	Affiche l'allocation des ressources au format texte plutôt qu'au format tableau.

Modes de commande

scope ssa/scope slot/create app-instance/

Historique des commandes

Version	Modification
2.4(1)	Commande ajoutée.

Instructions d'utilisation

Pour afficher les ressources disponibles, saisissez **show monitor detail**.

Exemple

Voici un exemple de sortie de la commande **show resource**.

```
firepower# scope ssa
firepower /ssa # scope slot 1
firepower /ssa/slot # scope app-instance ftd LD1
firepower /ssa/slot/app-instance # show resource

Resource:
    Allocated Core NR Allocated RAM (MB) Allocated Data Disk (MB) Allocated Binary Disk
(MB)
    ----------------- ------------------ ------------------------ --------------------------

                    6              29593                    40960
3907
```

Voici un exemple de sortie de la commande **show resource detail**.

```
firepower# scope ssa
firepower /ssa # scope slot 1
firepower /ssa/slot # scope app-instance ftd LD1
firepower /ssa/slot/app-instance # show resource detail

Resource:
    Allocated Core NR: 6
    Allocated RAM (MB): 29593
    Allocated Data Disk (MB): 40960
    Allocated Binary Disk (MB): 3907
    Allocated Secondary Disk (MB): 0
```

Commandes associées

Commande	Description
show monitor detail	Affiche l'utilisation des ressources.

Commande	Description
show resource-profile	Affiche les informations sur les profils de ressources.
show resource-profile user-defined	Affiche les affectations de profils de ressources.

show resource-profile

Pour afficher les profils de ressources vDP et les profils de ressources à utiliser avec les instances de contenant, utilisez la commande **show resource-profile**.

show resource-profile [**system** [*name*] | **user-defined** [*name*] | **vdp** [*version* [*name*]]] [**detail**]

Description de la syntaxe

name	Spécifie le nom du profil.
system	Affiche uniquement les profils de ressources définis par le système.
user-defined	Affiche les profils d'instances de contenant définis par l'utilisateur, y compris le profil de ressource par défaut.
vdp	Affiche les profils vDP définis par le système.
version	Affiche vDP pour une version particulière.
detail	Affiche les détails sur les profils de ressources.

Modes de commande

scope ssa/

Historique des commandes

Version	Modification
2.4(1)	Ajout du mot clé **user-defined**.
1.1 (3)	Commande ajoutée.

Instructions d'utilisation

Spécifiez le profil de ressource à utiliser avec une instance d'application à l'aide de la commande **set resource-profile-name**. Vous pouvez ajouter des profils de ressources pour les instances de contenant à l'aide de la commande **create resource-profile**. Les profils de ressources vDP sont automatiquement créés par le système. Le châssis comprend un profil de ressource d'instance de contenant par défaut appelé « Default-Small », qui comprend le nombre minimal de cœurs. Vous pouvez modifier la définition de ce profil et même le supprimer s'il n'est pas utilisé. Notez que ce profil est créé lors du rechargement du châssis et qu'aucun autre profil n'existe sur le système.

Exemple

Voici un exemple de sortie de la commande **show resource-profile** :

```
firepower# scope ssa
firepower /ssa # show resource-profile
Profile Name       App Name   App Version  Is In Use  Security Model  CPU Logical Core Count
 RAM Size (MB)  Default Profile Profile Type Description
------------------ ---------- ------------ ---------- --------------- ----------------------
 -------------- --------------- ------------ -----------
bronze              N/A        N/A          No         all
 6              0 No              User Defined low end device
DEFAULT-4110-RESOURCE
                    vdp        8.13.01.09-2 No         FPR4K-SM-12
 4          16384 Yes             System
```

```
DEFAULT-RESOURCE   vdp        8.13.01.09-2 No         FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36,
 FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

 6          24576 Yes             System
gold              N/A        N/A          No         all
14                0 No              User Defined  highest
silver            N/A        N/A          No         all
 8                0 No              User Defined  mid-level
Default-Small     N/A        N/A          Yes        all
 6              N/A No              User Defined
VDP-10-CORES      vdp        8.13.01.09-2 No         FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36,
 FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

10          40960 No              System
VDP-2-CORES       vdp        8.13.01.09-2 No         all
 2           8192 No              System
VDP-4-CORES       vdp        8.13.01.09-2 No         all
 4          16384 No              System
VDP-8-CORES       vdp        8.13.01.09-2 No         FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36,
 FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24
                                                    8          32768 No              System
firepower /ssa #
```

Voici un exemple de sortie de la commande **show resource-profile user-defined** :

```
firepower# scope ssa
firepower /ssa # show resource-profile user-defined
Profile Name       Is In Use  CPU Logical Core Count Description
------------------ ---------- ---------------------- -----------
bronze               No               6              low end device
gold                 No               14             highest
silver               No               10             mid-level
firepower /ssa #
```

Commandes associées

Commande	Description
create resource-profile	Ajoute un profil de ressource d'instance de contenant.
set cpu-count	Définit le nombre de CPU pour le profil de ressource.
set resource-profile-name	Affecte le profil de ressource à l'instance d'application.
show monitor detail	Affiche l'utilisation des ressources pour le module de sécurité ou le logement de moteur.
show resource detail	Affiche l'affectation de ressources pour l'instance d'application.

show role

Pour afficher la liste des rôles et des privilèges, utilisez la commande **show role** .

show role [**detail** | **name**]

Description de la syntaxe

detail	Afficher la liste des rôles.
name	(Facultatif) Affiche le contenu du rôle spécifié.

Modes de commande

scope security

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Par défaut, il s'agit d'une sous-commande de la commande **show** dans scope security.

Exemple

Cet exemple montre comment afficher les certificats importés et vérifier la valeur d'état de ces certificats :

```
firepower# scope security
firepower /ssa # show roleRole:
    Role Name  Priv
    ---------- ----
    aaa        aaa
    admin      admin
    operations fault, operations
    read-only read-only
```

Cet exemple montre comment afficher le contenu des rôles dans un système :

```
firepower /security # show role detail
Role:
    Role Name: aaa
    Priv: aaa

    Role Name: admin
    Priv: admin

    Role Name: operations
    Priv: fault, operations

    Role Name: read-only
    Priv: read-only
```

Cet exemple montre comment afficher le contenu du rôle sélectionné :

```
firepower /security # show role aaa

Role:
    Role Name Priv
    ---------- ----
    aaa        aaa
```

show (scope fabric)

Pour afficher les informations sur un canal de port, utilisez la commande **show**.

show

Modes de commande

scope eth-uplink/scope fabric a/

Historique des commandes

Version	Modification
2.0.1	Commande ajoutée.

Instructions d'utilisation

Vous devez créer des canaux de ports avant d'utiliser cette commande.

Exemple

Cet exemple montre comment afficher des informations détaillées sur tous les canaux de ports :

```
firepower-9300# scope eth-uplink
firepower-9300 /eth-uplink # scope fabric a
firepower-9300 /eth-uplink/fabric # create port-channel 3
firepower-9300 /eth-uplink/fabric/port-channel* # show
  Port Channel:
Port Channel Id Name Port Type Admin
State Oper State State Reason
-------------- ---------------- ------------------ -----
------ ---------------- ------------
10 Port-channel10 Data Enabled Failed No operational members


firepower-9300 /eth-uplink/fabric/port-channel #
```

Commandes associées

Commande	Description
create port-channel	Crée le canal de port.
scope port-channel	Affiche des informations relatives au canal de port et au port.

show schedule infra-fw

Pour afficher la liste des micrologiciels d'infrastructure planifiés, utilisez la commande **show schedule infra-fw**.

show schedule infra-fw [**detail**]

Description de la syntaxe

detail	Affiche les informations détaillées sur les micrologiciels d'infrastructure planifiés.

Modes de commande

scope system

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope system.

Exemple

Cet exemple montre comment afficher toutes les informations sur les micrologiciels d'infrastructure planifiés sur le système :

```
Firepower /fabric-interconnect # scope system
Firepower /system # show schedule infra-fw
Schedule:
    Name
    ----
    infra-fw
```

Exemple

Cet exemple montre comment afficher des informations détaillées sur tous les micrologiciels d'infrastructure planifiés sur le système disponibles :

```
Firepower # show schedule infra-fw detail
Schedule:
    Name: infra-fw
    Description: Auto created by the system for Infrastructure upgrade
```

Exemple

Cet exemple montre comment afficher des informations détaillées de tous les micrologiciels d'infrastructure planifiés :

```
Firepower /system # show schedule infra-fw expand detail
Schedule:
    Name: infra-fw
    Description: Auto created by the system for Infrastructure upgrade

    One-Time Occurrence:
```

```
Name: infra-fw
Start Date: 2012-07-05T23:27:33.148
Max Duration (dd hh mm ss): None
Max Concur Tasks: Unlimited
Max Tasks: Unlimited
Min Interval (dd hh mm ss): None
Executed Tasks: 19
```

show security

Pour afficher les informations de sécurité relatives au mot de passe et à l'état du FSM, utilisez la commande**show security**.

show security [**detail** | **fsm**]

Description de la syntaxe

detail	(Facultatif) Affiche les informations de sécurité détaillées sur le mot de passe.
fsm status	(Facultatif) Affiche les informations sur l'état de la machine à états finis (FSM). Le mot de passe **status** est requis.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment afficher les informations développées du mode sécurité :

```
FP9300-A# show security detail

security mode:
    Password Strength Check: No
    Minimum Password Length: 8
    Current Task:
FP9300-A#
```

Commandes associées

Commande	Description
scope security	Permet d'accéder au mode sécurité.

show sel

Pour afficher le contenu du journal des événements système (SEL) d'un serveur, utilisez la commande **show sel**.

show sel *server_id*

Description de la syntaxe

server_id	Identifiant du serveur, sous forme de numéro de châssis/numéro de serveur (l'ID de rack n'est pas une option valide).

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment afficher le contenu du journal des événements système (SEL) du serveur 1 dans le châssis 1 :

```
FP9300-A# show sel 1/1
 show sel 1/1
1 | 12/16/2015 23:09:55 | CIMC | Event Logging Disabled DDR4_
P2_H2_ECC #0x99 | Log Area Reset/Cleared |  | Asserted
2 | 12/16/2015 23:09:56 | CIMC | Processor P2_THERMTRIP_N #0x
7a | Limit Not Exceeded | Asserted
3 | 12/16/2015 23:09:57 | CIMC | Processor P1_THERMTRIP_N #0x
79 | Limit Not Exceeded | Asserted
4 | 12/16/2015 23:10:00 | CIMC | Platform alert LED_SYS_ACT #
0xa4 | LED is on | Asserted
5 | 12/16/2015 23:10:00 | CIMC | Platform alert LED_SYS_ACT #
0xa4 | LED color is green | Asserted
6 | 12/16/2015 23:10:01 | CIMC | Processor DDR4_P2_H3_TMP #0x
73 | Limit Not Exceeded | Asserted
7 | 12/16/2015 23:10:01 | CIMC | Platform alert LED_LOM_FAULT
 #0xa3 | LED is off | Asserted
8 | 12/16/2015 23:10:01 | CIMC | Platform alert LED_LOM_FAULT
 #0xa3 | LED color is blue | Asserted
9 | 12/16/2015 23:10:03 | CIMC | Processor DDR4_P2_H2_TMP #0x
72 | Limit Not Exceeded | Asserted
--More--

    <--- remaining lines removed for brevity --->

FP9300-A#
```

Commandes associées

Commande	Description
scope server	Permet d'accéder au mode serveur.

show server actual-boot-order

Pour afficher l'ordre de démarrage du serveur réellement utilisé par le BIOS lors du dernier démarrage du serveur, utilisez la commande **show server actual-boot-order**.

show server actual-boot-order [*server_id* | **uuid** *dynamic_uuid*]

Description de la syntaxe

server_id	(Facultatif) Affiche l'ordre de démarrage réel d'un serveur spécifique, sous forme de numéro de châssis/numéro de serveur (l'ID de rack n'est pas une option valide).
uuid *dynamic_uuid*	(Facultatif) Affiche l'ordre de démarrage réel d'un serveur spécifique à l'aide de son identifiant unique universel (UUID) dynamique; spécifié sous la forme NNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande affiche les informations sur l'ordre de démarrage réel de tous les serveurs.

Exemple

Cet exemple montre comment afficher l'ordre de démarrage réel de tous les serveurs :

```
firepower# show server actual-boot-order
Server 1/1:
    Last Update: 2017-07-19T17:43:14.982
    LocalStorageAny
        (1) Not found. Please verify presence of device and p
resence of UEFI loader on device

Server 1/2:
    Last Update: 2017-07-19T17:43:14.980
    LocalStorageAny
        (1) Not found. Please verify presence of device and p
resence of UEFI loader on device

firepower#
```

Commandes associées

Commande	Description
show server boot-order	Affiche l'ordre de démarrage des serveurs.

show server adapter

Pour afficher les informations sur les adaptateurs réseau d'un serveur, utilisez la commande **show server adapter**.

show server adapter [*server_id* | **detail** | **identity** | **inventory** | **status** | **uuid** *dynamic_uuid*]

Description de la syntaxe

server_id	(Facultatif) Affiche les informations sur les adaptateurs réseau pour un serveur spécifique, sous forme de numéro de châssis/numéro de serveur (l'ID de rack n'est pas une option valide). Le mot clé **detail** est disponible avec cette option.
detail	(Facultatif) Affiche les informations détaillées sous forme de liste.
identity	(Facultatif) Affiche les informations d'identité complètes pour chaque adaptateur disponible. Les mots clés **uuid** et *server_id* sont disponibles avec cette option.
inventory	(Facultatif) Répertorie les adaptateurs réseau installés. Les mots clés **detail** , **uuid** et *server_id* sont disponibles avec cette option.
status	(Facultatif) Affiche l'état global des adaptateurs réseau installés. Les mots clés **detail** , **uuid** et *server_id* sont disponibles avec cette option.
uuid *dynamic_uuid*	(Facultatif) Affiche les informations sur les adaptateurs réseau d'un serveur particulier, spécifié avec son identifiant unique universel (UUID) dynamique; saisi sous la forme NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN. Le mot clé **detail** est disponible avec cette option.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande répertorie les adaptateurs disponibles sur chaque serveur. Il s'agit des mêmes informations affichées avec le mot clé **inventory**.

Exemple

Cet exemple montre comment afficher les informations d'identité sur les adaptateurs réseau installés :

```
firepower# show server adapter identity
Server 1/1:
    Burned-In UUID: 84928111-2710-4e7c-b664-91bce5b5dfbd
    Dynamic UUID: 84928111-2710-4e7c-b664-91bce5b5dfbd
    Adapter 1:
        Product Name: Cisco Firepower 9000 series MLOM Adapter
        PID: FPR-C9300-MP
        VID: V01
        Vendor: Cisco Systems Inc
        Serial: JAD190702J1
        Revision: 0
```

```
        Eth Interface:

        Adapter Interface Dynamic MAC Address
        ------- --------- ------------------
              1         1 00:15:A5:01:01:00
              1         2 00:15:A5:00:00:8E
              1         3 B0:AA:77:2F:5A:4C
              1         4 B0:AA:77:2F:5A:7C
              1         5 B0:AA:77:2F:5A:6C
              1         6 00:15:A5:00:00:CF
              1         7 00:15:A5:00:00:DF
              1         8 00:15:A5:00:01:0F
              1         9 00:15:A5:00:00:BF
              1        10 00:15:A5:00:00:6E
              1        11 00:15:A5:00:01:0C
              1        12 00:15:A5:00:00:EF
              1        13 00:15:A5:00:01:1F
              1        14 00:15:A5:00:00:1F
              1        15 00:15:A5:00:00:3F

        Ext Interface:

        Adapter Interface Mac
        ------- --------- ---
              1         1 BA:DB:AD:BA:D6:08
              1         5 BA:DB:AD:BA:D6:09

    Adapter 2:
        Product Name: Cisco Firepower 9000 series MEZZ Adapter

    <--- remaining lines removed for brevity --->

firepower#
```

Commandes associées

Commande	Description
scope adapter	Permet d’accéder au mode adaptateur.

show server assoc

Pour afficher le profil de service associé à chaque serveur, utilisez la commande **show server assoc**.

show server assoc [*server_id* | **uuid** *dynamic_uuid*]

Description de la syntaxe

server_id	(Facultatif) Affiche les informations sur un serveur particulier, spécifié à l'aide du numéro de châssis/numéro de serveur (l'ID de rack n'est pas une option valide).
uuid *dynamic_uuid*	(Facultatif) Affiche les informations d'un serveur particulier, spécifié avec son identifiant unique universel (UUID) dynamique; saisi sous la forme NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande répertorie les associations de profils de service sur chaque serveur.

Exemple

Cet exemple montre comment afficher les profils de service associés aux serveurs du système :

```
FP9300-A# show server assoc
Server  Association  Service Profile
------- ------------ ---------------
1/1     Associated   ssp-sprof-1
1/2     Associated   ssp-sprof-2

FP9300-A#
```

Commandes associées

Commande	Description
show service-profile	Affiche des informations sur le profil de service.

show server bios

Pour afficher les informations sur le micrologiciel BIOS du serveur, utilisez la commande **show server bios**.

show server bios [*server_id* | **detail** | **uuid** *dynamic_uuid*]

Description de la syntaxe

server_id	(Facultatif) Affiche les informations sur un serveur particulier, spécifié à l'aide du numéro de châssis/numéro de serveur (l'ID de rack n'est pas une option valide). Le mot clé **detail** est disponible avec cette option.
detail	(Facultatif) Affiche les informations détaillées sur le BIOS.
uuid *dynamic_uuid*	(Facultatif) Affiche les informations sur un serveur particulier, spécifié avec son identifiant unique universel (UUID) dynamique; saisi sous la forme NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN. Le mot clé **detail** est disponible avec cette option.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande répertorie les informations BIOS pour chaque serveur.

Exemple

Cet exemple montre comment afficher les informations détaillées sur le micrologiciel BIOS pour tous les serveurs :

```
FP9300-A# show server bios detail
Server 1/1:
    Model: FPR9K-SM-24
    Revision: 0
    Serial:
    Vendor: Cisco Systems, Inc.
    Running-Vers: FXOSSM1.1.2.1.3.031420161207
    Package-Vers: 2.0(1.135)
    Init Sequence: 0x0a:0x0a:0x0d:0x0d:0x0b:0x0b:0x01:0x01:0x
00:0x00:0x03:0x03:0x00:0x00:0x02:0x02:0x83:0x83:0xae:0xad
    Init Time: 2015-11-23T19:24:13.159

Server 1/2:
    Model: FPR9K-SM-24
    Revision: 0
    Serial:
    Vendor: Cisco Systems, Inc.
    Running-Vers: FXOSSM1.1.2.1.3.031420161207
    Package-Vers: 2.0(1.135)
    Init Sequence: 0x0a:0x0a:0x0d:0x0d:0x0b:0x0b:0x01:0x01:0x
00:0x00:0x03:0x03:0x00:0x00:0x02:0x02:0x83:0x83:0xae:0xad
    Init Time: 2015-11-23T18:56:23.148
FP9300-A#
```

Commandes associées

Commande	Description
show server version	Affiche les versions logicielles et les informations d'état actuelles du serveur.

show server boot-order

Pour afficher l'ordre de démarrage d'un serveur, utilisez la commande **show server boot-order**.

show server boot-order [*server_id* | **detail** | **uuid** *dynamic_uuid*]

Description de la syntaxe

server_id	(Facultatif) Affiche l'ordre de démarrage d'un serveur spécifique, sous forme de numéro de châssis/numéro de serveur (l'ID de rack n'est pas une option valide). Le mot clé **detail** est disponible avec cette option.
detail	(Facultatif) Affiche des informations détaillées sur l'ordre de démarrage.
uuid *dynamic_uuid*	(Facultatif) Affiche l'ordre de démarrage d'un serveur spécifique à l'aide de son identifiant unique universel (UUID) dynamique; spécifié sous la forme NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN. Le mot clé **detail** est disponible avec cette option.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande affiche les informations sur l'ordre de démarrage de tous les serveurs.

Exemple

Cet exemple montre comment afficher l'ordre de démarrage de tous les serveurs :

```
FP9300-A# show server boot-order
Boot Definition:
    Full Name: sys/chassis-1/blade-1/boot-policy
    Reboot on Update: No
    Boot Mode: Uefi

    Boot Storage:
        Order: 1

        Local Storage:
            Name: local-storage

            Boot Any Local Device:
                Order: 1
                Type: Local Any

    Full Name: sys/chassis-1/blade-2/boot-policy
    Reboot on Update: No
    Boot Mode: Uefi

    Boot Storage:
        Order: 1

        Local Storage:
            Name: local-storage
```

```
            Boot Any Local Device:
                Order: 1
                Type: Local Any

    <--- remaining lines removed for brevity --->

FP9300-A#
```

Commandes associées

Commande	Description
show server actual-boot-order	Affiche l'ordre de démarrage réel des serveurs.

show server cpu

Pour afficher des informations sur les CPU du serveur, utilisez la commande **show server cpu**.

show server cpu [*server_id* | **detail** | **uuid** *dynamic_uuid*]

Description de la syntaxe

server_id	(Facultatif) Affiche les informations sur le CPU pour un serveur spécifique, sous forme de numéro de châssis/numéro de serveur (l'ID de rack n'est pas une option valide). Le mot clé **detail** est disponible avec cette option.
detail	(Facultatif) Affiche les informations détaillées sur le CPU sous forme de liste.
uuid *dynamic_uuid*	(Facultatif) Affiche les informations sur le CPU pour un serveur particulier, spécifié avec son identifiant unique universel (UUID) dynamique; saisi sous la forme NNNNNNNN-NNNN-NNNN-NNNNNNNNNN. Le mot clé **detail** est disponible avec cette option.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande affiche les informations sur le CPU pour tous les serveurs.

Exemple

Cet exemple montre comment afficher des informations sur les CPU du serveur 1 dans le châssis 1 :

```
FP9300-A# show server cpu 1/1
Server 1/1:
    ID  Presence             Architecture      Socket Cores
     Speed (GHz)
    --- -------------------- ----------------- ------ -------
---- -----------
      1 Equipped             Xeon              CPU1   12
     2.200000
      2 Equipped             Xeon              CPU2   12
     2.200000

FP9300-A#
```

Commandes associées

Commande	Description
show server inventory	Affiche des informations sur les serveurs installés dans cet appareil.

show server decommissioned

Pour afficher la liste des serveurs désactivés, utilisez la commande **show server decommissioned**.

show server decommissioned

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment afficher la liste de serveurs désactivés :

```
FP9300-A# show server decommissioned
Vendor            Model         Serial (SN) Server
----------------- ----------    ----------- ------
Cisco Systems Inc R210-2121605W QCI1442AHFX 2

FP9300-A #
```

Commandes associées

Commande	Description
show server inventory	Affiche des informations sur les serveurs installés dans cet appareil.

show server detail

Pour afficher le serveur en détail, utilisez la commande **show server detail**.

show server [**detail** | **expand**]

Description de la syntaxe

detail	Affiche les informations détaillées sur la configuration d'exportation.
expand	(Facultatif) Affiche des informations développées pour le serveur.

Modes de commande

scope security/radius, scope chassis 1

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope system.

Exemple

Cet exemple affiche les informations sur le serveur.

```
Firepower# scope security
Firepower /security # scope radius
Firepower /security/radius # show server detail
RADIUS server:
    Hostname, FQDN or IP address: RADIUSserver
    Descr:
    Order: 1
    Auth Port: 1812
    Key: ****
    Timeout: 5
    Retries: 4
Note: server details can be configured based on user requirements
as shown below.
Firepower /security/radius # create server RADIUSserver
Firepower /security/radius/server* # set authport 1812
Firepower /security/radius/server* # set order 1
Firepower /security/radius/server* # set key
Enter the key:
Confirm the key:
Firepower /security/radius/server* # set timeout 5
Firepower /security/radius/server* # set retries 4
Firepower /security/radius/server* # commit-buffer
Firepower /security/radius/server # exit
```

Cet exemple montre comment afficher les informations sur tous les serveurs du système :

```
Firepower# scope chassis 1
Firepower /chassis #
Firepower /chassis # show server
Server:
```

```
    Slot    Overall Status        Service Profile
    ------- --------------------- ---------------
          1 Ok                    ssp-sprof-1
          2 Ok                    ssp-sprof-2
Firepower /chassis # show server detail
Server:
    Slot: 1
    Name:
    User Label:
    Overall Status: Ok
    Oper Qualifier: N/A
    Service Profile: ssp-sprof-1
    Association: Associated
    Discovery: Complete
    Conn Path: A
    Conn Status: A
    Managing Instance: A
    Admin Power: Policy
    Oper Power: On
    BIOS POST State: Complete
    Admin State: In Service
    Product Name: Cisco Firepower 9000 Series Security Module
    PID: FPR9K-SM-24
    VID: V01
    Vendor: Cisco Systems Inc
    Serial (SN): FLM1949C6X0
    HW Revision: 0
    Mfg Date: 2016-01-11T00:00:00.000
    Part Number: 73-17705-01
    Memory (MB): 262144
    Effective Memory (MB): 262144
    Operating Memory Speed (MHz): 2133
    Operating Memory Voltage: Regular Voltage
    Cores: 24
    Num Of Cores Enabled: 24
    Adapters: 2
    Eth Host Interfaces: 169
    FC Host Interfaces: 0
    Burned-In UUID: bd1b3bfe-eb58-44d2-ad24-4a73ba0b24d4
    Dynamic UUID: bd1b3bfe-eb58-44d2-ad24-4a73ba0b24d4
    Last Adaptor Crash Reset:
    Last BIOS Hang Reset: 2022-09-02T01:31:14.658
    Last CATERR Reset: 1970-01-01T00:00:00.000
    Current Task 1:
    Current Task 2:
    Current Task 3:

    Slot: 2
    Name:
    User Label:
    Overall Status: Ok
    Oper Qualifier: N/A
    Service Profile: ssp-sprof-2
    Association: Associated
    Discovery: Complete
    Conn Path: A
    Conn Status: A
    Managing Instance: A
    Admin Power: Policy
    Oper Power: On
    BIOS POST State: Complete
    Admin State: In Service
    Product Name: Cisco Firepower 9000 Series Security Module
    PID: FPR9K-SM-24
```

```
    VID: V01
    Vendor: Cisco Systems Inc
    Serial (SN): FCH1837703M
    HW Revision: 0
    Mfg Date: 2016-01-06T00:00:00.000
    Part Number: 73-17705-01
    Memory (MB): 262144
    Effective Memory (MB): 262144
    Operating Memory Speed (MHz): 2133
    Operating Memory Voltage: Regular Voltage
    Cores: 24
    Num Of Cores Enabled: 24
    Adapters: 2
    Eth Host Interfaces: 169
    FC Host Interfaces: 0
    Burned-In UUID: 8c4d2cd2-f3f6-46f0-afd3-f46e95c81469
    Dynamic UUID: 8c4d2cd2-f3f6-46f0-afd3-f46e95c81469
    Last Adaptor Crash Reset:
    Last BIOS Hang Reset: 2022-09-02T01:31:38.690
    Last CATERR Reset: 1970-01-01T00:00:00.000
    Current Task 1:
    Current Task 2:
    Current Task 3:
```

Cet exemple montre les informations développées sur les **serveurs**

```
Firepower /chassis # show server detail expand
Server:
    Slot: 1
    Name:
    User Label:
    Overall Status: Ok
    Oper Qualifier: N/A
    Service Profile: ssp-sprof-1
    Association: Associated
    Discovery: Complete
    Conn Path: A
    Conn Status: A
    Managing Instance: A
    Admin Power: Policy
    Oper Power: On
    BIOS POST State: Complete
    Admin State: In Service
    Product Name: Cisco Firepower 9000 Series Security Module
    PID: FPR9K-SM-24
    VID: V01
    Vendor: Cisco Systems Inc
    Serial (SN): FLM1949C6X0
    HW Revision: 0
    Mfg Date: 2016-01-11T00:00:00.000
    Part Number: 73-17705-01
    Memory (MB): 262144
    Effective Memory (MB): 262144
    Operating Memory Speed (MHz): 2133
    Operating Memory Voltage: Regular Voltage
    Cores: 24
    Num Of Cores Enabled: 24
    Adapters: 2
    Eth Host Interfaces: 169
    FC Host Interfaces: 0
    Burned-In UUID: bd1b3bfe-eb58-44d2-ad24-4a73ba0b24d4
    Dynamic UUID: bd1b3bfe-eb58-44d2-ad24-4a73ba0b24d4
    Last Adaptor Crash Reset:
```

```
Last BIOS Hang Reset: 2022-09-02T01:31:14.658
Last CATERR Reset: 1970-01-01T00:00:00.000
Current Task 1:
Current Task 2:
Current Task 3:

Adapter:
    Id: 1
    Product Name: Cisco Firepower 9000 series MLOM Adapter
    PID: FPR-C9300-MP
    VID: V01
    Vendor: Cisco Systems Inc
    Serial: JAD19500B7X
    Revision: 0
    Mfg Date: 2015-12-11T00:00:00.000
    Slot: N/A
    Overall Status: Operable
    Conn Path: A
    Conn Status: A
    Managing Instance: A
    Product Description: Cisco Firepower 9000 series MLOM Adapter
```

show server environment

Pour afficher des informations sur l'état actuel du serveur, utilisez la commande **show server environment**.

show server environment [*server_id* | **adapter** | **board** | **cpu** | **detail** | **expand** | **memory** | **uuid** *dynamic_uuid*]

Description de la syntaxe

server_id	(Facultatif) Affiche les informations sur l'état d'un serveur particulier, spécifié à l'aide du numéro de châssis/numéro de serveur (l'ID de rack n'est pas une option valide).
adapter	(Facultatif) Affiche l'état du serveur et les informations sur l'état de chaque adaptateur. Les mots clés **board**, **cpu**, **detail** et **memory** sont également disponibles.
board	(Facultatif) Affiche l'état du serveur et les informations sur l'état de chaque carte mère. Les mots clés **adapter**, **cpu**, **detail** et **memory** sont également disponibles.
cpu	(Facultatif) Affiche l'état du serveur, les informations sur la carte mère et les informations sur l'état de chaque CPU. Les mots clés **adapter**, **board**, **detail** et **memory** sont également disponibles.
detail	(Facultatif) Affiche des informations d'état détaillées sous forme de liste.
expand	(Facultatif) Affiche des informations d'état développées, notamment des informations sur l'adaptateur, la carte mère, la matrice mémoire, les modules DIMM et le processeur. Le mot clé **detail** est également disponible.
memory	(Facultatif) Répertorie des informations d'état sur les serveurs, les cartes mères, les matrices mémoire et les modules DIMM. Les mots clés **adapter**, **board**, **cpu** et **detail** sont également disponibles.
uuid *dynamic_uuid*	(Facultatif) Affiche les informations sur l'état d'un serveur particulier, spécifié avec son identifiant unique universel (UUID) dynamique; saisi sous la forme `NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN`.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande répertorie des informations sur l'environnement de base de chaque serveur.

Exemple

Cet exemple montre comment afficher des informations détaillées sur l'état des adaptateurs réseau installés sur tous les serveurs :

```
FP9300-A# show server environment adapter detail

Server 1/1:
    Overall Status: Ok
    Operability: Operable
    Oper Power: On

    Adapter 1:
        Threshold Status: N/A
        Overall Status: Operable
        Operability: Operable
        Power State: On
        Thermal Status: N/A
        Voltage Status: N/A

    Adapter 2:
        Threshold Status: N/A
        Overall Status: Operable
        Operability: Operable
        Power State: On
        Thermal Status: N/A
        Voltage Status: N/A

Server 1/2:
    Overall Status: Ok
    Operability: Operable
    Oper Power: On

    Adapter 1:
        Threshold Status: N/A
        Overall Status: Operable
        Operability: Operable

    <--- remaining lines removed for brevity --->

FP9300-A#
```

Commandes associées

Commande	Description
show system	Affiche les informations sur les systèmes configurés sur cet appareil.

show server firmware

Pour afficher les versions du micrologiciel du serveur et les informations d'état, utilisez la commande **show server firmware**.

show server firmware [*server_id* | **adapter** | **bios** | **boardcontroller** | **cimc** | **detail** | **fxos** | **storage** | **uuid** *dynamic_uuid*]

Description de la syntaxe

server_id	(Facultatif) Affiche des informations sur le micrologiciel et l'état d'un serveur particulier, spécifié à l'aide du numéro de châssis/numéro de serveur (l'ID de rack n'est pas une option valide).
adapter	(Facultatif) Affiche la version du micrologiciel et les informations sur l'état de chaque adaptateur. Le mot clé **detail** est également disponible.
bios	(Facultatif) Affiche les versions et l'état du micrologiciel BIOS du serveur. Le mot clé **detail** est également disponible.
boardcontroller	(Facultatif) Affiche les versions et l'état du contrôleur de gestion. Le mot clé **detail** est également disponible.
cimc	(Facultatif) Affiche les versions et l'état de Cisco Integrated Management Controller. Le mot clé **detail** est également disponible.
detail	(Facultatif) Affiche des informations détaillées sur le micrologiciel et l'état sous forme de liste.
fxos	(Facultatif) Affiche des informations sur la version et l'état des systèmes d'exploitation des logements de sécurité (SSP) installés. Le mot clé **detail** est également disponible.
storage	(Facultatif) Répertorie les informations sur la version et l'état des contrôleurs de disque local et RAID. Le mot clé **detail** est également disponible.
uuid *dynamic_uuid*	(Facultatif) Affiche les informations sur le micrologiciel et l'état d'un serveur particulier, spécifié à l'aide de son identifiant unique universel (UUID) dynamique; saisi sous la forme `NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN`.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande répertorie les informations de base sur le micrologiciel de chaque serveur.

Exemple

Cet exemple montre comment afficher les informations sur le micrologiciel et l'état des contrôleurs de disque local et RAID sur tous les serveurs :

```
FP9300-A# show server firmware storage
Server 1/1:
    RAID Controller 1:
        Running-Vers: 24.5.0-0021
        Package-Vers:
        Activate-Status: Ready

Server 1/2:
    RAID Controller 1:
        Running-Vers: 24.5.0-0021
        Package-Vers:
        Activate-Status: Ready

    Local Disk 1:
        Running-Vers: EM14
        Package-Vers:
        Activate-Status: Ready

    Local Disk 2:
        Running-Vers: EM14
        Package-Vers:
        Activate-Status: Ready


    Local Disk 1:
        Running-Vers: EM14
        Package-Vers:
        Activate-Status: Ready

    Local Disk 2:
        Running-Vers: EM14
        Package-Vers:
        Activate-Status: Ready

FP9300-A#
```

Commandes associées

Commande	Description
scope firmware	Permet d’accéder au mode micrologiciel.

show server fsm status

Pour afficher les détails sur l'état du FSM du serveur, utilisez la commande **show server fsm status**.

show server fsm [**status**]

Description de la syntaxe

status	Affiche l'état du FSM du serveur.

Modes de commande

scope chassis 1

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope system.

Exemple

Cet exemple montre comment afficher les informations sur l'état du FSM du serveur dans le système :

```
Firepower /chassis # show server fsm status
Slot: 1
Server: sys/chassis-1/blade-1

    FSM 1:
        Remote Result: Not Applicable
        Remote Error Code: None
        Remote Error Description:
        Status: Nop
        Previous Status: Turnup Success
        Timestamp: 2022-12-15T07:20:11.679
        Try: 0
        Flags: 0
        Progress (%): 100
        Current Task:

    FSM 2:
        Status: Nop
        Previous Status: Identify Success
        Timestamp: 2022-12-15T07:18:37.610
        Try: 0
        Progress (%): 100
        Current Task:

    FSM 3:
        Status: Nop
        Previous Status: Configure Success
        Timestamp: 2022-12-15T07:20:09.067
        Try: 0
        Flags: 0
        Progress (%): 100
        Current Task:

Slot: 2
Server: sys/chassis-1/blade-2
```

```
FSM 1:
    Remote Result: Not Applicable
    Remote Error Code: None
    Remote Error Description:
    Status: Nop
    Previous Status: Turnup Success
    Timestamp: 2022-12-15T07:19:54.682
    Try: 0
    Flags: 0
    Progress (%): 100
    Current Task:
FSM 2:
    Status: Nop
    Previous Status: Identify Success
    Timestamp: 2022-12-15T07:18:37.597
    Try: 0
    Progress (%): 100
    Current Task:

FSM 3:
    Status: Nop
    Previous Status: Configure Success
    Timestamp: 2022-12-15T07:19:52.003
    Try: 0
    Flags: 0
    Progress (%): 100
    Current Task:
```

show server identity

Pour afficher les informations d'identité des serveurs, adaptateurs et interfaces, utilisez la commande **show server identity**.

show server identity [*server_id* | **uuid** *dynamic_uuid*]

Description de la syntaxe

server_id	(Facultatif) Affiche les informations d'identification sur un serveur particulier, spécifié à l'aide du numéro de châssis/numéro de serveur (l'ID de rack n'est pas une option valide).
uuid *dynamic_uuid*	(Facultatif) Affiche les informations d'identification d'un serveur particulier, spécifié avec son identifiant unique universel (UUID) dynamique; saisi sous la forme `NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN`.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande répertorie les informations d'identification pour chaque serveur.

Exemple

Cet exemple montre comment afficher les informations d'identité sur le serveur 2 dans le châssis 1 :

```
FP9300-A# show server identity 1/2
Server 1/2:
    Burned-In UUID: b3fd461c-b1c7-437b-ab08-c5cb28a84132
    Dynamic UUID: b3fd461c-b1c7-437b-ab08-c5cb28a84132

    Eth Interface:

    Adapter Interface Dynamic MAC Address
    ------- --------- ------------------
          1         1 00:15:A5:01:02:00
          1         2 00:15:A5:00:00:7D
          1         3 B0:AA:77:2F:F0:CD
          1         4 B0:AA:77:2F:F0:ED
          1         5 B0:AA:77:2F:F0:DD
          1         6 00:15:A5:00:00:9D
          1         7 00:15:A5:00:00:BE
          1         8 00:15:A5:00:00:FE
          1         9 00:15:A5:00:00:8D
          1        10 00:15:A5:00:00:5D
          1        11 00:15:A5:00:00:6D
          1        12 00:15:A5:00:00:CE
          1        13 00:15:A5:00:00:DE
          1        14 00:15:A5:00:01:1E
          1        15 00:15:A5:00:00:1E
          2         1 B0:AA:77:2F:F0:FD
          2         2 B0:AA:77:2F:F0:CE
          2         3 B0:AA:77:2F:F0:EE
```

```
            2         4 00:15:A5:00:01:0E
            2         5 00:15:A5:00:00:0E
            2         6 00:15:A5:00:00:3E
            2         7 00:15:A5:00:00:EE
            2         8 00:15:A5:00:00:4D
            2         9 00:15:A5:00:00:AE
            2        10 00:15:A5:00:00:2E
            2        11 00:15:A5:00:00:5E
            2        12 00:15:A5:00:00:4E
            2        13 00:15:A5:00:00:7E

    Ext Interface:

    Adapter Interface Mac
    ------- --------- ---
          1         1 B0:AA:77:21:19:1E
          1         5 B0:AA:77:21:19:1F
          2         1 B0:AA:77:21:19:42
          2         5 B0:AA:77:21:19:43

FP9300-A#
```

Commandes associées

Commande	Description
scope server	Permet d'accéder au mode serveur.

show server inventory

Pour afficher des informations sur les serveurs installés sur cet appareil, utilisez la commande **show server inventory**.

show server inventory
[*id* | *server_id* | **adapter** | **bios** | **board** | **cpu** | **detail** | **expand** | **memory** | **mgmt** | **storage** | **uuid** *dynamic_uuid*]

Description de la syntaxe

id	(Facultatif) Affiche les informations sur le serveur indiqué. L'ID doit être un nombre compris entre 1 et 255.
server_id	(Facultatif) Affiche l'inventaire matériel d'un serveur particulier, spécifié à l'aide du numéro de châssis/numéro de serveur.
adapter	(Facultatif) Affiche des informations sur le serveur ainsi que sur chaque adaptateur. Les mots clés **bios**, **board**, **cpu**, **detail**, **memory**, **mgmt** et **storage** sont également disponibles avec ce mot clé.
bios	(Facultatif) Affiche des informations sur le serveur ainsi que sur le BIOS. Les mots clés **adapter**, **board**, **cpu**, **detail**, **memory**, **mgmt** et **storage** sont également disponibles avec ce mot clé.
board	(Facultatif) Affiche des informations sur le serveur ainsi que sur la carte mère. Les mots clés **adapter**, **bios**, **cpu**, **detail**, **memory**, **mgmt** et **storage** sont également disponibles avec ce mot clé.
cpu	(Facultatif) Affiche des informations sur le serveur ainsi que sur le CPU. Les mots clés **adapter**, **bios**, **board**, **detail**, **memory**, **mgmt** et **storage** sont également disponibles avec ce mot clé.
detail	(Facultatif) Affiche l'inventaire matériel de chaque serveur.
expand	(Facultatif) Affiche les informations système développées de chaque serveur. Le mot clé **detail** est également disponible.
memory	(Facultatif) Affiche des informations sur le serveur ainsi que sur le module DIMM. Les mots clés **adapter**, **bios**, **board**, **cpu**, **detail**, **mgmt** et **storage** sont également disponibles avec ce mot clé.
mgmt	(Facultatif) Affiche des informations sur la gestion du serveur. Les mots clés **adapter**, **bios**, **board**, **cpu**, **detail**, **memory** et **storage** sont également disponibles avec ce mot clé.
storage	(Facultatif) Affiche les informations sur le serveur, ainsi que sur le disque et le RAID. Les mots clés **adapter**, **bios**, **board**, **cpu**, **detail**, **memory** et **mgmt** sont également disponibles avec ce mot clé.
uuid *dynamic_uuid*	(Facultatif) Affiche les informations sur le micrologiciel et l'état d'un serveur particulier, spécifié avec son identifiant unique universel (UUID) dynamique; saisi sous la forme `NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN`.

Modes de commande Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation Par défaut, cette commande répertorie l'inventaire matériel de chaque serveur.

Exemple

Cet exemple montre comment afficher les informations de base sur l'inventaire matériel :

```
FP9300-A# show server inventory
Server  Equipped PID Equipped VID Equipped Serial (SN) Slot S
tatus      Ackd Memory (MB) Ackd Cores
------- ------------ ------------ -------------------- ------
---------- ---------------- ----------
1/1     FPR9K-SM-24  V01          FLM1949C6J5          Equipp
ed                   262144         24
1/2     FPR9K-SM-24  V01          FLM1949C6J1          Equipp
ed                   262144         24
1/3                                                     Empty

FP9300-A#
```

Commandes associées

Commande	Description
show server environment	Affiche des informations sur l'état actuel du serveur.

show server memory

Pour afficher des informations sur les modules de mémoire DIMM (Dual In-line Memory Module) installés dans cet appareil, utilisez la commande **show server memory**.

show server memory [*server_id* | **detail** | **uuid** *dynamic_uuid*]

Description de la syntaxe

server_id	(Facultatif) Affiche les informations sur la mémoire d'un serveur spécifique, identifié par son numéro de châssis/numéro de serveur (l'ID de rack n'est pas une option valide).
detail	(Facultatif) Affiche les informations détaillées sur la mémoire de chaque serveur.
uuid *dynamic_uuid*	(Facultatif) Affiche les informations sur la mémoire d'un serveur particulier, spécifié par son identifiant unique universel (UUID) dynamique; saisi sous la forme `NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN`.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande répertorie les informations sur la mémoire de chaque serveur.

Exemple

Cet exemple montre comment afficher les informations détaillées sur la mémoire :

```
FP9300-A# show server memory detail
Server 1/1:
    Array 1:
        CPU ID: 1
        Current Capacity (MB): 262144
        Error Correction: Undisc
        Max Capacity (MB): 1572864
        Max Devices: 24
        Populated: 16

        DIMMS:

        ID 1:
            Location: A1
            Presence: Equipped
            Overall Status: Operable
            Visibility: Yes
            Vendor: 0xAD00
            Vendor Part Number: HMA42GR7MFR4N-TF
            Vendor Serial (SN): 244BC0A6
            HW Revision: 0
            Form Factor: DIMM
            Type: Undisc
            Capacity (MB): 16384
```

```
            Clock: 2133
            Latency: 0.500000
            Width: 64

        ID 2:
            Location: A2
            Presence: Equipped
            Overall Status: Operable
            Visibility: Yes
            Vendor: 0xAD00
            Vendor Part Number: HMA42GR7MFR4N-TF
            Vendor Serial (SN): 245C4A07
            HW Revision: 0
            Form Factor: DIMM
            Type: Undisc
            Capacity (MB): 16384
            Clock: 2133
            Latency: 0.500000
            Width: 64

        ID 3:
            Location: A3
            Presence: Missing
            Overall Status: Removed
            Visibility: No
            Vendor:
            Vendor Part Number:
            Vendor Serial (SN):
            HW Revision: 0
            Form Factor: Undisc
            Type: Undisc
            Capacity (MB): Unknown
            Clock: Unknown
            Latency: Unknown
            Width: Unknown

    <--- remaining lines removed for brevity --->

FP9300-A#
```

Commandes associées

Commande	Description
show server identity	Affiche les informations d'identité des serveurs, adaptateurs et interfaces.

show server status

Pour afficher des informations sur l'état d'un serveur, utilisez la commande **show server status**.

show server status [*id* | *server_id* | **detail** | **uuid** *dynamic_uuid*]

Description de la syntaxe

id	(Facultatif) Affiche les informations sur le serveur indiqué. L'ID doit être un nombre compris entre 1 et 255.
server_id	(Facultatif) Affiche les informations sur l'état d'un serveur particulier, spécifié comme numéro de châssis/numéro de serveur.
detail	(Facultatif) Affiche les informations détaillées sur l'état de chaque serveur.
uuid *dynamic_uuid*	(Facultatif) Affiche les informations sur l'état d'un serveur particulier, spécifié avec son identifiant unique universel (UUID) dynamique; saisi sous la forme `NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN`.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, la commande répertorie les informations sur l'état de tous les serveurs.

Exemple

Cet exemple montre comment afficher les informations sur l'état d'un serveur spécifique à l'aide des ID de châssis et de lame :

```
FP9300-A# show server status 1/1
Server    Slot Status      Overall Status      Discovery
------    -----------      --------------      ---------
1/1        Equipped        Ok                  Complete
1/2        Equipped        Ok                  Complete
1/3        Empty

FP9300-A#
```

Commandes associées

Commande	Description
show server inventory	Affiche des informations sur les serveurs installés sur cet appareil.

show server storage

Pour afficher des informations sur le disque et le RAID du serveur, utilisez la commande **show server storage**.

show server storage [*server_id* | **detail** | **uuid** *dynamic_uuid*]

Description de la syntaxe

server_id	(Facultatif) Affiche des informations sur le stockage d'un serveur particulier, spécifié à l'aide du numéro de châssis/numéro de serveur (l'ID de rack n'est pas une option valide).
detail	(Facultatif) Affiche des informations détaillées sur le stockage de chaque serveur.
uuid *dynamic_uuid*	(Facultatif) Affiche les informations sur le stockage d'un serveur particulier, spécifié par son identifiant unique universel (UUID) dynamique; saisi sous la forme `NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN`.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande répertorie les informations de stockage pour chaque serveur.

Exemple

Cet exemple montre comment afficher les informations de base sur le stockage :

```
firepower# show server storage
Server 1/1:
    RAID Controller 1:
        Type: SAS
        Vendor: Cisco Systems Inc
        Model: UCSB-MRAID12G
        Serial: LSV194501YW
        HW Revision: C0
        PCI Addr: 01:00.0
        Raid Support: RAID0, RAID1
        OOB Interface Supported: Yes
        Rebuild Rate: 30
        Controller Status: Optimal

        Local Disk 1:
            Vendor: SAMSUNG
            Model: MZIES800HMHP/003
            Serial: S1N2NYAG800062
            HW Rev: 0
            Operability: Operable
            Presence: Equipped
            Size (MB): 761985
            Drive State: Online
            Power State: Active
            Link Speed: 12 Gbps
```

```
            Device Type: SSD

        Local Disk 2:
            Vendor: SAMSUNG
            Model: MZIES800HMHP/003
            Serial: S1N2NYAG800100
            HW Rev: 0

    <--- remaining lines removed for brevity --->

firepower#
```

Commandes associées

Commande	Description
show server inventory	Affiche des informations sur les serveurs installés sur cet appareil.

show server version

Pour afficher les versions logicielles actuelles du serveur et les informations d'état, utilisez la commande **show server version**.

show server version [*server_id* | **adapter** | **bios** | **boardcontroller** | **cimc** | **detail** | **fxos** | **storage** | **uuid** *dynamic_uuid*]

Description de la syntaxe

server_id	(Facultatif) Affiche les informations sur le micrologiciel et l'état d'un serveur particulier, spécifiées sous la forme numéro de châssis/numéro de serveur ou ID de rack.
adapter	(Facultatif) Affiche la version du micrologiciel et les informations sur l'état de chaque adaptateur. Le mot clé **detail** est également disponible.
bios	(Facultatif) Affiche les versions et l'état du micrologiciel BIOS du serveur. Le mot clé **detail** est également disponible.
boardcontroller	(Facultatif) Affiche les versions et l'état du contrôleur de gestion. Le mot clé **detail** est également disponible.
cimc	(Facultatif) Affiche les versions et l'état de Cisco Integrated Management Controller. Le mot clé **detail** est également disponible.
detail	(Facultatif) Affiche des informations détaillées sur le micrologiciel et l'état sous forme de liste.
fxos	(Facultatif) Affiche des informations sur la version et l'état des systèmes d'exploitation des logements de sécurité (SSP) installés. Le mot clé **detail** est également disponible.
storage	(Facultatif) Répertorie les informations sur la version et l'état des contrôleurs de disque local et RAID. Le mot clé **detail** est également disponible.
uuid *dynamic_uuid*	(Facultatif) Affiche les informations sur le micrologiciel et l'état d'un serveur particulier, spécifié avec son identifiant unique universel (UUID) dynamique; saisi sous la forme `NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN`.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande répertorie les informations logicielles de base pour chaque serveur.

Exemple

Cet exemple montre comment afficher les versions logicielles et les informations d'état des contrôleurs de disque local et RAID sur tous les serveurs :

```
FP9300-A# show server version storage
Server 1/1:
    RAID Controller 1:
        Running-Vers: 24.5.0-0021
        Package-Vers:
        Activate-Status: Ready

Server 1/2:
    RAID Controller 1:
        Running-Vers: 24.5.0-0021
        Package-Vers:
        Activate-Status: Ready

    Local Disk 1:
        Running-Vers: EM14
        Package-Vers:
        Activate-Status: Ready

    Local Disk 2:
        Running-Vers: EM14
        Package-Vers:
        Activate-Status: Ready


    Local Disk 1:
        Running-Vers: EM14
        Package-Vers:
        Activate-Status: Ready

    Local Disk 2:
        Running-Vers: EM14
        Package-Vers:
        Activate-Status: Ready

FP9300-A#
```

Commandes associées

Commande	Description
show server firmware	Affiche les versions et l'état des micrologiciels du serveur.

show service-profile

Pour afficher les informations sur le profil de service, utilisez la commande **show service-profile**.

show service-profile { **assoc** | **circuit** | **connectivity** | **identity** | **inventory** | **path** | **status** }

Description de la syntaxe

assoc	Affiche les informations sur le serveur et l'association pour chaque profil de service. Les mots clés facultatifs suivants sont disponibles : • **detail** : affiche les informations d'association détaillées pour les profils de service. • **org** *name* : affiche les informations d'association des profils de service pour l'organisation spécifiée. • **server** { *id* | *server_id* } : affiche les informations d'association de profils de service pour le serveur spécifié. • **uuid** { **derived** | *dynamic_uuid* } : affiche les informations d'association de profils de service pour l'UUID spécifié.
circuit	Affiche les informations sur le circuit de réseau pour les profils de service. Les mots clés facultatifs suivants sont disponibles : • **detail** : affiche les informations détaillées sur le circuit réseau pour les profils de service. • **name** *name* : affiche les informations sur le circuit réseau pour le profil de service spécifié. • **org** *org_name* : affiche les informations sur le circuit de profil de service pour l'organisation spécifiée. • **server** { *id* | *server_id* } : affiche les informations sur le circuit de profil de service pour le serveur spécifié; *id* est une valeur comprise entre 1 et 255; *server_id* est spécifié sous la forme numéro de châssis/numéro de lame. • **uuid** { **derived** | *dynamic_uuid* } : affiche les informations sur le circuit de profil de service pour l'UUID spécifié, saisies sous la forme NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN.

identity	Affiche les informations sur l'identité de profil de service (ensemble UUID). Ces mots clés facultatifs sont disponibles : • **name** *name* : affiche les informations sur l'identité du profil de service spécifié. • **org** *org_name* : affiche les informations sur l'identité de profil de service pour l'organisation spécifiée. • **server** {*id* | *server_id*} : affiche les informations sur l'identité de profil de service pour le serveur spécifié; *id* est une valeur comprise entre 1 et 255; *server_id* est spécifié sous la forme numéro de châssis/numéro de lame. • **uuid** {**derived** | *dynamic_uuid*} : affiche les informations sur l'identité de profil de service pour l'UUID spécifié, saisies sous la forme NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN.

inventory	Répertorie l'inventaire actuel du profil de service, avec les informations sur le type, le serveur attribué et l'état de l'association. Les mots clés facultatifs suivants sont disponibles : • **adapter** : affiche les informations sur les adaptateurs associés aux profils de service. • **bios** : affiche les informations sur le serveur et le BIOS associés aux profils de service. • **board** : affiche les informations sur le serveur et la carte mère associés aux profils de service. • **cpu** : affiche les informations sur les serveurs et les CPU associés aux profils de service. • **detail** : affiche les informations d'inventaire détaillées pour les profils de service. • **expand** : affiche les informations d'inventaire développées pour les profils de service. • **memory** : affiche les informations sur le serveur et le module DIMM associés aux profils de service. • **mgmt** : affiche les informations sur la configuration du serveur associée aux profils de service. • **name** *name* : affiche les informations d'inventaire pour le profil de service spécifié. • **org** *org_name* : affiche les informations sur l'inventaire du profil de service pour l'organisation spécifiée. • **server** {*id* | *server_id*} : affiche les informations sur l'inventaire du profil de service pour le serveur spécifié; *id* est une valeur comprise entre 1 et 255; *server_id* est spécifié sous la forme numéro de châssis/numéro de lame. • **storage** : affiche les informations sur le serveur, le disque local et le RAID associés aux profils de service. • **uuid** {**derived** | *dynamic_uuid*} : affiche les informations d'inventaire du profil de service pour l'UUID spécifié, saisies sous la forme `NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN`.

path	Affiche les informations sur le chemin réseau du profil de service, y compris le type de connexion et les informations sur le port. Les mots clés facultatifs suivants sont disponibles : • **detail** : affiche les informations détaillées sur le chemin d'accès réseau pour les profils de service. • **name** *name* : affiche les informations sur le chemin pour le profil de service spécifié. • **org** *org_name* : affiche les informations sur le chemin réseau pour l'organisation spécifiée. • **server** {*id* | *server_id*} : affiche les informations sur le chemin réseau du profil de service pour le serveur spécifié; *id* est une valeur comprise entre 1 et 255; *server_id* est spécifié sous la forme numéro de châssis/numéro de lame. • **uuid** {**derived** | *dynamic_uuid*} : affiche les informations sur le chemin réseau pour le profil de service spécifié par l'UUID donné, saisies sous la forme `NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN`.
status	Affiche l'état du profil de service, avec l'état opérationnel, le serveur attribué et les informations sur l'état de l'association. Les mots clés facultatifs suivants sont disponibles : • **detail** : affiche les informations détaillées sur l'état pour les profils de service. • **expand** : affiche les informations développées sur l'état pour les profils de service. • **name** *name* : affiche les informations sur l'état pour le profil de service spécifié. • **org** *org_name* : affiche les informations sur l'état du profil de service pour l'organisation spécifiée. • **power** : affiche les informations sur l'alimentation et l'état du serveur pour les profils de service. • **server** {*id* | *server_id*} : affiche les informations sur l'état du profil de service pour le serveur spécifié; *id* est une valeur comprise entre 1 et 255; *server_id* est spécifié sous la forme numéro de châssis/numéro de lame. • **thermal** : affiche l'état, la température et les informations thermiques du serveur pour les profils de service. • **uuid** {**derived** | *dynamic_uuid*} : affiche les informations sur l'état pour le profil de service spécifié par l'UUID donné, saisies sous la forme `NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN`. • **voltage** : affiche les informations sur l'état, l'alimentation et la tension du serveur pour les profils de service.

Modes de commande Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation Par défaut, cette commande répertorie les informations pour chaque profil de service.

Exemples

Cet exemple montre comment afficher les informations d'inventaire pour un profil de service spécifique :

```
FP9300-A# show service-profile inventory name ssp-sprof-1

Service Profile Name Type              Server  Assignment Association
-------------------- ----------------- ------- ---------- -----------
ssp-sprof-1          Instance          1/1     Assigned   Associated

FP9300-A#
```

Cet exemple montre comment afficher les informations sur l'état de l'alimentation pour les profils de service :

```
FP9300-A# show service-profile status power
Service Profile Name: ssp-sprof-1
Type: Instance
Server: 1/1
Description: ssp service profile
Assignment: Assigned
Association: Associated
Power State: On
Op State: Ok
Oper Qualifier: N/A
Conf State: Applied
Config Qual (Deprecated): N/A
Server Config Issues: N/A
Network Config Issues: N/A
Storage Config Issues: N/A
vNIC Config Issues: N/A
iSCSI Config Issues: N/A
Current Task:
    Server 1/1:
        Overall Status: Ok
        Operability: Operable
        Oper Power: On

        Motherboard:
            Threshold Status: OK
            Overall Status: N/A
            Operability: N/A
            Oper Power: On
            Power State: Ok
            Thermal Status: OK
            Voltage Status: OK
            CMOS Battery Voltage Status: Ok
            Mother Board Power Usage Status: Ok

            Motherboard Temperature Statistics:
                Motherboard Front Temperature (C): 42.000000
```

```
                Motherboard Rear Temperature (C): 57.000000

    <--- remaining lines removed for brevity --->

FP9300-A#
```

Commandes associées

Commande	Description
scope service-profile	Permet d'accéder au mode profil de service.

show session expand detail

Pour afficher les détails de la session de surveillance du trafic, utilisez la commande **show session expand detail**.

show session expand detail

Description de la syntaxe

Show session expand detail	Afficher les détails de la session de surveillance du trafic, comme le nom de la session de capture de paquets, l'utilisation de la mémoire de session, la longueur de l'instantané de la session Pcap, l'état de réussite/échec de la configuration, la raison de l'échec, etc.

Modes de commande

scope packet-capture

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande se trouve dans scope packet-capture.

Exemples

Cet exemple montre comment afficher les détails de la session de surveillance du trafic :

```
Firepower# scope packet-capture
Firepower /packet-capture # enter session test
Firepower /packet-capture/session* # create phy-port Ethernet3/1
Firepower /packet-capture/session/phy-port* # commit-buffer
Firepower /packet-capture/session/phy-port # exit
Firepower /packet-capture/session # exit
Firepower /packet-capture #
Firepower /packet-capture # show session expand detail

Traffic Monitoring Session:
    Packet Capture Session Name: test
    Session: 1
    Admin State: Enabled
    Oper State: Up
    Oper State Reason: Active
    Config Success: Yes
    Config Fail Reason:
    Append Flag: Overwrite
    Session Mem Usage: 512  MB
    Session Pcap Snap Len: 1518  Bytes
    Error Code: 0
    Drop Count: 0
Firepower /packet-capture #
```

show shell-session-limits

Pour afficher la liste des sessions shell disponibles sur le système, utilisez la commande **show shell-session-limits**.

show shell-session-limits [**detail**]

Description de la syntaxe

detail	Affiche des informations détaillées sur les limites des sessions shell.

Modes de commande

scope system/scope services

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope system, scope services.

Exemples

Cet exemple montre comment afficher des informations sur les limites de session du shell système :

```
Firepower /fabric-interconnect # scope system
Firepower /system #scope services
Firepower /system/services # show shell-session-limits
Shell Sessions:
    Maximum logins for single user Maximum Sessions
    ------------------------------ ----------------
    32                             32
```

Exemple

Cet exemple montre comment afficher des informations détaillées sur toutes les sessions shell :

```
Firepower /system/services # show shell-session-limits detail
Shell Sessions:
    Maximum logins for single user: 32
    Maximum Sessions: 32
```

show (slot)

Pour afficher les informations SSP actuelles, utilisez la commande **show** en mode logement.

show [**app-instance** | **detail** | **event** | **expand** | **fault** | **fsm** | **heartbeat** | **heartbeat-config** | **monitor**]

Description de la syntaxe

app-instance	(Facultatif) Affiche les informations sur l'instance d'application du module. Les options suivantes sont également disponibles : • *app-name* : affiche les informations sur l'instance spécifiée uniquement. • **detail** : affiche les informations détaillées sur l'instance d'application. Le mot clé **expand** est disponible avec cette option. • **expand** : affiche les informations développées sur l'instance d'application. Le mot clé **detail** est disponible avec cette option. • **fsm** : affiche les informations sur la machine à états finis (Finite State Machine ou FSM) pour l'instance d'application.
detail	(Facultatif) Affiche les informations détaillées sur l'instance d'application du module. Le mot clé **expand** est disponible avec cette option.
event	(Facultatif) Affiche les informations sur la gestion des événements pour l'application. Les mots clés **detail** et **expand** sont disponibles avec cette option.
expand	(Facultatif) Affiche les informations développées pour l'instance d'application du module. Le mot clé **detail** est disponible avec cette option.
fault	(Facultatif) Affiche les informations sur les défaillances qui se sont produites sur le SSP. Les options suivantes sont également disponibles avec ce mot clé : • *fault_ID* : affiche les informations pour la défaillance spécifiée. • **cause** : affiche les informations pour le type de cause spécifié uniquement. • **detail** : affiche les informations détaillées sur la défaillance. • **severity** : affiche les informations pour le niveau de gravité spécifié uniquement. • **suppressed** : répertorie les défaillances supprimées. Les mots clés **cause**, **detail** et **severity** sont disponibles avec cette option.
fsm task	(Facultatif) Affiche les informations sur les tâches FSM pour le SSP. Le mot clé **detail** est disponible avec cette option.
heartbeat	(Facultatif) Affiche les informations sur la dernière pulsation reçue. Les mots clés **detail** et **expand** sont disponibles avec cette option.
heartbeat-config	(Facultatif) Affiche des informations sur la configuration des pulsations actuelle pour le SSP. Les mots clés **detail** et **expand** sont disponibles avec cette option.

monitor	(Facultatif) Affiche les informations de surveillance pour le SSP. Les mots clés **detail** et **expand** sont disponibles avec cette option.

Modes de commande

scope ssa/scope slot

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande affiche les informations générales sur la configuration du module.

Exemple

Cet exemple montre comment afficher les informations générales sur les logements :

```
firepower# scope ssa
firepower /ssa # scope slot 2
firepower /ssa/slot # show
Slot:
    Slot ID    Log Level Admin State  Oper State
    ---------- --------- ------------ ----------
    2          Info      Ok           Online
firepower /ssa/slot #
```

Commandes associées

Commande	Description
scope slot	Permet d'accéder au mode configuration du module pour un logement spécifique.

show slot

Pour afficher la liste des logements, comme l'état administratif et l'état de fonctionnement disponibles sur le système, utilisez la commande **show slot**.

show [**detail** | **expand**]

Description de la syntaxe

detail	Afficher les informations détaillées sur les logements.
expand	(Facultatif) Affiche les informations développées sur les logements.

Modes de commande

scope ssa

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** en mode scope ssa.

Exemple

Cet exemple montre comment afficher les informations sur tous les logements du système :

```
Firepower / fabric-interconnect # scope ssa
Firepower /ssa # show slot

Slot ID    Log Level Admin State  Oper State
    ---------- --------- ------------ ----------
    1          Info      Ok           Online

This example shows detailed information for all available slots.

Firepower /ssa # show slot detail
    Slot ID: 1
    Log Level: Info
    Admin State: Ok
    Oper State: Online
    Disk Format State: Ok
    Disk Format Status: 100%
    Clear Log Data: Available
    Error Msg:
#
```

Exemple

```
Firepower /ssa # show slot detail
  Slot:
    Slot ID: 1
    Log Level: Info
    Admin State: Ok
    Oper State: Online
    Disk Format State: Ok
    Disk Format Status: 100%
    Clear Log Data: Available
```

```
    Error Msg:

    Slot ID: 2
    Log Level: Info
    Admin State: Ok
    Oper State: Online
    Disk Format State: Ok
    Disk Format Status: 100%
    Clear Log Data: Available
    Error Msg:

    Slot ID: 3
    Log Level: Info
    Admin State: Ok
    Oper State: Not Available
    Disk Format State: Ok
    Disk Format Status:
    Clear Log Data: Available
    Error Msg:
```

Exemple

Cet exemple montre comment afficher les informations détaillées sur tous les logements disponibles.

```
Firepower /ssa # show slot detail expand
Slot:
    Slot ID: 1
    Log Level: Info
    Admin State: Ok
    Oper State: Online
    Disk Format State: Ok
    Disk Format Status: 100%
    Clear Log Data: Available
    Error Msg:

    Heartbeat:
        Last Received Time: 2022-12-16T09:59:35.056
        Heartbeat Interval: 5
        Max Number of Missed heartbeats Permitted: 3

    Monitor:
        OS Version: 82.14(2.4)
        CPU Total Load 1 min Avg: 0.190000
        CPU Total Load 5 min Avg: 0.190000
        CPU Total Load 15 min Avg: 0.190000
        Memory Total (MB): 257689
        Memory Free (MB): 231380
        Memory Used (MB): 25328
        CPU Cores Total: 48
        CPU Cores Available: 46
        Memory App Total (MB): 226969
        Memory App Available (MB): 226969
        Data Disk Total (MB): 699651
        Data Disk Available (MB): 699651
        Secondary Disk Total (MB): 0
        Secondary Disk Available (MB): 0
        Disk File System Count: 5
        Blade Uptime: up 1 day,  2:36
        Last Updated Timestamp: 2022-12-16T09:59:10.374

        Disk File System:
            File System: /dev/sda1
```

```
            Mount Point: /mnt/boot
            Disk Total (MB): 7614
            Disk Free (MB): 7453
            Disk Used (MB): 161

            File System: /dev/sda2
            Mount Point: /opt/cisco/config
            Disk Total (MB): 1846
            Disk Free (MB): 1744
            Disk Used (MB): 7

            File System: /dev/sda3
            Mount Point: /opt/cisco/platform/logs
            Disk Total (MB): 4629
            Disk Free (MB): 4283
            Disk Used (MB): 107

            File System: /dev/sda5
            Mount Point: /var/data/cores
            Disk Total (MB): 46679
            Disk Free (MB): 44243
            Disk Used (MB): 52

            File System: /dev/sda6
            Mount Point: /opt/cisco/csp
            Disk Total (MB): 699651
            Disk Free (MB): 664106
            Disk Used (MB): 35545

Slot ID: 2
Log Level: Info
Admin State: Ok
Oper State: Online
Disk Format State: Ok
Disk Format Status: 100%
Clear Log Data: Available
Error Msg:

Heartbeat:
    Last Received Time: 2022-12-16T09:59:31.983
    Heartbeat Interval: 5
    Max Number of Missed heartbeats Permitted: 3

Monitor:
    OS Version: 82.14(2.4)
    CPU Total Load 1 min Avg: 0.200000
    CPU Total Load 5 min Avg: 0.200000
    CPU Total Load 15 min Avg: 0.200000
    Memory Total (MB): 257689
    Memory Free (MB): 231381
    Memory Used (MB): 25328
    CPU Cores Total: 48
    CPU Cores Available: 46
    Memory App Total (MB): 226969
    Memory App Available (MB): 226969
    Data Disk Total (MB): 509009
    Data Disk Available (MB): 509009
    Secondary Disk Total (MB): 0
    Secondary Disk Available (MB): 0
    Disk File System Count: 5
    Blade Uptime: up 1 day,  2:36
    Last Updated Timestamp: 2022-12-16T09:59:16.897

    Disk File System:
```

```
            File System: /dev/sda1
            Mount Point: /mnt/boot
            Disk Total (MB): 7614
            Disk Free (MB): 7453
            Disk Used (MB): 161

            File System: /dev/sda2
            Mount Point: /opt/cisco/config
            Disk Total (MB): 1846
            Disk Free (MB): 1744
            Disk Used (MB): 7

            File System: /dev/sda3
            Mount Point: /opt/cisco/platform/logs
            Disk Total (MB): 4629
            Disk Free (MB): 4289
            Disk Used (MB): 101

            File System: /dev/sda5
            Mount Point: /var/data/cores
            Disk Total (MB): 46679
            Disk Free (MB): 44243
            Disk Used (MB): 52

            File System: /dev/sda6
            Mount Point: /opt/cisco/csp
            Disk Total (MB): 509009
            Disk Free (MB): 473654
            Disk Used (MB): 35356

    Slot ID: 3
    Log Level: Info
    Admin State: Ok
    Oper State: Not Available
    Disk Format State: Ok
    Disk Format Status:
    Clear Log Data: Available
    Error Msg:

    Heartbeat:
        Last Received Time: 1970-01-01T00:00:00.000
        Heartbeat Interval: 3
        Max Number of Missed heartbeats Permitted: 5

    Monitor:
        OS Version:
        CPU Total Load 1 min Avg: 0.000000
        CPU Total Load 5 min Avg: 0.000000
        CPU Total Load 15 min Avg: 0.000000
        Memory Total (MB): 0
        Memory Free (MB): 0
        Memory Used (MB): 0
        CPU Cores Total: 0
        CPU Cores Available: 0
        Memory App Total (MB): 0
        Memory App Available (MB): 0
        Data Disk Total (MB): 0
        Data Disk Available (MB): 0
        Secondary Disk Total (MB): 0
        Secondary Disk Available (MB): 0
        Disk File System Count: 0
        Blade Uptime:
        Last Updated Timestamp: 1970-01-01T00:00:00.000
```

show snmp (connect fxos)

Pour afficher des informations détaillées sur la configuration actuelle du protocole SNMP (Simple Network Management Protocol), utilisez la commande **show snmp** lorsque vous êtes connecté au shell de commande FXOS.

show snmp [**community** | **context** | **engineID** | **group** | **host** | **internal** | **mib** | **sessions** | **source-interface** | **trap** | **user**]

Description de la syntaxe

community	(Facultatif) Afficher l'identifiant de communauté SNMP actuel et les groupes auxquels l'accès est attribué.
context	(Facultatif) Répertorier les entrées de mappage de contexte SNMP.
engineID	(Facultatif) Afficher l'ID du moteur SNMP local.
group	(Facultatif) Répertorer les rôles SNMP et leurs autorisations d'accès.
host	(Facultatif) Afficher les destinations SNMP actuellement définies.
internal	(Facultatif) Afficher diverses informations internes sur SNMP. Utilisez le mot clé **?** pour afficher les options supplémentaires.
mib	(Facultatif) Afficher le cache MIB SNMP ou les tables d'interface Utilisez le mot clé **?** pour afficher les options supplémentaires.
sessions	(Facultatif) Afficher les sessions SNMP actuelles.
source-interface	(Facultatif) Afficher l'interface source du protocole SNMP pour les deux types de notifications.
trap	(Facultatif) Répertorier tous les types de déroutements SNMP activés.
user	(Facultatif) Répertorier tous les utilisateurs SNMPv3 actuellement définis et leurs paramètres. Utilisez l'option *name* pour afficher les informations d'un utilisateur spécifique.

Modes de commande

connect fxos/

Historique des commandes

Version	Modification
1.1.1	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande affiche les informations de configuration SNMP actuelles, notamment l'identifiant de communauté, le contact système et l'emplacement du système, ainsi que la liste des types de paquets d'entrée et de sortie SNMP.

Exemple

L'exemple suivant montre comment vous connecter au shell FXOS et utiliser la commande **show snmp** pour afficher les informations SNMP actuelles :

```
firepower # connect fxos
firepower(fxos) # show snmp
Community            Group / Access      context    acl_filter
---------            --------------      -------    ----------
SNMPcommunity         network-operator
sys contact: R_Admin
sys location:

0 SNMP packets input
        0 Bad SNMP versions
        0 Unknown community name
        0 Illegal operation for community name supplied
        0 Encoding errors
        0 Number of requested variables
        0 Number of altered variables
        0 Get-request PDUs
        0 Get-next PDUs
        0 Set-request PDUs
398 SNMP packets output
        0 Too big errors
        0 No such name errors
        0 Bad values errors
        0 General errors
        0 In No such name PDU
        0 In Bad vlaue PDU
        0 In Read only PDU
        0 In General errors
        0 In Get Responses
        0 Unknown Context name
        398 Out Traps PDU
        0 Out Get Requests
        0 Out Get Next Requests
        0 Out Set Requests
        0 Out Get Responses
        0 Silent Drops



_____
                  SNMP USERS
_____

User                          Auth  Priv(enforce) Groups
____                          ____  _____________ ______
test1                         sha   no            network-operator

snmp-user1                    sha   no            network-operator

snmp-user2                    sha   no            network-operator

_____
 NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
_____

User                          Auth  Priv
____                          ____  ____
```

```
SNMP Tcp Authentication Flag : Enabled.

------------------------------------------------------------------------------------------
Port Monitor : unset
------------------------------------------------------------------------------------------


Policy Name : default
Admin Status: Not Active
Oper Status: Not Active
Port type   : All Ports
------------------------------------------------------------------------------------------
Counter                Threshold  Interval Rising Threshold event Falling Threshold  event
 In Use
-------                ---------  -------- ---------------- ----- ------------------ -----
 ------
Link Loss                Delta      60       5                4     1                  4
   Yes
Sync Loss                Delta      60       5                4     1                  4
   Yes
Invalid Words            Delta      60       5                4     1                  4
   Yes
Invalid CRC's            Delta      60       1                4     0                  4
   Yes
RX Performance           Delta      60       5                4     1                  4
   Yes
LR RX                    Delta      60       200              4     10                 4
   Yes
LR TX                    Delta      60       5                4     1                  4
   Yes
Timeout Discards         Delta      60       5                4     1                  4
   Yes
Credit Loss Reco         Delta      60       200              4     10                 4
   Yes
TX Credit Not Available  Delta      1        1                4     0                  4
   Yes
RX Datarate              Delta      1        10               4     0                  4
   Yes
TX Datarate              Delta      60       80               4     20                 4
   Yes
ASIC Error Pkt from Port Delta      60       80               4     20                 4
   Yes
------------------------------------------------------------------------------------------


SNMP protocol : Enabled


-----------------------------------------------------------------------
Context                          [Protocol instance, VRF, Topology]
                                 [vlan, MST]
-----------------------------------------------------------------------
1                               ,
                                ,
                                ,
                                1,

-----------------------------------------------------------------------
101                             ,
                                ,
                                ,
                                101,
```

```
-----------------------------------------------------------------------
102                             ,
                                ,
                                ,
                                102,

-----------------------------------------------------------------------

    <--- remaining lines removed for brevity --->

firepower(fxos) #
```

Commandes associées

Commande	Description
enable snmp	Active le protocole SNMP.
set snmp	Définit les paramètres de configuration du protocole SNMP.
show snmp (monitoring)	Affiche les informations de base sur la configuration SNMP actuelle.

show snmp (monitoring)

Pour afficher des informations de base sur la configuration actuelle du protocole SNMP (Simple Network Management Protocol), utilisez la commande **show snmp**.

show snmp [**community**]

Description de la syntaxe

community	(Facultatif) Affiche le nom de communauté SNMP actuel. **Remarque** Ce mot clé est obsolète, car pour des raisons de sécurité, seul un champ vide est affiché.

Modes de commande

scope monitoring/

Historique des commandes

Version	Modification
1.1.1	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande affiche les informations de configuration SNMP actuelles, notamment l'état d'administration, le contact système et l'emplacement du système.

Exemple

L'exemple suivant montre comment cibler le mode surveillance et utiliser la commande **show snmp** pour afficher la configuration SNMP actuelle :

```
firepower# scope monitoring
firepower /monitoring # show snmp
Name: snmp
    Admin State: Enabled
    Port: 161
    Is Community Set: Yes
    Sys Contact: R_Admin
    Sys Location:
firepower /monitoring #
```

Commandes associées

Commande	Description
enable snmp	Active le protocole SNMP.
set snmp	Définit les paramètres de configuration du protocole SNMP.
show snmp (connect fxos)	Affiche les informations détaillées sur la configuration SNMP actuelle.

show snmp-trap

Pour afficher des informations sur les déroutements SNMP actuellement définis, saisissez la commande **show snmp-trap**.

show snmp-trap [**detail** | *trap_ID*]

Description de la syntaxe

detail	(Facultatif) Utilisez ce mot clé pour afficher des informations détaillées sur les déroutements SNMP.
trap_ID	(Facultatif) Spécifiez le nom de domaine ou l'adresse IP d'une destination de déroutement SNMP donnée pour afficher les informations sur ce déroutement. (Cette option est uniquement disponible en mode scope monitoring/.) Le mot clé **detail** est disponible avec cette option.

Modes de commande

scope monitoring/

scope monitoring/snmp-trap/

Historique des commandes

Version	Modification
1.1.1	Commande ajoutée.

Instructions d'utilisation

En mode scope monitoring/, cette commande affiche par défaut la liste actuelle des déroutements SNMP.

En mode scope monitoring/snmp-trap/, cette commande affiche des informations sur le déroutement actuel.

Exemple

L'exemple suivant vous montre comment accéder au mode surveillance et utiliser la commande **show snmp-trap** pour afficher la liste des déroutements SNMP actuels :

```
firepower# scope monitoring
firepower /monitoring # show snmp-trap

SNMP Trap:
    SNMP Trap                Port     Community  Version V3 Privilege Notification Type
    ------------------------ -------- ---------- ------- ------------ -----------------
    trap1_informs            162      ****       V2c     Noauth       Informs
    192.168.10.100           162      ****       V3      Noauth       Traps
firepower /monitoring #
```

Commandes associées

Commande	Description
create snmp-trap	Crée un déroutement SNMP.
enable snmp	Active le protocole SNMP.
set (snmp-trap)	Spécifie les paramètres d'un déroutement SNMP existant.

Commande	Description
show snmp (monitoring)	Affiche les informations de base sur la configuration SNMP actuelle.
show snmp (connect fxos)	Affiche les informations détaillées sur la configuration SNMP actuelle.

show snmp-user

Pour afficher des informations sur les utilisateurs SNMPv3 actuellement définis, saisissez la commande **show snmp**.

show snmp-user [**detail** | **fault** | *nom_utilisateur*]

Description de la syntaxe

detail	(Facultatif) Utilisez ce mot clé pour afficher des informations détaillées sur le(s) utilisateur(s) SNMPv3.
fault	(Facultatif) Utilisez ce mot clé pour afficher des informations sur les défaillances pour cet utilisateur. Les mots clés facultatifs suivants sont disponibles avec cette option : • **cause** : utilisez ce mot clé pour filtrer les informations de défaillance par cause. • **detail** : utilisez ce mot clé pour afficher les informations détaillées de défaillance. • **severity** : utilisez ce mot clé pour filtrer les informations de défaillance par gravité. • **suppressed** : utilisez ce mot clé pour afficher uniquement les défaillances supprimées. • *fall_ID* : vous pouvez spécifier une défaillance particulière en saisissant son numéro d'ID; les valeurs valides sont comprises entre 0 et 18446744073709551615. **Remarque** Cette option est disponible uniquement en mode scope monitoring/snmp-user/.
user_name	(Facultatif) Spécifiez le nom d'un utilisateur SNMP donné pour afficher les informations le concernant. (Cette option est uniquement disponible en mode scope monitoring/.) Le mot clé **detail** est disponible avec cette option.

Modes de commande

scope monitoring/

scope monitoring/snmp-user/

Historique des commandes

Version	Modification
1.1.1	Commande ajoutée.

Instructions d'utilisation

En mode scope monitoring/, cette commande affiche par défaut la liste actuelle des utilisateurs SNMPv3 avec le type d'authentification pour chacun.

En mode scope monitoring/snmp-trap/, cette commande affiche des informations sur l'utilisateur SNMPv3 actuel.

Exemple

L'exemple suivant vous montre comment cibler le mode surveillance et utiliser la commande **show snmp-user** pour afficher la liste des utilisateurs SNMPv3 actuels, ainsi que les informations de configuration détaillées sur un utilisateur spécifique :

```
firepower# scope monitoring
firepower /monitoring # show snmp-user

SNMPv3 User:
    Name                    Authentication type
    ----------------------- -------------------
    snmp-user1              Sha
    testuser                Sha
    snmp-user2              Sha
firepower /monitoring # show snmp-user snmp-user1 detail

SNMPv3 User:
    Name: snmp-user1
    Authentication type: Sha
    Password: ****
    Privacy password: ****
    Use AES-128: Yes
firepower /monitoring #
```

Commandes associées

Commande	Description
create snmp-user	Crée un utilisateur SNMPv3.
enable snmp	Active le protocole SNMP.
set (snmp-user)	Spécifie les paramètres d'un utilisateur SNMPv3 existant.
show snmp (monitoring)	Affiche les informations de base sur la configuration SNMP actuelle.
show snmp (connect fxos)	Affiche les informations détaillées sur la configuration SNMP actuelle.

show ssh-server

Pour afficher des informations sur le serveur SSH, utilisez la commande **show ssh-server**.

show server [**host-key**]

Description de la syntaxe

host-key	(Facultatif) Affiche la taille de la clé d'hôte du serveur SSH et si la clé a été supprimée.

Modes de commande

Mode de service

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour afficher les informations de connexion et d'authentification SSH.

Exemple

Cet exemple montre comment afficher les informations sur le serveur SSH :

```
FP9300-A # scope system
FP9300-A /system # scope services
FP9300-A /system/services # show ssh-server
Name: ssh
    Admin State: Enabled
    Port: 22
    Kex algorithm: diffie-hellman-group14-sha1
    Mac algorithm: hmac-sha1,hmac-sha2-256,hmac-sha2-512
    Encrypt algorithm:
aes128-ctr,aes192-ctr,aes256-ctr,3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc
    Authentication algorithm: Rsa
    Host Key Size: 2048
    Rekey Limit Volume: None Time: None
FP9300-A /system/services #
```

Commande	Description
create ssh-server	Crée une clé d'hôte de serveur SSH.
delete ssh-server	Supprime la clé d'hôte existante du serveur SSH.
set ssh-server	Définit la taille de la clé d'hôte SSH.

show stats

Pour afficher les statistiques IPSec, utilisez la commande **show stats**.

show stats [**detail** | **listauthor** | **listcert** | **listconn** | **listsa** | **status**]

Description de la syntaxe

detail	(Facultatif) Affiche les statistiques IPSec supplémentaires.
listauthor	(Facultatif) Affiche tous les points de confiance disponibles. Le mot clé **detail** est disponible avec cette option.
listcert	(Facultatif) Affiche toutes les certifications disponibles. Le mot clé **detail** est disponible avec cette option.
listconn	(Facultatif) Affiche l'état opérationnel de toutes les connexions. Le mot clé **detail** est disponible avec cette option.
listsa	(Facultatif) Affiche l'état opérationnel de toutes les associations de sécurité (SA) IPSec. Le mot clé **detail** est disponible avec cette option.
status	(Facultatif) Affiche l'état général d'IPsec. Le mot clé **detail** est disponible avec cette option.

Modes de commande

Mode IPSec

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour afficher les statistiques IPSec.

Exemple

Cet exemple montre comment afficher les informations de connexion IPSec pour une connexion spécifiée :

```
FP9300-A # scope security
FP9300-A /security # scope ipsec
FP9300-A /security/ipsec # show stats

Ipsec Stats:
    Stats Type: Status
    Stats Data: Status of IKE charon daemon (strongSwan 5.3.5, Linux 3.14.39ltsi, i686):
  uptime: 11 days, since Jun 29 17:36:39 2018
  malloc: sbrk 2289664, mmap 0, used 199808, free 2089856
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 0
  loaded plugins: charon aes des rc2 sha1 sha2 md5 random nonce x509 revocation constraints
 pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl fips-prf xcbc cmac hmac files
 attr kernel-netlink resolve socket-default stroke vici updown xauth-generic
Listening IP addresses:
  10.122.150.220
  192.15.1.250
  192.15.1.251
```

```
  192.3.0.254
  192.5.254.1
  192.5.1.254
  192.7.254.1
  192.9.0.1
  192.128.254.1
  203.0.113.126
  192.16.254.1
Connections:
Security Associations (0 up, 0 connecting):
  none

    Time Stamp: 2018-07-11T17:20:17.542
FP9300-A /security/ipsec #
```

Commandes associées

Commande	Description
show connection	Affiche les informations de configuration pour les connexions IPSec actuelles.
show ipsec-log	Affiche les journaux de connexion IPSec.

show storage

Pour afficher toutes les partitions et leur utilisation actuelle de l'espace disque sur un disque, utilisez la commande **show storage**.

show storage

Modes de commande

scope fabric-interconnect

Historique des commandes

Version	Modification
2.11.1	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour afficher l'utilisation du disque.

Exemple

L'exemple suivant affiche le stockage sur un lecteur flash local d'interconnexion de structure :

```
firepower /fabric-interconnect # show storage
Storage on local flash drive of fabric interconnect:
    Partition        Size (MBytes)    Used Percentage
    ---------------- ---------------- ---------------
    bootflash        106540           43
    callhome         128              Empty
    dev-shm          512              59
    isan             4000             36
    mnt-cfg-0        73               3
    mnt-cfg-1        73               3
    mnt-plog         47               3
    mnt-pss          73               41
```

show subinterface

Pour afficher des informations sur la sous-interface, utilisez la commande **show subinterface**.

show subinterface [**detail**]

Description de la syntaxe

detail	Affiche les informations sur chaque sous-interface dans un format non tabulaire.

Modes de commande

scope eth-uplink/scope fabric a/scope interface/

scope eth-uplink/scope fabric a/create port-channel/

Historique des commandes

Version	Modification
2.4(1)	Commande ajoutée.

Instructions d'utilisation

Les sous-interfaces ne sont prises en charge que pour les instances de contenant.

Exemple

Voici un exemple de sortie de la commande **show subinterface**.

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # enter interface ethernet1/8
firepower /eth-uplink/fabric/interface # show subinterface

Sub Interface:
    Sub-If Id  Sub-Interface Name VLAN        Port Type
    ---------- ------------------ ----------- ---------
           100 Ethernet1/5.100    100         Data
```

Voici un exemple de sortie de la commande **show subinterface detail**.

```
firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # enter interface ethernet1/8
firepower /eth-uplink/fabric/interface # show subinterface detail

Sub Interface:
    Sub-If Id: 100
    Sub-Interface Name: Ethernet1/5.100
    VLAN: 100
    Port Type: Data
```

Commandes associées

Commande	Description
create port-channel	Crée un EtherChannel (canal de port).
create subinterface	Ajoute une sous-interface.

Commande	Description
scope interface	Permet d'accéder à l'objet d'interface physique.
set port-type	Définit le type d'interface.

show sup

Pour afficher les informations sur la version du superviseur de châssis, utilisez la commande **show sup version**.

show sup version [**detail**]

Description de la syntaxe

detail	(Facultatif) Affiche les informations détaillées sur la version du superviseur.

Modes de commande

Mode châssis

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande répertorie les informations sur la version du superviseur ROMMON et FPGA.

Exemple

Cet exemple montre comment afficher les informations détaillées sur le micrologiciel du superviseur pour tous les serveurs :

```
FP9300-A /chassis # show sup version detail
SUP FIRMWARE:
    ROMMON:
        Running-Vers: 1.0.11
        Package-Vers: 1.0.11
        Activate-Status: Ready
        Upgrade Status: SUCCESS
    FPGA:
        Running-Vers: 1.05
        Package-Vers: 1.0.11
        Activate-Status: Ready

FP9300-A /chassis #
```

Commandes associées

Commande	Description
show version	Affiche les versions logicielles actuelles et les informations sur l'état de chaque serveur sur le châssis.

show system

Pour afficher les informations sur les systèmes configurés sur cet appareil, utilisez la commande **show system**.

show system [**detail** | **firmware** | **version**]

Description de la syntaxe

detail	(Facultatif) Affiche les informations détaillées sur le système.
firmware	(Facultatif) Affiche les informations sur la version et l'état du micrologiciel du système. Les mots clés facultatifs **detail** et **expand** sont également disponibles.
version	(Facultatif) Affiche les informations sur la version et l'état du système. Les mots clés facultatifs **detail** et **expand** sont également disponibles.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande affiche le nom, le mode et les adresses IP de chaque système configuré.

Exemple

Cet exemple montre comment afficher les informations développées sur la version du système :

```
FP9300-A# show system version expand
FPRM:
    Running-Vers: 4.2(1.62)
    Package-Vers: 2.2(1.63)
    Activate-Status: Ready

Catalog:
    Running-Vers: 4.2(1.62)T
    Package-Vers: 2.2(1.63)
    Activate-Status: Ready

Management Extension:
    Running-Vers: 2.2(1.8)
    Package-Vers: 2.2(1.63)
    Activate-Status: Ready

Fabric Interconnect A:
    Running-Kern-Vers: 5.0(3)N2(4.21.62)
    Running-Sys-Vers: 5.0(3)N2(4.21.62)
    Package-Vers: 2.2(1.63)
    Startup-Kern-Vers: 5.0(3)N2(4.21.62)
    Startup-Sys-Vers: 5.0(3)N2(4.21.62)
    Act-Kern-Status: Ready
    Act-Sys-Status: Ready
    Bootloader-Vers:
```

```
Chassis 1:
    Server 1:
        CIMC:
            Running-Vers: 3.1(20a)
            Package-Vers: 2.2(1.63)
            Update-Status: Ready
            Activate-Status: Ready

        Adapter 1:
            Running-Vers: 4.0(1.57)
            Package-Vers: 2.2(1.63)
            Update-Status: Ready
            Activate-Status: Ready
        Adapter 2:
            Running-Vers: 4.0(1.57)

    <--- remaining lines removed for brevity --->

FP9300-A#
```

Commandes associées

Commande	Description
scope system	Permet d'accéder au mode système.

show system reset-reason

Pour afficher des informations sur la raison de la réinitialisation du système, utilisez la commande **show system reset-reason**.

show system reset-reason

Description de la syntaxe

reset-reason	(Facultatif) Affiche les informations détaillées sur la raison de la réinitialisation.

Modes de commande

connect fxos

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande affiche les informations sur la raison de la réinitialisation.

Exemple

Cet exemple montre comment afficher les informations sur la raison de la réinitialisation d'un module :

```
firepower#
firepower# connect fxos
...
firepower(fxos)# show system reset-reason
----- reset reason for Supervisor-module 1 (from Supervisor in slot 1) ---
1) At 826701 usecs after Sun Jul 11 09:14:12 2021
    Reason: Reset Requested by CLI command reload <=========Manual reboot requested from
CLI.
    Service:
    Version: 5.0(3)N2(4.81)

2) At 865598 usecs after Wed Apr 21 17:10:58 2021
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 5.0(3)N2(4.61)
```

show stats system-stats

Pour afficher les informations sur les statistiques du système, utilisez la commande **show stats system-stats**.

show stats system-stats detail

Description de la syntaxe

detail	(Facultatif) Affiche les statistiques IPSec supplémentaires.

Modes de commande

scope fabric-interconnect a

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope fabric-interconnect a.

Exemple

Cet exemple montre comment afficher les informations sur les statistiques du système :

```
FP9300-A # scope fabric-interconnect a
FP9300-A /fabric-interconnect  # show stats system-stats
 System Stats:
    Time Collected: 2012-07-15T06:55:00.187
    Monitored Object: sys/switch-A
    Suspect: No
    Load: 3.800000
    Mem Available (MB): 11762
    Mem Cached (MB): 2008
    Thresholded: 0

This example shows detailed information of stats history system stats:
QP1 /fabric-interconnect # show stats history system-status
System Stats:
    Time Collected: 2012-07-15T06:54:00.249
    Monitored Object: sys/switch A/sysstats
    Suspect: No
    Load: 3.930000
    Mem Available (MB): 11814
    Mem Cached (MB): 2008
    Thresholder: 0

    Time Collected: 2012-07-15T06:46:30.804
    Monitored Object: sys/switch A/sysstats
    Suspect: No
    Load: 3.480000
    Mem Available (MB): 11814
    Mem Cached (MB): 2009
    Thresholded: 0

    Time Collected: 2012-07-15T06:39:00.173
    Monitored Object: sys/switch-A/sysstats
    Suspect: No
    Load: 3.780000
    Mem Available (MB): 11758
    Mem Cached (MB): 2009
```

Cet exemple montre comment afficher les informations détaillées sur les statistiques du système dans l'historique des statistiques :

```
FP9300-A /fabric-interconnect # show stats history system-status detail

System Stats:
    Time Collected: 2012-07-15T06:54:00.249
    Monitored Object: sys/switch-A/sysstats
    Suspect: No
    Load: 3.930000
    Load Min: 3.380000
    Load Max: 5.300000
    Load Avg: 4.320666
    Mem Available (MB): 11814
    Mem Available Min (MB): 11796
    Mem Available Max (MB): 11815
    Mem Available Avg (MB): 11804
    Mem Cached (MB): 2008
    Mem Cached Min (MB): 2008
    Mem Cached Max (MB): 2010
    Mem Cached Avg (MB): 2008
    Thresholded: 0

    Time Collected: 2012-07-15T06:46:30.804
    Monitored Object: sys/switch-A/sysstats
    Suspect: No
    Load: 3.480000
    Load Min: 3.480000
```

show system uptime (connect fxos)

Pour afficher des informations sur le temps de disponibilité du système pour chaque système configuré, utilisez la commande **show system uptime**.

show system uptime

Description de la syntaxe

system uptime	Affiche des informations sur le temps de disponibilité du système.

Modes de commande

connect fxos

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande affiche le temps de disponibilité pour le système configuré.

Exemple

Cet exemple montre comment afficher des informations sur le temps de disponibilité du système :

```
firepower#
firepower# connect fxos
...
firepower(fxos)# show system uptime
System start time:          Sun Jul 11 09:19:55 2021
System uptime:              89 days, 23 hours, 20 minutes, 21 seconds
Kernel uptime:              89 days, 23 hours, 22 minutes, 59 seconds
Active supervisor uptime:   89 days, 23 hours, 20 minutes, 21 seconds
```

show tech-support

Pour afficher ou enregistrer des informations de dépannage sur le matériel et les logiciels du périphérique, utilisez la commande **show tech-support**.

```
(module)#  show tech-support
```

```
(local-mgmt)#  show tech-support  { chassis  chassis_ID | fprm | module  module_ID [
app-instance  application_name  application_ID | brief | detail ] }
```

Description de la syntaxe

	En mode module, cette commande ne contient aucun argument ou mot clé.
chassis *chassis_ID* [**brief** | **detail**]	Collecte les données de dépannage relatives au châssis; *chassis_ID* correspond toujours à 1. Les options suivantes sont disponibles : • **brief** : utilisez ce mot clé pour répertorier un ensemble condensé d'informations de dépannage sur votre terminal. Vous pouvez utiliser les opérateurs > et >> pour enregistrer ces informations dans un fichier; pour plus de renseignements, consultez Enregistrer la sortie d'une commande « show », à la page 17. • **detail** : utilisez ce mot clé pour enregistrer des informations de dépannage détaillées dans un fichier du répertoire `techsupport` sur le périphérique. Si vous ne saisissez aucun mot clé, la sortie **brief** s'affiche sur l'écran du terminal.
fprm [**brief** | **detail**]	L'option **fprm** est obsolète dans la version 2.8(1) et ne peut plus être utilisée.
module *module_ID* [**app-instance** *application_name application_ID* | **brief** | **detail**]	Collecte des données de dépannage pour le module spécifié par *module_ID*. Les options suivantes sont disponibles : • **app-instance** : dans un environnement à instances multiples, vous pouvez utiliser ce mot clé pour répertorier les informations sur l'instance d'application spécifiée par *application_name* et *application_ID*. • **brief** : utilisez ce mot clé pour répertorier un ensemble condensé d'informations de dépannage sur votre terminal. • **detail** : utilisez ce mot clé pour répertorier des informations de dépannage détaillées sur votre terminal. Vous pouvez utiliser les opérateurs > et >> pour enregistrer ces informations dans un fichier; pour plus de renseignements, consultez Enregistrer la sortie d'une commande « show », à la page 17. Si vous ne saisissez aucun mot clé, la sortie **brief** s'affiche sur l'écran du terminal.

Modes de commande

connect local-mgmt

connect module

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.
2.4(1)	Le mot clé **app-instance** a été ajouté à l'option **module**.
2.8(1)	L'option **fprm** est obsolète dans la version 2.8(1) et ne peut plus être utilisée. Utilisez la commande **show tech-support {chassis}**.

Instructions d'utilisation

Utilisez cette commande pour afficher ou enregistrer un ensemble de messages de journal, d'informations de configuration et de sortie de commande à des fins de transmission à l'assistance technique de Cisco; ces données sont utilisées pour déterminer l'état du matériel et des logiciels de l'appareil.

Utilisez la commande **copy** en mode gestion locale pour transférer un fichier de dépannage vers un autre appareil ou emplacement.

Remarque En mode module, cette commande répertorie simplement les informations de dépannage collectées pour le module spécifié sur votre terminal.

Exemples

Cet exemple montre comment générer un fichier d'informations de dépannage détaillées sur le châssis :

```
firepower # connect local-mgmt
Firepower(local-mgmt)# show tech-support chassis 1 detail

The show tech support file will be located at
/workspace/techsupport/20191105041703_firepower-9300_BC1_all.tar

Initiating tech-support information task on FABRIC A ...

Initiating tech-support information task on Chassis 1 Fabric Extender 1 ...
Initiating tech-support information task on Chassis 1 CIMC 1 ...
Initiating tech-support information task on Adaptor 1 on Chassis/Server 1/1 ...
Initiating tech-support information task on Adaptor 2 on Chassis/Server 1/1 ...
Initiating tech-support information task on Chassis 1 CIMC 2 ...
Initiating tech-support information task on Adaptor 1 on Chassis/Server 1/2 ...
Initiating tech-support information task on Adaptor 2 on Chassis/Server 1/2 ...
Completed initiating tech-support subsystem tasks (Total: 8)
Waiting (Timeout: 900 Elapsed: 30) for completion of subsystem tasks (1/8).
Waiting (Timeout: 900 Elapsed: 50) for completion of subsystem tasks (2/8).
Waiting (Timeout: 900 Elapsed: 70) for completion of subsystem tasks (5/8).
Waiting (Timeout: 900 Elapsed: 90) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 110) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 130) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 150) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 170) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 190) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 210) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 230) for completion of subsystem tasks (7/8).
--More--
```

```
The detailed tech-support information is located at workspace:///techsupport/201--More--
91105041703_firepower-9300_BC1_all.tar
```

Cet exemple montre comment enregistrer un fichier d'informations de dépannage pour le module de sécurité et confirmer son emplacement sur l'appareil :

```
firepower # connect local-mgmt
firepower(local-mgmt)# show tech-support module 1 detail
The show tech support file will be located at
/workspace/techsupport/20191107082242_firepower-9300_BC_CIMC1.tar

Try connecting to Firepower-module 1...
Last login: Wed Oct 23 09:03:56 CDT 2019 from 127.128.254.1 on pts/0
Cisco Firepower Extensible Operating System (FX-OS) Software. TAC support:
http://www.cisco.com/tac Copyright (c) 2009-2016, Cisco Systems, Inc. All rights reserved.
 The copyrights to certain works contained in this software are owned by other third parties
 and used and distributed under license. Certain components of this software are licensed
under the 'GNU General Public License, version 3' provided with ABSOLUTELY NO WARRANTY under
 the terms of 'GNU General Public License, Version 3', available here:
http://www.gnu.org/licenses/gpl.html. See User Manual (''Licensing'') for details. Certain
 components of this software are licensed under the 'GNU General Public License, version
2' provided with ABSOLUTELY NO WARRANTY under the terms of 'GNU General Public License,
version 2', available here: http://www.gnu.org/licenses/old-licenses/gpl-2.0.html. See User
 Manual (''Licensing'') for details. Certain components of this software are licensed under
 the 'GNU LESSER GENERAL PUBLIC LICENSE, version 3' provided with ABSOLUTELY NO WARRANTY
under the terms of 'GNU LESSER GENERAL PUBLIC LICENSE' Version 3, available here:
http://www.gnu.org/licenses/lgpl.html. See User Manual (''Licensing'') for details. Certain
 components of this software are licensed under the 'GNU Lesser General Public License,
version 2.1' provided with ABSOLUTELY NO WARRANTY under the terms of 'GNU Lesser General
Public License, version 2', available here:
http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html. See User Manual (''Licensing'') for
 details. Certain components of this software are licensed under the 'GNU Library General
Public License, version 2' provided with ABSOLUTELY NO WARRANTY under the terms of 'GNU
Library General Public License, version 2', available here:
http://www.gnu.org/licenses/old-licenses/lgpl-2.0.html. See User Manual (''Licensing'') for
 details.


            Cisco Security Services Platform
                  Type ? for list of commands
Firepower-module1>support  send_diag_archive
Creating default Archive...
Archive created in 11 secs.
Starting to transfer Firepower-Module1_11_07_2019_08_22_44.tar of 5109760 bytes.
Transferred Firepower-Module1_11_07_2019_08_22_44.tar successfully to MIO at
/bladelog/blade-1/ in 1 sec(s).
Firepower-module1>support send_allcontainerlogs size 3063
Upload container logs triggered from Supervisor Module, Starting upload ....
No container instances running, skipping container logs

The detailed tech-support information is located at
workspace:/techsupport/Firepower-Module1_11_07_2019_08_22_44.tar
```

L'exécution de **show tech-support module 1|2|3 [detail]** peut expirer si la lame est en mode hors ligne ou dans d'autres états d'erreur. Dans de tels scénarios, suivez les étapes ci-dessous pour collecter les informations d'assistance technique du module (détails) :

1. Connectez-vous à la lame prévue à l'aide de connect module 1|2|3 console|telnet

   ```
   FPR4110# connect module 1 console
   Telnet escape character is '~'.
   Trying 127.5.1.1...
   Connected to 127.5.1.1.
   Escape character is '~'.
   ```

```
CISCO Serial Over LAN:
Close Network Connection to Exit
```

2. Générez le paquet de diagnostic

```
Firepower-module1>support diagnostic

======= Diagnostic =======

 1. Create default diagnostic archive
 2. Manually create diagnostic archive
 3. Exit

Please enter your choice: 1

Creating Default archive

ASA running ...

Done with extracting tech support information from ASA. Log file saved as
asa_tech_support.log

1. Added file: cspCfg_cisco-asa.9.16.1__asa_001_JMX2309L046K6AY356.xml
2. Added file: tech_support_report.txt
3. Added file: ssp-cardmgmt.log
4. Added file: ssp_ntp.log.2
5. Added file: ssp_tz.log
6. Added file: ssp_ntp.log.1
7. Added file: ssp-pm.log
```

3. Copiez le paquet de diagnostic sur Supervisor (MIO)

```
Firepower-module1>support fileupload
Please choose from following:
================================
1. Archive Files
2. View selected files
3. Start upload and Exit
4. View transfer Status
Please enter your choice [x] to Exit:1
-----------files------------
2021-09-29 17:24:36.571927 | 4065280    | Firepower-Module1_09_29_2021_17_23_17.tar
2021-09-29 17:27:34.094890 | 4065280    | Firepower-Module1_09_29_2021_17_26_15.tar
2021-09-29 17:24:38.211954 | 10240      |
Firepower-module1_09_29_2021_17_24_38_container.tar

([s] to select files or [x] to Exit):s

Type the partial name of the file to add, [<] to cancel
> Firepower-Module1_09_29_2021_17_26_15.tar
Firepower-Module1_09_29_2021_17_26_15.tar
Are you sure you want to add these files? (y/n) y
=== Package Contents ===
[Added] Firepower-Module1_09_29_2021_17_26_15.tar
========================

Type the partial name of the file to add, [<] to cancel
> <
Please choose from following:
================================
1. Archive Files
2. View selected files
3. Start upload and Exit
4. View transfer Status
```

```
Please enter your choice [x] to Exit:3
Transfer of Firepower-Module1_09_29_2021_17_26_15.tar started.
Firepower-module1>support fileupload
Please choose from following:
==============================
1. Archive Files
2. View selected files
3. Start upload and Exit
4. View transfer Status
Please enter your choice [x] to Exit:4
File Transfer Status:
-------------------------------------------
Firepower-Module1_09_29_2021_17_26_15.tar       Status: Completed.
```

4. Quittez la console du module avec ~ et quittez, localisez le fichier dans MIO

```
Firepower-module1>
telnet> quit
Connection closed.
FPR4110# connect local-mgmt
FPR4110(local-mgmt)# dir workspace:/bladelog/blade-1/
<>
1 4065280 Sep 29 17:30:04 2021 Firepower-Module1_09_29_2021_17_26_15.tar <---
<>
```

Commandes associées

Commande	Description
copy	En mode gestion locale, crée une copie du fichier spécifié.
dir	En mode gestion locale, répertorie le contenu du répertoire actuel.

show timezone

Pour afficher le fuseau horaire actuellement configuré, utilisez la commande **show timezone**.

show timezone

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment afficher le fuseau horaire actuel :

```
FP9300-A# show timezone
Timezone: America/Chicago
FP9300-A#
```

Commandes associées

Commande	Description
set timezone	Définit le fuseau horaire de l'appareil.

show trustpoint

Pour afficher la liste (ou chaîne) des certificats de tous les points de confiance ou d'un point de confiance spécifique, utilisez la commande **show trustpoint**.

show trustpoint [**detail** | *trustpoint_name*]

Description de la syntaxe

detail	Affiche les informations détaillées sur les certificats.
trustpoint_name	Affiche les informations sur le certificat d'un point de confiance spécifié. Ce nom peut comporter entre 1 et 32 caractères alphanumériques. Vous ne pouvez pas utiliser des espaces ni de caractères spéciaux autres que - (tiret), _ (trait de soulignement), : (deux-points) et . (point), et vous ne pouvez pas modifier ce nom après l'enregistrement de l'objet.

Modes de commande

Mode sécurité

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour afficher les informations sur les certificats des points de confiance.

Vous pouvez également utiliser la commande **show** en mode point de confiance (/security/trustpoint) pour afficher les informations sur le certificat du point de confiance connecté.

Exemple

Cet exemple montre comment afficher les informations sur le certificat d'un point de confiance spécifique :

```
FP9300-A# scope security
FP9300-A /security # show trustpoint CHdefault

Trustpoint CA:
    Trustpoint Name Trustpoint certificate chain Cert Status
    --------------- ---------------------------- -----------
    CHdefault       -----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTowOAYDVQQLEzEoYykgMjAwNiBWZXJp
U2lnbiwgSW5jLiAtIEZvciBhdXRob3JpemVkIHVzZSBvbmx5MUUwQwYDVQQDEzxW
ZXJpU2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCByjEL
MAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQLExZW
ZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTowOAYDVQQLEzEoYykgMjAwNiBWZXJpU2ln
biwgSW5jLiAtIEZvciBhdXRob3JpemVkIHVzZSBvbmx5MUUwQwYDVQQDEzxWZXJp
U2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9y
aXR5IC0gRzUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCvJAgIKXo1
nmAMqudLO07cfLw8RRy7K+D+KQL5VwijZIUVJ/XxrcgxiV0i6CqqpkKzj/i5Vbex
t0uz/o9+B1fs70PbZmIVYc9gDaTY3vjgw2IIPVQT60nKWVSFJuUrjxuf6/WhkcIz
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0PO7gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
```

```
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR0OBBYEFH/TZafC3ey78DAJ80M5+gKv
MzEzMA0GCSqGSIb3DQEBBQUAA4IBAQCTJEowX2LP2BqYLz3q3JktvXf2pXkiOOzE
p6B4Eq1iDkVwZMXnl2YtmAl+X6/WzChl8gGqCBpH3vn5fJJaCGkgDdk+bW48DW7Y
5gaRQBi5+MHt39tBquCWIMnNZBU4gcmU7qKEKQsTb47bDN0lAtukixlE0kF6BWlK
WE9gyn6CagsCqiUXObXbf+eEZSqVir2G3l6BFoMtEMze/aiCKm0oHw0LxOXnGiYZ
4fQRbxC1lfznQgUy286dUV4otp6F01vvpX1FQHKOtw5rDgb7MzVIcbidJ4vEZV8N
hnacRHr2lVz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
 Valid

FP9300-A /security #
```

Commande	Description
set certchain	Permet d’accéder à la liste (ou chaîne) de certificats d’un point de confiance.
set trustpoint	Définit le point de confiance de certificat d’un trousseau de clés.

show user-sessions

Pour afficher des informations sur les sessions utilisateur locales et distantes, utilisez la commande **show user-sessions**.

show user-sessions

Modes de commande

scope security

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Par défaut, cette commande affiche les informations sur les sessions utilisateur.

Exemple

Cet exemple montre comment afficher les informations sur les sessions utilisateur locales et distantes :

```
firepower# scope security
firepower /security # show user-sessions local
Session Id      User            Host                Login Time
--------------- --------------- ------------------- ----------
pts_0_1_24360*  admin           192.0.2.1           2021-10-11T20:46:16.000


firepower# show user-sessions local detail
Session Id pts_0_1_24360*:
    Fabric ID: A
    Term: pts/0
    User: admin
    Host: 192.0.2.1
    Pid: 24360
    Login Time: 2021-10-11T20:46:16.000
    Refresh Period (in secs): 0
    Session Timeout (in secs) for web, ssh, telnet sessions: 0
    Absolute Session Timeout (in secs) for web, ssh, telnet sessions: 0


firepower /security # show user-sessions remote

Session Id      User            Host                Login Time
--------------- --------------- ------------------- ----------
pts_1_1_9578    test1           192.0.2.2           2021-10-11T21:39:52.000


firepower /security # show user-sessions remote detail
Session Id pts_1_1_9578:
    Fabric ID: A
    Term: pts/1
    User: test1
    Host: 192.0.2.2
    Pid: 9578
    Login Time: 2021-10-11T21:39:52.000
    Refresh Period (in secs): 0
    Session Timeout (in secs) for web, ssh, telnet sessions: 0
```

```
Absolute Session Timeout (in secs) for web, ssh, telnet sessions: 0
```

show validate-task

Pour consulter l'état d'une vérification d'image lancée manuellement, utilisez la commande **show validate-task**.

show validate-task [**detail** | **fsm** | *pack_version*]

Description de la syntaxe

detail	(Facultatif) Affiche des informations détaillées sur l'état de tous les packages de plateforme disponibles.
fsm status	(Facultatif) Répertorie l'état de validation de la machine à états finis (FSM). Le mot clé **expand** et la variable *pack_version* sont également disponibles.
pack_version	(Facultatif) Affiche les informations de validation sur le package spécifié. Le mot clé **detail** est également disponible avec cette option.

Modes de commande

Mode micrologiciel

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Si vous n'incluez pas d'élément *pack-version*, la commande **show validate-task** répertorie les informations pour chaque image de micrologiciel sur l'appareil.

Vous pouvez utiliser cette commande ou la commande **show validation package** pour déterminer le numéro de version de package souhaité.

Exemple

Cet exemple montre comment afficher l'historique de validation d'un package de micrologiciel spécifique :

```
FP9300-A# scope firmware
FP9300-A /firmware # show validate-task 2.3(1.51)

Validate task:
    Pack Name: fxos-k9-bundle-infra.2.3.1.51.SPA
    Pack Version: 2.3(1.51)
    Validation Time Stamp: Never
    Validation State: None
    Overall Status String:

    Pack Name: fxos-k9-bundle-server.2.3.1.51.SPA
    Pack Version: 2.3(1.51)
    Validation Time Stamp: Never
    Validation State: None
    Overall Status String:

    Pack Name: fxos-k9.2.3.1.51.SPA
    Pack Version: 2.3(1.51)
    Validation Time Stamp: 2017-10-25T16:53:30.914
    Validation State: None
    Overall Status String: Ok
```

```
FP9300-A /firmware #
```

Commandes associées

Commande	Description
download image	Télécharge une image logicielle FXOS sur le châssis Firepower 4100/9300.
verify platform-pack	Vérifie l'intégrité d'une offre groupée de plateforme FXOS téléchargée.

show version

Pour afficher les informations sur la version logicielle du système actuel, utilisez la commande **show version**.

show version [**detail**]

Pour afficher les informations sur la version logicielle et l'état pour tous les composants du châssis, utilisez la commande **show version** en mode châssis.

show version [**detail** | **package-version**]

Pour afficher les informations sur la version logicielle et l'état des composants d'un serveur, utilisez la commande **show version** en mode serveur. En mode serveur, vous pouvez également afficher les informations sur la version des composants individuels.

show version [**adapter** | **bios** | **boardcontroller** | **cimc** | **detail** | **fxos** | **package-version** | **storage** |]

Description de la syntaxe

adapter	(Facultatif) Afficher les informations sur la version pour les adaptateurs installés sur le serveur connecté. Ce mot clé est uniquement disponible en mode serveur.
bios	(Facultatif) Affiche les informations sur la version du BIOS pour le serveur connecté. Ce mot clé est uniquement disponible en mode serveur.
boardcontroller	(Facultatif) Affiche les informations sur la version du contrôleur de gestion pour le serveur connecté. Ce mot clé est uniquement disponible en mode serveur.
cimc	(Facultatif) Affiche la version CIMC et les informations d'état pour le serveur connecté. Ce mot clé est uniquement disponible en mode serveur.
detail	(Facultatif) Affiche des informations supplémentaires sur la version.
fxos	(Facultatif) Affiche des informations sur la version du système d'exploitation SSP pour le serveur connecté. Ce mot clé est uniquement disponible en mode serveur.
package-version	(Facultatif) Affiche les informations sur la version du package uniquement. Ce mot clé est uniquement disponible dans les modes adaptateur, châssis, interconnexion de structures, serveur et système.
storage	(Facultatif) Affiche les informations sur la version pour les contrôleurs RAID et de disque local du serveur connecté. Ce mot clé est uniquement disponible en mode serveur.

Modes de commande

Tout mode de commande : affiche les informations sur la version du logiciel système

Mode châssis : affiche la version du logiciel et les informations d'état de tous les composants du châssis

Mode serveur : affiche la version du logiciel et les informations d'état des composants du serveur connecté

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Le mot clé **package-version** est uniquement disponible dans les modes adaptateur, châssis, interconnexion de structure, serveur et système.

En mode interconnexion de structure, cette commande affiche des informations supplémentaires sur la version; consultez l'exemple suivant.

Exemples

Cet exemple montre comment afficher des informations détaillées sur la version du système de gestion :

```
FP9300-A# show version detail
FPRM:
    Running-Vers: 4.2(1.62)
    Package-Vers: 2.2(1.63)
    Activate-Status: Ready
    Startup-Vers: 4.2(1.62)

FP9300-A#
```

Cet exemple montre comment afficher des informations sur la version en mode interconnexion de structure :

```
FP9300-A# scope fabric-interconnect a
FP9300-A /fabric-interconnect #show version
Fabric Interconnect A:
    Running-Kern-Vers: 5.0(3)N2(4.31.60)
    Running-Sys-Vers: 5.0(3)N2(4.31.60)
    Package-Vers: 2.3(1.51)
    Startup-Kern-Vers: 5.0(3)N2(4.31.60)
    Startup-Sys-Vers: 5.0(3)N2(4.31.60)
    Act-Kern-Status: Ready
    Act-Sys-Status: Ready
    Bootloader-Vers:

FP9300-A /fabric-interconnect #
```

Cet exemple montre comment afficher des informations sur la version des composants du châssis :

```
FP9300-A# scope chassis 1
FP9300-A /chassis # show version detail
Chassis 1:
    Server 1:
        CIMC:
            Running-Vers: 3.1(23a)
            Package-Vers: 2.3(1.51)
            Update-Status: Ready
            Activate-Status: Ready

        Adapter 1:
            Running-Vers: 4.0(1.67)
            Package-Vers: 2.3(1.51)
            Update-Status: Ready
            Activate-Status: Ready
            Bootloader-Update-Status: Ready
```

```
        Adapter 2:
            Running-Vers: 4.0(1.67)
            Package-Vers: 2.3(1.51)
            Update-Status: Ready
            Activate-Status: Ready
            Bootloader-Update-Status: Ready
        BIOS:
            Running-Vers: FXOSSM1.1.2.1.6.072020171212
            Package-Vers: 2.3(1.51)
            Update-Status: Ready
            Activate-Status: Ready

        SSP OS:
            Running-Vers: 2.3(1.50)
            Package-Vers: 2.3(1.51)
            Update-Status: Ready
            Activate-Status:

        RAID Controller 1:
            Running-Vers: 24.12.1-0203|6.30.03.0|NA
            Package-Vers: 2.3(1.51)
            Activate-Status: Ready

        BoardController:
            Running-Vers: 14.0
            Package-Vers: 2.3(1.51)
            Activate-Status: Ready

        Local Disk 1:
            Running-Vers: EM14
            Package-Vers:
            Activate-Status: Ready

        Local Disk 2:
            Running-Vers: EM14
            Package-Vers:
            Activate-Status: Ready

    Server 2:
        CIMC:
            Running-Vers: 3.1(23a)
            Package-Vers: 2.3(1.51)
            Update-Status: Ready
            Activate-Status: Ready

    <--- remaining lines removed for brevity --->

FP9300-A /chassis #
```

Commandes associées

Commande	Description
show server version	Affiche les versions logicielles et les informations d'état actuelles du serveur.

shutdown

Pour éteindre l'appareil, utilisez la commande **shutdown**.

shutdown [**no-prompt** | *reason*]

Description de la syntaxe

no-prompt	(Facultatif) Utilisez ce mot clé pour lancer immédiatement l'arrêt. Sinon, une commande **commit-buffer** est requise pour lancer l'arrêt.
reason	(Facultatif) Chaîne de texte à ajouter au journal d'arrêt; peut comporter jusqu'à 510 caractères.

Modes de commande

Mode châssis

Mode gestion locale : obsolète

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Nous vous recommandons de sauvegarder la configuration système avant l'arrêt.

Cette commande est obsolète en mode gestion locale; utilisez **shutdown** en mode châssis.

Exemple

Cet exemple montre comment accéder au mode châssis et arrêter le système :

```
Firepower # scope chassis 1
Firepower /chassis # shutdown no-prompt
Starting chassis shutdown. Monitor progress with the command "show fsm status".
Please set the power switch to the off position after "INIT: no more processes left in this
 runlevel" message is seen.
Firepower /chassis #
Broadcast message from root@Firepower (Tue Jul 14 11:40:47 2020):

All shells being terminated due to system /sbin/shutdown

Cisco FPR Series Security Appliance
INIT: Sending processes the TERM signal
Jul 14 11:40:53 %TTYD-2-TTYD_ERROR TTYD Error ttyd bad select

INIT: no more processes left in this runlevel
```

Commandes associées

Commande	Description
reboot	Redémarre le châssis ou l'interconnexion de structure.

show web-session-limits

Pour afficher la liste des sessions Web disponibles sur le système, utilisez la commande **show web-session-limits**.

show validate-task [**detail**]

Description de la syntaxe

detail	Affiche la liste des limites détaillées de session Web.

Modes de commande

scope system/scope services

Historique des commandes

Version	Modification
2.3.1	Commande ajoutée.

Instructions d'utilisation

Il s'agit d'une sous-commande de la commande **show** dans scope system, scope services.

Exemple

Cet exemple montre comment afficher les informations sur les limites de session Web du système :

```
Firepower /fabric-interconnect # scope system
Firepower /system # scope services
Firepower /system/services # show web-session-limits

Web Sessions:
    Maximum logins for single user Maximum Sessions
    ------------------------------ ----------------
    32                             256
```

Exemple

Cet exemple montre comment afficher les informations détaillées sur les sessions Web disponibles :

```
Firepower /system/services # show web-session-limits detail

Web Sessions:
    Maximum logins for single user: 32
    Maximum Sessions: 256
```

PARTIE III

Commandes T – W

• Commandes T – W, à la page 719

Commandes T – W

- terminal, à la page 720
- haut, à la page 721
- traceroute (connect local-mgmt), à la page 722
- traceroute6 (connect local-mgmt), à la page 723
- up, à la page 724
- verify platform-pack, à la page 725
- where, à la page 727

terminal

Pour définir le nombre et la largeur des lignes affichées dans la fenêtre de terminal, utilisez la commande **terminal**.

terminal { **length** *lines* | **width** *characters* }

Description de la syntaxe

length *lines*	Nombre de lignes affichées dans la fenêtre de terminal. Les valeurs valides sont comprises entre 0 et 255. Saisissez 0 pour supprimer les pauses.
width *characters*	Nombre de caractères affichés par ligne dans la fenêtre de terminal. Les valeurs valides sont comprises entre 24 et 511 caractères.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour définir le nombre de lignes et de caractères par ligne à afficher dans la fenêtre de terminal.

Exemple

Cet exemple montre comment définir le nombre de lignes affichées dans la fenêtre de terminal sur 12 :

```
FP9300-A# terminal length 12
FP9300-A *# commit-buffer
FP9300-A#
```

Commandes associées

Commande	Description
set cli	Spécifie si les lignes de sortie des commandes doivent être renvoyées à la ligne ou tronquées, si les en-têtes de tableau sont affichés et si des virgules ou des espaces sont utilisés pour séparer les champs dans les tableaux de sortie des commandes.

haut

Pour accéder au mode root (EXEC) depuis n'importe quel autre mode, utilisez la commande **top**.

top

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment accéder au mode root à partir de n'importe quel mode :

```
FP9300-A /system/services # top

FP9300-A#
```

Commandes associées

Commande	Description
up	Remonte d'un mode.

traceroute (connect local-mgmt)

Pour tracer la route vers un autre appareil sur le réseau en utilisant son nom de domaine ou son adresse IPv4, utilisez la commande **traceroute**.

traceroute {*hostname* | *IPv4_address*} [**source** *header_IP*]

Description de la syntaxe

hostname	*IPv4_address*	Nom de domaine ou adresse IP de l'appareil à contacter. Le nombre maximal de caractères autorisé pour le nom de domaine est de 510.
source *header_IP*	(Facultatif) Utilisez ce mot clé pour spécifier l'adresse IP de l'appareil à inclure dans les en-têtes de paquets.

Modes de commande

connect local-mgmt

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour tracer la route des paquets IP vers un hôte réseau.

Si vous ne spécifiez pas l'adresse IP **source** à inclure dans les en-têtes de paquets, l'adresse du port de gestion est utilisée.

Exemple

Cet exemple montre comment se connecter à l'interface de ligne de commande de gestion locale, puis tracer la route vers un autre appareil sur le réseau :

```
firepower# connect local-mgmt
firepower(local-mgmt)# traceroute 198.51.100.10
traceroute to 198.51.100.10 (198.51.100.10), 30 hops max, 40 byte packets
 1  198.51.100.57 (198.51.100.57)  0.640 ms  0.737 ms  0.686 ms
 2  net1-gw1-13.cisco.com (198.51.100.101)  2.050 ms  2.038 ms  2.028 ms
 3  net1-sec-gw2.cisco.com (198.51.100.201)  0.540 ms  0.591 ms  0.577 ms
 4  net1-fp9300-19.cisco.com (198.51.100.108)  0.336 ms  0.267 ms  0.289 ms

firepower(local-mgmt)#
```

Commandes associées

Commande	Description
ping	Envoie un message Ping à l'appareil à une destination spécifiée (adresse IPv4).

traceroute6 (connect local-mgmt)

Pour tracer la route vers un autre appareil sur le réseau en utilisant son nom de domaine ou son adresse IPv6, utilisez la commande **traceroute6**.

traceroute6 {*hostname* | *ipv6_address*} [**source** *header_ip*]

Description de la syntaxe

hostname	*ipv6_address*	Nom de domaine ou adresse IPv6 de l'appareil à contacter. Le nombre maximal de caractères autorisé pour le nom de domaine est de 510.
source *header_ip*	(Facultatif) Utilisez ce mot clé pour spécifier l'adresse IP de l'appareil à inclure dans les en-têtes de paquets.

Modes de commande

connect local-mgmt

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

Utilisez cette commande pour tracer la route des paquets IP vers un hôte réseau.

Si vous ne spécifiez pas l'adresse IP **source** à inclure dans les en-têtes de paquets, l'adresse du port de gestion est utilisée.

Exemple

Cet exemple montre comment se connecter à l'interface de ligne de commande de gestion locale, puis tracer la route vers un autre appareil sur le réseau :

```
firepower# connect local-mgmt
firepower(local-mgmt)# traceroute 2001:DB8:1::1
traceroute to 2001:DB8:1::1 (2001:DB8:1::1), 30 hops max, 40 byte packets
 1  2001:DB8:1::4 (2001:DB8:1::4)  0.640 ms  0.737 ms  0.686 ms
 2  net1-gw1-13.cisco.com (2001:DB8:1::6)  2.050 ms  2.038 ms  2.028 ms
 3  net1-sec-gw2.cisco.com (2001:DB8:1::8)  0.540 ms  0.591 ms  0.577 ms
 4  net1-fp9300-19.cisco.com (2001:DB8:1::7)  0.336 ms  0.267 ms  0.289 ms

firepower(local-mgmt)#
```

Commandes associées

Commande	Description
ping6	Envoie un message Ping à l'appareil à une destination spécifiée (adresse IPv6).

up

Pour monter d'un niveau dans la hiérarchie du mode de commande, utilisez la commande **up**.

up

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment monter d'un mode :

```
FP9300-A /org/service-profile # up
FP9300-A /org #
```

Commandes associées

Commande	Description
exit	Quitte la session d'interface de ligne de commande actuelle et se déconnecte du périphérique, ou quitte un mode d'objet connecté et revient au niveau racine (EXEC).
top	Permet d'accéder à la racine (EXEC) à partir de n'importe quel mode.

verify platform-pack

Pour vérifier manuellement l'intégrité d'une offre groupée de plateforme FXOS téléchargée, utilisez la commande **verify platform-pack**.

verify platform-pack version *version_number*

Description de la syntaxe

version *version_number*	Spécifie le numéro de version du package de plateforme à vérifier.

Modes de commande

Mode micrologiciel

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Instructions d'utilisation

L'intégrité de l'image est automatiquement vérifiée lorsqu'une nouvelle image est téléchargée sur le châssis Firepower 4100/9300. Utilisez cette commande pour vérifier manuellement et ultérieurement l'intégrité d'une image téléchargée.

Vous pouvez utiliser la commande **show validate-task** ou **show validation package** pour déterminer le numéro de version du package souhaité.

Vous pouvez également utiliser la commande **show validate-task** pour surveiller le processus de vérification. L'affichage de la sortie n'actualise pas automatiquement et vous pouvez être amené à saisir plusieurs fois la commande.

Exemple

Cet exemple montre comment vérifier un package de plateforme spécifique :

```
FP9300-A# scope firmware
FP9300-A /firmware # show validation package
Firmware Package 2.2(2.19):
    Validation Time Stamp: 2017-10-26T14:34:24.925
    Pack Name: fxos-k9.2.2.2.19.SPA
    Validation State: None
    Overall Status Code: Ok

Firmware Package 2.3(1.51):
    Validation Time Stamp: 2017-10-25T16:53:30.914
    Pack Name: fxos-k9.2.3.1.51.SPA
    Validation State: None
    Overall Status Code: Ok
FP9300-A /firmware # verify platform-pack version 2.3(1.51)
The currently installed FXOS platform software package is 2.3(1.51)
All the Security Modules will be installed with these software components:
    Security Module Adapter  4.0(1.67)
    Security Module BIOS     FXOSSM2.1.3.1.13.0927171811
    Security Module FXOS     2.3(1.50)

INFO: There is no service impact to install this FXOS platform software 2.3(1.51)


Verifying FXOS platform software package 2.3(1.51). Verification could take several minutes.
```

```
Do you want to proceed? (yes/no) [yes]:
```

Commandes associées

Commande	Description
download image	Télécharge une image logicielle FXOS sur le châssis Firepower 4100/9300.
show validate-task	Affiche l'état du processus de vérification d'image.

where

Pour savoir où vous vous situez dans la hiérarchie des commandes de l'interface de ligne de commande, utilisez la commande **where**.

where

Description de la syntaxe

Cette commande ne contient aucun argument ou mot clé.

Modes de commande

Tout mode de commande

Historique des commandes

Version	Modification
1.1(1)	Commande ajoutée.

Exemple

Cet exemple montre comment savoir où vous vous trouvez dans l'interface de ligne de commande :

```
FP9300-A /org/service-profile # where
Mode: /org/service-profile
Mode Data:
       scope org
       enter org org10
       enter service-profile sp10 instance
FP9300-A /org/service-profile #
```

Commandes associées

Commande	Description
top	Permet de revenir au niveau supérieur (EXEC) depuis n'importe quel mode.
up	Remonte d'un mode.

PARTIE IV

Commandes connect *shell*

• Commandes connect *shell*, à la page 731

Commandes connect *shell*

- Liste des commandes connect adapter, à la page 732
- Liste des commandes connect cimc, à la page 737
- Liste des commandes connect fxos, à la page 741
- Liste de commandes connect local-mgmt, à la page 756
- Liste des commandes connect module, à la page 762

Liste des commandes connect adapter

Après avoir utilisé la commande Supervisor **connect adapter** pour vous connecter au shell de commande d'un adaptateur spécifique, les commandes suivantes sont disponibles dans ce shell. Consultez connect adapter, à la page 40 pour plus de renseignements sur la commande **connect adapter**.

Attention Ces commandes ne doivent être utilisées que lors du dépannage des adaptateurs réseau virtualisés, et ce, sous la supervision du centre d'assistance technique Cisco.

Notez que lorsque vous vous connectez à un shell de commande d'adaptateur, l'invite de ligne de commande passe de votre invite par défaut, qui est le nom que vous avez attribué au périphérique, à `adaptateur n/n/n`, où `n/n/n` correspond à la combinaison châssis/serveur/ID de l'adaptateur que vous avez saisie pour la connexion.

Pour quitter le mode adaptateur, saisissez **exit**.

Exemple

L'exemple suivant montre comment se connecter au shell de commande de l'adaptateur et afficher les commandes disponibles :

```
firepower# connect adapter 1/2/1
adapter 1/2/1 # help
Available commands:
  connect             - Connect to remote debug shell
  exit                - Exit from subshell
  help                - List available commands
  history             - Show command history
  show-fwlist         - Show firmware versions on the adapter
  show-identity       - Show adapter identity
  show-phyinfo        - Show adapter phy info
  show-systemstatus   - Show adapter status
adapter 1/2/1 # exit
firepower#
```

Tableau 6 : Commandes disponibles dans le shell de commande principal de l'adaptateur

Commande	Autres renseignements
connexion	Se connecte au shell de débogage; permet d'accéder aux commandes répertoriées dans le tableau suivant.
exit	Permet de quitter le shell de commande de l'adaptateur.
help	Répertorie les commandes disponibles dans ce shell.
history	Affiche la liste des commandes exécutées depuis le démarrage de ce shell.
show-fwlist	Affiche les versions de micrologiciel sur l'adaptateur.

Commande	Autres renseignements
show-identity	Afficher l'identité de l'adaptateur
show-phyinfo	Afficher les informations phy sur l'adaptateur
show-systemstatus	Afficher l'état de l'adaptateur

Les commandes suivantes sont disponibles dans le sous-shell de débogage; accessible en saisissant la commande **connect** dans le shell de commande principal de l'adaptateur.

Remarque Lorsque vous vous connectez à un sous-shell de débogage du shell de l'adaptateur, l'invite de ligne de commande passe de l'invite de `adapter n/n/n` à `adapter n/n/n (top) :n`, où `(top) :` indique que vous vous trouvez en haut du sous-shell du shell de commande de l'adaptateur, et `n` représente le nombre de lignes de commande présentées jusqu'à présent dans cette session de débogage.

Pour quitter le sous-shell de débogage, saisissez **exit**.

Exemple

L'exemple suivant montre comment se connecter au sous-shell de débogage de l'adaptateur et afficher les commandes disponibles :

```
adapter 1/2/1 # connect
No entry for terminal type "dumb";
using dumb terminal settings.
adapter 1/2/1 (top):1# help
Available commands:
  attach-fls      - Attach to fls
  attach-mcp      - Attach to mcp
  estat           - Run fc performance monitor
  exit            - Exit from subshell
  help            - List available commands
  history         - Show command history
  phy-read        - Read PHY register
  show-acltab     - Show ACL table
  show-fru        - Show FRU contents
  show-fwdtab     - Show forwarding table
  show-log        - Show system log
  show-macstats   - Show MAC statistics
  show-pcisw      - Show PCIE switch status
adapter 1/2/1 (top):2# exit
adapter 1/2/1 #
```

Tableau 7 : Commandes disponibles dans le sous-shell de débogage de l'adaptateur

Commande	Autres renseignements
attach-fls	Se connecte au service de connexion de la structure de l'adaptateur; permet d'accéder aux commandes répertoriées dans le tableau suivant.
attach-mcp	Se connecte au programme de contrôle principal. Un grand nombre de commandes d'informations de débogage sont disponibles; utilisez la commande **help** pour afficher la liste. Encore une fois, ces commandes ne doivent être utilisées que sous la supervision du centre d'assistance technique Cisco.
estat	Permet de lancer un moniteur de performances Fibre Channel.
exit	Permet de quitter ce sous-shell.
help	Répertorie les commandes disponibles dans ce sous-shell.
history	Affiche la liste des commandes exécutées depuis le démarrage de ce sous-shell.
phy-read	Lire le registre PHY
show-acltab	Afficher le tableau ACL
show-fru	Afficher le contenu FRU
show-fwdtab	Afficher le tableau de transfert
show-log	Afficher le journal du système
show-macstats	Afficher les statistiques MAC
show-pcisw	Afficher l'état du commutateur PCIE

Les commandes suivantes sont disponibles dans le sous-shell FLS (Fabric Login Service); accessible en saisissant la commande **attach-fls** dans le shell de débogage de l'adaptateur.

Remarque Lorsque vous vous connectez au sous-shell FLS d'un sous-shell de débogage de l'adaptateur, l'invite de la ligne de commande passe de `adaptater n/n/n (top) :n`, à `adapter n/n/n (fls) :n` où `(fls):` indique vous vous trouvez dans le sous-shell FLS du sous-shell de débogage, et *n* représente le nombre de lignes de commande présentées jusqu'à présent dans cette session FLS.

Pour quitter la sous-shell FLS, saisissez **exit**; vous revenez au sous-shell de débogage.

Exemple

L'exemple suivant montre comment se connecter au sous-shell FLS à partir du sous-shell de débogage et afficher les commandes disponibles :

```
adapter 1/2/1 # connect
No entry for terminal type "dumb";
using dumb terminal settings.
adapter 1/2/1 (top):1#  attach-fls
No entry for terminal type "dumb";
using dumb terminal settings.
adapter 1/2/1 (fls):1# help
Available commands:
         d - dumps the contents of the last fw request
      exit - Exit from subshell
  fwactive - retrieve active fcpu exchanges
     fwcqs - retrieves fcpu cq information
    fwexch - retrieves fcpu exchange data
     fwlif - retrieves fcpu lif data
    fwvnic - retrieves fcpu vnic data
      help - List available commands
   history - Show command history
       lif - Show lif information
     login - Show login information pertaining to vnic
   lunlist - Show Nameserver and Report LUN's response information for vnic
    lunmap - Show lunmap information pertaining to vnic
      vnic - Show vnic information

adapter 1/2/1 (fls):2# exit
adapter 1/2/1 (top):2#
```

Tableau 8 : Commandes disponibles dans le sous-shell FLS

Commande	Autres renseignements
d	Extrait le contenu de la dernière demande de micrologiciel.
exit	Quitte le sous-shell FLS.
fwactive	Récupère les échanges de fcpu actifs
fwcqs	Récupère les informations fcpu cq
fwexch	Récupère les données des échanges fcpu
fwlif	Récupère les données fcpu lif
fwvnic	Récupère les données fcpu vnic
help	Répertorie les commandes disponibles
history	Affiche l'historique des commandes
lif	Affiche les informations lif
connexion	Affiche les informations de connexion vnic
lunlist	Affiche les informations de réponse du serveur de noms et des LUN de rapport pour vnic

Commande	Autres renseignements
lunmap	Affiche les informations de mappage de LUN (lunmap) relatives à la vnic
vnic	Affiche les informations sur la vnic

Liste des commandes connect cimc

Après avoir utilisé la commande Supervisor **connect cimc** pour vous connecter à l'utilitaire de débogage du micrologiciel CIMC pour un module spécifiques, les commandes suivantes sont disponibles dans ce shell. Consultez connect cimc, à la page 44 pour plus de renseignements sur la commande **connect cimc**.

Cet utilitaire donne accès à un shell en lecture seule doté de commandes qui vous permettent de visualiser les informations de débogage CIMC en temps réel. Ces commandes sont utilisées principalement pour résoudre les problèmes CIMC : affichage des alarmes, des journaux des événements système, des échecs d'intégration et des contrôles d'alimentation.

Remarque Lorsque vous vous connectez au shell de commande CIMC, l'invite de ligne de commande passe de votre invite par défaut, qui correspond au nom que vous avez attribué à l'appareil, à `[ xxx ]`, où *xxx* correspond à la dernière commande que vous avez saisie; consultez l'exemple suivant.

Pour quitter le shell CIMC, saisissez **exit**.

Exemple

L'exemple suivant montre comment se connecter au mode CIMC, puis répertorier les commandes disponibles :

```
firepower# connect cimc 1/1
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '^]'.

CIMC Debug Firmware Utility Shell [ support ]
[ help ]# help
_____________________________________________
          Debug Firmware Utility
_____________________________________________
Command List
_____________________________________________
alarms
cores
dimmbl
exit
i2cstats
images
mctools
memory
messages
mrcout
network
obfl
post
power
programmables
sensors
sel
fru
tasks
top
```

```
update
users
version
cert
sldp
help
help [COMMAND]

_____________________________________________
 Notes:
"enter Key" will execute last command
"COMMAND ?" will execute help for that command

_____________________________________________
[ help ]# power
OP:[ status ]
Power-State:                [ on ]
Master-State:               [ Master ]
VDD-Power-Good:             [ active ]
Power-On-Fail:              [ inactive ]
Power-Ctrl-Lock:            [ unlocked ]
Power-System-Status:        [ Good ]
Front-Panel Power Button:   [ Disabled ]
Front-Panel Reset Button:   [ Disabled ]
Source of Last Power Change: [ Software - "mcserver" ]
OP-CCODE:[ Success ]
[ power ]# exit
Connection closed by foreign host.
firepower#
```

Tableau 9 : Commandes disponibles dans le shell de débogage CIMC

Commande	Autres renseignements
alarms	Affiche l'état actuel du voyant d'état (StatusLED) et, le cas échéant, les capteurs en alarme. Niveaux d'alarme : 1 : OK (VERT FIXE) 2 : initialisation mémoire (VERT CLIGNOTANT) 3 : erreur mineure (ORANGE FIXE) 4 : erreur sévère (ORANGE CLIGNOTANT)
cores	Énumère le répertoire de vidage de la mémoire.
exit	Quitte la sous-shell CIMC.
fru	Répertorie toutes les informations relatives aux unités remplaçables sur site (FRU).
help [COMMAND]	La saisie de la commande **help** répertorie toutes les commandes disponibles. La saisie de **help** *de nomd_cmd*ou *nom_de_cmd* **?** affiche les informations d'aide sur la commande spécifiée.
i2cstats	Affiche les informations sur le registre du contrôleur I^{2C}, les compteurs du pilote et les données de trace de débogage multi-primaire.

Commande	Autres renseignements
images	Affiche la version d'image logicielle et les informations d'état.
mctools	Affiche les informations sur l'état actuel de MCtools : informations sur la taille du connecteur et de la mémoire cache du fichier de partage.
memory	Répertorie les statistiques de mémoire et de charge.
messages	messages [dump|follow|tail] dump : extraire le fichier /var/log/messages follow : suivre le fichier /var/log/messages tail : extraire les 100 derniers messages
mezz1fru	Afficher les informations sur la carte mezz 1 FRU
mezz2fru	Afficher les informations sur la carte mezz 2 FRU
mrcout	Dump MrcOut*.txt
network	Afficher l'état du réseau en temps réel; Extraire les informations réseau
obfl	Extraire OBFL : journal des défaillances intégré dump : extraire OBFL follow : suivre OBFL tail : extraire les 100 derniers messages
post	Extraire les informations du post du BIOS
power	Afficher l'état de l'alimentation en temps réel Extraire l'état d'alimentation de la lame
programmables	Extraire les versions programmables de la carte
sensors	Afficher tous les capteurs en temps réel sensors [all|power|temp|fault|pres|led] all : extraire tous les capteurs (par défaut) power : extraire les capteurs d'alimentation uniquement time : extraire les capteurs de température uniquement fault : extraire les capteurs de défaillance uniquement pres : extraire les capteurs de présence uniquement led : extraire les capteurs DEL uniquement
sel	Afficher les informations SEL de la lame - journal d'événements système

Commande	Autres renseignements
sldp	Débogage interactif CIMC Cette commande effectue une authentification de débogage interactive avec l'aide de l'utilisateur et du personnel d'assistance de Cisco.
tasks	Extraire les informations des tâches en cours
top	Exécuter la surveillance des processus TOP
update	État actuel de la mise à jour du micrologiciel
users	Extraire les utilisateurs IPMI
version	Obtenir les informations de version

Liste des commandes connect fxos

Après avoir utilisé la commande Supervisor **connect fxos** pour vous connecter au shell de l'interface de ligne de commande FXOS de la structure de commutation, les commandes suivantes sont disponibles dans ce shell. Consultez connect adapter, à la page 40 pour plus de renseignements sur la commande **connect fxos**.

Remarque Lorsque vous vous connectez au shell de commande FXOS, l'invite de ligne de commande passe de votre invite par défaut, qui correspond au nom que vous avez attribué à l'appareil, à l'invite par défaut à laquelle est ajouté `(fxos)`; consultez l'exemple suivant.

Pour quitter le shell FXOS, saisissez **exit**.

Exemple

L'exemple suivant montre comment se connecter au shell de commande FXOS et afficher les commandes disponibles :

```
firepower# connect fxos
firepower(fxos)# ?
  clear         Reset functions
  cli           CLI commands
  debug         Debugging functions
  debug-filter  Enable filtering for debugging functions
  ethanalyzer   Configure cisco packet analyzer
  no            Negate a command or set its defaults
  ntp           NTP configuration
  show          Show running system information
  system        System management commands
  terminal      Set terminal line parameters
  test          Test command
  undebug       Disable Debugging functions (See also debug)
  end           Go to exec mode
  exit          Exit from command interpreter
  pop           Pop mode from stack or restore from name
  push          Push current mode to stack or save it under name
  where         Shows the cli context you are in

firepower(fxos)# exit
firepower#
```

Tableau 10 : Commandes disponibles dans le shell FXOS de la structure de commutation

Commande	Autres renseignements
clear	Fonctions de réinitialisation counters : effacer les compteurs logging : effacer les informations de journalisation mac : MAC

Commande	Autres renseignements
cli	Commandes de l'interface de ligne de commande var : définir une variable
debug	Fonctions de débogage; voir le tableau suivant
debug-filter	Activer le filtrage pour les fonctions de débogage ip : événements IP ipv6 : événements IPv6 pktmgr : Pm debug-filter routing : événements de routage
ethanalyzer	Configurer l'analyseur de paquets Cisco local : commencer la capture locale des trames à Sup
no	Annuler une commande ou définir ses valeurs par défaut debug : fonctions de débogage debug-filter : activer le filtrage des fonctions de débogage ethanalyzer : configurer l'analyseur de paquets Cisco terminal : définir les paramètres de ligne du terminal test : commande de test
ntp	Configuration du protocole NTP sync-retry : retenter la synchronisation avec les serveurs configurés
show	Afficher les informations sur le système en cours d'exécution; voir le tableau suivant
system	Commandes du système de gestion hap-reset : permet la réinitialisation du superviseur local ou distant en cas de défaillances HA. heartbeat : active la pulsation no : annuler une commande ou définir ses valeurs par défaut
terminal	Définir les paramètres de ligne de terminal; voir le tableau suivant
test	Commande de test aaa : authentification AAA eltm : afficher les informations eltm forwarding : informations Fib hardware : tester les paramètres matériels otv

Commande	Autres renseignements
undebug	Désactiver les fonctions de débogage (voir aussi debug) all : désactiver tout le débogage icmpv6 : commandes de débogage ICMPv6 ip : événements IP ipv6 : événements IPv6 l2 : couche 2 l3vm : informations de débogage L3VM pktmgr : informations sur le débogage et le tunnel du gestionnaire de paquets rpm : gestionnaire de politique de routage (RPM) sockets : connecteurs system : activer le débogage des composants système
end	Accéder au mode d'exécution
exit	Quitter l'interpréteur de commandes
pop	Dépiler le mode ou le restaurer à partir d'un nom *name* : nom (facultatif)
push	Empiler le mode actuel ou l'enregistrer sous un nom *name* : nom (facultatif)
where	Affiche le contexte d'interface de ligne de commande dans lequel vous vous trouvez detail : affiche chaque entrée sur une ligne distincte (facultatif)

Tableau 11 : Commandes de débogage, d'affichage et de terminal disponibles dans le shell de commande FXOS

Commande	Autres renseignements
debug	

Commande	Autres renseignements
	Fonctions de débogage aaa : activer le débogage pour aaa aclcomp : configurer le débogage aclcomp acllog : configure le débogage acllog aclmgr : configurer le débogage aclmgr afm : configurer le débogage afm assc : association entre ID Original et ID Traduit bcm-usd : BCM USD **Remarque** Pour bcm-usd, les valeurs d'utilisation du CPU sont toujours élevées, même en cas de trafic normal. Il s'agit d'un comportement attendu, sans incidence fonctionnelle. bootvar : activer le débogage bootvar callhome : activer le débogage pour Callhome cdp : configurer le débogage CDP cert-enroll : configurer le débogage pour le démon d'inscription de certificat. confs : activer le débogage pour CFS cli : déboguer l'interface de ligne de commande clis : déboguer le serveur de l'interface de ligne de commande clk_mgr : configurer le débogage clk_mgr copp : configurer le débogage copp core : configurer le débogage du démon core csm : activer les débogages csm device-alias : configurer les débogages pour le service de distribution d'alias d'appareil. dstats : configurer le débogage des statistiques delta eltm : configurer le débogage eltm ethpc : configurer le débogage ethpc ethpm : configurer le débogage ethpm evmc : débogage du client du gestionnaire d'événements fc-mac : informations sur le débogage fcp fc2 : configurer le débogage FC2 fc2d : configurer le débogage fc2d fcdomain : activer le débogage fcdomain

Commande	Autres renseignements
	fcwd : activer le débogage fcwd fcns : déboguer le serveur de noms fcoe_klm : configurer le débogage FCOE_KLM fcpc : configurer le débogage fcpc fcs : configurer le débogage du serveur de configuration de structure fdmi : configurer le débogage fdmi fex : déboguer l'interface de ligne de commande pour le processus FEX fex : configurer le débogage fex fgi : configurer le débogage fgi fm : configurer le débogage du gestionnaire de fonctionnalités fsf : configurer le débogage FSPF hardware : déboguer le matériel, paramètres des modules chargeables du noyau icmpv6 : commandes de débogage ICMPv6 idehsd : configurer le débogage du gestionnaire Idehsd im : configurer le débogage im ip : événements IP ipconf : configurer le débogage ipconf ipfib : configurer le débogage ipfib ipqos : configurer le débogage du gestionnaire IP QoS ipv6 : événements IPv6 klm : déboguer les paramètres des modules chargeables du noyau l2 : couche 2 l3vm : informations de débogage L3VM lacp : configurer le débogage lacp ldap : configurer le débogage ldap ledmgr : configurer le débogage du gestionnaire de voyants DEL license : activer le débogage pour les licences lldp : configurer le débogage lldp logfile : diriger la sortie de débogage vers un fichier journal logging : configurer la journalisation ou le débogage syslogd m2rib : configurer le débogage m2rib mcec : configurer le débogage MCEC mcm : configurer le débogage mcm

Commande	Autres renseignements
	mfdm : configurer le débogage mfdm monitor : configurer les sessions SPAN Ethernet msp : configurer le débogage msp mvsh : déboguer le serveur MVSH nf : configurer le débogage nf nohms : configurer le débogage nohms nPACL : configurez la fonction NPACL nsmgr : configurer le débogage nsmgr ntp : déboguer le module NTP obfl : configurer le débogage obfl pfm : configurer le débogage pfm pfstat : configurer le débogage pfstat pktmgr : informations sur le débogage et le tunnel du gestionnaire de paquets plateform : configurer le débogage de la plateforme plateform : informations internes de la plateforme platform : plateforme plog : configurer le débogage plog pltfm_config : configurer le débogage pltfm_config plugin : configurer le débogage des modules d‘extension port : configurer le débogage des ports port-channel : configurer le débogage des canaux de ports port-profile : activer le débogage du gestionnaire des profils de ports port-resources : configurer le débogage prm port-security : commande liée à la sécurité du port private-vlan : configurer les indicateurs de débogage du VLAN privé process-sap : SAP du processus à déboguer provision : configurer le débogage provision psshelper : débogage psshelper psshelper_gsvc : débogage psshelper ptplc : configurer le débogage ptplc qd : afficher les informations sur qd radius : configurer le débogage pour le démon radius res_mgr : configurer le débogage res_mgr

Commande	Autres renseignements
	rib : configurer le débogage rib rlir : configurer le débogage RLIR rpm : gestionnaire de politique de routage (RPM) rscn : configurer le débogage RSCN sal : configurer le débogage sal san-port-channel : configurer le débogage san-port-channel scsi-target : configurer le débogage du démon cible ssi security : configurer le débogage pour la sécurité session-mgr : activer le débogage du gestionnaire de session snm : configurer le débogage snm snmp : configurer le débogage du serveur snmp sockets : connecteurs spm : configurer le débogage spm statsclient : statistiques system : activer le débogage des composants système system : déboguer le système tacacs+ : configurer le débogage pour TACACS+ track – Configurer le débogage du suivi transceiver : commandes de débogage de l'émetteur-récepteur FC tunnel : configurer le débogage du tunnel udld : configurer le débogage udld **Remarque** FXOS ne prend pas en charge la détection de liaison unidirectionnelle (UDLD); ignorer toute référence à UDLD. ufdm : configurer le débogage ufdm vim : configurer le débogage vim vlan : configurer les indicateurs de débogage pour le gestionnaire VLAN vmm : configurer le débogage vmm vms : configurer le débogage vms vsan : activer le débogage du gestionnaire VSAN willsden : configurer le débogage willsden wwn : configurer le débogage du gestionnaire WWN xml : agent XML zone : commandes de débogage du serveur de zones

Commande	Autres renseignements
	zshk : configurer le débogage zshk

Commande	Autres renseignements
show	

Commande	Autres renseignements
	Afficher les données du système en cours d'exécution aaa : afficher les informations aaa access-lists : répertorier les listes d'accès accounting : afficher la configuration de la comptabilisation banner : afficher le message de bannière de motd actuel boot : afficher les variables Bootvar callhome : afficher les informations callhome cdp : afficher les informations sur le protocole de découverte Cisco cfs : gestionnaire de commandes d'affichage CFS class-map : afficher les cartes de trafic cli : afficher les informations sur l'interface de ligne de commande clock : afficher la date actuelle cluster-state : afficher l'état de la grappe configuration : afficher les informations sur les sessions de configuration copyright : informations sur les droits d'auteur debug : afficher les indicateurs de débogage device-alias : afficher les informations sur le service de distribution d'alias d'appareil diagnostic : commandes de diagnostic ecmp-groups : afficher tous les groupes ECMP environment : informations sur l'environnement du système fc2 : afficher les tableaux et statistiques fc2 fc2d : afficher les informations fc2d fcalias : commandes d'affichage fcalias fcdomain : afficher les informations fcdomain fcdroplatex : afficher la latence du commutateur ou du réseau fcflow : afficher les informations fcflow fcid-allocation : afficher les informations sur la liste d'allocation fcid fcns : afficher les tableaux du serveur de noms fcroute : afficher les routes FC fcs : afficher les informations sur le serveur de configuration de structure fctimer : afficher les temporisateurs Fibre Channel. fdmi : afficher les informations fdmi

Commande	Autres renseignements
	flogi : afficher les informations sur LOGI fp : Fp fspf : afficher les informations sur FSPF hardware : afficher les informations sur le matériel hostname : afficher le nom de domaine du système hosts : afficher les informations sur le DNS in-order-warrantee : afficher la configuration de la garantie de livraison dans l'ordre incompatibility : afficher les configurations incompatibles install : afficher l'incidence de l'installation logicielle entre deux images interface : afficher l'état et les informations de l'interface inventory : afficher l'inventaire physique ip : afficher les informations IP ip : informations IP ipmc-groups : afficher tous les groupes IPMC ipv6 : afficher les informations IPv6 klm : afficher les informations sur le module de noyau l2-class-id : allocation d'ID de classe L2 l2-table : afficher toutes les entrées L2 lacp : afficher les informations LACP ldap-server : afficher les informations de configuration LDAP line : afficher la configuration de la ligne lldp : afficher les informations sur lldp loadbalancing : afficher l'équilibrage de charge monodiffusion d'un certain flux ou échange locator-led : afficher l'état du voyant de localisation sur l'appareil logging : afficher la configuration de journalisation et le contenu du fichier journal mac : MAC module : afficher les informations sur le module monitor : afficher les informations SPAN Ethernet msp : commandes msp nsm : Afficher les informations du gestionnaire de segments réseau ntp : afficher les informations NTP phy-bypass : contournement matériel

Commande	Autres renseignements
	plateform : afficher la liste des événements reçus par le gestionnaire de plateforme policy-map : afficher les listes de politiques port : afficher les informations sur le port port-canal : afficher les informations sur le canal de port port-profile : afficher le profil de port port-security : commande liée à la sécurité du port queuing : afficher les informations de mise en file d'attente de l'interface radius-server : afficher les informations de configuration RADIUS redondance : afficher l'état de redondance du système resource : afficher la configuration des ressources pour VDC rlir : afficher les informations RLIR rmon : afficher les statistiques RMON role : afficher la configuration du rôle routage : afficher les informations de routage routing-context : afficher le contexte de routage actuel rscn : afficher les informations RSCN running-config : configuration en cours d'exécution san-port-channel : afficher les informations sur le canal de port scsi-target : afficher les informations sur la cible scsi détectée snmp : afficher les informations snmp smp : contenu SPROM ssh : afficher les informations SSH startup-config : configuration de démarrage actuelle svs : afficher les informations svs switchname : afficher le nom de domaine du système system : commandes d'affichage liées au système tacacs-server : afficher les informations de configuration TACACS+ tech-support : recueillir des informations pour la résolution de problèmes telnet : afficher la configuration du serveur telnet terminal : affiche les paramètres de configuration du terminal topology : afficher les informations sur les commutateurs connectés track : informations de suivi trunk : afficher les informations de liaison

Commande	Autres renseignements
	udld : protocole UDLD **Remarque** FXOS ne prend pas en charge la détection de liaison unidirectionnelle (UDLD); ignorer toute référence à UDLD. user-account : afficher les informations sur l'utilisateur users : afficher les utilisateurs actuellement connectés au système vdc : afficher les contextes d'appareils virtuels version : afficher la version logicielle vifs : interfaces virtuelles vlan : commandes VLAN vms : commandes vms vmware : en rapport avec VMware vrf : afficher les informations VRF vsan : afficher les informations vsan wwn : afficher les informations wwn xml : agent XML zone : commandes d'affichage de zone zoneset : commandes d'affichage d'ensemble de zone

Commande	Autres renseignements
terminal	Définir les paramètres de ligne du terminal alias : afficher les alias (en l'absence d'arguments); créer des alias « exec » (non persistants) Les alias persistants sont en mode configuration, voir « alias cli » color : activer la colorisation de l'invite (verte si la dernière commande a abouti, rouge en cas d'erreur), de la ligne de commande (bleue) et de la sortie (couleur par défaut) dont-ask : ne pas demander de confirmation; utiliser la réponse par défaut edit-mode : définir les clés d'édition de la ligne de commande (vi ou emacs; emacs par défaut) event-manager : événement d'interface de ligne de commande du gestionnaire d'événements history : configurer les propriétés d'historique du terminal length : définir le nombre de lignes à l'écran monitor : copier la sortie du journal système sur la ligne de terminal actuelle no : annuler une commande ou définir ses valeurs par défaut output : comment formater la sortie des commandes d'affichage prompt : configurer l'apparence de l'invite redirection-mode : définir le mode de redirection session-timeout : définir le délai d'expiration de la session persistent-mode : rechercher la correspondance de commande dans le mode actuel uniquement terminal-type : définir le type de terminal time : enregistrer l'heure actuelle sous une variable tree-update : mettre à jour l'arborescence d'analyse principale verify-only : vérifier la commande sans l'exécuter width : définir la largeur du terminal d'affichage

Liste de commandes connect local-mgmt

Après avoir utilisé la commande Supervisor **connect local-mgmt** pour vous connecter au shell de gestion locale, les commandes suivantes sont disponibles dans ce shell. Consultez connect adapter, à la page 40 pour plus de renseignements sur la commande **connect local-mgmt**.

Dans ce shell, vous pouvez effectuer des opérations sur l'interconnexion de structures, notamment la copie de fichiers, le redémarrage de l'interconnexion de structures, l'exécution des commandes ping et traceroute, voire la génération de fichiers de dépannage.

Lorsque vous vous connectez au shell de commande de gestion locale, l'invite de ligne de commande passe de votre invite par défaut, qui correspond au nom que vous avez attribué à l'appareil, à l'invite par défaut à laquelle est ajouté `(local-mgmt)` ; consultez l'exemple suivant.

Pour quitter le mode gestion locale, saisissez **exit**.

Exemple

L'exemple suivant montre comment se connecter au shell de commande de gestion locale et afficher les commandes disponibles :

```
firepower# connect local-mgmt
firepower(local-mgmt)#  ?
  cd                Change current directory
  clear             Clear managed objects
  cluster           Cluster mode
  connect           Connect to Another CLI
  copy              Copy a file
  cp                Copy a file
  delete            Delete managed objects
  dir               Show content of dir
  enable            Enable
  end               Go to exec mode
  erase             Erase
  erase-log-config  Erase the mgmt logging config file
  exit              Exit from command interpreter
  fips              FIPS compliance
  ls                Show content of dir
  mgmt-port         Management Port
  mkdir             Create a directory
  move              Move a file
  mv                Move a file
  ping              Test network reachability
  ping6             Test IPv6 network reachability
  pwd               Print current directory
  reboot            Reboots Fabric Interconnect
  restore-check     Check if in restore mode
  rm                Remove a file
  rmdir             Remove a directory
  run-script        Run a script
  show              Show system information
  shutdown          Shutdown
  ssh               SSH to another system
  tail-mgmt-log     tail mgmt log file
  telnet            Telnet to another system
  terminal          Terminal
  top               Go to the top mode
  traceroute        Traceroute to destination
```

```
  traceroute6       Traceroute to IPv6 destination
  verify            Verify Application Image

firepower(local-mgmt)# exit
firepower#
```

Tableau 12 : Commandes disponibles dans le shell de gestion locale

Commande	Autres renseignements
cd	Modifier le répertoire actuel usbdrive : URI du fichier volatile : URI du fichier workspace : URI du fichier clear : effacer les objets gérés. sshkey : clé SSH publique de l'hôte
cluster	Mode grappe force : forcer l'interconnexion de structures locale à devenir principale lead : faire de l'interconnexion de structures subordonnée la principale
connect	Se connecter à une autre interface de ligne de commande. adapter : adaptateur mezzanine cimc : Cisco Integrated Management Controller fxos : se connecter à l'interface de ligne de commande FXOS local-mgmt : se connecter à l'interface de ligne de commande de gestion locale module : console de module de sécurité
copy	Copier un fichier ftp : URI du fichier source scp : URI du fichier source sftp : URI du fichier source tftp : URI du fichier source usbdrive : URI du fichier source volatile : URI du fichier source workspace : URI du fichier source **Remarque** Cette commande n'est pas prise en charge sur les URI de fichiers HTTP.

Commande	Autres renseignements
cp	Copier un fichier ftp : URI du fichier source scp : URI du fichier source sftp : URI du fichier source tftp : URI du fichier source usbdrive : URI du fichier source volatile : URI du fichier source workspace : URI du fichier source **Remarque** Cette commande n'est pas prise en charge sur les URI de fichiers HTTP.
delete file	Supprimer les objets gérés usbdrive : URI du fichier source volatile : URI du fichier source workspace : URI du fichier source
dir	Afficher le contenu du répertoire order (Facultatif) : trier les fichiers par heure usbdrive (Facultatif) : URI du fichier volatile (Facultatif) : URI du fichier workspace (Facultatif) : URI du fichier
enable cluster	Activer le mode grappe a.b.c.d : adresse IpV4 de la grappe ipv6 : mode grappe IPv6
end	Accéder au mode d'exécution
erase	Effacer configuration : configuration système
erase-log-config	Effacer le fichier de configuration de la journalisation de gestion
exit	Quitter l'interpréteur de commandes
fips	Conformité FIPS fault-test : exécuter les tests de défaillance FIPS self-test : exécuter l'autotest FIPS sur demande

Commande	Autres renseignements
ls	Afficher le contenu du répertoire order (Facultatif) : trier les fichiers par heure usbdrive (Facultatif) : URI du fichier volatile (Facultatif) : URI du fichier workspace (Facultatif) : URI du fichier
mgmt-port	Port de gestion no-shut (facultatif) : port de gestion activé shutdown (facultatif) : port de gestion désactivé
mkdir	Crée un répertoire usbdrive (Facultatif) : URI du fichier volatile (Facultatif) : URI du fichier workspace (Facultatif) : URI du fichier
move	Déplacer un fichier usbdrive (Facultatif) : URI du fichier volatile (Facultatif) : URI du fichier workspace (Facultatif) : URI du fichier
mv	Déplacer un fichier usbdrive (Facultatif) : URI du fichier volatile (Facultatif) : URI du fichier workspace (Facultatif) : URI du fichier
ping	remote_host : nom de domaine ou adresse IP (taille minimale 0, taille maximale 510)
ping6	Tester l'accessibilité du réseau Tester l'accessibilité du réseau IPv6 remote_host : nom de domaine ou adresse IP (taille minimale 0, taille maximale 510)
pwd	Imprimer le répertoire actuel
reboot	Redémarrer l'interconnexion de structures
	Vérifier si le mode restauration est activé

Commande	Autres renseignements
rm	Supprimer un fichier usbdrive (Facultatif) : URI du fichier volatile (Facultatif) : URI du fichier workspace (Facultatif) : URI du fichier
rmdir	Supprimer un répertoire usbdrive (Facultatif) : URI du fichier volatile (Facultatif) : URI du fichier workspace (Facultatif) : URI du fichier
run-script	Exécuter un script workspace : nom d'un script à exécuter
show	Affiche les données système cli : informations sur l'interface de ligne de commande clock : horloge file : commandes de fichiers license : afficher les informations sur les licences mgmt-ip-debug : informations sur le débogage IP mgmt-port : port de gestion open-network-ports : afficher les ports réseau ouverts pmon : pmon processes : processus sel : journal des événements système software : logiciels sshkey : clé SSH tech-support : assistance technique
shutdown	Arrêter
ssh	Connexion SSH vers à un autre système remote_system : saisir le nom de domaine ou utilisateur@nom_de_domaine (taille minimale 0, taille maximale 510)
tail-mgmt-log	Consulter les dernières entrées du fichier journal de gestion module : nom du module (taille minimale 0, taille maximale 510)

Commande	Autres renseignements
telnet	Connexion Telnet vers un autre système remote_host : nom de domaine ou adresse IP (taille minimale 0, taille maximale 510)
terminal	Définir les paramètres de ligne du terminal length : définir le nombre de lignes à l'écran width : définir la largeur du terminal d'affichage
top	Accéder au mode supérieur
traceroute	Traceroute vers la destination remote_host : nom de domaine ou adresse IP (taille minimale 0, taille maximale 510)
traceroute6	Traceroute vers la destination IPv6 remote_host : nom de domaine ou adresse IP (taille minimale 0, taille maximale 510)
verify signature	Vérifier l'image de l'application bootflash : nom du fichier image usbdrive : nom du fichier image volatile : nom du fichier image workspace : nom du fichier image

Remarque Vous noterez des différences en termes de valeurs d'utilisation du CPU si vous utilisez simultanément les commandes **show processes** et **show system resources**. Les valeurs d'utilisation du CPU diffèrent en raison du nombre d'itérations et d'intervalles que chaque CLI utilise par défaut pour résumer la sortie après échantillonnage.

Liste des commandes connect module

Après avoir utilisé la commande Supervisor **connect module** pour vous connecter à une console de module spécifique, les commandes suivantes sont disponibles sur cette console. Consultez connect module, à la page 52 pour plus de renseignements sur la commande **connect module**.

Dans ce shell, vous pouvez effectuer des opérations sur l'interconnexion de structures, notamment la copie de fichiers, le redémarrage de l'interconnexion de structures et l'exécution des commandes ping et traceroute.

Remarque Lorsque vous vous connectez au shell de commande d'un module, l'invite de ligne de commande passe de votre invite par défaut, qui correspond au nom que vous avez attribué à l'appareil, à `Firepower-module`*n*, où *n* correspond au numéro du module auquel vous vous êtes connecté; consultez l'exemple suivant.

Exemples

L'exemple suivant montre comment se connecter au module 1 à l'aide de Telnet et afficher les commandes disponibles :

```
firepower# connect module 1 telnet
Type exit or Ctrl-] followed by . to quit.
Firepower-module1>?
    secure-login     => Enable blade secure login
    show             => Display system information. Enter show ? for options
    config           => Configure the system. Enter config ? for options
    terminalLength   => Terminal settings. Enter terminal ? for options
    ping             => Ping a host to check reachability
    nslookup         => Look up an IP address or host name with the DNS servers
    traceroute       => Trace the route to a remote host
    connect          => Connect to specific csp console (asa, etc)
    support          => System file operations
    testcrashinfo    => Test crashinfo support
    exit             => Exit the session
    help             => Get help on command syntax
Firepower-module1> <Ctrl-], .>
firepower#
```

Tableau 13 : Commandes disponibles sur une console de module

Commande	Autres renseignements
secure-login	Activer la connexion sécurisée de la lame

Commande	Autres renseignements
show	Afficher les informations système. Saisir show ? pour les options diskusage : afficher l'utilisation actuelle de l'espace disque time : afficher la date et l'heure actuelles du système faults : afficher les défaillances du module de sécurité, le cas échéant memoryusage : afficher l'utilisation de la mémoire système cpuinfo : afficher les informations sur le CPU du système users : afficher les utilisateurs connectés et leurs opérations uptime : afficher le temps de disponibilité du système slot : afficher le numéro de logement du SSP auquel cette lame est connectée processes : afficher tous les processus du système hosts : afficher les hôtes route : afficher les routes configurées interfaces : afficher les interfaces actuellement configurées version : afficher la version du produit netstat : afficher les connexions réseau vnicmap : afficher les cartes réseau virtuelles avec interfaces Ethernet platform : aucune memory : afficher la configuration du moniteur de mémoire disk : afficher la configuration du moniteur de disque cpu : afficher la configuration du moniteur de CPU ntp : afficher les informations de synchronisation de l'heure NTP coredump : afficher la configuration de coredump maxRestart : afficher maxRestart turboBoost : Afficher la configuration turboBoost services : afficher l'état des services process : afficher les détails du processus cgroups : afficher les cgroups tech-support : générer un rapport d'informations système à des fins de résolution de problèmes

Commande	Autres renseignements
config	Configurer le système. Saisir config ? pour les options vnic : configurer la carte réseau virtuelle spécifiée memory : configurer le moniteur de mémoire disk : configurer le moniteur de disque process : configurer le moniteur de CPU de processus maxRestart : configurer le nombre maximal de redémarrages CSP La valeur 0 doit désactiver la fonctionnalité. Valeur par défaut : 8 restartTimeInter : configurer le délai en secondes pour bloquer le démarrage de tous les CSP si le serveur redémarre maxRestart durant cet intervalle. Valeur par défaut : 1 200 restartCounters : réinitialiser le nombre de redémarrages coredump : configurer coredump {...} turboBoost : configurer turboBoost {...}
terminalLength	Paramètres du terminal. Saisir terminal ? pour les options enable : activer la longueur du terminal disable : désactiver la longueur du terminal
ping	Envoyer un message Ping à un hôte pour vérifier l'accessibilité *host*
nslookup	Rechercher une adresse IP ou un nom de domaines avec les serveurs DNS *host*
traceroute	Tracer la route vers un hôte distant *hôte*
connect	Se connecter à une console CSP spécifique (ASA, etc.) *appname apphost*

Commande	Autres renseignements
support	Opérations des fichiers système platform : opérations de plateforme fileupload : copier les fichiers d'archive vers MIO diagnostic : créer un fichier d'archive de diagnostic filelist : répertorier les fichiers existants dans les répertoires système fileview : afficher les fichiers du système filetail : suivre les fichiers du système deleteBootImage : supprimer l'image de démarrage certdownload : télécharger le certificat depuis le serveur syslog distant verify : vérifier l'image generate : prendre en charge la génération de {command..} tunnel : prendre en charge la tunnellisation de {command..} dplug-access : activer l'accès dplug send_diag_archiv : charger une archive par défaut vers MIO send_logs : charger les fichiers sélectionnés vers MIO
testcrashinfo	Tester la prise en charge des informations de plantage singleprocess : tester la prise en charge des informations de plantage avec un processus unique multiprocess : tester la prise en charge des informations de plantage avec plusieurs processus multithread : tester la prise en charge de plantage avec plusieurs fils
help	Obtenir de l'aide sur la syntaxe des commandes

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.