

Contrôle d'accès basé sur les attributs

Les attributs sont des objets réseau personnalisés à utiliser dans votre configuration. Vous pouvez les définir et les utiliser dans les configurations ASA pour filtrer le trafic associé à une ou plusieurs machines virtuelles dans un environnement VMware ESXi géré par VMware vCenter. Les attributs vous permettent de définir des listes de contrôle d'accès (ACL) pour attribuer des politiques au trafic provenant de groupes de machines virtuelles partageant un ou plusieurs attributs. Vous attribuez des attributs aux machines virtuelles dans l'environnement ESXi et configurez un agent d'attribut, qui se connecte à vCenter ou à un seul hôte ESXi à l'aide du protocole HTTPS. L'agent demande et récupère ensuite une ou plusieurs liaisons qui mettent en corrélation des attributs spécifiques avec l'adresse IP principale d'une machine virtuelle.

Le contrôle d'accès basé sur les attributs est pris en charge sur toutes les plateformes matérielles et sur toutes les plateformes ASA virtuel fonctionnant sur les hyperviseurs ESXi, KVM ou HyperV. Les attributs ne peuvent être récupérés qu'à partir de machines virtuelles fonctionnant sur un hyperviseur ESXi.

- Lignes directrices relatives aux objets réseau basés sur les attributs, à la page 1
- Configurer le contrôle d'accès basé sur les attributs, à la page 2
- Surveillance des objets réseau basés sur les attributs , à la page 9
- Historique du contrôle d'accès basé sur les attributs, à la page 11

Lignes directrices relatives aux objets réseau basés sur les attributs

Lignes directrices pour IPv6

- Adresses IPv6 non prises en charge par vCenter pour les informations d'authentification de l'hôte.
- IPv6 est pris en charge pour les liaisons de machine virtuelle où l'adresse IP principale de la machine virtuelle est une adresse IPv6.

Lignes directrices et limites additionnelles

- Le mode multi-contexte n'est pas pris en charge. Les objets réseau basés sur les attributs sont pris en charge pour le contexte en mode unique uniquement.
- Les objets réseau basés sur les attributs prennent en charge uniquement la liaison à l'adresse principale de la machine virtuelle. La liaison à plusieurs vNIC sur une seule machine virtuelle n'est pas prise en charge.

- Les objets réseau basés sur les attributs ne peuvent être configurés que pour les objets utilisés pour les groupes d'accès. Les objets réseau pour d'autres fonctionnalités (NAT, etc.) ne sont pas pris en charge.
- Les machines virtuelles doivent exécuter les outils VMware afin de signaler les adresses IP principales à vCenter. L'ASA n'est pas informé des modifications d'attributs, sauf si vCenter sait l'adresse IP de la machine virtuelle. Il s'agit d'une restriction vCenter.
- Les objets réseau basés sur les attributs ne sont pas pris en charge dans les environnements Amazon Web Services (AWS) ou Microsoft Azure.

Configurer le contrôle d'accès basé sur les attributs

La procédure suivante fournit une séquence générale pour la mise en œuvre du contrôle d'accès basé sur les attributs sur les machines virtuelles gérées dans un environnement VMware ESXi.

Procédure

Étape 1 Attribuez des types d'attributs et des valeurs personnalisés à vos machines virtuelles gérées. Consultez Configurer les attributs des machines virtuelles vCenter, à la page 2.

Étape 2 Configurez un agent d'attributs pour une connexion à votre serveur vCenter ou à votre hôte ESXi. Consultez Configurer un agent d'attribut de VM, à la page 4.

Étape 3 Configurez les objets réseau basés sur les attributs nécessaires pour votre schéma de déploiement. Consultez Configurer les objets réseau basés sur les attributs, à la page 6.

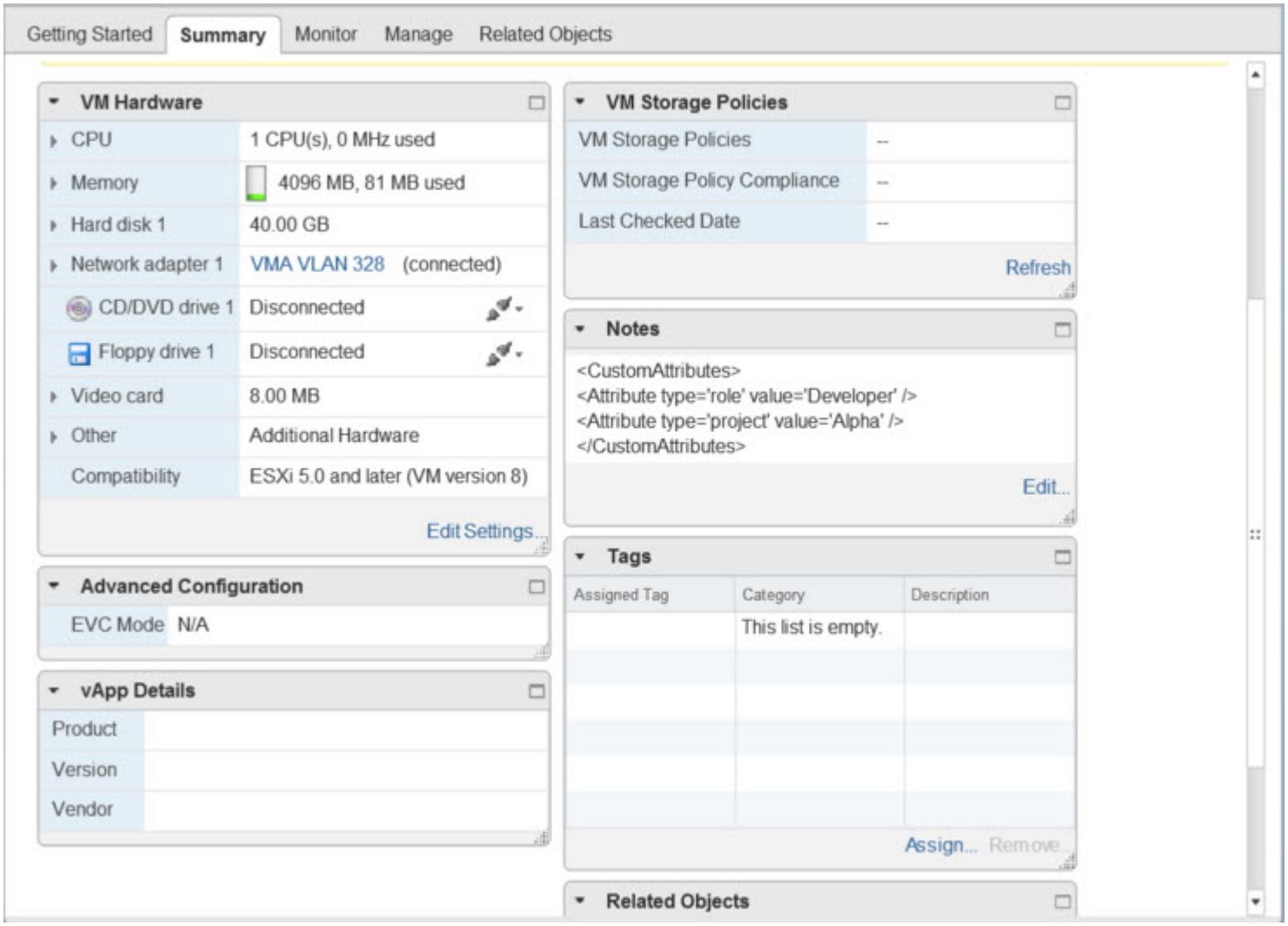
Étape 4 Configurez les listes de contrôle d'accès et les règles. Voir Configurer le contrôle d'accès à l'aide d'objets réseau basés sur les attributs, à la page 8 .

Configurer les attributs des machines virtuelles vCenter

Vous attribuez des types d'attributs et des valeurs personnalisés aux machines virtuelles et associez ces attributs aux objets réseau. Vous pouvez ensuite utiliser ces objets réseau basés sur des attributs pour appliquer des listes de contrôle d'accès à un ensemble de machines virtuelles ayant des caractéristiques communes définies par l'utilisateur. Par exemple, vous pouvez isoler les machines de version de développeur des machines de test, ou regrouper les machines virtuelles par projet et/ou emplacement. Pour que l'ASA surveille les machines virtuelles à l'aide des attributs, vous devez mettre les attributs à la disposition de vCenter à partir des machines virtuelles gérées. Vous le faites en insérant un fichier texte formaté dans le champ Notes, qui se trouve sur la page Summary (Résumé) des machines virtuelles dans vCenter.

Vous pouvez voir le champ Notes dans la figure suivante.

Illustration 1 : Onglet Summary (Résumé) d'une machine virtuelle dans vCenter



Pour spécifier des attributs personnalisés, vous copiez un fichier XML correctement formaté dans le champ Notes de la machine virtuelle. Le format du fichier est :

```
<CustomAttributes>
<Attribute type='attribute-type' value='attribute-value'/>
...
</CustomAttributes>
```

Une seule machine virtuelle peut avoir plusieurs attributs définis par la répétition de la deuxième ligne ci-dessus. Notez que chaque ligne doit identifier un type d'attribut unique. Si le même type d'attribut est défini avec plusieurs valeurs d'attribut, chaque mise à jour de liaison pour ce type d'attribut remplacera la précédente.

Pour les valeurs d'attribut de chaîne, la valeur associée à la définition d'objet doit correspondre exactement à la valeur signalée à vCenter par la machine virtuelle. Par exemple, une valeur d'attribut *Build Machine* ne correspond pas à la valeur d'inscription *build machine* sur la machine virtuelle. Aucune liaison ne sera ajoutée à la liste d'hôte pour cet attribut.

Vous pouvez définir plusieurs types d'attributs uniques dans un seul fichier.

Procédure

Étape 1 Sélectionnez la machine virtuelle dans votre inventaire vCenter.

Étape 2 Cliquez sur l'onglet **Summary** (Résumé) de la machine virtuelle.

Étape 3 Dans le champ **Notes**, cliquez sur le lien **de modification**.

Étape 4 Collez le fichier texte des attributs personnalisés dans la zone **Modifier les notes**. Le fichier texte doit suivre le format du modèle XML :

Exemple :

```
<CustomAttributes>
<Attribute type='attribute-type' value='attribute-value'/>
...
</CustomAttributes>
```

Étape 5 Cliquez sur **OK**.

Exemple

L'exemple suivant montre un fichier texte XML correctement formaté qui définit les attributs personnalisés du « Rôle » et du « Projet » que vous pouvez appliquer aux machines virtuelles :

```
<CustomAttributes>
<Attribute type='role' value='Developer'/>
<Attribute type='project' value='Alpha'/>
</CustomAttributes>
```

Configurer un agent d'attribut de VM

Vous configurez un agent d'attribut de VM pour communiquer avec vCenter ou un seul hôte ESXi. Lorsque vous attribuez des attributs aux machines virtuelles dans l'environnement VMware, l'agent d'attributs envoie un message à vCenter pour indiquer quels attributs ont été configurés, et vCenter répond par une mise à jour de liaison pour chaque machine virtuelle pour laquelle un type d'attribut correspondant est configuré.

L'agent d'attributs de VM et vCenter échangent des mises à jour de liaison comme suit :

- Si l'agent émet une demande contenant un nouveau type d'attribut, vCenter répond avec une mise à jour de liaison pour chaque machine virtuelle où le type d'attribut est configuré. Passé ce point, vCenter n'émet une nouvelle liaison que lorsqu'une valeur d'attribut est ajoutée ou modifiée.
- Si un attribut surveillé change pour une ou plusieurs machines virtuelles, un message de mise à jour de liaison est reçu. Chaque message de liaison est identifié par l'adresse IP de la machine virtuelle qui signale la valeur de l'attribut.
- Si plusieurs attributs sont surveillés par un seul agent, une seule mise à jour de liaison contient la valeur actuelle de tous les attributs surveillés pour chaque machine virtuelle.
- Si un attribut spécifique surveillé par l'agent n'est pas configuré sur une machine virtuelle, la liaison contiendra une valeur d'attribut vide pour cette machine virtuelle.

- Si une machine virtuelle n'a pas été configurée avec des attributs surveillés, vCenter n'envoie pas de mise à jour de liaison.

Chaque agent d'attribut communique avec exactement un hôte vCenter ou ESXi. Un seul ASA peut avoir plusieurs agents d'attributs définis, chacun communiquant avec un vCenter différent, ou un ou plusieurs communiquant avec le même vCenter.

Procédure

Étape 1 Créez l'agent d'attribut de VM pour communiquer avec vCenter : **attribute source-group** *agent-name* **type** *agent-type*

Exemple :

```
hostname(config)# attribute source-group VMAgent type esxi
```

L'argument *agent-name* spécifie le nom de l'agent de l'attribut VM. L'argument *de type* est le type d'agent d'attribut.

Remarque
Actuellement, ESXi est le seul type d'agent pris en charge.

Étape 2 Configurez les informations d'authentification de votre hôte vCenter : **host** *ip-address* **username** *ESXi-username* **password** *ESXi-password*

Exemple :

```
hostname(config-attr)# host 10.122.202.217 user admin password Cisco123
```

Étape 3 Configurez les paramètres Keepalive pour la communication avec vCenter : **keepalive retry-interval** *interval* **retry-count** *count*

Exemple :

```
hostname(config-attr)# keepalive retry-timer 10 retry-count 3
```

Les valeurs par défaut du temporisateur Keepalive sont de 3 tentatives à des intervalles de 30 secondes.

Étape 4 Examinez la configuration de l'agent de l'attribut VM : **show attribute source-group** *agent-name*

Exemple :

```
hostname(config-attr)# sh attribute source-group VMAgent

   Attribute agent VMAgent
   Agent type: ESXi
   Agent state: Inactive
   Connection state: Connected
   Host Address: 10.122.202.217
   Retry interval: 30 seconds
   Retry count: 3
```

Agent State (État de l'agent) reste inactif jusqu'à ce que vous configuriez un objet réseau et spécifiiez les attributs à associer à l'objet.

Étape 5 Quitter le mode de configuration des attributs : **exit**

Exemple :

```
hostname(config-attr)# exit
```

Configurer les objets réseau basés sur les attributs

Les objets réseau basés sur les attributs filtrent le trafic en fonction des attributs associés à une ou plusieurs machines virtuelles dans un environnement VMware ESXi. Vous pouvez définir des listes de contrôle d'accès (ACL) pour affecter des politiques au trafic provenant de groupes de machines virtuelles partageant un ou plusieurs attributs.

Par exemple, vous pouvez configurer des règles d'accès qui permettent aux machines ayant un attribut *engineering* d'accéder aux machines avec un attribut *eng_lab*. Un administrateur réseau peut ajouter ou supprimer des machines d'ingénierie et des serveurs de laboratoire pendant que la politique de sécurité gérée par l'administrateur de sécurité continue de fonctionner automatiquement sans mises à jour manuelles des règles d'accès.

Procédure

Étape 1 Activer la recherche de groupe d'objets : **object-group-search access-control**

Exemple :

```
hostname(config)# object-group-search access-control
```

Vous devez activer object-group-search pour configurer les objets réseau basés sur les attributs.

Étape 2 Créez ou modifiez un objet réseau basé sur les attributs en utilisant le nom de l'objet : **object network** *object-id*

Exemple :

```
hostname(config)# object network dev
```

Étape 3 Spécifiez un agent, le type d'attribut et la valeur d'attribut à associer à l'objet : **attribute** *agent-name attribute-type attribute-value*

Exemple :

```
hostname(config-network-object)# attribute VMAgent custom.role Developer
```

L'argument *agent-name* spécifie l'agent d'attribut de VM ; voir <XREF>. Si vous configurez un objet réseau basé sur les attributs pour utiliser un agent d'attribut qui n'a pas été configuré, un agent d'espace réservé est automatiquement créé sans informations d'authentification et avec des valeurs keepalive par défaut. Cet agent

reste dans l'état No credentials available (Aucun identifiant disponible) jusqu'à ce que les informations d'authentification de l'hôte soient fournies à l'aide de la sous-commande **host**.

Ensemble, la paire *attribute-type* et *attribute-value* définit un attribut unique. L'argument *attribute-type* est une chaîne arbitraire et doit inclure le préfixe **custom.** préfixe Si vous définissez le même type d'attribut plus d'une fois avec plusieurs valeurs d'attribut, la dernière valeur définie remplace la précédente.

Exemples

L'exemple suivant crée l'objet réseau basé sur les attributs *dev* pour un groupe de développement, avec le rôle de « Developer ». L'agent d'attribut de VM communique avec vCenter et renvoie toutes les liaisons de machine virtuelle qui correspondent à l'attribut *custom.role*.

```
hostname(config)# object network dev
hostname(config-network-object)# attribute VMAgent custom.role Developer
```

L'exemple suivant crée l'objet réseau basé sur les attributs *test* pour un groupe de tests, avec le rôle « Automation ». L'agent d'attribut de VM communique avec vCenter et renvoie toutes les liaisons de machine virtuelle qui correspondent à l'attribut *custom.role*. Notez qu'il s'agit de la même liste de machines virtuelles que dans l'exemple précédent :

```
hostname(config)# object network test
hostname(config-network-object)# attribute VMAgent custom.role Automation
```

L'exemple suivant crée l'objet réseau basé sur les attributs *project* pour un groupe de projets, avec le rôle « Alpha ». L'agent d'attribut de VM communique avec vCenter et renvoie toutes les liaisons de machine virtuelle qui correspondent à l'attribut *custom.project*. Notez que certaines machines chevauchent plus d'un attribut :

```
hostname(config)# object network project
hostname(config-network-object)# attribute VMAgent custom.project Alpha
```

L'exemple suivant montre un agent d'attributs de VM dans un état actif avec des demandes d'attributs en attente :

```
hostname(config-attr)# show attribute source-group VMAgent

   Attribute agent VMAgent
   Agent type: ESXi
   Agent state: Active
   Connection state: Connected
   Host Address: 10.122.202.217
   Retry interval: 30 seconds
   Retry count: 3
   Attribute requests pending:
       'custom.project'
       'custom.role'
```

Configurer le contrôle d'accès à l'aide d'objets réseau basés sur les attributs

Vous pouvez utiliser des objets réseau basés sur les attributs lorsque vous définissez des ACL (ACL) pour le trafic provenant de groupes de machines virtuelles partageant un ou plusieurs attributs. Les listes d'accès sont composées d'une ou de plusieurs entrées de contrôle d'accès (ACE). Une ACE est une entrée unique dans une liste d'accès qui spécifie une règle d'autorisation ou de refus (pour transférer ou abandonner le paquet). En règle générale, une règle d'autorisation ou de refus est appliquée à un protocole, à une adresse IP source et de destination ou à un réseau et, éventuellement, aux ports source et de destination.

Lorsque vous utilisez des objets réseau basés sur des attributs, vous pouvez remplacer les adresses IP de source et/ou de destination par ces objets. À mesure que les machines virtuelles sont déployées, déplacées ou retirées, les attributs peuvent être mis à jour sur les machines virtuelles tandis que les politiques de contrôle d'accès attribuées peuvent rester en vigueur sans modification de configuration.

Pour des informations complètes sur toutes les options disponibles pour les ACL, consultez Configurer les ACL.

Procédure

Étape 1 Créez et configurez une entrée d'ACL étendue (ACE) à l'aide d'objets réseau basés sur les attributs : **access-list** *access_list_name* **extended** {**deny | permit**} *protocol_argument* **object** *source_object_name* **object** *dest_object_name*

Exemple :

```
hostname(config)# access-list lab-access extended permit ip object dev object test
```

Remarque
Répétez l'opération autant de fois que nécessaire pour vos politiques.

Les options sont les suivantes :

- *access_list_name* : nom de la liste de contrôle d'accès nouvelle ou existante.
- Autoriser ou refuser : le mot-clé **deny** refuse ou exempte un paquet si les conditions sont remplies. Le mot-clé **permit** autorise ou inclut un paquet si les conditions correspondent.
- Protocole : *protocol_argument* spécifie le protocole IP.
  - *name* or *number* : spécifie le nom ou le numéro du protocole. Précisez **ip** pour appliquer à tous les protocoles.
  - **object-group** *protocol_grp_id* : spécifie un groupe d'objets de protocole créé à l'aide de la commande **object-group protocol**.
- Objet source :**object** spécifie un objet réseau basé sur les attributs créé à l'aide de la commande **object network**. Le *source_object_name* spécifie l'objet à partir duquel le paquet est envoyé.
- Objet de destination :**object** spécifie un objet réseau basé sur les attributs créé à l'aide de la commande **object network**. Le *dest_object_name* spécifie l'objet vers lequel le paquet est envoyé.

Étape 2 Lier l'ACL à une interface ou l'appliquer globalement : **access-group** *access_list_name* {**in interface** *interface_name* | **global**}

Exemple :

```
hostname(config)# access-group lab-access in interface inside
```

Pour un groupe d'accès spécifique à l'interface :

- Précisez le nom de l'ACL étendue. Vous pouvez configurer une commande **access-group** par type d'ACL et par interface.
- Le mot-clé **in** applique l'ACL au trafic entrant.
- Précisez le nom de l'**interface**.

Pour un groupe d'accès global, spécifiez le mot-clé **global** pour appliquer l'ACL étendue à la direction entrante de toutes les interfaces.

Exemple

L'exemple suivant montre comment appliquer globalement une liste de contrôle d'accès étendue basée sur des attributs :

```
hostname(config)# access-list lab-access extended permit ip object dev object test
hostname(config)# access-group lab-access global
hostname(config)# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list lab-access; 1 elements; name hash: 0x62b4790b
access-list lab-access line 1 extended permit ip object dev object test (hitcnt=0) 0x64a1be76

  access-list lab-access line 1 extended permit ip object dev(2) object test(3) (hitcnt=0)
 0x64a1be76
```

Surveillance des objets réseau basés sur les attributs

Pour surveiller les objets réseau basés sur les attributs, entrez les commandes suivantes :

- **show attribute host-map**

  Affiche les liaisons d'attribut pour l'agent, le type et la valeur d'un attribut donné.

- **show attribute object-map**

  Affiche les liaisons objet-attribut.

- **show attribute source-group**

  Affiche les agents d'attribut de VM configurés.

Exemples

L'exemple suivant montre une liste des liaisons hôtes-attributs :

```
hostname# show attribute host-map /all
IP Address-Attribute Bindings Information

         Source/Attribute                          Value
=========================================================================
VMAgent.custom.project                          'Alpha'
     10.15.28.34
     10.15.28.32
     10.15.28.31
     10.15.28.33
VMAgent.custom.role                             'Automation'
     10.15.27.133
     10.15.27.135
     10.15.27.134
VMAgent.custom.role                             'Developer'
     10.15.28.34
     10.15.28.12
     10.15.28.31
     10.15.28.13
```

L'exemple suivant montre un mappage des liaisons hôte-attribut :

```
hostname# show attribute object-map /all
Network Object-Attribute Bindings Information

Object
         Source/Attribute                          Value
=========================================================================
dev
     VMAgent.custom.role                          'Developer'
test
     VMAgent.custom.role                          'Automation'
project
     VMAgent.custom.project                       'Alpha'
```

L'exemple suivant montre la configuration de l'agent d'attributs :

```
hostname# show attribute source-group
   Attribute agent VMAgent
   Agent type: ESXi
   Agent state: Active
   Connection state: Connected
   Host Address: 10.122.202.217
   Retry interval: 30 seconds
   Retry count: 3
   Attributes being monitored:
      'custom.role' (2)
```

Historique du contrôle d'accès basé sur les attributs

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge des objets réseau basés sur les attributs	9.7(1)	Vous pouvez désormais contrôler l'accès réseau à l'aide des attributs de la machine virtuelle en plus des caractéristiques du réseau traditionnelles telles que les adresses IP, les protocoles et les ports. Les machines virtuelles doivent se trouver dans un environnement VMware ESXi. Nous avons introduit les commandes suivantes : **object network** *attribute* **attribute** *agent-name attribute-type attribute-value* **attribute source-group** *agent-name* **type** *agent-type* **host** *ip-address* **username** *ESXi-username* **password** *ESXi-password* **keepalive retry-interval** *interval* **retry-count** *count*
Suppression de la prise en charge des objets réseau basés sur les attributs de VM de l'ASA 5506-X (tous les modèles), 5508-X, 5512-X, 5516-X.	9.10(1)	Vous ne pouvez plus utiliser d'objets réseau basés sur des attributs de VM sur les plateformes suivantes : ASA 5506-X (tous les modèles), 5508-X, 5512-X, 5516-X.

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.

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.

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.

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.

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.