

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. Vous pouvez définir des listes de contrôle d'accès (ACL) pour affecter des politiques au trafic provenant de groupes de VM 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 virtuelles 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 7
- Historique du contrôle d'accès basé sur les attributs, à la page 7

Lignes directrices relatives aux objets réseau basés sur les attributs

Directives 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.

Directives 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 5.

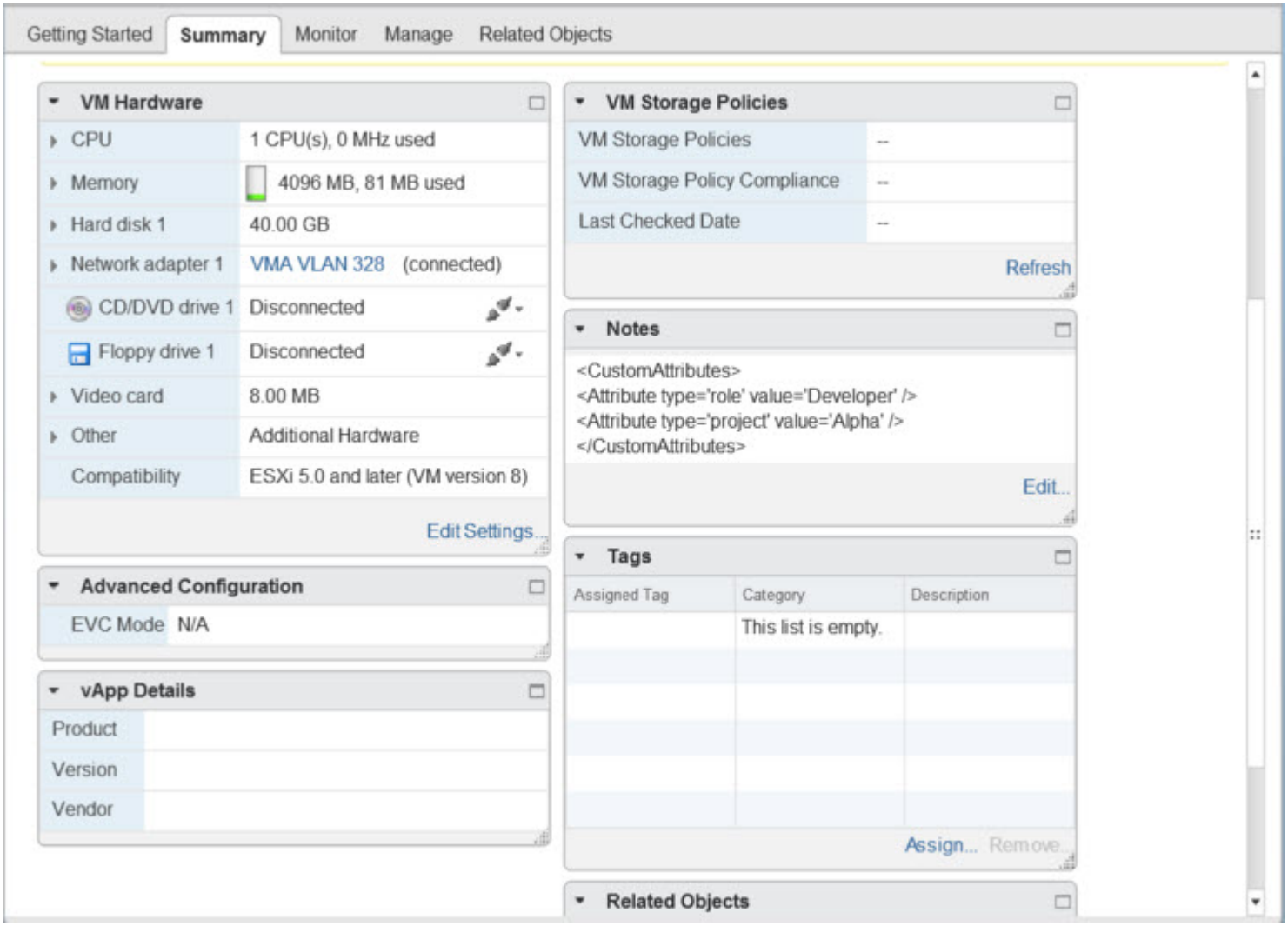
Étape 4 Configurez les listes de contrôle d'accès et les règles. Voir Configurer les règles d'accès à l'aide d'objets réseau basés sur les attributs, à la page 6 .

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**.

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 Choisissez **Configuration** > **Firewall (Pare-feu)** > **VM Attribute Agent (Agent d'attribut de VM)**.

Étape 2 Cliquez sur **Add** (ajouter).

Étape 3 Dans la zone Informations sur l'hôte :

a) Choisissez d'activer l'adresse IP et les informations d'authentification.
b) Saisissez le nom d'hôte ou l'adresse IP.
c) Saisir un nom d'utilisateur.
d) Sélectionnez le type de mot de passe : **Clear Text** (Texte en clair), **UnEncrypted** (Non chiffré) ou **Encrypted** (Chiffré).
e) Saisissez le mot de passe

Étape 4 Dans la zone d'informations Keepalive Information (Informations keepalive) :

a) Saisissez l' **intervalle de nouvelle tentative**. Saisissez une valeur entre 1 et 65 535. La valeur par défaut est 30.
b) Saisissez le **nombre de tentatives**. Saisissez une valeur entre 1 et 32. La valeur par défaut est de 3.

Étape 5 Cliquez sur **OK**.

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 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Access Rules (Règles d'accès)** > **Advanced Options (Options avancées)**.

Étape 2 Cochez la case **Enable Object Group Search Algorithm** (Activer l'algorithme de recherche de groupe d'objets).

Vous devez activer la recherche de groupe d'objets pour configurer les attributs de VM.

Étape 3 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Network Objects/Groups (Objets/groupes de services réseau)**.

Étape 4 Effectuez l'une des opérations suivantes :

- Choisissez **Add (Ajouter) > Network Object Attributes (Attributs d'objet réseau)** pour ajouter un nouvel objet réseau basé sur les attributs. Saisissez un nom et, éventuellement, une description.
- Choisissez un objet réseau existant basé sur les attributs et cliquez sur **Edit** (Modifier).

Étape 5 Pour un nouvel objet réseau basé sur les attributs, saisissez des valeurs dans les champs suivants :

a) **Agent Name** (Nom de l'agent) : cliquez sur le bouton de navigation et sélectionnez un agent d'attribut de VM (ou définissez-en un nouveau).

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.

b) **Attribute Type** (Type d'attribut) : cette entrée de chaîne définit le type d'attribut et doit inclure le préfixe **custom**. Par exemple, custom.role.

c) **Attribute Value** (Valeur d'attribut) : cette entrée de chaîne associe une valeur au type d'attribut.

Ensemble, la paire *Attribute Type (Type d'attribut)* et *Attribute Value (Valeur d'attribut)* définit un attribut unique. Cela vous permet de définir plusieurs attributs qui correspondent à votre schéma de déploiement particulier. Si vous définissez le même type d'attribut plus d'une fois avec plusieurs valeurs d'attribut, la dernière valeur définie remplace la précédente.

Étape 6 Cliquez sur **OK**.

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

Pour appliquer une règle d'accès à l'aide d'objets réseau basés sur des attributs, procédez comme suit.

Procédure

Étape 1 Choose **Configuration** > **Firewall (Pare-feu)** > **Access Rules (Règles d'accès)**.

Les règles sont classées par interface et direction, avec un groupe distinct pour les règles globales. Si vous configurez des règles d'accès de gestion, elles sont répétées sur cette page. Ces groupes sont équivalents à la liste de contrôle d'accès étendue qui est créée et affectée à l'interface ou globalement en tant que groupe d'accès. Ces ACL apparaissent également sur la page ACL Manager (Gestionnaire d'ACL).

Étape 2 Effectuez l'une des actions suivantes :

- Pour ajouter une nouvelle règle, choisissez Add (Ajouter) **> Add Access Rule** (Ajouter une règle d'accès).
- Pour insérer une règle à un emplacement spécifique dans un conteneur, sélectionnez une règle existante et choisissez **Add (Ajouter) > Insert (Insérer)** pour ajouter la règle au-dessus, ou choisissez **Add (Ajouter) > Insert After (Insérer après)**.
- Pour modifier une règle, sélectionnez-la et cliquez sur **Edit** (Modifier).

Étape 3 Renseignez les propriétés de la règle. Les principales options à sélectionner sont les suivantes :

- **Interface** : l'interface à laquelle la règle s'applique. Sélectionnez Any (Tous) pour créer une règle globale. Pour les groupes de ponts en mode routé, vous pouvez créer des règles d'accès pour l'interface virtuelle de pont (BVI) et chaque interface de membre de groupe de ponts.
- **Action : Permit/Deny (Autoriser/Refuser)** : précisez si vous autorisez le trafic décrit ou si vous le bloquez.
- **Source/Destination criteria** (Critères source/destination) : sélectionnez l'objet réseau basé sur l'attribut source (objet d'origine) et l'objet réseau basé sur l'attribut de destination (objet cible du flux de trafic). Vous pouvez également préciser un nom d'utilisateur ou de groupe d'utilisateurs pour la source. En outre, vous pouvez utiliser le champ Service pour identifier le type spécifique de trafic si vous souhaitez cibler la règle de manière plus étroite que tout le trafic IP. Si vous mettez en œuvre Cisco TrustSec, vous pouvez utiliser des groupes de sécurité pour définir la source et la destination.

Pour des informations détaillées sur les options, consultez Propriétés de la règle d'accès.

Lorsque vous avez terminé de définir la règle, cliquez sur **OK** pour l'ajouter au tableau.

Étape 4 Cliquez sur **Apply** (Appliquer) pour enregistrer la règle d'accès dans votre configuration.

Surveillance des objets réseau basés sur les attributs

Pour les objets réseau basés sur des attributs, vous pouvez analyser l'utilisation d'un objet individuel. À partir de leur page dans le dossier **Configuration > Firewall (Pare-feu) > Objects (Objets) > Network Objects/Groups (Objets/groupes réseau)**, cliquez sur le bouton **Where Used** (Où utilisé).

Pour les objets réseau basés sur des attributs, vous pouvez également cliquer sur le bouton Not Used (Non utilisé) pour rechercher les objets qui ne sont utilisés dans aucune règle. Cet affichage vous donne un raccourci pour supprimer ces objets inutilisés.

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 ou modifié les écrans suivants : **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Network Object Attributes (Attributs d'objet réseau)**. Nous avons introduit l'écran suivant : **Configuration** > **Firewall** (Pare-feu) > VM **Attribute Agent (Agent d'attributs de VM)** .

Nom de la caractéristique	Versions de plateforme	Description
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.