Mise en oeuvre de l'amélioration des fonctionnalités SNMP ASA

Contenu

Introduction

Ce document décrit les nouvelles fonctionnalités SNMP (Simple Network Management Protocol) disponibles pour le pare-feu de la gamme ASA 5500-X de Cisco dans les versions 9.1.5 et 9.2.1 et ultérieures du logiciel.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations de ce document sont basées sur le pare-feu de la gamme Cisco ASA 5500-X qui exécute le logiciel Cisco ASA® version 9.1.5 et 9.2.1 et ultérieures.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Dans les versions 9.1.5 et 9.2.1 d'ASA, ces améliorations SNMP sont présentées :

- La prise en charge de 128 hôtes SNMP est ajoutée.
- La prise en charge des identificateurs d'objet SNMP (OID) cpmCPUTotal5minRev est ajoutée.
- La prise en charge des messages SNMP de 1 472 octets est ajoutée.

Prise en charge de 128 hôtes SNMP

Cette fonctionnalité permet à l'ASA de prendre en charge plus que les 32 hôtes SNMP actuels.

Objectif

Actuellement, l'ASA a une limite de 32 hôtes SNMP au total. Cela inclut les hôtes qui peuvent être configurés pour les pièges et pour l'interrogation. Les sections suivantes décrivent les effets de cette fonction sur les modes à contexte unique et multicontexte.

Mode de contexte unique

- Permet de configurer un nombre d'entrées significativement plus élevé (nombre total d'hôtes), jusqu'à 4 096. Cependant, sur ces entrées, seulement 128 peuvent être utilisées pour des pièges.
- Pour la configuration des interrogations, jusqu'à 4 096 hôtes d'interrogation et 128 hôtes de déroutement sont autorisés à être configurés. Cependant, le nombre réel de serveurs qui interrogent le système doit être limité à moins de 128, car les impacts sur les performances d'un nombre plus élevé d'hôtes sont inconnus et ne sont pas pris en charge.

Mode multicontexte

- Aux fins de configuration, jusqu'à 4 000 hôtes par contexte sont autorisés et une limite de 64 000 hôtes au total est imposée à l'ensemble du système.
- Sur le total des hôtes configurés, seuls 128 (par contexte) peuvent être utilisés pour les interruptions et la limite système globale pour les interruptions en mode multicontexte est de

32 000.

- Bien que vous puissiez configurer jusqu'à 4 000 hôtes au total par contexte, le nombre réel de serveurs qui interrogent n'importe quel contexte doit être limité à 128.

Description

Vous pouvez préférer surveiller les périphériques réseau à partir d'un grand pool d'hôtes SNMP. Idéalement, vous souhaitez pouvoir spécifier une plage IP et/ou un sous-réseau des adresses IP autorisées à surveiller les périphériques réseau. L'ASA n'offre actuellement pas cette flexibilité et limite le nombre maximal d'hôtes SNMP à 32.

La prise en charge de cette fonctionnalité comporte deux aspects :

- Fournir la capacité de l'ASA à gérer jusqu'à 128 hôtes SNMP.

- Fournissez les commandes de configuration requises pour que vous puissiez configurer un nombre d'hôtes sensiblement plus élevé, comme indiqué dans la section précédente, via une seule commande.

La conception actuelle de l'ASA est telle que des hôtes individuels peuvent être configurés via l'interface de ligne de commande. Pour cette fonction, les exigences de conception supplémentaires suivantes ont été prises en compte :

- Introduction de la commande CLI **snmp-server host-group** avec rétention de commande CLI **snmp-server host**.

- Possibilité pour les entrées de venir à la fois des commandes CLI **snmp-server host-group** et **snmp-server host**.

- Pour SNMP Version 3, introduction de la commande CLI **snmp-server userlist** avec rétention de commande CLI **snmp-server user**.

- Un chevauchement de configuration doit également être pris en charge. Par exemple, les commandes **host-group** multiples peuvent être fournies avec des hôtes qui se chevauchent dans les objets réseau. De même, vous pouvez spécifier un hôte avec une adresse IP qui chevauche les hôtes actuels ou le groupe d'hôtes. Ceci fournit un mécanisme qui peut être utilisé afin de remplacer les paramètres de quelques hôtes dans un groupe, sans avoir à reconfigurer le groupe complet.

Certaines restrictions et restrictions logicielles associées à cette fonctionnalité sont les suivantes :

- Dans le cadre de la commande **snmp-server host-group**, la valeur par défaut est **poll** si **[trap|poll]** n'est pas spécifiée. Il est également important de noter que pour cette commande, les interceptions et les interrogations ne peuvent pas être activées pour le même groupe hôte. Si cela est nécessaire, Cisco vous recommande d'utiliser la commande **snmp-server host** pour les hôtes concernés.

- Vous pouvez spécifier des objets réseau qui se chevauchent dans différentes commandes **host-group**. Les valeurs spécifiées dans le dernier groupe d'hôtes prennent effet pour le jeu

commun d'hôtes des différents objets réseau.

Voici un exemple :

```
object network network1
range 64.103.236.40 64.103.236.50
object network network2
range 64.103.236.35 64.103.236.55

snmp-server host-group inside network1 poll version 3 user-list SNMP-List
snmp-server host-group inside network2 poll version 3 user-list SNMP-List
```

Entrez la commande **show snmp-server host** afin d'afficher les entrées d'hôte :

```
asa(config)# show snmp-server host
host ip = 64.103.236.35, interface = inside poll version 3 cisco1
host ip = 64.103.236.36, interface = inside  poll version 3 cisco1
host ip = 64.103.236.37, interface = inside  poll version 3 cisco1
host ip = 64.103.236.38, interface = inside  poll version 3 cisco1
host ip = 64.103.236.39, interface = inside  poll version 3 cisco1
host ip = 64.103.236.40, interface = inside  poll version 3 cisco1
host ip = 64.103.236.41, interface = inside  poll version 3 cisco1
host ip = 64.103.236.42, interface = inside  poll version 3 cisco1
host ip = 64.103.236.43, interface = inside  poll version 3 cisco1
host ip = 64.103.236.44, interface = inside  poll version 3 cisco1
host ip = 64.103.236.45, interface = inside  poll version 3 cisco1
host ip = 64.103.236.46, interface = inside  poll version 3 cisco1
host ip = 64.103.236.47, interface = inside  poll version 3 cisco1
host ip = 64.103.236.48, interface = inside  poll version 3 cisco1
host ip = 64.103.236.49, interface = inside  poll version 3 cisco1
host ip = 64.103.236.50, interface = inside  poll version 3 cisco1
host ip = 64.103.236.51, interface = inside  poll version 3 cisco1
host ip = 64.103.236.52, interface = inside  poll version 3 cisco1
host ip = 64.103.236.53, interface = inside  poll version 3 cisco1
host ip = 64.103.236.54, interface = inside  poll version 3 cisco1
host ip = 64.103.236.55, interface = inside  poll version 3 cisco1
```

Voici quelques remarques importantes sur l'utilisation de cette fonctionnalité :

- Si un groupe d'hôtes ou un hôte qui chevauche d'autres groupes d'hôtes est supprimé, les hôtes sont à nouveau configurés avec les valeurs utilisées pour les groupes d'hôtes configurés.
- Les valeurs ou paramètres associés aux hôtes dépendent de l'ordre dans lequel les commandes sont exécutées.
- La liste d'utilisateurs configurée ne peut pas être supprimée si elle est utilisée par un groupe d'hôtes particulier.
- L'utilisateur SNMP ne peut pas être supprimé si l'utilisateur est référencé dans une liste d'utilisateurs particulière.
- Un objet réseau ne peut pas être supprimé s'il est utilisé par la commande CLI **host-group**.

Configuration

Utilisez les informations décrites dans cette section afin de configurer l'ASA afin que cette nouvelle fonctionnalité soit implémentée.

> **Note**: Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Commandes CLI

Pour SNMP Version 3, l'administrateur peut associer différents utilisateurs à un groupe d'hôtes spécifié. Cela est utile si l'administrateur souhaite qu'un ensemble d'utilisateurs ait la possibilité d'accéder à l'ASA à partir d'un groupe d'hôtes. Cette commande CLI est utilisée afin de configurer une liste d'utilisateurs pour plusieurs utilisateurs :

```
ASA(config)# [no] snmp-server user-list
```

Afin d'associer la liste des utilisateurs à un groupe d'hôtes, entrez cette commande dans l'interface de ligne de commande :

```
[no] snmp-server host-group
```

Avec cette commande unique, vous pouvez spécifier un objet réseau afin d'indiquer les hôtes multiples qui doivent être ajoutés. Avec l'objet réseau, vous pouvez spécifier un masque de sous-réseau ou la plage d'adresses IP à ajouter, à l'aide d'une seule commande. Toutes les adresses IP répertoriées comme faisant partie de l'objet réseau sont ajoutées en tant qu'entrées d'hôte SNMP. De même, pour chacun des utilisateurs spécifiés dans la liste des utilisateurs, il existe une entrée hôte SNMP distincte.

Ces commandes sont utilisées afin de permettre aux administrateurs d'effacer et d'afficher les nouvelles options de configuration pour les serveurs SNMP :

- clear configure snmp-server user-list
- clear configure snmp-server host-group
- show running-config snmp-server user-list
- show running-config snmp-server host-group

Exemple de configuration

Complétez ces étapes afin d'utiliser les nouvelles options de groupe SNMP et de créer un groupe d'hôtes de serveur SNMP pour l'interrogation de la version 2c :

1. Créer un objet réseau :

```
asa(config)# object network network1
asa(config-network-object)# range 64.103.236.40 64.103.236.50
```

2. Définissez le groupe d'hôtes SNMP :

```
asa(config)#snmp-server host-group inside network1 poll community ***** version 2c
```

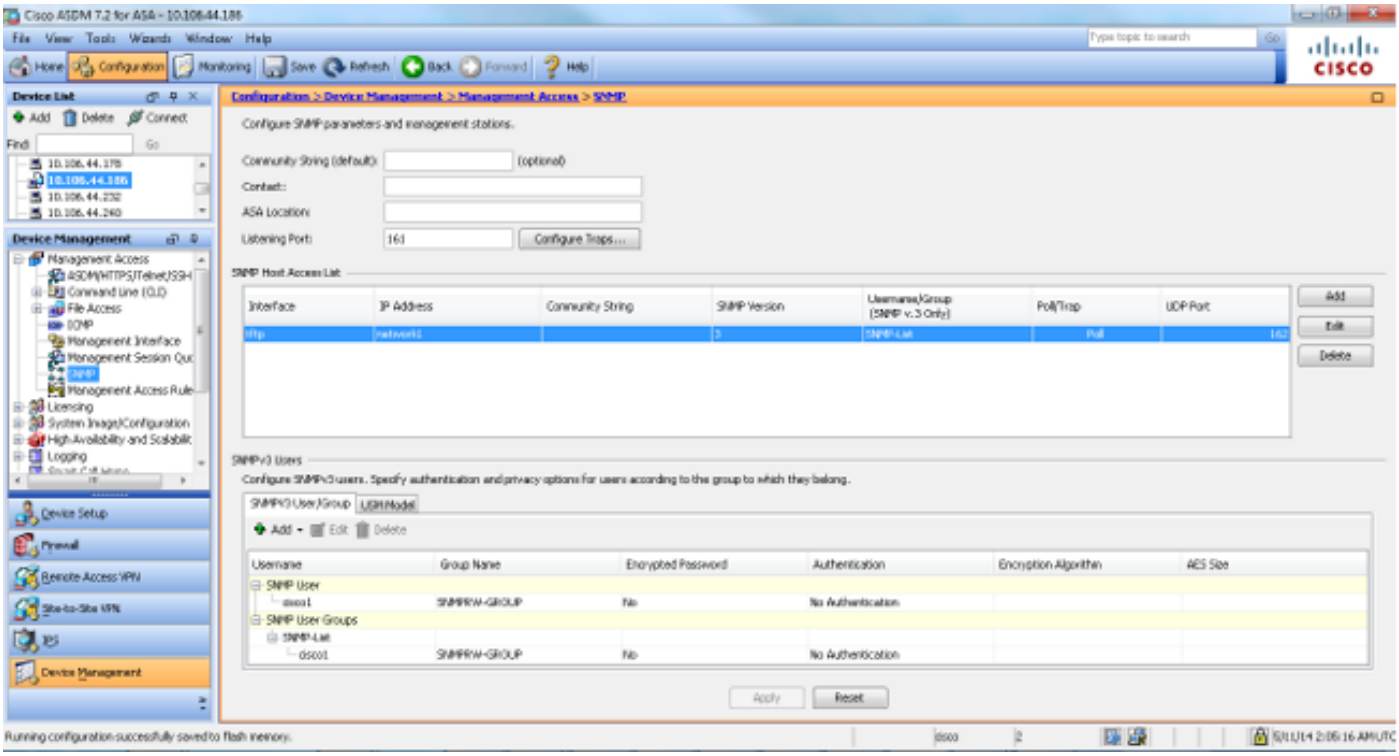
3. Définissez le groupe SNMP version 3 :

```
asa(config)#snmp-server group SNMPRW-GROUP v3 noauth
```

4. Associez les groupes aux utilisateurs :

```
asa(config)#snmp-server user cisco1 SNMPRW-GROUP v3
asa(config)#snmp-server user-list SNMP-List username cisco1
asa(config)#snmp-server host-group inside  network1 poll version 3 user-list SNMP-List
```

Cette image illustre les modifications apportées dans Cisco Adaptive Security Device Manager (ASDM) :



Prise en charge des OID SNMP cpmCPUTotal5minRev

Cette fonctionnalité permet à l'ASA de prendre en charge les OID SNMP **cpmCPUTotal5minRev**.

Objectif

Cette fonctionnalité ajoute la prise en charge des OID **cpmCPUTotal5minRev** et **cpmCPUTotal1minRev** sur l'ASA et désapprouve les OID actuellement pris en charge **cpmCPUTotal5min** et **cpmCPUTotal1min**. L'objectif de ces OID est de surveiller l'utilisation du processeur. Les OID actuellement pris en charge vont de 1 à 100, tandis que les OID nouvellement pris en charge vont de 0 à 100. C'est pourquoi des OID plus récents ont été pris en charge, car ils couvrent une plus large gamme.

Il est important de noter que puisque les OID déconseillés (**cpmCPUTotal5min** et **cpmCPUTotal1min**) ne sont plus pris en charge sur l'ASA, si l'ASA est mis à niveau et que les OID déconseillés sont interrogés, l'ASA ne renvoie aucune information pour ces OID. Après une mise à niveau de l'ASA, vous devez maintenant surveiller le **cpmCPUTotal5minRev** et **cpmCPUTotal1minRev** pour l'utilisation du CPU.

Commandes CLI

Aucune modification CLI n'a été introduite avec cette nouvelle fonctionnalité.

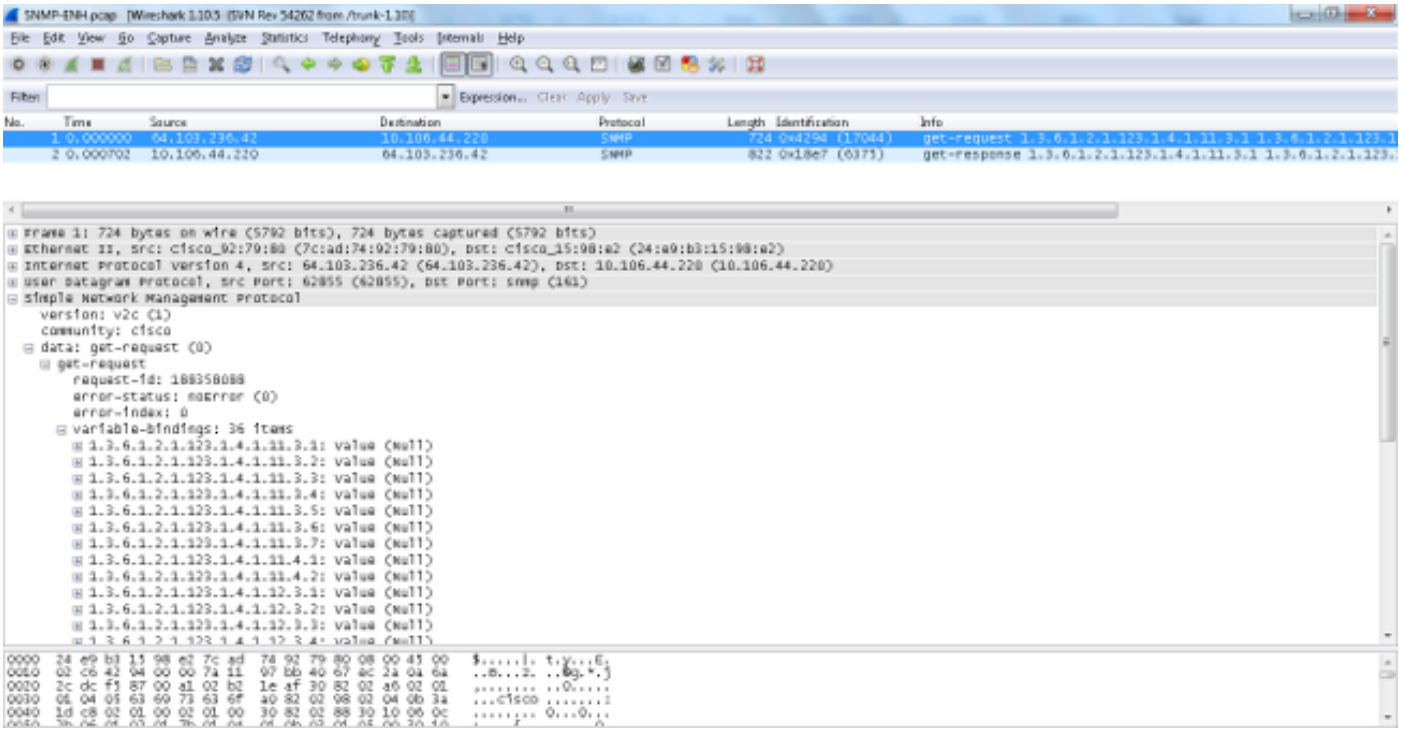
Nouveaux OID

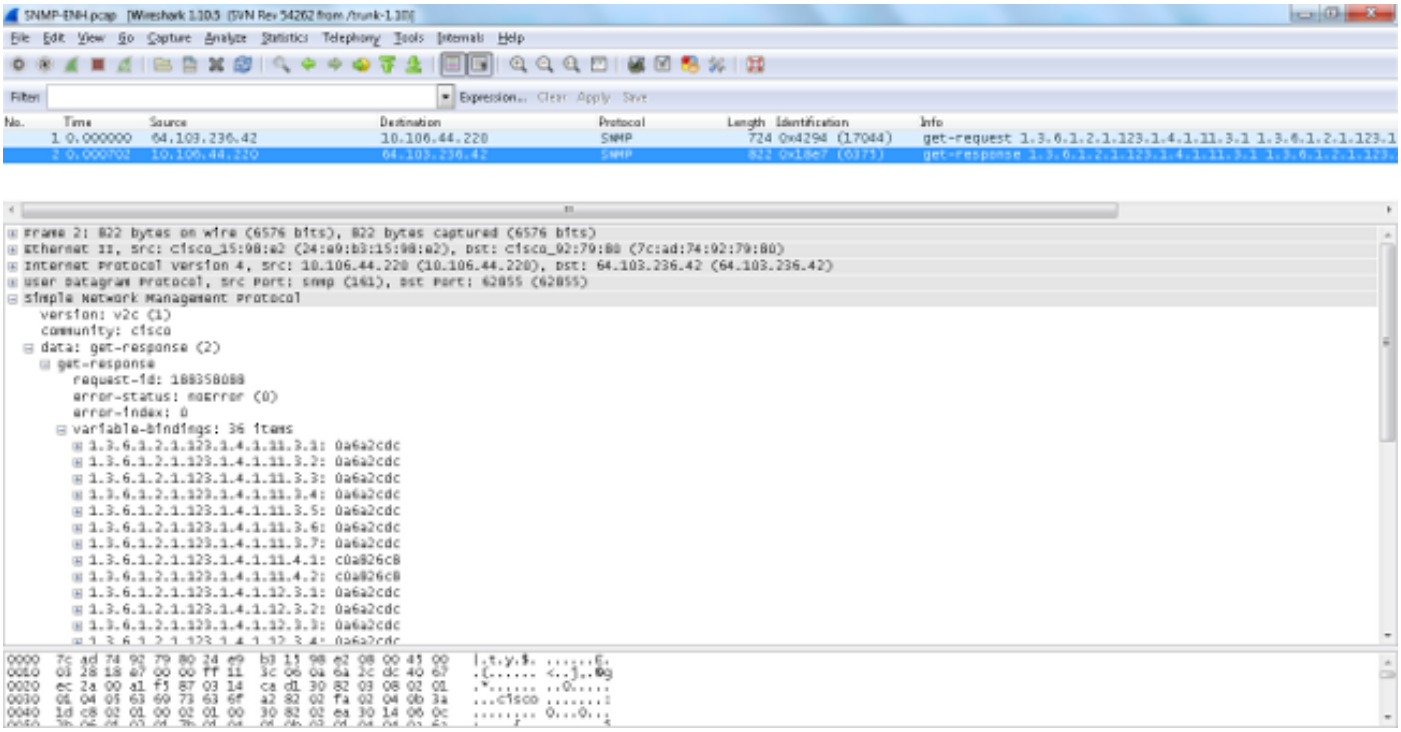
Voici les nouveaux OID ajoutés avec cette fonctionnalité :

- **1.3.6.1.4.1.9.9.109.1.1.1.1.7 . cpmCPUTotal1minRev**
- **1.3.6.1.4.1.9.9.109.1.1.1.1.8 . cpmCPUTotal5minRev**

Prise en charge des messages SNMP de 1 472 octets

Les plates-formes ASA limitent la taille de paquet maximale pour les requêtes SNMP à 512 octets. Lorsque vous exécutez une requête en masse pour un grand nombre d'OID MIB dans une seule requête SNMP, le délai de connexion SNMP et un syslog d'erreur sont générés sur l'ASA. Le RFC3417 suggère que la taille maximale de paquet pour les requêtes SNMP doit être de 1 472 octets. Il s'agit de la taille de la charge utile SNMP pour le paquet. En outre, l'en-tête Ethernet et la taille de l'en-tête IP doivent être ajoutés afin de calculer la taille totale du paquet.





Note: Cette fonctionnalité prend en charge les modes de contexte unique et de contexte multiple.

Dépannage

Cette section fournit des informations que vous pouvez utiliser afin de dépanner les problèmes système sur l'ASA.

Commandes show

Ces commandes **show** peuvent être utiles lorsque des tentatives sont faites pour résoudre des problèmes sur l'ASA :

- asa# **show run snmp-server host-group**
  snmp-server host-group inside network1 poll version 3 user-list SNMP-List
- asa# **show run snmp-server user-list**
  snmp-server user-list SNMP-List username cisco1
- asa# **show snmp-server host**

Cette commande CLI affiche les entrées présentes dans la table d'adresses du serveur SNMP, qui inclut les configurations de l'hôte et du groupe d'hôtes :

```
asa(config)#show run object network
object network network1
range 64.103.236.40 64.103.236.50
object network network2
range 64.103.236.35 64.103.236.55
```

```
object network network3
range 64.103.236.60 64.103.236.70

ciscoasa/admin(config)# show run snmp-server
snmp-server group cisco-group v3 noauth
snmp-server user user1 cisco-group v3
snmp-server user user2 cisco-group v3
snmp-server user user3 cisco-group v3
snmp-server user-list cisco username user1
snmp-server user-list cisco username user2
snmp-server user-list cisco username user3
snmp-server host-group management0/0 net2 poll version 3 user-list cisco
no snmp-server locationno snmp-server contact

ciscoasa/admin(config)# show snmp-server host
host ip = 64.103.236.35, interface = inside poll version 3 cisco1
host ip = 64.103.236.36, interface = inside  poll version 3 cisco1
host ip = 64.103.236.37, interface = inside  poll version 3 cisco1
host ip = 64.103.236.38, interface = inside  poll version 3 cisco1
host ip = 64.103.236.39, interface = inside  poll version 3 cisco1
host ip = 64.103.236.40, interface = inside  poll version 3 cisco1
host ip = 64.103.236.41, interface = inside  poll version 3 cisco1
host ip = 64.103.236.42, interface = inside  poll version 3 cisco1
```

Comme indiqué, ces commandes affichent tous les hôtes configurés via la commande **host-group**. Vous pouvez utiliser cette commande afin de vérifier si toutes les entrées sont disponibles et également vérifier de manière croisée les groupes hôtes qui se chevauchent.