Guide de mise en œuvre de Symantec™ Network Access Control Enforcer

Guide de mise en œuvre de Symantec Network Access Control Enforcer

Version de documentation 11.00.03.01.00

Mentions légales

présentation ou communication du Logiciel sous licence et de la documentation par le gouvernement des Etats-Unis ne peut se faire que conformément aux conditions du présent contrat.

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014 Etats-Unis

http://www.symantec.fr

Support technique

Le support technique de Symantec met à jour des centres de support globalement. Le rôle primaire du support technique est de réagir aux requêtes spécifiques au sujet des fonctions et de la fonctionnalité d'un produit. Le groupe de support technique crée également le contenu pour notre base de données en ligne. Le groupe de support technique travaille en collaboration avec les autres domaines fonctionnels de Symantec pour répondre à vos questions en temps utile. Par exemple, le groupe de support technique travaille avec l'ingénierie de produit et Symantec Security Response pour fournir des services d'alerte et des mises à jour de définitions de virus.

Les offres de maintenance de Symantec incluent ce qui suit :

- Un intervalle des options de support qui vous donnent la flexibilité de sélectionner la bonne quantité de service pour les sociétés de toutes tailles
- Le support est pris en charge par téléphone et sur Internet et fournit une réponse rapide et les informations de dernière minute
- L'assurance de mise à niveau fournit la protection de la mise à niveau de logiciels automatique
- Prise en charge globale est disponible 24 heures sur 24, 7 jours sur 7
- Dispositifs avancés, y compris la gestion de compte Services

Pour plus d'informations au sujet des programmes de maintenance de Symantec, vous pouvez visiter notre site Web sur l'URL suivante :

www.symantec.com/techsupp/

Contacter le support technique

Les clients avec un contrat de maintenance en cours peuvent accéder aux informations de support technique sur l'URL suivante :

www.symantec.com/techsupp/

Avant de contacter le support technique, vérifiez que vous répondez à la configuration requise indiquée dans la documentation du produit. En outre, nous vous conseillons être devant l'ordinateur sur lequel le problème se pose, au cas où il serait nécessaire de répliquer le problème.

Quand vous entrez en contact avec le support technique, ayez les informations disponibles suivantes en votre possession :

- Niveau de version du produit
- Les informations sur l'équipement

- Mémoire disponible, espace disque et informations NIC
- Système d'exploitation
- Version et niveau de correctif
- Topologie réseau
- Routeur, passerelle et informations d'Adresse IP
- Description du problème :
  - Messages d'erreur et fichiers journaux
  - Dépannage effectué avant de contacter Symantec
  - Les modifications récentes de la configuration logicielle et les modifications réseau

Programme de licences et d'enregistrement

Si votre produit Symantec requiert un enregistrement ou une clé de licence, accédez à notre page Web de support technique à l'URL suivante :

www.symantec.com/techsupp/

Service client

Les informations du service client sont disponibles sur l'URL suivante :

www.symantec.com/techsupp/

Le service client est disponible pour aider avec les types de problèmes suivants :

- Questions concernant le programme de licences ou la numérotation de produit
- Mises à jour d'enregistrement de produit, telles que l'adresse ou les changements de nom
- Les informations générales sur le produit (fonctions, disponibilité de langue, distributeurs locaux)
- Les dernières informations sur les mises à jour et les mises à niveau du produit
- Informations sur l'assurance et les contrats de maintenance de mise à niveau
- Informations sur les Programmes d'achats Symantec
- Conseil sur les options du support technique Symantec
- Questions non techniques d'avant-vente
- Problèmes liés au CD-ROM ou aux manuels

Ressources de contrat de maintenance

Si vous voulez entrer en contact avec Symantec concernant un contrat de maintenance existant, veuillez contactez l'équipe administrative de contrat de maintenance pour votre région comme suit :

Asie Pacifique et Japon	contractsadmin@symantec.com
Europe, Moyen-Orient et Afrique	semea@symantec.com
Amérique du Nord et Amérique latine	supportsolutions@symantec.com

Services d'entreprise supplémentaires

Symantec offre un ensemble complet de services qui vous permettent d'optimiser votre investissement dans les produits Symantec et de développer votre connaissance, expertise et perspicacité globale, pour vous permettre de gérer vos risques d'affaires de manière proactive.

Les services destinés aux entreprises disponibles incluent ce qui suit :

Symantec Early Warning Solutions	Ces solutions fournissent l'alerte instantanée des cyberattaques, de l'analyse de menace complète et les contre-mesures qui empêchent les attaques avant qu'elles se produisent.
Services de supervision de la sécurité	Ces services suppriment la charge que représente la gestion et le contrôle des périphériques et des événements de sécurité, assurant l'intervention rapide face aux menaces réelles.
Services de conseil	Les services de conseil Symantec fournissent l'expertise technique sur site de Symantec et de ses partenaires approuvés. Les services de conseil Symantec offrent une série d'options préemballées et personnalisables qui incluent l'évaluation, la conception, la mise en place, la surveillance et les fonctions de gestion. Chacun se concentré pour établir et mettre à jour l'intégrité et la disponibilité de vos ressources informatiques.
Services éducatif	Les services éducatifs fournissent un ensemble complet de formation technique, d'éducation de sécurité, de certification de sécurité et de programmes de communication de connaissance.

Pour accéder à plus d'informations sur les services destinés aux entreprises, visitez s'il vous plaît notre site Web sur l'URL suivante :

www.symantec.com

Sélectionnez votre pays ou langue dans le sommaire du site.

Contacter le support technique

Les clients avec un contrat de maintenance en cours peuvent accéder aux informations de support technique sur l'URL suivante :

www.symantec.com/techsupp/

Avant de contacter le support technique, vérifiez que vous répondez à la configuration requise indiquée dans la documentation du produit. En outre, nous vous conseillons être devant l'ordinateur sur lequel le problème se pose, au cas où il serait nécessaire de répliquer le problème.

Quand vous entrez en contact avec le support technique, ayez les informations disponibles suivantes en votre possession :

- Niveau de version du produit
- Les informations sur l'équipement
- Mémoire disponible, espace disque et informations NIC
- Système d'exploitation
- Version et niveau de correctif
- Topologie réseau
- Routeur, passerelle et informations d'Adresse IP
- Description du problème :
  - Messages d'erreur et fichiers journaux
  - Dépannage effectué avant de contacter Symantec
  - Les modifications récentes de la configuration logicielle et les modifications réseau

Programme de licences et d'enregistrement

Si votre produit Symantec requiert un enregistrement ou une clé de licence, accédez à notre page Web de support technique à l'URL suivante :

www.symantec.com/techsupp/

Service client

Les informations du service client sont disponibles sur l'URL suivante :

www.symantec.com/techsupp/

Le service client est disponible pour aider avec les types de problèmes suivants :

- Questions concernant le programme de licences ou la numérotation de produit

- Mises à jour d'enregistrement de produit, telles que l'adresse ou les changements de nom
- Les informations générales sur le produit (fonctions, disponibilité de langue, distributeurs locaux)
- Les dernières informations sur les mises à jour et les mises à niveau du produit
- Informations sur l'assurance et les contrats de maintenance de mise à niveau
- Informations sur les Programmes d'achats Symantec
- Conseil sur les options du support technique Symantec
- Questions non techniques d'avant-vente
- Problèmes liés au CD-ROM ou aux manuels

Ressources de contrat de maintenance

Si vous voulez entrer en contact avec Symantec concernant un contrat de maintenance existant, veuillez contactez l'équipe administrative de contrat de maintenance pour votre région comme suit :

Asie Pacifique et Japon	contractsadmin@symantec.com
Europe, Moyen-Orient et Afrique	semea@symantec.com
Amérique du Nord et Amérique latine	supportsolutions@symantec.com

Services d'entreprise supplémentaires

Symantec offre un ensemble complet de services qui vous permettent d'optimiser votre investissement dans les produits Symantec et de développer votre connaissance, expertise et perspicacité globale, pour vous permettre de gérer vos risques d'affaires de manière proactive.

Les services destinés aux entreprises disponibles incluent ce qui suit :

Symantec Early Warning Solutions	Ces solutions fournissent l'alerte instantanée des cyberattaques, de l'analyse de menace complète et les contre-mesures qui empêchent les attaques avant qu'elles se produisent.
Services de supervision de la sécurité	Ces services suppriment la charge que représente la gestion et le contrôle des périphériques et des événements de sécurité, assurant l'intervention rapide face aux menaces réelles.

Services de conseil	Les services de conseil Symantec fournissent l'expertise technique sur site de Symantec et de ses partenaires approuvés. Les services de conseil Symantec offrent une série d'options préemballées et personnalisables qui incluent l'évaluation, la conception, la mise en place, la surveillance et les fonctions de gestion. Chacun se concentré pour établir et mettre à jour l'intégrité et la disponibilité de vos ressources informatiques.
Services éducatif	Les services éducatifs fournissent un ensemble complet de formation technique, d'éducation de sécurité, de certification de sécurité et de programmes de communication de connaissance.

Pour accéder à plus d'informations sur les services destinés aux entreprises, visitez s'il vous plaît notre site Web sur l'URL suivante :

www.symantec.com

Sélectionnez votre pays ou langue dans le sommaire du site.

Table des matières

Section 1

Installer et configurer des boîtiers Symantec Network Access Control Enforcer

- Interface de ligne de commande de boîtier Enforcer
- Référence d'interface de ligne de commande de boîtier Enforcer
- Dépanner un boîtier Enforcer
- Questions fréquemment posées au sujet des boîtiers Gateway Enforcer, DHCP Enforcer ou LAN Enforcer

Chapitre 1

Présentation du boîtier Enforcer

Ce chapitre traite des sujets suivants :

A propos des boîtiers Symantec Enforcer

Les modules Enforcer Symantec sont des composants de réseau facultatifs qui fonctionnent avec Symantec Endpoint Protection Manager.

Les boîtiers Symantec Enforcer basés sur Linux suivants fonctionnent avec des clients réseau, tels que les clients Symantec Endpoint Protection et Symantec Network Access Control, pour protéger le réseau d'entreprise :

- Boîtier Symantec Network Access Control Gateway Enforcer
- Boîtier Symantec Network Access Control DHCP Enforcer
- Boîtier Symantec Network Access Control LAN Enforcer

Tous les boîtiers Symantec Enforcer basés sur Windows fonctionnent avec les clients réseau, tels que les clients Symantec Endpoint Protection et Symantec Network Access Control, pour protéger le réseau d'entreprise.

Remarque : Symantec Network Access Control Integrated Enforcer pour Microsoft Network Access Protection ne fonctionne pas avec les clients invités, tels que les clients Symantec Network Access Control On-Demand sur les plates-formes Windows et Macintosh.

Les instructions d'installation, de configuration et d'administration sont comprises dans la documentation pour les modules d'application Enforcer basés sur Windows suivants :

- Symantec Network Access Control Integrated Enforcer pour serveurs DHCP Microsoft
  Se reporter à "A propos de Symantec NAC Integrated Enforcer pour serveurs DHCP Microsoft" à la page 331.
- Symantec Network Access Control Integrated Enforcer pour Microsoft Network Access Protection
  Se reporter à "A propos du module d'application Integrated Enforcer pour Microsoft Network Access Protection" à la page 401.
- Symantec Network Access Control Integrated DHCP Enforcer pour serveurs DHCP Alcatel-Lucent VitalQIP®
  Se reporter à "A propos d'Integrated Enforcer for Alcatel-Lucent VitalQIP DHCP Servers (Integrated Lucent Enforcer)" à la page 349.

Public visé

La documentation est destinée à toute personne responsable de l'installation et du déploiement d'un boîtier Enforcer facultatif. Les lecteurs doivent avoir une bonne compréhension des concepts de réseau et être familiarisés avec l'administration de Symantec Endpoint Protection Manager.

Le boîtier Enforcer facultatif fonctionne uniquement avec des versions spécifiques d'autres composants.

Se reporter à "A propos de la mise à niveau et de la migration des images de boîtier Enforcer vers la version 11.0.3000" à la page 73.

Si vous avez l'intention d'utiliser un boîtier Enforcer facultatif avec une version précédente de Symantec Network Access Control, consultez la documentation fournie avec le boîtier Enforcer au moment de l'achat.

Types d'application

Tableau 1-1 liste les boîtiers Enforcer facultatifs et les modules d'application Enforcer basés sur Windows.

Tableau 1-1 Types d'application

Type de boîtier Enforcer	Description
Boîtier Symantec Gateway Enforcer	Fournit l'application aux points d'accès pour les ordinateurs externes qui se connectent à distance par une des méthodes suivantes : ■ Virtual private network (VPN) ■ Réseau sans fil local ■ Serveur d'accès distant (RAS) Un boîtier Gateway Enforcer peut également être configuré pour limiter l'accès à certains serveurs en autorisant seulement les adresses IP spécifiées. Symantec Gateway Enforcer est pris en charge sur les boîtiers Enforcer. Se reporter à "Fonctionnement du boîtier Gateway Enforcer" à la page 39. Se reporter à "Planification d'installation pour un boîtier Gateway Enforcer" à la page 48.
Boîtier Symantec LAN Enforcer	Fournit l'application pour les clients qui se connectent au réseau par un commutateur ou un point d'accès sans fil qui prend en charge l'authentification 802.1x. Le boîtier LAN Enforcer agit en tant que proxy RADIUS (Remote Authentication Dial-In User Service). Il peut fonctionner avec ou sans un serveur RADIUS qui fournit l'authentification au niveau utilisateur. Symantec LAN Enforcer est pris en charge sur les boîtiers Enforcer. Se reporter à "Fonctionnement du boîtier LAN Enforcer" à la page 41. Se reporter à "Planification d'installation pour un boîtier LAN Enforcer" à la page 68.

Type de boîtier Enforcer	Description
Boîtier Symantec DHCP Enforcer	Fournit l'application pour les clients qui accèdent au réseau. Les clients reçoivent une adresse IP dynamique par l'intermédiaire d'un serveur DHCP (Dynamic Host Configuration Protocol). Symantec DHCP Enforcer est pris en charge sur un boîtier Enforcer. Se reporter à "Fonctionnement du boîtier DHCP Enforcer" à la page 40. Se reporter à "Planification d'installation pour un boîtier DHCP Enforcer" à la page 59.
Symantec Integrated Enforcer pour serveurs DHCP Microsoft	Fournit l'application pour les clients qui accèdent au réseau. Les clients reçoivent une adresse IP dynamique par un serveur DHCP (Dynamic Host Configuration Protocol). Symantec Integrated DHCP Enforcer est pris en charge sur la plate-forme Windows. Symantec Integrated Enforcer pour serveurs DHCP Microsoft n'est pas pris en charge sur les boîtiers Enforcer. Se reporter à "Fonctionnement d'un module d'application Integrated Enforcer pour serveurs DHCP Microsoft" à la page 332. Se reporter à "Planification de l'emplacement d'un module d'application Integrated Enforcer pour serveurs DHCP Microsoft" à la page 339.
Symantec Integrated Enforcer pour Microsoft Network Access Protection	Fournit l'application pour les clients qui accèdent au réseau. Les clients reçoivent une adresse IP dynamique ou passent l'authentification 802.1x par l'intermédiaire d'un serveur DHCP (Dynamic Host Configuration Protocol). Symantec Integrated NAP Enforcer est pris en charge sur la plate-forme Windows Server 2008. Symantec Integrated Enforcer pour Microsoft Network Access Protection n'est pas pris en charge sur les boîtiers Enforcer.
Symantec Integrated Enforcer for Alcatel-Lucent VitalQIP DHCP Servers	Fournit l'application pour les clients qui accèdent au réseau. Les clients reçoivent une adresse IP dynamique ou passent l'authentification 802.1x par l'intermédiaire d'un serveur DHCP (Dynamic Host Configuration Protocol). Symantec Integrated DHCP Enforcer est pris en charge sur la plate-forme Windows. Symantec Integrated DHCP Enforcer pour serveurs DHCP Alcatel-Lucent VitalQIP n'est pas pris en charge sur les boîtiers Enforcer.

Opérations possibles avec les boîtiers Symantec Network Access Control Enforcer

Le boîtier Enforcer facultatif s'installe aux extrémités réseau pour les clients externes ou internes.

Par exemple, vous pouvez installer un boîtier Enforcer entre le réseau et un serveur VPN ou devant un serveur DHCP. Vous pouvez également l'installer pour l'application sur les ordinateurs client qui se connectent au réseau par un commutateur compatible 802.1x ou un point d'accès sans fil.

Le boîtier Enforcer effectue l'authentification de l'hôte plutôt que l'authentification au niveau utilisateur. Il vérifie que les ordinateurs client qui essayent de se connecter au réseau d'entreprise sont conformes aux politiques de sécurité de l'entreprise. Vous pouvez configurer les politiques de sécurité d'une entreprise sur la console Symantec Endpoint Protection Manager.

Si le client ne se conforme pas aux politiques de sécurité, le boîtier Enforcer peut prendre les mesures suivantes :

- Bloquer son accès au réseau.
- Lui fournir l'accès à des ressources limitées seulement.

Le boîtier Enforcer facultatif peut rediriger le client vers une zone de quarantaine avec un serveur de résolution. Le client peut alors obtenir les logiciels, les applications, les fichiers de signature ou les correctifs requis auprès du serveur de résolution.

Par exemple, une partie d'un réseau peut être déjà configurée pour les clients qui se connectent au réseau local par des commutateurs compatibles 802.1x. Dans ce cas, vous pouvez utiliser un boîtier LAN Enforcer pour ces clients.

Vous pouvez également utiliser un boîtier LAN Enforcer pour les clients qui se connectent par un point d'accès sans fil compatible 802.1x.

Se reporter à "Fonctionnement du boîtier LAN Enforcer" à la page 41.

Se reporter à "Planification d'installation pour un boîtier LAN Enforcer" à la page 68.

Vous pouvez avoir d'autres parties du réseau qui ne sont pas configurées pour la prise en charge de type 802.1x. Vous pouvez utiliser un boîtier DHCP Enforcer pour gérer l'application pour ces clients.

Se reporter à "Fonctionnement du boîtier DHCP Enforcer" à la page 40.

Se reporter à "Planification d'installation pour un boîtier DHCP Enforcer" à la page 59.

Si vous avez des employés qui travaillent à distance et se connectent par un VPN ou à distance, vous pouvez utiliser le boîtier Gateway Enforcer pour ces clients.

Vous pouvez également utiliser le boîtier Gateway Enforcer si un point d'accès sans fil n'est pas compatible 802.1x.

Se reporter à "Fonctionnement du boîtier Gateway Enforcer" à la page 39.

Se reporter à "Planification d'installation pour un boîtier Gateway Enforcer" à la page 48.

Si la haute disponibilité est requise, vous pouvez installer plusieurs boîtiers Gateway, DHCP ou LAN Enforcer au même emplacement pour assurer le basculement.

Se reporter à "Planifier le basculement pour les boîtiers Gateway Enforcer" à la page 55.

Se reporter à "Planifier le basculement pour les boîtiers DHCP Enforcer" à la page 64.

Se reporter à "Planifier le basculement pour les boîtiers LAN Enforcer" à la page 71.

Si vous souhaitez mettre en œuvre la haute disponibilité pour les boîtiers LAN Enforcer, vous devez en installer plusieurs avec un commutateur compatible 802.1x. La haute disponibilité est rendue possible grâce à ce commutateur. Si vous installez uniquement les boîtiers LAN Enforcer, la haute disponibilité échoue. Vous pouvez configurer le commutateur compatible 802.1x pour la haute disponibilité.

Pour plus d'informations sur la configuration d'un commutateur compatible 802.1x pour la haute disponibilité, consultez la documentation d'accompagnement du commutateur.

Dans certaines configurations réseau, un client peut se connecter au réseau par plus d'un boîtier Enforcer. Tous les boîtiers Enforcer successifs doivent authentifier le client à la suite du premier pour que le client puisse se connecter au réseau.

A propos des politiques d'intégrité de l'hôte et le boîtier Enforcer

Les polices de sécurité que tous les boîtiers Enforcer vérifient sur les ordinateurs client sont appelées politiques d'intégrité de l'hôte. Ces politiques d'Intégrité de l'hôte sont créées et gérées sur une console Symantec Endpoint Protection Manager.

Les politiques d'intégrité de l'hôte spécifient le logiciel qui est requis pour s'exécuter sur un client. Vous pouvez par exemple spécifier que le logiciel de

sécurité suivant, situé sur un ordinateur client, doit être conforme à certaines conditions :

- Logiciel antivirus
- Logiciel antispyware
- Logiciel pare-feu
- Correctifs
- Service packs

Si les conditions pré-définies ne répondent pas à vos besoins, vous pouvez également personnaliser les conditions.

Consultez le *Guide d'administration pour Symantec Endpoint Protection et Symantec Network Access Control* pour plus d'informations sur la configuration et la personnalisation des politiques d'intégrité de l'hôte.

Vous pouvez configurer des clients pour exécuter des vérifications de l'intégrité de l'hôte à diverses heures. Quand un client essaye de se connecter au réseau, il exécute une vérification de l'intégrité de l'hôte. Il envoie ensuite les résultats à un boîtier Enforcer.

Généralement, le boîtier Enforcer est configuré pour vérifier que l'ordinateur client réussit la vérification d'intégrité de l'hôte avant d'accorder l'accès réseau au client. Si le client passe la vérification de l'intégrité de l'hôte, il est conforme à la politique d'intégrité de l'hôte dans votre entreprise. Toutefois, chaque type de boîtier Enforcer définit différemment les critères d'accès au réseau.

Se reporter à "Fonctionnement du boîtier Gateway Enforcer" à la page 39.

Se reporter à "Fonctionnement du boîtier DHCP Enforcer" à la page 40.

Se reporter à "Fonctionnement du boîtier LAN Enforcer" à la page 41.

Communiquer entre un boîtier Enforcer et Symantec Endpoint Protection Manager

Le boîtier Enforcer reste connecté à Symantec Endpoint Protection Manager. A intervalles réguliers (nommés battement), le boîtier Enforcer récupère les paramètres du serveur de gestion qui contrôle son fonctionnement. Lorsque vous apportez des modifications sur le serveur de gestion qui affectent le boîtier Enforcer, le boîtier Enforcer reçoit la mise à jour pendant le battement suivant. Le boîtier Enforcer transmet ses informations d'état au serveur de gestion. Il peut consigner les événements qu'il transmet au serveur de gestion. Les informations apparaissent alors dans les journaux sur le serveur de gestion.

Symantec Endpoint Protection Manager conserve une liste de serveurs de gestion avec les informations de base de données répliquées. Il télécharge la liste de serveurs de gestion vers les modules d'application Enforcer connectés, les clients réseau et les clients invités. Si le boîtier Enforcer perd la communication avec un serveur de gestion, il peut se connecter à un autre serveur de gestion inclus dans la liste de serveurs de gestion. Si le boîtier Enforcer est redémarré, il utilise la liste de serveurs de gestion pour établir une nouvelle connexion à un serveur de gestion.

Quand un client essaye de se connecter au réseau par le boîtier Enforcer, le boîtier Enforcer authentifie l'identificateur unique (UID) du client. Le boîtier Enforcer envoie l'UID au serveur de gestion et reçoit une réponse d'approbation ou de refus.

Si un boîtier Enforcer est configuré pour authentifier l'UID, il peut récupérer des informations du serveur de gestion. Il peut alors déterminer si le profil du client a été mis à jour avec les dernières politiques de sécurité. Si les informations client, telles que l'identifiant client ou le profil client, sont modifiées sur le serveur de gestion, le serveur de gestion peut envoyer ces informations au boîtier Enforcer. Le boîtier Enforcer peut effectuer une nouvelle authentification d'hôte sur le client.

Communication entre le boîtier Enforcer et les clients

La communication entre Enforcer et un client démarre au moment où le client essaie de se connecter au réseau. Le boîtier Enforcer peut détecter si un client est en cours d'exécution. Si un client s'exécute, Enforcer commence la procédure d'authentification par le client. Le client réagit en exécutant une vérification de l'intégrité de l'hôte et en envoyant les résultats, avec ses données de profil, à Enforcer.

Le client envoie également son identificateur unique (UID), qu'Enforcer transmet au Manager pour l'authentification. Le boîtier Enforcer utilise les informations de profil pour vérifier si le client est mis à jour avec les dernières politiques de sécurité. Si ce n'est pas le cas, Enforcer informe le client de la nécessité de mettre à jour son profil.

Une fois que le boîtier DHCP Enforcer ou Gateway Enforcer autorise la connexion du client au réseau, la communication se poursuit à un intervalle prédéfini régulier. Cette communication permet au boîtier Enforcer de continuer l'authentification du client. Pour le boîtier LAN Enforcer, c'est le commutateur 802.1x qui gère cette authentification périodique. Par exemple, le commutateur 802.1 démarre une nouvelle session d'authentification il est temps d'effectuer une réauthentification.

Le boîtier Enforcer doit être constamment exécuté. Sinon, le client essayant de se connecté au réseau d'entreprise peut être bloqué.

Fonctionnement du boîtier Gateway Enforcer

Les boîtiers Gateway Enforcer exécutent une vérification à sens unique. Ils vérifient les clients qui essayent de se connecter au réseau de la compagnie par l'intermédiaire de la carte d'interface réseau externe du boîtier Gateway Enforcer.

Un boîtier Gateway Enforcer utilise les processus suivants pour authentifier un client :

- Quand un client tente d'accéder au réseau, le boîtier Gateway Enforcer vérifie d'abord si le client exécute le client Symantec Endpoint Protection ou le client Symantec Network Access Control. Si le client exécute l'un des logiciels clients, le boîtier Gateway Enforcer commence la procédure d'authentification d'hôte.
- Le client qui s'exécute sur l'ordinateur d'un utilisateur exécute une vérification de l'intégrité de l'hôte. Il transmet alors les résultats au boîtier Gateway Enforcer avec ses informations d'identification et les informations sur l'état de sa politique de sécurité.
- Le boîtier Gateway Enforcer vérifie avec Symantec Endpoint Protection Manager que le client est un client légitime et que sa politique de sécurité est à jour.
- Le boîtier Gateway Enforcer vérifie que le client a réussi la vérification d'intégrité de l'hôte et est donc conforme aux politiques de sécurité.
- Si tous les processus réussissent, le boîtier Gateway Enforcer permet au client de se connecter au réseau.

Si un client ne répond pas aux exigences pour l'accès, le boîtier Gateway Enforcer peut être configuré pour exécuter les actions suivantes :

- Surveiller et consigner certains événements.
- Bloquer les utilisateurs si la vérification d'intégrité de l'hôte échoue.
- Afficher un message instantané sur le client.
- Fournir au client un accès limité au réseau pour permettre d'utiliser les ressources réseau pour la résolution.

Pour configurer l'authentification du boîtier Gateway Enforcer, vous pouvez configurer les adresses IP client à contrôler. Vous pouvez spécifier les adresses IP externes approuvées que le boîtier Enforcer permet sans authentification. Pour la résolution, vous pouvez configurer le boîtier Gateway Enforcer pour permettre l'accès de clients à des adresses IP internes approuvées. Par exemple, vous pouvez permettre à des clients d'avoir accès à un serveur de mise à jour ou à un serveur de fichiers contenant les fichiers DAT de l'antivirus.

Pour des clients sans logiciel Symantec, vous pouvez rediriger des requêtes HTTP client vers un serveur Web. Par exemple, vous pouvez fournir d'autres instructions

sur la manière d'obtenir un logiciel de résolution ou autoriser un client à télécharger un logiciel client.

Vous pouvez également configurer le boîtier Gateway Enforcer pour permettre à des clients non Windows d'accéder au réseau. Le boîtier Gateway Enforcer fonctionne comme un pont plutôt que comme un routeur. Dès que le client est authentifié, le boîtier Gateway Enforcer transfère des paquets pour permettre au client d'accéder au réseau.

Fonctionnement du boîtier DHCP Enforcer

Le boîtier DHCP Enforcer est utilisé en ligne comme pont d'application de politique sécurisé pour protéger un réseau interne. Les clients qui tentent de se connecter au réseau envoient une requête DHCP d'adresse IP dynamique. Le commutateur ou le routeur, qui agit en tant que client de relais DHCP, achemine la requête DHCP au boîtier DHCP Enforcer. Le boîtier DHCP Enforcer est configuré en ligne devant le serveur DHCP. Avant d'acheminer la requête DHCP au serveur DHCP, le boîtier Enforcer vérifie que les clients sont conformes aux politiques de sécurité.

Si un client est conforme aux politiques de sécurité, le boîtier DHCP Enforcer envoie la demande d'adresse IP du client au serveur DHCP normal. Si l'agent n'est pas conforme aux politiques de sécurité, Enforcer le connecte au serveur DHCP de quarantaine. Le serveur de quarantaine affecte le client à une configuration réseau de quarantaine.

Vous pouvez installer un serveur DHCP sur un ordinateur et le configurer pour fournir une configuration réseau normale et une configuration réseau de quarantaine. Pour finaliser la solution de boîtier DHCP Enforcer, l'administrateur doit configurer un serveur de résolution. Le serveur de résolution restreint l'accès des clients mis en quarantaine afin que ces clients ne puissent interagir qu'avec le serveur de résolution. Si une haute disponibilité est requise, vous pouvez installer deux boîtiers DHCP Enforcer ou plus pour fournir des fonctions de basculement.

DHCP Enforcer applique des politiques de sécurité sur les clients qui essayent d'accéder à un serveur DHCP. Il ne bloque pas la requête DHCP si l'authentification client échoue. Le boîtier DHCP Enforcer transmet la requête DHCP à un serveur DHCP de quarantaine pour une configuration réseau de plage restreinte sur le court terme.

Lorsque le client envoie la requête DHCP, le boîtier DHCP Enforcer la transmet au serveur DHCP de quarantaine pour une adresse IP temporaire avec un bail court. Le boîtier DHCP Enforcer peut alors commencer son processus d'authentification avec le client.

Le boîtier DHCP Enforcer authentifie les clients au moyen de l'une des méthodes suivantes :

- Lorsqu'un client tente d'accéder au réseau d'entreprise, le boîtier Enforcer vérifie d'abord si l'ordinateur client exécute le logiciel client Symantec Network Access Control. Si l'ordinateur client exécute le logiciel client Symantec Network Access Control, le boîtier Enforcer commence le processus d'authentification d'hôte.
- Le logiciel client Symantec exécuté sur l'ordinateur client réalise une vérification d'intégrité d'hôte. Le client transmet alors les résultats au boîtier Enforcer avec ses informations d'identification et les informations sur l'état de sa politique de sécurité.
- Le boîtier DHCP Enforcer vérifie avec Symantec Endpoint Protection Manager que le client est un client légitime et que sa politique de sécurité est à jour.
- Le boîtier DHCP Enforcer vérifie que le client a réussi la vérification d'intégrité de l'hôte et est donc conforme aux politiques de sécurité.
- Si toutes les étapes sont réussies, le boîtier DHCP Enforcer s'assure que l'adresse IP de quarantaine est libérée. Le boîtier DHCP Enforcer envoie alors la requête DHCP client au serveur DHCP normal. Le client reçoit alors une adresse IP normale et une configuration réseau.

Si le client ne satisfait pas les conditions de sécurité, le boîtier DHCP Enforcer s'assure que la requête DHCP est renouvelé avec le serveur DHCP de quarantaine. Le client reçoit une configuration réseau de quarantaine, qui doit être configurée pour permettre l'accès à un serveur de résolution.

Le boîtier DHCP Enforcer peut être configuré pour permettre à des clients non-Windows d'avoir accès au serveur DHCP normal.

Fonctionnement du boîtier LAN Enforcer

Le boîtier LAN Enforcer agit en tant que proxy RADIUS (Remote Authentication Dial-In User Service).

Vous pouvez utiliser le boîtier LAN Enforcer avec un serveur RADIUS pour exécuter les actions suivantes :

- Effectuer l'authentification utilisateur traditionnelle 802.1x/EAP.
  Vous refusez l'accès réseau aux ordinateurs nuisibles. Tous les utilisateurs qui essayent de se connecter au réseau doivent d'abord s'authentifier par le biais du serveur RADIUS.
- Vérifier que les ordinateurs client sont conformes aux politiques de sécurité définies sur le serveur de gestion (authentification de l'hôte).

Vous pouvez imposer des politiques de sécurité, par exemple s'assurer que l'ordinateur contient le logiciel antivirus, les correctifs ou tout autre logiciel approprié. Vous pouvez confirmer que l'ordinateur client exécute le client Symantec et qu'il a réussi la vérification d'intégrité de l'hôte.

Dans les réseaux qui n'utilisent pas de serveur RADIUS, le boîtier LAN Enforcer effectue seulement l'authentification de l'hôte.

Le boîtier LAN Enforcer communique avec un commutateur ou un point d'accès sans fil qui prend en charge l'authentification EAP/802.1x. Le commutateur ou le point d'accès sans fil est souvent configuré en deux ou plusieurs réseaux locaux virtuels (VLAN). Les clients Symantec sur les ordinateurs client transmettent les informations EAP ou les informations pour la vérification d'intégrité de l'hôte au commutateur en utilisant le protocole EAPOL (EAP sur réseau local). Le commutateur fait suivre les informations au boîtier LAN Enforcer pour authentification.

Vous pouvez configurer le boîtier LAN Enforcer avec un ensemble de réponses possibles à un échec d'authentification. Les réponses dépendent du type d'échec d'authentification : authentification de l'hôte ou authentification utilisateur EAP.

Si vous utilisez un commutateur ou un point d'accès sans fil, vous pouvez configurer le boîtier LAN Enforcer pour qu'il dirige un client authentifié vers différents VLAN. Le commutateur ou le point d'accès sans fil doit fournir la fonction VLAN dynamique. Les VLAN peuvent inclure un VLAN de résolution.

Si vous utilisez LAN Enforcer avec un serveur RADIUS, vous pouvez configurer des connexions de serveur RADIUS multiples pour Enforcer. Si une connexion de serveur RADIUS est en panne, LAN Enforcer peut commuter sur une autre connexion. En outre, plusieurs boîtiers LAN Enforcer peuvent être configurés pour se connecter au commutateur. Si un boîtier LAN Enforcer ne réagit pas, un autre boîtier LAN Enforcer peut prendre en charge l'authentification.

Fonctionnement de la configuration de base de LAN Enforcer

Si vous êtes familier avec l'authentification 802.1x, vous pouvez afficher des détails au sujet des clients qui essayent d'accéder au réseau en utilisant la configuration de base. Vous pouvez utiliser ces informations pour le dépannage des connexions réseau.

Dans sa configuration de base, l'application réseau 802.1x fonctionne de la manière suivante :

- Un supplicant (par exemple, un ordinateur client) essaye d'accéder au réseau par un dispositif d'authentification (par exemple, un commutateur 802.1x).
- Le commutateur voit l'ordinateur et demande une identification.

- Le supplicant 802.1x sur l'ordinateur demande à l'utilisateur un nom d'utilisateur et un mot de passe et réagit avec son identification.
- Le commutateur fait suivre ces informations à LAN Enforcer, qui les transfère alors au serveur RADIUS.
- Le serveur RADIUS génère un défi EAP en sélectionnant un type EAP basé sur sa configuration.
- LAN Enforcer reçoit ce défi, ajoute un défi d'Intégrité de l'hôte et fait suivre au commutateur.
- Celui-ci fait suivre l'EAP et les défis d'Intégrité de l'hôte au client.
- Le client reçoit les défis et envoie une réponse.
- Le commutateur reçoit la réponse et la fait suivre à LAN Enforcer.
- LAN Enforcer examine le résultat de la vérification d'intégrité de l'hôte et les informations d'état de client et les fait suivre au serveur RADIUS.
- Le serveur RADIUS effectue l'authentification EAP et renvoie le résultat à LAN Enforcer.
- LAN Enforcer reçoit les résultats d'authentification et fait suivre le résultat et l'action à effectuer.
- Le commutateur sélectionne l'action appropriée et permet l'accès normal au réseau, en bloquant ou en permettant l'accès à un VLAN alternatif selon les résultats.

Fonctionnement du mode transparent de LAN Enforcer

Le mode transparent de LAN Enforcer fonctionne des manières suivantes :

- Un supplicant (par exemple, un ordinateur client) essaye d'accéder au réseau par un dispositif d'authentification (par exemple, un commutateur 802.1x).
- Le dispositif d'authentification voit l'ordinateur et envoie un paquet d'authentification d'EAP (trafic EAP seul permis).
- Le client servant de supplicant EAP voit le paquet d'authentification et répond avec l'authentification d'intégrité de l'hôte.
- Le commutateur envoie les résultats d'authentification d'intégrité d'hôte pour le boîtier LAN Enforcer exécuté en serveur RADIUS Proxy.
- Le boîtier LAN Enforcer répond au commutateur avec les informations d'affectations VLAN correspondant aux résultats de l'authentification.

A propos de l'authentification 802.1x

IEEE 802.1X-2001 est une norme qui définit le contrôle d'accès pour les réseaux sans fil et câblés. La norme fournit une architecture pour authentifier et contrôler le trafic des utilisateurs sur un réseau protégé. La norme spécifie l'utilisation du protocole d'authentification extensible (EAP), qui utilise un serveur d'authentification centralisé, tel que RADIUS (Remote Authentication Dial-In User Service).

Le serveur authentifie chaque utilisateur qui essaye d'accéder au réseau. La norme 802.1x inclut les spécifications d'EAP sur réseau local (EAPOL). EAPOL est utilisé pour encapsuler des messages EAP dans des trames de couche liaison (par exemple Ethernet) et fournit également des fonctions de contrôle.

L'architecture 802.1x inclut les composants clés suivants :

Dispositif d'authentification	Entité en charge de l'authentification, tel que le point d'accès sans fil ou le commutateur LAN conforme 802.1x.
Serveur d'authentification	Entité fournissant l'authentification, c-à-d. qui valide les coordonnées fournies en réponse à la demande, par exemple un serveur RADIUS.
Supplicant	Entité recherchant un accès réseau et essayant d'effectuer une authentification avec succès, par exemple un ordinateur.

Quand un périphérique de supplicant est connecté à un commutateur réseau d'authentification avec 802.1x activé, le processus suivant se produit :

- Le commutateur émet une demande d'identité EAP.
- Le logiciel de supplicant EAP répond avec une Identité Réponse EAP, qui est transférée au serveur d'authentification (par exemple RADIUS) par le commutateur.
- Le serveur d'authentification émet un défi EAP, qui est transféré au supplicant par le commutateur.
- L'utilisateur entre les coordonnées d'authentification (nom d'utilisateur, mot de passe, jeton, etc.).
- Le supplicant envoie une Réponse Défi EAP, incluant les informations d'authentification fournies par l'utilisateur, au commutateur qui la fait suivre au serveur d'authentification.
- Le serveur d'authentification valide les informations d'authentification et répond avec un résultat EAP ou d'authentification utilisateur, ce qui indique la réussite ou l'échec de l'authentification.

- Si l'authentification réussit, le commutateur accorde l'accès pour le trafic normal. Si l'authentification échoue, l'accès du périphérique client est bloqué. Le supplicant est avisé du résultat dans l'un ou l'autre cas.

Seul le trafic EAP est autorisé pendant la procédure d'authentification

Pour obtenir des détails sur EAP, consultez le RFC 2284 de IETF à l'URL suivante :

http://www.ietf.org/rfc/rfc2284.txt

Pour des informations supplémentaires sur la norme IEEE 802.1x, consultez le texte de la norme sur l'URL suivante :

http://standards.ieee.org/getieee802/download/802.1x-2001.pdf

Prise en charge de solutions d'application tierces

Symantec fournit des solutions d'application pour les éditeurs tiers suivants :

- API d'application universelle
  Symantec a développé l'API d'application universelle pour permettre à d'autres fournisseurs possédant une technologie apparentée d'intégrer leurs solutions avec le logiciel de Symantec.
- Cisco Network Admissions Control
  Les clients Symantec peuvent prendre en charge la solution d'application Cisco Network Admissions Control.

Informations supplémentaires sur les modules d'application Symantec Enforcer

Tableau 1-2 liste les diverses sources d'informations sur les tâches associées éventuellement nécessaires avant ou après l'installation d'un boîtier Enforcer.

Tableau 1-2 Documentation de Symantec Enforcer

Document de module Enforcer	Utilisation
Guide d'installation Symantec Endpoint Protection et Symantec Network Access Control	Décrit comment installer Symantec Endpoint Protection Manager, le client Symantec Endpoint Protection et les clients Symantec Network Access Control. Il explique également la configuration de la base de données Microsoft SQL intégrée et l'installation de la réplication.

Document de module Enforcer	Utilisation
Guide d'administration de Symantec Endpoint Protection et Symantec Network Access Control	Décrit comment configurer et gérer Symantec Endpoint Protection Manager ainsi que les clients Symantec Endpoint Protection et Symantec Network Access Control. Il décrit également l'installation des politiques d'intégrité de l'hôte utilisées par le module d'application Enforcer pour mettre en application la conformité sur les ordinateurs client.
Guide client de Symantec Endpoint Protection et de Symantec Network Access Control	Décrit comment utiliser les clients Symantec Endpoint Protection et Symantec Network Access Control.
Guide de mise en œuvre de Symantec™ Network Access Control Enforcer	Décrit comment installer et gérer tous les types des boîtiers de Symantec Network Access Control et de modules d'application Enforcer intégrés. Explique également comment utiliser les clients à la demande pour Macintosh et Linux.
Aide en ligne	Explique comment utiliser Symantec Endpoint Protection Manager ainsi que les clients Symantec Endpoint Protection et Symantec Network Access Control. Explique également l'utilisation de chacun des modules d'application Enforcer intégrés.
Aide en ligne pour les clients à la demande	Explique comment utiliser les clients à la demande Macintosh et Linux.
Aide de l'interface de ligne de commande de module Enforcer	Fournit de l'aide lorsque vous appuyez sur la touche ? de l'interface de ligne de commande.
fichier readme.txt	Comprend les dernières informations sur les défauts critiques liés au module d'application Enforcer pouvant également affecter Symantec Endpoint Protection Manager.

Chapitre 2

Planifier l'installation du boîtier Enforcer

Ce chapitre traite des sujets suivants :

Planifier l'installation de boîtiers Enforcer

Vous devez prévoir l'emplacement d'intégration dans un réseau des boîtiers Symantec Network Access Control Enforcer basés sur Linux suivants :

- Boîtier Symantec Network Access Control Gateway Enforcer
  Se reporter à "Planification d'installation pour un boîtier Gateway Enforcer" à la page 48.
- Boîtier Symantec Network Access Control DHCP Enforcer
  Se reporter à "Planification d'installation pour un boîtier DHCP Enforcer" à la page 59.
- Boîtier Symantec Network Access Control LAN Enforcer
  Se reporter à "Planification d'installation pour un boîtier LAN Enforcer" à la page 68.

- Symantec Network Access Control Integrated DHCP Enforcer pour serveurs DHCP Microsoft
  Se reporter à "A propos de la planification de l'installation d'Integrated Enforcer pour serveurs DHCP Microsoft" à la page 337.
- Symantec Network Access Control Integrated DHCP Enforcer pour serveurs Microsoft Network Access Protection
  Se reporter à "A propos de la planification de l'installation de Symantec Integrated NAP Enforcer" à la page 403.
- Symantec Network Access Control Integrated DHCP Enforcer pour serveurs DHCP Alcatel-Lucent VitalQIP
  Se reporter à "A propos de la planification de l'installation d'un module d'application Integrated Lucent Enforcer" à la page 355.

Planification d'installation pour un boîtier Gateway Enforcer

Plusieurs types d'informations de planification peuvent vous aider à mettre en application des boîtiers Gateway Enforcer dans un réseau.

Vous pouvez placer le boîtier Gateway Enforcer de manière à protéger les zones suivantes d'un réseau :

- Disposition générale
  Se reporter à "Où placer le boîtier Gateway Enforcer" à la page 49.
- Se reporter à "Directives pour les adresses IP d'un boîtier Gateway Enforcer" à la page 51.
- Se reporter à "Série de deux boîtiers Gateway Enforcer" à la page 51.
- Se reporter à "Protection d'accès VPN par un boîtier Gateway Enforcer" à la page 52.
- Se reporter à "Protection de points d'accès sans fil par un boîtier Gateway Enforcer" à la page 52.
- Se reporter à "Protection des serveurs par un boîtier Gateway Enforcer" à la page 52.
- Se reporter à "Protection des serveurs et des clients non Windows par un boîtier Gateway Enforcer" à la page 53.
- Se reporter à "Conditions requises pour l'autorisation de clients non-Windows sans authentification" à la page 54.

Où placer le boîtier Gateway Enforcer

Vous pouvez placer des modules d'application Gateway Enforcer aux emplacements où tout le trafic doit passer par un boîtier Gateway Enforcer avant qu'un client puisse :

- se connecter à un réseau d'entreprise ;
- atteindre les zones sécurisées d'un réseau.

Se reporter à "Directives pour les adresses IP d'un boîtier Gateway Enforcer" à la page 51.

Vous pouvez placer des boîtiers Gateway Enforcer aux emplacements suivants :

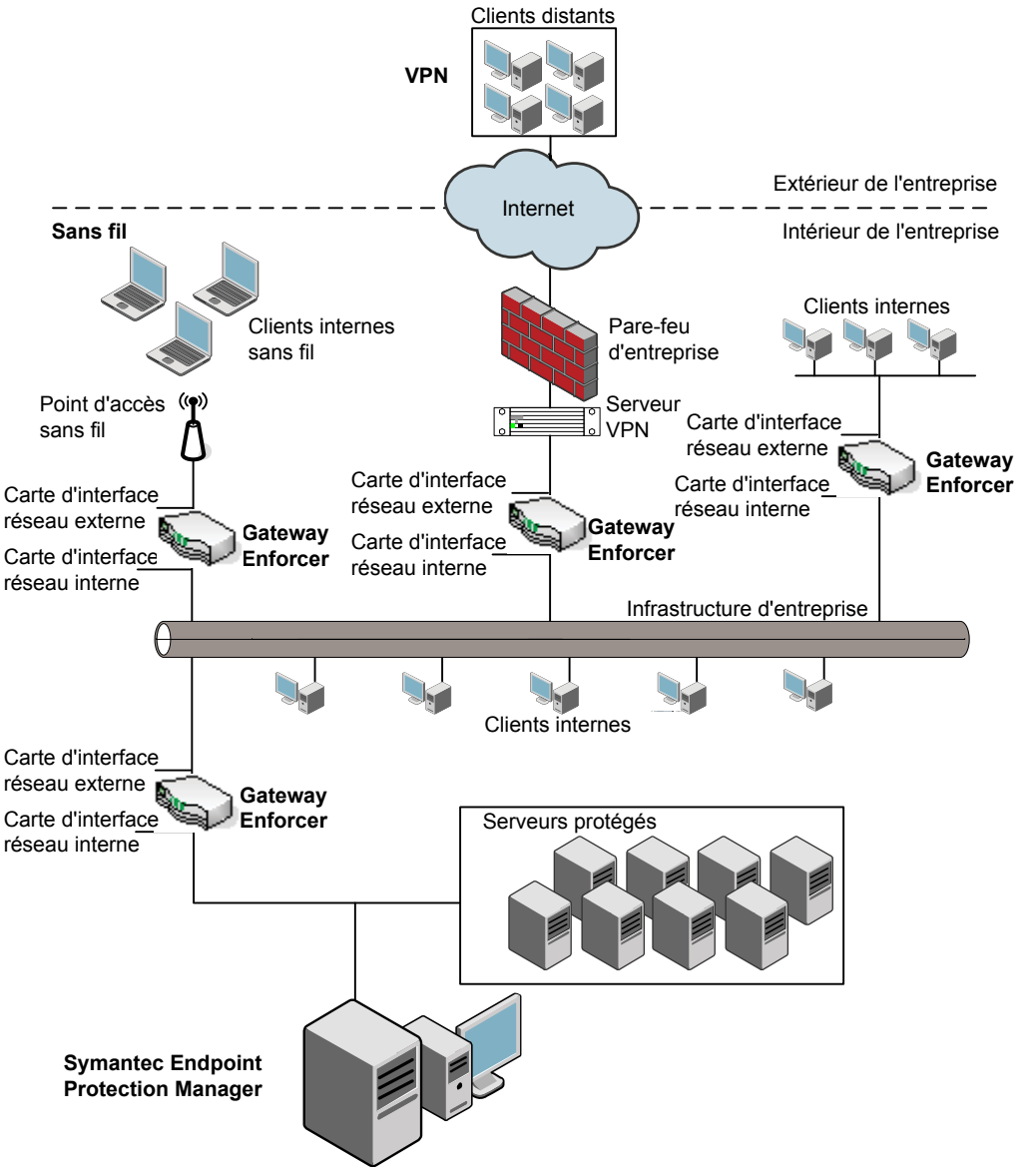
VPN	Entre les concentrateurs VPN et le réseau d'entreprise
Point d'accès sans fil (WAP)	Entre un point d'accès sans fil et le réseau d'entreprise
Serveurs	Devant les serveurs d'entreprise

Les organisations de grande taille peuvent nécessiter un boîtier Gateway Enforcer pour protéger chaque point d'accès réseau. Les modules d'application Gateway Enforcer se trouvent typiquement dans différents sous-réseaux. Dans la plupart des cas, vous pouvez intégrer des boîtiers Gateway Enforcer dans un réseau d'entreprise sans devoir apporter des modifications à la configuration matérielle.

Vous pouvez placer des boîtiers Gateway Enforcer à côté d'un point d'accès sans fil (WAP) ou d'un réseau privé virtuel (VPN). Dans un réseau d'entreprise, vous pouvez également protéger les serveurs qui contiennent des informations sensibles. Les boîtiers Gateway Enforcer doivent utiliser deux cartes d'interface réseau (cartes d'interface réseau).

Figure 2-1 donne un exemple de placement des boîtiers Gateway Enforcer dans configuration réseau globale.

Figure 2-1 Disposition de boîtiers Gateway Enforcer



Un autre emplacement où un boîtier Gateway Enforcer protège un réseau est un serveur d'accès distant (RAS). Les clients peuvent utiliser l'accès à distance pour se connecter à un réseau d'entreprise. Les clients d'accès à distance sont configurés comme les clients sans fil et VPN. La carte d'interface réseau externe se connecte au serveur RAS et la carte d'interface réseau interne se connecte au réseau.

Directives pour les adresses IP d'un boîtier Gateway Enforcer

Lors de la configuration de l'adresse de carte d'interface réseau interne pour un boîtier Gateway Enforcer, respectez les directives suivantes :

- La carte d'interface réseau interne d'un boîtier Gateway Enforcer doit pouvoir communiquer avec un gestionnaire Symantec Endpoint Protection Manager. Par défaut, la carte d'interface réseau interne doit faire face à un gestionnaire Symantec Endpoint Protection Manager.
- Les clients doivent pouvoir communiquer avec l'adresse IP interne du boîtier Gateway Enforcer. Le serveur VPN ou WAP peut être dans un sous-réseau différent si les requêtes des clients peuvent être réacheminées vers le même sous-réseau que celui de l'adresse IP interne du boîtier Gateway Enforcer.
- Pour le boîtier Gateway Enforcer qui protège les serveurs internes, la carte d'interface réseau interne se connecte au VLAN qui à son tour se connecte aux serveurs.
- Si vous utilisez plusieurs boîtiers Gateway Enforcer dans une configuration de basculement, l'adresse IP de la carte d'interface réseau interne sur chaque boîtier Gateway Enforcer doit avoir sa propre adresse IP.

Le boîtier Gateway Enforcer génèrera une adresse factice pour la carte d'interface réseau externe, basée sur l'adresse de la carte d'interface réseau interne. Vous n'avez pas besoin de configurer ceci de nouveau si vous installez un autre boîtier Gateway Enforcer.

Série de deux boîtiers Gateway Enforcer

Si un réseau prend en charge deux boîtiers Gateway Enforcer en série de sorte qu'un client se connecte au réseau par plus d'un boîtier Gateway Enforcer, vous devez spécifier le boîtier le plus proche du gestionnaire Symantec Endpoint Protection Manager comme adresse IP interne approuvée de l'autre boîtier Gateway Enforcer. Autrement un retard de cinq minutes peut se produire avant que le client puisse se connecter au réseau.

Ce retard peut se produire quand le client exécute une vérification de l'intégrité de l'hôte qui échoue. En tant qu'élément de la résolution d'intégrité d'hôte, le client télécharge les mises à jour de logiciel requises. Ensuite, le client exécute la

vérification de l'intégrité de l'hôte de nouveau. La vérification de l'intégrité de l'hôte réussit alors mais l'accès au réseau est retardé.

Consultez le *Guide d'administration pour Symantec Endpoint Protection et Symantec Network Access Control* pour des informations sur les adresses IP internes approuvées.

Protection d'accès VPN par un boîtier Gateway Enforcer

La protection de l'accès VPN est la raison principale et la plus commune pour utiliser un boîtier Gateway Enforcer. Vous pouvez placer des boîtiers Gateway Enforcer aux points d'accès VPN pour sécuriser l'accès à un réseau d'entreprise. Le boîtier Gateway Enforcer est placé entre le serveur VPN et le réseau d'entreprise. Il permet l'accès aux utilisateurs autorisés seulement et empêche l'accès à n'importe qui d'autre.

Protection de points d'accès sans fil par un boîtier Gateway Enforcer

Les boîtiers Enforcer protègent le réseau d'entreprise aux points d'accès sans fil (WAP). Le boîtier Gateway Enforcer s'assure que toute personne se connectant au réseau en utilisant la technologie sans fil exécute le client et satisfait aux exigences de sécurité.

Dès lors que ces conditions sont remplies, l'accès au réseau est accordé au client. Le boîtier Gateway Enforcer est placé entre le WAP et le réseau d'entreprise. La carte d'interface réseau externe est dirigée vers le WAP et la carte d'interface réseau interne est dirigée vers le réseau d'entreprise.

Protection des serveurs par un boîtier Gateway Enforcer

Les boîtiers Gateway Enforcer peuvent protéger les serveurs d'entreprise qui contiennent des informations sensibles dans le réseau d'entreprise. Une société peut placer des données importantes sur les serveurs qui peuvent se trouver dans une salle informatique verrouillée. Seuls les administrateurs système peuvent avoir accès à la salle informatique verrouillée.

Le boîtier Gateway Enforcer agit comme un verrou supplémentaire sur la porte. Il assure ce rôle en ne permettant l'accès aux serveurs protégés qu'aux seuls utilisateurs qui répondent à ses critères. Les serveurs localisent la carte d'interface réseau interne dans cette installation. Toutefois, les utilisateurs qui essayent d'y accéder doivent passer par la carte d'interface réseau externe.

Pour protéger ces serveurs, vous pouvez limiter l'accès aux clients ayant les adresses IP indiquées et configurer des règles strictes d'intégrité de l'hôte. Par exemple, vous pouvez configurer un boîtier Gateway Enforcer pour protéger des

serveurs dans un réseau. Un boîtier Gateway Enforcer peut se trouver entre des clients sur un réseau local d'entreprise et les serveurs qu'il protège. La carte d'interface réseau externe est dirigées vers le réseau local d'entreprise à l'intérieur de l'entreprise et la carte d'interface réseau interne est dirigée vers les serveurs protégés. Cette configuration empêche des utilisateurs ou des clients non-autorisés d'accéder aux serveurs.

Protection des serveurs et des clients non Windows par un boîtier Gateway Enforcer

Vous pouvez installer les serveurs et les clients sur un système d'exploitation autre que Microsoft Windows. Toutefois, le boîtier Gateway Enforcer ne peut authentifier aucun serveur ou client qui ne s'exécute pas sur un ordinateur qui ne prend pas en charge Microsoft Windows.

Si une organisation comprend des serveurs et des clients avec des systèmes d'exploitation sur lesquels le logiciel client n'est pas installé, vous devez appliquer l'une des méthodes suivantes :

- Mettre en application la prise en charge par un boîtier Gateway Enforcer.
- Se reporter à "Mise en œuvre de la prise en charge non-Windows par le biais d'un boîtier Gateway Enforcer" à la page 53.
- Mettre en application la prise en charge sans boîtier Gateway Enforcer.
  Se reporter à "Mise en oeuvre des plate-formes non-Windows sans le boîtier Gateway Enforcer" à la page 53.

Mise en œuvre de la prise en charge non-Windows par le biais d'un boîtier Gateway Enforcer

Vous pouvez mettre en application la prise en charge de clients non-Windows en configurant le boîtier Gateway Enforcer pour permettre à tous les clients non-Windows d'accéder au réseau. Si vous configurez le boîtier Gateway Enforcer de cette façon, il exécute la détection du système d'exploitation pour identifier les clients qui exécutent des systèmes d'exploitation non-Windows.

Mise en oeuvre des plate-formes non-Windows sans le boîtier Gateway Enforcer

Vous pouvez mettre en œuvre la prise en charge de clients non Windows en permettant à ceux-ci d'accéder au réseau par un point d'accès séparé.

Vous pouvez connecter les clients suivants qui prennent en charge des systèmes d'exploitation non Windows à travers un serveur VPN séparé :

- Un serveur VPN peut prendre en charge les clients qui disposent du logiciel client installé. Les ordinateurs client basés sur Windows peuvent se connecter au réseau d'entreprise par le biais d'un boîtier Gateway Enforcer.
- Un autre serveur VPN peut prendre en charge les clients qui exécutent des systèmes d'exploitation non-Windows. L'ordinateur client non basé sur Windows peut alors se connecter au réseau d'entreprise sans boîtier Gateway Enforcer.

Conditions requises pour l'autorisation de clients non-Windows sans authentification

Vous pouvez configurer le boîtier Gateway Enforcer pour autoriser les clients non-Windows sans authentification.

Se reporter à "Conditions requises pour les clients non-Windows" à la page 55.

Lorsque un client tente d'accéder au réseau d'entreprise par un boîtier Gateway Enforcer, le boîtier Enforcer vérifie d'abord si le logiciel client a été installé sur l'ordinateur client. Si le client ne s'exécute pas et si l'option qui autorise les clients non-Windows est sélectionnée, le boîtier Gateway Enforcer vérifie le système d'exploitation..

Il vérifie le système d'exploitation en envoyant des paquets de données pour sonder le client afin de détecter le type de système d'exploitation qu'il exécute actuellement. Si le client exécute un système d'exploitation non-Windows, le client est autorisé à accéder au réseau.

Conditions requises pour les clients Windows

Lorsqu'un boîtier Gateway Enforcer est configuré pour permettre la connexion de clients non-Windows à un réseau, il essaye d'abord de déterminer le système d'exploitation d'un client. Si le système d'exploitation est basé sur Windows, le boîtier Gateway Enforcer authentifie le client. Sinon, le boîtier Gateway Enforcer autorise le client à se connecter au réseau sans authentification.

Pour que le boîtier Gateway Enforcer détecte correctement qu'un système d'exploitation est un système d'exploitation Windows, les conditions ci-après doivent être satisfaites sur le client Windows :

- L'option client pour les réseaux Microsoft doit être installée et activée sur le client.
  Consultez la documentation de Windows.
- Le port UDP 137 doit être ouvert sur le client. Il doit être accessible par Gateway Enforcer.

Si un client Windows ne répond pas à ces exigences, le boîtier Enforcer de passerelle peut interpréter le client Windows pour être un client non-Windows. Par conséquent le boîtier Gateway Enforcer peut permettre au client non-Windows de se connecter au réseau sans authentification.

Conditions requises pour les clients non-Windows

Le boîtier Gateway Enforcer doit répondre aux exigences suivantes avant de permettre à un client Macintosh de se connecter à un réseau :

- Le partage Windows doit être activé.
  Ce paramètre est activé par défaut.
- Le pare-feu intégré de Macintosh doit être désactivé.
  Ce paramètre est celui par défaut.

Pour autoriser un client Linux, Gateway Enforcer requiert la condition suivante ::

- Le système Linux doit exécuter le service Samba.

Planifier le basculement pour les boîtiers Gateway Enforcer

Une entreprise peut prendre en charge deux boîtiers Gateway Enforcer configurés pour continuer les opérations en cas d'échec de l'un d'entre eux. Si un boîtier Gateway Enforcer échoue dans un réseau qui n'est pas configuré pour le basculement, alors l'accès au réseau à cet emplacement est automatiquement bloqué. Si un boîtier Gateway Enforcer échoue dans un réseau qui ne prévoit pas le basculement, les clients ne peuvent plus se connecter au réseau. Les clients ne pourront pas se connecter au réseau tant que le problème avec le boîtier Gateway Enforcer n'aura pas été corrigé.

Pour un boîtier Gateway Enforcer, le basculement est mis en œuvre par le boîtier Gateway Enforcer lui-même, et non par des commutateurs tiers. Si la configuration matérielle est définie correctement, Symantec Endpoint Protection Manager synchronise automatiquement les paramètres pour les boîtiers Gateway Enforcer de basculement.

Utiliser le basculement avec des boîtiers Gateway Enforcer dans le réseau

Le boîtier Gateway Enforcer qui est opérationnel est désigné par boîtier Gateway Enforcer actif. Le boîtier Gateway Enforcer de sauvegarde est désigné par boîtier Gateway Enforcer de réserve. Le boîtier Gateway Enforcer actif est aussi désigné

par boîtier Gateway Enforcer principal. Si le boîtier Gateway Enforcer actif échoue, le boîtier Gateway Enforcer de réserve assure les tâches d'application.

Les deux boîtiers Gateway Enforcer sont démarrés dans l'ordre suivant :

- Quand le premier boîtier Gateway Enforcer est démarré, il s'exécute en mode 'attente'. En restant dans ce mode, il interroge le réseau pour déterminer si un autre boîtier Gateway Enforcer s'exécute. Il envoie trois requêtes pour rechercher un autre Gateway Enforcer. Son passage à l'état Online (En ligne) peut donc prendre quelques minutes.
- Si le premier boîtier Gateway Enforcer ne détecte aucun autre boîtier Gateway Enforcer, le premier boîtier Gateway Enforcer devient le boîtier Gateway Enforcer actif.
- Pendant son exécution, le boîtier Gateway Enforcer actif diffuse des paquets de basculement sur les réseaux internes et externes. Il continue à diffuser des paquets de basculement.
- Dès que le deuxième boîtier Gateway Enforcer est démarré, il s'exécute en mode 'attente'. Il interroge le réseau pour déterminer si un autre boîtier Gateway Enforcer s'exécute.
- Le deuxième boîtier Gateway Enforcer détecte alors le boîtier Gateway Enforcer actif en cours d'exécution et reste donc en mode 'attente'.
- Si le boîtier Gateway Enforcer actif échoue, il cesse de diffuser des paquets de basculement. Le boîtier Gateway Enforcer de réserve ne détecte plus aucun boîtier Gateway Enforcer actif. Par conséquent il devient le boîtier Gateway Enforcer actif qui prend en charge les connexions réseau et la sécurité à cet emplacement.
- Si vous démarrez l'autre boîtier Gateway Enforcer, il reste en veille puisqu'il détecte qu'un autre boîtier Gateway Enforcer est actif.

Placer les boîtiers Gateway Enforcer pour le basculement dans un réseau avec un ou plusieurs VLAN

Vous configurez un boîtier Gateway Enforcer pour le basculement par son emplacement physique et la configuration réalisée dans Symantec Endpoint Protection Manager. Si vous utilisez un hub prenant en charge plusieurs VLAN, vous ne pouvez utiliser qu'un VLAN à moins d'intégrer un commutateur 802.1q-aware au lieu d'un hub.

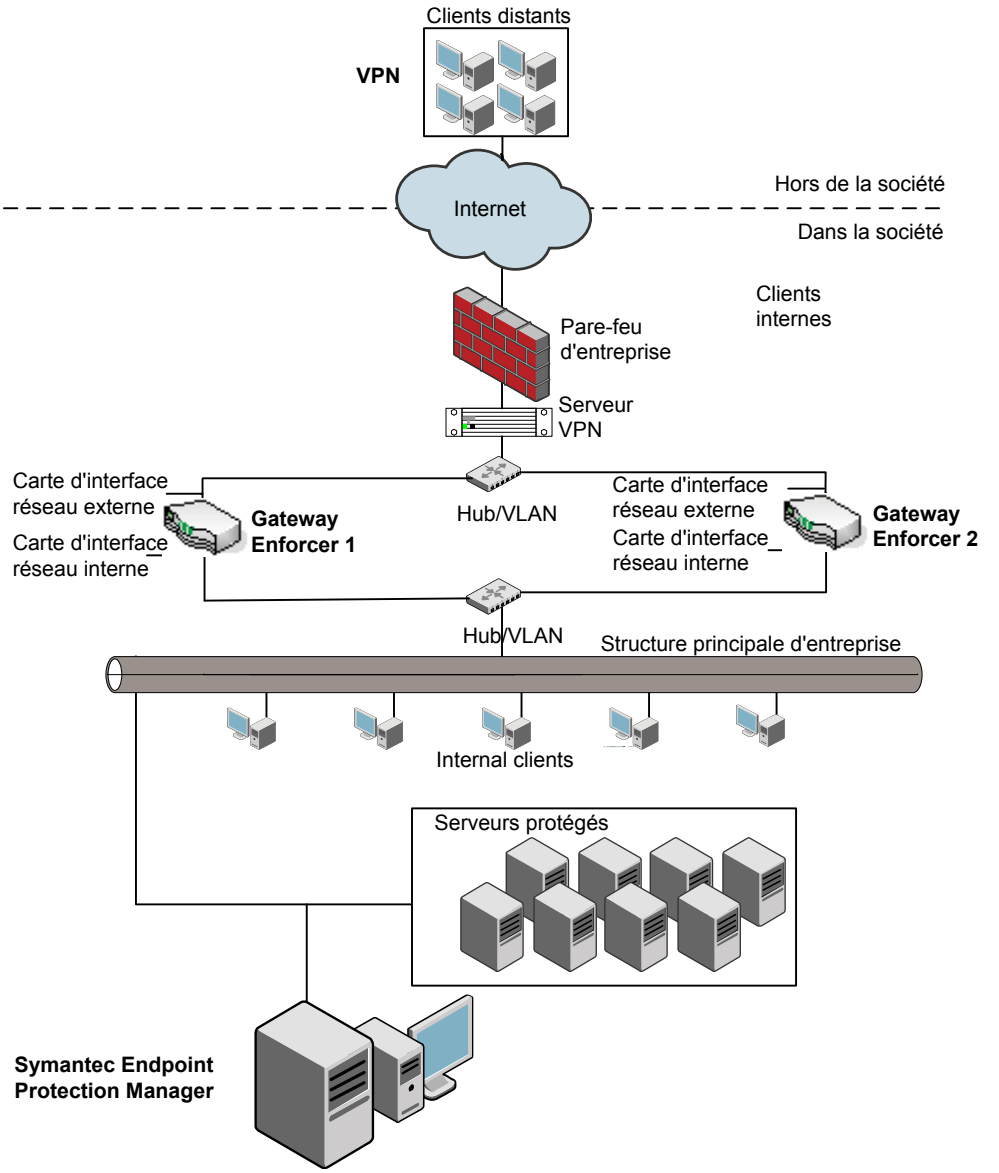
Le boîtier Gateway Enforcer pour le basculement doit être configuré sur le même segment de réseau. Ni un routeur ni une passerelle ne peuvent être installés entre les deux boîtiers Gateway Enforcer. Un routeur ou une passerelle ne transfère pas le paquet de basculement. Les cartes d'interface réseau internes doivent toutes

les deux se connecter au réseau interne par le même commutateur ou hub. Les cartes d'interface réseau externes doivent toutes les deux se connecter au serveur VPN ou au point d'accès externe par le même commutateur ou hub.

Vous utilisez des processus semblables pour configurer des boîtiers Gateway Enforcer pour basculement sur un point d'accès (AP) sans fil, sur des serveurs d'accès à distance ou sur d'autres points d'accès. Les cartes d'interface réseau des deux boîtiers Gateway Enforcer se connectent au réseau externe par le biais d'un serveur WAP ou RAS. Les cartes d'interface réseau interne se connectent au réseau interne ou à la zone protégée.

Figure 2-2 montre comment configurer deux boîtiers Gateway Enforcer de basculement pour protéger l'accès au réseau à un concentrateur de VPN.

Figure 2-2 Disposition de deux boîtiers Gateway Enforcer



Installer les boîtiers Gateway Enforcer pour le basculement

Vous devriez vous familiariser avec les concepts impliqués dans le basculement de boîtiers Gateway Enforcer avant d'installer les modules d'application Enforcer de réserve.

Se reporter à "Utiliser le basculement avec des boîtiers Gateway Enforcer dans le réseau" à la page 55.

Installer des boîtiers Gateway Enforcer pour le basculement

1. Placez les ordinateurs dans le réseau.

   Se reporter à "Placer les boîtiers Gateway Enforcer pour le basculement dans un réseau avec un ou plusieurs VLAN" à la page 56.

2. Installez les cartes d'interface réseau internes.

   Les cartes d'interface réseau internes sur boîtiers Gateway Enforcer multiples doivent chacune avoir une adresse IP différente.

   Se reporter à "Directives pour les adresses IP d'un boîtier Gateway Enforcer" à la page 51.

Planification d'installation pour un boîtier DHCP Enforcer

Plusieurs types d'informations de planification peuvent vous aider à mettre en application des boîtiers DHCP Enforcer dans un réseau.

Vous pouvez placer le boîtier DHCP Enforcer de manière à protéger les zones suivantes d'un réseau :

- Se reporter à "Où placer les boîtiers DHCP Enforcer dans un réseau" à la page 59.
- Se reporter à "Adresses IP de boîtier DHCP Enforcer" à la page 61.
- Se reporter à "Protection des clients non-Windows avec l'application DHCP" à la page 62.
- Se reporter à "A propos du serveur DHCP" à la page 63.

Où placer les boîtiers DHCP Enforcer dans un réseau

Si vous voulez vous assurer que le boîtier DHCP Enforcer peut intercepter tous les messages DHCP entre les clients et les serveurs DHCP, vous devez l'installer comme périphérique en ligne. Le module DHCP Enforcer doit être installé entre les clients et le serveur DHCP.

La carte d'interface réseau interne du boîtier DHCP Enforcer se connecte aux serveurs DHCP. La carte d'interface réseau externe du boîtier DHCP Enforcer se connecte aux clients via un routeur ou un commutateur qui assure le rôle de relais DHCP. Symantec Endpoint Protection Manager se connecte également à la carte d'interface réseau externe du boîtier DHCP Enforcer.

Vous pouvez configurer un boîtier DHCP Enforcer pour communiquer avec plusieurs serveurs DHCP. Par exemple, vous pouvez avoir plusieurs serveurs DHCP sur le même sous-réseau à des fins de basculement. Si vous avez des serveurs DHCP dans différents emplacements sur le réseau, chacun d'entre eux a besoin d'un boîtier DHCP Enforcer distinct.

Pour chacun de vos emplacements de serveur DHCP, vous configurez un serveur DHCP normal et un serveur DHCP de quarantaine. Vous pouvez configurer le boîtier Enforcer de sorte à ce qu'il reconnaisse plusieurs serveurs DHCP en quarantaine, comme plusieurs serveurs DHCP normaux.

Remarque : Vous pouvez installer un serveur DHCP sur un ordinateur et le configurer en réseau normal et en réseau de quarantaine.

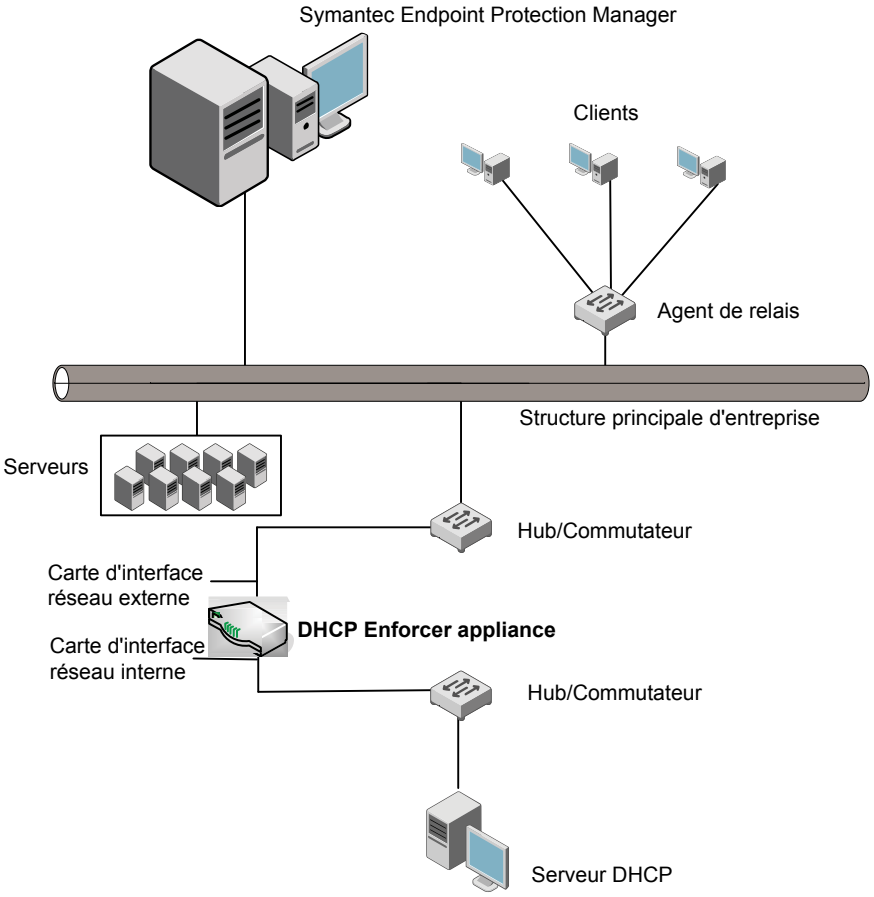
Vous devez également installer un serveur de résolution de sorte que les clients qui reçoivent des configurations de quarantaine puissent se connecter par le biais de ce dernier. Symantec Endpoint Protection Manager peut éventuellement s'exécuter sur le même ordinateur que le serveur de résolution. Ni Symantec Endpoint Protection Manager ni le serveur de résolution ne nécessitent de connexion directe avec le boîtier DHCP Enforcer ou les serveurs DHCP.

Si le client répond aux exigences de sécurité, le boîtier DHCP Enforcer agit comme agent de relais DHCP. Le boîtier DHCP Enforcer connecte le client au serveur DHCP normal et le client reçoit une configuration réseau régulière. Si le client ne répond pas aux exigences de sécurité, le boîtier DHCP Enforcer se connecte à un serveur DHCP de quarantaine. Le client reçoit alors une configuration réseau de quarantaine.

Figure 2-3 affiche un exemple des divers composants requis pour un boîtier DHCP Enforcer et de leurs emplacements.

Remarque : Bien que l'illustration indique un serveur DHCP de quarantaine sur un ordinateur distinct, seul un ordinateur est requis. Si vous utilisez seulement un ordinateur, vous devez configurer le serveur DHCP pour fournir deux configurations réseau différentes. Une des configurations réseau doit être une configuration réseau de quarantaine.

Figure 2-3 Disposition d'un boîtier DHCP Enforcer



Adresses IP de boîtier DHCP Enforcer

Quand vous configurez une adresse IP pour un boîtier DHCP Enforcer, vous devez suivre certaines directives.

Suivez ces directives quand vous installez la carte d'interface réseau interne pour un boîtier DHCP Enforcer :

- L'adresse IP interne du boîtier DHCP Enforcer doit être dans le même sous-réseau que les serveurs DHCP.

- Les clients doivent pouvoir communiquer avec l'adresse IP interne du boîtier DHCP Enforcer.
- Si vous utilisez plusieurs boîtiers DHCP Enforcer en configuration de basculement, l'adresse IP de la carte d'interface réseau interne sur chaque boîtier DHCP Enforcer doit être différente.
- Si vous utilisez plusieurs boîtiers DHCP Enforcer en configuration de basculement, les clients doivent pouvoir communiquer avec l'adresse IP interne des boîtiers DHCP Enforcer actifs et de réserve.

Suivez ces directives quand vous installez la carte d'interface réseau externe pour un boîtier DHCP Enforcer :

- L'adresse IP externe du boîtier DHCP Enforcer doit pouvoir communiquer avec Symantec Endpoint Protection Manager. Elle doit être dans le même sous-réseau que l'intervalle IP de la carte d'interface réseau interne. Dans ce cas, Symantec Endpoint Protection Manager et le boîtier DHCP Enforcer sont situés de part et d'autre d'un commutateur.
- Si vous utilisez plusieurs boîtiers DHCP Enforcer en configuration de basculement, l'adresse IP de la carte d'interface réseau externe de chaque boîtier DHCP Enforcer doit être différente.

Protection des clients non-Windows avec l'application DHCP

Vous pouvez installer le logiciel de Symantec Endpoint Protection ou le logiciel de Symantec Network Access Control sur des clients exécutant le système d'exploitation Microsoft Windows. Le module DHCP Enforcer ne peut pas authentifier des clients sans le logiciel Symantec Endpoint Protection. Si une organisation comprend des clients avec des systèmes d'exploitation ne prenant pas en charge le logiciel, comme Linux ou Solaris, votre planification doit inclure la gestion de ces clients.

Si vous pouvez effectuer la prise en charge des clients non-Windows, vous pouvez configurer le boîtier DHCP Enforcer pour permettre à tous les clients non-Windows de se connecter au réseau. Lorsque le boîtier DHCP Enforcer est configuré de cette façon, il effectue la détection du système d'exploitation pour identifier les clients exécutant des systèmes d'exploitation non-Windows.

Comme méthode alternative, vous pouvez configurer le DHCP Enforcer pour permettre aux adresses MAC spécifiques d'accéder au réseau d'entreprise. Lorsqu'un client avec une adresse MAC approuvée essaye de se connecter au réseau, le module d'application DHCP Enforcer fait suivre la requête DHCP du client au serveur DHCP normal sans authentification.

A propos du serveur DHCP

Vous pouvez installer un serveur DHCP de quarantaine sur un ordinateur distinct. Vous pouvez également configurer ce serveur DHCP en mode réseau normal et de quarantaine.

La configuration réseau de quarantaine doit permettre d'accéder aux composants suivants :

- Serveur de résolution
- Symantec Endpoint Protection Manager
- serveur DHCP
- Boîtier DHCP Enforcer

Si vous utilisez plusieurs boîtiers DHCP Enforcer pour le basculement, la configuration réseau de quarantaine doit permettre d'accéder à ces composants.

L'adresse IP de quarantaine est utilisée comme suit pendant l'authentification du module DHCP Enforcer :

- Le boîtier DHCP Enforcer obtient initialement une adresse IP de quarantaine temporaire pour que le client effectue l'authentification avec un client.
  Si l'authentification est réussie, le boîtier DHCP Enforcer envoie un message de notification au client l'invitant à libérer l'adresse IP et à la renouveler immédiatement.
  Vous pouvez attribuer un temps de réservation restreint à la configuration de quarantaine. Symantec recommande une période de deux minutes.
- Si vous prenez en charge deux serveurs DHCP, vous pouvez définir une plage d'adresses IP différente de la plage d'adresses IP de réseau normales. Vous pouvez utiliser n'importe quelle adresse IP de la plage différente pour la quarantaine de clients non autorisés. Toutefois, la plage d'adresses IP utilisée pour la quarantaine doit être située dans le même sous-réseau que les adresses IP de réseau normales. Vous pouvez attribuer quelques adresses IP restreintes utilisables par le serveur DHCP de quarantaine. Vous pouvez également utiliser un routeur ou un commutateur compatible ACL pour empêcher ces adresses IP restreintes d'accéder aux ressources de réseau régulières.
- Si vous utilisez un serveur DHCP, vous devez configurer une classe d'utilisateur appelée SYGATE_ENF qui est utilisée pour la configuration de quarantaine. Certaines des étapes de configuration sont effectuées sur le serveur DHCP. D'autres tâches de configuration sont effectuées sur la console Enforcer une fois l'installation terminée.

Serveur DHCP normal et en quarantaine sur un seul serveur DHCP

Vous pouvez utiliser le même serveur pour le serveur DHCP normal et le serveur DHCP de quarantaine. Il est recommandé d'utiliser deux serveurs.

Si vous voulez utiliser un serveur DHCP à la fois comme serveur DCHP normal et de quarantaine, vous devez tenir compte des directives suivantes :

- Les serveurs DHCP Microsoft ne prennent pas en charge plusieurs sous-réseaux. Si vous utilisez des serveurs DHCP Microsoft, vous pouvez avoir besoin de deux serveurs DHCP.
- Si vous voulez utiliser seulement un serveur DHCP Microsoft, tous les ordinateurs doivent utiliser le même sous-réseau d'adresse IP.
- Si votre environnement utilise deux sous-réseaux différents, vous devez vérifier que les routeurs peuvent gérer deux sous-réseaux sur une interface de routage unique. Par exemple, les routeurs de Cisco possèdent une fonction appelée IP secondaire.
  Pour plus d'informations, consultez la documentation du routeur.

Planifier le basculement pour les boîtiers DHCP Enforcer

Une entreprise peut configurer deux boîtiers DHCP Enforcer dans un réseau pour garantir un fonctionnement continu en cas d'échec de l'un d'entre eux. Si un boîtier DHCP Enforcer échoue dans un réseau qui n'est pas configuré pour le basculement, alors l'accès au réseau à cet emplacement est automatiquement bloqué. Si un boîtier DHCP Enforcer échoue dans un réseau qui ne prévoit pas le basculement, les clients ne peuvent plus se connecter au réseau. Ce problème persiste jusqu'à ce que la défaillance du boîtier DHCP Enforcer soit corrigée.

Pour un boîtier DHCP Enforcer, le basculement est mis en œuvre par le boîtier DHCP Enforcer lui-même, et non par des commutateurs tiers. Si la configuration matérielle a été définie correctement, Symantec Endpoint Protection Manager synchronise automatiquement les paramètres pour les boîtiers DHCP Enforcer de basculement.

Fonctionnement du basculement avec les boîtiers DHCP Enforcer dans le réseau

Le boîtier DHCP Enforcer qui est opérationnel est désigné par boîtier DHCP Enforcer actif. Le boîtier DHCP Enforcer de sauvegarde est désigné par boîtier DHCP Enforcer de réserve. Le boîtier DHCP Enforcer actif est aussi désigné par

boîtier DHCP Enforcer principal. Si le boîtier DHCP Enforcer actif échoue, le boîtier DHCP Enforcer de réserve assure les tâches d'application.

La séquence dans laquelle les deux boîtiers DHCP Enforcer sont démarrés est la suivante :

- Quand le premier boîtier DHCP Enforcer est démarré, il s'exécute en mode veille pendant qu'il interroge le réseau pour déterminer si un autre boîtier DHCP Enforcer s'exécute. Il envoie trois requêtes pour rechercher un autre DHCP Enforcer. Son passage à l'état Online (En ligne) peut donc prendre quelques minutes.
- S'il ne détecte pas d'autre boîtier DHCP Enforcer, il devient le boîtier DHCP Enforcer actif.
- Pendant son exécution, le boîtier DHCP Enforcer actif diffuse des paquets de basculement sur les réseaux internes et externes. Il continue à diffuser des paquets de basculement.
- Le deuxième boîtier DHCP Enforcer est ensuite démarré. Il s'exécute en mode veille pendant qu'il interroge le réseau pour déterminer si un autre boîtier DHCP Enforcer s'exécute.
- Le deuxième boîtier DHCP Enforcer détecte le boîtier DHCP Enforcer actif qui est en cours d'exécution et reste donc en mode veille.
- Si le boîtier DHCP Enforcer actif échoue, il cesse de diffuser des paquets de basculement. Le boîtier DHCP Enforcer en veille ne détecte plus aucun boîtier DHCP Enforcer actif. Par conséquent il devient le boîtier DHCP Enforcer actif qui prend en charge les connexions réseau et la sécurité à cet emplacement.
- Si vous démarrez l'autre boîtier DHCP Enforcer, il reste en veille puisqu'il détecte qu'un autre boîtier DHCP Enforcer est actif.

Où placer les boîtiers DHCP Enforcer pour le basculement dans un réseau avec un seul ou plusieurs VLAN

Vous configurez un boîtier DHCP Enforcer pour le basculement avec son emplacement physique et la configuration que vous effectuez dans Symantec Endpoint Protection Manager. Si vous utilisez un hub prenant en charge plusieurs VLAN, vous ne pouvez utiliser qu'un VLAN à moins d'intégrer un commutateur 802.1q-aware au lieu d'un hub.

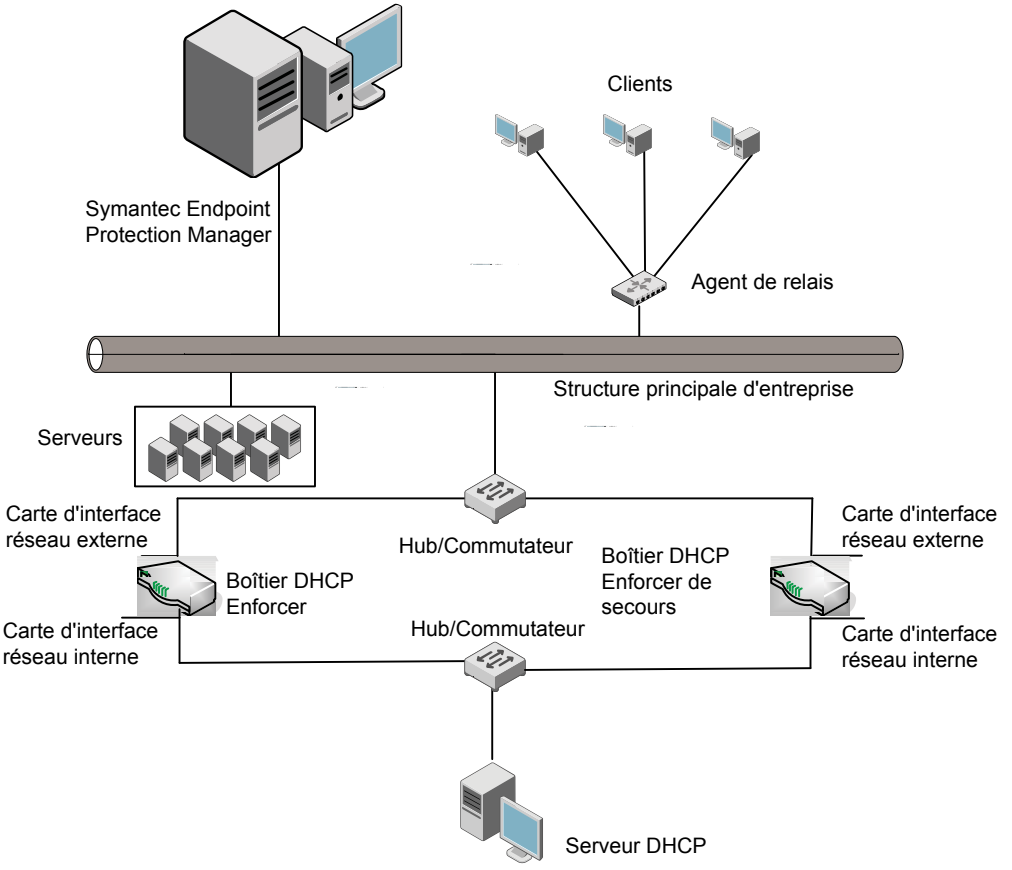
Le boîtier DHCP Enforcer pour le basculement doit être configuré sur le même segment de réseau. Ni un routeur ni une passerelle ne pourront être installés entre les deux boîtiers DHCP Enforcer. Un routeur ou une passerelle ne transfère pas le paquet de basculement. Les cartes d'interface réseau internes doivent toutes les deux se connecter au réseau interne par le même commutateur ou hub. Les

cartes d'interface réseau externes doivent toutes les deux se connecter au serveur VPN ou au point d'accès externe par le même commutateur ou hub.

La configuration de boîtiers DHCP Enforcer pour le basculement sur un point d'accès sans fil, un RAS d'accès à distance ou d'autres points d'accès est similaire. La carte d'interface réseau NIC des deux boîtiers DHCP Enforcer se connecte au réseau externe via un serveur RAS ou AP sans fil. Les cartes d'interface réseau internes se connectent au réseau interne ou à la zone protégée.

Figure 2-4 montre comment configurer deux boîtiers DHCP Enforcer de basculement pour protéger l'accès au réseau à un concentrateur de VPN.

Figure 2-4 Placement de deux boîtiers DHCP Enforcer



Configurer les boîtiers DHCP Enforcer pour le basculement

Vous devriez vous familiariser avec les concepts impliqués dans le basculement de boîtier DHCP Enforcer avant de configurer des boîtiers DHCP Enforcer de réserve.

Se reporter à "Fonctionnement du basculement avec les boîtiers DHCP Enforcer dans le réseau" à la page 64.

Pour configurer des boîtiers DHCP Enforcer pour le basculement

1. Placez les ordinateurs dans le réseau.

   Se reporter à "Où placer les boîtiers DHCP Enforcer pour le basculement dans un réseau avec un seul ou plusieurs VLAN" à la page 65.

2. Configurez les cartes d'interface réseau externes et internes.

   Les cartes d'interface réseau externes sur plusieurs boîtiers DHCP Enforcer doivent chacune avoir une adresse IP différente. Les cartes d'interface réseau internes sur plusieurs boîtiers DHCP Enforcer doivent chacune avoir une adresse IP différente.

   Se reporter à "Adresses IP de boîtier DHCP Enforcer" à la page 61.

3. Installez et démarrez le boîtier DHCP Enforcer principal.

   Si le boîtier DHCP Enforcer principal ne localise aucun autre module d'application DHCP Enforcer, il assure le rôle de boîtier DHCP Enforcer actif.

4. Installez et démarrez le boîtier DHCP Enforcer de réserve.

5. Connectez le boîtier DHCP Enforcer de réserve à la console Symantec Endpoint Protection Manager à laquelle est connecté le boîtier DHCP Enforcer actif.

   Si les deux boîtiers DHCP Enforcer ont été exécutés pendant la même durée, celui disposant de l'adresse IP la plus basse devient le boîtier DHCP Enforcer principal.

   Le basculement est activé par défaut sur Symantec Endpoint Protection Manager. La console Symantec Endpoint Protection Manager affecte automatiquement le boîtier DHCP Enforcer en veille au même groupe Enforcer. Par conséquent, les paramètres des boîtiers DHCP Enforcer principal et en veille sont synchronisés.

   Les paramètres de basculement suivants sont activés par défaut :

   - Le paramètre par défaut pour le port UDP de basculement est le port 39999.
     Un boîtier DHCP Enforcer de basculement utilise ce port pour communiquer.

- Le paramètre par défaut pour le niveau de sensibilité de basculement est High (Haut - moins de cinq secondes).
  Le niveau de sensibilité de basculement détermine la vitesse à laquelle le boîtier DHCP Enforcer devient le boîtier principal. Le basculement ne se produit que lorsque le boîtier DHCP Enforcer en veille détecte que le boîtier principal n'est plus actif.

Planification d'installation pour un boîtier LAN Enforcer

Plusieurs types d'informations de planification peuvent vous aider à mettre en application des boîtiers LAN Enforcer dans un réseau.

Se reporter à "Emplacement des boîtiers LAN Enforcer" à la page 68.

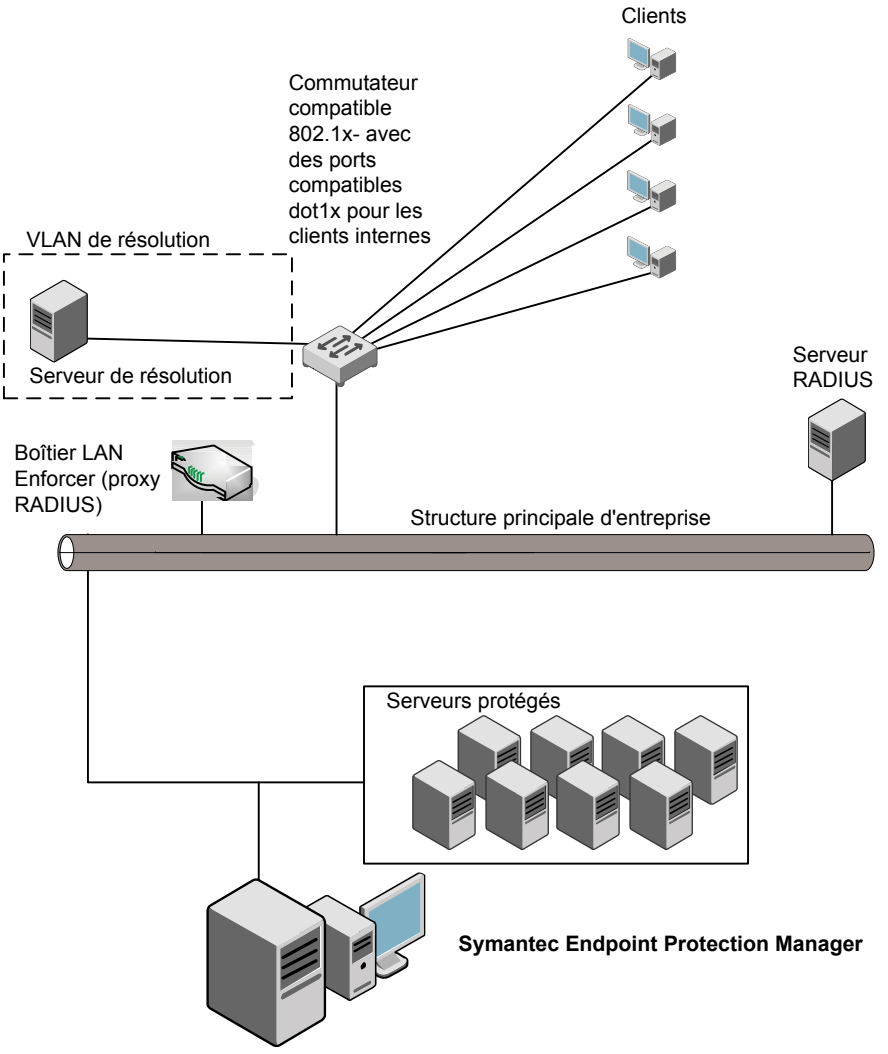
Emplacement des boîtiers LAN Enforcer

le boîtier LAN Enforcer agit en tant que proxy de RADIUS. Les administrateurs utilisent en général un boîtier LAN Enforcer avec un serveur RADIUS pour appliquer une authentification EAP 802.1x (Extensible Authentication Protocol) dans un réseau d'entreprise. Si vous utilisez un boîtier LAN Enforcer dans cette configuration, il doit pouvoir communiquer avec le serveur RADIUS.

Par exemple, vous pouvez connecter un boîtier LAN Enforcer à une option LAN compatible 802.1x sur un VLAN interne avec Symantec Endpoint Protection Manager, un serveur RADIUS et des clients. Un ordinateur qui ne possède pas le logiciel client ne peut pas se connecter au réseau. Toutefois, le client est dirigé vers un serveur de résolution sur lequel il peut obtenir le logiciel nécessaire pour devenir conforme.

Figure 2-5 donne un exemple de placement des boîtiers LAN Enforcer dans la configuration réseau interne globale.

Figure 2-5 Disposition de boîtiers LAN Enforcer



Si votre commutateur prend en charge la commutation VLAN dynamique, des VLAN supplémentaires peuvent être configurés sur le commutateur compatible 802.1x et devenir accessibles par l'intermédiaire du boîtier LAN Enforcer. Le commutateur compatible 802.1x peut dynamiquement placer le client dans un VLAN après avoir reçu une réponse du serveur RADIUS. Certains commutateurs compatibles 802.1x incluent également un paramètre VLAN par défaut ou invité.

Si un client n'a aucun supplicant 802.1x, le commutateur compatible 802.1x peut le mettre dans un VLAN par défaut.

Vous pouvez installer le boîtier LAN Enforcer afin de pouvoir activer l'authentification EAP dans tout le réseau avec le matériel déjà déployé. Les boîtiers LAN Enforcer peuvent fonctionner avec les serveurs RADIUS, les supplicants 802.1x et les commutateurs compatibles 802.1x existants. Ils exécutent l'authentification de niveau de l'ordinateur. Ils veillent à la conformité du client avec les politiques de sécurité.

Par exemple, ils vérifient que le logiciel antivirus a été mis à jour avec le dernier fichier de signature et les correctifs logiciels nécessaires. Le supplicant 802.1x et le serveur RADIUS effectuent l'authentification au niveau de l'utilisateur. Il vérifie si les clients qui essayent de se connecter au réseau sont bien ceux qui ils prétendent être.

Sinon, un boîtier LAN Enforcer peut également fonctionner en mode transparent, supprimant le besoin de serveur RADIUS. En mode transparent, le client transmet des données d'intégrité de l'hôte au commutateur compatible 802.1x en réponse à la sollicitation EAP. Le commutateur fait alors suivre ces données à LAN Enforcer. Un boîtier LAN Enforcer renvoie alors des résultats d'authentification au commutateur compatible 802.1x. Les données envoyées par LAN Enforcer sont basées sur les résultats de la validation d'intégrité de l'hôte. Par conséquent, le boîtier LAN Enforcer ne requiert aucune communication avec un serveur RADIUS.

Les configurations suivantes sont disponibles pour un boîtier LAN Enforcer :

- Configuration de base :
  Cette configuration requiert un serveur RADIUS et des supplicants 802.1x tiers. L'authentification utilisateur EAP traditionnelle et la validation d'intégrité de l'hôte Symantec sont exécutées.
- Mode transparent
  Cette configuration ne requiert ni un serveur RADIUS ni l'utilisation de supplicants 802.1x tiers. Seule la validation d'intégrité de l'hôte est exécutée.

Vous pouvez considérer les questions suivantes :

- Prévoyez-vous d'avoir un supplicant 802.1x installé sur chaque ordinateur ?
  Si vous prévoyez d'installer un supplicant 802.1x sur chaque ordinateur, vous pouvez utiliser la configuration de base.
- Voulez-vous exécuter une authentification au niveau utilisateur en plus de la vérification de l'intégrité de l'hôte ?
  Si vous voulez exécuter une authentification de niveau utilisateur en plus de la vérification de l'intégrité de l'hôte, vous devez utiliser la configuration de base.
- Prévoyez-vous d'utiliser un serveur RADIUS en configuration réseau ?

Si vous prévoyez d'utiliser un serveur RADIUS en configuration réseau, vous pouvez utiliser la configuration de base ou le mode transparent. Si vous ne prévoyez pas d'utiliser un serveur RADIUS en configuration réseau, vous devez utiliser le mode transparent.

Planifier le basculement pour les boîtiers LAN Enforcer

Si vous avez installé deux boîtiers LAN Enforcer dans un réseau, le basculement est pris en charge par le commutateur 802.1x-aware. Un commutateur compatible 802.1x peut prendre en charge plusieurs boîtiers LAN Enforcer. Vous pouvez facilement synchroniser les paramètres des boîtiers LAN Enforcer dans le Symantec Endpoint Protection Manager en utilisant les paramètres de synchronisation.

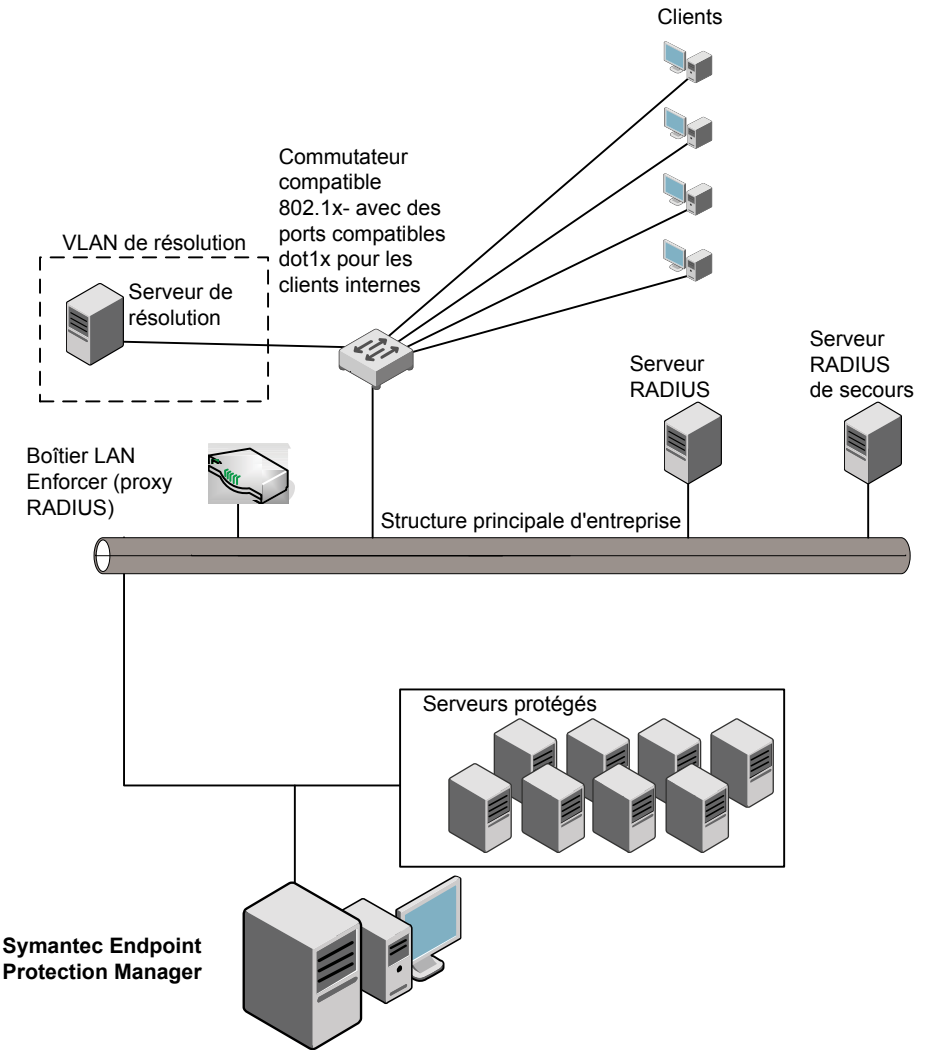
Si vous voulez synchroniser les paramètres d'un boîtier LAN Enforcer avec un autre, vous devez spécifier le même nom de groupe Enforcer sur la console Enforcer.

Si vous utilisez un serveur RADIUS dans votre réseau, vous pouvez prévoir le basculement de serveur RADIUS en configurant le boîtier LAN Enforcer de manière à ce qu'il se connecte à plusieurs serveurs RADIUS. Si tous les serveurs RADIUS configurés pour ce boîtier LAN Enforcer sont désactivés, le commutateur suppose que le boîtier LAN Enforcer l'est également. Par conséquent, le commutateur compatible 802.1x se connecte à un boîtier LAN Enforcer différent qui fournit une autre prise en charge de basculement.

Emplacement des boîtiers LAN Enforcer pour le basculement dans un réseau

Figure 2-6 décrit comment fournir le basculement pour les boîtiers LAN Enforcer.

Figure 2-6 Placement de deux boîtiers LAN Enforcer



Chapitre 3

Mettre à niveau et migrer les images du boîtier Enforcer

Ce chapitre traite des sujets suivants :

A propos de la mise à niveau et de la migration des images de boîtier Enforcer vers la version 11.0.3000

Vous pouvez déterminer la version du logiciel du boîtier Enforcer avant de prévoir de mettre à jour, migrer ou réimager un logiciel de boîtier Enforcer.

Se reporter à "Déterminer la version actuelle d'une image de boîtier Enforcer" à la page 74.

Il peut s'avérer nécessaire de mettre à niveau l'image d'un boîtier Enforcer vers la version 11.0.3000 pour la connexion à Symantec Endpoint Protection Manager version 11.0.3. La mise à niveau vous permet de bénéficier des nouvelles fonctionnalités fournies par le boîtier Symantec Network Access Control Enforcer version 11.0.3000.

Vous pouvez sélectionner une des méthodes suivantes pour mettre à niveau l'image du boîtier Enforcer :

- Mettre à niveau l'image du boîtier Enforcer en cours.
  Se reporter à "Mettre à niveau l'image de boîtier Enforcer de 11.0 ou 11.0.2000 vers 11.0.3000" à la page 75.
- Migrer l'image du boîtier de 5.1.x Enforcer vers 11.0.2000 Enforcer.
  Se reporter à "Migrer l'image du boîtier Enforcer de 5.1.x vers 11.0.3000" à la page 75.
- Installer une différente image de boîtier Enforcer sur une image de boîtier Enforcer précédente.
  Se reporter à "Recréer une image de boîtier Enforcer" à la page 76.
  Le boîtier Symantec Network Access Control Enforcer version 11.0.3000 fonctionne avec les versions suivantes de Symantec Endpoint Protection Manager :
  - Version 11.0.2
  - Version 11.0.3

Déterminer la version actuelle d'une image de boîtier Enforcer

Déterminez la version actuelle de l'image prise en charge sur le boîtier Enforcer. La dernière version est 11.0.3000. Si vous disposez d'une version antérieure à 11.0.3000, il est conseillé d'effectuer la mise à niveau ou la migration.

Par exemple, si vous déterminez la version d'une image de boîtier DHCP Enforcer, la sortie peut apparaître comme suit :

```
Symantec Network Access Control Enforcer 6100 Series - v11.0.1
build XXXX, 2007-11-29,19:09
DHCP Enforcer mode
```

Pour déterminer la version actuelle d'une image de boîtier Enforcer

- Tapez la commande suivante dans l'interface de ligne de commande d'un boîtier Enforcer : **show version**

Mettre à niveau l'image de boîtier Enforcer de 11.0 ou 11.0.2000 vers 11.0.3000

Vous pouvez utiliser la méthode suivante pour mettre à jour une image de boîtier Enforcer de la version 11.0 ou 11.0.2000 vers la version 11.0.3000.

Pour mettre à niveau l'image de boîtier Enforcer de 11.0 ou 11.0.2000 vers 11.0.3000

1. Insérez le CD dans le lecteur de CD-Rom du boîtier Enforcer.
2. Saisissez la commande suivante sur la console d'un boîtier Enforcer :

   ```
   Enforcer# update
   ```

Migrer l'image du boîtier Enforcer de 5.1.x vers 11.0.3000

Vous pouvez utiliser l'une des méthodes suivantes pour mettre à jour une image de boîtier Enforcer de la version 5.1.x vers la version 11.0.3000 :

- Migrer l'image de boîtier Enforcer de 5.1.x vers 11.0.3000 avec une clé USB (Universal Serial Bus).
- Migrer l'image de boîtier Enforcer de 5.1.x vers 11.0.3000 à partir d'un serveur TFTP.

Pour migrer l'image de boîtier Enforcer de 5.1.x vers 11.0.3 avec une clé USB

1. Copiez les deux fichiers de mise à jour, initrd-Enforcer.img.gpg et la liste de paquets, sur une clé USB.
2. Tapez la commande suivante pour mettre automatiquement à jour le boîtier Enforcer :

   Enforcer# `update`

   Se reporter à "Update" à la page 263.

Pour migrer l'image de boîtier Enforcer de 5.1.x vers 11.0.3000 à partir d'un serveur TFTP

1. Téléchargez les deux fichiers de mise à jour, initrd-Enforcer.img.gpg et la liste de paquets, sur un serveur TFTP (Trivial File Transfer Protocol) auquel le boîtier Enforcer peut se connecter.
2. Exécutez la commande suivante sur la console du boîtier Enforcer :

   Enforcer:# `update tftp://IP address of TFTP server`

   Se reporter à "Update" à la page 263.
3. Sélectionnez **Y** lorsque vous êtes invité à démarrer la nouvelle image.
4. Sélectionnez **1** pour redémarrer le boîtier Enforcer après avoir appliqué la nouvelle image.

   Il est déconseillé de lancer la nouvelle image sans redémarrer le boîtier Enforcer.
5. Connectez-vous au boîtier Enforcer.
6. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.

Recréer une image de boîtier Enforcer

Le boîtier Enforcer est livré avec un logiciel d'imagerie pour tous les boîtiers Enforcer : Gateway, LAN et DHCP. Le logiciel d'imagerie inclut le système d'exploitation Linux consolidé et le logiciel de boîtier Enforcer pour le remplacement d'une image de boîtier Enforcer.

Quand vous démarrez l'installation à partir du CD, le processus de création d'images efface la configuration existante sur le boîtier Enforcer. Les nouveaux fichiers remplacent tous les fichiers existants. Toute configuration précédemment définie sur le boîtier Enforcer est perdue.

Pour modifier le type de boîtier Enforcer que vous utilisez, installez une autre image de boîtier Enforcer. Si vous modifiez le type d'image d'un boîtier Enforcer, vous devrez éventuellement le replacer dans le réseau d'entreprise.

Se reporter à "Planifier l'installation de boîtiers Enforcer" à la page 47.

Pour créer des images pour un boîtier Enforcer

1. Insérez le CD dans le lecteur de CD-Rom du boîtier Enforcer.
2. A la ligne de commande, tapez la commande suivante :

   Enforcer:# `reboot`

   Cette commande redémarre le boîtier Enforcer.

3 Dans le menu Setup (Configuration), sélectionnez Setup Symantec Enforcer from the CD (Configurer Symantec Enforcer depuis le CD).

Si vous avez manqué le menu Setup, le boîtier Enforcer redémarre du disque plutôt que du CD. Pour créer une image, vous devez redémarrer à partir du CD.

4 Installez et configurez le boîtier Enforcer.

Se reporter à "Installer un boîtier Enforcer" à la page 84.

Chapitre 4

Première installation du boîtier Enforcer

Ce chapitre traite des sujets suivants :

Avant d'installer le boîtier Enforcer

Le boîtier Enforcer est un équipement qui impose le contrôle d'accès réseau aux clients qui essayent de se connecter au réseau. Si les clients sont conformes aux politiques de sécurité, l'accès aux ressources du réseau leur est permis.

Le type de boîtier Enforcer mis en œuvre dépend du type de produit Symantec Network Access Control dont vous avez fait l'acquisition.

Reportez-vous à votre accord de licence pour plus d'informations.

Vous pouvez déployer le boîtier Enforcer qui fonctionne avec Symantec Endpoint Protection Manager et les clients.

La gamme Enforcer inclut les types suivants :

- Boîtier Gateway Enforcer
- boîtier DHCP Enforcer
- LAN Enforcer, boîtier

A propos de l'installation du boîtier Gateway Enforcer

Un boîtier Gateway Enforcer est généralement utilisé en ligne comme pont d'application de politique sécurisée pour protéger un réseau d'entreprise des

intrus externes. Avant d'installer un boîtier Gateway Enforcer, vous devez penser à le localiser convenablement sur le réseau. Des boîtiers Gateway Enforcer peuvent être placés dans toute l'entreprise pour s'assurer que tous les terminaux client sont conformes à la politique de sécurité.

Vous pouvez utiliser des boîtiers Enforcer de passerelle pour protéger les serveurs au sein de l'entreprise. Ils peuvent s'assurer que seuls les clients de confiance ou authentifiés ont accès aux serveurs.

Les boîtiers Gateway Enforcer sont typiquement en service dans les emplacements réseau suivants :

- VPN
- Point d'accès sans fil (WAP)
- A distance (serveur d'accès à distance [RAS])
- Segments Ethernet (réseau LAN)

Se reporter à "Où placer le boîtier Gateway Enforcer" à la page 49.

A propos de l'installation du boîtier DHCP Enforcer

DHCP Enforcer est utilisé en ligne comme pont d'application de politique sécurisé pour protéger un réseau interne.

Les clients qui essayent de se connecter au réseau envoient une requête DHCP pour une adresse IP dynamique. Le commutateur ou le routeur (client de relais DHCP) achemine la requête DHCP. La requête DHCP est envoyée au boîtier DHCP Enforcer, configuré en série devant le serveur DHCP. Avant que le boîtier Enforcer de DHCP fasse suivre à la requête DHCP au serveur DHCP, le boîtier DHCP Enforcer vérifie que les clients sont conformes aux politiques de sécurité.

Si un client est conforme aux politiques de sécurité, le boîtier DHCP Enforcer envoie une demande client d'adresse IP au serveur DHCP normal.

Si le client ne se conforme pas aux politiques de sécurité, le boîtier DHCP Enforcer le connecte au serveur DHCP de quarantaine. Le serveur DHCP de quarantaine attribue au client une configuration réseau en quarantaine.

Pour finaliser la configuration DHCP Enforcer, vous devez paramétrer un serveur de résolution et restreindre l'accès des clients en quarantaine. Les clients restreints peuvent interagir seulement avec le serveur de résolution.

Si la haute disponibilité est requise, vous pouvez installer deux boîtiers DHCP Enforcer ou plus pour fournir des fonctions de basculement.

Se reporter à "Où placer les boîtiers DHCP Enforcer dans un réseau" à la page 59.

A propos de l'installation du boîtier LAN Enforcer

Le boîtier LAN Enforcer peut effectuer l'authentification d'hôte et agir en tant que serveur pseudo-RADIUS (même sans serveur RADIUS). Le client d'application agit en tant que supplicant 802.1x. Il répond à la stimulation EAP (Extensible Authentication Protocol) du commutateur avec les données d'état d'intégrité de l'hôte et de numéro de politique. L'adresse IP de serveur RADIUS est définie sur 0 dans ce cas et aucune authentification utilisateur EAP traditionnelle n'a lieu. Le boîtier LAN Enforcer vérifie l'intégrité de l'hôte. Il peut autoriser, bloquer ou affecter de manière dynamique une fonction VLAN, tel que nécessaire, selon les résultats de la vérification de l'intégrité de l'hôte.

Si vous avez Symantec Endpoint Protection, une autre configuration est également disponible. Vous pouvez utiliser le boîtier LAN Enforcer avec un serveur RADIUS pour imposer l'authentification 802.1x EAP dans un réseau d'entreprise. Si un boîtier LAN Enforcer est utilisé dans cette configuration, vous devez le placer de sorte qu'il puisse communiquer avec le serveur RADIUS.

Si votre commutateur prend en charge la commutation dynamique VLAN, des VLAN supplémentaires peuvent être configurés sur le commutateur et être accédés par le boîtier LAN Enforcer. L'option peut dynamiquement mettre le client dans un VLAN qui est basé sur la réponse du boîtier LAN Enforcer. Vous pouvez ajouter des VLAN pour la quarantaine et la résolution.

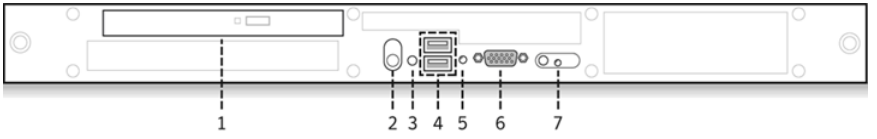
Se reporter à "Emplacement des boîtiers LAN Enforcer" à la page 68.

A propos des indicateurs et des commandes d'Enforcer

Le boîtier Enforcer est installé sur un châssis montable en rack 1U avec prise en charge pour les rails statiques.

Figure 4-1 illustre les commandes, les indicateurs et les connecteurs situés derrière le panneau en option sur le panneau avant.

Figure 4-1 Panneau avant du boîtier Enforcer

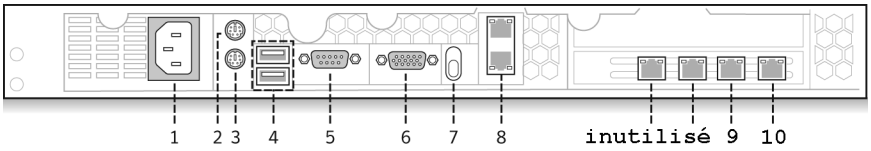


1	Lecteur de CD-ROM
2	Interrupteur d'alimentation
3	Icône de réinitialisation

4	Ports USB
5	Témoin lumineux du disque dur
6	Moniteur
7	Réservé ; ne pas utiliser

Figure 4-2 illustre le panneau arrière du système.

Figure 4-2 Panneau arrière du boîtier Enforcer (modèle Ouvert par défaut affiché)



1	Connecteur de cordon d'alimentation
2	Connecteur de souris
3	Connecteur de clavier
4	Ports USB
5	Port série
6	Moniteur
7	Réservé ; ne pas utiliser
8	Ports réseau réservés ; ne pas utiliser
9	port réseau eth0
10	port réseau eth1

Vous pouvez utiliser le port série fourni et le câble série pour connecter un autre système accroché à un écran et à un clavier. Alternativement, vous pouvez connecter un écran ou un clavier directement. Si vous vous connectez en utilisant le port série, la vitesse en bauds par défaut qui est définie sur Enforcer est 9600. Vous devez configurer la même connexion sur l'autre système. Se connecter par le port série est la méthode préférée. Cela vous permet de transférer des fichiers (tels que des informations de débogage) vers l'ordinateur connecté pour le dépannage.

Tableau 4-1 répertorie les spécifications matérielles du boîtier Enforcer.

Tableau 4-1 spécifications matérielles

Composant	Description
Unité de base	521, 2,8-GHz/1 Mo cache, Pentium 4 800-MHz bus latéral avant
Memory	1 Go DDR2, 533-MHz, 2x512 DIMM à rang unique
Disque dur	160 Go, SATA, 1-inch, disque dur 7200-RPM
Cartes réseau	Carte réseau unique à deux ports (par défaut, eth0 est le port interne de carte d'interface réseau et eth1 le port externe de carte d'interface réseau). Le modèle Ouvert par défaut a quatre ports, dont deux ne sont pas utilisés.
Lecteur de CD-ROM	24X, CD, 650 Mo, interne

Paramètres de carte d'interface réseau de boîtier Gateway Enforcer ou DHCP Enforcer

Sur un boîtier Gateway Enforcer ou DHCP Enforcer, les cartes d'interface réseau (cartes NIC) sont par défaut configurées comme suit :

eth0 — Carte d'interface réseau interne

Si vous utilisez un boîtier Gateway Enforcer, cette carte interne doit être connectée à la console Symantec Endpoint Protection Manager.

eth1 — Carte d'interface réseau externe

Si vous utilisez un boîtier DHCP Enforcer, cette carte externe doit être connectée à la console Symantec Endpoint Protection Manager.

Utilisez la commande configure interface-role (configurer le rôle de l'interface) si vous devez intervertir les cartes d'interface réseau externe et interne.

Se reporter à "Configure interface-role" à la page 276.

Pour DHCP Enforcer, utilisez cette commande avec l'option de manager, pour spécifier la carte d'interface réseau qui est utilisée pour se connecter à Symantec Endpoint Protection Manager.

L'exemple suivant affiche la syntaxe :

```
configure interface-role manager eth1
```

Se reporter à "Installer un boîtier Enforcer" à la page 84.

Installer un boîtier Enforcer

Avant de commencer l'installation d'un boîtier Enforcer, vous devez vous familiariser avec les emplacements des composants de votre réseau.

Se reporter à "Planifier l'installation de boîtiers Enforcer" à la page 47.

Le boîtier Symantec Network Access Control Enforcer est livré avec un CD d'installation appelé CD2 contenant le logiciel pour les composants suivants :

- Boîtier Gateway Enforcer
- LAN Enforcer, boîtier
- boîtier DHCP Enforcer

Vous sélectionnez le type de boîtier Enforcer que vous voulez choisir pendant l'installation.

Pendant l'installation d'un boîtier Enforcer, vous devez disposer des informations suivantes :

- Nom d'hôte à attribuer au boîtier Enforcer
  Le nom d'hôte par défaut est "Enforcer". Vous pouvez vouloir modifier ce nom pour faciliter l'identification des différents boîtiers Enforcer du réseau.
- Adresses IP des cartes d'interface réseau (cartes NIC) sur le boîtier Enforcer
- Adresse IP, nom d'hôte ou ID de domaine du serveur DNS le cas échéant
  Si vous voulez que le boîtier Enforcer se connecte à Symantec Endpoint Protection Manager à l'aide d'un nom d'hôte, il doit se connecter à un serveur DNS. Seuls les serveurs DNS peuvent résoudre les noms d'hôte. Vous pouvez configurer l'adresse IP du serveur DNS pendant l'installation.
  Toutefois, vous pouvez utiliser la commande configure DNS pour modifier l'adresse IP d'un serveur DNS.
  Se reporter à "Configure DNS" à la page 275.

L'installation d'un boîtier Enforcer implique les tâches suivantes :

- Installation du boîtier Enforcer
- Configuration du boîtier Enforcer

Pour installer un boîtier Enforcer

1. Déballer le boîtier Enforcer.
2. Montez le boîtier Enforcer en rack ou le déposer au niveau du sol.

   Consultez les instructions de montage de support fournies avec le boîtier Enforcer.
3. Branchez-le sur une prise électrique.

4 Connectez le boîtier Enforcer à l'aide d'une des méthodes suivantes :

- Connectez un autre ordinateur au boîtier Enforcer en utilisant un port série.
  Utilisez un câble de modem nul avec un connecteur DB9 (femelle). Vous devez utiliser un logiciel de terminal, tel que le HyperTerminal, CRT ou le NetTerm, pour accéder à la console d'Enforcer. Définissez votre logiciel de terminal sur 9600 bps, 8 bits de données, aucune parité, 1 bit d'arrêt, contrôle de débit nul.
  La connexion via la console série est la méthode conseillée, car elle permet les transferts de fichiers à partir du boîtier Enforcer.
- Reliez un clavier et un moniteur VGA directement au boîtier Enforcer.

5 Reliez les câbles Ethernet aux ports d'interface réseau comme suit :

boîtier Gateway Enforcer	Connectez deux câbles Ethernet : Un câble se connecte au port eth0 (carte d'interface réseau interne). L'autre câble se connecte au port eth1 (carte d'interface réseau externe) sur l'arrière du boîtier Enforcer. La carte d'interface réseau interne se connecte au réseau protégé et à Symantec Endpoint Protection Manager. La carte d'interface réseau externe se connecte aux terminaux client.
boîtier DHCP Enforcer	Connectez deux câbles Ethernet. Un câble se connecte au port eth0 (carte d'interface réseau interne). L'autre câble se connecte au port eth1 (carte d'interface réseau externe) à l'arrière du boîtier Enforcer. La carte d'interface réseau interne est reliée au serveur DHCP et la carte d'interface réseau externe est reliée aux terminaux client et au Symantec Endpoint Protection Manager.
LAN Enforcer, boîtier	Connectez un câble Ethernet au port eth0 à l'arrière du boîtier Enforcer. Ce câble se connecte au réseau interne. Le câble réseau est connecté à un commutateur compatible 802.1x ainsi qu'à tout autre commutateur 802.1x supplémentaire de votre réseau.

6 Mettez l'appareil sous tension.

Le boîtier Enforcer démarre.

7 Appuyez sur **Entrée** deux fois.

8 A l'invite, connectez-vous comme suit :

Console Login: root

Password: symantec

Le boîtier Enforcer déconnecte automatiquement les utilisateurs après 90 secondes d'inactivité.

Pour configurer un boîtier Enforcer

1 Spécifiez le type de boîtier Enforcer comme suit, en répondant aux invites du module d'application Enforcer :

```
1. Select Enforcer mode
[G] Gateway  [D] DHCP  [L] LAN
```

où :

G	Boîtier Gateway Enforcer
D	Boîtier DHCP Enforcer
L	Boîtier LAN Enforcer

2 Modifiez le nom d'hôte du boîtier Enforcer ou appuyez sur **Entrée** pour laisser le nom d'hôte du boîtier Enforcer inchangé.

Le nom d'hôte ou par défaut du boîtier Enforcer est "Enforcer". Le nom du boîtier Enforcer s'enregistre automatiquement sur Symantec Endpoint Protection Manager lors du prochain battement.

A l'invite, saisissez la commande suivante si vous voulez modifier le nom d'hôte du boîtier Enforcer :

```
2. Set the host name
Note:
1) Input new hostname or press "Enter" for no change. [Enforcer]:
```

`hostname` *hostname*

Se reporter à "Commande hostname" à la page 259.

où *hostname* représente le nouveau nom d'hôte du boîtier Enforcer.

Prenez-soin d'inscrire le nom d'hôte du boîtier Enforcer sur le serveur DNS proprement dit.

3 Saisissez la commande suivante pour confirmer le nouveau nom d'hôte du boîtier Enforcer :

```
show hostname
```

4 Saisissez l'adresse IP du serveur DNS et appuyez sur **Entrée**.

5 Tapez le nouveau mot de passe racine à l'invite en tapant d'abord la commande suivante :

mot de passe

Old password: symantec

New password: *new password*

Vous devez modifier le mot de passe racine utilisé pour ouvrir la session sur le boîtier Enforcer. L'accès à distance n'est pas activé jusqu'à ce que vous modifiiez votre mot de passe. Le nouveau mot de passe doit comporter au moins 9 caractères et contenir une lettre minuscule, une lettre majuscule, un chiffre et un symbole.

6 Tapez le nouveau mot de passe admin.

7 Définissez le fuseau horaire en suivant ces invites.

```
Set the time zone (Définissez le fuseau horaire)
Current time zone is [+0000]. Change it? [Y/n]
Si vous cliquez sur 'Y', suivez les étapes ci-dessous :
1) Select a continent or ocean (Sélectionnez un continent ou un océan)
2) Select a country (Sélectionnez un pays)
3) Select one of the time zone regions (Sélectionnez un fuseau horaire)
4) Set the date and time (Définissez la date et l'heure)
Enable the NTP feature (Activer la fonction NTP) [Y/n]
Set the NTP server (Définissez le serveur de NTP) :
Remarque : nous définissons le serveur NTP sous forme d'adresse IP
```

8 Définissez la date et l'heure.

9 Configurez les paramètres réseau et terminez l'installation en suivant les invites du module d'application Enforcer.

```
Entrez les paramètres réseau

Configure eth0:
Remarque : entrez de nouveaux paramètres.
IP address []:
Subnet mask []:
Set Gateway? [Y/n]
   Gateway IP[]:

   Apply all settings (Appliquer tous les paramètres) [Y/N] :
```

A propos du verrou de boîtier Enforcer

Le boîtier Enforcer est livré avec un panneau séparé qui peut être attaché au panneau avant. Il inclut une clé. Vous pouvez donc verrouiller le boîtier Enforcer pour plus de sécurité. L'utilisation du panneau est facultatif. Elle est recommandée pour plus de sécurité. Vous devez placer la clé dans un emplacement sécurisé.

Chapitre 5

Effectuer des tâches de base sur la console d'un boîtier Enforcer

Ce chapitre traite des sujets suivants :

A propos de l'exécution de tâches de base sur la console d'un boîtier Enforcer

Vous devez avoir déjà configuré les paramètres suivants pendant l'installation du boîtier Enforcer :

- Nom d'hôte du boîtier Enforcer
- Nom du groupe de boîtiers Enforcer auquel appartient un boîtier Enforcer particulier
- Adresses IP des cartes d'interface réseau interne et externe (cartes NIC)

- Adresse IP du serveur DNS, le cas échéant
- Adresse IP du serveur NTP, le cas échéant

Cependant, vous devez encore configurer une connexion entre un boîtier Enforcer et une installation Symantec Endpoint Protection Manager. Pour configurer cette connexion, exécutez la commande spm sur la console du boîtier Enforcer. Vous ne pouvez pas commencer l'utilisation d'un boîtier Enforcer avant d'avoir effectué cette tâche.

Se reporter à "Configurer une connexion entre un boîtier Enforcer et Symantec Endpoint Protection Manager" à la page 91.

Bien que vous gériez typiquement un boîtier Enforcer sur la console Symantec Endpoint Protection Manager après avoir terminé l'installation initiale et la configuration d'un boîtier Enforcer, vous pouvez encore devoir effectuer plusieurs tâches administratives sur la console d'un boîtier Enforcer. Si vous gérez de multiples boîtiers Enforcer, il est commode de les gérer tous à partir d'un emplacement centralisé.

Tous les boîtiers Enforcer disposent également une interface de ligne de commande (CLI) permettant d'exécuter des commandes de modification de tous les paramètres requis.

Se reporter à "A propos de la hiérarchie de commande d'interface de ligne de commande de boîtier Enforcer" à la page 231.

Se connecter à un boîtier Enforcer

Quand vous activez ou redémarrez le boîtier Enforcer, l'invite de connexion pour la console de boîtier Enforcer apparaît :

```
Connexion au module d'application
```

Les niveaux d'accès suivants sont disponibles :

Superuser (Superutilisateur)	Accès à toutes les commandes
Normal	Accès uniquement aux commandes `clear`, `exit`, `help` et `show` pour chaque niveau de hiérarchie de commande

Remarque : Le boîtier Enforcer déconnecte automatiquement les utilisateurs après 90 secondes d'inactivité.

Pour vous connecter à un boîtier Enforcer avec l'accès à toutes les commandes

1. Sur la ligne de commande, connectez-vous à un boîtier Enforcer avec l'accès à toutes les commandes en tapant la commande suivante :

   ```
   root
   ```

2. Entrez le mot de passe créé pendant l'installation initiale.

   Le mot de passe par défaut est symantec.

   L'invite de commande de la console pour la racine est Enforcer#.

Pour vous connecter à un boîtier Enforcer avec l'accès limité aux commandes

1. Si vous voulez vous connecter à un boîtier Enforcer avec l'accès limité aux commandes, tapez la commande suivante sur la ligne de commande :

   ```
   admin
   ```

2. Entrez le mot de passe à la ligne de commande.

   Le mot de passe par défaut est symantec.

   L'invite de commande de la console pour la racine est Enforcer$.

Configurer une connexion entre un boîtier Enforcer et Symantec Endpoint Protection Manager

Vous devez établir la communication entre le boîtier Enforcer et Symantec Endpoint Protection Manager sur la console Enforcer. Vous devez également avoir terminé l'installation du boîtier Enforcer et la configuration des cartes d'interface réseau internes et externes sur le boîtier Enforcer.

Se reporter à "Installer un boîtier Enforcer" à la page 84.

Pour établir la communication entre un boîtier Enforcer et Symantec Endpoint Protection Manager sur la console Enforcer, vous devez disposer des informations suivantes :

- adresse IP de Symantec Endpoint Protection Manager
  Vérifiez auprès de l'administrateur du serveur sur lequel Symantec Endpoint Protection Manager a été installé pour obtenir l'adresse IP.
- nom du groupe Enforcer auquel vous voulez attribuer le boîtier Enforcer
  Une fois terminée la configuration du nom de groupe Enforcer auquel vous voulez attribuer le boîtier Enforcer sur la console du boîtier, le nom du groupe est automatiquement enregistré sur Symantec Endpoint Protection Manager.
- Numéro de port utilisé pour communiquer avec le boîtier Enforcer sur Symantec Endpoint Protection Manager

Le numéro de port par défaut est 80.

- Le mot de passe chiffré créé pendant l'installation initiale de Symantec Endpoint Protection Manager

Pour configurer une connexion entre un boîtier Enforcer et Symantec Endpoint Protection Manager

1. A la ligne de commande sur la console d'un boîtier Enforcer, tapez `configure` (configurer).
2. Type

   `spm ip` *`adresse_IP`* `group` *`nom_groupe_Enforcer`* `http` *`numéro_port`* `key` *`mot de passe chiffré`*

   Se reporter à "Configure SPM" à la page 279.

   Vous pouvez vous baser sur l'exemple suivant :

   ```
   spm ip 192.168.0.64 group CorpAppliance
   http 80 key symantec
   ```

   Cet exemple configure le boîtier Enforcer pour communiquer avec le Symantec Endpoint Protection Manager d'adresse IP 192.168.0.64 dans le groupe CorpAppliance. Il utilise le protocole HTTP sur le port 80 avec un mot de passe chiffré ou un secret partagé de Symantec.
3. Vérifiez l'état de communication du boîtier Enforcer et de Symantec Endpoint Protection Manager.

   Se reporter à "Vérifier l'état de communication d'un boîtier Enforcer sur la console Enforcer" à la page 93.
4. Configurez, déployez et installez ou téléchargez le logiciel client si vous ne l'avez pas déjà fait.

   Reportez-vous au *Guide d'installation pour Symantec Endpoint Protection et Symantec Network Access Control* pour plus d'informations sur la configuration, le déploiement et l'installation des clients Symantec Endpoint Protection ou Symantec Network Access Control, également appelés client réseau.

   Si vous voulez que les invités - également appelés ordinateurs client autonomes - puissent télécharger automatiquement le client à la demande Symantec Network Access Control sur des plates-formes Windows et Macintosh, vous devez configurer un boîtier Gateway ou DHCP Enforcer pour gérer le processus de téléchargement automatique.

   Se reporter à "Activation de clients à la demande Symantec Network Access Control pour une connexion temporaire à un réseau " à la page 221.

Vérifier l'état de communication d'un boîtier Enforcer sur la console Enforcer

Vous pouvez vérifier l'état de communication d'un boîtier Enforcer depuis la console Enforcer.

Pour vérifier l'état de communication d'un boîtier Enforcer sur la console Enforcer

1 Connectez-vous à la console du boîtier Enforcer.

Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.

2 Tapez la commande suivante : **show status**

Vous pouvez afficher des informations sur l'état actuel de la connexion.

L'exemple suivant indique que le boîtier Enforcer est en ligne et connecté à Symantec Endpoint Protection Manager pour adresse IP 192.168.0.1 et pour port de communication 80 :

```
Enforcer#: show status
Enforcer Status:           ONLINE(ACTIVE)
Policy Manager Connected:  YES
Policy Manager:            192.168.0.1 HTTP 80
Packets Received:          3659
Packets Transmitted:       3615
Packet Receive Failed:     0
Packet Transfer Failed:    0
Enforcer Health:           EXCELLENT
Enforcer Uptime:           10 days 01:10:55
Policy ID:                 24/12/2007  21:31:55
```

Accès distant à un boîtier Enforcer

Pour communiquer de manière sécurisée avec le boîtier Enforcer pour un accès en ligne de commande, veuillez utiliser l'une des méthode suivantes :

- Commutateur KVM en réseau ou équivalent
- Client SSH prenant en charge le serveur de console SSH v2 Terminal
- Câble série

Rapports Enforcer et journaux de débogage

Vous pouvez afficher les rapports Enforcer et les journaux de débogage dans la console Symantec Endpoint Protection Manager et dans la console Enforcer.

Se reporter à "Rapports Enforcer" à la page 439.

Se reporter à "A propos des journaux Enforcer" à la page 440.

Chapitre 6

Configurer le boîtier Symantec Gateway Enforcer sur la console Symantec Endpoint Protection Manager

Ce chapitre traite des sujets suivants :

A propos de la configuration de boîtier Symantec Gateway Enforcer sur la console Symantec Endpoint Protection Manager

Vous pouvez ajouter ou modifier des paramètres de configuration pour le boîtier Gateway Enforcer dans la console Symantec Endpoint Protection Manager.

Avant de poursuivre, vous devez effectuer les tâches suivantes :

- Installez le logiciel de Symantec Endpoint Protection Manager sur un ordinateur.
  Consultez le *Guide d'installation de Symantec Endpoint Protection et de Symantec Network Access Control*.
  L'ordinateur sur lequel le logiciel Symantec Endpoint Protection Manager est installé est également désigné sous le nom de serveur de gestion.
- Connectez le boîtier Symantec Gateway Enforcer au réseau.
  Se reporter à "Pour installer un boîtier Enforcer" à la page 84.
- Configurez le boîtier de Symantec Gateway Enforcer sur la console Gateway Enforcer locale pendant l'installation.
  Se reporter à "Pour configurer un boîtier Enforcer" à la page 86.

Après avoir terminé ces tâches, vous pouvez spécifier des paramètres de configuration supplémentaires pour le boîtier Gateway Enforcer sur un serveur de gestion.

Quand vous installez un boîtier Gateway Enforcer, un certain nombre de paramètres par défaut et de ports sont automatiquement configurés. Les paramètres par défaut pour le boîtier Gateway Enforcer sur Symantec Protection Manager permettent à tous les clients de se connecter au réseau si le client réussit la vérification d'intégrité de l'hôte. Le boîtier Gateway Enforcer agit en tant que pont. Par conséquent, vous pouvez terminer la configuration du boîtier Gateway Enforcer et le déploiement des clients sans bloquer l'accès au réseau.

Cependant, vous devez modifier les paramètres par défaut sur Protection Manager afin de limiter les clients dont l'accès est autorisé sans authentification. En option, il existe d'autres paramètres par défaut du module Enforcer pour le boîtier Gateway Enforcer que vous pouvez personnaliser avant de démarrer l'application.

Modification des paramètres de configuration de boîtier Gateway Enforcer sur un serveur de gestion

Vous pouvez modifier les paramètres de configuration de boîtier Gateway Enforcer sur un serveur de gestion. Les paramètres de configuration sont automatiquement téléchargés depuis le serveur de gestion vers le boîtier Gateway Enforcer au cours du battement suivant.

Pour modifier les paramètres de configuration du boîtier Gateway Enforcer dans la console Symantec Endpoint Protection Manager

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez le groupe de modules Enforcer auxquels appartient le boîtier Gateway Enforcer.

   Le groupe de modules Enforcer doit inclure le boîtier Gateway Enforcer pour lequel les paramètres de configuration doivent être modifiés.
4. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez le boîtier Gateway Enforcer pour lequel les paramètres de configuration doivent être modifiés.

5 Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).

6 Dans la boîte de dialogue Settings (Paramètres), modifiez les paramètres de configuration.

La boîte de dialogue Settings (Paramètres) de Gateway Enforcer propose les catégories de paramètres de configuration suivantes :

General (Général)	Paramètres de description de groupe Enforcer et de liste de serveurs de gestion. Se reporter à "Utiliser les paramètres généraux" à la page 100.
Authentication (Authentification)	Réglages d'une série de paramètres qui affectent la procédure d'authentification client. Si une adresse correspondante n'est toujours pas localisée, le boîtier Gateway Enforcer commence la session d'authentification et envoie le paquet de stimulation. Se reporter à "Utiliser les paramètres d'authentification" à la page 103.
Auth Range (Plage d'authentification)	Paramètres spécifiant une adresse IP individuelle ou des plages IP pour un ou plusieurs clients à authentifier. Vous pouvez également spécifier une adresse IP individuelle ou des plages pour les clients autorisés à se connecter au réseau sans authentification. Se reporter à "Paramètres de plage d'authentification" à la page 118.
Advanced (Avancé)	Paramètres de délai d'authentification et de délai d'expiration de message de boîtier Gateway Enforcer. Paramètres d'adresses MAC pour les hôtes approuvés que le boîtier Gateway Enforcer autorise à se connecter sans authentification (facultatifs). Paramètres pour l'usurpation DNS et l'authentification locale. Paramètres de protocoles autorisés sans bloquage des clients. Se reporter à "Utilisation des paramètres avancés de boîtier Gateway Enforcer" à la page 129.

Log Settings (Paramètres de journal)	Paramètres permettant d'activer la consignation des journaux de serveur, des journaux d'activités client et de spécifier les paramètres de fichier journal. Se reporter à "Rapports Enforcer" à la page 439. Se reporter à "A propos des journaux Enforcer" à la page 440. Se reporter à "Configurer les paramètres du journal Enforcer" à la page 443.

Utiliser les paramètres généraux

Vous pouvez ajouter ou modifier la description d'un boîtier Gateway Enforcer ou d'un groupe de boîtiers Gateway Enforcer dans la console Symantec Endpoint Protection Manager.

Se reporter à "Ajout ou modification de la description d'un groupe de boîtiers Gateway Enforcer" à la page 101.

Se reporter à "Ajout ou modification de la description d'un boîtier Gateway Enforcer" à la page 101.

Vous ne pouvez pas ajouter ou modifier le nom d'un groupe de boîtiers Gateway Enforcer dans la console Symantec Endpoint Protection Manager. Vous ne pouvez pas ajouter ou modifier l'adresse IP ou le nom d'hôte d'un boîtier Gateway Enforcer dans la console Symantec Endpoint Protection Manager. Au lieu de cela, vous devez effectuer ces tâches sur la console Enforcer.

Vous pouvez ajouter ou modifier l'adresse IP ou le nom d'hôte d'un boîtier Gateway Enforcer dans une liste de serveurs de gestion.

Se reporter à "Ajout ou modification de l'adresse IP ou du nom d'hôte d'un boîtier Gateway Enforcer" à la page 102.

Vous pouvez également ajouter ou modifier l'adresse IP ou le nom d'hôte de Symantec Endpoint Protection Manager dans une liste de serveurs de gestion.

Se reporter à "Etablissement de la connexion entre un boîtier Gateway Enforcer et Symantec Endpoint Protection Manager via une liste de serveur de gestion" à la page 102.

Ajout ou modification de la description d'un groupe de boîtiers Gateway Enforcer

Vous pouvez ajouter ou modifier le nom d'un groupe d'Enforcer dont un boîtier Symantec Gateway Enforcer est membre. Vous pouvez effectuer cette tâche sur la console Symantec Endpoint Protection Manager au lieu de la console Enforcer.

Pour ajouter ou modifier la description d'un boîtier Gateway Enforcer

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. A la page Admin, sous View Servers (Afficher serveurs), sélectionnez et développez le groupe de boîtiers Gateway Enforcer dont vous souhaitez ajouter ou modifier la description.
4. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans la boîte de dialogue Settings (Paramètres), dans l'onglet Basic Settings (Paramètres de base), ajoutez ou modifiez une description pour le groupe de boîtiers Gateway Enforcer dans le champ Description.
6. Cliquez sur **OK**.

Ajout ou modification de la description d'un boîtier Gateway Enforcer

Vous pouvez ajouter ou modifier la description d'un boîtier Gateway Enforcer. Vous pouvez effectuer cette tâche sur la console Symantec Endpoint Protection Manager au lieu de la console Enforcer. Après avoir terminé cette tâche, la description apparaît dans le champ Description (Description) du volet Management Server (Gestion du serveur).

Pour ajouter ou modifier la description d'un boîtier Gateway Enforcer

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. A la page Admin, sous View Servers (Afficher serveurs), sélectionnez et développez le groupe de boîtiers Gateway Enforcer dont vous souhaitez ajouter ou modifier la description.
4. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez le boîtier Gateway Enforcer dont vous voulez ajouter ou modifier la description.

5 Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Enforcer Properties** (Modifier les propriétés d'Enforcer).

6 Dans la boîte de dialogue Properties (Propriétés) du module Enforcer, ajoutez ou modifiez une description pour le module Gateway Enforcer dans le champ Description.

7 Cliquez sur **OK**.

Ajout ou modification de l'adresse IP ou du nom d'hôte d'un boîtier Gateway Enforcer

Vous ne pouvez modifier l'adresse IP ou le nom d'hôte d'un boîtier Gateway Enforcer sur la console Gateway Enforcer que pendant l'installation. Si vous souhaitez modifier ultérieurement l'adresse IP ou le nom d'hôte d'un boîtier Gateway Enforcer, vous pouvez le faire dans la console Gateway Enforcer.

Se reporter à "Pour installer un boîtier Enforcer" à la page 84.

Se reporter à "Configure interface" à la page 275.

Se reporter à "Configure interface-role" à la page 276.

Etablissement de la connexion entre un boîtier Gateway Enforcer et Symantec Endpoint Protection Manager via une liste de serveur de gestion

Les boîtiers Gateway Enforcer doivent pouvoir se connecter aux serveurs sur lesquels Symantec Endpoint Protection Manager est installé. Symantec Endpoint Protection Manager comprend un fichier qui aide à la gestion du trafic entre les clients, les gestionnaires Symantec Endpoint Protection Manager et les modules d'application Enforcer facultatifs tels que le boîtier Gateway Enforcer.

Ce fichier est appelé liste de serveurs de gestion. La liste de serveurs de gestion spécifie à quel serveur Symantec Endpoint Protection Manager se connecte un module d'application Gateway Enforcer. Elle spécifie également à quel serveur Symantec Endpoint Protection un module d'application Gateway Enforcer se connecte en cas de défaillance d'un serveur de gestion.

Une liste de serveurs de gestion par défaut est automatiquement créée pour chaque site pendant l'installation initiale. Tous les gestionnaires Symantec Endpoint Protection Manager disponibles sur le site sont automatiquement ajoutés à la liste de serveurs de gestion par défaut.

La liste de serveurs de gestion par défaut comprend les adresses IP ou les noms d'hôte du serveur de gestion auxquels les boîtiers Gateway Enforcer peuvent se connecter après l'installation initiale. Vous pouvez créer une liste de serveurs de

gestion personnalisée avant de déployer des boîtiers Gateway Enforcer. Si vous créez une liste de serveurs de gestion personnalisée, vous pouvez spécifier la priorité de connexion d'un boîtiers Gateway Enforcer aux serveurs de gestion.

Si un administrateur a créé plusieurs listes de serveurs de gestion, vous pouvez sélectionner la liste de serveurs de gestion spécifique comprenant les adresses IP ou les noms d'hôte des serveurs de gestion auxquels vous voulez que le boîtier Gateway Enforcer se connecte. Si le site ne comprend qu'un seul serveur de gestion, vous pouvez sélectionner la liste de serveurs de gestion par défaut.

Consultez le *Guide d'administration de Symantec Endpoint Protection et Symantec Network Access Control* pour plus d'informations sur la personnalisation des listes de serveurs de gestion.

Pour établir la communication entre Gateway Enforcer et Symantec Endpoint Protection Manager

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.

   Le groupe Enforcer doit contenir le boîtier Gateway Enforcer dont vous souhaitez modifier l'adresse IP ou le nom d'hôte dans une liste de serveur de gestion.
4. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans la boîte de dialogue Paramètres, dans l'onglet Paramètres de base, sous Communication, sélectionnez la liste de serveurs de gestion à utiliser par ce boîtier Gateway Enforcer.
6. Dans la boîte de dialogue Paramètres, dans l'onglet Paramètres de base, sous Communication, cliquez sur **Aperçu**.

   Vous pouvez afficher les adresses IP et les noms d'hôte de tous les serveurs de gestion disponibles, ainsi que les priorités qui leur ont été attribuées.
7. Dans la boîte de dialogue Listes de serveurs de gestion, cliquez sur **Fermer**.
8. Dans la boîte de dialogue Settings (Paramètres), cliquez sur **OK**.

Utiliser les paramètres d'authentification

Vous pouvez spécifier un certain nombre de paramètres d'authentification pour une session d'authentification de boîtier Gateway Enforcer. Lorsque vous appliquez

ces modifications, elles sont envoyées automatiquement au boîtier Gateway Enforcer sélectionné, pendant le battement suivant.

A propos de l'utilisation des paramètres d'authentification

Vous pouvez mettre en application un certain nombre de paramètres d'authentification pour sécuriser d'avantage le réseau.

Tableau 6-1 fournit plus d'informations sur les options de l'onglet Authentification.

Tableau 6-1 Paramètres de configuration d'authentification pour un boîtier Gateway Enforcer

Option	Description
Nombre maximal de paquets par session d'authentification	Nombre maximal de paquets de sollicitation que lr boîtier Gateway Enforcer envoie dans chaque session d'authentification. Le nombre par défaut est de 10. Il peut varier entre 2 et 100 paquets. Se reporter à "Spécifier le nombre maximum de paquets pendant une session d'authentification" à la page 108.
Durée (en secondes) entre les paquets en session d'authentification	Durée (en secondes) entre les paquets de sollicitation envoyés par Enforcer. La valeur par défaut est 3 secondes. Elle peut varier entre 3 et 10 secondes. Se reporter à "Spécification de la fréquence des paquets de stimulation à envoyer aux clients" à la page 109.
Durée de bloquage du client rejeté (en secondes)	Durée en secondes du bloquage d'un client ayant échoué à l'authentification. Le paramètre par défaut est 30 secondes. L'intervalle est compris entre 10 et 300 secondes. Se reporter à "Spécifier la période pendant laquelle un client est bloqué après échec de son authentification" à la page 110.
Durée d'autorisation du client authentifié (en secondes)	Durée en secondes de l'autorisation de maintien de la connexion réseau du client sans réauthentication. Le paramètre par défaut est 30 secondes. L'intervalle est compris entre 10 et 300 secondes. Se reporter à "Spécifier la période durant laquelle un client est autorisé à maintenir sa connexion réseau sans réauthentification" à la page 111.

Option	Description
Autoriser tous les clients, mais continuer à consigner les clients non authentifiés	Si cette option est activée, le boîtier Gateway Enforcer authentifie tous les utilisateurs en vérifiant qu'ils exécutent un client. Le boîtier d'application Gateway Enforcer vérifie également si le client a réussi la vérification de l'intégrité de l'hôte. Si le client a réussi la vérification de l'intégrité de l'hôte, le boîtier Gateway Enforcer consigne les résultats. Il transfère alors la demande Gateway de recevoir une configuration réseau normale plutôt qu'une configuration réseau de quarantaine, indépendamment de l'échec ou de la réussite des vérifications. Le paramètre n'est pas activé par défaut. Se reporter à "Autorisation de tous les clients avec la connexion continue des clients non-authentifiés" à la page 112.
Permettre tous les clients avec des systèmes d'exploitation non Windows	Si cette option est activée, Gateway Enforcer vérifie le système d'exploitation du client. Le boîtier Gateway Enforcer permet alors à tous les clients n'exécutant pas le système d'exploitation Windows de recevoir une configuration réseau normale sans être authentifié. Si cette option n'est pas activée, les clients reçoivent une configuration réseau de quarantaine. Le paramètre n'est pas activé par défaut. Se reporter à "Autorisation des clients non-Windows à se connecter à un réseau sans authentification" à la page 113.
Vérifier le numéro de série de politique du Client avant de permettre au client d'accéder au réseau	Si cette option est activée, le boîtier Gateway Enforcer vérifie si le client a reçu les dernières politiques de sécurité du serveur de gestion. Si le numéro de série de politique n'est pas le plus récent, Gateway Enforcer informe le client de la nécessité de mise à jour de sa politique de sécurité. Le client transfère alors la demande Gateway de recevoir une configuration réseau de quarantaine. Si cette option n'est pas activée et si la vérification de l'intégrité de l'hôte réussit, le boîtier Gateway Enforcer transfère la demande Gateway de recevoir une configuration réseau normale. Gateway Enforcer transfère la demande même si le client n'a pas la dernière politique de sécurité. Le paramètre n'est pas activé par défaut. Se reporter à "Vérification par le boîtier Gateway Enforcer du numéro de série de politique sur un client" à la page 114.

Option	Description
Activer le message instantané sur le client si le logiciel client ne s'exécute pas	Si cette option est activée, un message est affiché pour les utilisateurs des ordinateurs Windows sans client qui essaient de se connecter à un réseau d'entreprise. Le message par défaut est défini pour s'afficher une seule fois. Le message indique aux utilisateurs que leur accès au réseau est bloqué en raison de l'absence de client en cours d'exécution et leur indique de l'installer. Pour modifier le message ou sa fréquence d'affichage, vous pouvez cliquer sur Message. La longueur maximale du message est de 128 caractères. Le paramètre par défaut est activé. Se reporter à "Envoi d'un message de non-conformité du boîtier Gateway Enforcer à un client" à la page 115.
Activer la redirection HTTP du client si le logiciel client ne s'exécute pas	Si cette option est activée, le boîtier Gateway Enforcer peut rediriger les clients vers un site Web de résolution. Si cette option est activée, le boîtier Gateway Enforcer redirige les requêtes HTTP vers un serveur Web interne si le client n'est pas exécuté. Cette option ne peut pas être activée sans avoir spécifié une URL. Le paramètre par défaut est activé, avec la valeur http://localhost. Se reporter à "Rediriger des requêtes HTTP vers une page Web" à la page 117.
URL de redirection HTTP	Vous pouvez indiquer une URL contenant jusqu'à 255 caractères lorsque vous redirigez les clients vers un site Web de résolution. Le paramètre par défaut pour l'URL de redirection est http://localhost. Se reporter à "Rediriger des requêtes HTTP vers une page Web" à la page 117.
Port de redirection HTTP	Vous pouvez indiquer un numéro de port autre que 80 lorsque vous redirigez les clients vers un site Web de résolution. Le paramètre par défaut pour le serveur Web est le port 80. Se reporter à "Rediriger des requêtes HTTP vers une page Web" à la page 117.

A propos des sessions d'authentification sur un boîtier Gateway Enforcer boîtier

Lorsqu'un client essaie d'accéder au réseau interne, le boîtier Gateway Enforcer établit une session d'authentification. Une session d'authentification représente un ensemble de paquets envoyés à un client depuis un boîtier Gateway Enforcer.

Pendant la session d'authentification, le boîtier Gateway Enforcer envoie un paquet au client à une fréquence spécifiée. Le paramètre par défaut est de toutes les trois secondes. Gateway Enforcer continue à envoyer des paquets jusqu'à ce qu'il reçoive une réponse du client ou qu'il ait envoyé le nombre maximum spécifié de paquets. Le nombre par défaut est de 10.

Si le client réagit et réussit l'authentification, le boîtier Gateway Enforcer l'autorise à accéder au réseau interne pendant un nombre spécifié de secondes. Le paramètre par défaut est de 30 secondes. Le boîtier Gateway Enforcer démarre une nouvelle session d'authentification pendant laquelle le client doit réagir pour conserver sa connexion au réseau interne. Le boîtier Gateway Enforcer déconnecte les clients ne répondant pas ou ayant été rejetés suite à un échec d'authentification.

Si le client ne réagit pas ou échoue à l'authentification, le boîtier Gateway Enforcer le bloque pendant un nombre spécifié de secondes. Le paramètre par défaut est 30 secondes. Tout client qui essaie de se connecter à l'aide de cette adresse IP doit être authentifié à nouveau.

Vous pouvez configurer la session d'authentification pour chaque boîtier Gateway Enforcer sur le serveur de gestion.

A propos de l'authentification client sur un boîtier Gateway Enforcer boîtier

Le boîtier Gateway Enforcer authentifie les clients distants avant de les autoriser à accéder au réseau. L'authentification client effectuée par Gateway Enforcer propose les fonctions suivantes :

- Elle permet de choisir entre une authentification ou une autorisation sans authentification du client.
  Dans l'onglet Plage d'authentification, vous pouvez spécifier un client ou une plages d'adresses IP que vous souhaitez authentifier ou auxquels vous souhaitez faire confiance.
- Elle permet de procéder à la session d'authentification.
  Vous configurez les paramètres pour la session d'authentification dans l'onglet Authentification.

Gateway Enforcer met à jour les listes suivantes d'adresses IP approuvées qui sont autorisées à se connecter au réseau par son biais :

- Une liste statique :
  adresses IP externes approuvées qui sont configurées pour Enforcer dans l'onglet Plage d'authentification.
- Une liste dynamique :
  Les adresses IP approuvées supplémentaires qui sont ajoutées et laissées en tant que clients sont authentifiées, autorisées à se connecter au réseau, puis enfin déconnectées.

Lorsque le trafic arrive à partir d'un nouveau client, le boîtier Gateway Enforcer détermine si le client est compris dans la liste des adresses IP client approuvées. Si le client possède une adresse IP approuvée, il est autorisé sur le réseau sans autre authentification.

Si le client n'a pas d'adresse IP approuvée, le boîtier Gateway Enforcer vérifie si l'adresse IP approuvée figure dans la plage IP des clients devant être authentifiés. Si l'adresse IP du client figure dans cette plage, le boîtier Gateway Enforcer démarre une session d'authentification.

Au cours de la session d'authentification, le client envoie son numéro d'identification unique, les résultats de la vérification de l'intégrité de l'hôte ainsi que son numéro de série de politique. Le numéro de série de politique permet de vérifier que les politiques de sécurité du client sont à jour.

Le boîtier Gateway Enforcer vérifie les résultats. Il peut éventuellement cocher la case Policy Serial Number (Numéro de série de police). Si les résultats sont valides, le boîtier Gateway Enforcer donne un état authentifié au client et lui autorise l'accès au réseau. Si les résultats sont invalides, le boîtier empêche le client de se connecter au réseau.

Quand un client est authentifié, son adresse IP est ajoutée à la liste dynamique avec un temporisateur. L'intervalle par défaut du temporisateur est de 30 secondes. Une fois que l'intervalle de la minuterie est écoulé, le boîtier Gateway Enforcer démarre une nouvelle session d'authentification avec le client. Si le client ne répond pas ou si l'authentification échoue, son adresse IP est supprimée de la liste. L'adresse IP est également bloquée pendant un intervalle spécifique. Le paramètre par défaut est 30 secondes. Lorsqu'un autre client essaie de se connecter au moyen de la même adresse IP, il doit être authentifié à nouveau.

Spécifier le nombre maximum de paquets pendant une session d'authentification

Pendant la session d'authentification, le boîtier Gateway Enforcer envoie un paquet de stimulation au client à une fréquence spécifiée.

Le boîtier Gateway Enforcer continue d'envoyer des paquets jusqu'à ce que les conditions suivantes soient remplies :

- Le boîtier Gateway Enforcer reçoit une réponse du client.
- Le boîtier Gateway Enforcer a envoyé le nombre maximum spécifié de paquets.

Le paramètre par défaut pour le nombre maximum de paquets de stimulation pour une session d'authentification est 10. Il peut varier entre 2 et 100 paquets.

Pour spécifier le nombre maximum de paquets de stimulation pendant une session d'authentification

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.

   Le groupe de modules d'application Enforcer doit inclure le boîtier Gateway Enforcer pour lequel vous voulez spécifier le nombre maximum de paquets de stimulation pendant une session d'authentification.
4. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans la boîte de dialogue Gateway Settings (Paramètres de la passerelle), dans l'onglet Authentication (Authentification), sous Authentication Parameters (Paramètres d'authentification), saisissez le nombre maximum de paquets que vous voulez autoriser pendant une session d'authentification dans le champ **Maximum number of packets per authentication session** (Nombre maximum de paquets par session d'authentification).

   Le paramètre par défaut est 10 secondes. Il peut varier entre 2 et 100 paquets.
6. Dans la boîte de dialogue Gateway Settings (Paramètres de la passerelle), dans l'onglet Authentication (Authentification), cliquez sur **OK**.

Spécification de la fréquence des paquets de stimulation à envoyer aux clients

Pendant la session d'authentification, le boîtier Gateway Enforcer envoie un paquet de stimulation au client à une fréquence spécifiée.

Le boîtier Gateway Enforcer continue d'envoyer des paquets jusqu'à ce que les conditions suivantes soient remplies :

- Le boîtier Gateway Enforcer reçoit une réponse du client
- Le boîtier Gateway Enforcer a envoyé le nombre de paquets maximum spécifié.

Le paramètre par défaut est toutes les 3 secondes. L'intervalle est comprise entre 3 à 10 secondes.

Pour spécifier la fréquence des paquets de stimulation à envoyer aux clients

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.

   Le groupe de boîtiers Enforcer doit inclure le boîtier Gateway Enforcer pour lequel vous voulez spécifier la fréquence des paquets de stimulation à envoyer aux clients.
4. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans la boîte de dialogue Settings (Paramètres), dans l'onglet Authentication (Authentification), sous Authentication Parameters (Paramètres d'authentification), tapez le nombre maximum de paquets de stimulation que le module Gateway Enforcer doit envoyer à un client pendant une session d'authentification dans le champ Time between packets in authentication session (Temps entre les paquets pendant la session d'authentification).

   Le paramètre par défaut est de 3 secondes. L'intervalle est compris entre 3 et 10 secondes.
6. Dans la boîte de dialogue Settings (Paramètres), sur l'onglet Authentication (Authentification), cliquez sur **OK**.

Spécifier la période pendant laquelle un client est bloqué après échec de son authentification

Vous pouvez spécifier le laps de temps pendant lequel un client est bloqué après échec de son authentification.

Le paramètre par défaut est de 30 secondes. L'intervalle est compris entre 10 et 300 secondes.

Pour spécifier la période pendant laquelle un client est bloqué après échec de son authentification

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).

3 Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.

Le groupe de modules d'application Enforcer doit inclure le boîtier Gateway Enforcer pour lequel vous voulez spécifier le temps pendant lequel un client est bloqué en cas d'échec de son authentification.

4 Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).

5 Dans la boîte de dialogue Settings (Paramètres), dans l'onglet Authentication (Authentification), sous Authentication Parameters (Paramètres d'authentification), saisissez le nombre de secondes pour la durée de temps pendant laquelle un client est bloqué en cas d'échec de son authentification dans le champ de **temps de blocage du client rejeté (secondes)**.

Le paramètre par défaut est 30 secondes. L'intervalle est comprise entre 10 à 300 secondes.

6 Cliquez sur **OK**.

Spécifier la période durant laquelle un client est autorisé à maintenir sa connexion réseau sans réauthentification

Vous pouvez spécifier la durée de temps en secondes pendant lequel un client est autorisé à maintenir sa connexion réseau sans réauthentification.

Le paramètre par défaut est de 30 secondes. L'intervalle est compris entre 10 et 300 secondes.

Pour spécifier la période durant laquelle un client est autorisé à maintenir sa connexion réseau sans réauthentification

1 Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).

2 Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).

3 Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.

Le groupe de modules d'application Enforcer doit inclure le boîtier Gateway Enforcer pour lequel vous voulez spécifier le temps pendant lequel un client est bloqué en cas d'échec de son authentification.

4 Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).

5 Dans la boîte de dialogue Settings (Paramètres), dans l'onglet Authentication (Authentification), sous Authentication Parameters (Paramètres d'authentification), saisissez le nombre de secondes pendant lesquelles un client est autorisé à maintenir sa connexion réseau sans réauthentification dans le champ pour le **temps durant lequel un client authentifié est autorisé (secondes)**.

   Le paramètre par défaut est 30 secondes. L'intervalle est comprise entre 10 à 300 secondes.

6 Cliquez sur **OK**.

Autorisation de tous les clients avec la connexion continue des clients non-authentifiés

Déployer l'ensemble des logiciels client peut prendre un certain temps. Vous pouvez vouloir configurer le boîtier Gateway Enforcer pour permettre à tous les clients de se connecter au réseau jusqu'à ce que vous ayez fini de distribuer le paquet client à tous les utilisateurs. Un boîtier Gateway Enforcer bloque tous les clients qui n'exécutent pas le client. Puisque le client ne s'exécute pas sur les systèmes d'exploitation non-Windows tels que Linux ou Solaris, le boîtier Gateway Enforcer bloque ces clients. Vous pouvez choisir d'autoriser tous les clients non-Windows à se connecter au réseau.

Si un client n'est pas authentifié avec ce paramètre, le boîtier Gateway Enforcer détecte le type de système d'exploitation. Par conséquent, les clients sont bloqués et les clients non Windows sont autorisés à accéder au réseau.

Le paramètre n'est pas activé par défaut.

Suivez les directives ci-dessous quand vous appliquez les paramètres de configuration :

- Ce paramètre doit être une mesure temporaire parce qu'il rend le réseau moins sécurisé.
- Lorsque ce paramètre est en vigueur, vous pouvez passer en revue les journaux Enforcer. Vous pouvez vous renseigner sur les types de clients qui essayent de se connecter au réseau à cet emplacement.

  Par exemple, vous pouvez passer en revue le journal d'activités client pour savoir si des clients ne disposent pas du logiciel client. Vous pouvez ensuite vérifier que le logiciel client est installé sur ces clients avant de désactiver cette option.

Pour autoriser tous les clients avec la connexion continue des clients non-authentifiés

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.

   Le groupe Enforcer doit inclure le boîtier Gateway Enforcer pour lequel vous voulez autoriser tous les clients tout en continuant la consignation des clients non-authentifiés.
4. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans la boîte de dialogue Paramètres, dans l'onglet Authentification, cochez **Allow all clients, but continue to log which clients are not authenticated** (Autoriser tous les clients, mais continuer à consigner les clients non authentifiés).

   Le paramètre n'est pas activé par défaut.
6. Dans la boîte de dialogue Settings (Paramètres), sur l'onglet Authentication (Authentification), cliquez sur **OK**.

Autorisation des clients non-Windows à se connecter à un réseau sans authentification

Le boîtier Gateway Enforcer ne peut pas authentifier un client utilisant un système d'exploitation non-Windows. Par conséquent les clients non-Windows ne peuvent pas se connecter au réseau à moins que vous ne les autorisiez spécifiquement à se connecter au réseau sans authentification.

Le paramètre n'est pas activé par défaut.

Vous pouvez utiliser une des méthodes suivantes pour activer les clients qui prennent en charge une plate-forme non-Windows pour se connecter au réseau :

- Spécifiez chaque client non-Windows comme hôte approuvé.
- Autorisez tous les clients avec des systèmes d'exploitation non-Windows

Le boîtier Gateway Enforcer détecte le système d'exploitation du client et authentifie les clients Windows. Cependant, il ne permet pas à des clients non-Windows de se connecter au boîtier Gateway Enforcer sans authentification.

Si vous voulez que des clients non-Windows se connectent au réseau, vous devez configurer des paramètres supplémentaires sur la console Symantec Endpoint Protection Manager.

Se reporter à "Conditions requises pour l'autorisation de clients non-Windows sans authentification" à la page 54.

Pour autoriser des clients non-Windows à se connecter à un réseau sans authentification

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.

   Le groupe Enforcer doit inclure le boîtier Gateway Enforcer pour lequel vous voulez autoriser l'ensemble des clients non-Windows à se connecter à un réseau.
4. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans la boîte de dialogue Settings (Paramètres), dans l'onglet Authentication (Authentification), cochez **Allow all clients with non-Windows operating systems** (Autoriser tous les clients avec des systèmes d'exploitation non-Windows).

   Le paramètre n'est pas activé par défaut.
6. Cliquez sur **OK**.

Vérification par le boîtier Gateway Enforcer du numéro de série de politique sur un client

Symantec Endpoint Protection Manager met à jour le numéro de série de politique d'un client chaque fois que la politique de sécurité du client change. Quand un client se connecte à Symantec Endpoint Protection Manager, il reçoit les dernières politiques de sécurité et le dernier numéro de série de politique.

Lorsqu'un client essaye de se connecter au réseau via le boîtier Gateway Enforcer, ce dernier récupère le numéro de série de politique à partir de Symantec Endpoint Protection Manager. Le boîtier Gateway Enforcer compare ensuite le numéro de série de politique à celui qu'il reçoit du client. Si les numéros de série de politique correspondent, cela signifie que le boîtier Gateway Enforcer a validé l'exécution par le client d'une politique de sécurité à jour.

La valeur par défaut pour ce paramètre n'est pas activée.

Les directives suivantes s'appliquent :

- Si l'option Vérifier le numéro de série de la politique du client avant de permettre à un client d'accéder au réseau est cochée, un client doit disposer de la dernière politique de sécurité avant de pouvoir se connecter au réseau par le boîtier Gateway Enforcer. Si le client ne dispose pas de la dernière politique de sécurité, le client est informé qu'il doit télécharger la dernière politique. Le boîtier Gateway Enforcer fait alors suivre sa requête Gateway pour recevoir une configuration réseau de quarantaine.
- Si l'option Vérifier le numéro de série de la politique du client avant de permettre à un client d'accéder au réseau n'est pas cochée et si la vérification de l'intégrité de l'hôte est réussie, le client peut se connecter au réseau. Le client peut se connecter via le boîtier Gateway Enforcer même si sa police de sécurité n'est pas à jour.

Pour faire vérifier par le boîtier Gateway Enforcer le numéro de série de politique sur un client

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Administrateur), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de boîtiers Gateway Enforcer.

   Le groupe Enforcer doit inclure le boîtier Gateway Enforcer qui vérifie le numéro de série de politique des clients.
4. Dans la boîte de dialogue Paramètres, dans l'onglet Authentification, cochez **Vérifier le numéro de série de politique sur le client avant de permettre à un client d'accéder au réseau**.
5. Cliquez sur **OK**.

Envoi d'un message de non-conformité du boîtier Gateway Enforcer à un client

Vous pouvez informer le client qui ne peut pas se connecter au réseau avec un message déroulant de Windows. Généralement, le message informe l'utilisateur final qu'un client ne peut pas se connecter au réseau. Le client ne peut pas se connecter au réseau parce qu'il n'exécute pas le client Symantec Network Access Control.

La plupart des administrateurs entrent des instructions sur la nécessité d'exécuter le client Symantec Endpoint Protection ou le client Symantec Network Access Control. Le message peut comprendre des informations sur un site de téléchargement où les utilisateurs finaux peuvent télécharger le logiciel client

requis. Vous pouvez également fournir un numéro de téléphone de contact ou d'autres informations importantes.

Ce paramètre est activé par défaut. Il s'applique seulement aux clients qui n'exécutent pas le client Symantec Endpoint Protection ou le client Symantec Network Access Control.

Dès que vous terminez cette tâche, le message instantané s'affiche sur le client s'il exécute Windows Messenger.

Pour envoyer un message de non-conformité depuis un boîtier Gateway Enforcer vers un client

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.
4. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans la boîte de dialogue Settings (Paramètres), dans l'onglet Authentication (Authentification), sélectionnez **Enable pop-up message on client if Client is not running** (Activer le message instantané sur le client si le logiciel client ne s'exécute pas).
6. Cliquez sur **Message**.
7. Dans la boîte de dialogue Settings (Paramètres) des messages instantanés, sélectionnez la fréquence d'affichage du message sur un client dans la liste Following message will pop-up (Le message suivant s'affichera).

   Vous pouvez sélectionner les intervalles suivants :

   - Once (Une fois)
     La valeur par défaut est Une fois.
   - Every 30 seconds (Toutes les 30 secondes)
   - Every minute (Toutes les minutes)
   - Every 2 minutes (Toutes les 2 minutes)
   - Every 5 minutes (Toutes les 5 minutes)
   - Every 10 minutes (Toutes les 10 minutes)

8 Tapez le message à afficher dans la zone de texte.

Vous pouvez saisir jusqu'à 125 caractères, y compris les espaces et les signes de ponctuation.

Le message par défaut est :

```
You are blocked from accessing the network because you
do not have the Symantec Client running.  You will need to
install it.
```

9 Cliquez sur **OK**.

10 Dans la boîte de dialogue Settings (Paramètres), sur l'onglet Authentication (Authentification), cliquez sur **OK**.

Rediriger des requêtes HTTP vers une page Web

Le boîtier Gateway Enforcer a une option de redirection des requêtes HTTP vers un serveur Web interne si le client essaye d'accéder à un site Web interne par un navigateur et si un client ne s'exécute pas sur le client. Si vous ne spécifiez pas d'URL, le message instantané du boîtier Gateway Enforcer apparaît en tant que corps du message HTML pour la première page HTML. Vous souhaitez peut-être connecter des utilisateurs à une page Web que vous avez définie. Les clients peuvent télécharger un logiciel de résolution à partir de ce site Web. Le boîtier Gateway Enforcer peut rediriger la requête HTTP GET vers un URL que vous spécifiez.

Ce paramètre est activé par défaut.

Par exemple, vous pouvez rediriger une requête vers un serveur Web à partir duquel le client peut télécharger le logiciel client, les correctifs ou les versions à jour des applications.

Pour rediriger des requêtes HTTP vers une page Web

1 Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).

2 Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).

3 Dans la page Admin (Administrateur), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de boîtiers Gateway Enforcer.

4 Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).

5 Dans la boîte de dialogue Gateway Settings (Paramètres de la passerelle), dans l'onglet Authentication (Authentification), cochez l'option **Check HTTP redirect on client if the client is not running** (Vérifier la redirection HTTP sur le client si celui-ci ne s'exécute pas).

6 Tapez l'URL dans le champ URL de redirection HTTP.

L'hôte de l'URL de redirection doit être Symantec Endpoint Protection Manager ou une adresse IP listée comme faisant partie de l'intervalle d'IP interne approuvé.

L'URL peut comporter jusqu'à 255 caractères.

Si vous voulez spécifier le nom d'un serveur Web, vous devez également activer l'option Allow all DNS request packets (Autoriser tous les paquets de requête DNS) dans l'onglet Advanced (Avancé).

Si vous laissez le champ URL vide puis cliquez sur **OK**, le message suivant s'affiche :

```
The HTTP redirect URL must be a valid URL.
```

Il utilise également le message contextuel Gateway Enforcer en corps HTML pour la première page HTML renvoyée au client.

7 Dans la boîte de dialogue Gateway Settings (Paramètres de passerelle), dans l'onglet Authentication (Authentification), cliquez sur **OK**.

Paramètres de plage d'authentification

Vous pouvez configurer les paramètres suivants :

- Adresses IP client que le boîtier Gateway Enforcer authentifie
- Adresses IP externes que le boîtier Gateway Enforcer n'authentifie pas.
- Adresses IP internes auxquelles le boîtier Gateway Enforcer autorise l'accès

Une fois que vous avez appliqué ces paramètres, les modifications sont envoyées au boîtier Gateway Enforcer sélectionné pendant le battement suivant. Gardez à l'esprit les informations suivantes :

- L'option Authentifier seulement les clients avec ces adresses IP est sélectionnée par défaut. Si cette option reste sélectionnée et si vous ne spécifiez aucune adresse IP à authentifier, le boîtier Gateway Enforcer sert de pont de réseau et autorise l'accès à tous les clients.
- Pour les adresses IP externes approuvées, vous devez ajouter l'adresse IP du serveur VPN d'entreprise ainsi que toutes les autres adresses IP autorisées à accéder au réseau d'entreprise sans exécuter un client. Il se peut que vous

souhaitiez également inclure les périphériques ayant normalement accès au réseau et qui exécutent un autre système d'exploitation que Windows.

- Pour les adresses IP internes approuvées, vous devez spécifier des adresses, telles qu'un serveur de mise à jour, un serveur contenant des fichiers de signature antivirus, un serveur utilisé pour la résolution ou un serveur DNS ou WINS requis pour résoudre les noms de domaine ou d'hôte.
- Si vous indiquez que le boîtier Gateway Enforcer doit vérifier que le profil du client est à jour, les clients peuvent avoir besoin de se connecter à la console Symantec Endpoint Protection Manager pour télécharger les dernières politiques de sécurité. Si vous utilisez cette option quand vous vous référez à Symantec Endpoint Protection Manager par nom DNS ou nom d'hôte, vous devez ajouter l'adresse IP du serveur DNS ou du serveur WINS à la liste d'adresses IP internes approuvées.

Comparaison des plages d'adresses IP du client et des adresses IP externes approuvées

La plage d'adresses IP du client est semblable à une liste noire. Vous pouvez spécifier les adresses IP client indiquant au boîtier Gateway Enforcer de ne vérifier que ces adresses IP spécifiques pour voir si elles exécutent le client et satisfont les polices de sécurité. Un client qui ne figure pas dans la liste IP client est considéré comme ayant reçu une adresse IP approuvée.

Contrairement à la plage d'adresses IP du client, les adresses IP externes approuvées sont semblables à une liste blanche. Si vous cochez la case Assigning Trusted External IP addresses (Affectation d'adresses IP externes approuvées), le boîtier Gateway Enforcer valide tout client essayant de se connecter de l'extérieur, à l'exception des clients dont les adresses IP externes sont approuvées. Ce processus est à l'opposé de Client IP Range (Plage d'adresses IP du client), qui indique quant à lui au boîtier Gateway de valider uniquement les clients des plages d'adresses IP du client.

Quand utiliser des plages d'adresses IP client

Plage d'adresses IP du client permet à des administrateurs de spécifier une plage d'adresses IP qui représentent les ordinateurs que le boîtier Gateway Enforcer doit authentifier. Les ordinateurs dont les adresses figurent hors de la plage d'adresses IP du client sont autorisés à transiter par le boîtier Gateway Enforcer sans requérir le logiciel client ou toute autre authentification.

Les raisons de l'utilisation des plages d'adresses IP du client incluent :

- Autoriser l'accès réseau aux sites Web externes

- Authentifier un sous-ensemble de clients

Autoriser l'accès réseau aux sites Web externes

Une raison d'utiliser des plages d'adresses IP du client est d'autoriser l'accès réseau aux sites Web externes depuis votre réseau interne. Si une organisation dispose d'ordinateurs sur le réseau d'entreprise passant par le boîtier Gateway Enforcer pour accéder à des sites Web Internet, comme Symantec ou Yahoo, les clients internes peuvent effectuer des requêtes sur Internet. Toutefois, le boîtier Gateway Enforcer essaie d'authentifier les sites Web tentant de répondre à la requête client.

Par conséquent, les clients internes se connectant à Internet via le boîtier Gateway Enforcer ne peuvent pas accéder à Internet à moins que vous ne configuriez la plage d'adresses IP du client.

La plage d'adresses IP du client peut correspondre à toutes les adresses IP qu'un serveur VPN attribuerait à un client.

Par exemple, un client interne peut accéder à Internet si la plage d'adresses IP du client est configurée. Lorsqu'un utilisateur interne contacte un site Web, le site peut répondre au client car son adresse IP est située à l'extérieur de la plange d'adresses IP du client. L'utilisateur interne n'a donc pas besoin d'être authentifié.

Authentification d'un sous-ensemble de clients

Vous pouvez également utiliser des adresses IP client pour que le boîtier Gateway Enforcer authentifie un sous-ensemble limité de clients d'une entreprise. Par exemple, vous pouvez utiliser des adresses IP client lors de la distribution du client.

Le boîtier Gateway Enforcer vérifie uniquement ces clients se connectant via un sous-réseau si vous avez déjà installé les clients sur tous les ordinateurs. Les autres clients qui accèdent au réseau d'entreprise à cet emplacement sont autorisés à transiter sans requérir l'authentification. Vu que le client est installé sur d'autres clients, vous pouvez ajouter leurs adresses à la plage d'adresses IP du client ou utiliser une autre stratégie d'authentification.

A propos des adresses IP approuvées

Sur un module d'application Gateway Enforcer, vous utilisez les types suivants d'adresses IP approuvées :

- Adresses IP externes approuvées
  Une adresse IP externe approuvée est l'adresse IP d'un ordinateur externe autorisé à accéder au réseau d'entreprise sans exécuter le client.
- Adresses IP internes approuvées

Une adresse IP interne approuvée est l'adresse IP d'un ordinateur à l'intérieur du réseau d'entreprise auquel tous les clients externes peuvent accéder.

Vous pouvez ajouter des adresses IP approuvées des deux types par le biais de la console Symantec Endpoint Protection Manager. Le trafic vers Symantec Endpoint Protection Manager est toujours autorisé à partir du boîtier Gateway Enforcer.

Adresses IP externes approuvées

L'un des objectifs principaux du boîtier Gateway Enforcer est de vérifier que tous les ordinateurs essayant d'accéder au réseau exécutent le client. Certains ordinateurs, des serveurs notamment, peuvent ne pas exécuter le système d'exploitation Windows ou ne pas exécuter le client.

Par exemple, en général, les serveurs VPN et les serveurs sans fil n'exécutent pas le client. En outre, une configuration réseau peut inclure des périphériques qui accèdent généralement au réseau en exécutant un autre système d'exploitation que Windows. Si ces ordinateurs doivent contourner un boîtier Gateway Enforcer, vous devez vous assurer que le boîtier possède des informations les concernant. Vous pouvez réaliser cet objectif en créant une plage d'adresses IP externes approuvées. De plus, vous pouvez également affecter une adresse IP figurant dans cette plage à un client.

Adresses IP internes approuvées

Une adresse IP interne approuvée représente l'adresse IP d'un ordinateur à l'intérieur du réseau d'entreprise auquel des clients externes peuvent accéder. Vous pouvez transformer certaines adresses IP internes en adresses IP internes approuvées.

Lorsque vous spécifiez des adresses IP internes approuvées, les clients peuvent y accéder de l'extérieur du réseau d'entreprise que les conditions suivantes sont remplies ou pas :

- Le logiciel client a été installé sur l'ordinateur client.
- Le client est conforme à la politique de sécurité.

Les adresses IP internes approuvées sont les adresses IP internes auxquelles vous voulez que les utilisateurs hors entreprise puissent accéder.

Voici des exemples d'adresses internes que vous pouvez spécifier en tant qu'adresses IP approuvées :

- Un serveur de mise à jour
- Un serveur contenant des fichiers de signature antivirus
- Un serveur utilisé pour la résolution

- Un serveur DNS ou WINS requis pour résoudre des noms de domaine ou d'hôte

Lorsqu'un client tente d'accéder au réseau interne et n'est pas authentifié par le boîtier Gateway Enforcer, il peut être mis en quarantaine sous les circonstances suivantes :

- Le client n'exécute pas le logiciel client sur l'ordinateur client
- La vérification de l'intégrité de l'hôte a échoué
- Le client n'a pas de politique à jour

Le client est tout de même autorisé à accéder à certaines adresses IP : les adresses IP internes approuvées.

Par exemple, un client externe devant accéder au réseau d'entreprise pour obtenir le client ou tout autre logiciel dont il a besoin est l'exemple type du client ayant accès aux adresses IP internes approuvées. Le boîtier Gateway Enforcer permet au client externe d'accéder à un ordinateur répertorié dans la liste d'adresses IP internes approuvées.

Ajouter des plages d'adresses IP client à la liste des adresses nécessitant une authentification

Vous pouvez spécifier les clients portant des adresses IP que le boîtier Gateway Enforcer devra authentifier.

Gardez à l'esprit les problèmes suivants :

- Vous devez cocher l'option Enable (Activer) située en regard de l'adresse ou de la plage d'adresses IP si vous voulez qu'elles soient authentifiées. Si vous souhaitez désactiver temporairement l'authentification d'une adresse ou d'une plage, décochez la case Enable (Activer).
- Si vous tapez une adresse IP erronée, vous recevez un message d'erreur quand vous essayez de l'ajouter à la liste IP client.

Pour restreindre l'accès au réseau d'un client en dépit de l'authentification

1. Dans la console Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administration).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de boîtiers Gateway Enforcer.
4. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).

5. Dans la boîte de dialogue Gateway Settings (Paramètres de passerelle), dans l'onglet Auth Range (Plage d'authentification), dans la zone Authenticate Client IP Range (Plage d'adresses IP d'authentification de client), cochez la case Only authenticate clients with these IP addresses (Authentifier uniquement les clients avec ces adresses IP).

   Si vous ne cochez pas cette option, les adresses IP listées sont ignorées. Tous les clients essayant de se connecter au réseau sont alors authentifiés. Si vous cochez cette option, le boîtier Gateway Enforcer authentifie uniquement les clients dont les adresses IP ont été ajoutées à la liste.

6. Cliquez sur **Add** (Ajouter).

7. Dans la boîte de dialogue Add Single IP Address (Ajouter une adresse IP unique), sélectionnez de Single IP address à IP Range ou Subnet (Adresse IP unique à Plage IP ou Sous-réseau).

   Les champs se modifient pour vous permettre d'entrer les informations appropriées.

8. Sélectionnez si vous voulez ajouter :

   - Une adresse IP unique
   - Une plage IP
   - Une adresse IP plus un masque de sous-réseau

9. Tapez une adresse IP unique, l'adresse de début et l'adresse de fin d'une plage ou une adresse IP plus un masque de sous-réseau.

10. Cliquez sur **OK**.

    L'information d'adresse que vous avez tapée est ajoutée au tableau Client IP Range (Plage d'adresses IP du client), avec l'option Enable (Activer) sélectionnée.

11. Cliquez à nouveau sur **Add** et indiquez les autres adresses IP ou plages d'adresses IP à faire authentifier par Gateway Enforcer.

12. Cliquez sur **OK**.

Modifier les plages d'adresses IP client dans la liste d'adresses nécessitant une authentification

Il peut s'avérer nécessaire de modifier les plages d'adresses IP client à authentifier.

Pour modifier les plages d'adresses IP client dans la liste d'adresses nécessitant une authentification

1. Dans la console Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administration).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.
4. Sélectionnez le groupe de modules d'application Enforcer pour lesquels vous voulez modifier les plages d'adresses IP client dans la liste des adresses nécessitant une authentification.
5. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
6. Dans la boîte de dialogue Gateway Settings (Paramètres de passerelle), dans l'onglet Auth Range (Plage d'authentification), dans la zone Client IP Range (Plage d'adresses IP client), cliquez sur la colonne des adresses IP, puis sur **Edit all** (Modifier tous).
7. Cliquez sur **OK**.
8. Dans la boîte de dialogue Gateway Settings (Paramètres de la passerelle), cliquez sur **OK**.

Supprimer des plages d'adresses IP client de la liste d'adresses nécessitant une authentification

Il peut s'avérer nécessaire de supprimer des plages d'adresses IP client.

Pour supprimer des plages d'adresses IP client de la liste d'adresses nécessitant une authentification

1. Dans la console Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administration).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.
4. Sélectionnez le groupe de boîtiers Gateway Enforcer dont vous souhaitez modifier la plage d'adresses IP dans la liste des adresses nécessitant une authentification.
5. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).

6 Dans la boîte de dialogue Gateway Settings (Paramètres de passerelle), dans l'onglet Auth Range (Plage d'authentification), dans la zone Client IP Range (Plage d'adresses IP client), cliquez sur la ligne contenant l'adresse IP que vous voulez supprimer.

7 Cliquez sur **Remove** (Supprimer).

8 Cliquez sur **OK**.

Ajouter une adresse IP interne approuvée pour des clients sur un serveur de gestion

Le tableau Trusted Internal IP (Adresses IP internes approuvées) contient une liste d'adresses IP interne avec lesquelles les clients externes sont autorisés à communiquer, et ce que le client exécute/ait passé la vérification d'intégrité d'hôte ou non.

Si vous exécutez deux boîtiers Gateway Enforcer en série pour qu'un client se connecte par le biais de plusieurs boîtiers Gateway Enforcer, le boîtier Gateway Enforcer le plus proche de Symantec Endpoint Protection Manager doit être indiqué comme adresse IP interne approuvée de l'autre boîtier Gateway Enforcer. Si un client échoue une première fois à la vérification d'intégrité d'hôte avant de la réussir, un délai de cinq minutes peut être nécessaire avant que le client ne puisse se connecter au réseau.

Pour ajouter une adresse IP interne approuvée pour des clients sur un serveur de gestion

1 Dans la console Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administration).

2 Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).

3 Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.

4 Sélectionnez le groupe de boîtiers Gateway Enforcer pour lesquels vous voulez modifier les plages d'adresses IP client dans la liste des adresses nécessitant une authentification.

5 Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).

6 Dans la boîte de dialogue Gateway Settings (Paramètres de passerelle), dans l'onglet Auth Range (Plage d'authentification), dans la zone Trusted IP Range (Plage d'adresses IP approuvées), sélectionnez Trusted Internal IP Range (Intervalle IP interne approuvé) dans la liste déroulante.

7 Cliquez sur **Add** (Ajouter).

8 Dans la boîte de dialogue Paramètres d'adresse IP, tapez une adresse IP ou une plage d'adresses.

9 Cliquez sur OK.

L'adresse IP est ajoutée à la liste et une coche apparaît dans la colonne Enable (Activer).

10 Dans la boîte de dialogue Settings (Paramètres), cliquez sur **OK**.

Spécifier les adresses IP externes approuvées

Si vous ajoutez des adresses IP externes approuvées, le boîtier Gateway Enforcer permet aux clients à ces adresses de se connecter au réseau même s'ils n'exécutent pas un logiciel client.

Puisqu'un client n'est pas installé sur des serveurs VPN, vous devez ajouter l'adresse IP de serveur à la liste d'adresses IP approuvées si un serveur VPN requiert l'accès au réseau par le biais de Gateway Enforcer.

Si vous entrez une adresse IP erronée, vous recevez un message d'erreur.

Remarque : Vous devez d'abord ajouter l'adresse IP interne du serveur VPN d'entreprise dans le champ des adresses IP externes approuvées.

Pour spécifier les adresses IP externes approuvées

1 Dans la console Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administration).

2 Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).

3 Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.

4 Sélectionnez le groupe de modules d'application Enforcer pour lesquels vous voulez spécifier les adresses IP externes approuvées.

5 Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).

6 Dans la boîte de dialogue Gateway Settings (Paramètres de passerelle), dans l'onglet Auth Range (Plage d'authentification), dans la zone Trusted IP Range (Plage d'adresses IP approuvées), sélectionnez Trusted External IP Range (Intervalle IP externe approuvé).

7 Cliquez sur **Add** (Ajouter).

8 Dans la boîte de dialogue Paramètres d'adresse IP, tapez une adresse IP ou une plage d'adresses.

9 Cliquez sur **OK**.

L'adresse IP est ajoutée à la liste et une coche apparaît dans la colonne Activer.

10 Dans la boîte de dialogue Settings (Paramètres), cliquez sur **OK**.

Modifier une adresse IP interne ou externe approuvée

Il peut arriver que vous deviez modifier des adresses IP internes et externes approuvées.

Pour modifier une adresse IP interne ou externe approuvée

1 Dans la console Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administration).

2 Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).

3 Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.

4 Sélectionnez le groupe de modules d'application Enforcer pour lesquels vous voulez modifier une adresse IP interne ou externe approuvée.

5 Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).

6 Dans la boîte de dialogue Gateway Settings (Paramètres de passerelle), dans l'onglet Auth Range (Plage d'authentification), dans la zone Trusted IP Range (Plage d'adresses IP approuvées), sélectionnez Trusted External IP Range ou Trusted Internal IP Range (Intervalle IP externe approuvé ou Intervalle IP interne approuvé) dans la liste déroulante.

Les adresses pour le type sélectionné sont affichées dans le tableau.

7 Dans le tableau **Trusted IP Range** (Plage d'adresses IP approuvées), cliquez dans la colonne des adresses IP et cliquez sur **Edit all** (Modifier tous).

8 Dans la boîte de dialogue Editeur d'adresses IP, recherchez toutes les adresses que vous voulez modifier et procédez à la modification.

9 Cliquez sur **OK**.

10 Dans la boîte de dialogue Settings (Paramètres), cliquez sur **OK**.

Supprimer une adresse IP interne ou externe approuvée

Si vous ne voulez plus autoriser les utilisateurs externes qui ne sont pas entièrement authentifiés à accéder à un emplacement interne particulier, vous pouvez supprimer leur adresse IP du tableau des adresses IP internes approuvées.

Pour supprimer une adresse IP interne ou externe approuvée

1. Dans la console Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administration).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de boîtiers Gateway Enforcer.
4. Sélectionnez le groupe de boîtiers Gateway Enforcer pour lequel vous souhaitez supprimer une adresse IP approuvée (interne ou externe).
5. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
6. Dans la boîte de dialogue Gateway Settings (Paramètres de passerelle), dans l'onglet Auth Range (Plage d'authentification), dans la zone Trusted IP Range (Plage d'adresses IP approuvées), sélectionnez Trusted External IP Range ou Trusted Internal IP Range (Intervalle IP externe approuvé ou Intervalle IP interne approuvé) dans la liste déroulante.

   Les adresses pour le type sélectionné sont affichées dans le tableau.
7. Dans le tableau, cliquez sur la ligne contenant l'adresse IP que vous voulez supprimer.
8. Cliquez sur **Remove** (Supprimer).
9. Dans la boîte de dialogue Settings (Paramètres), cliquez sur **OK**.

Ordre de vérification d'une plage IP

Si la plage d'adresses IP client et les adresses IP internes approuvées sont en cours d'utilisation en même temps, le boîtier Gateway Enforcer vérifie les adresses client dans l'ordre suivant lors de la réception d'un paquet d'un client :

- Si la plage d'adresses IP du client est activée, le boîtier Gateway Enforcer recherche dans le tableau Plage d'adresses IP du client une adresse correspondant à l'IP source du client.
- Si la plage d'adresses IP du client n'inclut pas d'adresse IP pour ce client, le boîtier Gateway Enforcer autorise le client sans authentification.
- Si la plage d'adresses IP du client inclut une adresse IP pour ce client, le boîtier Gateway Enforcer recherche ensuite dans la plage d'adresses IP externes approuvées une adresse correspondante.
- Si une adresse correspondant au client est trouvée dans la plage d'adresses IP externes approuvées, le boîtier Enforcer autorise le client.

- Si aucune adresse correspondante n'est trouvée dans la plage d'adresses IP externes approuvées, le boîtier Gateway Enforcer compare l'adresse cible à la plage d'adresses IP internes approuvées et à la liste des gestionnaires Symantec Endpoint Protection Manager.
  Si une adresse correspondante n'est toujours pas localisée, le boîtier Gateway Enforcer commence la session d'authentification et envoie le paquet de stimulation.

Utilisation des paramètres avancés de boîtier Gateway Enforcer

Vous pouvez configurer les paramètres de configuration avancés Gateway Enforcer suivants :

- Allow all DHCP request packets (Autoriser tous les paquets de requête DHCP).
- Allow all DNS request packets (Autoriser tous les paquets de requête DNS).
- Allow all ARP request packets (Autoriser tous les paquets de requête ARP).
- Allow other protocols besides IP and ARP (Autoriser d'autres protocoles que IP et ARP).
  Vous pouvez indiquer les types de protocoles que vous souhaitez autoriser dans le champ Filter (Filtre).
  Se reporter à "Spécification de types de paquets et protocoles" à la page 129.
- Autorisation de clients hérités
  Se reporter à "Autorisation d'un client hérité à se connecter au réseau avec un boîtier Gateway Enforcer" à la page 131.
- Activation d'authentification locale
  Se reporter à "Activation de l'authentification locale sur le boîtier Gateway Enforcer" à la page 131.

Lorsque vous appliquez les paramètres, les modifications apportées sont envoyées au boîtier Gateway Enforcer sélectionné lors du battement suivant.

Spécification de types de paquets et protocoles

Vous pouvez spécifier que le boîtier Gateway Enforcer autorise certains types de paquets à passer sans qu'un client n'exécute ou ne requiert d'authentification.

Pour spécifier les types de paquets et protocoles

1. Dans la console Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administration).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de boîtiers Gateway Enforcer.
4. Sélectionnez le groupe de boîtiers Gateway Enforcer pour lequel vous souhaitez spécifier des types de paquets et protocoles.
5. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
6. Dans la boîte de dialogue Gateway Settings (Paramètres de passerelle), dans l'onglet Advanced (Avancés), cochez ou décochez les types de paquets ou protocoles suivants :

   - Allow all DHCP request packets (Autoriser tous les paquets de requête DHCP).
     Si la case est cochée, le boîtier Gateway Enforcer transmet toutes les requêtes DHCP depuis le réseau externe vers le réseau interne. Etant donné que cette option empêche le client d'obtenir une adresse IP et étant donné que le client requiert une adresse IP pour communiquer avec un boîtier Gateway Enforcer, il est recommandé de maintenir cette option activée.
     Le paramètre par défaut est enabled (activé).
   - Allow all DNS request packets (Autoriser tous les paquets de requête DNS).
     Lorsque cette option est activée, Enforcer transfère toutes les requêtes DNS du réseau externe dans le réseau interne. Cette option doit être activée si le client est configuré pour communiquer avec Symantec Endpoint Protection Manager par nom plutôt que par adresse IP. Cette option doit également être activée si vous souhaitez utiliser l'option de requêtes de redirection HTTP de l'onglet Authentication (Authentification).
     Le paramètre par défaut est enabled (activé).
   - Allow all ARP request packets (Autoriser tous les paquets de requête ARP).
     Lorsque cette option est activée, le boîtier Gateway Enforcer autorise tous les paquets d'ARP du réseau interne. Sinon, le boîtier Gateway Enforcer traite le paquet comme paquet IP normal et utilise l'IP de l'expéditeur comme IP source et l'IP cible comme IP de destination, puis procède à l'authentification.
     Le paramètre par défaut est enabled (activé).
   - Allow other protocols besides IP and ARP (Autoriser d'autres protocoles que IP et ARP).

Lorsque cette option est activée, le boîtier Gateway Enforcer transfère tous les paquets avec d'autres protocoles. Sinon, il les abandonne.

Le paramètre par défaut est désactivé.

Si vous avez coché Allow other protocols besides IP and ARP (Autoriser d'autres protocoles que IP et ARP), vous pouvez compléter le champ Filter (Filtre).

7 Cliquez sur **OK**.

Autorisation d'un client hérité à se connecter au réseau avec un boîtier Gateway Enforcer

Vous pouvez activer un boîtier Gateway Enforcer de sorte à ce qu'il se connecte à des clients hérités 5.1.x. Si votre réseau prend en charge une console Symantec Endpoint Protection Manager 11.0.2 ainsi qu'un boîtier Symantec Gateway Enforcer et qu'il doit prendre en charge des clients hérités 5.1.x, vous pouvez activer la prise en charge des clients hérités 5.1.x sur la console du serveur de gestion afin que le boîtier Symantec Gateway Enforcer ne les bloque pas.

Pour autoriser un client hérité à se connecter au réseau avec un boîtier Gateway Enforcer

1 Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).

2 Dans la page Admin, cliquez sur **Servers** (Serveurs).

3 Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de boîtiers Gateway Enforcer.

4 Dans la page Admin, sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).

5 Dans la boîte de dialogue Settings (Paramètres), dans l'onglet Advanced (Avancés), sélectionnez **Allow legacy clients** (Autoriser les clients hérités).

6 Cliquez sur **OK**.

Activation de l'authentification locale sur le boîtier Gateway Enforcer

L'authentification locale étant activée, le boîtier Gateway Enforcer perd sa connexion avec le serveur sur lequel Symantec Endpoint Protection Manager est installé. Par conséquent, le boîtier Gateway Enforcer authentifie un client localement.

Pour activer l'authentification locale sur le boîtier Gateway Enforcer

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin, cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de boîtiers Gateway Enforcer.
4. Dans la page Admin, sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans la boîte de dialogue Settings (Paramètres), dans l'onglet Advanced (Avancé), sélectionnez **Enable Local Authentication** (Activer l'authentification locale).
6. Cliquez sur **OK**.

Chapitre 7

Configurer le boîtier Symantec DHCP Enforcer sur la console Symantec Endpoint Protection Manager

Ce chapitre traite des sujets suivants :

A propos de la configuration du boîtier Symantec DHCP Enforcer sur la console Symantec Endpoint Protection Manager.

Vous pouvez ajouter ou modifier les paramètres de configuration pour le boîtier DHCP Enforcer dans la console Symantec Endpoint Protection Manager.

Avant de poursuivre, vous devez effectuer les tâches suivantes :

- Installez le logiciel de Symantec Endpoint Protection Manager sur un ordinateur.
  Consultez le *Guide d'installation de Symantec Endpoint Protection et de Symantec Network Access Control*.
  L'ordinateur sur lequel le logiciel Symantec Endpoint Protection Manager est installé est également désigné sous le nom de serveur de gestion.
- Connectez le boîtier Symantec DHCP Enforcer au réseau.
  Se reporter à "Pour installer un boîtier Enforcer" à la page 84.
- Configurez le boîtier Symantec DHCP Enforcer sur la console Enforcer pendant l'installation.
  Se reporter à "Pour configurer un boîtier Enforcer" à la page 86.

Après avoir terminé ces tâches, vous pouvez spécifier des paramètres de configuration supplémentaires pour le boîtier DHCP Enforcer sur un serveur de gestion.

Modification des paramètres de configuration du boîtier DHCP Enforcer sur un serveur de gestion

Vous pouvez modifier les paramètres de configuration du boîtier DHCP Enforcer sur un serveur de gestion. Les paramètres de configuration sont automatiquement téléchargés à partir du serveur de gestion au boîtier DHCP Enforcer pendant le battement suivant.

Pour modifier les paramètres de configuration du boîtier DHCP Enforcer sur un serveur de gestion

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).

3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez le groupe de boîtiers DHCP Enforcer dont le boîtier DHCP Enforcer est membre.

   Le groupe de boîtiers DHCP Enforcer doit inclure les boîtiers DHCP Enforcer dont les paramètres de configuration doivent être modifiés.

4. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez le boîtier DHCP Enforcer dont les paramètres de configuration doivent être modifiés.

5 Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).

6 Dans la boîte de dialogue Settings (Paramètres), modifiez les paramètres de configuration.

La boîte de dialogue Settings (Paramètres) DHCP Enforcer fournit les catégories suivantes de paramètres de configuration :

General (Général)	Paramètres pour la description du groupe de boîtiers DHCP Enforcer et liste de serveurs de gestion. Se reporter à "Utiliser les paramètres généraux" à la page 137.
Authentication (Authentification)	Réglages d'une série de paramètres qui affectent la procédure d'authentification client. Se reporter à "Utiliser les paramètres d'authentification" à la page 140.
Serveurs DHCP	Paramètres qui spécifient l'adresse IP, le numéro de port et la priorité pour les serveurs DHCP normaux et de quarantaine. Ces informations sont requises Vous devez configurer les informations sur le serveur DHCP avant de commencer l'application. Se reporter à "Utiliser les paramètres de serveurs DHCP" à la page 151.
Advanced (Avancé)	Paramètres pour les dépassements de délai et les délais de messages DHCP. Paramètres pour des adresses MAC des hôtes fiables que le boîtier DHCP Enforcer autorise à se connecter sans authentification (facultative). Paramètres pour l'usurpation DNS et l'authentification locale. Se reporter à "Utilisation des paramètres avancés de boîtier DHCP Enforcer" à la page 155.
Paramètres de journal	Paramètres permettant d'activer la consignation des journaux de serveur, des journaux d'activités client et de spécifier les paramètres de fichier journal. Se reporter à "Rapports Enforcer" à la page 439. Se reporter à "A propos des journaux Enforcer" à la page 440. Se reporter à "Configurer les paramètres du journal Enforcer" à la page 443.

Utiliser les paramètres généraux

Vous pouvez ajouter ou modifier la description d'un module DHCP Enforcer ou d'un groupe DHCP Enforcer dans la console Symantec Endpoint Protection Manager.

Se reporter à "Ajout ou modification du nom d'un groupe de modules Enforcer avec un module DHCP Enforcer" à la page 137.

Se reporter à "Ajout ou modification de la description d'un groupe d'Enforcer avec un module DHCP Enforcer" à la page 137.

Toutefois, vous ne pouvez pas ajouter ou modifier le nom d'un groupe DHCP Enforcer dans la console Symantec Endpoint Protection Manager. Vous ne pouvez pas ajouter ni modifier l'adresse IP ou le nom d'hôte d'un module DHCP Enforcer dans la console Symantec Endpoint Protection Manager. Au lieu de cela, vous devez effectuer ces tâches sur la console Enforcer.

Se reporter à "Ajout ou modification de l'adresse IP ou du nom d'hôte d'un module DHCP Enforcer" à la page 138.

Vous pouvez également ajouter ou modifier l'adresse IP ou le nom d'hôte de Symantec Endpoint Protection Manager dans une liste de serveurs de gestion.

Se reporter à "Connexion de DHCP Enforcer à Symantec Endpoint Protection Manager" à la page 139.

Ajout ou modification du nom d'un groupe de modules Enforcer avec un module DHCP Enforcer

Vous pouvez ajouter ou modifier le nom d'un groupe de modules d'application Enforcer dont un boîtier DHCP Enforcer est membre. Effectuez ces tâches sur la console Enforcer pendant l'installation. Plus tard, si vous voulez modifier le nom d'un groupe Enforcer, vous pourrez le faire sur la console Enforcer.

Consultez le *Guide de mise en œuvre de Symantec Network Access Control Enforcer* pour plus d'informations sur la façon d'ajouter ou de modifier le nom d'un groupe Enforcer.

Tous les modules Enforcer d'un groupe partagent les mêmes paramètres de configuration.

Ajout ou modification de la description d'un groupe d'Enforcer avec un module DHCP Enforcer

Vous pouvez ajouter ou modifier le nom d'un groupe d'Enforcer dont un boîtier Symantec DHCP Enforcer est membre. Vous pouvez effectuer cette tâche sur la

console Symantec Endpoint Protection Manager au lieu de la console DHCP Enforcer.

Pour ajouter ou modifier la description d'un groupe d'Enforcer avec un module DHCP Enforcer

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin, sous Afficher les serveurs, sélectionnez et développez le groupe Enforcer dont vous voulez ajouter ou modifier la des cription.
4. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans la boîte de dialogue Settings (Paramètres), sous l'onglet Basic Settings (Paramètres de base), ajoutez ou modifiez une description pour le groupe de boîtiers Enforcer dans le champ Description.
6. Dans la boîte de dialogue Settings (Paramètres), cliquez sur **OK**.

Ajout ou modification de l'adresse IP ou du nom d'hôte d'un module DHCP Enforcer

Vous pouvez seulement changer l'adresse IP ou le nom d'hôte d'un module DHCP Enforcer sur la console d'Enforcer pendant l'installation. Si vous voulez modifier ultérieurement l'adresse IP ou le nom d'hôte d'un module DHCP Enforcer, vous pouvez le faire sur la console DHCP Enforcer.

Consultez le *Guide de mise en œuvre de Symantec Network Access Control Enforcer* pour plus d'informations.

Ajout ou modification de la description d'un module DHCP Enforcer

Vous pouvez ajouter ou modifier la description d'un module DHCP Enforcer. Vous pouvez effectuer cette tâche sur la console Symantec Endpoint Protection Manager au lieu de la console DHCP Enforcer. Après avoir terminé cette tâche, la description apparaît dans le champ Description du volet Gestion du serveur.

Pour ajouter ou modifier la description d'un module DHCP Enforcer

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).

3 Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe d'Enforcer qui inclut le module DHCP Enforcer dont vous voulez ajouter ou modifier la description.

4 Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez le module DHCP Enforcer dont vous voulez ajouter ou modifier la description.

5 Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Enforcer Properties** (Modifier les propriétés d'Enforcer).

6 Dans la boîte de dialogue Properties (Propriétés) du module Enforcer, ajoutez ou modifiez une description pour le module DHCP Enforcer dans le champ Description.

7 Dans la boîte de dialogue Properties (Propriétés) du module Enforcer, cliquez sur **OK**.

Connexion de DHCP Enforcer à Symantec Endpoint Protection Manager

Les modules d'application Enforcer doivent pouvoir se connecter aux serveurs sur lesquels Symantec Endpoint Protection Manager est installé. Symantec Endpoint Protection Manager comprend un fichier qui aide à la gestion du trafic entre les clients, les gestionnaires Symantec Endpoint Protection Manager et les modules d'application Enforcer facultatifs tels que DHCP Enforcer.

Ce fichier est appelé liste de serveurs de gestion. La liste de serveurs de gestion spécifie à quel serveur Symantec Endpoint Protection Manager se connecte un module d'application DHCP Enforcer. Elle spécifie également à quel serveur Symantec Endpoint Protection un module d'application DHCP Enforcer se connecte en cas de défaillance d'un serveur de gestion.

Une liste de serveurs de gestion par défaut est automatiquement créée pour chaque site pendant l'installation initiale. Tous les gestionnaires Symantec Endpoint Protection Manager disponibles sur le site sont automatiquement ajoutés à la liste de serveurs de gestion par défaut.

La liste de serveurs de gestion par défaut comprend les adresses IP ou les noms d'hôte du serveur de gestion auxquels les modules d'application Integrated Enforcer peuvent se connecter après l'installation initiale. Vous pouvez créer une liste de serveurs de gestion personnalisée avant de déployer des modules d'application Enforcer. Si vous créez une liste de serveurs de gestion personnalisée, vous pouvez spécifier la priorité de connexion d'un module d'application DHCP Enforcer aux serveurs de gestion.

Vous pouvez sélectionner la liste de serveurs de gestion spécifique comprenant les adresses IP ou les noms d'hôte des serveurs de gestion auxquels vous voulez

que DHCP Enforcer se connecte. Si le site ne comprend qu'un seul serveur de gestion, vous pouvez sélectionner la liste de serveurs de gestion par défaut.

Consultez le *Guide d'administration de Symantec Endpoint Protection et Symantec Network Access Control* pour plus d'informations sur la personnalisation des listes de serveurs de gestion.

Pour connecter DHCP Enforcer à Symantec Endpoint Protection Manager

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.

   Le groupe Enforcer doit comprendre le module d'application DHCP Enforcer dont vous voulez modifier l'adresse IP ou le nom d'hôte dans une liste de serveurs de gestion.
4. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans la boîte de dialogue Settings (Paramètres), dans l'onglet Basic Settings (Paramètres de base), sous Communication, sélectionnez la liste de serveurs de gestion à utiliser par ce module DHCP Enforcer.
6. Dans la boîte de dialogue Settings (Paramètres), dans l'onglet Basic Settings (Paramètres de base), sous Communication, cliquez sur **Preview** (Aperçu).

   Vous pouvez afficher les adresses IP et les noms d'hôte de tous les serveurs de gestion disponibles, ainsi que les priorités qui leur ont été attribuées.
7. Dans la boîte de dialogue Management Server List (Listes de serveurs de gestion), cliquez sur **Close** (Fermer).
8. Dans la boîte de dialogue Settings (Paramètres), cliquez sur **OK**.

Utiliser les paramètres d'authentification

Vous pouvez spécifier un certain nombre de paramètres d'authentification pour une session d'authentification de module DHCP Enforcer. Lorsque vous appliquez ces modifications, elles sont envoyées automatiquement au module DHCP Enforcer sélectionné pendant le battement suivant.

A propos de l'utilisation des paramètres d'authentification

Vous pouvez mettre en application un certain nombre de paramètres d'authentification pour sécuriser d'avantage le réseau.

Tableau 7-1 fournit plus d'informations sur les options de l'onglet Authentification.

Tableau 7-1 Paramètres de configuration d'authentification pour un DHCP Enforcer

Option	Description
Nombre maximal de paquets par session d'authentification	Nombre maximal de paquets de sollicitation que DHCP Enforcer envoie dans chaque session d'authentification. Le nombre par défaut est de 10. Se reporter à "Spécifier le nombre maximum de paquets pendant une session d'authentification" à la page 144.
Temps entre les paquets en session d'authentification	Temps (en secondes) entre les paquets de sollicitation envoyés par Enforcer. La valeur par défaut est 3. Se reporter à "Spécification de la fréquence des paquets de stimulation à envoyer aux clients" à la page 145.
Autoriser tous les clients, mais continuer à consigner les clients non authentifiés	Si cette option est activée, Enforcer authentifie tous les utilisateurs en vérifiant qu'ils exécutent un client. Le DHCP Enforcer vérifie également si le client a réussi la vérification de l'intégrité de l'hôte. Si le client a réussi la vérification de l'intégrité de l'hôte, le DHCP Enforcer consigne les résultats. Il transfère alors la demande DHCP de recevoir une configuration réseau normale plutôt qu'une configuration réseau de quarantaine, indépendamment de l'échec ou de la réussite des vérifications. Le paramètre par défaut n'est pas activé. Se reporter à "Autorisation de tous les clients avec la connexion continue des clients non-authentifiés" à la page 146.

Option	Description
Permettre tous les clients avec des systèmes d'exploitation non Windows	Si cette option est activée, DHCP Enforcer vérifie le système d'exploitation du client. DHCP Enforcer permet alors à tous les clients n'exécutant pas le système d'exploitation Windows de recevoir une configuration réseau normale sans être authentifié. Si cette option n'est pas activée, les clients reçoivent une configuration réseau de quarantaine. Le paramètre par défaut n'est pas activé. Se reporter à "Autorisation des clients non-Windows à se connecter à un réseau sans authentification" à la page 147.
Vérifier le numéro de série de politique du Client avant de permettre au client d'accéder au réseau	Si cette option est activée, DHCP Enforcer vérifie si le client a reçu les dernières politiques de sécurité du serveur de gestion. Si le numéro de série de politique n'est pas le plus récent, DHCP Enforcer informe le client de la nécessité de mise à jour de sa politique de sécurité. Le client transfère alors la demande DHCP de recevoir une configuration réseau de quarantaine. Si cette option n'est pas activée et si la vérification de l'intégrité de l'hôte réussit, DHCP Enforcer transfère la demande DHCP de recevoir une configuration réseau normale. DHCP Enforcer transfère la demande DHCP même si le client n'a pas la dernière politique de sécurité. Le paramètre par défaut n'est pas activé. Se reporter à "Vérification par le module d'application DHCP Enforcer du numéro de série de politique d'un client" à la page 148.
Activer le message instantané sur le client si le logiciel client ne s'exécute pas	Si cette option est activée, un message est affiché pour les utilisateurs des ordinateurs Windows sans client qui essaient de se connecter à un réseau d'entreprise. Le message par défaut est défini pour s'afficher une seule fois. Le message indique aux utilisateurs que leur accès au réseau est bloqué en raison de l'absence de client en cours d'exécution et leur indique de l'installer. Pour modifier le message ou sa fréquence d'affichage, vous pouvez cliquer sur Message. La longueur maximale du message est de 128 caractères. Le paramètre par défaut est activé. Se reporter à "Envoi d'un message de non-conformité du boîtier DHCP Enforcer à un client" à la page 149.

A propos des sessions d'authentification

Lorsqu'un client essaye d'accéder au réseau interne, le boîtier DHCP Enforcer détecte d'abord si le client exécute un logiciel client. Si oui, le boîtier DHCP Enforcer transfère le message DHCP client au serveur DHCP pour obtenir une adresse IP de quarantaine restreinte. Ce processus est utilisé en interne par le boîtier DHCP Enforcer pour son procédé d'authentification.

Le boîtier DHCP Enforcer commence alors sa session d'authentification avec le client. Une session d'authentification est un ensemble de paquets de sollicitation que le boîtier DHCP Enforcer envoie à un client.

Pendant la session d'authentification, le boîtier DHCP Enforcer envoie un paquet de stimulation au client à une fréquence spécifiée.

Le paramètre par défaut est toutes les trois secondes.

Le boîtier DHCP Enforcer continue à envoyer des paquets jusqu'à ce que l'une des conditions suivantes soit remplie :

- Le boîtier DHCP Enforcer reçoit une réponse du client
- Le boîtier DHCP Enforcer a envoyé le nombre maximum de paquets spécifiés. Le paramètre par défaut est 10.

La fréquence (3 secondes) multipliée par le nombre de paquets (10) est la valeur utilisée pour le battement du boîtier DHCP Enforcer. Le battement est l'intervalle pendant lequel le boîtier DHCP Enforcer permet au client de rester connecté avant de démarrer une nouvelle session d'authentification.

Le paramètre par défaut est 30 secondes.

Le client envoie des données au boîtier DHCP Enforcer contenant les éléments suivants :

- Identificateur unique (UID)
- Son numéro de série de profil actuel
- Les résultats de la vérification d'intégrité de l'hôte

Le boîtier DHCP Enforcer vérifie l'identificateur UID et le numéro de série de politique du client auprès de Symantec Endpoint Protection Manager. Si le client a été mis à jour avec les dernières politiques de sécurité, son numéro de série de politique correspond à celui que le boîtier DHCP Enforcer reçoit du serveur de gestion. Les résultats de vérification d'intégrité de l'hôte montrent si le client est conforme aux politiques de sécurité actuelles.

Si les données client vérifient les conditions d'authentification, le boîtier DHCP Enforcer fait suivre sa requête DHCP au serveur DHCP. Le boîtier DHCP Enforcer s'attend à recevoir une configuration réseau DHCP normale. Sinon, le boîtier DHCP

Enforcer transfère la requête au serveur DHCP de quarantaine pour recevoir une configuration réseau de quarantaine.

Vous pouvez installer un serveur DHCP sur un ordinateur et le configurer pour fournir une configuration réseau normale et une configuration réseau de quarantaine.

Se reporter à "Planification d'installation pour un boîtier DHCP Enforcer" à la page 59.

Après l'intervalle de battement ou toutes les fois que le client essaye de renouveler son adresse IP, le boîtier DHCP Enforcer démarre une nouvelle session d'authentification. Le client doit répondre pour maintenir la connexion au réseau interne.

Le boîtier DHCP Enforcer déconnecte les clients qui ne répondent pas.

Pour les clients précédemment authentifiés mais qui échouent maintenant à l'authentification, le boîtier DHCP Enforcer envoie un message au serveur DHCP. Le message est une demande de libérer l'adresse IP actuelle. Le boîtier DHCP Enforcer envoie alors un message DHCP au client. Le client envoie alors une demande de renouvellement de l'adresse IP et de la configuration réseau au boîtier DHCP Enforcer. DHCP Enforcer fait suivre cette demande au serveur DHCP de quarantaine.

Spécifier le nombre maximum de paquets pendant une session d'authentification

Pendant la session d'authentification, le boîtier DHCP Enforcer envoie un paquet de stimulation au client à une fréquence spécifiée.

Le boîtier DHCP Enforcer continue à envoyer des paquets jusqu'à ce que les conditions suivantes soient remplies :

- Le boîtier DHCP Enforcer reçoit une réponse du client
- Le boîtier DHCP Enforcer a envoyé le nombre maximum spécifié de paquets.

Le paramètre par défaut pour le nombre maximum de paquets pour une session d'authentification : 10.

Pour spécifier le nombre maximum de paquets de stimulation pendant une session d'authentification

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).

3 Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.

Le groupe de boîtiers DHCP Enforcer doit inclure le module DHCP Enforcer pour lequel vous voulez spécifier le nombre maximum de paquets de stimulation envoyés pendant une session d'authentification.

4 Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).

5 Dans l'onglet Authentication (Authentification), sous Authentication Parameters (Paramètres d'authentification), saisissez le nombre maximum de paquets de stimulation à autoriser pendant une session d'authentification dans le champ **Maximum number of packets per authentication session** (Nombre maximum de paquets par session d'authentification).

Le paramètre par défaut est 10.

6 Dans la boîte de dialogue Settings (Paramètres), sur l'onglet Authentication (Authentification), cliquez sur **OK**.

Spécification de la fréquence des paquets de stimulation à envoyer aux clients

Pendant la session d'authentification, le boîtier DHCP Enforcer envoie un paquet de stimulation au client à une fréquence spécifiée.

Le boîtier DHCP Enforcer continue à envoyer des paquets jusqu'à ce que les conditions suivantes soient remplies :

- Le boîtier DHCP Enforcer reçoit une réponse du client
- Le boîtier DHCP Enforcer a envoyé le nombre maximum spécifié de paquets.

Le paramètre par défaut est toutes les 3 secondes.

Pour spécifer la fréquence d'envoi des paquets aux clients

1 Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).

2 Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).

3 Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.

Le groupe de boîtiers DHCP Enforcer doit inclure le boîtier DHCP Enforcer pour lequel vous voulez spécifier la fréquence d'envoi de paquets de stimulation aux clients.

4. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans l'onglet Authentication (Authentification), sous Authentication Parameters (Paramètres d'authentification), saisissez le nombre maximum de paquets de stimulation que DHCP Enforcer doit continuer d'envoyer à un client pendant une session d'authentification dans le champ **Time between packets in authentication session** (Temps entre les paquets en session d'authentification).

   Le paramètre par défaut est 10.
6. Dans la boîte de dialogue Settings (Paramètres), sur l'onglet Authentication (Authentification), cliquez sur **OK**.

Autorisation de tous les clients avec la connexion continue des clients non-authentifiés

Déployer l'ensemble des logiciels client peut prendre un certain temps. Vous pouvez configurer le boîtier DHCP Enforcer pour autoriser tous les clients à se connecter au réseau après avoir distribué le paquet client à tous les utilisateurs. Ces utilisateurs se connectent tous à un serveur DHCP à l'emplacement de ce boîtier Enforcer DHCP.

Le boîtier DHCP Enforcer authentifie toujours tous les utilisateurs en vérifiant qu'ils exécutent un client, en vérifiant l'intégrité de l'hôte et en consignant les résultats. Il fait suivre les requêtes DHCP pour recevoir la configuration réseau de serveur DHCP normale au lieu de la configuration réseau de quarantaine. Ce processus se produit indépendamment de l'échec ou de la réussite des vérifications de l'intégrité de l'hôte.

Le paramètre n'est pas activé par défaut.

Suivez les directives ci-dessous quand vous appliquez les paramètres de configuration :

- Ce paramètre doit être une mesure temporaire parce qu'il rend le réseau moins sécurisé.
- Lorsque ce paramètre est en vigueur, vous pouvez passer en revue les journaux Enforcer. Vous pouvez vous renseigner sur les types de clients qui essayent de se connecter au réseau à cet emplacement.
  Par exemple, vous pouvez passer en revue le journal d'activités client pour savoir si des clients ne disposent pas du logiciel client. Vous pouvez ensuite vérifier que le logiciel client est installé sur ces clients avant de désactiver cette option.

Pour autoriser tous les clients avec la connexion continue des clients non-authentifiés

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.

   Le groupe Enforcer doit inclure le module d'application DHCP Enforcer pour lequel vous voulez autoriser tous les clients tout en continuant la consignation des clients non-authentifiés.
4. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans la boîte de dialogue Paramètres, dans l'onglet Authentification, cochez **Allow all clients, but continue to log which clients are not authenticated** (Autoriser tous les clients, mais continuer à consigner les clients non authentifiés).

   Le paramètre n'est pas activé par défaut.
6. Cliquez sur **OK**.

Autorisation des clients non-Windows à se connecter à un réseau sans authentification

Le boîtier DHCP Enforcer ne peut pas authentifier un client utilisant un système d'exploitation non-Windows. Par conséquent les clients non-Windows ne peuvent pas se connecter au réseau à moins que vous ne les autorisiez spécifiquement à se connecter au réseau sans authentification.

Le paramètre n'est pas activé par défaut.

Vous pouvez utiliser une des méthodes suivantes pour activer les clients qui prennent en charge une plate-forme non-Windows pour se connecter au réseau :

- Spécifiez chaque client non-Windows comme hôte approuvé.
- Autorisez tous les clients avec des systèmes d'exploitation non-Windows

Le boîtier DHCP Enforcer détecte le système d'exploitation du client et authentifie les clients Windows. Cependant, il ne permet pas à des clients non-Windows de se connecter au serveur DHCP normal sans authentification.

Pour autoriser des clients non-Windows à se connecter à un réseau sans authentification

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.

   Le groupe de boîtiers DHCP Enforcer doit inclure le boîtier DHCP Enforcer pour lequel vous voulez autoriser l'ensemble des clients non-Windows à se connecter à un réseau.
4. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans la boîte de dialogue Settings (Paramètres), dans l'onglet Authentication (Authentification), cochez **Allow all clients with non-Windows operating systems** (Autoriser tous les clients avec des systèmes d'exploitation non-Windows).

   Le paramètre n'est pas activé par défaut.
6. Cliquez sur **OK**.

Vérification par le module d'application DHCP Enforcer du numéro de série de politique d'un client

Symantec Endpoint Protection Manager met à jour le numéro de série de politique d'un client chaque fois que la politique de sécurité du client change. Quand un client se connecte à Symantec Endpoint Protection Manager, il reçoit les dernières politiques de sécurité et le dernier numéro de série de politique.

Quand un client essaye de se connecter au réseau via le boîtier DHCP Enforcer, ce dernier récupère le numéro de série de politique à partir de Symantec Endpoint Protection Manager. Le boîtier DHCP Enforcer compare ensuite le numéro de série de politique à celui qu'il reçoit du client. Si les numéros de série de politique correspondent, cela signifie que le boîtier DHCP Enforcer a validé l'exécution par le client d'une politique de sécurité à jour.

La valeur par défaut pour ce paramètre n'est pas activée.

Les directives suivantes s'appliquent :

- Si l'option Vérifier le numéro de série de la politique du client avant d'autoriser l'accès au réseau est cochée, un client doit disposer de la dernière politique de sécurité avant de pouvoir se connecter au réseau par le serveur DHCP normal. Si le client ne dispose pas de la dernière politique de sécurité, le client est

informé qu'il doit télécharger la dernière politique. Le boîtier DHCP Enforcer fait alors suivre sa requête DHCP pour recevoir une configuration réseau de quarantaine.

- Si l'option Check the Policy Serial Number on Client before allowing Client into network (Vérifier le numéro de série de la politique du client avant d'autoriser l'accès au réseau) n'est pas cochée et si la vérification de l'intégrité de l'hôte est réussie, le client peut se connecter au réseau. Le client peut se connecter par le serveur DHCP normal même si sa politique de sécurité n'est pas à jour.

Pour faire vérifier le numéro de série de politique d'un client par le module DHCP Enforcer

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.

   Le groupe de boîtiers DHCP Enforcer doit inclure le boîtier DHCP Enforcer qui vérifie le numéro de série de politique sur un client.
4. Dans la boîte de dialogue Paramètres, dans l'onglet Authentification, cochez **Vérifier le numéro de série de politique sur le client avant de permettre à un client d'accéder au réseau**.
5. Cliquez sur **OK**.

Envoi d'un message de non-conformité du boîtier DHCP Enforcer à un client

Vous pouvez informer le client qui ne peut pas se connecter au réseau avec un message déroulant de Windows. Généralement, le message informe l'utilisateur final qu'un client ne peut pas se connecter au réseau. Le client ne peut pas se connecter au réseau parce qu'il n'exécute pas le client Symantec Endpoint Protection ou le client Symantec Network Access Control.

La plupart des administrateurs entrent des instructions sur la nécessité d'exécuter le client Symantec Endpoint Protection ou le client Symantec Network Access Control. Le message peut comprendre des informations sur un site de téléchargement où les utilisateurs finaux peuvent télécharger le logiciel client requis. Vous pouvez également fournir un numéro de téléphone de contact ou d'autres informations importantes.

Ce paramètre est activé par défaut. Il s'applique seulement aux clients qui n'exécutent pas le client Symantec Endpoint Protection ou le client Symantec Network Access Control.

Dès que vous terminez cette tâche, le message instantané s'affiche sur le client s'il exécute Windows Messenger.

Pour envoyer un message de non-conformité depuis un boîtier DHCP Enforcer vers un client

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.
4. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans la boîte de dialogue Settings (Paramètres), dans l'onglet Authentication (Authentification), sélectionnez **Enable pop-up message on client if Client is not running** (Activer le message instantané sur le client si le logiciel client ne s'exécute pas).
6. Dans la boîte de dialogue Settings (Paramètres), dans l'onglet Authentication (Authentification), cliquez sur **Message**.
7. Dans la boîte de dialogue Pop-up Message Settings (Paramètres des messages instantanés), sélectionnez la fréquence d'affichage du message sur un client.

   Vous pouvez sélectionner les intervalles suivants :

   - Once (Une fois)
     La valeur par défaut est Une fois.
   - Every 30 seconds (Toutes les 30 secondes)
   - Every minute (Toutes les minutes)
   - Every 2 minutes (Toutes les 10 minutes)
   - Every 5 minutes (Toutes les 10 minutes)
   - Every 10 minutes (Toutes les 10 minutes)

8 Tapez le message à afficher dans la zone de texte.

Vous pouvez saisir jusqu'à 125 caractères, y compris les espaces et les signes de ponctuation.

Le message par défaut est :

```
Votre accès au réseau est bloqué parce que vous
n'exécutez pas le logiciel client Symantec. Vous devez l'installer
au préalable.
```

9 Dans la boîte de dialogue Paramètres des messages instantanés, cliquez sur **OK**.

10 Dans la boîte de dialogue Settings (Paramètres), sur l'onglet Authentication (Authentification), cliquez sur **OK**.

Utiliser les paramètres de serveurs DHCP

Vous pouvez spécifier un certain nombre de paramètres de serveur DHCP. Les modifications sont envoyées automatiquement au boîtier DHCP Enforcer sélectionné pendant le battement suivant.

A propos de l'utilisation des paramètres de serveurs DHCP

Vous pouvez spécifier jusqu'à 256 serveurs DHCP. Si vous spécifiez plusieurs serveurs DHCP, vous pouvez assurer le basculement et la répartition de charge. Vous pouvez utiliser le paramètre de priorité de serveur DHCP pour faire envoyer par le boîtier DHCP Enforcer des requêtes DHCP à plusieurs serveurs DHCP en même temps.

Vous pouvez également installer des serveurs DHCP normaux et de quarantaine sur des ordinateurs séparés ou sur un ordinateur. Si un client est autorisé à se connecter au réseau, le serveur DHCP normal attribue une adresse IP au client. Si vous installez un serveur DHCP de quarantaine, un client non-autorisé peut encore se connecter au réseau. Cependant, le client non-autorisé peut seulement communiquer avec les ordinateurs limités dans le réseau.

Se reporter à "Ajouter un serveur DHCP normal" à la page 153.

Se reporter à "Ajouter un serveur DHCP de quarantaine" à la page 154.

Si vous prévoyez d'installer un serveur DHCP normal et un serveur de quarantaine sur le même ordinateur, vous devez sélectionner l'option Activer l'identification de classe d'utilisateurs.

Si vous sélectionnez l'option Enable User Class ID option (Activer l'identification de classe d'utilisateurs), le boîtier DHCP Enforcer ajoute une classe d'utilisateurs en quarantaine dans les messages DHCP. Ces messages de DHCP sont transférés au serveur DHCP. Le serveur DHCP attribue alors au client la configuration de quarantaine qui est basée sur la présence de cet identificateur de classe d'utilisateurs. Vous pouvez utiliser un serveur DHCP qui fonctionne en tant que serveur normal et en tant que serveur de quarantaine.

Se reporter à "Combiner un serveur DHCP normal et un serveur DHCP en quarantaine sur un ordinateur" à la page 152.

Si vous désactivez l'option Enable User Class ID (Activer l'identification de classe d'utilisateurs), vous devez installer deux serveurs DHCP distincts. Un des serveurs DHCP fonctionne comme serveur DHCP normal. Le deuxième serveur DHCP fonctionne comme serveur DHCP de quarantaine.

Se reporter à "Activer les serveurs DHCP distincts normaux et mis en quarantaine" à la page 153.

Combiner un serveur DHCP normal et un serveur DHCP en quarantaine sur un ordinateur

L'option Activer l'identification de classe d'utilisateurs vous permet d'installer un serveur DHCP normal et un serveur DHCP en quarantaine sur un ordinateur. Vous aurez donc besoin de peu d'ordinateurs pour réaliser la sécurité maximale.

Pour combiner un serveur DHCP normal et un serveur DHCP en quarantaine sur un ordinateur

1. Dans la console Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administration).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.
4. Dans la page Admin, sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans la boîte de dialogue Settings (Paramètres), dans l'onglet DHCP Servers (Serveurs DHCP), sélectionnez l'option **Enable User Class ID** (Activer l'identification de classe d'utilisateurs).
6. Dans la boîte de dialogue Settings (Paramètres), sur l'onglet DHCP Servers (Serveurs DHCP), cliquez sur **OK**.

Activer les serveurs DHCP distincts normaux et mis en quarantaine

L'option Enable User Class ID (Activer l'identification de classe d'utilisateurs) permet d'installer des serveurs DHCP normaux distincts ainsi que des serveurs DHCP de quarantaine. Vous pouvez ainsi obtenir une sécurité maximale si le trafic dans un réseau l'exige.

Pour activer les serveurs DHCP distincts normaux et mis en quarantaine

1. Dans la console Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administration).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.
4. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans la boîte de dialogue Setting (Paramètres), dans l'onglet Serveurs DHCP, désélectionnez l'option **Enable User Class ID** (Activer l'identification de classe d'utilisateurs).
6. Cliquez sur **OK**.

Ajouter un serveur DHCP normal

Les informations pour le serveur DHCP normal apparaissent sous forme de ligne dans un tableau dans la boîte de dialogue Paramètres.

Pour ajouter un serveur DHCP normal

1. Dans la console Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administration).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.
4. Dans la page Admin, sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans la boîte de dialogue Paramètres, dans l'onglet Serveurs DHCP, sous Serveurs DHCP normaux, cliquez sur **Add** (Ajouter).
6. Dans la boîte de dialogue Ajouter un serveur DHCP, sélectionnez **Enable** (Activer).
7. Tapez l'adresse IP ou le nom d'hôte du serveur DHCP dans la zone de texte IP du serveur DHCP.

8. Tapez le numéro de port du serveur DHCP dans la zone de texte du port de serveur DHCP.

   Le paramètre de port par défaut sur le serveur DHCP est 67.

9. Sélectionnez le nombre de priorité pour le serveur DHCP dans la zone de texte de priorité de serveur DHCP.

   Le paramètre par défaut pour la priorité est 1.

   Si vous utilisez un serveur DHCP sur un ordinateur en tant que serveur normal et de quarantaine, ajoutez le serveur DHCP dans cette boîte de dialogue en tant que serveur DHCP normal et de quarantaine. Complétez les mêmes informations dans la boîte de dialogue Ajouter un serveur DHCP pour les deux types de serveurs DHCP.

   Vous pouvez attribuer une priorité de 0 à 15 à un serveur DHCP. Ce paramètre est utilisé pour la répartition de charge. Si vous configurez deux serveurs DHCP avec la même priorité, DHCP Enforcer fait suivre la requête aux deux serveurs DHCP en même temps. Si l'un des serveurs DHCP est occupé, l'autre peut répondre. Si vous configurez plusieurs serveurs DHCP avec différentes priorités, DHCP Enforcer fait suivre d'abord les requêtes DHCP au serveur DHCP qui a la priorité la plus élevée. Ensuite, le serveur DHCP fait suivre les requêtes DHCP aux autres.

10. Cliquez sur **OK**.

    Dans la boîte de dialogue Settings (Paramètres), sur l'onglet DHCP Servers (Serveurs DHCP), cliquez sur **OK**.

Ajouter un serveur DHCP de quarantaine

Les informations pour le serveur DHCP normal apparaissent sous forme de ligne dans un tableau dans la boîte de dialogue Paramètres.

Pour ajouter un serveur DHCP de quarantaine

1. Dans la console Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administration).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.
4. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans la boîte de dialogue Paramètres, dans l'onglet Serveurs DHCP, sous Serveurs DHCP de quarantaine, cliquez sur **Ajouter**.

6 Dans la boîte de dialogue Ajouter un serveur DHCP, sélectionnez **Activer** si cela n'a pas déjà été fait.

7 Tapez l'adresse IP ou le nom d'hôte du serveur DHCP dans la zone de texte IP du serveur DHCP.

8 Tapez le numéro de port du serveur DHCP dans la zone de texte du port de serveur DHCP.

Le paramètre de port par défaut sur le serveur DHCP est 67.

9 Sélectionnez le nombre de priorité pour le serveur DHCP dans la zone de texte de priorité de serveur DHCP.

Le paramètre par défaut pour la priorité est 1.

Si vous utilisez un serveur DHCP sur un ordinateur en tant que serveur normal et de quarantaine, ajoutez le serveur DHCP dans cette boîte de dialogue en tant que serveur DHCP normal et de quarantaine. Complétez les mêmes informations dans la boîte de dialogue Ajouter un serveur DHCP pour les deux types de serveurs DHCP.

Vous pouvez attribuer une priorité de 0 à 15 à un serveur DHCP. Ce paramètre est utilisé pour la répartition de charge. Si vous configurez deux serveurs DHCP avec la même priorité, DHCP Enforcer fait suivre la requête aux deux serveurs DHCP en même temps. Si l'un des serveurs DHCP est occupé, l'autre peut répondre. Si vous configurez plusieurs serveurs DHCP avec différentes priorités, le boîtier DHCP Enforcer fait suivre d'abord les requêtes DHCP au serveur DHCP qui a la priorité la plus élevée, puis aux autres.

10 Cliquez sur **OK**.

Dans la boîte de dialogue Settings (Paramètres), sur l'onglet Serveurs DHCP, cliquez sur **OK**.

Utilisation des paramètres avancés de boîtier DHCP Enforcer

Vous pouvez configurer les paramètres de configuration avancés DHCP Enforcer suivants :

- Authentication timeout (Délai d'authentification)
  Se reporter à "Configurer une quarantaine automatique pour un client qui échoue à l'authentification" à la page 156.
- DHCP message timeout (Délai d'expiration de message DHCP)
  Se reporter à "Pour spécifier la période d'attente du boîtier DHCP Enforcer avant qu'il n'accorde un accès client au réseau" à la page 157.

- Adresses MAC des hôtes approuvés dont le module DHCP Enforcer autorise la connexion au serveur DHCP normal sans authentification
  Se reporter à "Autorisation des serveurs, des clients et des périphériques à se connecter au réseau en tant qu'hôtes approuvés sans authentification" à la page 157.
- Enabling DNS spoofing (Activation de l'usurpation DNS)
  Se reporter à "Empêcher l'usurpation DNS" à la page 159.
- Allowing legacy clients (Autorisation de clients hérités)
  Se reporter à "Autorisation d'un client hérité à se connecter au réseau avec DHCP Enforcer" à la page 159.
- Enabling local authentication (Activation de l'authentification locale)
  Se reporter à "Activation de l'authentification locale sur le boîtier DHCP Enforcer" à la page 160.

Lorsque vous appliquez l'un de ces paramètres de configuration, les modifications sont envoyées au module DHCP Enforcer sélectionné lors du battement suivant.

Configurer une quarantaine automatique pour un client qui échoue à l'authentification

Vous pouvez spécifier la durée pendant laquelle le boîtier DHCP Enforcer attend une réponse d'un client. La réponse permet de vérifier si le client Symantec Endpoint Protection ou le client Symantec Network Access Control a été installé. Si le boîtier DHCP Enforcer considère que le logiciel client n'a pas été installé pendant l'intervalle spécifié, le client est maintenu en quarantaine.

Pour configurer une quarantaine automatique pour un client qui échoue à l'authentification

1. Dans la console Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administration).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.
4. Dans la console Symantec Endpoint Protection Manager, sous View Servers (Afficher les serveurs), sélectionnez le boîtier Enforcer DHCP pour lequel vous voulez définir le paramètre de configuration.
5. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).

6 Dans la boîte de dialogue Paramètres, dans l'onglet Avancé, sous Paramètres d'expiration, sélectionnez **Délai d'authentification**.

Le paramètre par défaut est de trois secondes.

7 Cliquez sur **OK**.

Spécifier la période de l'attente du boîtier DHCP Enforcer avant qu'il n'accorde un accès client au réseau

Vous pouvez spécifier combien de temps un boîtier DHCP Enforcer doit attendre une réponse après avoir envoyé des messages DHCP à un client ou à un serveur DHCP. Si un boîtier DHCP Enforcer ne reçoit pas de réponse après un intervalle indiqué, il réinitialise son état interne au sujet du client ou du serveur DHCP. Par conséquent, le boîtier DHCP Enforcer peut seulement recevoir un premier message.

Pour spécifier la période d'attente du boîtier DHCP Enforcer avant qu'il n'accorde un accès client au réseau

1 Dans la console Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administration).

2 Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).

3 Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.

4 Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez le boîtier DHCP Enforcer pour lequel vous voulez définir le paramètre de configuration.

5 Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).

6 Dans la boîte de dialogue Settings (Paramètres), dans l'onglet Advanced (Avancé), sous Timeout Parameters (Paramètres d'expiration), sélectionnez **DHCP message timeout** (Dépassement de délai de message DHCP).

Le paramètre par défaut est de trois secondes.

7 Cliquez sur **OK**.

Autorisation des serveurs, des clients et des périphériques à se connecter au réseau en tant qu'hôtes approuvés sans authentification

Un hôte approuvé est habituellement un serveur qui ne peut pas installer le logiciel client, un serveur non-Windows par exemple, ou un périphérique, une imprimante par exemple. Vous pouvez également vouloir identifier des clients non-Windows en tant qu'hôtes approuvés parce que le module DHCP Enforcer est incapable

d'authentifier tous les clients qui n'exécutent pas le client Symantec Endpoint Protection ou le client Symantec Network Access Control.

Vous pouvez utiliser des adresses MAC pour spécifier certains serveurs, clients et périphériques comme hôtes approuvés.

Lorsque vous spécifiez des serveurs, des clients et des périphériques comme hôtes approuvés, le boîtier DHCP Enforcer transmet tous les messages DHCP de l'hôte approuvé au serveur DHCP normal sans authentifier l'hôte approuvé.

Pour autoriser des serveurs, des clients et des périphériques à se connecter au réseau en tant qu'hôtes approuvés sans authentification

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.
4. Dans la page Admin, sous Afficher les serveurs, sélectionnez le boîtier DHCP Enforcer qui autorise les serveurs, les clients et les périphériques qui ont été spécifiés en tant qu'hôtes approuvés à se connecter au réseau sans authentification.
5. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
6. Dans la boîte de dialogue Paramètres, dans l'onglet Avancé, sous Hôtes approuvés, cliquez sur **Ajouter**.
7. Dans la boîte de dialogue Ajouter un hôte approuvé, tapez Adresse MAC pour le client ou l'hôte approuvé dans le champ Adresse MAC de l'hôte.

   Vous pouvez également copier des adresses MAC à partir d'un fichier texte.

   Quand vous spécifiez une adresse MAC, vous pouvez utiliser un caractère générique si vous le tapez dans chacun des trois champs de droite.

   Par exemple, 11-22-23-*-*-* est un exemple d'utilisation correcte du caractère générique. Cependant, 11-22-33-44-*-66 ne représente pas une utilisation correcte du caractère générique.
8. Cliquez sur **OK**.
9. Dans la boîte de dialogue Paramètres, dans l'onglet Avancé, cliquez sur **OK**.

   L'adresse MAC de l'hôte approuvé que vous avez ajouté apparaît maintenant dans la zone Adresse MAC de la boîte de dialogue Paramètres.
10. Cliquez sur **OK**.

Empêcher l'usurpation DNS

Vous pouvez tenter d'éviter l'usurpation DNS. A cet effet, le boîtier DHCP Enforcer doit modifier les messages DHCP appropriés qui sont envoyés à un client. Le boîtier DHCP Enforcer remplace l'adresse IP du serveur DNS dans le message DHCP par l'adresse IP externe du boîtier DHCP Enforcer. Par conséquent le boîtier DHCP Enforcer agit en tant que serveur DNS pour les clients et empêche ainsi l'usurpation DNS. Cette fonction doit être activée si vous voulez proposer des clients à la demande Symantec Network Access Control à partir d'un boîtier DHCP Enforcer.

Pour empêcher l'usurpation DNS

1. Dans la console Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administration).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.
4. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans la boîte de dialogue Paramètres, dans l'onglet Avancé, sélectionnez **Enable DNS Spoofing** (Autoriser l'usurpation DNS).

Utilisez l'adresse IP local de l'Enforcer en tant que réponse à la demande de DNS	Le module d'application le boîtier DHCP Enforcer remplace l'adresse IP officiellement demandée par sa propre adresse IP externe. Le boîtier DHCP Enforcer agit en tant que serveur DNS quand il répond à une requête DNS en utilisant sa propre adresse IP.
Utilisez les adresses IP suivantes en tant que réponse de demande de DNS	Le boîtier DHCP Enforcer remplace l'adresse IP officiellement demandée par l'une des adresses IP que vous avez spécifiées. Le boîtier DHCP Enforcer agit en tant que serveur DNS quand il répond à une requête DNS en utilisant l'une des adresses IP que vous avez spécifiées.

6. Cliquez sur **OK**.

Autorisation d'un client hérité à se connecter au réseau avec DHCP Enforcer

Vous pouvez activer un boîtier DHCP Enforcer de sorte à ce qu'il se connecte à des clients hérités 5.1.x. Si votre réseau prend en charge une console Symantec Endpoint Protection Manager 11.0.2 ainsi qu'un boîtier Symantec DHCP Enforcer et qu'il doit prendre en charge des clients hérités 5.1.x, vous pouvez activer la

prise en charge des clients hérités 5.1.x sur la console du serveur de gestion afin que le boîtier Symantec DHCP Enforcer ne les bloque pas.

Pour autoriser un client hérité à se connecter au réseau avec un boîtier DHCP Enforcer

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin, cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de boîtiers DHCP Enforcer.
4. Dans la page Admin, sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans la boîte de dialogue Settings (Paramètres), dans l'onglet Advanced (Avancés), sélectionnez **Allow legacy clients** (Autoriser les clients hérités).
6. Cliquez sur **OK**.

Activation de l'authentification locale sur le boîtier DHCP Enforcer

L'authentification locale étant activée, le boîtier DHCP Enforcer perd sa connexion avec le serveur sur lequel Symantec Endpoint Protection Manager est installé. Par conséquent, le boîtier DHCP Enforcer authentifie un client localement.

Pour activer l'authentification locale sur le boîtier DHCP Enforcer

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de boîtiers DHCP Enforcer.
4. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans la boîte de dialogue Settings (Paramètres), dans l'onglet Advanced (Avancé), sélectionnez **Enable Local Authentication** (Activer l'authentification locale).
6. Cliquez sur **OK**.

Chapitre 8

Configurer le boîtier Symantec LAN Enforcer sur la console Symantec Endpoint Protection Manager

Ce chapitre traite des sujets suivants :

A propos de la configuration de Symantec LAN Enforcer sur la console de boîtier Symantec Endpoint Protection Manager

Vous pouvez ajouter ou modifier des paramètres de configuration pour le module LAN Enforcer dans la console Symantec Endpoint Protection Manager. Symantec Endpoint Protection Manager est également désigné sous le nom de serveur de gestion.

Avant de poursuivre, vous devez effectuer les tâches suivantes :

- Installez le logiciel de Symantec Endpoint Protection Manager sur un ordinateur.
  Consultez le *Guide d'installation de Symantec Endpoint Protection et de Symantec Network Access Control*.
  L'ordinateur sur lequel le logiciel Symantec Endpoint Protection Manager est installé est également désigné sous le nom de serveur de gestion.
- Connectez le boîtier Symantec LAN Enforcer au réseau.
- Configurez le boîtier Symantec LAN Enforcer sur la console LAN Enforcer locale pendant l'installation.

Après avoir effectué ces tâches, vous pouvez spécifier les paramètres de configuration supplémentaires du boîtier LAN Enforcer sur un serveur de gestion.

A propos de la configuration de serveurs RADIUS sur un boîtier LAN Enforcer

Vous pouvez modifier les paramètres LAN Enforcer dans la console Symantec Endpoint Protection. Le module d'application Enforcer doit être installé et connecté à Symantec Endpoint Protection Manager avant que vous puissiez le configurer pour imposer des politiques d'intégrité de l'hôte sur le client.

Vous pouvez configurer les options suivantes pour LAN Enforcer :

- Définissez le nom de groupe et la description d'Enforcer, le port d'écoute et la liste de serveurs de gestion.
- Configurez le ou les serveurs RADIUS. Vous configurez le nom d'hôte ou l'adresse IP, le port d'authentification et le secret partagé. Si vous configurez les serveurs multiples dans le groupe et que l'un s'arrête, LAN Enforcer se connecte au serveur suivant dans la liste.
- Configurez un commutateur ou un groupe de commutateurs.

- Paramètres pour activer la connexion et spécifier des paramètres de fichier journal.
- Activez et désactivez l'authentification locale.
- Configurez des clients pour l'authentification 802.1x.

Si un paramètre se rapporte à un commutateur 802.1x, les mêmes instructions s'appliquent pour configurer des points d'accès sans fil.

Se reporter à "Configurer des points d'accès sans fil 802.1x sur un boîtier LAN Enforcer" à la page 163.

Configurer des points d'accès sans fil 802.1x sur un boîtier LAN Enforcer

Le boîtier LAN Enforcer prend en charge un certain nombre de protocoles sans fil, dont WEP 56, WEP 128 et WPA/WPA2 avec 802.1x.

Vous pouvez configurer LAN Enforcer pour protéger le point d'accès (AP) sans fil autant qu'il protège un commutateur si les conditions suivantes sont vraies :

- Le réseau inclut un réseau local sans fil LAN Enforcer avec 802.1x.
- Les clients sans fil exécutent un supplicant qui prend en charge un de ces protocoles.
- Le point d'accès sans fil doit prendre en charge un de ces protocoles

Pour des connexions sans fil, le dispositif d'authentification est le port LAN logique sur le point d'accès sans fil.

Vous configurez un point d'accès sans fil pour 802.1x et pour des commutateurs de la même manière. Vous incluez des points d'accès sans fil aux paramètres LAN Enforcer en tant qu'élément d'un profil de commutateur. Là où une instruction ou une partie de l'interface utilisateur se rapporte à un commutateur, utilisez la terminologie de point d'accès sans fil comparable. Par exemple, si vous êtes chargé de sélectionner un modèle de commutateur, sélectionnez le modèle de point d'accès sans fil. Si le fournisseur de point d'accès sans fil est listé, sélectionnez-le pour le modèle. Si le fournisseur n'est pas listé, choisissez Autres.

La configuration de point d'accès sans fil pour 802.1x et pour des commutateurs incluent les différences suivantes :

- Seule la configuration de base est prise en charge.
  Le mode transparent n'est pas pris en charge.
- Il peut également y avoir des différences au niveau de la prise en charge pour des VLAN, selon le point d'accès sans fil.

Quelques commutateurs dynamiques de VLAN peuvent exiger que vous configuriez le point d'accès avec des Service Set Identifiers (SSID) multiples. Chaque SSID est associé à VLAN.
Consultez la documentation qui est livrée avec le commutateur dynamique de VLAN.

Selon le modèle de point d'accès sans fil que vous utilisez, vous pouvez utiliser une des options de contrôle d'accès suivantes au lieu de VLAN :

Listes de contrôle d'accès (ACL)	Certains points d'accès sans fil, tels qu'Aruba, prennent en charge les ACL qui permettent à l'administrateur réseau de définir des politiques pour la gestion du trafic réseau. Vous pouvez utiliser l'option générique sur LAN Enforcer en sélectionnant le nom de fournisseur de point d'accès sans fil. Vous pouvez également sélectionner Autres pour le modèle du commutateur compatible 802.1x (sinon il n'est pas listé). L'option générique envoie une balise d'attribut générique comprenant l'ID ou le nom de VLAN vers le point d'accès. Vous pouvez alors personnaliser le point d'accès. Le point d'accès peut maintenant indiquer la balise d'attribut générique pour l'ID de VLAN et la faire correspondre avec l'ID de l'ACL du point d'accès sans fil. Vous pouvez utiliser le tableau Action de commutation comme tableau Action d'ACL. La configuration supplémentaire sur le contrôleur de point d'accès sans fil ou normal peut être requise. Par exemple, vous devrez peut-être mapper la balise RADIUS qui est envoyée au point d'accès sans fil sur le contrôleur de point d'accès. Consultez la documentation sur le point d'accès sans fil pour des détails.
MAC niveau 802.1x	Vous pouvez brancher le point d'accès sans fil dans un commutateur qui prend en charge MAC niveau 802.1x. Pour cette mise en place, vous devez désactiver 802.1x sur le point d'accès sans fil. Vous ne pouvez l'utiliser que sur le commutateur. Le commutateur authentifie alors les clients sans fil en identifiant les nouvelles adresses MAC. Après avoir authentifié l'adresse MAC, il met cette adresse MAC sur le VLAN spécifié au lieu de tout le port. Chaque nouvelle adresse MAC doit être authentifiée. Cette option n'est pas aussi sécurisée. Cependant, cette option vous permet d'utiliser la fonction de commutation VLAN.

Modifier les paramètres de configuration de LAN Enforcer sur une console Symantec Endpoint Protection Manager

Vous pouvez modifier les paramètres de configuration du module LAN Enforcer sur un serveur de gestion. Les paramètres de configuration sont automatiquement téléchargés depuis le serveur de gestion vers le boîtier LAN Enforcer au cours du battement suivant.

Pour modifier les paramètres de configuration de LAN Enforcer sur une console Symantec Endpoint Protection Manager

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez le groupe de modules d'application Enforcer auxquels appartient le boîtier LAN Enforcer.

   Le groupe de modules d'application doit inclure le module LAN Enforcer dont les paramètres de configuration sont à modifier.
4. Dans la page Admin, sous View Servers (Afficher les serveurs), sélectionnez le boîtier LAN Enforcer dont les paramètres de configuration sont à modifier.
5. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
6. Dans la boîte de dialogue Settings (Paramètres), modifiez les paramètres de configuration.

   La boîte de dialogue Settings (Paramètres) de LAN Enforcer propose les catégories de paramètres de configuration suivantes :

   General (Général) — Cet onglet propose les paramètres de LAN Enforcer suivants :

   - Nom de groupe pour les boîtiers de LAN Enforcer
   - Port d'écoute
   - Description du groupe de boîtiers LAN Enforcer
   - Sélection de la liste de serveurs de gestion utilisée par le module LAN Enforcer

   Se reporter à "Utiliser les paramètres généraux" à la page 167.

Groupe de serveurs RADIUS	Cet onglet propose les paramètres de LAN Enforcer suivants : ■ Nom du groupe de serveurs RADIUS ■ Nom d'hôte ou Adresse IP du serveur RADIUS ■ Numéro de port du serveur RADIUS ■ Nom convivial du serveur RADIUS Se reporter à "Utiliser des paramètres de groupe de serveurs RADIUS" à la page 171.
Commutateur	Cet onglet propose les paramètres de LAN Enforcer suivants : ■ Activez la politique de commutateurs ■ Le nom de la politique de commutateurs ■ Le modèle de commutateur, sélectionné dans une liste de commutateurs pris en charge ■ Le secret partagé ■ Le groupe de serveur RADIUS ■ Le délai de reauthentication ■ Si le commutateur transfère d'autres protocoles en plus d'EAP ■ Adresse du commutateur ■ VLAN sur le commutateur ■ Action Se reporter à "Utiliser les paramètres de commutateur" à la page 179.
Advanced (Avancé)	Cet onglet propose les paramètres de LAN Enforcer suivants : ■ Enable local authentication (Activer l'authentification locale). ■ Allow legacy client (Autoriser client hérité) Se reporter à "Utilisation des paramètres avancés de boîtier LAN Enforcer" à la page 209.
Paramètres de journal	Paramètres permettant d'activer la consignation des journaux de serveur et des journaux d'activités client et de spécifier les paramètres de fichier journal. Se reporter à "Rapports Enforcer" à la page 439. Se reporter à "A propos des journaux Enforcer" à la page 440. Se reporter à "Configurer les paramètres du journal Enforcer" à la page 443.

Utiliser les paramètres généraux

Vous pouvez ajouter ou modifier la description d'un boîtier LAN Enforcer ou d'un groupe de boîtiers LAN Enforcer dans la console Symantec Endpoint Protection Manager.

Se reporter à "Ajout ou modification de la description d'un groupe d'Enforcer avec un module LAN Enforcer" à la page 169.

Se reporter à "Ajout ou modification de la description d'un module LAN Enforcer" à la page 169.

Vous devez établir un port d'écoute, qui est utilisé pour la communication entre le commutateur VLAN et le boîtier LAN Enforcer.

Se reporter à "Spécifier un port d'écoute utilisé pour la communication entre un commutateur VLAN et LAN Enforcer" à la page 168.

Toutefois, vous ne pouvez pas ajouter ou modifier le nom d'un groupe de boîtiers LAN Enforcer dans la console Symantec Endpoint Protection Manager. Vous ne pouvez pas ajouter ou modifier l'adresse IP ou le nom d'hôte d'un boîtier LAN Enforcer dans la console Symantec Endpoint Protection Manager. Vous devez à la place effectuer ces tâches dans la console Enforcer.

Se reporter à "Ajouter ou modifier le nom d'un groupe de boîtiers LAN Enforcer avec un module LAN Enforcer" à la page 167.

Vous pouvez seulement changer l'adresse IP ou le nom d'hôte d'un module LAN Enforcer sur la console Enforcer pendant l'installation. Si vous voulez modifier ultérieurement l'adresse IP ou le nom d'hôte d'un module LAN Enforcer, vous pouvez le faire sur la console LAN Enforcer.

Se reporter à "Ajout ou modification de l'adresse IP ou du nom d'hôte d'un module LAN Enforcer" à la page 169.

Vous pouvez également ajouter ou modifier l'adresse IP ou le nom d'hôte de Symantec Endpoint Protection Manager dans une liste de serveurs de gestion.

Se reporter à "Connexion de LAN Enforcer à Symantec Endpoint Protection Manager" à la page 170.

Ajouter ou modifier le nom d'un groupe de boîtiers LAN Enforcer avec un module LAN Enforcer

Vous pouvez ajouter ou modifier le nom d'un groupe de boîtiers LAN Enforcer dont un boîtier LAN Enforcer est membre. Effectuez ces tâches sur la console Enforcer pendant l'installation. Si vous voulez modifier ultérieurement le nom d'un groupe de boîtiers LAN Enforcer, vous pouvez le faire sur la console Enforcer.

Tous les modules Enforcer d'un groupe partagent les mêmes paramètres de configuration.

Spécifier un port d'écoute utilisé pour la communication entre un commutateur VLAN et LAN Enforcer

Quand vous configurez les paramètres d'un boîtier LAN Enforcer, vous spécifiez les ports d'écoute suivants :

- Port d'écoute qui est utilisé pour la communication entre le commutateur VLAN et LAN Enforcer.

  Le commutateur VLAN envoie le paquet RADIUS au port UDP.
- Port d'écoute qui est utilisé pour la communication entre LAN Enforcer et un serveur RADIUS.

  Vous spécifiez ce port quand vous spécifiez un serveur RADIUS.

Si le serveur RADIUS est installé sur le serveur de gestion, il ne devrait pas être configuré pour utiliser le port 1812. Les serveurs RADIUS sont configurés pour utiliser le port 1812 comme paramètre par défaut. Puisque le serveur de gestion utilise également le port 1812 pour communiquer avec LAN Enforcer, il y a un conflit.

Pour spécifier un port de écoute qui est utilisé pour la communication entre un commutateur VLAN et LAN Enforcer

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez le groupe Enforcer.
4. Dans la page Admin, sous View Servers (Afficher les serveurs), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Basic Settings (Paramètres de base), tapez le numéro du port UDP que vous voulez attribuer dans le champ Listen port (Port d'écoute).

   Le paramètre par défaut pour le port est 1812. L'intervalle va de 1 à 65535.
6. Dans la boîte de dialogue LAN Enforcer Settings (Paramètres de LAN Enforcer), dans l'onglet Basic Settings (Paramètres de base), cliquez sur **OK**.

Ajout ou modification de la description d'un groupe d'Enforcer avec un module LAN Enforcer

Vous pouvez ajouter ou modifier le nom d'un groupe d'Enforcer dont un boîtier Symantec LAN Enforcer est membre. Vous pouvez effectuer cette tâche sur la console Symantec Endpoint Protection Manager au lieu de la console LAN Enforcer.

Pour ajouter ou modifier la description d'un groupe d'Enforcer avec un module LAN Enforcer

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin, sous Afficher les serveurs, sélectionnez et développez le groupe Enforcer dont vous voulez ajouter ou modifier la des cription.
4. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans la boîte de dialogue Settings (Paramètres), sous l'onglet Basic Settings (Paramètres de base), ajoutez ou modifiez une description pour le groupe de boîtiers Enforcer dans le champ Description.
6. Dans la boîte de dialogue Settings (Paramètres), cliquez sur **OK**.

Ajout ou modification de l'adresse IP ou du nom d'hôte d'un module LAN Enforcer

Vous pouvez seulement changer l'adresse IP ou le nom d'hôte d'un module LAN Enforcer sur la console d'Enforcer pendant l'installation. Si vous voulez modifier ultérieurement l'adresse IP ou le nom d'hôte d'un module LAN Enforcer, vous pouvez le faire sur la console LAN Enforcer.

Consultez le *Guide d'installation de Symantec Endpoint Protection et de Symantec Network Access Control*.

Ajout ou modification de la description d'un module LAN Enforcer

Vous pouvez ajouter ou modifier la description d'un module LAN Enforcer. Vous pouvez effectuer cette tâche sur la console Symantec Endpoint Protection Manager au lieu de la console LAN Enforcer. Après avoir terminé cette tâche, la description apparaît dans le champ Description du volet Gestion du serveur.

Pour ajouter ou modifier la description d'un module LAN Enforcer

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe d'Enforcer qui inclut le module LAN Enforcer dont vous voulez ajouter ou modifier la description.
4. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez le module LAN Enforcer dont vous voulez ajouter ou modifier la description.
5. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Enforcer Properties** (Modifier les propriétés d'Enforcer).
6. Dans la boîte de dialogue Properties (Propriétés) du module Enforcer, ajoutez ou modifiez une description pour le module LAN Enforcer dans le champ Description (Description).
7. Dans la boîte de dialogue Properties (Propriétés) du module Enforcer, cliquez sur **OK**.

Connexion de LAN Enforcer à Symantec Endpoint Protection Manager

Les modules d'application Enforcer doivent pouvoir se connecter aux serveurs sur lesquels Symantec Endpoint Protection Manager est installé. Symantec Endpoint Protection Manager comprend un fichier qui aide à la gestion du trafic entre les clients, les gestionnaires Symantec Endpoint Protection Manager et les modules d'application Enforcer facultatifs tels que LAN Enforcer.

Ce fichier est appelé liste de serveurs de gestion. La liste de serveurs de gestion spécifie à quel serveur Symantec Endpoint Protection Manager se connecte un module d'application LAN Enforcer. Elle spécifie également à quel serveur Symantec Endpoint Protection un module d'application LAN Enforcer se connecte en cas de défaillance d'un serveur de gestion.

Une liste de serveurs de gestion par défaut est automatiquement créée pour chaque site pendant l'installation initiale. Tous les gestionnaires Symantec Endpoint Protection Manager disponibles sur le site sont automatiquement ajoutés à la liste de serveurs de gestion par défaut.

La liste de serveurs de gestion par défaut comprend les adresses IP ou les noms d'hôte du serveur de gestion auxquels les modules d'application Integrated Enforcer peuvent se connecter après l'installation initiale. Vous pouvez créer une liste de serveurs de gestion personnalisée avant de déployer des modules d'application Enforcer. Si vous créez une liste de serveurs de gestion personnalisée, vous pouvez

spécifier la priorité de connexion d'un module d'application LAN Enforcer aux serveurs de gestion.

Si un administrateur a créé plusieurs listes de serveurs de gestion, vous pouvez sélectionner la liste de serveurs de gestion spécifique comprenant les adresses IP ou les noms d'hôte des serveurs de gestion auxquels vous voulez que LAN Enforcer se connecte. Si le site ne comprend qu'un seul serveur de gestion, vous pouvez sélectionner la liste de serveurs de gestion par défaut.

Pour plus d'informations sur la personnalisation des listes de serveurs de gestion, consultez le *Guide d'administration de Symantec Endpoint Protection et Symantec Network Access Control*.

Connexion de LAN Enforcer à Symantec Endpoint Protection Manager

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.

   Le groupe Enforcer doit inclure le LAN Enforcer pour lequel vous voulez modifier la liste de serveurs de gestion.
4. Dans la page Admin (Admin), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans la boîte de dialogue Settings ()Paramètres, dans l'onglet Basic Settings (Paramètres de base), sous Communication, sélectionnez la liste de serveurs de gestion à utiliser par ce module LAN Enforcer.
6. Dans la boîte de dialogue Paramètres, dans l'onglet Général, sous Communication, cliquez sur **Sélectionner**.

   Vous pouvez afficher les adresses IP et les noms d'hôte de tous les serveurs de gestion disponibles, ainsi que les priorités qui leur ont été attribuées.
7. Dans la boîte de dialogue Management Server List (Listes de serveurs de gestion), cliquez sur **Close** (Fermer).
8. Dans la boîte de dialogue Settings (Paramètres), cliquez sur **OK**.

Utiliser des paramètres de groupe de serveurs RADIUS

Vous pouvez configurer LAN Enforcer pour vous connecter à un ou plusieurs serveurs RADIUS.

Vous devez spécifier des serveurs RADIUS en tant qu'élément de groupe de serveurs RADIUS. Chaque groupe peut contenir un ou plusieurs serveurs RADIUS.

Le but d'un groupe de serveurs RADIUS est que les serveurs RADIUS fournissent le basculement. Si un serveur RADIUS dans le groupe de serveurs RADIUS devient indisponible, LAN Enforcer essaie de se connecter avec un autre serveur RADIUS qui fait partie du groupe de serveurs RADIUS.

Vous pouvez ajouter, modifier et supprimer le nom d'un groupe de serveurs RADIUS dans la console Symantec Endpoint Protection Manager.

Se reporter à "Ajouter un nom de groupe de serveurs RADIUS et un serveur RADIUS" à la page 172.

Se reporter à "Modifier le nom d'un groupe de serveurs RADIUS" à la page 174.

Se reporter à "Supprimer le nom d'un groupe de serveurs RADIUS" à la page 178.

Vous pouvez ajouter, modifier et supprimer le nom, le nom d'hôte, l'adresse IP, le numéro de port d'authentification et le secret partagé d'un serveur RADIUS dans la console Symantec Endpoint Protection Manager.

Se reporter à "Ajouter un nom de groupe de serveurs RADIUS et un serveur RADIUS" à la page 172.

Se reporter à "Modifier le nom convivial d'un serveur RADIUS" à la page 174.

Se reporter à "Modifier le nom d'hôte ou l'adresse IP d'un serveur RADIUS" à la page 175.

Se reporter à "Modifier le numéro de port d'authentification d'un serveur RADIUS" à la page 176.

Se reporter à "Modifier le secret partagé d'un serveur RADIUS" à la page 177.

Se reporter à "Supprimer un serveur RADIUS" à la page 178.

Ajouter un nom de groupe de serveurs RADIUS et un serveur RADIUS

Vous pouvez ajouter un nom de groupe de serveurs RADIUS et un serveur RADIUS en même temps.

Pour ajouter un nom de groupe de serveurs RADIUS et un serveur RADIUS

1. Dans la console Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administration).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez le groupe Enforcer.
4. Dans la page Admin, sous View Servers (Afficher les serveurs), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).

5 Dans la boîte de dialogue Paramètres de LAN Enforcer, dans l'onglet Groupe de serveurs RADIUS, cliquez sur **Ajouter**.

Le nom de Groupe de serveurs RADIUS et l'adresse IP d'un serveur RADIUS existant apparaissent dans le tableau.

6 Dans la boîte de dialogue Ajouter un groupe de serveurs RADIUS, tapez le nom de groupe de serveurs RADIUS dans la zone de texte Groupe.

Le nom du groupe de serveurs RADIUS, le nom d'hôte ou l'adresse IP d'un serveur RADIUS existant et le numéro de port du serveur RADIUS apparaissent dans le tableau.

7 Dans la boîte de dialogue Ajouter un serveur RADIUS, cliquez sur **Add** (Add).

8 Dans la boîte de dialogue Add RADIUS Server (Ajouter un serveur RADIUS), tapez ce qui suit :

Dans le champ : Friendly name of RADIUS server (Nom convivial de serveur RADIUS)	Tapez un nom qui identifie facilement le nom du serveur RADIUS quand il apparaît dans la liste de serveurs pour ce groupe.
Dans le champ : Hostname or IP address (Nom du serveur ou adresse IP)	Tapez le nom ou l'adresse IP du serveur RADIUS.
Dans le champ : Authentication port (Port d'authentification)	Tapez le port réseau sur le serveur RADIUS où LAN Enforcer envoie le paquet d'authentification du client. Le paramètre par défaut est UDP 1812.
Dans le champ : Shared secret (Secret partagé)	Saisissez le secret partagé qui est utilisé pour la communication chiffrée entre le serveur Radius et LAN Enforcer. Le secret partagé entre un serveur RADIUS et un LAN Enforcer peut être différent du secret partagé entre un commutateur compatible 802.1x et un LAN Enforcer. Le secret partagé distingue les majuscules et minuscules.
Dans le champ : Confirm shared secret (Confirmer le secret partagé)	Tapez le secret partagé de nouveau.

9 Dans la boîte de dialogue Add RADIUS Server (Ajouter un serveur RADIUS), cliquez sur **OK**.

Le nom, l'adresse IP et le port pour le serveur RADIUS que vous avez ajouté apparaissent maintenant dans la liste Groupe de serveurs RADIUS dans la boîte de dialogue Ajouter un groupe de serveurs RADIUS.

10 Dans la boîte de dialogue Add RADIUS Server Group (Ajouter un groupe de serveurs RADIUS), cliquez sur **OK**.

11 Dans la boîte de dialogue Paramètres de LAN Enforcer, cliquez sur **OK**.

Modifier le nom d'un groupe de serveurs RADIUS

Vous pouvez modifier le nom du groupe de serveurs RADIUS à tout moment si les circonstances changent.

Modifier le nom d'un groupe de serveurs RADIUS

1 Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).

2 Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).

3 Dans la page Admin, sous View Servers (Afficher les serveurs), sélectionnez le groupe Enfoncer dont LAN Enforcer est un membre.

4 Dans la page Admin, sous View Servers (Afficher les serveurs), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).

5 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Groupe de serveurs RADIUS, cliquez sur le groupe de serveurs RADIUS dont vous voulez modifier le nom.

6 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet RADIUS Server Group (Groupe de serveurs RADIUS), cliquez sur **Edit** (Modifier).

7 Dans la boîte de dialogue Add RADIUS Server (Ajouter un serveur RADIUS), modifiez le nom du groupe de serveurs RADIUS dans le champ Nom du groupe.

8 Dans la boîte de dialogue Add RADIUS Server (Ajouter un serveur RADIUS), cliquez sur **OK**.

9 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet RADIUS Server Group (Groupe de serveurs RADIUS), cliquez sur **OK**.

Modifier le nom convivial d'un serveur RADIUS

Vous pouvez modifier le nom convivial d'un serveur RADIUS à tout moment si les circonstances changent.

Pour modifier le nom convivial d'un serveur RADIUS

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin, sous View Servers (Afficher les serveurs), sélectionnez le groupe Enfoncer dont LAN Enforcer est un membre.
4. Dans la page Admin, sous View Servers (Afficher les serveurs), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet RADIUS Server Group (Groupe de serveurs RADIUS), cliquez sur le groupe de serveurs RADIUS qui inclut le serveur RADIUS dont vous voulez modifier le nom convivial.
6. Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet RADIUS Server Group (Groupe de serveurs RADIUS), cliquez sur **Edit** (Modifier).
7. Dans la boîte de dialogue Add a RADIUS Server (Ajouter un serveur RADIUS), modifiez le nom convivial du serveur RADIUS dans le champ Friendly name of RADIUS server (Nom convivial de serveur RADIUS).
8. Dans la boîte de dialogue Add RADIUS Server (Ajouter un serveur RADIUS), cliquez sur **OK**.
9. Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet RADIUS Server Group (Groupe de serveurs RADIUS), cliquez sur **OK**.

Modifier le nom d'hôte ou l'adresse IP d'un serveur RADIUS

Vous pouvez modifier le nom d'hôte ou l'adresse IP du serveur RADIUS à tout moment si les circonstances changent.

Pour modifier le nom d'hôte ou l'adresse IP d'un serveur RADIUS

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Dans la page Admin, sous View Servers (Afficher les serveurs), sélectionnez le groupe Enfoncer dont LAN Enforcer est un membre.
4. Dans la page Admin, sous View Servers (Afficher les serveurs), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).

5 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet RADIUS Server Group (Groupe de serveurs RADIUS), cliquez sur le groupe de serveurs RADIUS qui inclut le serveur RADIUS dont vous voulez modifier le nom d'hôte ou l'adresse IP.

6 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet RADIUS Server Group (Groupe de serveurs RADIUS), cliquez sur **Edit** (Modifier).

7 Dans la boîte de dialogue Add a RADIUS Server (Ajouter un serveur RADIUS), modifiez le nom d'hôte ou l'adresse IP du serveur RADIUS dans le champ Hostname (Nom d'hôte) ou IP Address (Adresse IP).

8 Dans la boîte de dialogue Add RADIUS Server (Ajouter un serveur RADIUS), cliquez sur **OK**.

9 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet RADIUS Server Group (Groupe de serveurs RADIUS), cliquez sur **OK**.

Modifier le numéro de port d'authentification d'un serveur RADIUS

Vous pouvez modifier le numéro de port d'authentification du serveur RADIUS à tout moment si les circonstances changent.

Pour modifier le numéro de port d'authentification d'un serveur RADIUS

1 Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).

2 Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).

3 Dans la page Admin, sous View Servers (Afficher les serveurs), sélectionnez le groupe Enfoncer dont LAN Enforcer est un membre.

4 Dans la page Admin, sous View Servers (Afficher les serveurs), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).

5 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet RADIUS Server Group (Groupe de serveurs RADIUS), cliquez sur le groupe de serveurs RADIUS qui inclut le serveur RADIUS dont vous voulez modifier le numéro de port d'authentification.

6 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet RADIUS Server Group (Groupe de serveurs RADIUS), cliquez sur **Edit** (Modifier).

7 Dans la boîte de dialogue Add a RADIUS Server (Ajouter un serveur RADIUS), modifiez le numéro de port d'authentification du serveur RADIUS dans le champ Port d'authentification.

8 Dans la boîte de dialogue Add RADIUS Server (Ajouter un serveur RADIUS), cliquez sur **OK**.

9 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet RADIUS Server Group (Groupe de serveurs RADIUS), cliquez sur **OK**.

Modifier le secret partagé d'un serveur RADIUS

Vous pouvez modifier le secret partagé du serveur RADIUS à tout moment si les circonstances changent.

Pour modifier le secret partagé d'un serveur RADIUS

1 Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).

Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).

2 Dans la page Admin, sous View Servers (Afficher les serveurs), sélectionnez le groupe Enfoncer dont LAN Enforcer est un membre.

3 Dans la page Admin, sous View Servers (Afficher les serveurs), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).

4 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet RADIUS Server Group (Groupe de serveurs RADIUS), cliquez sur le groupe de serveurs RADIUS qui inclut le serveur RADIUS dont vous voulez modifier le secret partagé.

5 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet RADIUS Server Group (Groupe de serveurs RADIUS), cliquez sur **Edit** (Modifier).

6 Dans la boîte de dialogue Ajouter un serveur RADIUS, modifiez le secret partagé du serveur RADIUS dans le champ Secret partagé.

Le secret partagé est utilisé pour la communication chiffrée entre le serveur RADIUS et le LAN Enforcer. Le secret partagé entre un serveur RADIUS et un LAN Enforcer peut être différent du secret partagé entre un commutateur compatible 802.1x et un LAN Enforcer. Le secret partagé distingue les majuscules et minuscules.

7 Dans la boîte de dialogue Ajouter un serveur RADIUS, modifiez le secret partagé du serveur RADIUS dans le champ de confirmation du secret partagé.

8 Dans la boîte de dialogue Add RADIUS Server (Ajouter un serveur RADIUS), cliquez sur **OK**.

9 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet RADIUS Server Group (Groupe de serveurs RADIUS), cliquez sur **OK**.

Supprimer le nom d'un groupe de serveurs RADIUS

Vous pouvez supprimer le nom du groupe de serveurs RADIUS à tout moment si les circonstances changent.

Pour supprimer le nom d'un groupe de serveurs RADIUS

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).

   Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
2. Dans la page Admin, sous View Servers (Afficher les serveurs), sélectionnez le groupe Enfoncer dont LAN Enforcer est un membre.
3. Dans la page Admin, sous View Servers (Afficher les serveurs), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
4. Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Groupe de serveurs RADIUS, cliquez sur le groupe de serveurs RADIUS dont vous voulez supprimer le nom.
5. Dans la boîte de dialogue Paramètres de LAN Enforcer, dans l'onglet Groupe de serveurs RADIUS, cliquez sur **Supprimer**.
6. Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet RADIUS Server Group (Groupe de serveurs RADIUS), cliquez sur **OK**.

Supprimer un serveur RADIUS

Vous pouvez supprimer un serveur RADIUS à tout moment si les circonstances changent.

Pour supprimer un serveur RADIUS

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).

   Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
2. Dans la page Admin, sous View Servers (Afficher les serveurs), sélectionnez le groupe Enfoncer dont LAN Enforcer est un membre.
3. Dans la page Admin, sous View Servers (Afficher les serveurs), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
4. Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet RADIUS Server Group (Groupe de serveurs RADIUS), cliquez sur le groupe de serveurs RADIUS dont le serveur RADIUS que vous voulez supprimer est un membre.

5 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet RADIUS Server Group (Groupe de serveurs RADIUS), cliquez sur **Edit** (Modifier).

6 Dans la boîte de dialogue Add RADIUS Server (Ajouter un serveur RADIUS), cliquez sur le serveur RADIUS que vous voulez supprimer.

7 Dans la boîte de dialogue Add RADIUS Server (Ajouter un serveur RADIUS), cliquez sur **Remove** (Supprimer).

8 Dans la boîte de dialogue Add RADIUS Server (Ajouter un serveur RADIUS), cliquez sur **OK**.

9 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet RADIUS Server Group (Groupe de serveurs RADIUS), cliquez sur **OK**.

Utiliser les paramètres de commutateur

Vous configurez une politique de commutateur quand vous spécifiez des paramètres de LAN Enforcer pour des commutateurs. Une politique de commutateur est un ensemble de paramètres appliqués à un groupe de commutateurs du même fabricant ou modèle. La seule information que vous devez entrer séparément pour différents commutateurs est l'adresse IP du commutateur.

Utiliser les paramètres de commutateur

Vous devez spécifier les données de base suivantes pour que les boîtiers LAN Enforcer, les serveurs de gestion, les clients et commutateurs compatibles 802.1x fonctionnent ensemble :

- Un nom de votre choix pour la politique de commutateur
- Le constructeur et modèle de commutateur
  Sélectionnez le modèle de commutateur à partir d'une liste de commutateurs pris en charge.
- Mot de passe chiffré ou secret partagé
- Le groupe de serveurs RADIUS utilisé
- Le délai de réauthentification pour le commutateur compatible 802.1x
  Le paramètre par défaut est 30 secondes.
- Si le commutateur transfère d'autres protocoles en plus d'EAP
  Le paramètre par défaut est de transférer d'autres protocoles.

Se reporter à "Ajouter une politique de commutateur de 802.1x pour un boîtier LAN Enforcer avec un assistant" à la page 184.

Se reporter à "Modifier les informations de base de la politique de commutateur et les commutateurs compatibles 802.1x" à la page 193.

Vous devez spécifier l'ensemble des commutateurs compatibles 802.1x auxquels la politique de commutateur s'applique comme suit :

- Un nom de commutateur convivial de votre choix
- Une adresse IP, un intervalle IP ou un sous-réseau

Se reporter à "Ajouter une politique de commutateur de 802.1x pour un boîtier LAN Enforcer avec un assistant" à la page 184.

Se reporter à "Modifier les informations sur le commutateur compatible 802.1x" à la page 200.

Vous devez spécifier les informations VLAN suivantes :

- ID de VLAN
- Nom de VLAN
- En option, vous pouvez spécifier les attributs RADIUS personnalisés au format hexadécimal.

Se reporter à "Ajouter une politique de commutateur de 802.1x pour un boîtier LAN Enforcer avec un assistant" à la page 184.

Se reporter à "Modifier les informations de VLAN pour la politique de commutateur" à la page 202.

Si un commutateur 802.1x prend en charge la commutation dynamique de VLAN, vous pouvez spécifier que le client doit se connecter à un VLAN spécifique.

Vous devez spécifier les actions que le commutateur compatible 802.1x doit effectuer quand certains critères sont remplis :

- Résultat d'authentification de l'hôte : Passer, Echouer, Indisponible ou Ignorer les résultats
- Résultat d'authentification utilisateur : Passer, Echouer, Indisponible ou Ignorer les résultats
- Résultat de vérification de politique : Pass, Fail, Unavailable, or Ignore Result (Réussie, Echec, Indisponible ou Ignorer les résultats)

Se reporter à "Ajouter une politique de commutateur de 802.1x pour un boîtier LAN Enforcer avec un assistant" à la page 184.

A propos de la prise en charge des attributs de modèles de commutateur

Lorsque vous configurez un boîtier LAN Enforcer, vous spécifiez le modèle du commutateur compatible 802.1x. Les différents commutateurs compatibles 802.1x recherchent différents attributs pour déterminer quel client peut accéder au VLAN. Certains commutateurs identifient des VLAN par l'ID de VLAN et d'autres par le nom de VLAN. Certains périphériques ont une prise en charge de VLAN limitée ou nulle.

Le boîtier LAN Enforcer transfère des attributs du serveur RADIUS au commutateur. Au besoin, cependant, il modifie ou ajoute l'attribut VLAN en fonction du type de commutateur en utilisant des valeurs prises en charge. Si un conflit existe entre les informations d'attribut spécifiques au fabricant envoyées par le serveur RADIUS et les informations d'attribut de VLAN spécifiques au fabricant utilisées par LAN Enforcer, LAN Enforcer supprime les informations spécifiques au fabricant envoyées par le serveur RADIUS. LAN Enforcer remplace alors ces informations par les informations qui apparaissent dans le tableau suivant.

Si vous voulez garder les attributs du serveur RADIUS, vous pouvez sélectionner l'action appelée Port d'ouverture. Avec cette action, LAN Enforcer transfère tous les attributs du serveur RADIUS au commutateur compatible 802.1x sans aucune modification.

Le modèle de commutateur compatible 802.1x peut utiliser l'ID de VLAN ou le nom de VLAN pour exécuter des affectations de VLAN dynamique. Vous devez spécifier l'ID de VLAN et le nom de VLAN quand vous fournissez des informations de VLAN pour LAN Enforcer, excepté le commutateur Aruba.

Tableau 8-1 décrit les modèles et les attributs de commutateur compatible 802.1x.

Tableau 8-1 Prise en charge des attributs des modèles de commutateur

Modèle de commutateur	Attributs ajoutés par LAN Enforcer	Commentaires
Contrôleur Airespace Wireless	Le code de fabricant est 14179. Le numéro d'attribut assigné par le fabricant est 5. Le format d'attribut est "chaîne".	Le nom de VLAN est utilisé. Le nom est sensible à la casse.

Modèle de commutateur	Attributs ajoutés par LAN Enforcer	Commentaires
Alcatel	Vendor Specific (#26) (spécifique au fabricant) L'ID de fabricant d'Alcatel est 800. Tous les attributs "Vendor specific" (spécifiques au fabricant) de RADIUS ayant un ID de 800 sont supprimés en cas de conflit.	L'ID de VLAN est utilisé.
Aruba	Vendor Specific (#14823) Vendor ID est 14823 pour Aruba. L'attribut Aruba-User-Role permet d'installer des ID de VLAN ou des noms de VLAN.	Le nom de VLAN et l'ID de VLAN peuvent être utilisés tous les deux. Alternativement, vous pouvez utiliser seulement un nom de VLAN ou seulement un ID de VLAN Un ID de VLAN valide s'étend de 1 à 4094. Un nom de VLAN ne peut pas dépasser 64 octets.
Série Cisco Aironet	Dépend de l'utilisation ou non du contrôle d'accès SSID. Attributs utilisateur RADIUS utilisés pour l'affectation de VLAN-ID : IETF 64 (Tunnel Type) : Définissez cet attribut sur "VLAN" IETF 65 (Tunnel Medium Type): Définissez cet attribut sur "802" IETF 81 (Tunnel Private Group ID): Définissez cet attribut sur VLAN-ID Attribut utilisateur RADIUS utilisé pour le contrôle d'accès SSID : Cisco IOS/PIX RADIUS Attribute, 009\001 cisco-av-pair	L'ID de VLAN est utilisé.

Modèle de commutateur	Attributs ajoutés par LAN Enforcer	Commentaires
Série Cisco Catalyst	Tunnel Type (#64) (type de tunnel) Tunnel Medium Type (#65) (type de support de tunnel) Tunnel Private Group ID (#81) (ID de groupe privé de tunnel) Tunnel Type (type de tunnel) est défini sur 13 (VLAN) Tunnel Medium Type (type de support de tunnel) est défini sur 6 (support 802) Tunnel Private Group ID est définie sur Nom de VLAN. Tous les attributs avec ces 3 types de serveur RADIUS sont supprimés en cas de conflit. En outre, tous les attributs avec le type "Vendor specific" et l'ID de fabricant 9 (Cisco) sont également supprimés.	Le nom de VLAN est utilisé. Le nom est sensible à la casse.
Foundry, HP, Nortel,	Tunnel Type (#64) (type de tunnel) Tunnel Medium Type (#65) (type de support de tunnel) Tunnel Private Group ID (#81) (ID de groupe privé de tunnel) Tunnel Type (type de tunnel) est défini sur 13 (VLAN) Tunnel Medium Type (type de support de tunnel) est défini sur 6 (support 802) Tunnel Private Group ID est définie sur ID de VLAN. Tous les attributs avec ces 3 types de serveur RADIUS sont supprimés en cas de conflit.	L'ID de VLAN est utilisé.

Modèle de commutateur	Attributs ajoutés par LAN Enforcer	Commentaires

Enterasys	Filter ID (#11)
	Filter ID est défini sur
	`Enterasys :`
	`version=1 :`
	`mgmt=su :`
	`policy=NAME`
	Tous les attributs "Filter ID" (ID de filtre) du serveur RADIUS sont supprimés en cas de conflit.
		Le nom de VLAN est utilisé et représente l'attribut "Role name" (nom de rôle) dans le commutateur Enterasys. Le nom distingue les majuscules et minuscules.

Extreme	Vendor Specific (#26) (spécifique au fabricant) Vendor ID est 1916 pour Extreme. VLAN Name est ajouté après l'ID de fabricant. Tous les attributs spécifiques au fabricant du serveur RADIUS ayant un ID de 1916 sont supprimés en cas de conflit.	Le nom de VLAN est utilisé. Le nom distingue les majuscules et minuscules.

Ajouter une politique de commutateur de 802.1x pour un boîtier LAN Enforcer avec un assistant

Vous pouvez ajouter les commutateurs compatibles 802.1x multiples pour utiliser avec un boîtier LAN Enforcer en tant qu'élément d'une politique de commutateur. Vous devez entrer les informations nécessaires pour configurer l'interaction du boîtier LAN Enforcer avec le commutateur.

Pour ajouter une politique de commutateur 802.1x pour un boîtier LAN Enforcer à l'aide d'un assistant

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).

   Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).

2. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez le groupe Enforcer.

3. Dans la page Admin, sous View Servers (Afficher les serveurs), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
4. Dans la boîte de dialogue Paramètres de LAN Enforcer, dans l'onglet Commutateur, cliquez sur **Add** (Ajouter).
5. Dans le panneau Welcome to the Switch Policy Configuration Wizard (Bienvenue dans l'Assistant de configuration d'une politique de commutateur) de l'Assistant de configuration d'une politique de commutateur, cliquez sur **Next** (Suivant).
6. Dans le panneau Basic Information (Informations de base) de l'Assistant de configuration d'une politique de commutateur, effectuez les tâches suivantes :

Switch policy name (Nom de politique de commutateur)	Tapez un nom de votre choix pour identifier la politique de commutateur. Par exemple, vous pouvez utiliser le nom et le modèle de constructeur comme nom pour le nom de politique de commutateur.

Switch model (Modèle de commutateur)	LAN Enforcer utilise le modèle de commutateur pour déterminer l'attribut de serveur RADIUS spécifique au fabricant. Sélectionnez le modèle compatible 802.1x dans la liste des commutateurs pris en charge : ■ Other (Autre) Si votre modèle n'est pas listé, sélectionnez **Other** (Autre) pour utiliser un attribut de serveur RADIUS générique. ■ 3Com ■ Alcatel switch ■ Cisco Catalyst Series ■ Enterasys Matix Series ■ Extreme Summit Series ■ Foundry Networks ■ HP Procurve Series ■ Nortel BayStack Series ■ Cisco Aironet Series ■ Aruba Switches ■ Airespace Wireless Controller ■ Nortel Wireless ■ Enterasys wireless controller ■ Commutateur HuaWei **Remarque :** Si l'administrateur choisit le mode transparent sur le commutateur, il doit configurer la politique pour utiliser le mode transparent sur le client, plutôt que de permettre à l'utilisateur de sélectionner.
Mot de passe chiffré ou Secret partagé	Le secret partagé utilisé pour la communication entre le commutateur compatible 802.1x et LAN Enforcer. Le mot de passe chiffré ou le secret partagé distingue les majuscules et minuscules.
Confirmez le mot de passe chiffré ou le secret partagé	Vous devez taper le mot de passe chiffré ou le secret partagé de nouveau.
Groupe de serveurs RADIUS	Si vous utilisez le boîtier LAN Enforcer avec un serveur RADIUS, vous devez sélectionner le groupe de serveurs RADIUS dans la liste de groupes de serveurs RADIUS disponibles.

Période de réauthentification (secondes)	Tapez le délai en secondes dans lequel le client doit être authentifié à nouveau. Autrement le client est supprimé de la liste de clients connectés sur le LAN Enforcer. Vous devez définir la période de réauthentification pour être au moins le double du délai de réauthentification sur le commutateur. Par exemple, si l'intervalle de réauthentication sur le commutateur est de 30 secondes, la période de réauthentication du boîtier LAN Enforcer devrait être d'au moins 60 secondes. Autrement, le boitier LAN Enforcer suppose que le client est expiré. Par conséquent le client ne libère pas et ne renouvelle pas son adresse IP. Le paramètre par défaut est 30 secondes.
Protocoles de retransmission autres que EAP	Vous pouvez sélectionner pour permettre au boîtier LAN Enforcer de transférer les paquets RADIUS contenant des protocoles d'authentification autres que EAP. Les autres protocoles incluent Challenge Handshake Authentification Protocole (CHAP) et PAP. Le paramètre par défaut est activé.

7 Dans le panneau Basic Information (Informations de base) de l'Assistant de configuration d'une politique de commutateur, cliquez sur **Next** (Suivant).

8 Dans le panneau Switch List (Liste de commutateurs) de l'Assistant de configuration d'une politique de commutateur, cliquez sur **Add** (Ajouter).

9 Dans le panneau Switch List (Liste de commutateurs) de l'Assistant de configuration de politique de commutateur, effectuez les tâches suivantes :

Name (Nom)	Dans la boîte de dialogue Add Single Internal IP (Ajouter une adresse IP interne unique), tapez un nom convivial pour que la politique de commutateur identifie le commutateur compatible 802.1x dans le champ Nom.
Single IP Address (Adresse IP unique)	Dans la boîte de dialogue Add Single Internal IP (Ajouter une adresse IP interne unique), cliquez sur **Single IP address** (Adresse IP unique). Tapez alors l'adresse IP du commutateur compatible 802.1x dans le champ Adresse IP.
IP Address Range (Plage d'adresses IP)	Dans la boîte de dialogue Add Internal IP Address Range (Ajouter une plage d'adresses IP internes), cliquez sur **IP Address Range** (Plage d'adresses IP). Tapez l'adresse IP de début pour le commutateur compatible 802.1x dans le champ Starting IP Adress (Adresse IP de début). Tapez l'adresse IP de fin de la plage IP pour le commutateur compatible 802.1x dans le champ End IP (Adresse IP de fin).
Sous-réseau	Dans la boîte de dialogue Add Internal IP Address Subnet (Ajouter un sous-réseau d'adresses IP internes), cliquez sur **Subnet** (Sous-réseau). Tapez l'adresse IP pour le sous-réseau dans le champ d'adresse IP et le sous-réseau dans le champ de masque de sous-réseau.

Lorsque vous spécifiez une politique de commutateur pour un boîtier LAN Enforcer, vous pouvez associer la politique de commutateur à un ou plusieurs commutateurs compatibles 802.1x.

10 Dans la boîte de dialogue Add Internal IP address (Ajouter une adresse IP interne), cliquez sur **OK**..

11 Dans le panneau Switch List (Liste de commutateurs) de l'Assistant de configuration d'une politique de commutateur, cliquez sur **Next** (Suivant).

12 Dans le panneau Switch VLAN Configuration (Configuration VLAN du commutateur) de l'Assistant de configuration d'une politique de commutateur, cliquez sur **Add** (Ajouter).

13 Dans la boîte de dialogue Add VLAN (Ajouter un VLAN), effectuez les tâches suivantes :

VLAN ID (ID de VLAN)	Tapez un entier compris entre 1 et 4 094 dans le champ VLAN ID (ID de VLAN). L'ID de VLAN doit être identique à celui qui est configuré sur le commutateur compatible 802.1x excepté le commutateur Aruba. Si vous prévoyez d'ajouter des données de VLAN concernant un commutateur Aruba, vous pouvez configurer les informations de VLAN et de rôle autrement que pour d'autres commutateurs 802.1x. Se reporter à "Configurer les informations de VLAN et de rôle sur le commutateur Aruba compatible 802.1x" à la page 204.
VLAN Name (Nom de VLAN)	Tapez un nom de VLAN. Le nom pour VLAN peut faire jusqu'à 64 caractères. Il distingue les majuscules et minuscules. Le nom de VLAN doit être identique à celui qui est configuré sur le commutateur compatible 802.1x excepté le commutateur Aruba. Si vous prévoyez d'ajouter des informations de VLAN sur un commutateur Aruba, vous pouvez configurer les informations de VLAN et de rôle autres que celles des autres commutateurs 802.1x. Se reporter à "Configurer les informations de VLAN et de rôle sur le commutateur Aruba compatible 802.1x" à la page 204.
Send customized RADIUS attributes to switch (Envoyer les attributs RADIUS personnalisés au commutateur)	Cochez **Send customized RADIUS attributes to switch** (Envoyer les attributs RADIUS personnalisés au commutateur) si vous voulez que LAN Enforcer envoie un attribut RADIUS personnalisé au commutateur compatible 802.1x. Un attribut peut être une liste de contrôle d'accès (ACL). Se reporter à "A propos de la prise en charge des attributs de modèles de commutateur" à la page 181.
Customized attributes in hex format (Attributs personnalisés au format hexadécimal)	Tapez l'attribut RADIUS au format hexa. La longueur doit être paire.

Lorsque vous spécifiez une politique de commutateur pour LAN Enforcer, vous utilisez l'onglet VLAN pour ajouter les informations de VLAN pour chaque VLAN configuré sur le commutateur. Vous voulez que la politique de commutateur soit disponible à l'usage de LAN Enforcer en tant qu'action. Il est recommandé de spécifier au moins un VLAN de correction.

14 Dans la boîte de dialogue Add VLAN (Ajouter un VLAN), cliquez sur **OK**.

15 Dans le volet Switch VLAN Configuration (Configuration VLAN du commutateur) de l'Assistant de configuration d'une politique de commutateur, cliquez sur **Next** (Suivant).

16 Dans le volet Switch Action Configuration (Configuration d'action de commutateur) de l'Assistant de configuration d'une politique de commutateur, cliquez sur **Add** (Ajouter).

17 Dans la boîte de dialogue Add Switch Action (Ajouter une action de commutateur), effectuez les tâches suivantes :

Host Authentication (Authentification d'hôte)	Cliquez sur l'une des conditions suivantes : ■ Passed (Réussie) ■ Failed (Echec) ■ Unavailable (Indisponible) ■ Ignore Result (Ignorer le résultat) Une situation typique dans laquelle une vérification de l'intégrité de l'hôte devient indisponible serait le résultat d'un client ne s'exécutant pas. Si vous définissez l'authentification de l'hôte sur Unavailable (Indisponible), vous devez également définir le contrôle de la politique sur Indisponible.

User Authentication (Authentification d'utilisateur)	Cliquez sur l'une des conditions suivantes : ■ Passed (Réussie) Le client a réussi l'authentification utilisateur. ■ Failed (Echec) Le client n'a pas réussi l'authentification utilisateur. ■ Unavailable (Indisponible) Le résultat d'authentification utilisateur est toujours indisponible si l'authentification utilisateur n'est pas exécutée en mode transparent. Si vous utilisez LAN Enforcer en mode transparent, vous devez créer une action pour l'état Indisponible. Si vous utilisez la configuration de base, vous pouvez également configurer une action pour l'authentification utilisateur comme état d'erreur. Par exemple, si un supplicant 802.1x utilise une méthode d'authentification d'utilisateur incorrecte ou si le serveur RADIUS échoue au milieu de la transaction d'authentification. L'état indisponible de l'authentification utilisateur peut également se produire sur quelques serveurs RADIUS si le nom d'utilisateur n'existe pas dans la base de données RADIUS. Par exemple, ce problème peut se poser avec Microsoft IAS. Par conséquent vous pouvez vouloir tester l'état d'un nom d'utilisateur manquant avec votre serveur RADIUS. Vous pouvez vouloir consulter s'il correspond aux états d'authentification utilisateur Failed (Echec) ou Unavailable (Indisponible). ■ Ignore Result (Ignorer le résultat) Une situation typique dans laquelle une vérification de l'intégrité de l'hôte devient indisponible serait le résultat d'un client ne s'exécutant pas. Si vous définissez le contrôle de politique sur Indisponible, vous devez également définir l'authentification de l'hôte sur Indisponible.

Policy Check (Contrôle de politique)	Cliquez sur l'une des conditions suivantes : ■ Passed (Réussi) Le client a réussi le contrôle de politique. ■ Failed (Echec) Le client n'a pas réussi le contrôle de politique. ■ Unavailable (Indisponible) Le résultat Indisponible pour la politique peut se produire dans les conditions suivantes : ■ Si le client a un identifiant non valide, LAN Enforcer ne peut obtenir aucune donnée de politique depuis le serveur de gestion. Ce problème peut se poser si le serveur de gestion qui a déployé la politique client n'est plus disponible. ■ Si le client est d'abord exporté et installé avant qu'il se connecte au serveur de gestion et reçoive sa politique. ■ Ignore Result (Ignorer le résultat)
Action	Vous pouvez sélectionner les actions suivantes que le commutateur compatible 802.1x effectue quand les conditions sont remplies : ■ Port d'ouverture Le commutateur compatible 802.1x permet l'accès au réseau sur VLAN par défaut auquel le port est normalement attribué. Il permet également l'accès réseau sur le VLAN spécifié dans un attribut envoyé depuis le serveur RADIUS. Par conséquent la prise en charge des utilisateurs ayant un accès VLAN est basée sur le rôle et l'ID de l'utilisateur. L'action par défaut est port d'ouverture. ■ Commutateur au *test* VLAN Permet l'accès au VLAN spécifié. Les VLAN disponibles à la sélection sont ceux configurés précédemment. ■ Close Port (Fermer port) Refuse l'accès au réseau sur le VLAN par défaut ou le VLAN spécifié par RADIUS. Sur quelques modèles de commutateur, selon la configuration de commutateur, le port est attribué à un invité VLAN. Pour le commutateur Aruba, vous pouvez restreindre l'accès selon un rôle spécifié aussi bien qu'un VLAN spécifié. Les restrictions dépendent de la façon dont vous avez configuré les informations de VLAN pour la politique de commutateur.

18 Dans la boîte de dialogue Add Switch Action (Ajouter une action de commutateur), cliquez sur **OK**.

19 Dans le panneau Switch Action Configuration (Configuration d'action de commutateur) de l'Assistant de configuration d'une politique de commutateur, dans le tableau Switch Action (Action du commutateur), cliquez sur la politique d'action de commutateur dont vous voulez modifier la priorité.

LAN Enforcer vérifie les résultats d'authentification par rapport aux entrées dans le tableau d'action de commutateur du haut du tableau vers le tableau. Après avoir trouvé un ensemble de conditions correspondant, il demande au commutateur compatible 802.1x d'appliquer cette action. Vous pouvez modifier l'ordre dans lequel des actions sont appliquées en modifiant l'ordre dans lequel elles sont listées dans le tableau.

20 Dans le panneau Switch Action Configuration (Configuration d'action de commutateur) de l'Assistant de configuration d'une politique de commutateur, cliquez sur **Move Up** (Vers le haut) ou **Move Down** (Vers le bas).

21 Dans le panneau Switch Action Configuration (Configuration de l'action du commutateur) de l'Assistant de configuration d'une politique de commutateur, cliquez sur **Next** (Suivant).

22 Dans le panneau Complete the Switch Policy Configuration (Terminer la configuration d'une politique de commutateur) de l'Assistant de configuration d'une politique de commutateur, cliquez sur **Finish** (Terminer).

Modifier les informations de base de la politique de commutateur et les commutateurs compatibles 802.1x

Vous pouvez modifier les paramètres suivants de la politique de commutateur et du commutateur compatibles 802.1x :

- Nom de politique de commutateur
  Se reporter à "Modifier le nom d'une politique de commutateur" à la page 194.
- Modèle de commutateur
  Se reporter à "Sélectionner un modèle de commutateur différent pour la politique de commutateur" à la page 195.
- Secret partagé
  Se reporter à "Modifier un mot de passe chiffré ou un secret partagé" à la page 196.
- Groupe de serveurs RADIUS
  Se reporter à "Sélectionner un groupe de serveurs RADIUS différent" à la page 197.

- Période de réauthentification
  Se reporter à "Modifier la période de réauthentification" à la page 198.
- Protocoles de retransmission autres que EAP
  Se reporter à "Activer des protocoles autres que EAP" à la page 199.

Modifier le nom d'une politique de commutateur

Vous pouvez modifier le nom de la politique de commutateur à tout moment si les circonstances changent.

Pour modifier le nom d'une politique de commutateur

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).

   Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
2. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez le groupe Enforcer.
3. Dans la page Admin, sous View Servers (Afficher les serveurs), sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
4. Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur) du tableau Switch Policy (Politique de commutateur), cliquez sur la politique de commutateur que vous voulez modifier.
5. Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur) du tableau Switch Policy (Politique de commutateur), cliquez sur **Edit** (Modifier).
6. Dans la boîte de dialogue Edit Switch Policy (Modifier la politique de commutateur) recherchez l'option *name of switch policy* (nom de la politique de commutateur), dans l'onglet Basic Information (Informations de base), modifiez le nom de la politique dans le champ Switch policy (Politique de commutateur).
7. Dans la boîte de dialogue Edit Switch Policy (Modifier la politique de commutateur) recherchez l'option *name of switch policy* (nom de la politique de commutateur), dans l'onglet Basic Information (Informations de base), cliquez sur **OK**.
8. Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur), cliquez sur **OK**.

Sélectionner un modèle de commutateur différent pour la politique de commutateur

Vous pouvez sélectionner un modèle de commutateur différent pour la politique de commutateur à tout moment si les circonstances évoluent.

Pour sélectionner un modèle de commutateur différent pour la politique de commutateur

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).

   Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).

2. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez le groupe Enforcer.

3. Dans la page Admin, sous View Servers (Afficher les serveurs), sous Tâches, cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).

4. Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur) du tableau Switch Policy (Politique de commutateur), cliquez sur la politique de commutateur dont vous voulez modifier le mode de commutation.

5. Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur) du tableau Switch Policy (Politique de commutateur), cliquez sur **Edit** (Modifier).

6. Dans la boîte de dialogue Edit Switch Policy (Modifier la politique de commutateur) pour *nom de la politique de commutateur*, dans l'onglet Basic Information (Informations de base), sélectionnez un modèle de commutateur différent à partir de la liste suivante de modèles de commutateur :

   - Other (Autres)
     Si votre modèle n'est pas listé, sélectionnez **Other** (Autres) pour utiliser un attribut de serveur RADIUS générique.
   - 3Com
   - Alcatel switch
   - Cisco Catalyst Series
   - Enterasys Matix Series
   - Extreme Summit Series
   - Foundry Networks
   - HP Procurve Series
   - Nortel BayStack Series

- Cisco Aironet Series
- Aruba Switches
- Airespace Wireless Controller
- Nortel Wireless
- Enterasys wireless controller
- Commutateur de HuaWei
  Si l'administrateur choisit le mode transparent sur le commutateur de HuaWei, il doit configurer la politique pour utiliser le modeon transparent sur le client, plutôt que de laisser choisir l'utilisateur.

7 Dans la boîte de dialogue Edit Switch Policy (Modifier la politique de commutateur) recherchez l'option *name of switch policy* (nom de la politique de commutateur), dans l'onglet Basic Information (Informations de base), cliquez sur **OK**.

8 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur), cliquez sur **OK**.

Modifier un mot de passe chiffré ou un secret partagé

Vous pouvez modifier le secret partagé à tout moment si les circonstances changent.

Pour modifier un mot de passe chiffré ou un secret partagé

1 Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).

Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).

2 Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez le groupe Enforcer.

3 Dans la page Admin, sous View Servers (Afficher les serveurs), sous Tâches, cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).

4 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur) du tableau Switch Policy (Politique de commutateur), cliquez sur la politique de commutateur dont vous voulez modifier le secret partagé.

5 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur) du tableau Switch Policy (Politique de commutateur), cliquez sur **Edit** (Modifier).

6 Dans la boîte de dialogue Edit Switch Policy (Modifier la politique de commutateur) pour *nom de la politique de commutateur*, dans l'onglet Basic Information (Informations de base), modifiez le nom du secret partagé dans le champ Shared secret (Secret partagé).

7 Dans la boîte de dialogue Edit Switch Policy (Modifier la politique de commutateur) pour *nom de la politique de commutateur*, dans l'onglet Basic Information (Informations de base), modifiez le nom du secret partagé dans le champ Confirm shared secret (Confirmer le secret partagé).

8 Dans la boîte de dialogue Edit Switch Policy (Modifier la politique de commutateur) recherchez l'option *name of switch policy* (nom de la politique de commutateur), dans l'onglet Basic Information (Informations de base), cliquez sur **OK**.

9 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur), cliquez sur **OK**.

Sélectionner un groupe de serveurs RADIUS différent

Vous pouvez sélectionner un groupe de serveurs RADIUS différent à tout moment si les circonstances changent.

Pour sélectionner un groupe de serveurs RADIUS différent

1 Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).

Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).

2 Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez le groupe Enforcer.

3 Dans la page Admin, sous View Servers (Afficher les serveurs), sous Tâches, cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).

4 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur) du tableau Switch Policy (Politique de commutateur), cliquez sur la politique de commutateur dont vous voulez modifier le secret partagé.

5 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur) du tableau Switch Policy (Politique de commutateur), cliquez sur **Edit** (Modifier).

6 Dans la boîte de dialogue Edit Switch Policy (Modifier la politique de commutateur) pour *le nom de la politique de commutateur*, dans l'onglet Basic Information (Informations de base), sélectionnez un groupe de serveurs RADIUS différent dans la liste RADIUS server group (Groupe de serveurs RADIUS).

   Vous devez avoir ajouté plusieurs groupes de serveurs RADIUS avant de pouvoir sélectionner un groupe de serveurs RADIUS différent.

7 Dans la boîte de dialogue Edit Switch Policy (Modifier la politique de commutateur) recherchez l'option *name of switch policy* (nom de la politique de commutateur), dans l'onglet Basic Information (Informations de base), cliquez sur **OK**.

8 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur), cliquez sur **OK**.

Modifier la période de réauthentification

Vous pouvez modifier la période de réauthentification à tout moment si les circonstances changent.

Vous devez spécifier le laps de temps en secondes durant lesquelles le client doit être authentifié à nouveau. Autrement le client est supprimé de la liste des clients connectés et déconnecté du réseau.

Vous devez définir la période de réauthentification pour être au moins le double du délai de réauthentification sur le commutateur.

Par exemple, si l'intervalle de réauthentification sur le commutateur est 30 secondes, la période de réauthentification de LAN Enforcer devrait être au moins de 60 secondes. Autrement LAN Enforcer suppose que le client est expiré. Par conséquent le client ne libère pas et ne renouvelle pas son adresse IP.

Le paramètre par défaut est 30 secondes.

Pour modifier la période de réauthentification

1 Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).

   Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).

2 Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez le groupe Enforcer.

3 Cliquez sur **Edit Group Properties** (Modifier les propriétés de groupe).

4 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur) du tableau Switch Policy (Politique de commutateur), cliquez sur la politique de commutateur que vous voulez modifier.

5 Dans l'onglet Switch (Commutateur) du tableau Switch Policy (Commutateur de politique), cliquez sur **Edit** (Modifier).

6 Dans la boîte de dialogue Edit Switch Policy (Modifier la politique de commutateur) pour *le nom de la politique de commutateur*, dans l'onglet Basic Information (Informations de base), modifiez la période de réauthentification dans le champ Reauthentication period (Période de réauthentification) en secondes.

7 Cliquez sur **OK**.

8 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur), cliquez sur **OK**.

Activer des protocoles autres que EAP

Vous pouvez sélectionner pour permettre à LAN Enforcer de transférer les paquets RADIUS qui contiennent d'autres protocoles d'authentification autres que EAP.

Les autres protocoles incluent :

- Challenge Handshake Authentication Protocol (CHAP)
- PAP

Le paramètre par défaut est activé.

Pour activer des protocoles autres que EAP

1 Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).

Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).

2 Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez le groupe Enforcer.

3 Cliquez sur **Edit Group Properties** (Modifier les propriétés de groupe).

4 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur) du tableau Switch Policy (Politique de commutateur), cliquez sur la politique de commutateur que vous voulez modifier.

5 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur) du tableau Switch Policy (Politique de commutateur), cliquez sur **Edit** (Modifier).

6 Dans la boîte de dialogue Edit Switch Policy (Modifier la politique de commutateur) pour *le nom de politique de commutateur*, dans l'onglet Basic Information (Informations de base), sélectionnez **Enable protocols besides EAP** (Activer les protocoles autres que EAP).

Vous pouvez faire transférer les protocoles suivants :

- Challenge Handshake Authentication Protocol (CHAP)
- PAP

7 Cliquez sur **OK**.

8 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur), cliquez sur **OK**.

Modifier les informations sur le commutateur compatible 802.1x

Vous pouvez modifier les paramètres suivants sur le commutateur compatible 802.1x :

- modifier l'adresse IP, le nom d'hôte ou le sous-réseau d'un commutateur compatible 802.1x ;
  Se reporter à "Modifier l'adresse IP, le nom d'hôte ou le sous-réseau d'un commutateur compatible 802.1x" à la page 200.
- supprimer un commutateur compatible 802.1x de la liste de commutateur.
  Se reporter à "Supprimer un commutateur compatible 802.1x de la liste de commutateur" à la page 201.

Modifier l'adresse IP, le nom d'hôte ou le sous-réseau d'un commutateur compatible 802.1x

Vous pouvez modifier l'adresse IP, le nom d'hôte ou le sous-réseau d'un commutateur compatible 802.1x à tout moment si les circonstances le requièrent.

Pour modifier l'adresse IP, le nom d'hôte et le sous-réseau d'un commutateur compatible 802.1x

1 Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).

  Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).

2 Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez le groupe Enforcer.

3 Sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés de groupe).

4 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur) du tableau Switch Policy (Politique de commutateur), cliquez sur la politique de commutateur que vous voulez modifier.

5 Cliquez sur **Edit** (Modifier).

6 Dans la boîte de dialogue Edit Switch Policy (Modifier la politique de commutateur) pour *nom de la politique de commutateur*, dans l'onglet Switch Address (Adresse du commutateur), sélectionnez **Edit All** (Modifier tout).

7 Dans la boîte de dialogue Modifier les adresses IP, ajoutez ou modifiez les adresses IP, l'hôte, noms ou les sous-réseaux pour le commutateur compatible 802.1x.

Le format de texte est comme suit :

Adresse IP unique	*nom*: *adresse*
Plage d'IP	*nom*: *adresse de démarrage - adresse de fin*
Sous-réseau	*nom*: *adresse de démarrage/masque de sous-réseau*

8 Dans la boîte de dialogue Edit Switch Policy (Modifier la politique de commutateur) pour *nom de la politique de commutateur*, dans l'onglet Switch Address (Adresse du commutateur), cliquez sur **OK**.

9 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur), cliquez sur **OK**.

Supprimer un commutateur compatible 802.1x de la liste de commutateur

Vous pouvez supprimer un commutateur compatible 802.1x de la liste de commutateur à tout moment si les circonstances la requièrent.

Pour supprimer un commutateur compatible 802.1x

1 Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).

Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).

2 Sous View Servers (Afficher les serveurs), sélectionnez le groupe Enforcer.

3 Sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés de groupe).

4 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur) du tableau Switch Policy (Politique de commutateur), cliquez sur le commutateur compatible 802.1x que vous voulez supprimer de la liste de commutateur.

5 Dans la boîte de dialogue settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur), cliquez sur **Remove** (Supprimer).

6 Cliquez sur **OK**.

Modifier les informations de VLAN pour la politique de commutateur

Vous pouvez modifier les paramètres suivants au sujet des VLAN sur le commutateur compatible 802.1x :

- Modifier l'ID de VLAN et le nom de VLAN d'un commutateur compatible 802.1x
  Se reporter à "Modifier l'ID de VLAN et le nom de VLAN d'un commutateur compatible 802.1x" à la page 202.
- Configurer les informations de VLAN et de rôle sur le commutateur Aruba compatible 802.1x
  Se reporter à "Configurer les informations de VLAN et de rôle sur le commutateur Aruba compatible 802.1x" à la page 204.
- Supprimer des VLAN sur un commutateur compatible 802.1x
  Se reporter à "Supprimer les VLAN sur un commutateur compatible 802.1x" à la page 203.

Modifier l'ID de VLAN et le nom de VLAN d'un commutateur compatible 802.1x

Vous pouvez modifier l'ID de VLAN et le nom de VLAN d'un commutateur compatible 802.1x à tout moment si les circonstances le requièrent.

Certains commutateurs, tels que le commutateur Cisco, ont une fonction d'invité VLAN. Le VLAN invité est normalement utilisé si l'authentification d'utilisateur EAP échoue. Si l'authentification EAP échoue, le commutateur connecte le client au VLAN invité automatiquement.

Si vous utilisez LAN Enforcer pour la commutation VLAN, il est recommandé de ne pas utiliser l'invité VLAN réservé en installant des VLAN et des actions sur LAN Enforcer. Autrement le supplicant 802.1x peut réagir comme si l'authentification EAP a échoué.

En installant les VLAN, assurez-vous que tous peuvent communiquer avec le serveur de gestion.

Pour modifier l'ID de VLAN et le nom de VLAN d'un commutateur compatible 802.1x

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).

   Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
2. Sous View Servers (Afficher les serveurs), sélectionnez le groupe Enforcer.
3. Sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés de groupe).
4. Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur) du tableau Switch Policy (Politique de commutateur), cliquez sur la politique de commutateur dont vous voulez modifier les informations VLAN.
5. Cliquez sur **Edit** (Modifier).
6. Dans la boîte de dialogue Edit Switch Policy (Modifier la politique de commutateur) pour *nom de la politique de commutateur*, dans l'onglet Switch Address (Adresse du commutateur), sélectionnez le VLAN que vous voulez modifier.
7. Dans l'onglet VLAN, cochez **Edit** (Modifier).
8. Dans la boîte de dialogue Edit VLAN (Modifier un VLAN), modifiez l'ID du VLAN dans le champ VLAN ID (ID de VLAN).
9. Modifiez le nom de VLAN dans le champ VLAN name (Nom de VLAN).

   Si vous prévoyez de modifier des informations de VLAN sur un commutateur Aruba, vous pouvez configurer les informations de VLAN et de rôle autrement que pour celles d'autres commutateurs 802.1x.

   Se reporter à "Configurer les informations de VLAN et de rôle sur le commutateur Aruba compatible 802.1x" à la page 204.
10. Dans la boîte de dialogue Edit Switch Policy (Modifier la politique de commutateur) pour *nom de la politique de commutateur*, dans l'onglet VLAN, cliquez sur **OK**.
11. Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur), cliquez sur **OK**.

Supprimer les VLAN sur un commutateur compatible 802.1x

Vous pouvez supprimer les VLAN sur un commutateur compatible 802.1x à tout moment si les circonstances le requièrent.

Pour supprimer les VLAN sur un commutateur compatible 802.1x

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).

   Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
2. Sous View Servers (Afficher les serveurs), sélectionnez le groupe Enforcer.
3. Sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés de groupe).
4. Dans la boîte de dialogue Paramètres de LAN Enforcer, dans l'onglet Commutateur du tableau de Politique de commutateur, cliquez sur la politique de commutateur dont vous voulez supprimer les informations VLAN.
5. Cliquez sur **Edit** (Modifier).
6. Dans la boîte de dialogue Edit Switch Policy (Modifier la politique de commutateur) pour *nom de la politique de commutateur*, dans l'onglet Switch Address (Adresse du commutateur), sélectionnez le VLAN que vous voulez supprimer.
7. Dans l'onglet VLAN, cochez **Remove** (Supprimer).
8. Cliquez sur **OK**.
9. Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur), cliquez sur **OK**.

Configurer les informations de VLAN et de rôle sur le commutateur Aruba compatible 802.1x

Si vous utilisez un commutateur Aruba, vous pouvez laisser les champs ID de VLAN ou Nom de VLAN vides. Cependant, pour d'autres commutateurs, vous devez entrer les informations dans les deux champs. Pour le commutateur Aruba, vous pouvez utiliser ces champs pour spécifier un VLAN ou un rôle ou les deux comme suit :

- Pour spécifier un VLAN, entrez l'ID de VLAN dans le champ ID de VLAN.
- Pour spécifier un rôle, entrez le nom de rôle dans le champ Nom de VLAN.

Pour le commutateur Aruba, vous pouvez également utiliser cette boîte de dialogue pour installer des actions de commutateur séparées pour des rôles multiples sur un VLAN ou des VLAN multiples pour un rôle.

Pour configurer les informations de VLAN et de rôle sur le commutateur Aruba compatible 802.1x

1. Si vous aviez un ID de VLAN 1 avec le rôle A et le rôle B, complétez l'ID de VLAN comme 1 et le nom de VLAN comme A. cliquez sur **OK**.
2. Cliquez sur **Ajouter** à nouveau. Dans la boîte de dialogue Ajouter un VLAN, complétez l'ID de VLAN comme 1 et le nom de VLAN comme B et cliquez sur **OK**.

   Deux choix séparés deviennent disponibles pour la configuration sur le tableau d'action de commutateur.

Modifier les informations d'action pour la politique de commutateur

Vous pouvez modifier les paramètres suivants au sujet des VLAN sur le commutateur compatible 802.1x :

- Définir l'ordre de la vérification des états
  Se reporter à "Définir l'ordre de la vérification des états" à la page 206.
- Sélectionner un état différent d'authentification d'hôte, d'authentification utilisateur ou de contrôle de politique
  Se reporter à "Sélectionner un état différent d'authentification d'hôte, d'authentification utilisateur ou de contrôle de politique" à la page 207.
- Sélectionner des actions différentes
  Se reporter à "Sélectionner des actions différentes" à la page 208.

A propos des problèmes avec la politique de commutateur, les états associées et les actions

En configurant des politiques de commutateur, maintenez les problèmes suivants à l'esprit :

- Le tableau Action de commutateur doit contenir au moins une entrée.
- Si vous ne sélectionnez pas une action pour une combinaison particulière de résultats, l'action par défaut, Port d'ouverture, est exécutée.
- Pour spécifier une action par défaut pour n'importe quelle combinaison possible de résultats, sélectionnez Ignorer le résultat pour chacun des trois résultats.
- Quand vous ajoutez les actions au tableau, vous pouvez modifier n'importe quelle cellule en cliquant sur le coin droit d'une colonne et d'une ligne pour afficher une liste déroulante.
- Certains commutateurs, tels que le commutateur Cisco, ont une fonction d'invité VLAN. L'invité VLAN est normalement destiné à être utilisé si

l'authentification utilisateur échoue. En d'autres termes, si l'authentification utilisateur échoue, le commutateur connecte le client à l'invité VLAN automatiquement.
Si vous utilisez LAN Enforcer pour la commutation VLAN, il est recommandé de ne pas utiliser l'invité VLAN réservé en installant des VLAN et des actions sur LAN Enforcer. Autrement le supplicant 802.1x peut réagir comme si l'authentification utilisateur a échoué.

- Si vous déployez des clients et n'êtes pas prêt à mettre en application les pleines fonctions de LAN Enforcer, vous pouvez spécifier une action pour permettre l'accès au réseau interne qui est basé sur l'état Ignorer le résultat pour la vérification de l'intégrité de l'hôte et le contrôle de politique. Si vous voulez négliger les résultats de l'authentification utilisateur et permettre l'accès au réseau indépendamment des résultats, vous pouvez faire ainsi avec l'état Ignorer le résutat pour des résultats d'authentification utilisateur.

Définir l'ordre de la vérification des états

Vous pouvez modifier un état différent d'authentification d'hôte, d'authentification d'utilisateur ou de contrôle de politique pour une politique de commutateur à tout moment si les circonstances le requièrent.

Vous pouvez ajouter une entrée au tableau Action de commutateur pour chacune des combinaisons possibles de résultats d'authentification.

Quand vous installez les conditions à rechercher, souvenez-vous que la seule circonstance dans laquelle chacun des trois résultats peuvent être Réussite ou Echec est le cas de la configuration de base. Dans la configuration de base, le client exécute un supplicant 802.1x qui fournit des informations au sujet de l'authentification utilisateur et un client qui fournit des informations au sujet de l'intégrité de l'hôte et du numéro de série de politique.

Si vous exécutez seulement un supplicant 802.1x sans client, les résultats pour la vérification de l'intégrité de l'hôte et de la politique sont toujours indisponibles. Si l'exécution s'effectue en mode transparent sans vérification d'authentification utilisateur, le résultat d'authentification utilisateur est toujours indisponible.

LAN Enforcer vérifie les résultats d'authentification par rapport aux entrées dans le tableau, du haut du tableau vers le bas du tableau. Lorsque LAN Enforcer a trouvé un ensemble de conditions correspondant, il demande au commutateur compatible 802.1x d'appliquer cette action. Vous pouvez modifier l'ordre dans lequel des actions sont appliquées en modifiant l'ordre dans lequel elles sont listées dans le tableau.

Si LAN Enforcer ne peut localiser aucune entrée qui correspond l'état actuel, une mesure de fermeture de port est prise.

Pour définir la commande de vérification de condition

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).

   Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
2. Sous View Servers (Afficher les serveurs), sélectionnez le groupe Enforcer.
3. Sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés de groupe).
4. Dans la boîte de dialogue LAN Enforcer Settings (Paramètres de LAN Enforcer), dans l'onglet Switch (Commutateur) du tableau Switch Policy (Politique de commutateur), cliquez sur la politique de commutateur dont vous voulez modifier l'ordre des conditions de vérification.
5. Cliquez sur **Edit** (Modifier).
6. Dans la boîte de dialogue Edit Switch Policy (Modifier la politique de commutateur) pour *nom de la politique de commutateur*, dans l'onglet Action, sélectionnez la politique de commutateur dont vous souhaitez modifier l'ordre des conditions de vérification.
7. Cliquez sur **Move Up** (Vers le haut) ou **Move Down** (Vers le bas).
8. Cliquez sur **OK**.
9. Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur), cliquez sur **OK**.

Sélectionner un état différent d'authentification d'hôte, d'authentification utilisateur ou de contrôle de politique

Vous pouvez sélectionner un état différent d'authentification d'hôte, d'authentification d'utilisateur ou de contrôle de politique pour une politique de commutateur à tout moment si les circonstances le requièrent.

Pour sélectionner un état différent d'authentification d'hôte, d'authentification d'utilisateur ou de contrôle de politique

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).

   Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
2. Sous View Servers (Afficher les serveurs), sélectionnez le groupe Enforcer.
3. Sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés de groupe).

4. Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur) du tableau Switch Policy (Politique de commutateur), cliquez sur la politique de commutateur dont vous voulez modifier les conditions d'authentification.
5. Cliquez sur **Edit** (Modifier).
6. Dans la boîte de dialogue Edit Switch policy (Modifier la politique de commutateur) pour *nom de politique de commutateur*, dans l'onglet Action (Action), cliquez sur l'une des conditions d'authentification que vous voulez modifier dans l'une des colonnes suivantes :
   - Authentification d'hôte
   - Authentification d'utilisateur
   - Contrôle de politique
7. Sélectionnez l'une des opérations suivantes à effectuer par le commutateur compatible 802.1x lorsque certains critères sont remplis :
   - Résultat d'authentification de l'hôte : Passer, Echouer, Indisponible ou Ignorer les résultats
   - Résultat d'authentification de l'utilisateur : Passer, Echouer, Indisponible ou Ignorer les résultats
   - Résultat de vérification de politique : Passer, Echouer, Indisponible ou Ignorer les résultats
8. Cliquez sur **OK**.
9. Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur), cliquez sur **OK**.

Sélectionner des actions différentes

Pour sélectionner un état différent d'authentification d'hôte, d'authentification utilisateur ou de contrôle de politique

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).

   Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
2. Sous View Servers (Afficher les serveurs), sélectionnez le groupe Enforcer.
3. Sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés de groupe).

4 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur) du tableau Switch Policy (Politique de commutateur), cliquez sur la politique de commutateur dont vous voulez modifier les actions.

5 Cliquez sur **Edit** (Modifier).

6 Dans l'onglet Action, cliquez sur les actions que vous voulez modifier dans la colonne Action.

7 Sélectionnez l'une des opérations suivantes à effectuer par le commutateur compatible 802.1x lorsque certains critères sont remplis :

- Port d'ouverture
  Le commutateur compatible 802.1x permet l'accès au réseau sur VLAN par défaut auquel le port est normalement attribué. Il permet également l'accès réseau sur le VLAN spécifié dans un attribut envoyé depuis le serveur RADIUS. Par conséquent la prise en charge des utilisateurs ayant un accès VLAN est basée sur le rôle et l'ID de l'utilisateur.
  L'action par défaut est port d'ouverture.
- Commutateur au *test* VLAN
  Permet à l'accès au VLAN spécifié. Les VLAN qui sont disponibles pour une sélection sont ceux que vous avez configurés précédemment.
- Port de fermeture
  Refuse l'accès au réseau sur le VLAN par défaut ou le VLAN spécifié par RADIUS. Sur quelques modèles de commutateur, selon la configuration de commutateur, le port est attribué à un invité VLAN.

8 Cliquez sur **OK**.

9 Dans la boîte de dialogue Settings (Paramètres) de LAN Enforcer, dans l'onglet Switch (Commutateur), cliquez sur **OK**.

Utilisation des paramètres avancés de boîtier LAN Enforcer

Vous pouvez configurer les paramètres de configuration avancés LAN Enforcer suivants :

- Allow a legacy client (Autoriser un client hérité).
  Se reporter à "Autoriser un client hérité à se connecter au réseau avec un boîtier LAN Enforcer" à la page 210.
- Enable local authentication (Activer l'authentification locale).
  Se reporter à "Activation de l'authentification locale sur le boîtier LAN Enforcer" à la page 210.

Autoriser un client hérité à se connecter au réseau avec un boîtier LAN Enforcer

Vous pouvez activer un boîtier LAN Enforcer de sorte à ce qu'il se connecte à des clients hérités 5.1.x. Si votre réseau prend en charge une console Symantec Endpoint Protection Manager 11.0.2 ainsi qu'un boîtier Symantec LAN Enforcer et qu'il doit prendre en charge des clients hérités 5.1.x, vous pouvez activer la prise en charge des clients hérités 5.1.x sur la console du serveur de gestion afin que le boîtier Symantec LAN Enforcer ne les bloque pas.

Pour autoriser un client hérité à se connecter au réseau avec un boîtier LAN Enforcer

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin, cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de boîtiers LAN Enforcer.
4. Dans la page Admin, sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans la boîte de dialogue Settings (Paramètres), dans l'onglet Advanced (Avancés), sélectionnez **Allow legacy clients** (Autoriser les clients hérités).
6. Cliquez sur **OK**.

Activation de l'authentification locale sur le boîtier LAN Enforcer

Si un boîtier LAN Enforcer perd la connexion à l'ordinateur sur lequel est installé Symantec Endpoint Protection Manager, le boîtier LAN Enforcer peut authentifier un client localement.

Pour activer l'authentification locale sur le boîtier LAN Enforcer

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin, cliquez sur **Servers** (Serveurs).
3. Sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de boîtiers LAN Enforcer.
4. Sélectionnez le groupe de boîtier LAN Enforcer pour lequel vous souhaitez activer l'authentification locale.
5. Sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés de groupe).

6 Dans la boîte de dialogue LAN Settings (Paramètres LAN), dans l'onglet Advanced (Avancé), sélectionnez **Enable Local Authentication** (Activer l'authentification locale).

7 Cliquez sur **OK**.

Utilisation de l'authentification 802.1x

Si votre réseau d'entreprise utilise LAN Enforcer pour l'authentification, vous devez configurer l'ordinateur client pour effectuer l'authentification IEEE 802.1x.

Le procédé d'authentification 802.1x inclut les étapes suivantes :

- Un client non authentifié ou un supplicant tierce partie envoie les informations utilisateur et les informations de conformité à un commutateur réseau 802.11 géré.
- Le commutateur réseau retransmet les informations au boîtier LAN Enforcer. Le boîtier LAN Enforcer envoie les informations utilisateur au serveur d'authentification pour l'authentification. Le serveur RADIUS est le serveur d'authentification.
- Si le client échoue à l'authentification au niveau utilisateur ou n'est pas conforme à la politique d'intégrité de l'hôte, Enforcer peut bloquer l'accès au réseau. En se référant au tableau Switch Action (Action de commutateur), le boîtier LAN Enforcer place l'ordinateur client non conforme sur un réseau où l'ordinateur peut être corrigé.
- Après que le client ait corrigé l'ordinateur et l'ait rendu conforme, le protocole 802.1x authentifie à nouveau l'ordinateur et lui accorde l'accès au réseau.

Pour travailler avec le boîtier LAN Enforcer, le client peut utiliser un supplicant tiers ou un supplicant intégré.

Tableau 8-2 décrit les types d'options que vous pouvez configurer pour l'authentification 802.1x.

Tableau 8-2 options d'authentification 802.1x

Option	Description
Supplicant tiers	Utilise un supplicant tiers 802.1x. Le boîtier LAN Enforcer fonctionne avec un serveur RADIUS et des supplicants tiers 802.1x pour effectuer l'authentification utilisateur. Le supplicant 802.1x demande aux utilisateurs les informations utilisateur, que LAN Enforcer transmet au serveur RADIUS pour l'authentification au niveau utilisateur. Le client envoie le profil client et l'état d'Intégrité de l'hôte au boîtier LAN Enforcer pour qu'il authentifie l'ordinateur. **Remarque :** Si vous voulez utiliser le client Symantec Network Access Control avec un tiers supplicant, alors vous devez installer le module de protection contre les menaces réseau du client Symantec Network Access Control. Pour utiliser un supplicant 802.1x tiers, vous devez : ■ Configurer le commutateur 802.1x pour utiliser le boîtier LAN Enforcer comme serveur Radius, de sorte que le commutateur transfère les paquets d'authentification au boîtier LAN Enforcer. ■ Ajouter le boîtier LAN Enforcer en tant que client du serveur Radius de sorte qu'il accepte des requêtes du boîtier LAN Enforcer. ■ Dans la console, vous devez spécifier les informations du serveur Radius et activer l'authentification 802.1x pour les clients.

Option	Description
Mode transparent	Utilise le client pour s'exécuter en tant que supplicant 802.1x. Vous utilisez cette méthode si vous ne voulez pas utiliser un serveur Radius pour effectuer l'authentification utilisateur. Le boitier LAN Enforcer s'exécute dans le mode transparent et agit en tant que serveur pseudo-RADIUS. Le mode transparent signifie que le supplicant ne demande pas aux utilisateurs les données utilisateur. Dans le mode transparent, le client agit en tant que supplicant 802.1x. Le client répond à la sollicitation EAP du commutateur avec le profil client et l'état d'intégrité de l'hôte. Le commutateur, à son tour, fait suivre les informations au boîtier LAN Enforcer, qui agit en tant que serveur pseudo-RADIUS. Le boîtier LAN Enforcer valide l'intégrité de l'hôte et les données de profil de client du commutateur et peut permettre, bloquer ou attribuer dynamiquement un VLAN, comme approprié. **Remarque :** Pour utiliser un client en tant que supplicant 802.1x, vous devez désinstaller ou désactiver les supplicants tiers 802.1x sur l'ordinateur client. Dans le mode transparent, vous pouvez laisser vides les informations du serveur Radius dans la boîte de dialogue Paramètres de LAN Enforcer. L'adresse IP du serveur Radius est donc définie à 0 et aucune authentification utilisateur traditionnelle EAP n'a lieu.
Supplicant intégré	Utilise le supplicant 802.1x intégré de l'ordinateur client. Les protocoles d'authentification intégrés incluent Smart Card, PEAP ou TLS. Après avoir activé l'authentification 802.1x, vous ou les utilisateurs devez spécifier le protocole d'authentification à l'utiliser.

Avertissement : Vous devez savoir si votre réseau d'entreprise utilise le serveur RADIUS comme serveur d'authentification. Si vous configurez l'authentification de 802.1x de façon incorrecte, la connexion au réseau peut être interrompue.

Remarque : Pour permettre à l'utilisateur de configure l'authentification 802.1x sur le client, vous devez définir le client en contrôle client.

Pour configurer le client pour utiliser le mode transparent ou un supplicant intégré

1. Dans la console, cliquez sur **Clients**.
2. Sous View Clients (Afficher les clients), sélectionnez le groupe des clients qui doivent effectuer l'authentification 802.1x.

3. Dans l'onglet Policies (Politiques), sous Settings (Paramètres), cliquez sur **General Settings** (Paramètres généraux).
4. Dans l'onglet Security Settings (Paramètres de sécurité), sélectionnez **Enable 802.1x authentication** (Activer l'authentification 802.1x).
5. Sélectionnez **Use the client as an 802.1x supplicant** (Utiliser le client comme supplicant 802.1x).
6. Effectuez l'une des opérations suivantes :
   - Pour sélectionner le mode transparent, sélectionnez Use Symantec Transparent Mode (Utiliser le mode transparent Symantec).
   - Pour permettre à l'utilisateur de configurer un supplicant intégré, sélectionnez Allows user to select the authentication protocol (Autoriser l'utilisateur à sélectionner le protocole d'authentification).
     Les utilisateurs peuvent choisir le protocole d'authentification pour leur connexion réseau.
7. Cliquez sur **OK**.

Pour configurer le client pour utiliser un supplicant tiers

1. Dans la console, cliquez sur **Clients**.
2. Sous View Clients (Afficher les clients), sélectionnez le groupe des clients qui doivent effectuer l'authentification 802.1x.
3. Dans l'onglet Policies (Politiques), sous Settings (Paramètres), cliquez sur **General Settings** (Paramètres généraux).
4. Dans l'onglet Security Settings (Paramètres de sécurité), sélectionnez **Enable 802.1x authentication** (Activer l'authentification 802.1x).
5. Cliquez sur **OK**.

   Vous pouvez configurer le client pour utiliser le supplicant intégré. Vous activez le client pour l'authentification 802.1x et en tant que supplicant 802.1x.

A propos de la réauthentification sur l'ordinateur client

Si l'ordinateur client réussit la vérification d'intégrité de l'hôte mais qu'Enforcer bloque l'ordinateur, les utilisateurs peuvent devoir réauthentifier leur ordinateur. Dans des circonstances normales, les utilisateurs ne doivent jamais avoir à authentifier à nouveau leur ordinateur.

Enforcer peut bloquer l'ordinateur lorsque l'un des événements suivants survient :

- L'authentification de l'utilisateur a échoué sur l'ordinateur client car les utilisateurs ont mal saisi leur nom d'utilisateur ou leur mot de passe.

- L'ordinateur client est dans le mauvais VLAN.
- L'ordinateur client n'obtient pas de connexion réseau. Une connexion réseau interrompue se produit habituellement parce que le commutateur entre l'ordinateur client et LAN Enforcer n'a pas authentifié le nom d'utilisateur et le mot de passe.
- Les utilisateurs doivent ouvrir une session sur un ordinateur client qui a authentifié un utilisateur précédent.
- L'ordinateur client a échoué au contrôle de conformité.

Les utilisateurs ne peuvent authentifier à nouveau l'ordinateur que si vous l'avez configuré avec un supplicant intégré. Le menu qui s'ouvre avec un clic sur le bouton droit de la souris sur l'icône de la zone de notification de l'ordinateur client affiche une commande de réauthentification.

Chapitre 9

Configurer les connexions temporaires pour les clients à la demande Symantec Network Access Control

Ce chapitre traite des sujets suivants :

A propos de la configuration de connexions temporaires pour les clients Symantec Network Access Control On-Demand

Les utilisateurs finaux doivent souvent se connecter temporairement à un réseau d'entreprise même si leurs ordinateurs ne sont pas équipés de logiciels approuvés. Si un réseau d'entreprise comprend un boîtier Gateway ou DHCP Enforcer, l'administrateur peut configurer le boîtier afin de permettre aux ordinateurs client

non conformes de se connecter temporairement au réseau d'entreprise en tant qu'invités.

L'administrateur peut configurer un boîtier Gateway ou DHCP Enforcer afin qu'il télécharge automatiquement les clients Symantec Network Access Control On-Demand sur les plates-formes Windows et Macintosh. Dès que le client à la demande Symantec Network Access Control est téléchargé vers un ordinateur client, le client peut essayer de se connecter au réseau de l'entreprise.

Si l'ordinateur client vérifie toutes les conditions requises, une connexion entre l'ordinateur client et Symantec Endpoint Protection Manager est automatiquement établie. L'ordinateur client conforme peut ainsi effectuer toutes les tâches que l'administrateur a activées pour ce groupe dans Symantec Endpoint Protection Manager.

Si l'ordinateur client ne vérifie pas toutes les conditions requises, la connexion entre l'ordinateur client et Symantec Endpoint Protection Manager ne peut pas être automatiquement établie. L'utilisateur final doit résoudre les conditions requises non conformes sur l'ordinateur client.

Avant de configurer les clients Symantec Network Access Control On-Demand sur une console Gateway ou DHCP Enforcer

Avant de pouvoir configurer le téléchargement automatique des clients Symantec Network Access Control On-Demand pour Windows et Macintosh, vous devez déjà avoir effectué les tâches suivantes :

- Installation du logiciel Symantec Network Access Control situé sur le deuxième CD-ROM, nommé CD2. Ce logiciel inclut le logiciel Symantec Endpoint Protection Manager que vous devez installer. Si vous installez par erreur le logiciel Symantec Endpoint Protection situé sur le premier CD-ROM nommé CD1, le logiciel Symantec Endpoint Protection Manager ne peut pas installer tous les composants requis.
  Consultez le *Guide d'installation pour Symantec Endpoint Protection et Symantec Network Access Control*.
- Relevé du mot de passe chiffré mis en place pendant l'installation du logiciel Network Access Control.
  Consultez le guide *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control*.
- Installation et configuration d'un boîtier Gateway or DHCP Enforcer.
  Quand vous installez et configurez un boîtier Enforcer pour la première fois, il attribue un nom au groupe Enforcer pendant la procédure d'installation. Vous devez prévoir l'attribution des adresses IP, des noms d'hôte, ainsi que la configuration des cartes d'interface réseau. Si les cartes d'interface réseau

sont configurées de manière incorrecte, l'installation échoue ou se comporte de manière inattendue.

Se reporter à "Avant d'installer le boîtier Enforcer" à la page 79.

Le nom du groupe Enforcer apparaît automatiquement sur la console Symantec Endpoint Protection Manager dans le volet Server (Serveur) qui est associé à chaque boîtier Enforcer.

Consultez le *Guide d'administration pour Symantec Endpoint Protection et Symantec Network Access Control*.

- Vérification de l'état de la connexion entre le boîtier Enforcer et le serveur Symantec Endpoint Protection Manager sur la console du boîtier Enforcer.

  Se reporter à "Vérifier l'état de communication d'un boîtier Enforcer sur la console Enforcer" à la page 93.

  Se reporter à "Show" à la page 261.

- A activé une redirection HTTP ou une usurpation DNS sur la console de Symantec Endpoint Protection Manager.

  La redirection HTTP ou l'usurpation DNS est l'adresse IP de la carte d'interface réseau interne (eth0) située sur un boîtier Gateway ou DHCP Enforcer.

  Pour la redirection HTTP, vous ajoutez l'URL dans la page Admin sur Symantec Endpoint Protection Manager. Après avoir affiché la page Admin, vous devez afficher le volet Servers (Serveurs) et sélectionner le groupe Enforcer sous View Servers (Afficher les serveurs). Si vous sélectionnez le groupe Enforcer dont Gateway ou DHCP Enforcer fait partie, cliquez sur Edit Group Properties (Modifier les propriétés du groupe) sous Tasks (Tâches). Dans la boîte de dialogue Settings (Paramètres) du module Enforcer, sélectionnez l'onglet Authentication (Authentification) et tapez l'URL dans le champ HTTP redirect URL (URL de redirection HTTP).

  Par exemple, vous pouvez saisir http://10.127.33.190 pour l'usurpation DNS. Vous le faites en faisant modifier par le boîtier DHCP Enforcer les messages appropriés de DHCP qui sont envoyés à un client. Le boîtier DHCP Enforcer remplace l'adresse IP du serveur DNS dans le message DHCP par l'adresse IP externe du boîtier DHCP Enforcer. Par conséquent le boîtier DHCP Enforcer agit en tant que serveur DNS pour les clients et empêche ainsi l'usurpation DNS.

  Consultez le *Guide d'administration pour Symantec Endpoint Protection et Symantec Network Access Control*.

- Vous devez créer le groupe de clients en tant que sous-groupe du groupe Global avec les droits Full Access (Accès complet).

  Vous ajoutez le groupe de clients à la page Clients en tant que sous-groupe du groupe Global sur Symantec Endpoint Protection Manager.

  Notez bien le nom du groupe Enforcer qui gère les clients Symantec Network Access Control On-Demand. Si vous ne créez pas de groupe séparé, c'est le

groupe par défaut de Symantec Endpoint Protection Manager qui assure la gestion des clients à la demande Symantec Network Access Control.
Consultez le *Guide d'administration pour Symantec Endpoint Protection et Symantec Network Access Control*.

- Créé un emplacement séparé facultatif pour un groupe de clients Enforcer sur la console Symantec Endpoint Protection Manager.
  Si vous ne créez pas d'emplacement séparé pour le groupe qui gère les clients Symantec Network Access Control On-Demand ou les clients invités, l'emplacement par défaut est automatiquement attribué aux clients invités. Il est recommandé de créer un emplacement séparé pour le groupe client Enforcer sur Symantec Endpoint Protection Manager.
  Les critères d'emplacement vous aident à définir les critères qui peuvent identifier les clients Symantec Network Access Control On-Demand ou les clients invités à l'aide de leur adresse IP, adresse MAC, nom d'hôte ou d'autres critères. Il est recommandé de créer un emplacement séparé auquel tous les clients Symantec Network Access Control On-Demand ou clients invités sont automatiquement attribués s'ils veulent se connecter à un réseau de manière temporaire sans disposer des informations d'authentification correctes.
  Vous pouvez ajouter et attribuer un emplacement au groupe client Enforcer dans la page Clients, sous Tasks, sur Symantec Endpoint Protection Manager.
  Consultez le *Guide d'administration pour Symantec Endpoint Protection et Symantec Network Access Control*.
- Ajouté et attribué une politique d'intégrité de l'hôte facultative au groupe de clients et à l'emplacement Enforcer sur la console Symantec Endpoint Protection Manager.
  Bien que l'ajout et l'attribution d'une politique d'intégrité de l'hôte au groupe client et à l'emplacement Enforcer sur la console Symantec Endpoint Protection Manager soient facultatifs, il est recommandé de spécifier les critères suivants :
  - Fréquence d'exécution d'une vérification de l'intégrité de l'hôte
  - Type de politique d'intégrité de l'hôte que vous voulez mettre en application

  Vous pouvez ajouter et attribuer une politique d'intégrité de l'hôte facultative à un groupe client et emplacement Enforcer dans la page Policies (Politiques), sous Tasks, sur Symantec Endpoint Protection Manager.
  Consultez le *Guide d'administration pour Symantec Endpoint Protection et Symantec Network Access Control*.
- Activé un message instantané facultatif sur la console Symantec Endpoint Protection Manager.
  Consultez le *Guide d'administration pour Symantec Endpoint Protection et Symantec Network Access Control*.

- Obtention du numéro d'identification (ID) du domaine qui se trouve sur la console Symantec Endpoint Protection Manager.
  Consultez le *Guide d'administration pour Symantec Endpoint Protection et Symantec Network Access Control*.
  Vous devez avoir l'ID du domaine à portée de main car il doit encore être configuré sur le boîtier Gateway ou DHCP Enforcer avec la commande on-demand spm-domain (domaine spm à la demande).
  Se reporter à "Activation de clients à la demande Symantec Network Access Control pour une connexion temporaire à un réseau " à la page 221.

Activation de clients à la demande Symantec Network Access Control pour une connexion temporaire à un réseau

Pour activer le téléchargement automatique d'un client à la demande de Symantec Network Access Control sur un ordinateur client avec plate-forme Windows ou Macintosh, vous devez avoir complété certaines tâches de configuration.

Se reporter à "Avant de configurer les clients Symantec Network Access Control On-Demand sur une console Gateway ou DHCP Enforcer" à la page 218.

Avant de permettre aux clients à la demande de Symantec Network Access Control de se connecter à un réseau, vous devez configurer les commandes suivantes :

- Exécutez la commande `spm-domain`.
- Exécutez la commande `client-group` (groupe client).
- Exécutez la commande `enable` (Activer).
- Exécutez la commande `authentication enable` (Activer l'authentification). Cette commande est facultative.

Se reporter à "Pour activer des clients à la demande Symantec Network Access Control pour une connexion temporaire à un réseau " à la page 221.

Pour activer des clients à la demande Symantec Network Access Control pour une connexion temporaire à un réseau

1. Connectez-vous à la console du boîtier Gateway Enforcer ou du boîtier DHCP Enforcer en tant que superutilisateur.

   Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.

2. Sur la console du boîtier Gateway Enforcer ou DHCP Enforcer, tapez la commande suivante :

   Enforcer #`on-demand`

3 Tapez la commande suivante :

Enforcer (on-demand)# `spm-domain`

où :

spm-domaine représente une chaîne automatiquement affichée dans le module d'application Enforcer.

Se reporter à "Avant de configurer les clients Symantec Network Access Control On-Demand sur une console Gateway ou DHCP Enforcer" à la page 218.

4 Tapez la commande suivante :

Enforcer (à la demande)# `groupe de clients "Global/`*`nom du groupe de clients Enforcer`*`"`

où :

nom du groupe client Enforcer représente le nom du groupe de clients Enforcer paramétré à la page Clients sous View Clients (Afficher les clients) de la console Symantec Endpoint Protection Manager. Vous devez déjà avoir défini ce groupe de clients Enforcer comme sous-groupe du groupe Global avec des droits d'accès complets. Si vous n'avez pas défini le groupe de client Enforcer sur la console de Symantec Endpoint Protection Manager, module d'application Enforcer s'enregistrera dans le groupe par défaut. Les informations sur le groupe de clients Enforcer sont automatiquement envoyées pendant le battement suivant.

Vous pouvez maintenant configurer l'authentification pour les clients à la demande Symantec Network Access Control.

Se reporter à "Installer l'authentification sur la console Gateway ou DHCP Enforcer pour les clients à la demande de Symantec Network Access Control" à la page 223.

5 Tapez la commande suivante :

Enforcer (à la demande)# `activer`

Désactiver des clients à la demande de Symantec Network Access Control pour les ordinateurs client

Le téléchargement automatique des clients à la demande de Symantec Network Access Control peut être désactivé.

Pour désactiver des clients à la demande de Symantec Network Access Control pour les ordinateurs client

1. Connectez-vous à la console du boîtier Gateway Enforcer ou du boîtier DHCP Enforcer en tant que superutilisateur.

   Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.
2. Sur la console du boîtier Gateway Enforcer ou DHCP Enforcer, tapez `on-demand` (à la demande).
3. Tapez `disable` (désactiver).
4. Tapez `exit` (quitter).
5. Tapez `exit` (quitter) pour fermer la session.

Installer l'authentification sur la console Gateway ou DHCP Enforcer pour les clients à la demande de Symantec Network Access Control

Vous pouvez authentifier des utilisateurs finaux en ajoutant des noms d'utilisateur et le mot de passe pour chaque utilisateur final dans une base de données locale qui est intégrée au boîtier Gateway ou DHCP Enforcer.

Se reporter à "Configurer l'authentification avec une base de données locale intégrée" à la page 223.

Si vous ne voulez pas utiliser la base de données locale intégrée au boîtier Gateway ou DHCP Enforcer, vous pouvez configurer les boîtiers Enforcer pour utiliser Microsoft Windows Server 2003 Active Directory pour gérer l'authentification des utilisateurs finaux.

Se reporter à "Configurer l'authenticaton avec Microsoft Windows Server 2003 Active Directory" à la page 224.

Configurer l'authentification avec une base de données locale intégrée

Vous pouvez configurer jusqu'à 1000 utilisateurs finaux sur la base de données intégrée.

Se reporter à "Commandes on-demand authentication local-db" à la page 299.

Pour configurer l'authentification avec une base de données locale

1. Connectez-vous à la console du boîtier Gateway Enforcer ou du boîtier DHCP Enforcer en tant que superutilisateur.

   Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.

2. Sur la console d'un boîtier Gateway ou DHCP Enforcer, tapez la commande suivante :

   Enforcer #`on-demand`

3. Sur la console d'un boîtier Gateway ou DHCP Enforcer, tapez la commande suivante :

   Enforcer (on-demand)# `authentication`

4. Tapez la commande suivante :

   Enforcer (authentication)# `enable`

5. Tapez la commande suivante :

   Enforcer (authentication)# `local-db enable`

6. Tapez la commande suivante :

   Enforcer (local-db)# `adduser username` *`nom_utilisateur`* `password` *`mot_de_passe`*

   où :

nom d'utilisateur	*nom_utilisateur* représente le nom de l'utilisateur final que vous voulez ajouter, comme dupond_pierre.
password	*mot_de_passe* représente le mot de passe que vous devez ajouter pour l'utilisateur final.

Configurer l'authenticaton avec Microsoft Windows Server 2003 Active Directory

La passerelle et les boîtiers Enforcer DHCP établissent une connexion à Microsoft Windows Serveur 2003 par le nom de domaine au lieu de l'adresse IP. Par conséquent vous devez avoir installé un serveur DNS (DNS) dans le réseau qui peut résoudre le nom de domaine.

Se reporter à "Commandes on-demand authentication ad" à la page 297.

Pour configurer l'authentification avec un serveur Active Directory

1. Connectez-vous à la console du boîtier Gateway Enforcer ou du boîtier DHCP Enforcer en tant que superutilisateur.

   Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.

2. Sur la console d'un boîtier Gateway ou DHCP Enforcer, tapez la commande suivante :

   Enforcer #`on-demand`

3. Tapez la commande suivante :

   Enforcer (on-demand)# `authentication`

4. Tapez la commande suivante :

   Enforcer (authentication)# `enable`

5. Tapez la commande suivante :

   Enforcer (authentication)# `ad enable`

6. Tapez la commande suivante :

   Enforcer (authentication)# `ad` *`ID_domaine`*

   où :

   ID_domaine représente le nom de domaine de Microsoft Windows Server 2003 Active Directory. Par exemple, www.symantec.fr.

Installer le client à la demande sous Windows pour l'authentification avec le protocole dot1x

Pour installer le client à la demande sous Windows pour l'authentification avec le protocole dot1x

1. Sur la console Enforcer, saisissez : `Enforcer#on-demand`
2. Tapez la commande suivante : `Enforcer(on-demand)# dot1x`
3. Tapez la commande suivante : `Enforcer(dot1x)# protocol tls`
4. Tapez la commande suivante : `Enforcer (tls)# show protocol`

   Le protocole doit être défini sur tls. For example, `Active Protocol: TLS`
5. Tapez la commande suivante : `Enforcer (tls)# validate-svr enable`
6. Tapez la commande suivante : `Enforcer (cert-svr)# exit`

7 Tapez la commande suivante : `Enforcer (tls)# show tls`

Assurez-vous que le certificat de serveur tls est activé. Par exemple :

```
TLS Validate Server Certificate:        ENABLED
TLS Certificate Server:                 ENABLED
TLS Certificate Server:                 127.0.0.1
```

8 Tapez la commande suivante : `Enforcer (dot1x)# certificate import tftp 10.34.68.69 password symantec username janedoe user-cert qa.pfx root-cert qa.ce`

où :

10.34.68.69 est le serveur tftp à partir duquel le boîtier Enforcer peut importer le certificat par tftp.

symantec est le mot de passe du certificat d'utilisateur

janedoe est le nom d'utilisateur avec lequel vous vous connectez sur le client.

qa.pfx est le nom du certificat d'utilisateur.

qa.cer est le nom du certificat racine

Installer le client à la demande sous Windows pour l'authentification avec le protocole peap

Pour installer le client à la demande sous Windows pour l'authentification avec le protocole peap

1 Sur la console Enforcer, saisissez : `Enforcer#on-demand`

2 Tapez la commande suivante : `Enforcer(on-demand)# dot1x`

3 Tapez la commande suivante : `Enforcer(dot1x)# protocol peap`

4 Tapez la commande suivante : `Enforcer (peap)# show protocol`

Assurez-vous que le certificat de serveur peap est activé ; par exemple :

```
PEAP Validate Server Certificate:       ENABLED
PEAP Certificate Server:                DISABLED
PEAP Certificate Server:                127.0.0.1
PEAP Fast Reconnected:                  DISABLED
```

5 Tapez la commande suivante : `Enforcer (peap) cert-svr host snac`

où :

`snac` est l'ordinateur qui est le serveur de CA pour le nom de certificat peap.

Modifier la bannière de la page d'accueil

Vous pouvez modifier le texte de la bannière par défaut sur la page d'accueil du client à la demande Symantec Network Access Control.

Pour modifier la bannière de la page d'accueil

1. Connectez-vous à la console du boîtier Gateway Enforcer ou du boîtier DHCP Enforcer en tant que superutilisateur.

   Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.

2. Saisissez la commande suivante sur la console d'un boîtier Gateway ou DHCP Enforcer :

   Enforcer #`on-demand`

3. Tapez la commande suivante :

   Enforcer(banner)# `banner`.

   Appuyez sur **Entrée**.

4. Dans la fenêtre contextuelle, tapez le message que vous voulez que les utilisateurs voient sur la page d'accueil du client Symantec Network Access Control On-Demand.

   Vous pouvez utiliser jusqu'à 1024 caractères.

Dépanner la connexion entre le module d'application Enforcer et les clients à la demande

Il y a plusieurs domaines et problèmes connus que vous pouvez étudier pour dépanner votre connexion entre le module d'application Enforcer et les clients à la demande.

Tableau 9-1

Symptôme	Solution
Le pare-feu bloque le fonctionnement du client quand l'utilisateur télécharge l'agent par PPTP VPN, CheckPoint VPN ou Juniper VPN	Plusieurs solutions possibles : ■ Modifier les paramètres de pare-feu pour débloquer le port UDP 39999. ■ Ajouter un itinéraire statique à l'itinéraire du module d'application Enforcer Par exemple : `route add IP netmask NM device eth0` où IP et NM sont l'adresse IP et le masque réseau du pool d'adresses IP du client. Ce pool est configuré sur le VPN par l'administrateur.
Les temps de téléchargement sont parfois longs	Le client envoie parfois le trafic à Verisign, rendant la vitesse de téléchargement quelque peu longue. Une solution de contournement est que l'administrateur ajoute Verisign à la liste des adresses IP de confiance.
La vérification de l'intégrité de l'hôte est parfois longue la première fois	Ce problème est dû à la résolution DNS et ne devrait pas apparaître après la première vérification de l'intégrité de l'hôte.
Le pare-feu du client empêche le client à la demande de fonctionner quand l'utilisateur n'a pas des droits d'administrateur	L'utilisateur peut modifier les paramètres de pare-feu pour débloquer le port UDP 39999. Alternativement, configurez le pare-feu pour autoriser `cclientctl.exe`
La mise à niveau du module d'application Enforcer ne contient pas initialement le paquet d'installation manuel	La raison en est la taille des paquets pris ensemble. La solution de contournement est de mettre à niveau le module d'application Enforcer et d'importer d'abord le paquet d'installation manuelle de client sur Symantec Endpoint Protection Manager, puis d'activer la fonctionnalité à la demande sur le module d'application Enforcer. Cela ajoutera les fichiers de l'installation manuelle.
L'URL de redirection sur le module d'application Enforcer écrasera une URL de redirection précédente sur SEPM	Cela se produit seulement quand la fonction à la demande est activée sur le module d'application Enforcer. C'est un comportement attendu.
Les clients Vista ne reçoivent parfois pas d'adresse IP du serveur DHCP	C'est un problème de synchronisation. Modifiez le délai DHCP pour 12 secondes ou plus.

Symptôme	Solution
Un utilisateur normal ne peut pas installer l'agent s'il n'y a aucun JRE installé.	La solution de contournement est de s'assurer que le JRE est installé. Autrement, seuls les utilisateurs admin peuvent installer.
Le service sans fil est déconnecté quand le client à la demande est installé et fermé, quand l'authentification 802.1x est utilisée	L'utilisateur doit redémarrer la connexion sans fil.
Les systèmes exécutant Norton 360 V. 2.x ont un problème pour recevoir le client	Suivez le lien "téléchargement manuel", téléchargez et installez le client et cela fonctionnera.
Avec Firefox, il n'est pas possible de télécharger le client et le plug-in NP avec seulement des droits d'utilisateur	L'installation du plug-in NP requiert des droits d'Admin.
L'installation manuelle échoue parfois	Cela peut nécessiter l'installation du correctif Microsoft KB893803. Ce correctif est inclus avec l'installation manuelle et devrait être installé avant l'installation du client. Des privilèges d'administrateur sont requis.
L'authentification 802.1x échoue	L'agent doit installer un pilote pour fonctionner. Si l'utilisateur a besoin de l'authentification 802.1x sur Windows, il doit ouvrir le navigateur avec la méthode "Exécuter en tant qu'administrateur" ou désactiver UAC pour s'assurer que l'agent fonctionne avec des droits d'administrateur.
Le message "Old version of ActiveX detected" apparaît	Vous devez supprimer la version d'ActiveX existante en cliquant sur Outils > Gérer les add-on > Activer ou désactiver les add-on > Contrôles ActiveX téléchargées, effacez Classe HodaAgt.
Le navigateur affiche le message "Affichage de la page Web impossible" et le client ne peut pas effectuer le téléchargement	Le client est peut-être déjà en cours d'exécution. Pour des raisons de sécurité, vous ne pouvez pas télécharger un nouveau client à l'intérieur d'une session client en cours d'exécution.

Symptôme	Solution
Le navigateur Firefox ne peut parfois pas télécharger le client	Ceci se produit quand Firefox est exécuté pour la première fois. Un ou deux redémarrages de Firefox sont requis pour qu'il termine sa configuration. Ensuite, le client à la demande devrait se télécharger.
Les ordinateurs sous Mac OS 10.4 ne s'authentifient parfois pas correctement en raison d'un nom d'hôte modifié	Cela semble dû à un problème avec cette version de Mac OS. La version 10.5 n'a pas le problème. La solution de contournement pour la version 10.4 est de définir le nom d'hôte dans `/etc/hostconfig/`.
Les vérifications de l'intégrité de l'hôte personnalisées qui dépendent de la variable système %temp% ne fonctionnent pas	La raison en est la nature transitoire de %temp%. La solution de contournement est d'indiquer d'autres emplacements.
Les règles d'ntégrité de l'hôte personnalisées qui pointent vers des valeurs de registre ne fonctionnent pas correctement	La raison en est la nature transitoire des sessions utilisateur.
L'installation du logiciel Panda Titanium 2007 ou Panda Internet Security 2007 ou 2008 fait apparaître le message "Veuillez patienter pendant que Windows configure Symantec Network Access Control".	Panda supprime un fichier essentiel de SNAC. Ce fichier est automatiquement réinstallé et vous pouvez ne prendre aucune mesure.

Chapitre 10

Interface de ligne de commande de boîtier Enforcer

Ce chapitre traite des sujets suivants :

A propos de la hiérarchie de commande d'interface de ligne de commande de boîtier Enforcer

Le boîtier Enforcer a une interface de ligne de commande (CLI) qui est organisée en hiérarchie de commande. Les commandes principales (de niveau supérieur) incluent les groupes de commandes suivants qui accèdent aux commandes supplémentaires :

- `capture`
- `configure`
- `console`
- `debug`

- `mab`
- `monitor`
- `on-demand`
- `snmp`

Hiérarchie de commande d'interface de ligne de commande

Tableau 10-1 décrit la hiérarchie pour les commandes Enforcer.

Tableau 10-1 Hiérarchie de commande d'interface de ligne de commande de boîtier Enforcer

Commandes de niveau supérieur	Commandes de premier sous-niveau	Commandes de deuxième sous-niveau
capture	Les commandes clear, exit, help et show (respectivement effacer, quitter, aide et afficher) sont uniquement disponibles aux connexions administration et root (superutilisateur). Vous pouvez utiliser les commandes de sous-niveau suivantes : ■ clear (effacer) ■ compress (compresser) ■ exit (quitter) ■ filter (filtrer) ■ help (aide) ■ show (afficher) ■ start (démarrer) ■ upload (charger) ■ verbose	non disponible
clear	non disponible	non disponible

Commandes de niveau supérieur	Commandes de premier sous-niveau	Commandes de deuxième sous-niveau
configure	Les commandes clear, exit, help et show (respectivement effacer, quitter, aide et afficher) sont uniquement disponibles aux connexions administration et root (superutilisateur). Vous pouvez utiliser les commandes de sous-niveau suivantes : ■ advanced (avancé) ■ clear (effacer) ■ dns ■ exit (quitter) ■ help (aide) ■ interface ■ interface-role (rôle d'interface) ■ ntp ■ redirect (rediriger) ■ route (router) ■ show (afficher) ■ spm	Seule la commande advanced a un ensemble de commandes de sous-niveau
console	baud-rate, clear, exit, help, show, ssh et sshkey Les commandes clear, exit, help et show sont disponibles à la connexion d'administration et root (superutilisateur).	non disponible
date	■ date ■ time (heure) ■ timezone (fuseau horaire)	non disponible
debug	clear, exit, destination, help, level, show et upload Les commandes clear, exit, help et show sont disponibles à la connexion d'administration et root (superutilisateur).	non disponible
exit	non disponible	non disponible
help	non disponible	non disponible
hostname	non disponible	non disponible

Commandes de niveau supérieur	Commandes de premier sous-niveau	Commandes de deuxième sous-niveau
mab	Les commandes clear, exit, help et show (respectivement effacer, quitter, aide et afficher) sont uniquement disponibles aux connexions administration et root (superutilisateur). ■ clear ■ database (base de données) ■ disable (désactiver) ■ enable (activer) ■ exit ■ help ■ ldap ■ show	non disponible
monitor	■ clear ■ exit ■ help ■ refresh ■ show	all or IP *ip address*
on-demand	Les commandes clear, exit, help et show (respectivement effacer, quitter, aide et afficher) sont uniquement disponibles aux connexions administration et root (superutilisateur). ■ authentification ■ banner ■ clear ■ client-group (groupe client) ■ disable ■ dot1x ■ enable ■ exit ■ help ■ mac-compliance (conformité mac) ■ show ■ spm-domain (domaine spm)	Reportez-vous à chaque commande pour plus d'informations sur les commandes du deuxième sous-niveau.
password	non disponible	non disponible
ping	non disponible	non disponible

Commandes de niveau supérieur	Commandes de premier sous-niveau	Commandes de deuxième sous-niveau
reboot	non disponible	non disponible
show	non disponible	non disponible
shutdown	non disponible	non disponible
snmp	■ disable (désactiver) ■ enable (activer) ■ heartbeat (battement) ■ receiver (récepteur) ■ show (afficher) ■ trap (piéger) ■ exit (quitter) ■ clear (effacer) ■ help (aide)	
start	non disponible	non disponible
stop	non disponible	non disponible
traceroute	non disponible	non disponible
update	non disponible	non disponible

Déplacement au sein de la hiérarchie de commande

Si vous voulez accéder à une commande qui est plus basse dans la hiérarchie, tapez la commande de niveau supérieur et la commande de niveau inférieur. Si vous avez plusieurs commandes que vous voulez exécuter dans un groupe de commandes, vous pouvez taper seulement la commande de niveau supérieur. Vous devez alors appuyer sur Entrée pour entrer le groupe de commandes. Le même processus s'applique si vous voulez obtenir une liste de commandes dans un groupe. Vous pouvez alors taper n'importe quelle commande fournie par ce groupe.

Par exemple, le groupe de capture contient une commande show permettant d'afficher les paramètres de configuration de capture. Pour accéder à la commande show à partir du niveau supérieur, tapez la commande de capture suivante :

```
Enforcer# capture show
```

Si vous tapez seulement la commande qui donne l'accès à un groupe de commandes et appuyez sur Entrée, l'invite suivante affiche le groupe de commandes entre parenthèses.

Par exemple :

```
Enforcer# capture

Enforcer(capture)#
```

Si vous voulez vous déplacer vers le haut de la hiérarchie et accéder à des commandes en dehors du groupe, vous devez d'abord quitter le groupe de commandes.

```
Enforcer(capture)# exit

Enforcer#
```

Raccourcis clavier de l'interface de ligne de commande de boîtier Enforcer

Quand vous utilisez l'interface de ligne de commande, vous pouvez utiliser des raccourcis clavier au lieu de taper des commandes ou obtenir l'aide pour le remplissage des commandes.

Tableau 10-2 indique les raccourcis clavier et l'aide d'interface de ligne de commande.

Tableau 10-2 Raccourcis clavier et aide d'interface de ligne de commande

Touches ou combinaisons de touches	Action
Touche Tab ou ?	■ Liste toutes les commandes ou options disponibles. ou ■ Complète la commande ou le nom d'option ou liste toutes les commandes ou options possibles commençant par les lettres que vous avez tapées. Pour plus d'informations : Se reporter à "Accès à l'aide des commandes d'interface de ligne de commande" à la page 237.
CTRL+D	Quitte un groupe de commandes.
CTRL+C	Supprime tous les caractères sur la ligne de commande.

Touches ou combinaisons de touches	Action

!	Liste les commandes dans le tampon d'historique des opérations.
	Les commandes que vous tapez sont enregistrées dans un tampon d'historique de 16k. Les commandes sont indexés en commençant par 1. En cas de dépassement de tampon, la commande la plus ancienne est remplacée et le chiffre d'index est modifié, de sorte que la commande la plus ancienne ait toujours l'incrément 1.
	La commande ! liste toutes les commandes dans le tampon d'historique des opérations. Si vous tapez un nombre suivi de !, la console Enforcer restaure la commande qui a ce nombre. La commande n'est pas exécutée jusqu'à ce que vous appuyiez sur Entrée.
	Ce qui suit est un exemple :
	`Enforcer# !`
	`1. con`
	`2. configure`
	`3. ping 192.168.0.1`
	`4. traceroute 192.168.0.16`
	`Enforcer# !3`
	`Enforcer# ping 192.168.0.1`

Touche flèche orientée vers le haut Touche flèche orientée vers le bas	Restaure les commandes dans le tampon d'historique des opérations en se déplaçant en haut et en bas.
Touche flèche orientée vers la gauche Touche flèche orientée vers la droite	Déplace le curseur un caractère vers la gauche et vers la droite.
Touches Origine et Fin	Déplace le curseur au début ou à la fin de la ligne de commande.
touche d'effacement arrière	Supprime un caractère sur la ligne de commande situé à gauche du curseur.
touche Supprimer	Supprime un caractère à l'emplacement du curseur.

Accès à l'aide des commandes d'interface de ligne de commande

Quand vous utilisez l'interface de ligne de commande, il y a plusieurs façons d'obtenir de l'aide pour les commandes et les options de commande.

Tableau 10-3 affiche les façons dont vous pouvez obtenir de l'aide pour les commandes d'interface de ligne de commande.

Tableau 10-3 Accès à l'aide des commandes d'interface de ligne de commande

Que voulez-vous faire ?	Action
Lister toutes les commandes disponibles avec une description courte	A l'invite de commandes, appuyez sur la touche Tab ou ? Toutes les commandes disponibles au niveau actuel de hiérarchie sont listées. Exemple : après avoir saisi la commande de configuration et appuyé sur Entrée pour accéder au groupe de commandes de configuration, appuyez sur Tab ou ? pour afficher toutes les commandes de configuration disponibles.
Afficher une description courte d'une commande spécifique	A l'invite de commandes, tapez Help suivi du nom de la commande. La commande doit être disponible sur le niveau actuel de hiérarchie.

Terminer le nom de commande ou lister toutes les commandes possibles qui commencent par les lettres tapées.	Tapez une ou plusieurs lettres du début du nom de la commande et appuyez sur Tab ou ?
	Par exemple :
	quand vous tapez co, puis appuyez sur Tab ou ? à l'invite de commande principale, la console Enforcer liste toutes les commandes disponibles qui commencent par co. Selon les indications de l'exemple suivant, deux commandes commencent par con. Par conséquent la console Enforcer remplit la lettre n.
	Exemple :
	`Enforcer# co?`
	`configure Configure Enforcer setting`
	`console Console setting`
	`Enforcer# con`

Afficher toutes les options pour une commande spécifique, avec une description courte de chaque option	Tapez la commande et appuyez sur Tab ou ? Par exemple : si vous êtes dans le groupe de commandes de configuration et voulez afficher les options pour la commande d'interface, tapez interface et appuyez sur Tab ou ? Exemple : `Enforcer(configure)# interface?` Chaque option d'interface est listée avec une description succinte.

Que voulez-vous faire ?	Action

Terminer le nom d'option ou lister toutes les options disponibles qui commencent par les lettres tapées.	Après avoir tapé le nom de l'option, tapez une ou plusieurs lettres du début du nom de l'option et appuyez sur Tab ou ?
	Par exemple :
	si vous tapez la commande show suivie de la lettre f, le module d'application Enforcer liste les deux options qui commencent par la lettre f. Puisque toutes les deux commencent par les lettres fil, la console complète il.
	Par exemple :
	`Enforcer# capture show f?`
	`files  Display packet capture files`
	`filter Display current packet capture filter`
	`Enforcer# capture show fil`

Chapitre 11

Référence d'interface de ligne de commande de boîtier Enforcer

Ce chapitre traite des sujets suivants :

Conventions de commande

Les conventions suivantes décrivent la syntaxe et l'utilisation des commandes d'interface de ligne de commande (CLI) du boîtier Enforcer :

Tableau 11-1 Conventions pour les commandes

Syntaxe	Utilisation
n	Les variables apparaissent en italique. Par exemple, n représente une variable :
accolades {}	Si une commande a des arguments multiples, les arguments multiples sont entourés dans des accolades {}. Ce qui suit est un exemple d'arguments multiples où n représente une variable : {width *n* | height *n*}
crochets []	Les arguments facultatifs sont placés entre crochets []. Ce qui suit est un exemple d'argument facultatif : [metric]
barre verticale |	Si une commande a des arguments multiples qui s'excluent, une barre verticale | sépare les arguments. Ce qui suit est un exemple d'arguments multiples qui s'excluent : {width *n* | height *n*}

Référence alphabétique d'interface de ligne de commande de boîtier Enforcer

Les commandes du boîtier Enforcer sont organisées dans une hiérarchie avec quelques commandes au niveau supérieur et d'autres sous les commandes suivantes : capture (capturer), configure (configurer), console, debug (débogage), mab, monitor (configurer), et on-demand (à la demande).

Les commandes clear, exit, help et show sont disponibles depuis tous les niveaux de la hiérarchie. Cependant, elles sont seulement listées dans le tableau au niveau supérieur. Les commandes sont disponibles si vous êtes connecté en tant qu'administrateur. Toutes les autres commandes sont disponibles seulement en se connectant en tant que root.

Pour afficher une description de toutes les commandes disponibles au niveau de hiérarchie actuel, vous pouvez taper un point d'interrogation (?) ou appuyez sur la touche de tabulation.

Le Tableau 11-2 donne une brève description des commandes.

Tableau 11-2 Résumé des commandes d'interface de ligne de commande

Commande	Description
capture	Accède aux commandes de capture de paquet. Se reporter à "Capture commands" à la page 263.
capture filter	Configure le filtre à appliquer à la capture de paquet. Se reporter à "Capture Filter" à la page 264.
capture show	Affiche la configuration de capture et liste les fichiers capturés. Se reporter à "Capture Show" à la page 265.
capture start	Lance la capture de paquet. Se reporter à "Capture Start " à la page 266.
capture upload	Utilise le protocole tftp pour envoyer un ou plusieurs fichiers. Se reporter à "Capture upload " à la page 267.
capture verbose	Active/désactive l'affichage des détails de capture de paquet. Se reporter à "Capture Verbose " à la page 267.
clear	Efface l'écran. Se reporter à "Clear" à la page 257.
configure	Permet d'accéder aux commandes Enforcer configure. Se reporter à "Configure commands" à la page 268.
configure advanced	Accède aux commandes de configuration avancées. Voir les commandes de configuration avancées qui sont listées dans ce tableau. Se reporter à "Commandes configure advanced" à la page 268.
configure advanced trunking	Active ou désactive la prise en charge de la liaison de jonction (Gateway Enforcer seulement). Se reporter à "Commandes configure advanced" à la page 268.
configure advanced catos	Active ou désactive la prise en charge de Cisco CATOS. (boîtier LAN Enforcer uniquement) Se reporter à "Advanced CATOS" à la page 268.
configure advanced check-uid	Active ou désactive l'identificateur client unique (UID) recherchant les agents hérités. (Gateway et DHCP Enforcer seulement) Se reporter à "Advanced check-uid" à la page 268.

Commande	Description
configure advanced dns-spoofing	Configure une adresse IP d'usurpation de DNS et l'active ou la désactive dans DHCP Enforcer. Désactiver la commande supprime l'adresse IP d'usurpation de DNS et la désactive dans DHCP Enforcer. (boîtiers DHCP Enforcer uniquement) Se reporter à "Advanced DNS spoofing" à la page 269.
configure advanced failover	Configure les paramètres de basculement de boîtier Enforcer. Se reporter à "Basculement avancé" à la page 269.
configure advanced legacy	Autorise ou bloque les agents hérités. Se reporter à "Advanced legacy" à la page 270.
configure advanced legacy-uid	Spécifie des UID hérités. (boîtiers Gateway et DHCP Enforcer uniquement) Se reporter à "Advanced legacy-uid" à la page 271.
configure advanced local-auth	Active ou désactive l'authentification de clients Enforcer. Se reporter à "Advanced RADIUS" à la page 272.
configure advanced re-initialize	Passe à un type différent de Enforcer. Cette option n'est pas disponible si vous êtes connecté à une session SSH. Se reporter à "Advanced re-initialize" à la page 272.
configure advanced radius	Active ou désactive le proxy de prise en charge de comptabilité de Radius. (boîtiers LAN Enforcer uniquement) Se reporter à "Advanced RADIUS" à la page 272.
configure advanced snacs	Définit l'IP de l'analyseur SNAC, le port et la clé pré-partagée (boîtiers Gateway et DHCP Enforcer uniquement). Utilisez cette commande pour réactiver l'analyseur SNAC s'il a été désactivé. Se reporter à "Advanced Symantec Network Access Control Server Scanner" à la page 272.
configure advanced user-class	Active ou désactive une classe d'utilisateurs. (boîtier DHCP Enforcer uniquement) Se reporter à "Commande advanced user-class" à la page 273.
configure dns	Ajoute ou supprime une entrée DNS. Se reporter à "Configure DNS" à la page 275.
configure interface	Configure l'interface réseau Adresse IP et le masque réseau. Se reporter à "Configure interface" à la page 275.
configure interface-role	Spécifie les interfaces réseau internes et externes. (Gateway et DHCP Enforcer seulement) Se reporter à "Configure interface-role" à la page 276.

Commande	Description
configure ntp	Etablit la communication entre un boîtier Enforcer et un serveur d'heure réseau ayant une adresse IP, un nom de domaine ou une adresse Web. Active ou désactive également la synchronisation d'heure entre le serveur d'heure réseau et le boîtier Enforcer. Se reporter à "Configure NTP" à la page 277.
configure redirect	Spécifie l'URL de redirection HTTP quand un client n'est pas installé sur un ordinateur. Se reporter à "Configure Redirect" à la page 278.
configure route	Configure les paramètres d'itinéraire. Se reporter à "Configure Route" à la page 278.
configure show	Affiche la configuration actuelle de chaque commande au groupe de configuration. Si aucun argument n'est spécifié, tous les paramètres apparaissent. Se reporter à "Configure Show" à la page 279.
configure spm	Configure la connexion Symantec Endpoint Protection Manager. Si vous modifiez un seul des arguments, vous devez tous les modifier, sinon les paramètres par défaut seront automatiquement utilisés à leur place. Se reporter à "Configure SPM" à la page 279.
console	Permet d'accéder aux commandes de configuration de la console. Se reporter à "Commandes Console" à la page 280.
console baud-rate	Définit la vitesse en bauds. Se reporter à "Console Baud-rate" à la page 280.
console ssh	Active ou désactive la connexion distante SSH. Se reporter à "Console SSH" à la page 281.
console sshkey	Définit et supprime la clé publique pour la connexion distante SSH sans mot de passe. Se reporter à "Console SSHKEY" à la page 281.
console show	Affiche les paramètres de configuration de la console d'un boîtier Enforcer. Se reporter à "Console Show" à la page 281.
date	Définit la date, l'heure et le fuseau horaire. Se reporter à "Date" à la page 258.
debug	Accéde aux commandes de débogage de boîtier Enforcer. Se reporter à "Commandes debug" à la page 282.

Commande	Description
debug destination	Définit la destination du débogage (mémoire, disque, les deux) Se reporter à "Debug Destination" à la page 282.
debug level	Définit le niveau des informations de débogage. Se reporter à "Debug Level" à la page 282.
debug show	Affiche les paramètres de configuration pour le débogage. Se reporter à "Debug Show" à la page 283.
debug upload	Utilise le protocole de transfert approuvé (tftp) pour envoyer un ou plusieurs fichiers à un autre ordinateur. Se reporter à "Debug upload" à la page 284.
exit	Ferme la connexion à la console d'un boîtier Enforcer lorsque la commande est utilisée comme commande de niveau supérieur ; sinon la commande ferme un groupe de commandes. Se reporter à "Exit" à la page 258.
help	Affiche l'aide sur une commande. Se reporter à "Commande Help" à la page 258.
hostname	Spécifie le nom d'hôte d'un boîtier Enforcer Se reporter à "Commande hostname" à la page 259.
mab	Fournit l'accès aux commandes sur un boîtier LAN Enforcer permettant d'appliquer la fonction MAB (MAC Authentication Bypass) sur des commutateurs compatibles 802.1x définis. Vous devez être connecté à la console d'un boîtier LAN Enforcer en tant que superutilisateur pour pouvoir exécuter cette commande. Se reporter à "Commandes MAB" à la page 284.
mab database	Permet d'accéder à toutes les commandes qui ajoutent et gèrent les entrées de base de données MAB locale sur un boîtier LAN Enforcer. Vous devez être connecté à la console d'un boîtier LAN Enforcer en tant que superutilisateur pour pouvoir exécuter cette commande.
monitor	Permet d'accéder aux commandes de monitor de Enforcer Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Commandes du groupe Monitor" à la page 288.

Commande	Description
monitor refresh	Met à jour les données d'adresse IP, de nom d'hôte, d'ID de politique et d'adresse MAC d'un client. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Commande monitor refresh " à la page 289.
monitor show	Affiche des données sur les hôtes bloqués, les invités connectés et les utilisateurs connectés. Se reporter à "Commande monitor show" à la page 289.
monitor show blocked-hosts	■ Affiche des données sur le nom d'hôte et l'ID de politique d'un hôte bloqué. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. ■ Affiche des données sur le nom d'hôte, l'ID de politique et l'adresse MAC d'un hôte bloqué. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Commande monitor show blocked-hosts" à la page 289.
monitor show connected-guests	■ Affiche des données sur l'adresse IP, le nom d'hôte et l'ID de politique d'un invité ou d'un client à la demande connecté. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. ■ Affiche des données sur l'adresse IP, le nom d'hôte, l'ID de politique et l'adresse MAC d'un invité ou d'un client à la demande connecté. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Commande monitor show connected-guests" à la page 291.
monitor show connected-users	■ Affiche des données sur l'adresse IP, le nom d'hôte, le nom d'utilisateur et l'ID de politique d'un utilisateur connecté ou d'un client géré. Un utilisateur connecté ou un client géré prend en charge les logiciels client Symantec Endpoint Protection et Symantec Network Access Control. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. ■ Affiche des données sur l'adresse IP, le nom d'hôte, l'ID de politique et l'adresse MAC d'un utilisateur connecté ou d'un client géré. Un utilisateur ou un client réseau connecté prend en charge le logiciel client Symantec Endpoint Protection et le logiciel client Symantec Network Access Control. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Commande monitor show connected-users" à la page 292.

Commande	Description
on-demand authentication local-db delete	Vous permet de supprimer un compte utilisateur existant de la base de données locale. Vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur avant que de pouvoir exécuter cette commande.
on-demand authentication local-db clear	Vous permet de nettoyer tous les comptes utilisateurs de la base de données locale. **Remarque :** Vous devez conserver au moins un compte utilisateur si vous utilisez l'authentification local-DB. Vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur avant que de pouvoir exécuter cette commande.
on-demand disable	Désactive le téléchargement automatique de clients Symantec Network Access Control On-Demand ou invités sur la console Gateway ou DHCP Enforcer. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90. Se reporter à "Désactiver des clients à la demande de Symantec Network Access Control pour les ordinateurs client" à la page 222.
on-demand enable	Active le téléchargement automatique de clients Symantec Network Access Control On-Demand ou invités sur la console Gateway ou DHCP Enforcer. Sinon l'installation échoue. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90. Se reporter à "Activation de clients à la demande Symantec Network Access Control pour une connexion temporaire à un réseau " à la page 221. Se reporter à "Commandes on-demand authentication local-db" à la page 299.

Commande	Description

on-demand authentication disable	Vous permet d'arrêter le processus d'authentification — le daemon auth — sur la console d'un boîtier Gateway ou DHCP pour un client Symantec Network Access Control On-Demand.
	
	Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur.
	
	Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.
	
	Se reporter à
	
	Vous pouvez arrêter le processus d'authentification (daemon auth) sur la console d'un boîtier Gateway ou DHCP pour un client à la demande Symantec Network Access Control.
	
	La commande on-demand authentication disable (désactiver l'authentification à la demande) utilise la syntaxe suivante :
	
	`on-demand authentication disable`
	
	Vous devez être connecté à une console Gateway ou DHCP Enforcer en tant que superutilisateur pour pouvoir exécuter cette commande.
	
	Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.
	
	L'exemple suivant décrit comment désactiver l'authentification pour un client Symantec Network Access Control On-Demand sur la console d'un boîtier Gateway ou DHCP Enforcer :
	
	`Enforcer# on-demand`
	`Enforcer (on-demand)# authentication disable`
	
	à la page 298.

on-demand authentication enable	Vous permet de démarrer le processus d'authentification — le daemon auth — sur la console d'un boîtier Gateway ou DHCP pour un client Symantec Network Access Control On-Demand. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90. Se reporter à "Commande on-demand authentication enable" à la page 299.
on-demand authentication ad disable	Désactive l'authentification de l'ordinateur client Symantec Network Access Control On-Demand. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90. Se reporter à "Commande on-demand authentication ad disable" à la page 297.

Commande	Description
on-demand authentication ad domain	Configure la communication entre un boîtier Enforcer et un répertoire actif pour l'authentification d'un ordinateur de client à la demande. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90. Se reporter à "Commande on-demand authentication ad domain" à la page 297.
on-demand authentication ad enable	Active l'authentification de l'ordinateur de client à la demande. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90. Se reporter à "Commande on-demand authentication ad enable" à la page 298.
on-demand authentication local-db	Permet d'accéder aux commandes on-demand authentication local-db. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90. Se reporter à "Commandes on-demand authentication local-db" à la page 299.
on-demand authentication local-db add	Vous permet de configurer le nom et le mot de passe de connexion sur une console de boîtier DHCP pour un utilisateur final qui veut télécharger automatiquement un client à la demande de Symantec Network Access Control sur un ordinateur client. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.
on-demand authentication local-db disable	Vous permet de désactiver une configuration d'authentification pour un ordinateur de client à la demande par rapport à une base de données locale. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.
on-demand authentication local-db enable	Vous permet d'activer une configuration d'authentification pour un ordinateur de client à la demande par rapport à une base de données locale. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.

Commande	Description
on-demand authentication show	Vous permet d'afficher les paramètres d'authentification pour un ordinateur de client à la demande. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.
on-demand banner	Vous permet de modifier le texte de la bannière par défaut sur la page d'accueil des clients Symantec Network Access Control On-Demand. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90. Se reporter à "Modifier la bannière de la page d'accueil" à la page 227. Se reporter à "Commande on-demand banner" à la page 302.
on-demand spm-domain	Vous permet de configurer l'ID de domaine sur la console d'un boîtier Gateway ou DHCP Enforcer. Sinon, l'installation de client à la demande échoue. Se reporter à "Activation de clients à la demande Symantec Network Access Control pour une connexion temporaire à un réseau " à la page 221. Après la connexion à Symantec Endpoint Protection Manager, l'ID de domaine apparaît sur le boîtier Enforcer. Consultez le *Guide d'administration pour Symantec Endpoint Protection et Symantec Network Access Control* sur la manière de localiser l'ID de domaine. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90. Se reporter à "Commande on-demand spm-domain" à la page 314.
on-demand dot1x	Vous permet d'activer votre configuration d'authentification de contrôle d'accès réseau 802.1x basée sur le port pour les sessions de client à la demande. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.
on-demand dot1x default-user	Vous permet de configurer une authentification de contrôle d'accès réseau 802.1x basée sur le port anonyme pour les sessions de client à la demande. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.

Commande	Description
on-demand dot1x certificate	Vous permet de configurer un certificat utilisateur et une racine d'authentification 802.1x. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90. Se reporter à "Commandes on-demand dot1x certificate" à la page 303.
on-demand dot1x certificate import	Vous permet d'importer un certificat d'authentification 802.1x. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90. Se reporter à "Commande on-demand dot1x certificate import" à la page 304.
on-demand dot1x certificate remove	Vous permet de supprimer un certificat d'authentification 802.1x. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90. Se reporter à "Commande on-demand dot1x certificate remove command" à la page 305.
on-demand dot1x peap	Vous permet de configurer un protocole 802.1x PEAP (Protected Extensible Authentication Protocol) pour authentifier les clients à la demande sur le réseau protégé. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90. Se reporter à "Commande on-demand dot1x peap" à la page 306.
on-demand dot1x peap validate-svr enable	Vous permet d'activer la validation d'un certificat de serveur de protocole 802.1x PEAP (Protected Extensible Authentication Protocol) pour l'accès des clients à la demande au réseau protégé. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90. Se reporter à "Commande on-demand dot1x peap cert-svr" à la page 307.

Commande	Description
on-demand dot1x peap validate-svr disable	Vous permet de désactiver la validation d'un certificat de serveur de protocole 802.1x PEAP (Protected Extensible Authentication Protocol) pour l'accès des clients à la demande au réseau protégé. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90. Se reporter à "Commande on-demand dot1x peap cert-svr" à la page 307.
on-demand dot1x peap cert-svr	Vous permet de configurer un protocole 802.1x PEAP (Protected Extensible PEAP (Protected Extensible Authentication Protocol), ainsi qu'un certificat d'utilisateur pour l'accès des clients à la demande au réseau protégé. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.
on-demand dot1x peap fast-reconn enable	Vous permet d'activer la reconnexion rapide de protocole 802.1x PEAP (Protected Extensible Authentication Protocol) au certificat de serveur racine pour l'accès des clients à la demande au réseau protégé. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.
on-demand dot1x peap fast-reconn disable	Vous permet de désactiver la reconnexion rapide de protocole 802.1x PEAP (Protected Extensible Authentication Protocol) au certificat de serveur racine pour l'accès des clients à la demande au réseau protégé. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.
on-demand dot1x peap show	Vous permet d'afficher les paramètres de configuration d'une authentification de protocole 802.1x PEAP (Protected Extensible Authentication Protocol) pour un client à la demande afin de confirmer que PEAP est le protocole actif. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.

Commande	Description
on-demand dot1x peap exit	Vous permet de quitter la hiérarchie de configuration d'interface de ligne de commande pour le protocole 802.1x PEAP (Protected Extensible Authentication Protocol). Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.
on-demand dot1x protocol	Vous permet de configurer un protocole 802.1x PEAP (Protected Extensible Authentication Protocol) pour l'accès des clients à la demande au réseau protégé en tant que PEAP ou TLS.. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.
on-demand dot1x show	Vous permet d'afficher dans l'interface de ligne de commande la configuration de protocole 802.1x PEAP (Protected Extensible Authentication Protocol) pour un client à la demande afin de confirmer que le protocole configuré est PEAP ou TLS. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.
on-demand dot1x tls	Vous permet d'entrer en mode de configuration pour le protocole 802.1x TLS (transport layer security). Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.
on-demand dot1x tls validate-svr enable	Vous permet d'activer la validation d'un certificat de serveur racine pour une configuration de protocole 802.1x TLS (transport layer security). Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90. Se reporter à "Commande on-demand dot1x peap cert-svr" à la page 307.
on-demand dot1x tls validate-svr disable	Vous permet de désactiver la validation d'un certificat de serveur racine pour une configuration de protocole 802.1x TLS (transport layer security). Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.

Commande	Description
on-demand dot1x tls cert-svr enable	Vous permet de configurer un certificat de serveur racine pour un protocole 802.1x TLS (transport layer security) pour l'authentification des clients à la demande. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.
on-demand dot1x tls cert-svr disable	Désactive le serveur de certificats TLS.
on-demand dot1x tls cert-svr host	Définit le nom d'hôte du serveur de certificats TLS.
on-demand dot1x tls show	Vous permet d'afficher les paramètres de configuration d'un protocole 802.1x TLS (transport layer security) pour l'authentification des clients à la demande. Vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur pour pouvoir exécuter cette commande. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.
on-demand dot1x tls exit	Vous permet de quitter le mode d'interface de ligne de commande pour la configuration 802.1x TLS. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.
à la demande client-groupez	Vous permet de configurer preferGroup sur la console Gateway ou DHCP Enforcer et sur la console Symantec Endpoint Protection Manager. Sinon l'installation échoue. Bien qu'elle soit facultative pour l'installation d'un groupe séparé pour les clients à la demande de Symantec Network Access Control, elle est recommandée. Si vous n'installez pas un groupe séparé, tous les clients à la demande de Symantec Network Access Control deviennent automatiquement membres du groupe par défaut sur la console Symantec Endpoint Protection Manager. Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90. Se reporter à "Activation de clients à la demande Symantec Network Access Control pour une connexion temporaire à un réseau " à la page 221. Se reporter à "Commande on-demand client-group" à la page 302. Consultez le *Guide d'administration pour Symantec Endpoint Protection et Symantec Network Access Control* sur la manière d'installer un groupe pour les clients à la demande ou invités de Symantec Network Access Control.

Commande	Description
on-demand mac-compliance	Vous permet de configurer le client à la demande de Symantec Network Access Control sur une plate-forme de Macintosh pour éviter qu'un utilisateur final n'installe des programmes ou des fichiers non-autorisés. Se reporter à "Commandes on-demand mac-compliance" à la page 315. Vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur pour pouvoir exécuter cette commande.
on-demand mac-compliance enable	Vous permet de configurer les options d'intégrité d'hôte pour une plateforme Macintosh de client à la demande. Se reporter à "Commandes on-demand mac-compliance" à la page 315. Vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur pour pouvoir exécuter cette commande. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.
on-demand mac-compliance disable	Vous permet de désactiver la configuration d'intégrité d'hôte pour une plateforme Macintosh de client à la demande. Se reporter à "Commandes on-demand mac-compliance" à la page 315. Vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur pour pouvoir exécuter cette commande. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.
on-demand mac-compliance show	Vous permet de configurer la liste des options logicielles d'intégrité d'hôte pour une plateforme Macintosh de client à la demande. Se reporter à "Commandes on-demand mac-compliance" à la page 315. Vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur pour pouvoir exécuter cette commande. Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.
on-demand mac-compliance interval	Vous permet de définir l'intervalle de contrôle de conformité (en minutes) pour les clients à la demande Symantec Network Access Control.
password	Modifie le mot de passe pour se connecter au boîtier Enforcer. Se reporter à "Password" à la page 259.
ping	Envoie un écho ICMP à un hôte distant. Se reporter à "Ping" à la page 260.
reboot	Redémarre le boîtier Enforcer. Se reporter à "Reboot" à la page 260.

Commande	Description
show	Affiche les informations d'état et de configuration de boîtier Enforcer. Se reporter à "Show" à la page 261.
shutdown	Désactive un boîtier Enforcer. Se reporter à "Shutdown" à la page 261.
snmp	Prise en charge du protocole SNMP (Simple Network Management Protocol).
snmp disable	Désactive SNMP.
snmp enable	Active SNMP.
snmp heartbeat	Permet de définir le battement pour le protocole SNMP.
snmp receiver	Paramètres de récepteur SNMP.
snmp show	Affiche la configuration et le statut du protocole SNMP.
snmp trap	Définition du nombre d'essais et du délai de dépassement SNMP
start	Démarre un service de module d'application Enforcer. Se reporter à "Start" à la page 262.
stop	Arrête un service de module d'application Enforcer. Se reporter à "Stop" à la page 262.
traceroute	Imprime l'itinéraire pris par les paquets jusqu'à l'hôte réseau. Se reporter à "Traceroute" à la page 262.
update	Met à jour le logiciel de boîtier Enforcer. Se reporter à "Update" à la page 263.

Commandes de niveau supérieur

Les commandes de niveau supérieur sont disponibles dans l'interface de ligne de commande d'Enforcer. Ce sont des commandes d'administration générale. Certaines des commandes, telles que clear, exit, help et show, sont disponibles pour tous les niveaux de la hiérarchie.

Clear

La commande clear efface le contenu de l'écran.

Voici un exemple de syntaxe :

```
Enforcer# clear
```

Date

La commande date définit l'heure ou le fuseau horaire de système pour le boîtier.

Voici un exemple de syntaxe :

```
date {day <MM/JJ/AA> | time <HH:MM:SS> |timezone}
```

Exit

La commande exit (quitter) permet de quitter la console lorsqu'elle est utilisée comme commande principale ou permet de quitter un groupe de commandes lorsqu'elle est utilisée depuis un groupe de commandes. Vous pouvez également utiliser la combinaison de touches Ctrl+D au lieu de la commande exit.

Voici un exemple de syntaxe :

```
Enforcer# exit
```

Commande Help

La commande help (aide) affiche les informations d'aide pour une commande spécifiée. Pour afficher l'aide pour toutes les commandes disponibles, tapez un point d'interrogation (?) ou appuyez sur la touche de tabulation.

Remarque : Quelques commandes sont spécifiques aux modules d'application Gateway Enforcer ou DHCP Enforcer uniquement. Ces commandes n'apparaissent pas sur les autres modules d'application Enforcer.

Voici un exemple de syntaxe pour le groupe de commandes Main (Principal) :

```
help {capture | clear | configure | console | date |
debug | exit | hostname| mab | monitor| on-demand |
password | ping | reboot | show | shutdown | start |
stop | traceroute | update | snmp}
```

Quand vous utilisez la commande help au sein d'un groupe de commandes, elle affiche des informations d'aide pour une commande individuelle du groupe. Pour afficher l'aide pour toutes les commandes du groupe, vous pouvez taper un point d'interrogation (?) ou appuyez sur la touche de tabulation.

Voici un exemple de syntaxe pour le groupe de commandes Capture (Capturer) :

```
help {clear | compress | exit | filter | show | start |
verbose | ymodem | upload}
```

Voici un exemple de syntaxe pour le groupe de commandes Configure (Configurer) :

```
help {advanced | clear | dns | exit | interface |
interface-role | route | show | spm | redirect | ntp}
```

Voici un exemple de syntaxe pour le groupe de commandes Configure Advanced :

```
help {catos | check-uid | clear | dnsspoofing | exit |
 failover
| legacy | legacy-uid | local-auth | snacs | user-class | show |
 trunking}
```

Ce qui suit est un exemple de syntaxe pour le groupe de commandes Console :

```
help {baud-rate | clear | dimensions | exit
| re-initialize | serial-port | show | ssh | sshkey}
```

Voici un exemple de syntaxe pour le groupe de commandes Debug (Débogage) :

```
help {clear | compress | destination | exit | level |
 show
 |ymodem | upload}
```

Commande hostname

La commande hostname (nom d'hôte) modifie le nom d'hôte du boîtier Enforcer. Le nom d'hôte par défaut est Enforcer. Si vous modifiez le nom d'un boîtier Enforcer, vous pouvez distinguer plusieurs boîtiers Enforcer sur le gestionnaire Symantec Endpoint Protection Manager et dans les journaux Enforcer.

Le nom d'hôte est automatiquement enregistré sur Symantec Endpoint Protection Manager lors du battement suivant. Si vous modifiez le nom d'hôte d'un boîtier Enforcer, vous devrez éventuellement modifier l'entrée sur le serveur DNS.

Ce qui suit est un exemple de syntaxe pour la commande hostname :

```
hostname nom_hôte
```

Password

La commande password modifie le mot de passe du compte. Vous devez confirmer le mot de passe existant avant de spécifier et confirmer le nouveau mot de passe.

Le nouveau mot de passe doit contenir une lettre minuscule, une lettre majuscule, un chiffre et un symbole.

Ce qui suit est un exemple de syntaxe pour la commande password :

```
password
```

Ping

La commande ping vérifie les connexions à un hôte distant qui ont été spécifiées avec une adresse IP ou un nom d'hôte. La commande utilise une demande d'écho ICMP et des paquets de réponse d'écho pour déterminer si un système IP particulier sur un réseau est fonctionnel. Vous pouvez utiliser la commande ping pour diagnostiquer les échecs de réseau IP ou de routeur. La commande ping vous permet de vérifier si Enforcer peut communiquer avec Symantec Endpoint Protection Manager.

Ce qui suit est un exemple de la syntaxe pour la commande ping :

```
ping adresse_ip | nom_hôte
```

Exemple

```
ping 192.168.0.1

PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.

64 bytes from 192.168.0.1: icmp_seq=0 ttl=64 time=0.585 ms

64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.149 ms

64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.131 ms

64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.128 ms

--- 192.168.0.1 ping statistics ---

4 packets transmitted, 4 received, 0% packet loss, time 57ms

rtt min/avg/max/mdev = 0.128/0.248/0.585/0.194 ms, pipe 2,
ipg/ewma 19.043/0.436 ms
```

Reboot

La commande reboot redémarre le boîtier Enforcer.

Ce qui suit est un exemple de la syntaxe pour la commande reboot :

```
reboot
```

Shutdown

La commande shutdown arrête le boîtier Enforcer.

Ce qui suit est un exemple de la syntaxe pour la commande shutdown :

```
shutdown
```

Show

La commande show (afficher) affiche les informations sur la configuration ou l'état du boîtier Enforcer.

Ce qui suit est un exemple de syntaxe pour la commande show (afficher) :

```
show { capture | configure | console | date | debug |
 hostname| status | update | version }
```

où :

capture	Affiche les paramètres de capture de paquet tels que le protocole, les filtres et la compression
configure	Affiche le réseau Enforcer et la configuration de Symantec Endpoint Protection Manager
console	Affiche la configuration de console
status	Affiche l'état de groupe de service Enforcer
update	Affiche la mise à jour disponible pour l'installation à partir du tftp, du CD-ROM ou du lecteur USB
version	Affiche la version d'Enforcer et les informations de copyright
date	Affiche l'heure locale et l'heure UTC
déboguer	Affiche la configuration de débogage du module d'application Enforcer
hostname	Affiche le nom d'hôte de l'appareil

L'exemple suivant répertorie les résultats de la commande show status (afficher l'état) :

```
show status
Enforcer Status: ONLINE(ACTIVE)
Policy Manager Connected:     NO
Policy Manager:     192.168.0.64 HTTP 80
Packets Received:    26
Packets Transmitted:  1
Packets Rx. Echec :   0
Packets Tx. Echec :   0
Enforcer Health:    EXCELLENT
Enforcer Uptime:    0 days 00:00:28
Policy ID:
```

L'exemple suivant répertorie les résultats de la commande show version sur un boîtier Enforcer DHCP :

```
show version
Symantec Network Access Control Enforcer 6100 Series - v11.0.1
build XXXX, 2007-11-29,19:09
DHCP Enforcer mode
```

Start

La commande start démarre le service d'Enforcer.

Ce qui suit est un exemple de la syntaxe pour la commande start :

```
Enforcer# start
```

Stop

La commande stop arrête le service d'Enforcer.

Ce qui suit est un exemple de la syntaxe pour la commande stop :

```
Enforcer# Stop
```

Traceroute

La commande traceroute trace l'itinéraire que les paquets prennent pour parvenir à un hôte distant. L'hôte distant a été spécifié avec une adresse IP ou un nom d'hôte.

Ce qui suit est un exemple de la syntaxe pour la commande traceroute :

```
traceroute [ adresse_ip | nom_hôte ]
```

Exemple

```
traceroute 10.50.0.180

traceroute to 10.50.0.180 (10.50.0.180), 30 hops max, 38-byte packets

 1 192.168.0.1 (192.168.0.1) 0.391 ms 0.132 ms 0.111 ms

 2 10.50.2.1 (10.50.2.1) 0.838 ms 0.596 ms 0.589 ms

 3 oldserver1.sygate.dev (10.50.0.180) 1.170 ms 0.363 ms 0.469 ms
```

Update

La commande update (mettre à jour) met à jour le progiciel Enforcer à partir d'un serveur tftp, d'un disque dur USB ou d'un CD-ROM.

Ce qui suit est un exemple de la syntaxe pour la commande update :

```
Enforcer:# update
```

Capture commands

Les commandes du groupe de commandes de capture du boîtier Enforcer vous permettent de capturer des paquets sur les cartes d'interface réseau du boîtier Enforcer. Les paquets sont enregistrés dans un fichier. Des commandes supplémentaires vous permettent d'envoyer le fichier en format simple ou compressé à un client avec divers protocoles de transfert de fichiers (tftp). Le boîtier Enforcer doit être connecté au client par le câble série fourni.

Toutes les commandes de ce groupe sont listées et décrites excepté les commandes `capture exit` (quitter capture) et `capture help` (aide capture). La commande `capture exit` (quitter capture) ferme le groupe de commandes. La commande `capture help` (aide capture) affiche des informations d'aide sur toutes les commandes du groupe.

Commande capture compress

La commande capture compress (compresser capture) permet de comprimer un fichier.

La commande capture compress utilise la syntaxe suivante :

```
compress {on | off}
```

où :

on (actif)	Active les compressions.
off (désactivé)	Désactive les compressions.

L'exemple suivant décrit la syntaxe pour la commande capture compress on (activer la compression de capture) sur la console d'un boîtier Enforcer :

```
Enforcer# capture

Enforcer(capture)# compress on
```

Capture Filter

La commande Capture filter (filtre de capture) définit un filtre qui spécifie quels paquets sont capturés.

Elle utilise la syntaxe suivante :

```
filter [auth] [spm] [failover] [all] [client ip-range]
```

où :

```
Enforcer :
```

auth	capture les paquets d'authentification qui circulent entre le client, le boîtier Enforcer et Symantec Endpoint Protection Manager L'argument par défaut est auth.
spm	capture les paquets de communication échangés par Symantec Endpoint Protection Manager et le module d'application Enforcer ; capturez un profil Enforcer en téléchargeant depuis Symantec Endpoint Protection Manager et consignez les paquets de chargement
failover	capture les paquets de basculement Enforcer (envoyés périodiquement pour rechercher un autre module d'application Enforcer sur le réseau). Le basculement n'est pas accessible avec la carte ouverte par défaut installée.
all	capture tous les paquets spécifiés

client *ip-range*

Cette option est seulement disponible avec Gateway Enforcer et DHCP Enforcer.

Définit l'intervalle d'IP client pour capturer des paquets d'authentification uniquement sur Gateway Enforcer et LAN Enforcer. *ip-range* peut être une combinaison d'adresses IP, d'intervalles d'IP et de sous-réseaux/masques. Une virgule sans espaces sépare les arguments. Vous pouvez utiliser les formats suivants :

- L'adresse IP est formatée en tant que nnn.nnn.nnn.nnn
- L'intervalle d'IP est formaté en tant que nnn.nnn.nnn.nnn-nnn.nnn.nnn.nnn
- Le sous-réseau/masque est formaté en tant que nnn.nnn.nnn.nnn/nnn.nnn.nnn.nnn

L'exemple suivant décrit la syntaxe pour la commande capture filter (filtre de capture) :

```
Enforcer# capture filter auth client

192.168.0.1,192.168.0.10-192.168.0.100,192.168.1.1/255.255.255.0
```

Cette commande filtre tous les paquets d'authentification pour les clients avec l'adresse IP 192.168.0.1. Elle filtre les clients dont l'adresse IP est comprise dans l'intervalle 192.168.0.10 à 192.168.0.100 et les clients dans le sous-réseau 192.168.1.1 avec un masque de réseau de 255.255.255.0.

Capture Show

La commande capture show (afficher capture) affiche la configuration de capture et liste les fichiers qui sont capturés.

La commande capture show utilise la syntaxe suivante :

```
show {compress | files | filter | verbose | ymodem}
```

où :

compress	affiche si la compression de fichiers est activée ou désactivée
files	Affiche tous les fichiers capturés dans le dossier de capture du boîtier Enforcer
filter (filtrer)	affiche la configuration actuelle du filtre
verbose (détaillé)	affiche la configuration détaillée actuelle

ymodem	affiche les paramètres d'option du protocole Ymodem

Exemple :

```
capture show

Capture Filter:  auth
Client IP Range:
Capture Verbose is ON.
Compress capture files before sending is ON.
YMODEM protocol option is YMODEM-g.
```

Capture Start

La commande capture start (démarrer capture) démarre la capture de paquets. Pour arrêter, appuyez sur Echap.

La commande capture start utilise la syntaxe suivante :

```
capture [start]
```

Exemple

```
Enforcer# capture

Enforcer(capture)# start


Captured packets are saved to /opt/GatewayEnforcer/bin/../capture/
Dec-07-200

5-12-24-23.cap.

Press ESC to stop capture...
0  0.000000 192.168.0.25 -> 192.168.0.211 UDP Heartbeat Ver 5.1.1915
Start Session to Agent. SEQ: 0f495cd8.

1  0.000000 192.168.0.25 -> 192.168.0.64 UDP RADIUS Access Request.
ID 64 192.168.0.211  Query Status

2  0.000000 192.168.0.211 -> 192.168.0.25 UDP Heartbeat Ver 5.0.0
Keep Alive to Enforcer. SEQ: 0f495cd8. HI Disabled.
Profile 85E0-10/20/2005 11:30:00 812.

Host Integrity check is disabled. Host Integrity policy is disabled by
```

```
administrator.

3  0.000000 192.168.0.64 -> 192.168.0.25 UDP RADIUS Access Accept. ID 64
192.168.0.211  Profile 85E0-10/20/2005 11:30:00 812

4 packets were captured.

Captured packets were saved to /opt/GatewayEnforcer/bin/../capture/
Mar-07-2006-1

2-24-23.cap.
```

Capture upload

La commande capture upload (chargement de capture) utilise le protocole tftp pour envoyer un ou plusieurs fichiers.

La commande capture upload utilise la syntaxe suivante :

```
capture upload {filename tftp://nnn.nnn.nnn.nnn}
```

Exemple :

```
Enforcer# capture

Enforcer(capture)# upload test.tar.gz tftp://10.200.38.221
```

Capture Verbose

La commande capture verbose (détails de la capture) active ou désactive l'affichage des détails du paquet pendant la capture.

La commande capture verbose utilise la syntaxe suivante :

```
verbose {on | off}
```

où :

on (activé)	affiche les détails du paquet
off (désactivé)	n'affiche pas des détails du paquet

Configure commands

Les commandes dans le groupe configure de l'interface de ligne de commande du boîtier Enforcer vous permettent d'afficher et de configurer les paramètres d'interface réseau et la connexion à Symantec Endpoint Protection Manager.

Toutes les commandes dans ce groupe sont listées et décrites excepté les commandes `exit` (quitter) et `help` (aide). La commande `exit` (quitter) ferme le groupe de commandes. La commande `help` (aide) affiche des informations d'aide sur les commandes individuelles du groupe.

Le groupe configure (configurer) contient une commande `advanced` (avancées) donnant accès à un ensemble d'options de configuration avancées.

Se reporter à "Commandes configure advanced" à la page 268.

Commandes configure advanced

Les commandes du groupe advanced d'interface de ligne de commande du boîtier Enforcer font partie du groupe configure. Elles vous permettent de configurer les paramètres de configuration avancés Enforcer.

Toutes les commandes dans ce groupe sont décrites excepté les commandes `exit` et `help`. La commande `exit` (quitter) ferme le groupe de commandes. La commande `help` affiche des informations d'aide sur les commandes individuelles du groupe.

Advanced CATOS

La commande advanced CATOS active ou désactive la prise en charge de Cisco CATOS.

La commande advanced CATOS utilise la syntaxe suivante (LAN Enforcer) :

```
advanced catos {enable | disable}
```

Advanced check-uid

La commande advanced check-uid active ou désactive l'UID recherchant les agents hérités.

La commande advanced check-uid utilise la syntaxe suivante (Gateway et DHCP Enforcer) :

```
advanced check-uid {enable | disable}
```

Advanced DNS spoofing

La commande advanced DNS spoofing configure une adresse IP d'usurpation de DNS et l'active ou la désactive dans DHCP Enforcer. Désactiver la commande supprime l'adresse IP d'usurpation de DNS et la désactive dans DHCP Enforcer.

La commande advanced dns spoofing utilise la syntaxe suivante (DHCP Enforcer) :

```
advanced dnsspoofing {enable [IP] adresse_ip | disable}
```

Basculement avancé

La commande advanced failover (basculement avancé) active ou désactive le basculement de boîtiers Enforcer et configure le port de basculement et le niveau de sensibilité.

Cette commande n'est pas accessible en cas d'activation de l'option Ouvert par défaut.

La commande advanced failover utilise la syntaxe suivante (boîtiers Gateway ou DHCP Enforcer) :

```
advanced failover disable | {enable [port <numéro_port>] [sensitive
 <niveau_sensibilité>]}
```

où :

disable	désactive le basculement de boîtier Enforcer
enable	active le basculement de boîtier Enforcer Le paramètre par défaut est activé.
port *numéro_port*	spécifie un numéro de port de basculement d'Enforcer de 1 à 65535
sensitive *niveau_sensibilité*	spécifie un niveau de sensibilité de basculement d'Enforcer de 0 à 4 pour indiquer la fréquence de recherche d'autres modules d'application Enforcer

Les boîtiers Gateway Enforcer et DHCP Enforcer possèdent les paramètres de configuration par défaut suivants :

- Le basculement est activé.
- Le port UDP que les modules d'application Enforcer de basculement utilisent pour communiquer entre eux est 39999.
- Le niveau par défaut de sensibilité de basculement est élevé (moins de 5 secondes).

Ce paramètre détermine avec quelle rapidité le boîtier Enforcer de réserve devient le boîtier Enforcer primaire en cas de détection d'une panne de l'Enforcer primaire. Plus le niveau qui est spécifié est élevé, plus courte est l'attente de la relève de l'Enforcer de réserve. En parallèle, il y a davantage de temps système dans le réseau et dans l'UC.
Les niveaux suivants sont disponibles :

Très haut (0)	Moins de 2 secondes
Haut (1)	Moins de 5 secondes
Moyen (2)	Moins de 10 secondes
Faible (3)	Moins de 15 secondes
Très faible (4)	Moins de 30 secondes

Advanced legacy

La commande advanced legacy active ou désactive la prise en charge des agents hérités. La prise en charge de l'agent hérité est activée par défaut.

Les agents hérités sont des agents qui exécutent le logiciel pre-5.x Sygate Security Agent. Pour les boîtiers LAN Enforcer, l'agent hérité représente les logiciels Sygate Security Agent qui exécutent la version 4.1 et ultérieure.

L'agent hérité représente les agents de sécurité Sygate qui exécutent la version 3.5 ou 4.x et n'incluent pas les versions 2.x, 3.0 et 3.1.

Remarque : La prise en charge pour les agents hérités s'applique uniquement aux boîtiers DHCP Enforcer et Gateway Enforcer.

La commande advanced legacy utilise la syntaxe suivante :

```
advanced legacy {allow | block}
```

où :

allow	autorise les agents hérités Le paramètre par défaut est allow.
block	bloque les agents hérités

Vous pouvez utiliser des boîtiers Enforcer sur les sites qui exécutent les versions (héritées) antérieures des agents. Si vous autorisez les agents hérités, le boîtier

Enforcer confirme que l'agent hérité s'exécute, puis vérifie les résultats de la vérification de l'intégrité de l'hôte. Si l'agent réussit la vérification de l'intégrité de l'hôte, il peut se connecter au réseau. Pour les agents hérités, le boîtier Enforcer ne vérifie pas l'identifiant de l'agent pour vérifier que cet agent est valide. Il ne vérifie pas non plus son numéro de série de profil pour confirmer que ses politiques sont à jour.

Advanced legacy-uid

La commande advanced legacy-uid spécifie le GUID du client hérité.

La commande advanced legacy-uid utilise la syntaxe suivante (boîtiers Gateway et DHCP Enforcer) :

```
advanced legacy-uid chaîne_uid
```

Advanced Local-auth

La commande advanced local-auth (authentification locale avancée) active ou désactive l'authentification du client par le module d'application Enforcer. Utilisez cette commande pour le dépannage.

L'authentification client est désactivée par défaut.

La commande advanced local-auth utilise la syntaxe suivante :

```
advanced local-auth {disable | enable}
```

où :

enable	Vérifie le client avec Symantec Endpoint Protection Manager et bloque le client s'il est incapable de se connecter à Symantec Endpoint Protection Manager. Le paramètre par défaut pour l'authentification client est enable (activé).
disable	Désactive la vérification du client et exécute uniquement la validation d'intégrité de l'hôte.

Par défaut, le boîtier Gateway Enforcer vérifie l'identificateur unique (UID) du client avec Symantec Endpoint Protection Manager. Si le module d'application Gateway Enforcer ne peut pas se connecter à Symantec Endpoint Protection Manager pour vérifier l'UID, il bloque le client. Bien que cela ne soit pas recommandé en tant qu'étape de dépannage, vous pouvez empêcher le boîtier Gateway Enforcer de vérifier l'UID.

Par défaut, le boîtier Gateway Enforcer vérifie l'UID. Au lieu de cela, le boîtier Gateway Enforcer effectue seulement un contrôle de validation d'intégrité de l'hôte. Prenez soin de réactiver ce paramètre si vous voulez que le boîtier Gateway Enforcer vérifie l'UID.

Advanced RADIUS

La commande advanced RADIUS configure et active ou désactive la prise en charge du proxy de comptabilité de RADIUS.

La commande advanced radius utilise la syntaxe suivante (boîtiers LAN Enforcer) :

```
advanced radius acc_proxy {enable | disable} | acc_port <1811-1813>
```

L'exemple suivant décrit la syntaxe pour la commande advanced radius (boîtier LAN Enforcer) :

```
Enforcer(advanced)# radius proxy {enable | disable}
```

Advanced re-initialize

La commande advanced re-initialize active le commutateur sur différents types de module d'application Enforcer en réinitialisant la configuration d'Enforcer. Cette commande n'est pas disponible si vous êtes connecté à session SSH.

La commande advanced re-initialize utilise la syntaxe suivante :

```
advanced re-initialize
```

Advanced Symantec Network Access Control Server Scanner

La commande advanced snacs définit l'adresse IP de l'analyseur Symantec Network Access Control, le numéro de port et la clé pré-partagée. Utilisez cette commande pour réactiver l'analyseur Symantec Network Access Control s'il a été désactivé.

Remarque : L'analyseur Symantec Network Access Control ne prend pas en charge une connexion d'imprimante à un boîtier Symantec DHCP Enforcer. Les imprimantes n'acceptent pas les itinéraires statiques configurés pour un boîtier Symantec DHCP Enforcer. Par conséquent, l'analyseur Symantec Network Access Control ne peut pas communiquer avec une imprimante connectée à un boîtier Symantec DHCP Enforcer.

La commande advanced snacs (snacs avancés) utilise la syntaxe suivante (boîtiers Gateway Enforcer et DHCP Enforcer) :

```
snacs enable | disable | set [ip <adresse_ip>]
[port <1811-1813>] [key <chaîne>]
```

L'exemple suivant décrit la syntaxe pour la commande advanced snacs (boîtier Gateway et DHCP Enforcer) :

```
Enforcer(advanced)# snacs

disable  disable snacs

set ip  set ip adresse_ip

set key  set key chaîne
```

Advanced show

La commande advanced show affiche les paramètres de configuration pour les commandes avancées d'Enforcer.

La commande show utilise la syntaxe suivante :

```
show
```

Exemple :

```
Enforcer# configure advanced show
Failover Status:        ENABLED
Failover Port:         39999
Failover Sensitivity Level:   1
Legacy Client:         ALLOW
Local Authentication:      ENABLED
```

Commande advanced user-class

La commande advanced user-class (classe d'utilisateurs avancée) active ou désactive l'ID de la classe d'utilisateurs SYGATE_ENF sur le boîtier Enforcer.

La commande advanced user-class utilise la syntaxe suivante (DHCP Enforcer) :

```
advanced user_class {disable | enable}
```

où :

disable (désactiver)	active l'ID de classe d'utilisateurs de boîtier Enforcer
enable (activer)	active l'ID de classe d'utilisateurs de boîtier Enforcer

Si vous voulez utiliser un serveur DHCP à la fois comme serveur DCHP normal et de quarantaine, vous devez effectuer les étapes de configuration suivantes :

- Après avoir installé le boîtier Enforcer, utilisez la commande advanced user-class pour activer l'ID de classe d'utilisateurs.
  Après avoir activé l'ID de classe d'utilisateurs, le boîtier Enforcer inclut l'ID de classe d'utilisateurs SYGATE_ENF dans la requête DHCP. Le boîtier Enforcer envoie alors la requête DHCP au serveur DHCP pour les clients qui ont besoin d'une configuration de quarantaine.
- Ajoutez la classe d'utilisateurs SYGATE_ENF au serveur DHCP et configurez le serveur DHCP. Ainsi, quand le serveur DHCP reçoit une requête avec l'ID de classe d'utilisateurs SYGATE_ENF, il fournit une adresse IP de quarantaine et une configuration de réseau.

Liaison de jonction avancée

La commande advanced trunking configure la fonction de liaison de jonction.

La commande advanced trunking utilise la syntaxe suivante :

```
advanced trunking enable | disable |
chall-vlist <liste_vlan> | nat-vid <id_vlan> |fail-vid
<id_vlan> | mgmt-vid <id_vlan>
```

où :

chall-vlist	Spécifie la liste de VLAN que Gateway Enforcer doit confronter. Format : n[-n][,n[-n]]... n:<1-4096> par exemple 1,2,3-6,8,10-15
disable	Disable trunking feature
enable (activer)	Enable trunking feature
fail-vid	Spécifie où Gateway Enforcer doit envoyer ou recevoir à partir de ces paquets de basculement
mgmt-vid	Spécifie l'ID de VLAN de gestion
nat-vid	Spécifie l'identification de VLAN de ces paquets non identifiés

Configure DNS

La commande configure DNS (configurer DNS) ajoute ou supprime une entrée de serveur DNS (domain name server). Par exemple, vous devez ajouter une entrée DNS si vous voulez spécifier un gestionnaire Symantec Endpoint Protection Manager avec un nom d'hôte.

La commande configure DNS utilise la syntaxe suivante :

```
configure {add | delete} <adresse IP>
```

où :

add (ajouter)	vous permet d'ajouter l'adresse IP d'un serveur DNS.
delete (supprimer)	vous permet de supprimer l'adresse IP d'un serveur DNS.

L'exemple suivant décrit comment ajouter l'adresse IP d'un serveur DNS sur la console d'un boîtier Enforcer :

```
Enforcer#: configure

Enforcer(configure)# dns

Enforcer(dns)# add 192.192.192.10
```

Configure interface

La commande configure interface ouvre ou ferme une carte d'interface réseau. Elle configure également l'adresse IP d'une carte d'interface réseau ou configure une carte d'interface réseau en tant que client DHCP.

La commande configure interface utilise la syntaxe suivante :

```
configure interface up <nom_carte_interface_réseau> | down
<nom_carte_interf_réseau> | failopen | set <nom_cartef_inter_réseau> ip
<adresse_ip> [netmask <masque_sous_réseau>]
```

où :

up *nom_carte_interface_réseau*	Nom de la carte d'interface réseau à démarrer, tel que eth0 ou eth1. eth0 ou eth1 distinguent les majuscules et minuscules.

down *nom_carte_interface_réseau*	Nom de la carte d'interface réseau à arrêter, tel que eth0 ou eth1. eth0 ou eth1 distinguent les majuscules et minuscules.
failopen [enable | disable]	Active ou désactive le mode de contournement pour la carte Ethernet ouverte par défaut. Si un boîtier Gateway Enforcer configuré comme passerelle échoue, la configuration active l'état de contournement sur le boîtier Gateway.
set *nom_carte_interface_réseau*	Nom de la carte d'interface réseau, tel que eth0 ou eth1, à configurer en tant que client DHCP. Le nom est sensible à la casse.
set IP address *adresse_IP* netmask *masque_réseau*	Nom de la carte d'interface réseau (eth0 ou eth1, sensible à la casse) pour laquelle vous souhaitez configurer l'adresse IP statique et le masque de sous-réseau : ■ IP address *adresse_IP* : adresse IP de la carte d'interface réseau ■ netmask *masque_réseau* : masque de sous-réseau de la carte d'interface réseau
set gateway *adresse_IP*	Nom de la carte d'interface réseau, tel que eth0 ou eth1, que vous pouvez configurer comme passerelle si vous voulez mettre en application un mode de contournement. eth0 ou eth1 distinguent les majuscules et minuscules.

Exemple :

```
configure interface set eth0 ip 10.0.0.1 netmask 255.0.0.0
```

Cette commande définit l'adresse IP de eth0 sur 10.0.0.1 avec un masque de réseau de 255.0.0.0. Remplacez l'adresse IP et le masque de réseau par les valeurs que vous voulez utiliser. Vous devez configurer une deuxième carte d'interface réseau (eth1) pour les boîtiers Gateway ou DHCP Enforcer.

Configure interface-role

La commande configure interface-role spécifie la carte d'interface réseau qui représente la carte d'interface réseau interne.

Vous pouvez également spécifier la carte d'interface réseau externe (boîtiers Gateway Enforcer et DHCP Enforcer seulement).

Vous pouvez également spécifier la carte d'interface réseau qui communique avec Symantec Endpoint Protection Manager (boîtier DHCP Enforcer seulement).

La commande configure interface-role utilise la syntaxe suivante :

```
interface-role internal <nom_carte_interface_réseau> |
external <nom_carte_interf_réseau> | manager <nom_carte_interf_réseau
_(DHCP Enforcer uniquement)>
```

où :

internal *nom*	Nom (tel que eth0 ou eth1) de la carte d'interface réseau qui se connecte au réseau interne. Le nom est sensible à la casse.
external *nom_carte_interface_réseau*	Nom (tel que eth0 ou eth1) de la carte d'interface réseau qui se connecte au réseau externe. Le nom distingue les majuscules et minuscules.
manager *nom_carte_interface_réseau (DHCP Enforcer uniquement)*	Nom (tel que eth0 ou eth1) de la carte d'interface réseau qui se connecte à Symantec Endpoint Protection Manager. Le nom distingue les majuscules et minuscules.

Configure NTP

La commande configure ntp string (chaîne de configuration NTP) établit la communication entre un boîtier Enforcer et un serveur d'heure réseau en spécifiant une adresse IP, un nom de domaine ou une adresse Web.

Les commandes configure ntp enable (activer la configuration ntp) ou configure ntp disable (désactiver la configuration ntp) permettent respectivement de démarrer et d'arrêter la synchronisation de l'heure entre un boîtier Enforcer et serveur d'heure réseau avec le protocole NTP (Network Time Protocol).

La commande configure ntp server (configurer le serveur NTP) utilise la syntaxe suivante :

```
ntp enable | disable | server <nom_d'hôte>
```

où :

ntp server <nom_d'hôte>	Vous pouvez établir la communication entre un boîtier Enforcer et un serveur d'heure réseau en spécifiant une adresse IP, un nom de domaine ou une adresse Web.

ntp enable	Vous pouvez démarrer la synchronisation temporelle entre un boîtier Enforcer et un serveur d'heure réseau avec le protocole NTP (Network Time Protocol). .
ntp disable	Vous pouvez arrêter la synchronisation temporelle entre un boîtier Enforcer et un serveur d'heure réseau avec le protocole NTP (Network Time Protocol). .

Configure Redirect

La commande configure redirect spécifie une adresse de redirection HTTP lorsqu'un client n'est pas installé sur un terminal client. (Boîtier Gateway Enforcer uniquement. Non applicable si Symantec Endpoint Protection Manager est déployé dans un environnement de réseau.)

La commande configure redirect utilise la syntaxe suivante :

```
configure redirect <url-string>
```

Configure Route

La commande configure route ajoute ou supprime une entrée dans la table des routes. Vous pouvez configurer plusieurs entrées.

La commande configure route utilise la syntaxe suivante :

```
configure route {add | delete} <adresse_ip>
netmask <masque_sous_réseau> device <nom_carte_interface_réseau>
[gateway <adresse_ip>] [metric <métrique>]
```

où :

add <adresse_ip> netmask <masque_sous_réseau>	Adresse IP et masque de sous-réseau de l'entrée à ajouter au tableau d'itinéraire
delete <adresse_ip> netmask <masque_sous_réseau>	Adresse IP et masque de sous-réseau de l'entrée à supprimer de la table des routes
device <nom_carte_interface_réseau>	Nom d'interface (eth0 ou eth1, sensibles à la casse) de l'entrée
gateway <adresse_ip>	Adresse IP de la passerelle pour l'entrée
metric <métrique>	Métrique de l'entrée, un entier de 1 à 32

L'exemple suivant ajoute une entrée dans un tableau de routage avec une adresse IP, un masque de sous-réseau, un nom de carte d'interface réseau et une adresse IP de passerelle :

```
Enforcer# configure

Enforcer(configure)# route

Enforcer(route)# add 192.168.45.0 netmask 255.255.255.0 device
eth0 gateway 192.168.40.1
```

Configure Show

La commande configure show (afficher la configuration) affiche la configuration actuelle de chaque commande du groupe de configuration. Si aucun argument n'est spécifié, tous les paramètres apparaissent.

La commande configure show (afficher la configuration) utilise la syntaxe suivante (boîtiers Gateway Enforcer ou DHCP Enforcer seulement) :

```
configure dns | interface [<nom NIC>] |
interface-role | ntp | redirect | route | spm
```

Configure SPM

La commande configure SPM configure la connexion entre le boîtier Enforcer et le console Symantec Endpoint Protection Manager.

Vous devez saisir toutes les valeurs si vous modifiez l'une des valeurs. Toutes les valeurs que vous ne spécifiez pas utilisent automatiquement les valeurs par défaut.

La commande configure SPM utilise la syntaxe suivante :

```
configure spm {[ip <adresse IP>] | [group
<nom groupe>] | [http <numéro port>] | https
<numéro port>] | [key <nom clé>]} | [del key
<clé partagée>]
```

où :

ip <adresse_ip>	permet d'ajouter l'adresse IP de la console Symantec Endpoint Protection Manager.
del key <clé partagée>	Supprime la clé de secret partagé.

group <nom groupe>	permet de spécifier un nom de groupe préféré pour le boîtier Enforcer. Par conséquent, il est recommandé d'attribuer un nom de groupe unique pour distinguer les boîtiers Enforcer sur la console Symantec Endpoint Protection Manager.
http <numéro port>	permet de spécifier le protocole HTTP et le numéro de port pour la communication avec Symantec Endpoint Protection Manager. Le protocole par défaut est HTTP. Par défaut, le numéro de port utilisé pour le protocole HTTP est 80.
https <numéro port>	permet de spécifier le protocole HTTPS et le numéro de port pour la communication avec Symantec Endpoint Protection Manager. Vous devriez seulement utiliser cette commande si Symantec Endpoint Protection Manager a été installée pour utiliser le protocole HTTPS. Par défaut, le numéro de port utilisé pour le protocole HTTPS est 443.
clé <nom clé>	permet de spécifier le mot de passe chiffré qui est requis s'il a été spécifié lors de l'installation de Symantec Endpoint Protection Manager.

L'exemple suivant décrit comment configurer un boîtier Enforcer pour communiquer avec Symantec Endpoint Protection Manager à l'adresse IP 192.168.0.64 dans un groupe Enforcer nommé CorpAppliance. Il utilise le protocole HTTP sur le port 80 avec le mot de passe chiffré "security".

```
configure spm ip 192.168.0.64 group CorpAppliance http 80 key security
```

Commandes Console

Les commandes du groupe console de l'interface de ligne de commande du boîtier Enforcer vous permettent de configurer les paramètres de la console.

Toutes les commandes dans ce groupe sont listées et décrites excepté les commandes `exit` et `help` (quitter et aide). La commande `exit` (quitter) ferme le groupe de commandes. La commande `help` (aide) affiche des informations d'aide sur les commandes individuelles du groupe.

Console Baud-rate

La commande console baud-rate (vitesse en bauds de la console) spécifie la vitesse en bauds que la console utilise pour communiquer avec un client par le port série. La vitesse en bauds définie sur le boîtier Enforcer doit correspondre à la vitesse en bauds définie pour cette connexion de communication sur le client.

La vitesse en bauds par défaut est 9600.

La commande console baud-rate utilise la syntaxe suivante :

```
console baud-rate {9600 | 19200 | 38400 | 57600 | 115200}
```

Console SSH

La commande console SSH démarre ou arrête le service distant de connexion SSH. Cette commande spécifie également s'il faut démarrer le service SSH quand l'ordinateur démarre.

La commande console ssh utilise la syntaxe suivante :

```
console ssh {start | stop} {off | on}
```

Console SSHKEY

La commande console sshkey définit et supprime la clé publique pour la connexion distante SSH sans mot de passe.

La commande console sshkey utilise la syntaxe suivante :

```
console sshkey set | delete
```

Exemple :

```
Enforcer(console)# sshkey set

Enforcer(console)# sshkey delete
```

Console Show

La commande console show (afficher console) affiche les paramètres de configuration de console.

La commande console show utilise la syntaxe suivante :

```
show
```

Voici un exemple de syntaxe pour la commande console show :

```
Enforcer# console show
Serial Port Number:  1
Baud Rate:       9600
Flow Control:     NONE
Console Width:     80
Console Height:    24
```

Commandes debug

Les commandes de ce groupe permettent à l'utilisateur de configurer les paramètres de débogage d'Enforcer et le transfert de fichiers de débogage en format normal ou compressé.

Toutes les commandes dans ce groupe sont listées excepté les commandes `exit` et `help` (quitter et aide). La commande `exit` (quitter) ferme le groupe de commandes. La commande `help` (aide) affiche des informations d'aide sur les commandes individuelles du groupe.

Debug Destination

La commande debug destination (emplacement de débogage) permet de définir où un boîtier Enforcer peut enregistrer les fichiers de débogage.

La commande debug destination utilise la syntaxe suivante :

```
destination {both | disk | memory}
```

où :

Both (les deux)	enregistre les fichiers de débogage dans la mémoire et sur le disque. Il s'agit du paramètre both.
Disk (disque)	enregistre les fichiers de débogage sur le disque dur seulement.
Memory (mémoire)	enregistre les fichiers de débogage dans la mémoire seulement.

Debug Level

La commande debug level (niveau de débogage) configure le niveau des informations de débogage stockées par Enforcer.

La commande debug level utilise la syntaxe suivante :

```
level {disabled | fatal | error | information | support | engineer}
```

où :

disabled (désactivé)	n'enregistre pas les informations de débogage
fatal	active le débogage et définit le niveau sur FATAL (enregistre seulement les messages de débogage de type fatal)

error (erreur)	active le débogage et définit le niveau sur ERROR (enregistre les messages de débogage de type fatal et error) L'argument par défaut est défini sur error.
information	active le débogage et définit le niveau sur INFORMATION (enregistre les messages de débogage de type fatal, error et information)
support (prise en charge)	active le débogage et définit le niveau sur SUPPORT (enregistre les messages de débogage de type fatal, error, information et support)
engineer (ingénieur)	active le débogage et définit le niveau sur ENGINEER (enregistre tous les messages de débogage)

Debug Show

La commande debug show (affficher le débogage) affiche la configuration des paramètres de débogage.

La commande debug show utilise la syntaxe suivante :

```
show [compress | destination | file |
files | kernel | kernel live |
level | user | user live | ymodem]
```

où :

compress (compresser)	indique si la compression est activée
destination	affiche la destination de débogage
file (fichier)	affiche le nom de fichier de débogage spécifié
files (fichiers)	liste tous les fichiers de débogage
kernel (noyau)	affiche le fichier de débogage du noyau
kernel_live	affiche le fichier de débogage du noyau avec live update
user (utilisateur)	affiche le fichier de débogage de l'utilisateur
user_live	affiche le fichier de débogage de l'utilisateur avec live update
ymodem	affiche le paramètre de protocole YMODEM

Debug upload

La commande debug upload (charger le débogage) utilise le protocole tftp pour transférer un fichier de débogage d'un boîtier Enforcer vers un hôte à distance.

La commande debug upload utilise la syntaxe suivante :

```
debug upload tftp <adresse_ip>nom_fichier<nom_fichier>
```

Exemple :

```
Enforcer# debug upload tftp 10.200.39.251 filename debug_file
```

Commandes MAB

Les commandes mab vous permettent d'appliquer une fonctionnalité MAB (Media Control access (MAC) Authentication Bypass) avec un boîtier LAN Enforcer sur les commutateurs compatibles 802.1x suivants :

- Commutateur de la gamme Cisco Catalyst 3550
- Extreme Networks
- Commutateur de la gamme Hewlett-Packard ProCurve 2600
- Foundry Networks
- Quand un boîtier LAN Enforcer reçoit une demande MAB, il recherche d'abord l'adresse dans la base de données MAB locale. Si l'entrée existe dans la base de données MAB locale, le boîtier LAN Enforcer authentifie le client en fonction du modèle de commutateur compatible 802.1x. Si une entrée est introuvable dans la base de données MAB locale, le boîtier LAN Enforcer essaye de se connecter à un serveur LDAP disponible.
  Si aucun serveur LDAP n'est disponible pour authentifier l'adresse MAC d'un client ou si l'adresse MAC d'un client n'est pas disponible dans la base de données du serveur LDAP, le boîtier LAN Enforcer essaye de se connecter à un serveur RADIUS disponible. Dès que le boîtier LAN Enforcer reçoit le résultat d'authentification, il envoie un message au serveur RADIUS pour accepter ou rejeter le paquet. Le boîtier LAN Enforcer termine alors la session d'authentification.

Commande MAB disable

La commande MAB disable permet de désactiver la fonctionnalité MAB (MAC Authentication Bypass) sur un boîtier LAN Enforcer.

La commande MAB disable utilise la syntaxe suivante (boîtier LAN Enforcer seulement) :

```
mab disable
```

L'exemple suivant explique comment désactiver la fonctionnalité MAB (MAC Authentication Bypass) sur un boîtier LAN Enforcer :

```
Enforcer: mab
Enforcer(mab)#disable
```

Commande MAB enable

La commande MAB enable permet d'activer la fonctionnalité MAB (MAC Authentication Bypass) sur les boîtiers LAN Enforcer.

La commande MAB enable utilise la syntaxe suivante (boîtier LAN Enforcer seulement) :

```
mab enable
```

L'exemple suivant explique comment activer la fonctionnalité MAB (MAC Authentication Bypass) sur un boîtier LAN Enforcer :

```
Enforcer: mab
Enforcer(mab)#enable
```

Commandes MAB LDAP

Les commandes MAB LDAP permettent d'établir la communication entre un boîtier LAN Enforcer et un serveur LDAP. Après avoir établi la communication entre ces deux périphériques, vous pouvez activer la fonctionnalité MAB (MAC Authentication Bypass) pour authentifier les clients à l'aide de la base de données sur un serveur LDAP au lieu de la base de données MAB locale sur un boîtier LAN Enforcer.

Commande MAB LDAP disable

La commande MAB LDAP disable (désactiver LDAP MAB) permet de désactiver la fonction MAB (MAC Authentication Bypass) sur un serveur LDAP au lieu d'un boîtier LAN Enforcer.

La commande MAB LDAP disable utilise la syntaxe suivante (boîtier LAN Enforcer seulement) :

```
mab ldap disable
```

L'exemple suivant explique comment désactiver la fonction MAB (MAC Authentication Bypass) sur un serveur LDAP au lieu d'un boîtier LAN Enforcer :

```
Enforcer:# mab
Enforcer(mab):# ldap disable
```

Commande MAB LDAP enable

La commande MAB LDAP enable (activer LDAP MAB) permet d'activer la fonction MAB (MAC Authentication Bypass) sur un serveur LDAP au lieu d'un boîtier LAN Enforcer.

La commande MAB LDAP enable utilise la syntaxe suivante (boîtier LAN Enforcer seulement) :

```
mab ldap enable
```

L'exemple suivant explique comment activer la fonction MAB (MAC Authentication Bypass) sur un serveur LDAP au lieu d'un boîtier LAN Enforcer :

```
Enforcer:# mab
Enforcer(mab):# ldap enable
```

Commande MAB LDAP host

La commande MAB LDAP host (hôte MAB LDAP) spécifie le nom d'hôte d'un serveur LDAP si vous prévoyez d'authentifier des clients à l'aide de la fonction MAB (MAC Authentification Bypass) sur un serveur LDAP au lieu d'un boîtier LAN Enforcer.

La commande MAB LDAP host utilise la syntaxe suivante (boîtier LAN Enforcer seulement) :

```
mab ldap host chaîne
```

où :

chaîne représente le nom d'hôte d'un serveur LDAP désigné avec lequel les boîtiers LAN Enforcer doivent établir une connexion.

L'exemple suivant explique comment spécifier le nom d'hôte d'un serveur LDAP si vous prévoyez d'authentifier des clients à l'aide de la fonction MAB (MAC Authentification Bypass) sur un serveur LDAP au lieu d'un boîtier LAN Enforcer :

```
Enforcer: mab
Enforcer(mab): ldap host www.symantec.com
```

Commande MAB LDAP password

La commande MAB LDAP password (mot de passe LDAP MAB) spécifie le mot de passe d'un serveur LDAP si vous prévoyez d'authentifier des clients à l'aide de la

fonction MAB (MAC Authentification Bypass) sur un serveur LDAP au lieu d'un boîtier LAN Enforcer.

La commande MAB LDAP password utilise la syntaxe suivante (boîtier LAN Enforcer seulement) :

```
mab ldap password chaîne
```

où :

chaîne représente le mot de passe qui permet au boîtier LAN Enforcer de se connecter à un serveur LDAP désigné.

L'exemple suivant explique comment spécifier le mot de passe d'un serveur LDAP si vous prévoyez d'authentifier des clients à l'aide de la fonction MAB (MAC Authentification Bypass) sur un serveur LDAP au lieu d'un boîtier LAN Enforcer :

```
Enforcer: mab
Enforcer(mab): ldap password symantec
```

Commande MAB LDAP port

La commande MAB LDAP port (port MAB LDAP) spécifie le numéro de port sur un serveur LDAP si vous prévoyez d'authentifier des clients à l'aide de la fonction MAB (MAC Authentification Bypass) sur un serveur LDAP au lieu d'un boîtier LAN Enforcer.

La commande MAB LDAP port utilise la syntaxe suivante (boîtier LAN Enforcer seulement) :

```
ldap enable | disable | host <nom_hôte> |
password <chaîne> | port <nombre>
```

où :

disable (désactiver)	Désactive la fonction de recherche du module d'application Enforcer MAB LDAP
enable (activer)	Active la fonction de recherche du module d'application Enforcer MAB LDAP
host	Configure l'hôte du serveur LDAP
mot de passe	Configure la clé pour accéder au serveur LDAP
port	Configure le port du serveur LDAP

L'exemple suivant explique comment spécifier le numéro de port sur un serveur LDAP si vous prévoyez d'authentifier des clients à l'aide de la fonction MAB (MAC Authentification Bypass) sur un serveur LDAP au lieu d'un boîtier LAN Enforcer :

```
Enforcer: mab
Enforcer(mab): ldap port 45298
```

Commande MAB show

La commande mab show (afficher mab) vous permet d'afficher les informations suivantes :

- Etat d'activation de la fonction MAB (MAC Authentication Bypass).
- Etat d'activation de la consultation de la base de données MAC LDAP sur le serveur LDAP.
- Nom d'hôte d'un serveur LDAP
- Numéro de port d'un serveur LDAP
- Mot de passe pour un serveur LDAP

La commande mab show utilise la syntaxe suivante :

```
show [ldap]
```

où :

ldap	Affiche la configuration de serveur LDAP

```
Enforcer(mab)# show

MAC Address Bypass:             Disable
MAC LDAP lookup:                Disable
LDAP server host:               www.symantec.com
LDAP server port:               1283
LDAP server password:           symantec
```

Commandes du groupe Monitor

La commande monitor (de contrôle) vous permet d'afficher les informations suivantes sur un client géré ou autonome :

- adresse IP
- Nom d'hôte

- Nom d'utilisateur (Gateway Enforcer uniquement)
- ID de politique
- Adresse MAC (DHCP Enforcer uniquement)

Pour exécuter l'une des commandes du groupe monitor, vous devez être connecté en tant que superutilisateur.

Commande monitor refresh

La commande monitor refresh (actualiser le contrôle) met à jour les informations sur le client (Gateway et DHCP Enforcer uniquement).

Pour exécuter cette commande, vous devez être connecté en tant que superutilisateur.

La commande monitor refresh utilise la syntaxe suivante :

```
monitor refresh
```

Commande monitor show

La commande montor show vous permet d'afficher différents types d'informations. Le paramètre par défaut est d'afficher toutes les informations de contrôle disponibles.

Commande monitor show blocked-hosts

La commande monitor show blocked-hosts (afficher hôtes bloqués) affiche l'adresse IP d'un client bloqué, le nom d'hôte, le nom d'utilisateur, le profil client, le profil requis, l'état de blocage et l'état d'intégrité d'hôte (boîtier Gateway Enforcer seulement). Un client bloqué inclut des informations sur les utilisateurs gérés et les clients connectés.

Cette commande affiche pour un client bloqué l'adresse IP, le nom d'hôte, le nom d'utilisateur, l'adresse MAC, le profil client, le profil requis, l'état de blocage et l'état d'intégrité d'hôte (boîtier DHCP Enforcer seulement).

Pour exécuter cette commande, vous devez être connecté en tant que superutilisateur.

La commande monitor show blocked-hosts utilise la syntaxe suivante (boîtiers Gateway Enforcer et DHCP Enforcer seulement) :

```
monitor [show blocked-hosts {all | ip <adresse IP>}]
```

où :

all	Affiche pour tous les clients bloqués les adresses IP, les noms d'hôte, les noms d'utilisateur, les profils client, les profils requis, l'état de blocage et l'état d'intégrité d'hôte sur les boîtiers Gateway Enforcer et DHCP Enforcer. En outre, toutes les adresses MAC des clients bloquées apparaissent sur un DHCP Enforcer.
ip <adresse_ip>	Affiche pour un client bloqué l'adresse IP, le nom d'hôte, le nom d'utilisateur, le profil client, le profil requis, l'état de blocage et l'état d'intégrité d'hôte sur les boîtiers Gateway Enforcer et DHCP Enforcer. en outre, l'adresse MAC d'un client bloqué apparaît sur un DHCP Enforcer.

L'exemple suivant fournit des informations sur l'état d'un client bloqué sur un Gateway Enforcer :

```
monitor
show blocked-hosts ip 100.0.0.242

Authentication blocked host statistics
IP address:       100.0.0.242
Hostname:         SNA-7D7911D97BA
Username:         guest
Client Profile:   Valid-DB1B 12/29/2007 12:35:00
Required Profile: Valid-DB1B 12/29/2007 12:35:00
Blocked:          Host Integrity or Policy check failed
HI status:        Host Integrity check failed.
```

L'exemple suivant fournit des informations sur l'état d'un client bloqué sur un DHCP Enforcer :

```
monitor
show blocked-hosts ip 100.0.0.242

Authentication blocked host statistics
IP address:       100.0.0.242
Hostname:         SNA-7D7911D97BA
Username:         guest
MAC address:      0-12-3f-10-a5-99
Client Profile:   Valid-DB1B 12/29/2007 12:35:00
Required Profile: Valid-DB1B 12/29/2007 12:35:00
Blocked:          Host Integrity or Policy check failed
HI status:        Host Integrity check failed.
```

Commande monitor show connected-guests

La commande monitor show connected-guests (afficher invités connectés) affiche l'adresse IP, le nom d'hôte, le nom d'utilisateur et l'ID politique d'un invité connecté ou à la demande (Gateway Enforcer seulement). En outre, cette commande affiche l'adresse MAC des clients non conformes pour un DHCP Enforcer.

Un invité connecté ou un client à la demande prend en charge le logiciel client Symantec Network Access Control sur les plates-formes Windows et Macintosh. L'invité connecté ou un client à la demande doit avoir été authentifié ou configuré en tant que client approuvé dans Symantec Endpoint Protection Manager. Sinon la commande monitor show connected-guests n'affiche aucune information sur les clients à la demande.

Pour exécuter cette commande, vous devez être connecté en tant que superutilisateur.

La commande monitor show connected-guests utilise la syntaxe suivante (boîtiers Gateway Enforcer et DHCP Enforcer) :

```
monitor [show connected-guests { all | ip
<adresse IP>}]
```

où :

all	Affiche pour tous les clients bloqués les adresses IP, les noms d'hôte, les noms d'utilisateur, les profils client, les profils requis, l'état de connexion et l'état d'intégrité d'hôte sur les boîtiers Gateway Enforcer et DHCP Enforcer. En outre, toutes les adresses MAC des clients bloquées apparaissent sur un DHCP Enforcer.
ip <adresse_ip>	Affiche pour un client bloqué l'adresse IP, le nom d'hôte, le nom d'utilisateur, le profil client, le profil requis, l'état de connexion et l'état d'intégrité d'hôte sur les boîtiers Gateway Enforcer et DHCP Enforcer. en outre, l'adresse MAC d'un client bloqué apparaît sur un DHCP Enforcer.

L'exemple suivant fournit des informations sur l'état d'un client bloqué sur un Gateway Enforcer :

```
monitor
show connected-guests ip 100.0.0.242

Authentication connected guests statistics
IP address:       100.0.0.242
Hostname:         SNA-7D7911D97BA
Username:         guest
```

```
Client Profile:   Valid-DB1B 12/29/2007 12:35:00
Required Profile: Valid-DB1B 12/29/2007 12:35:00
Connected:        Authenticated
HI status:        Host Integrity check passed.
```

L'exemple suivant fournit des informations sur l'état d'un client bloqué sur un DHCP Enforcer :

```
monitor
show connected-guests ip 100.0.0.242

Authentication connected guests statistics
IP address:       100.0.0.242
Hostname:         SNA-7D7911D97BA
Username:         guest
MAC address:      0-12-3f-10-a5-99
Client Profile:   Valid-DB1B 12/29/2007 12:35:00
Required Profile: Valid-DB1B 12/29/2007 12:35:00
Connected:        Authenticated
HI status:        Host Integrity check passed.
```

Commande monitor show connected-users

La commande monitor show connected-users (afficher utilisateurs connectés) affiche l'adresse IP, le nom d'hôte, le nom d'utilisateur et l'ID de politique de l'utilisateur connecté ou du client réseau (boîtier Gateway Enforcer seulement). En outre, cette commande affiche l'adresse MAC d'un utilisateur connecté ou d'un client géré pour un module DHCP Enforcer.

Un utilisateur connecté ou un client géré prend en charge les logiciels client Symantec Endpoint Protection et Symantec Network Access Control. L'utilisateur connecté ou le client géré doit avoir été authentifié. Sinon, la commande monitor show connected-users n'affiche aucune information sur le client.

Vous devez être connecté à une console Gateway ou DHCP Enforcer en tant que superutilisateur pour pouvoir exécuter cette commande.

La commande monitor show connected-users utilise la syntaxe suivante (boîtiers Gateway Enforcer et DHCP Enforcer) :

```
monitor [show connected-user {all|ip <adresse ip>}]
```

où :

all	Affiche pour tous les clients connectés les adresses IP, les noms d'hôte et les ID de politique (boîtiers Gateway et DHCP Enforcer). Les adresses MAC de tous les clients non conformes sont également affichées (boîtier DHCP Enforcer seulement).
ip <adresse_ip>	Affiche pour un client connecté l'adresse IP, le nom d'hôte et l'ID de politique (boîtiers Gateway Enforcer et DHCP Enforcer). L'adresse MAC d'un client non conforme est également affichée (boîtier DHCP Enforcer seulement).

Commandes SNMP

Les commandes SNMP suivantes vous permettent du travail avec le protocole SNMP.

Commande SNMP disable

Vous permet de désactiver la fonction de protocole SNMP.

La commande SNMP disable utilise la syntaxe suivante :

```
snmp disable
```

L'exemple suivant montre comment désactiver SNMP :

```
Enforcer(snmp)#disable
```

Commande SNMP enable

Vous permet d'activer la fonction de protocole SNMP.

La commande SNMP enable utilise la syntaxe suivante :

```
snmp enable
```

L'exemple suivant montre comment activer SNMP :

```
Enforcer(snmp)#enable
```

Commande SNMP heartbeat

Vous permet de définir le battement de la fonction de protocole SNMP.

La commande SNMP heartbeat utilise la syntaxe suivante :

```
heartbeat <secondes>
```

où :

Les secondes représentent le temps, entre 30 et 86400.

Le nombre de secondes par défaut est 30.

L'exemple suivant montre comment définir le battement SNMP sur 100 secondes :

```
Enforcer(snmp)#heartbeat 100
```

Commande SNMP receiver

Vous permet d'ajouter ou supprimer un récepteur SNMP.

La commande SNMP receiver utilise la syntaxe suivante :

```
receiver {add <nom_hôte>[:<port>] | delete <nom_hôte>[:<port>]
```

où :

add (ajouter)	Ajoute un récepteur SNMP au format <hôte[:port]>
delete (supprimer)	Supprime un récepteur SNMP au format <hôte[:port]>

L'exemple suivant montre comment ajouter ou supprimer un récepteur SMTP :

```
Enforcer(snmp)# receiver add abc

Enforcer(snmp)# receiver delete abc
```

Commande SNMP show

Montre la configuration et l'état SNMP.

La commande SNMP show utilise la syntaxe suivante :

```
show configure | status
```

Les exemples suivants montrent comment utiliser la commande show :

```
Enforcer(snmp)#show configure

SNMP Trap       : ENABLED
Heartbeat       : 30       second(s)
Timeout         : 1        second(s)
Retry           : 0        time(s)
Trap Receiver   : abc:162
```

```
Enforcer(snmp)#show status
CPU usage 3%
Memory usage 97%
lo rec/trans:9386498/9386498 byte
eth0 rec/trans:704234599/288693960 byte
eth1 rec/trans:228648902/179921169 byte
Connecté à Symantec Endpoint Protection Manager
```

Commande SNMP trap

Vous permet de définir le nombre de tentatives SNMP et la valeur du délai.

La commande SNMP trap utilise la syntaxe suivante :

```
trap retry <fois> | timeout <secondes>
```

où :

retry	Nombre de tentatives
timeout	Paramètre de délai en secondes

L'exemple suivant montre comment définir le nombre de tentatives et le délai SNMP :

```
Enforcer(snmp)# trap retry 3
Enforcer(snmp)# trap timeout 3
```

Commandes on-demand

Les commandes on-demand dans l'interface de ligne de commande de boîtier Enforcer vous permettent de configurer le téléchargement automatique du client Symantec Network Access Control On-Demand sur les plates-formes Windows et Macintosh. Vous pouvez uniquement exécuter les commandes on-demand sur les boîtiers Gateway Enforcer et DHCP Enforcer.

Toutes les commandes dans ce groupe sont décrites excepté les commandes `exit` et `help`. La commande `exit` (quitter) ferme le groupe de commandes. La commande `help` affiche des informations d'aide sur les commandes individuelles du groupe.

Commandes on-demand authentication

La plupart des entreprises peuvent vouloir configurer l'authentification pour les clients Symantec Network Access Control On-Demand.

Si vous voulez authentifier les clients à la demande Symantec Network Access Control sur les plates-formes Windows et Macintosh, vous pouvez utiliser l'un des types de bases de données suivants :

- Base de données locale qui réside sur un boîtier Gateway ou DHCP Enforcer.
  Si vous ne prenez pas en charge un serveur Active Directory dans un environnement réseau, vous pouvez utiliser la base de données intégrée locale pour ajouter des noms d'utilisateur et des mots de passe pour différents utilisateurs.
- Serveur Active Directory
  Vous devez vous connecter à Microsoft Windows Server 2003 Active Directory.

Tableau 11-3 fournit des informations au sujet de la commande on-demand authentication (authentification à la demande).

Tableau 11-3 Arguments de la commande on-demand authentication

Commande	Description
ad	Active l'authentification par le biais d'un serveur Active Directory au lieu de la base de données locale intégrée sur les boîtiers Gateway et DHCP Enforcer. Se reporter à "Commandes on-demand authentication ad" à la page 297.
enable	Active l'authentification des clients Symantec Network Access Control On-Demand sur les boîtiers Gateway et DHCP Enforcer. Si vous activez l'authentification sur le module d'application Enforcer, un utilisateur final doit passer l'authentification (entrer le nom d'utilisateur et le mot de passe corrects) avant le téléchargement des clients à la demande Symantec Network Access Control. Se reporter à "Commande on-demand authentication enable" à la page 299.
disable	Désactive l'authentification des clients Symantec Network Access Control On-Demand sur les boîtiers Gateway et DHCP Enforcer. Les utilisateurs finaux peuvent déclencher le téléchargement automatique des clients à la demande Symantec Network Access Control sur un ordinateur client sans authentification. Se reporter à "Commande on-demand authentication disable" à la page 298.

Commande	Description
local-db	Désactive l'authentification via l'utilisation de la base de données locale intégrée au lieu d'un serveur Active Directory sur les boîtiers Gateway et DHCP Enforcer. Se reporter à "Commandes on-demand authentication local-db" à la page 299.
show	Liste les informations d'état au sujet des différentes options et des différents arguments de la commande d'authentification.
upload	Envoyer à un serveur des fichiers liés à l'authentification.

Commandes on-demand authentication ad

Si un réseau d'entreprise prend en charge Microsoft Windows Serveur Active Directory 2003, vous pouvez authentifier des utilisateurs avec un serveur d'Active Directory. Sinon, vous devez installer la base de données à bord pour authentifier des utilisateurs.

Commande on-demand authentication ad disable

La commande on-demand authentication ad disable (désactiver l'authentification Active Directory à la demande) utilise la syntaxe suivante pour désactiver l'authentification des clients avec Microsoft Windows Server 2003 Active Directory :

Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur.

Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.

```
on-demand authentication ad disable
```

L'exemple suivant décrit comment désactiver l'authentification pour un client à la demande avec un serveur Microsoft Windows Server 2003 Active Directory :

```
on-demand authentication ad disable
```

Commande on-demand authentication ad domain

La commande on-demand authentication ad domain (domaine Active Directory d'authentification à la demande) utilise la syntaxe suivante pour spécifier l'ID de domaine ou l'adresse d'ID de domaine d'un serveur Microsoft Windows Server 2003 Active Directory :

```
on-demand authentication ad domain
<Nom de serveur de domaine Active Directory> |
  <Adresse IP de serveur de domaine Active Directory>
```

où :

Nom de serveur de domaine Active Directory	représente le nom de domaine du serveur Microsoft Windows Server 2003 Active Directory.
Adresse IP de serveur de domaine Active Directory	représente l'adresse IP de domaine du serveur Microsoft Windows Server 2003 Active Directory.

L'exemple suivant décrit comment spécifier l'ID de domaine d'un serveur Microsoft Windows Server 2003 Active Directory :

```
Enforcer# on-demand
Enforcer (on-demand)# authentication
Enforcer (authentication)# ad domain symantec.com
```

où :

symantec.com représente le nom de domaine du serveur Active Directory Microsoft Windows Server 2003.

Commande on-demand authentication ad enable

La commande on-demand authentication ad enable (activer l'authentification Active Directory à la demande) utilise la syntaxe suivante pour activer l'authentification des utilisateurs finaux avec un serveur Microsoft Windows Server 2003 Active Directory :

```
on-demand authentication ad enable
```

L'exemple suivant décrit comment activer l'authentification pour un client à la demande avec un serveur Microsoft Windows Server 2003 Active Directory :

```
Enforcer# on-demand
Enforcer (on-demand)# authentication
Enforcer (authentication)# ad enable
```

Commande on-demand authentication disable

Vous pouvez arrêter le processus d'authentification (daemon auth) sur la console d'un boîtier Gateway ou DHCP pour un client à la demande Symantec Network Access Control.

La commande on-demand authentication disable (désactiver l'authentification à la demande) utilise la syntaxe suivante :

```
on-demand authentication disable
```

Vous devez être connecté à une console Gateway ou DHCP Enforcer en tant que superutilisateur pour pouvoir exécuter cette commande.

Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.

L'exemple suivant décrit comment désactiver l'authentification pour un client Symantec Network Access Control On-Demand sur la console d'un boîtier Gateway ou DHCP Enforcer :

```
Enforcer# on-demand
Enforcer (on-demand)# authentication disable
```

Commande on-demand authentication enable

Vous pouvez démarrer le processus d'authentification — le daemon auth — sur la console d'un boîtier Gateway ou DHCP pour un client à la demande Symantec Network Access Control.

La commande on-demand authentication enable utilise la syntaxe suivante :

```
on-demand authentication enable
```

Vous devez être connecté à une console Gateway ou DHCP Enforcer en tant que superutilisateur pour pouvoir exécuter cette commande.

Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.

L'exemple suivant décrit comment activer l'authentification pour un client à la demande Symantec Network Access Control sur la console d'un boîtier Gateway ou DHCP Enforcer :

```
Enforcer# on-demand
Enforcer (on-demand)# authentication enable
```

Commandes on-demand authentication local-db

Si un réseau d'entreprise ne prend pas en charge Microsoft Windows Serveur Active Directory 2003, vous devez authentifier des utilisateurs avec la base de données intégrée que vous pouvez installer sur un boîtier Gateway Enforcer ou DHCP Enforcer.

Commande on-demand authentication local-db add

Si vous devez authentifier des utilisateurs avec la base de données intégrée, vous devez ajouter des comptes utilisateur pour chaque client sur un boîtier Gateway ou DHCP Enforcer.

Se reporter à "Configurer l'authentification avec une base de données locale intégrée" à la page 223.

Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur.

Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.

La commande on-demand local-db authentication add utilise la syntaxe suivante pour ajouter un compte utilisateur à la base de données intégrée que vous avez installée sur un boîtier Gateway ou DHCP Enforcer :

```
on-demand authentication local-db add user nom_utilisateur
```

où :

nom_utilisateur représentent un compte utilisateur que vous pouvez ajouter à la base de données intégrée.

La commande on-demand authentication local-db add user utilise la syntaxe suivante :

```
Enforcer# on-demand
Enforcer (on-demand)# authentication
Enforcer (authentication)# local-db add user jim
```

Commande on-demand authentication local-db disable

La commande on-demand local-db authentication disableutilise la syntaxe suivante pour désactiver la base de données intégrée que vous avez configurée sur un boîtier Gateway ou DHCP Enforcer :

```
on-demand authentication local-db disable
```

La commande on-demand authentication local-db enable utilise la syntaxe suivante :

```
Enforcer# on-demand
Enforcer (on-demand)# authentication
Enforcer (authentication)# local-db disable
```

Commande on-demand authentication local-db enable

La commande on-demand local-db authentication enable utilise la syntaxe suivante pour activer la base de données intégrée que vous avez configurée sur un boîtier Gateway ou DHCP Enforcer :

```
on-demand authentication local-db enable
```

La commande on-demand authentication local-db enable utilise la syntaxe suivante :

```
Enforcer# on-demand
Enforcer (on-demand)# authentication
Enforcer (authentication)# local-db enable
```

Commandes on-demand authentication local-db username

Les commandes on-demand local-db authentication username vous permettent d'ajouter, de supprimer et de modifier des noms d'utilisateur :

```
local-db add username <chaîne> password <chaîne>
local-db delete username <chaîne>
local-db edit username <chaîne> password <chaîne>
local-db enable |disable | clear
```

où :

add (ajouter)	Crée un nouveau compte utilisateur dans la base de données locale
clear	Nettoie tous les comptes utilisateur de la base de données locale
delete (supprimer)	Supprime un utilisateur existant de la base de données locale
disable (désactiver)	Désactive l'authentification de la base de données locale
edit	Modifie un compte utilisateur existant
enable (activer)	Active l'authentification de la base de données locale

L'exemple suivant montre comment configurer l'authentification de la base de données locale pour un client à la demande Symantec Network Access Control sur la console d'un boîtier Gateway ou DHCP Enforcer :

```
Enforcer# on-demand
Enforcer(on-demand)#authentication
Enforcer(authentication)# local-db disable
Local database authentication is disabled.

Enforcer(authentication)# local-db enable
Local database authentication is enabled.

Enforcer(authentication)# local add username test password test

Enforcer(authentication)# local-db delete username test
Your action will delete the user account " test " permanently.
  Please confirm. [Y/N]y

Enforcer(authentication)# local-db edit username test password b

Enforcer(authentication)# local-db clear
Notice that your action will remove ALL user account permanently!
  Please confirm. [Y/N]y
```

Commande on-demand banner

Vous pouvez modifier le texte de la bannière par défaut sur la page d'accueil des clients à la demande Symantec Network Access Control.

Vous devez être connecté à une console Gateway ou DHCP Enforcer en tant que superutilisateur pour pouvoir exécuter cette commande.

Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.

La commande on-demand banner (bannière à la demande) utilise la syntaxe suivante :

```
Enforcer(on-demand)# banner
Type the new banner text that cannot exceed 1024
characters, and press Ctrl-D to end:
```

A l'invite de la commande du boîtier Enforcer, remplacez le texte par défaut de la bannière par un texte de votre choix.

Le texte de la bannière est limité à 1024 caractères.

Commande on-demand client-group

La commande on-demand client-group (groupe client à la demande) vous permet de configurer le nom d'un groupe Enforcer sur la console d'un boîtier Gateway ou

DHCP Enforcer. Vous n'avez pas besoin de configurer le nom du module d'application Enforcer sur la console Enforcer si vous l'avez déjà configuré sur la console Symantec Endpoint Protection Manager.

Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur.

La commande on-demand client-group utilise la syntaxe suivante :

```
Enforcer# on-demand
Enforcer(on-demand)# client-group <nom_groupe>enable|disable
```

L'exemple suivant décrit comment ajouter le nom d'un groupe de boîtiers Enforcer sur la console d'un boîtier Gateway ou DHCP Enforcer :

```
Enforcer# on-demand
Enforcer(on-demand)# client-group mon entreprise/à la demande
```

où :

nom_groupe représente le nom du groupe Enforcer sur la console Symantec Endpoint Protection Manager pour un groupe particulier d'ordinateurs client à la demande.

Commandes on-demand dot1x

Vous devez configurer la commande dot1x sur la console d'un boîtier Gateway ou DHCP Enforcer si l'utilisateur final utilise l'authentification dot1x dans l'environnement de réseau local

Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur.

Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.

Commandes on-demand dot1x certificate

La commande on-demand dot1x certificate (certificat dot1x à la demande) permet d'accéder à un certain nombre de commandes pour effectuer les tâches suivantes :

- Importer et configurer un certificat de serveur racine pour authentifier un client à la demande avec un commutateur compatible 802.1x.
- Supprimer un certificat de serveur racine.
- Afficher les critères de configuration du certificat de serveur racine.

Vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur pour pouvoir exécuter cette commande.

Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.

La commande on-demand dot1x certificate utilise la syntaxe suivante :

```
on-demand dot1x certificate
{import| remove | show}
```

où :

import (importer)	Importe un certificat de serveur racine depuis un emplacement indiqué.
remove (supprimer)	Supprime un certificat de serveur racine pour un protocole 802.1x TLS (transport layer security).
show (afficher)	Affiche les paramètres de configuration d'un certificat de serveur racine pour un protocole 802.1x TLS (transport layer security).

L'exemple suivant décrit comment accéder à la commande on-demand dot1x certificate :

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x
Enforcer(dot1x)# certificate
Enforcer(certificate)#
```

Commande on-demand dot1x certificate import

La commande on-demand dot1x certificate import (importer certificat dot1x à la demande) permet d'importer et de configurer un certificat de serveur racine pour authentifier un client à la demande avec un commutateur compatible 802.1x.

Vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur pour pouvoir exécuter cette commande.

Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.

La commande on-demand dot1x certificate import utilise la syntaxe suivante :

```
import tftp <adresse_ip> username <chaîne>
password <chaîne> root-cert <chaîne> user-cert <chaîne>
```

où :

import tftp <adresse_ip>	Représente l'adresse IP de l'ordinateur depuis lequel le boîtier Enforcer importe le certificat.

password <chaîne>	représente le mot de passe à configurer pour se connecter au serveur TFTP.
username <chaîne>	représente le nom d'utilisateur de connexion à utiliser pour la connexion à l'ordinateur client à la demande.
user-cert <chaîne>	représente le nom du certificat d'utilisateur à importer.
root-cert <chaîne>	représente le nom du certificat de serveur à importer.

L'exemple suivant décrit comment importer et configurer un certificat de serveur racine pour authentifier un client à la demande avec un commutateur compatible 802.1x :

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x
Enforcer(dot1x)# certificate
Enforcer(certificate)# import tftp:10.200.39.251
password symantec username janedoe user-cert name.pfx
root-cert name.cer
```

où :

10.200.39.251	représente l'ordinateur à partir duquel le boîtier Enforcer importe le certificat.
password symantec	représente le mot de passe à configurer pour se connecter au serveur TFTP.
username janedoe	représente le nom d'utilisateur de connexion à utiliser pour la connexion à l'ordinateur client à la demande.
user-cert name.pfx	représente le nom du certificat d'utilisateur à importer.
root-cert name.cer	représente le nom du certificat de serveur à importer.

Commande on-demand dot1x certificate remove command

La commande on-demand dot1x certificate remove (supprimer certificat dot1x à la demande) permet de supprimer le nom d'un certificat dot1x.

La commande on-demand dot1x certificate remove utilise la syntaxe suivante :

```
on-demand dot1x certificate remove <chaîne>
```

où :

chaîne représente le nom du certificat dot1x que vous voulez supprimer.

L'exemple suivant décrit comment supprimer un certificat dot1x portant le nom de fichier packagelist.

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x
Enforcer(dot1x)# certificate
Enforcer(certificate)# remove packagelist
Are you sure that you want to remove " packagelist "? [Y/N]
Y
```

Commande on-demand dot1x show certificate

La commande on-demand dot1x show certificate (afficher certificat dot1x à la demande) permet d'afficher des informations sur le certificat dot1x.

La commande on-demand dot1x show certificate utilise la syntaxe suivante :

```
on-demand dot1x certificate show
```

L'exemple suivant décrit comment afficher un certificat dot1x.

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x
Enforcer(dot1x)# certificate
Enforcer(certificate)# show
Certificates: packagelist
```

Commande on-demand dot1x peap

La commande on-demand dot1x peap (peap dot1x à la demande) vous permet de configurer un protocole 802.1x PEAP (Protected Extensible Authentication Protocol) pour authentifier les clients à la demande dans le réseau protégé.

Vous devez vous connecter à la console d'un boîtier Gateway ou DHCP Enforce en tant que superutilisateur avant de configurer cette commande.

La commande on-demand dot1x peap utilise la syntaxe suivante :

```
on-demand dot1x peap { cert-svr | fast-reconn| validate-svr | show }
```

L'exemple suivant décrit comment configurer un protocole PEAP 802.1x sur la console d'un boîtier Gateway ou DHCP Enforcer :

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x peap
```

où :

la commande peap spécifie une configuration de protocole PEAP (Protected Extensible Authentication Protocol) en tant que protocole d'authentification dot1x des clients à la demande.

Commande on-demand dot1x peap validate-svr

La commande on-demand dot1x peap validate-svr (valider le serveur peap dot1x à la demande) vous permet d'activer ou désactiver la validation d'un certificat de serveur racine pour une configuration de protocole 802.1x PEAP (Protected Extensible Authentication Protocol).

Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur.

La commande on-demand dot1x peap validate-svr utilise la syntaxe suivante :

```
on-demand dot1x peap validate-svr [enable | disable]
```

L'exemple suivant décrit comment activer la validation d'un certificat de serveur racine pour le protocole PEAP 802.1x sur la console d'un boîtier Gateway ou DHCP Enforcer :

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x
Enforcer(dot1x)# peap validate-svr enable
```

où :

la commande validate-svr enable (activer la validation du serveur) définit la validation d'un certificat de serveur racine pour une configuration de protocole 802.1x PEAP (Protected Extensible Authentication Protocol).

Commande on-demand dot1x peap cert-svr

La commande on-demand dot1x peap cert-svr vous permet d'importer et de configurer un certificat de serveur racine pour un protocole 802.1x PEAP (Protected Extensible Authentication Protocol) pour l'authentification de clients à la demande.

Vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur pour pouvoir exécuter cette commande.

La commande on-demand dot1x peap cert-svr utilise la syntaxe suivante :

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x peap cert-svr
```

L'exemple suivant décrit comment importer et configurer un certificat pour le protocole PEAP 802.1x sur la console d'un boîtier Gateway ou DHCP Enforcer :

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x peap cert-svr
Enforcer(peap)# cert-svr host snac
Enforcer(peap)# cert-svr disable
Enforcer(peap)# cert-svr enable
```

où :

disable	Désactive le serveur de certificat PEAP
enable	Active le serveur de certificat PEAP
host	Définit le nom d'hôte du serveur de certificat PEAP

Commande on-demand dot1x peap fast-reconn

La commande on-demand dot1x peap fastreconn vous permet d'activer ou de désactiver la reconnexion rapide d'une configuration 802.1x PEAP (Protected Extensible Authentication Protocol) pour les clients à la demande.

Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur.

La commande on-demand dot1x peap fastreconn utilise la syntaxe suivante :

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x peap fastreconn {enable|disable}
```

L'exemple suivant décrit comment valider un certificat de serveur racine pour un protocole 802.1x PEAP (Protected Extensible Authentication Protocol) sur la console d'un boîtier Gateway ou DHCP Enforcer :

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x peap fastreconn enable
```

où :

validate-svr enable définit la validation d'un certificat de serveur racine pour une configuration de protocole PEAP 802.1x PEAP.

Commande on-demand dot1x peap show

La commande on-demand dot1x peap show (afficher peap dot1x à la demande) vous permet d'afficher les paramètres de configuration d'une authentification 802.1x PEAP (Protected Extensible Authentication Protocol) pour un client à la demande. Utilisez cette commande pour confirmer que le protocole actif est PEAP.

Vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur pour pouvoir exécuter cette commande.

La commande on-demand dot1x peap show utilise la syntaxe suivante :

```
show
```

L'exemple suivant décrit comment afficher les paramètres de configuration pour une authentification 802.1x PEAP (Protected Extensible Authentication Protocol) sur la console d'un boîtier Gateway ou DHCP Enforcer :

```
Enforcer(peap)# show
PEAP Validate Server Certificate:       DISABLED
PEAP Certificate Server:                DISABLED
PEAP Certificate Server:                snac
PEAP Fast Reconnected:                  ENABLED
```

Commande on-demand dot1x tls

La commande on-demand dot1x tls (tls dot1x à la demande) vous permet de configurer le protocole 802.1x TLS (transport layer security) pour des sessions de client à la demande.

Vous devez vous connecter à la console d'un boîtier Gateway ou DHCP Enforce en tant que superutilisateur avant de configurer cette commande.

La commande on-demand dot1x tls utilise la syntaxe suivante :

```
on-demand dot1x tls {cert-svr | validate-svr | show}
```

L'exemple suivant décrit la syntaxe de la commande on-demand dot1x tls sur la console d'un boîtier Gateway ou DHCP Enforcer :

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x tls
```

où :

la commande tls spécifie une configuration TLS (Transport Layer Security) pour votre configuration de protocole d'authentification dot1x du client à la demande.

Commande on-demand dot1x peap validate-svr

La commande on-demand dot1x tls validate-svr active ou désactive la validation d'un certificat de serveur racine pour une configuration de protocole 802.1x TLS (transport layer security).

Pour pouvoir exécuter cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur.

La commande on-demand configure dot1x tls validate-svr utilise la syntaxe suivante :

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x
Enforcer(dot1x)# tls validate-svr [enable|disable]
```

L'exemple suivant décrit la syntaxe pour la commande on-demand dot1x tls validate-svr sur la console d'un boîtier Gateway ou DHCP Enforcer :

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x tls validate-svr enable
```

où :

la commande validate-svr enable active la validation d'un certificat de serveur racine pour une configuration de protocole 802.1x TLS (transport layer security).

Commande on-demand dot1x tls cert-svr

La commande on-demand dot1x tls cert-svr vous permet d'importer et de configurer un certificat de serveur racine pour un protocole 802.1x TLS (transport layer security) pour l'authentification client à la demande.

Vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur pour pouvoir exécuter cette commande.

La commande on-demand dot1x tls cert-svr utilise la syntaxe suivante :

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x tls cert-svr
```

L'exemple suivant décrit la syntaxe pour la commande on-demand dot1x tls cert-svr sur la console d'un boîtier Gateway ou DHCP Enforcer :

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x
Enforcer(dot1x)# tls
Enforcer(tls)# cert-svr host snac
Enforcer(tls)# cert-svr disable
Enforcer(tls)# cert-svr enable
```

où :

disable	Désactive le certificat TLS
enable	Active le certificat TLS

host	Définit le nom d'hôte du serveur de certificat TLS

Commande on-demand dot1x tls show

La commande on-demand dot1x tls show vous permet d'afficher les paramètres de configuration d'un protocole 802.1x TLS (Transport Layer Security) pour l'authentification client à la demande. Utilisez cette commande pour vous assurer que le certificat de serveur tls est activé.

Vous devez vous connecter à la console d'un boîtier Gateway ou DHCP Enforce en tant que superutilisateur avant de configurer cette commande.

La commande on-demand dot1x tls show utilise la syntaxe suivante :

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x show [tls | peap]
```

L'exemple suivant décrit comment afficher les paramètres de configuration pour une authentification TLS sur la console d'un boîtier Gateway ou DHCP Enforcer :

```
Enforcer(tls)# show
TLS Validate Server Certificate:        DISABLED
TLS Certificate Server:                 ENABLED
TLS Certificate Server:                 snac
```

Commande on-demand dot1x protocol

La commande on-demand dot1x protocol (protocole dot1x à la demande) vous permet de définir le protocole d'authentification actif sur PEAP (Extensible Authentication Protocol) ou TLS (Transport Layer Security) pour authentifier des clients à la demande avec un commutateur compatible 802.1x disposant de ports activés dot1x.

Vous devez vous connecter à la console d'un boîtier Gateway ou DHCP Enforce en tant que superutilisateur avant de configurer cette commande.

La commande on-demand dot1x protocol utilise la syntaxe suivante :

```
on-demand dot1x protocol [tls | peap]
```

L'exemple suivant décrit comment définir le protocole d'authentification actif sur PEAP (Extensible Authentication Protocol) pour authentifier des clients à la demande avec un commutateur compatible 802.1x disposant de ports activés dot1x :

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x
Enforcer(dot1x)# protocol peap
```

L'exemple suivant décrit comment définir le protocole d'authentification actif sur TLS (Transport Layer Security) pour authentifier des clients à la demande avec un commutateur compatible 802.1x disposant de ports activés dot1x :

```
Enforcer# on-demand
Enforcer(on-demand)# dot1x
Enforcer(dot1x)# protocol tls
```

Commande on-demand dot1x default-user

La commande on-demand dot1x default-user vous permet de définir le protocole d'authentification actif sur l'authentification anonyme 802.1x pour client à la demande.

Vous devez être connecté à la console Gateway ou DHCP Enforcer en tant que superutilisateur pour pouvoir exécuter cette commande.

La commande on-demand configure dot1x default-user utilise la syntaxe suivante :

```
default-user username <chaîne> password <chaîne>
```

L'exemple suivant décrit la syntaxe de la commande on-demand dot1x anonymity sur la console d'un boîtier Gateway ou DHCP Enforcer :

```
Enforcer(dot1x)# default-user username snac password snac
```

Commande on-demand dot1x show

La commande on-deman dot1x show vous permet d'afficher les paramètres d'authentification 802.1x pour l'authentification de client à la demande.

Vous devez être connecté à la console Gateway ou DHCP Enforcer en tant que superutilisateur pour pouvoir exécuter cette commande.

La commande on-demand dot1x show utilise la syntaxe suivante :

```
show protocol | peap | tls | certificate | default-user
```

où :

certificate	Liste les certificats d'authentification importés
default-user	Affiche les données d'utilisateur par défaut

peap	Affiche les paramètres d'authentification PEAP
protocol	Affiche le protocole 802.1x actif actuellement
tls	Affiche les paramètres d'authentification Transport Layer Security

L'exemple suivant montre comment afficher le protocole sur la console d'un boîtier Gateway ou DHCP Enforcer :

```
Enforcer(dot1x)# show peap
PEAP Validate Server Certificate:       DISABLED
PEAP Certificate Server:                DISABLED
PEAP Certificate Server:                snac
PEAP Fast Reconnected:                  ENABLED
```

Commande on-demand show

La commande on-demand (afficher à la demande) vous permet d'afficher les paramètres de configuration pour les clients à la demande.

Pour pouvoir configurer cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur.

La commande on-demand show utilise la syntaxe suivante :

```
show [ banner | authentiction | dot1x | status | configuration ]
```

L'exemple suivant décrit la syntaxe de la commande on-demand show sur la console d'un boîtier Gateway ou DHCP Enforcer :

```
Enforcer(on-demand)# show
On-Demand:                              ENABLED
Policy Manager Connected:               YES
Policy Manager Domain ID:               BD751DAE0AC827F7015EFE3443254960
Client Group:                           Mon entreprise/mon groupe

Authentication:                         DISABLED
Local Database Authentication:          DISABLED
Active Directory Authentication:        DISABLED
Active Directory Domain ID:             (NULL)

Active Protocol:                        TLS
```

```
Banner:                                    (NULL)
```

Commande on-demand spm-domain

Vous devez configurer le spm-domain sur une console Gateway ou DHCP Enforcer. Sans cela, l'installation échoue. Le spm-domain peut être automatiquement envoyé à Symantec Endpoint Protection Manager. Si vous avez installé la version 11.2 ou ultérieure de Symantec Endpoint Protection Manager, le spm-domain est automatiquement envoyé à une console Symantec Endpoint Protection Manager. Vous pouvez compléter le spm-domain de manière automatique sur la console de tout boîtier Enforcer.

Toutes les versions de Symantec Endpoint Protection Manager antérieures à 11.2 doivent être configurées avec la commande on-demand spm-domain (domaine spm à la demande) sur une console de boîtier Gateway ou DHCP Enforcer.

Se reporter à "Activation de clients à la demande Symantec Network Access Control pour une connexion temporaire à un réseau " à la page 221.

Le spm-domain apparaît dans la page Clients sur la console Symantec Endpoint Protection Manager.

Consultez le *Guide d'administration pour Symantec Endpoint Protection et Symantec Network Access Control* sur la manière de localiser le spm-domain.

Pour pouvoir configurer cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur.

Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.

La commande on-demand spm-domain utilise la syntaxe suivante :

```
spm-domain {name <chaîne> | id <chaîne>}
```

L'exemple suivant décrit la syntaxe pour la commande on-demand spm-domain sur la console d'un boîtier Gateway ou DHCP Enforcer :

```
Enforcer# on-demand
Enforcer(on-demand)# spm-domain id BD751DAE0AC827F7015EFE3443254960

Enforcer(on-demand)# spm-domain name Default
```

où :

BD751DAE0AC827F7015EFE3443254960 représente le spm-domain situé sur la page Clients de la console Symantec Endpoint Protection Manager.

Commandes on-demand mac-compliance

Vous devez configurer la commande mac-compliance (conformité mac) sur une console de boîtier Gateway ou DHCP Enforcer. De plus, vous n'avez besoin d'exécuter la commande mac-hi que si le client Symantec Network Access Control On-Demand sur une plate-forme Macintosh doit être pris en charge. Sans cela, l'installation échoue.

Pour pouvoir configurer cette commande, vous devez être connecté à la console d'un boîtier Gateway ou DHCP Enforcer en tant que superutilisateur.

Se reporter à "Se connecter à un boîtier Enforcer" à la page 90.

La commande on-demand mac-compliance (conformité mac à la demande) utilise la syntaxe suivante :

```
on-demand mac-compliance {disable| enable| interval| show}
```

où :

disable	Désactive les règles de contrôle de conformité pour le client à la demande Symantec Network Access Control pour Mac
enable	Active les règles de contrôle de conformité pour le client à la demande Symantec Network Access Control pour Mac
interval	Définit l'intervalle de contrôle de conformité (en minutes) pour le client à la demande Symantec Network Access Control pour Mac
show	Affiche la configuration du contrôle de conformité pour le client à la demande Symantec Network Access Control pour Mac
exit	Quitte le paramètre de conformité pour Mac
clear	Efface l'écran
help	Affiche l'aide sur une commande.

Commande on-demand mac-compliance disable

La commande on-demand mac-compliance disable utilise la syntaxe suivante :

```
on-demand mac-compliance disable <numéro_règle>
```

L'exemple suivant décrit la syntaxe pour la commande on-demand mac-compliance disable sur la console d'un boîtier Gateway ou DHCP Enforcer :

```
Enforcer(mac-compliance)# disable 1
```

où l'utilisateur peut sélectionner l'une des règles suivantes par le numéro qui lui est associé, comme indiqué dans l'exemple :

```
<Number>        <State>        <Description>
1               ENABLED        Check system updated
2               ENABLED        Check SAV installed
3               ENABLED        Check SAV auto-protect started
4               ENABLED        Check IP firewall started
5               ENABLED        Check Norton confidential installed
6               ENABLED        Check screen saver inactivity/lock
```

Commande on-demand mac-compliance enable

La commande on-demand mac-compliance enable utilise la syntaxe suivante :

```
on-demand mac-compliance enable <numéro_règle>
```

L'exemple suivant décrit la syntaxe de la commande on-demand mac-compliance enable sur la console d'un boîtier Gateway ou DHCP Enforcer :

```
Enforcer(mac-compliance)# enable 1
```

où l'utilisateur peut sélectionner l'une des règles suivantes par le numéro qui lui est associé, comme indiqué dans l'exemple :

```
<Number>        <State>        <Description>
1               DISABLED       Check system updated
2               DISABLED       Check SAV installed
3               DISABLED       Check SAV auto-protect started
4               DISABLED       Check IP firewall started
5               DISABLED       Check Norton confidential installed
6               DISABLED       Check screen saver inactivity/lock
```

Commande on-demand mac-compliance interval

La commande on-demand mac-compliance interval utilise la syntaxe suivante :

```
on-demand mac-compliance interval <minutes>
```

où :

L'utilisateur peut définir l'intervalle de vérification de la conformité en minutes pour le client à la demande Symantec Network Access Control pour Mac, dans l'intervalle 1 à 14 398 560 minutes.

Commande on-demand mac-compliance show

La commande on-demand mac-compliance show utilise la syntaxe suivante :

```
on-demand mac-compliance show { rules | interval}
```

L'exemple suivant montre la commande on-demand mac-compliance show sur la console d'un boîtier Gateway ou DHCP Enforcer :

```
Enforcer(mac-compliance)# show rules
1       ENABLED         Check system updated
2       ENABLED         Check SAV installed
3       ENABLED         Check SAV auto-protect started
4       ENABLED         Check IP firewall started
5       ENABLED         Check Norton confidential installed
6       ENABLED         Check screen saver inactivity/lock

Enforcer(mac-compliance)# show interval
Interval:       3 (minutes)
```

Chapitre 12

Dépanner un boîtier Enforcer

Ce chapitre traite des sujets suivants :

Dépanner un boîtier Enforcer

Vous pouvez avoir à dépanner des problèmes de transmission avec entre des modules Enforcer et Symantec Endpoint Protection Manager.

Se reporter à "Questions relatives à Enforcer" à la page 323.

Sélectionnez l'une des rubriques ci-après :

- Enforcer ne peut pas s'inscrire sur Symantec Endpoint Protection Manager.
- Retard de connexion réseau via Enforcer.
- Le boîtier Gateway Enforcer bloque des clients.
- Le boîtier DHCP Enforcer bloque des clients.
- Le même boîtier LAN Enforcer s'inscrit deux fois sur la console Symantec Endpoint Protection Manager.
- Evénements de déconnexion client dans le journal client du boîtier LAN Enforcer.
- Le boîtier LAN Enforcer ne commute pas les clients au VLAN approprié.

Rubriques de dépannage générales et problèmes connus

Les rubriques suivantes sont plus larges et peuvent également fournir une aide :

Tableau 12-1

Symptôme	Solution
Le mot de passe racine du module d'application Enforcer est signalé non valide quand il est défini en utilisant l'interface de ligne de commande	Il y a une limite de 128 caractères à la taille des mots de passe. Utilisez un autre mot de passe de longueur plus courte.
La synchronisation échoue lors de l'installation sur Dell 850 d'un module d'applicatoin LAN Enforcer avec NTP activé et configuré	C'est un problème de matériel. La solution de contournement est de désactiver NTP et puis de l'activer.
La modification de la mémoire sur le R200 entraîne des erreurs matérielles	C'est dû au codage des IRQ "en dur". Supprimez la mémoire supplémentaire ou réinstallez le module d'application Enforcer après la modification matérielle. Nos tests ont indiqué que la mémoire supplémentaire n'offre pas une différence appréciable.
Le journal de débogage a été supprimé	Si l'entrée de registre debugFileSize ou debugOverwriteDay est modifiée sur le client, le journal est supprimé. Ne modifiez pas ces entrées sans extraire d'abord les valeurs.
Certains paramètres (Niveau de débogage, Capturer) retournent à leur valeur par défaut quand le module d'application Enforcer est mis à niveau	Cela peut apparaître sur la mise à niveau, mais n'apparaît pas ensuite.

Symptôme	Solution
Des problèmes apparaissent en exécutant SNMP avec le module d'application Enforcer et HP OpenView	Cela peut être résolu en configurant HP OpenView, comme suit : ■ Chargez le fichier MIB de Symantec, en utilisant le Option > Charger/décharger MIB ■ En utilisant Option > Configuration d'événement, choisissez OnDemandTraps (.1.3.6.1.4.1.393.588) et modifiez chaque trappe comme nécessaire. Par exemple sur Message sur les événements, choisissez Journal et affichage dans la catégorie. Sélectionnez ensuite une catégorie dans la liste déroulante. Définissez Message journal des événements en tant que **$1.**

A propos du transfert des informations de débogage sur le réseau

Lorsque des problèmes se posent sur un boîtier Enforcer, un journal de débogage est créé sur Enforcer (kernel.log). Si vous devez transférer les informations de débogage sur le réseau, utilisez l'une des commandes suivantes pour transférer les journaux de débogage :

debug upload Pour transférer un fichier vers un serveur tftp :

Le transfert de fichiers sur le réseau requiert une connexion série entre un ordinateur et le boîtier Enforcer.

L'exemple suivant représente le résultat d'un transfert de fichier réalisé par HyperTerminal :

```
<date>          <Time>     <File Name>
2008-08-01   16:32:26      user.log
2008-08-01   16:32:24      kernel.log
2008-08-01   14:30:03      ServerSylink[08-01-2008-14-30-03].xml
2008-08-01   14:29:59      ServerProfile[08-01-2008-14-29-59].xml
Enforcer(debug)# upload tftp 10.1.1.1 filename kernel.log
```

Chapitre 13

Questions fréquemment posées au sujet des boîtiers Gateway Enforcer, DHCP Enforcer ou LAN Enforcer

Ce chapitre traite des sujets suivants :

Questions relatives à Enforcer

Les points suivants apportent des réponses au sujet des problèmes d'application sur les boîtiers Gateway Enforcer, DHCP Enforcer ou LAN Enforcer :

- Se reporter à "Quel logiciel antivirus prend en charge l'intégrité de l'hôte ?" à la page 324.
- Se reporter à "Les politiques d'intégrité d'hôte peuvent-elles être définies au niveau du groupe ou au niveau global ?" à la page 325.
- Se reporter à "Pouvez-vous créer un message personnalisé d'intégrité d'hôte ?" à la page 325.
- Se reporter à "Que se produit si les boîtiers Enforcer ne peuvent pas communiquer avec Symantec Endpoint Protection Manager ?" à la page 325.
- Se reporter à "Un serveur RADIUS est-il requis lorsqu'un boîtier LAN Enforcer s'exécute en mode transparent ?" à la page 326.
- Se reporter à "Comment l'application gère-t-elle les ordinateurs sans clients ?" à la page 326.

Quel logiciel antivirus prend en charge l'intégrité de l'hôte ?

Symantec Network Access Control prend en charge les logiciels antivirus suivants :

- AVG Anti-Virus Free Edition 8.0
- AVG Internet Security Edition 8.0
- BitDefender Internet Security 2008
- BitDefender Total Security 2008
- CA Internet Security Suite Plus 2008
- CA Personal Firewall 2008
- eTrust EZ Antivirus 7.1.129
- eTrust EZ Antivirus 7.014
- Lavasoft Ad-Aware Pro 2008
- McAfee Internet Security Suite 2008
- McAfee VirusScan Professional 7.02
- McAfee VirusScan Corp Edition 7.1.0
- McAfee VirusScan Enterprise 8.0i
- McAfee VirusScan Professional 8.0
- McAfee VirusScan Home Edition 8.0
- McAfee VirusScan Home Edition 9.0
- McAfee VirusScanPlus 2008
- Norton 360 All in One Security
- Norton AntiVirus 2004
- Norton AntiVirus 2005
- Norton AntiVirus 2008
- Norton AntiVirus 9.0
- Norton Internet Security 2008
- Panda Internet Security 2008
- Panda Platinum Antivirus 7.0
- Panda Security Panda Antivirus + Firewall 2008
- Panda Titanium Antivirus 2004

- Sophos AntiVirus 3.87
- Trend Micro Internet Security 2008
- Trend Micro OfficeScan Corporate Edition 5.58
- Trend Micro OfficeScan Corporate Edition 6.5
- Trend Micro PC-cillin 2003
- Trend Micro PC-cillin Internet Security 2004
- Webroot Spy Sweeper 5.5

Les politiques d'intégrité d'hôte peuvent-elles être définies au niveau du groupe ou au niveau global ?

Vous pouvez attribuer des politiques d'intégrité de l'hôte par groupe et par emplacement dans la console Symantec Endpoint Protection Manager.

Pouvez-vous créer un message personnalisé d'intégrité d'hôte ?

Symantec Network Access Control peut créer des fenêtres contextuelles Intégrité d'hôte personnalisées pour chaque règle Intégrité d'hôte. Vous pouvez personnaliser la fenêtre, y compris l'icône et le titre. Vous pouvez réaliser cette personnalisation au moyen d'une règle Intégrité d'hôte personnalisée.

Que se produit si les boîtiers Enforcer ne peuvent pas communiquer avec Symantec Endpoint Protection Manager ?

Si vous prévoyez d'utiliser des modules d'application Enforcer avec Symantec Endpoint Protection, nous vous recommandons de disposer de managers redondants. Si Symantec Endpoint Protection Manager est indisponible, Enforcer bloque le trafic en provenance des clients.

Les serveurs de gestion redondants sont préférables. Enforcer envoie un paquet UDP sur le port 1812 via le protocole RADIUS vers Symantec Endpoint Protection Manager pour vérifier le GUID des clients. Si un pare-feu bloque ce port ou si Symantec Endpoint Protection Manager est indisponible, les clients sont bloqués.

Une option d'Enforcer autorise l'accès client au réseau quand Symantec Endpoint Protection Manager est indisponible. Si cette option est activée et Symantec Endpoint Protection Manager est indisponible, le contrôle du GUID et les contrôles de profil ne sont pas effectués. Seule la vérification de l'intégrité de l'hôte peut être exécutée sur le client quand Symantec Endpoint Protection Manager est indisponible.

Vous pouvez utiliser la commande advanced local-auth pour activer ou désactiver l'authentification Enforcer d'un client.

Se reporter à "Advanced Local-auth" à la page 271.

Un serveur RADIUS est-il requis lorsqu'un boîtier LAN Enforcer s'exécute en mode transparent ?

Les spécifications de serveur Radius dépendent de la configuration du commutateur est configuré et de ce que vous authentifiez avec le commutateur.

Prenez en considération les éléments suivants :

- Commutateurs ayant recours aux serveurs RADIUS à d'autres fins que l'authentification des utilisateurs 802.1x.
  Par exemple, quand vous vous connectez au commutateur, vous devez saisir un nom d'utilisateur et un mot de passe. Généralement, le serveur RADIUS effectue l'authentification pour cette connexion. Lorsque le boîtier LAN Enforcer est installé, cette authentification lui est envoyée. Si l'authentification est envoyée au boîtier LAN Enforcer, vous devez configurer l'adresse IP du serveur RADIUS dans ce boîtier. Vous devez également configurer le boîtier LAN Enforcer pour qu'il transfère toutes les demandes non-EAP directement au serveur RADIUS.
- Installation d'un supplicant 802.1x sur un système client. Si un supplicant 802.1x existe sur un système client, le boîtier LAN Enforcer essaie d'authentifier avec le serveur RADIUS. L'authentification 802.1x est activée par défaut sur Windows XP. Si vous l'autorisez à travailler en mode transparent, votre client ne désactive pas automatiquement le supplicant 802.1x intégré. Vous devez vous assurer qu'aucun supplicant 802.1x ne s'exécute sur aucun de vos ordinateurs client.
- Configuration d'Enforcer pour ignorer la demande RADIUS à partir de tout ordinateur client comportant un supplicant 802.1x tiers. Vous pouvez définir cette configuration à l'aide d'une adresse IP 0.0.0.0 pour le serveur RADIUS. Vous pouvez utiliser cette configuration pour exécuter LAN Enforcer en mode transparent. Certains clients peuvent avoir un supplicant 802.1x. Dans ce cas, vous pouvez spécifier que le boîtier LAN Enforcer n'envoie aucun trafic à un serveur RADIUS.

Comment l'application gère-t-elle les ordinateurs sans clients ?

Symantec Network Access Control ne peut appliquer des politiques de sécurité que sur les systèmes qui disposent de clients Symantec installés. La politique de sécurité adoptée par d'autres constructeurs ne peut pas être appliquée. Toute application par d'autres constructeurs peut perturber le réseau.

Les méthodes suivantes d'application sont disponibles :

Auto-application	L'auto-application par le pare-feu client n'a aucun effet sur les systèmes sans clients dans le réseau.
Application de passerelle	Dans les réseaux qui utilisent l'application de passerelle, les systèmes sans clients ne peuvent pas transiter par la passerelle. L'emplacement sur le réseau où vous placez Gateway Enforcer est essentiel ; il peut bloquer l'accès aux ressources critiques du réseau auxquelles d'autres systèmes doivent accéder. Vous pouvez faire des exceptions pour les adresses IP approuvées de sorte qu'elles puissent passer par la passerelle entrante ou sortante sans client. De même, la passerelle peut également dispenser de l'application des systèmes d'exploitation non-Microsoft. Une conception de réseau peut consister à placer les serveurs non critiques du côté de la passerelle. Cette configuration simplifie la conception réseau sans compromettre sérieusement la sécurité.
Application DHCP	L'application DHCP restreint les ordinateurs non conformes ou les systèmes sans clients. Elle limite ces systèmes à un espace d'adresse distinct ou leur fournit un sous-ensemble d'itinéraires sur le réseau. Cette restriction réduit les services réseau pour ces périphériques. Comme pour l'application de passerelle, vous pouvez faire des exceptions pour les adresses MAC approuvées et les systèmes d'exploitation non Microsoft.

Application LAN	L'application de LAN utilise le protocole 802.1x pour l'authentification entre le commutateur et les systèmes client qui se connectent au réseau. Pour utiliser cette méthode d'application, le logiciel de commutation doit prendre le protocole 802.1x en charge et sa configuration doit être correcte. Le logiciel du supplicant 802.1x est également requis si l'administrateur veut vérifier que l'identité de l'utilisateur a également l'état de NAC d'hôte. La configuration du commutateur doit prendre les exceptions pour des systèmes sans clients en charge, plutôt que n'importe quelle configuration de Symantec. Vous disposez de plusieurs méthodes pour installer cette configuration de commutateur. Elles varient selon le type du commutateur et la version de logiciel qu'il exécute. Une méthode typique met en œuvre le concept d'un invité VLAN. Les systèmes sans clients sont attribués à un réseau présentant un niveau de connexion inférieur. Une autre méthode consiste à baser les exceptions sur des adresses MAC. Vous pouvez désactiver 802.1x sur les ports sélectionnés. Cependant, désactiver les ports sélectionnés permet à n'importe qui de se connecter à l'aide du port ; ce n'est donc pas recommandé. De nombreux fournisseurs disposent de dispositions spéciales pour les téléphones VoIP qui peuvent automatiquement déplacer ces périphériques vers des VLAN téléphoniques spéciaux.
API d'application universelle	Lorsque vous utilisez l'API d'application universelle, l'implémentation de l'API du fournisseur tiers prend en charge les exceptions.
Application à l'aide de Cisco NAC	Quand vous utilisez la solution Symantec pour une connexion par interface à Cisco NAC, l'architecture Cisco NAC prend en charge toutes les exclusions.

Section 2

Installer Symantec NAC Integrated Enforcer pour serveurs DHCP Microsoft

Chapitre 14

Présentation de Symantec NAC Integrated Enforcer pour serveurs DHCP Microsoft

Ce chapitre traite des sujets suivants :

A propos de Symantec NAC Integrated Enforcer pour serveurs DHCP Microsoft

Symantec NAC Integrated Enforcer pour serveurs DHCP Microsoft collabore avec le serveur DHCP (Dynamic Host Configuration Protocol) Microsoft Windows. Il s'assure que les clients qui essayent de se connecter au réseau soient conformes aux politiques de sécurité configurées.

Integrated Enforcer pour serveurs DHCP Microsoft assure la sécurité par l'interception et la vérification des messages DHCP de chaque client qui reçoit

une adresse IP dynamique par le serveur DHCP. Il regroupe ensuite les ordinateurs non securisés dans une classe de quarantaine et leur fournit les ressources disponibles et limitées pour chaque configuration de politique établie.

Fonctionnement d'un module d'application Integrated Enforcer pour serveurs DHCP Microsoft

Le module d'application Integrated Enforcer pour serveurs DHCP Microsoft recherche les installations de clients Symantec Endpoint Protection ou Symantec Network Access Control sur tous les clients DHCP gérés par le serveur DHCP. Il applique alors pour ces clients les politiques configurées sur le gestionnaire Symantec Endpoint Security Manager.

Le module d'application Integrated Enforcer pour serveurs DHCP Microsoft vérifie également sur le client l'existence d'un agent, l'identificateur unique (GUID), l'intégrité de l'hôte et la version de profil pour chacune des politiques configurées. Il autorise alors le client ou le place en quarantaine en fonction de son résultat d'authentification.

Integrated Enforcer pour serveurs DHCP Microsoft utilise un plug-in pour interagir avec le serveur DHCP Microsoft. Bien que le module d'application Integrated Enforcer pour serveurs DHCP Microsoft et le serveur DHCP doivent être installés sur le même ordinateur, le module d'application Integrated Enforcer pour serveurs DHCP Microsoft ne dépend pas du serveur DHCP.

Remarque : L'arrêt du serveur DHCP n'arrête pas le module d'application Integrated Enforcer pour serveurs DHCP Microsoft. L'arrêt du module d'application Integrated Enforcer pour serveurs DHCP Microsoft n'arrête pas le serveur DHCP. Lorsque le module d'application Integrated Enforcer pour serveurs DHCP Microsoft réside sur le même ordinateur que le serveur DHCP, le module d'application élimine le besoin de matériel supplémentaire.

Le gestionnaire Symantec Endpoint Protection Manager permet de configurer les politiques de sécurité. Toutefois, leur application repose sur le module d'application Integrated Enforcer pour serveurs DHCP Microsoft.

Le module d'application Integrated Enforcer pour serveurs DHCP Microsoft authentifie les ordinateurs client à l'aide de leur réponse aux critères suivants :

- L'un des clients Symantec Endpoint Protection ou Symantec Network Access Control s'exécute-il sur l'ordinateur client ?
- Le client Symantec Endpoint Protection ou Symantec Network Access Control dispose-t-il d'un identificateur unique (GUID) correct ?

Le GUID est un nombre hexadécimal de 128 bits attribué à un ordinateur client qui exécute le client Symantec Endpoint Protection ou Symantec Network Access Control. Le serveur de gestion génère un GUID lors de la connexion initiale du client.

- Le client se conforme-t-il à la dernière politique d'intégrité de l'hôte définie par l'administrateur sur la console Symantec Endpoint Protection Manager ?
- Le client a reçu la dernière politique de sécurité.
- Le client est certifié par Network Access Control Scanner, possède une adresse MAC approuvée ou exécute un système d'exploitation approuvé, si configuré.

Si le module d'application Integrated Enforcer pour serveurs DHCP Microsoft ne peut pas authentifier le client, il lui fournit l'accès à une zone de quarantaine avec des ressources réseau limitées. La zone de quarantaine est configurée sur le même ordinateur que le module d'application Integrated Enforcer pour serveurs DHCP Microsoft et le serveur DHCP Microsoft.

Vous pouvez également définir l'accès à un serveur de résolution. Le serveur de résolution fournit aux clients des liens vers des logiciels qui leur permettent de se conformer à la sécurité.

Prise en main de l'installation d'un boîtier Integrated Enforcer pour serveurs DHCP Microsoft

La documentation décrit comment installer, configurer et utiliser Integrated Enforcer pour serveurs DHCP Microsoft. Effectuez les tâches de mise en route suivantes :

- Examinez les composants nécessaires pour l'installation d'un boîtier Integrated Enforcer pour serveurs DHCP Microsoft.
  Se reporter à "Composants requis pour Integrated Enforcer pour serveurs DHCP Microsoft" à la page 338.
- Examinez la configuration matérielle requise pour Integrated Enforcer pour serveurs DHCP Microsoft.
  Se reporter à "Configuration matérielle requise pour Integrated Enforcer pour serveurs DHCP Microsoft" à la page 338.
- Examinez le système d'exploitation requis pour Integrated Enforcer pour serveurs DHCP Microsoft.
  Se reporter à "Système d'exploitation requis pour Integrated Enforcer pour serveurs DHCP Microsoft" à la page 339.
- Où placer le boîtier Integrated Enforcer pour serveurs DHCP Microsoft dans un environnement réseau.

Se reporter à "Planification de l'emplacement d'un module d'application Integrated Enforcer pour serveurs DHCP Microsoft" à la page 339.

- Installez un boîtier Integrated Enforcer pour serveurs DHCP Microsoft.
  Se reporter à "Installer un module d'application Integrated Enforcer pour serveurs DHCP Microsoft" à la page 342.
- Configurez les connexions et les paramètres d'un boîtier Integrated Enforcer pour serveurs DHCP Microsoft sur une console Enforcer.
  Se reporter à "A propos de la configuration de Symantec NAC Integrated Enforcer sur une console Enforcer" à la page 370.

Informations supplémentaires sur la documentation relative à Integrated Enforcer pour serveurs DHCP Microsoft

Symantec NAC Integrated Enforcer pour serveurs DHCP Microsoft fait partie du logiciel Symantec Network Access Control.

Tableau 14-1 fournit les informations complémentaires sur les tâches éventuellement nécessaires avant ou après l'installation de Integrated Enforcer pour serveurs DHCP Microsoft.

Tableau 14-1 Documentation complémentaire sur Integrated Enforcer pour serveurs DHCP Microsoft

Titre du document	Description
Guide d'installation pour Symantec Endpoint Protection et Symantec Network Access Control	Décrit l'installation des composants logiciels suivants : ■ Symantec Endpoint Protection Manager ■ Client Symantec Endpoint Protection ■ Client Symantec Network Access Control Il explique également l'installation et la configuration de la base de données Microsoft SQL intégrée, ainsi que la mise en place de la réplication.

Titre du document	Description
Guide d'administration pour Symantec Endpoint Protection et Symantec Network Access Control	Décrit la configuration et l'administration des composants logiciels suivants : ■ Symantec Endpoint Protection Manager ■ Client Symantec Endpoint Protection ■ Client Symantec Network Access Control Il décrit également l'installation des politiques d'intégrité de l'hôte utilisées par le module d'application Enforcer pour mettre en application la conformité sur les ordinateurs client.
Aide en ligne pour Symantec Endpoint Protection et Symantec Network Access Control	Explique l'utilisation de Symantec Endpoint Protection Manager.
fichiers sep_readme.txt et snac_readme.txt	Comprend les dernières informations sur les défauts critiques liés au module d'application Enforcer pouvant également affecter Symantec Endpoint Protection Manager. Consultez le fichier sep_readme.txt situé sur le CD d'installation nommé CD1 pour plus d'informations sur les défauts concernant Symantec Endpoint Protection. Consultez le fichier snac_readme situé sur le CD d'installation nommé CD2 pour plus d'informations sur les défauts concernant Symantec Network Access Control.
Guide client pour Symantec Endpoint Protection et Symantec Network Access Control	Décrit l'utilisation des composants logiciels suivants : ■ Client Symantec Endpoint Protection ■ Client Symantec Network Access Control
Aide en ligne pour les clients Symantec Endpoint Protection et Symantec Network Access Control	Décrit l'utilisation des composants logiciels suivants : ■ Client Symantec Endpoint Protection ■ Client Symantec Network Access Control
Aide en ligne pour Integrated Enforcer pour serveurs DHCP Microsoft	Décrit la configuration du module d'application Integrated Enforcer pour serveurs DHCP Microsoft.

Titre du document	Description
Aide en ligne pour Integrated Enforcer pour Microsoft Network Access Protection (NAP)	Décrit la configuration du module d'application Integrated Enforcer pour Microsoft Network Access Protection.

Chapitre 15

Planifier l'installation de Symantec NAC Integrated Enforcer pour serveurs DHCP Microsoft

Ce chapitre traite des sujets suivants :

A propos de la planification de l'installation d'Integrated Enforcer pour serveurs DHCP Microsoft

Vous devez remplir un certain nombre de conditions requises avant que Symantec NAC Integrated Enforcer pour serveurs DHCP Microsoft puisse devenir opérationnel. Les conditions requises s'appliquent au matériel et aux logiciels, ainsi qu'à d'autres composants logiciels, y compris des applications tierces.

Le type de boîtier Enforcer mis en œuvre dépend du type de produit Symantec Network Access Control dont vous avez fait l'acquisition.

Reportez-vous à votre accord de licence pour plus d'informations.

Composants requis pour Integrated Enforcer pour serveurs DHCP Microsoft

Integrated Enforcer pour serveurs DHCP Microsoft fonctionne avec le serveur DHCP de Microsoft, Symantec Endpoint Protection Manager et le client Symantec Network Access Control. Il vérifie que les clients qui essayent de se connecter au réseau sont conformes aux politiques de sécurité configurées.

Installez les composants requis suivants avant d'utiliser Integrated Enforcer pour serveurs DHCP Microsoft :

Symantec Endpoint Protection Manager	Composant requis pour créer des politiques de sécurité dans un emplacement centralisé et pour les attribuer aux clients.
Client Symantec Network Access Control	Composant requis si vous voulez que les utilisateurs finaux soient protégés par l'application des politiques de sécurité fournies par Integrated Enforcer pour serveurs DHCP Microsoft.
Serveur DHCP de Microsoft Windows	Composant requis si vous voulez que les utilisateurs finaux soient protégés par les politiques appliquées par Integrated Enforcer pour serveurs DHCP Microsoft.
Integrated Enforcer pour serveurs DHCP Microsoft (installé sur le même ordinateur que le service DHCP)	Composant requis pour authentifier les clients et imposer des politiques de sécurité.

Configuration matérielle requise pour Integrated Enforcer pour serveurs DHCP Microsoft

La configuration matérielle requise du module d'application Integrated Enforcer pour serveurs DHCP Microsoft concerne la RAM, le processeur, l'espace de stockage, l'écran, l'adaptateur réseau et la carte d'interface réseau.

Pour des installations de 10 000 utilisateurs maximum, utilisez la configuration recommandée suivante :

- Pentium III 750 MHz
- 256 Mo de mémoire
- 120 Mo d'espace disque
- Adaptateurs réseau Fast Ethernet
- Une carte d'interface réseau (NIC) dotée de TCP/IP

Pour des installations de 10 000 utilisateurs minimum, utilisez la configuration recommandée suivante :

- Pentium 4 2.4 GHz
- 512 Mo de mémoire
- 512 Mo d'espace disque
- Adaptateurs réseau 1 Go
- Ecran de résolution 800 x 600, 256 couleurs (minimum)
- Une carte d'interface réseau (NIC) dotée de TCP/IP

Système d'exploitation requis pour Integrated Enforcer pour serveurs DHCP Microsoft

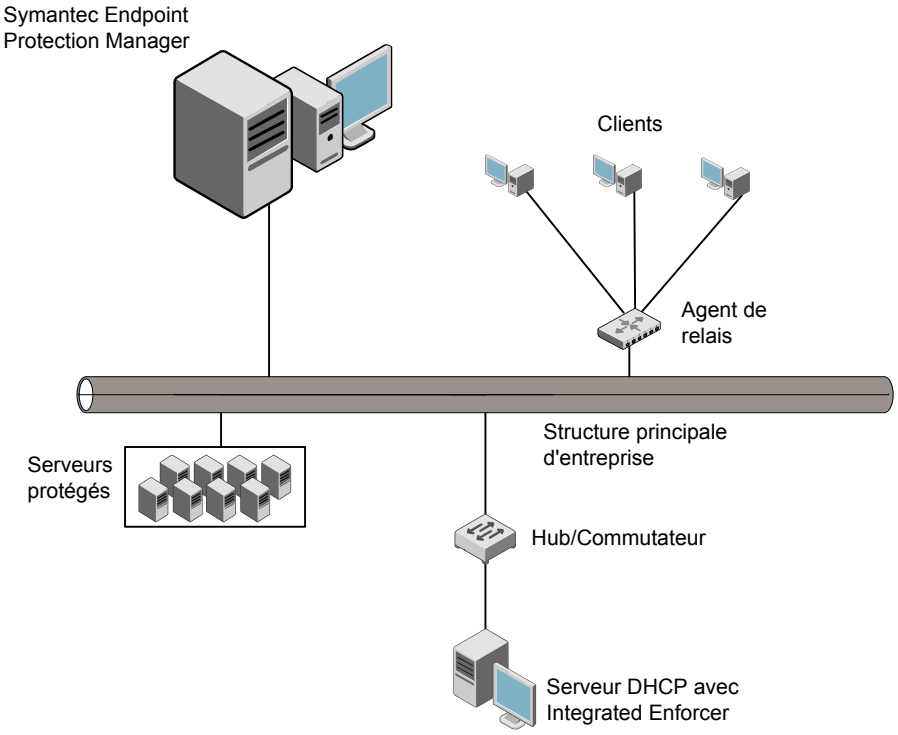
Symantec Integrated Enforcer nécessite que l'un des systèmes d'exploitation suivants soit installé avant de pouvoir installer Integrated Enforcer pour serveurs DHCP Microsoft :

- Windows Server 2000 Service Pack 4 et le serveur DHCP Microsoft
- Windows Server 2003 Service Pack et le serveur DHCP Microsoft
- Windows Server 2003 Service Pack 1 et le serveur DHCP Microsoft

Planification de l'emplacement d'un module d'application Integrated Enforcer pour serveurs DHCP Microsoft

Figure 15-1 illustre la disposition dans un réseau d'un module d'application Integrated Enforcer pour serveurs DHCP Microsoft, d'un serveur DHCP Microsoft et du gestionnaire Symantec Endpoint Protection Manager, ainsi que des clients internes ou distants.

Figure 15-1 Disposition d'un module d'application Symantec NAC Integrated Enforcer pour serveurs DHCP Microsoft



Chapitre 16

Installer Symantec NAC Integrated Enforcer pour serveurs DHCP Microsoft

Ce chapitre traite des sujets suivants :

Avant d'installer Integrated Enforcer pour serveurs DHCP Microsoft

Avant d'installer Symantec Integrated Enforcer, vous devez avoir terminé les installations et les tâches suivantes :

- Installation de Symantec Endpoint Protection Manager

Remarque : Il est conseillé d'installer Symantec Endpoint Protection Manager avant d'installer Integrated Enforcer pour serveurs DHCP Microsoft. Symantec Endpoint Protection Manager doit être installé pour permettre un fonctionnement correct d'Integrated Enforcer pour serveurs DHCP Microsoft.

Consultez le *Guide d'installation pour Symantec Enterprise Protection et Symantec Network Access Control* pour plus d'informations sur l'installation de Symantec Endpoint Protection Manager.

- Vérification de la configuration requise pour l'ordinateur sur lequel vous prévoyez d'installer le service DHCP et Integrated Enforcer pour serveurs DHCP Microsoft
  Se reporter à "Composants requis pour Integrated Enforcer pour serveurs DHCP Microsoft" à la page 338.
- Installation de Microsoft Windows 2000 Server ou de Microsoft Windows 2003 Server
  Consultez la documentation accompagnant l'application Microsoft Windows Server.
  Se reporter à "Composants requis pour Integrated Enforcer pour serveurs DHCP Microsoft" à la page 338.
- Configuration du service de DHCP sur Microsoft Windows 2000 Server ou Microsoft Windows 2003 Server
  Consultez la documentation du service DHCP, fournie avec l'application Microsoft Windows Server.

Installer un module d'application Integrated Enforcer pour serveurs DHCP Microsoft

Le module d'application Integrated Enforcer pour serveurs DHCP Microsoft doit être installé sur le même ordinateur sur lequel vous avez déjà installé le système d'exploitation Microsoft Windows Server ainsi que le service DHCP. Vous devez vous connecter en tant qu'administrateur ou utilisateur du groupe d'administrateurs.

Remarque : Après avoir installé le serveur DHCP Microsoft, vous devez configurer le module d'application Integrated Enforcer pour serveurs DHCP Microsoft. Le module d'application peut alors se connecter à Symantec Endpoint Protection Manager.

Vous pouvez installer le module d'application Integrated Enforcer pour serveurs DHCP Microsoft grâce aux méthodes d'installation suivantes :

- Assistant d'installation
  Se reporter à "Pour installer le module d'application Integrated Enforcer pour serveurs DHCP Microsoft à l'aide d'un assistant" à la page 363.
- Ligne de commande

Se reporter à "Pour installer le module d'application Integrated Enforcer pour serveurs DHCP Microsoft depuis la ligne de commande" à la page 365.

Pour installer le module d'application Integrated Enforcer pour serveurs DHCP Microsoft à l'aide d'un assistant

1. Insérez le CD2 d'installation.

   Si l'installation ne démarre pas automatiquement, cliquez deux fois sur **IntegratedEnforcerInstaller.exe**.

   Vous devez quitter l'installation et installer le serveur DHCP si le message suivant s'affiche :

   ```
   You must have the DHCP server on this machine to install this
   product (Vous devez avoir le serveur DHCP sur cet ordinateur
   pour installer ce produit). Pour installer le serveur DHCP,
   dans le Panneau de configuration, utilisez l'assistant
   Ajout/Suppression de composants Windows.
   ```

   Si le serveur DHCP est déjà installé, le volet Welcome to Symantec Integrated Enforcer Installation Wizard (Bienvenue dans l'Assistant d'installation de Symantec Integrated Enforcer) s'affiche.

2. Dans l'écran Welcome, cliquez sur **Next** (Suivant).
3. Dans le panneau License Agreement (Contrat de licence), cliquez sur **I accept the license agreement** (J'accepte le contrat de licence).
4. Cliquez sur **Next** (Suivant).
5. Dans le volet Destination Folder (Dossier de destination), effectuez l'une des opérations suivantes :
   - Pour accepter le dossier cible par défaut, cliquez sur **Next** (Suivant).
   - Pour modifier le dossier de destination, cliquez sur **Browse** (Parcourir), spécifiez un nouveau dossier cible, cliquez sur **OK**, puis cliquez sur **Next** (Suivant).
6. Si le volet Role Selection s'affiche, sélectionnez **DHCP Enforcement for Microsoft DHCP Server** (Application DHCP pour serveur DHCP Microsoft) et cliquez sur **Next** (Suivant).

   Le volet Role Selection (Sélection du rôle) ne s'affiche que si plus d'un type de module d'application Symantec NAC Integrated Enforcer peut être installé en fonction des services s'exécutant sur le serveur.
7. Dans le volet Ready to Install the Application (Prêt pour l'installation de l'application), cliquez sur **Next** (Suivant).

8 Lorsque vous êtes invité à redémarrer le serveur DHCP, effectuez l'une des tâches suivantes :

- Pour redémarrer le serveur DHCP immédiatement, cliquez sur **Oui**.
- Pour redémarrer le serveur DHCP manuellement plus tard, cliquez sur **No** (Non).
  Pour redémarrer le serveur DHCP ultérieurement, vous devez l'arrêter, puis le démarrer.

Vous devez redémarrer le serveur DHCP pour que Symantec Integrated Enforcer fonctionne.

Se reporter à "Pour arrêter et démarrer manuellement le serveur DHCP Microsoft" à la page 366.

9 Cliquez sur **Finish** (Terminer).

Si vous devez réinstaller le module d'application Integrated Enforcer, vous devez d'abord le désinstaller.

Se reporter à "Pour désinstaller le module d'application Integrated Enforcer pour serveurs DHCP Microsoft" à la page 344.

Se reporter à "Pour désinstaller le module d'application Integrated Enforcer pour serveurs DHCP Microsoft depuis la ligne de commande" à la page 345.

Pour installer le module d'application Integrated Enforcer pour serveurs DHCP Microsoft depuis la ligne de commande

1 Pour commencer l'installation à partir de la ligne de commande, ouvrez une invite de commande DOS.

L'installation à partir de la ligne de commande fait uniquement appel aux paramètres par défaut.

2 Sur la ligne de commande, spécifiez le répertoire où figure le programme d'installation d'Integrated Enforcer.

C:\Program Files\Symantec\Integrated Enforcer est l'emplacement par défaut de l'installation.

3 Entrez `IntegratedEnforcerInstaller.exe /qr` sur la ligne de commande et tapez : `Enter` (Entrée).

Pour désinstaller le module d'application Integrated Enforcer pour serveurs DHCP Microsoft

1 Dans la barre des tâches Windows, cliquez sur **Démarrer > Panneau de configuration > Ajout/Suppression de programmes**.

2 Cliquez sur **Symantec Integrated Enforcer**, puis sur **Supprimer**.

3 Lorsque vous êtes invité à supprimer le logiciel, cliquez sur **Oui**.

4 Lorsque vous êtes invité à redémarrer le serveur DHCP, effectuez l'une des tâches suivantes :

- Pour redémarrer le serveur DHCP immédiatement, cliquez sur **Oui**.
- Pour redémarrer le serveur DHCP manuellement plus tard (par défaut), cliquez sur **Non**.
  Pour redémarrer le serveur DHCP ultérieurement, vous devez l'arrêter, puis le démarrer.
  Vous devez redémarrer le serveur DHCP pour désinstaller complètement le module d'application Symantec Integrated Enforcer.

Pour désinstaller le module d'application Integrated Enforcer pour serveurs DHCP Microsoft depuis la ligne de commande

1 Ouvrez une invite de commandes DOS.

2 A l'invite de commande, entrez l'une des commandes suivantes selon la version installée :

version 11.0.0000	`MsiExec.exe /qn /X {C58BCCDF-A390-46CF-A328-323572E35735}`
version 11.0.1000 ou supérieure	`misexec.exe /qn /X <nom_fichier >`Le nom de fichier doit être sous Program Files\Common Files\Wise Installation Wizard.

Pour arrêter et démarrer manuellement le serveur DHCP Microsoft

1 Sur la barre des tâches Windows, cliquez sur **Démarrer > Panneau de configuration > Outils d'administration > Services**.

2 Cliquez sur **Serveur DHCP**.

3 Cliquez avec le bouton droit de la souris, puis cliquez sur **Arrêter**.

4 Cliquez sur **Démarrer**.

Mettre à niveau le module d'application Integrated Enforcer pour serveurs DHCP Microsoft

Le tâches suivantes détaillent la procédure de mise à niveau d'un module d'application Symantec NAC Integrated Enforcer :

Pour mettre à niveau votre module d'application Symantec NAC Integrated Enforcer

1 Désinstallez la version existante du module d'application Integrated Enforcer.

Se reporter à "Pour désinstaller le module d'application Integrated Enforcer pour serveurs DHCP Microsoft" à la page 344.

Se reporter à "Pour désinstaller le module d'application Integrated Enforcer pour serveurs DHCP Microsoft depuis la ligne de commande" à la page 345.

Remarque : Assurez-vous de redémarrer le service DHCP avant d'installer la nouvelle version du module d'application Integrated Enforcer.

---

2 Installez la nouvelle version du module d'application Integrated Enforcer.

Se reporter à "Pour installer le module d'application Integrated Enforcer pour serveurs DHCP Microsoft à l'aide d'un assistant" à la page 363.

Se reporter à "Pour installer le module d'application Integrated Enforcer pour serveurs DHCP Microsoft depuis la ligne de commande" à la page 365.

Section 3

Installer Symantec NAC Integrated Enforcer pour serveurs DHCP Alcatel-Lucent VitalQIP

Chapitre 17

Présentation de Symantec NAC Integrated Enforcer pour serveurs DHCP Alcatel-Lucent VitalQIP

Ce chapitre traite des sujets suivants :

A propos d'Integrated Enforcer for Alcatel-Lucent VitalQIP DHCP Servers (Integrated Lucent Enforcer)

Le module d'application Integrated Lucent Enforcer fonctionne avec Lucent VitalQIP DHCP Server, version 6.2.

Le module d'application Integrated Lucent Enforcer et Symantec Endpoint Protection Manager vérifient que les applications suivantes se conforment aux politiques de sécurité configurées :

- Client Symantec Endpoint Protection

- Client Symantec Network Access Control

Le module d'application Integrated Lucent Enforcer vérifie la conformité des ordinateurs client avec les politiques de sécurité que l'administrateur configure. Il assure la protection en interceptant et en vérifiant les messages DHCP de chaque client qui reçoit une adresse IP dynamique via le serveur DHCP d'entreprise Lucent VitalQIP. Le module d'application Integrated Lucent Enforcer regroupe alors les ordinateurs non-sécurisés dans une classe de quarantaine. Il fournit également des ressources disponibles mais limitées aux ordinateurs non-sécurisés pour chaque politique de sécurité établie.

Ce que permet le module d'application Integrated Lucent Enforcer

La console Integrated Lucent Enforcer permet d'effectuer les tâches principales suivantes :

- Configurer une connexion à un serveur Symantec Endpoint Protection.
- Démarrer et arrêter le service de module d'application Enforcer.
- Configurer les connexions aux analyseurs Network Access Control Scanners.
- Configurer des quarantaines automatiques.
- Afficher l'état de la connexion.
- Afficher le journal client et le journal système.
- Afficher les fournisseurs DHCP approuvés.

Fonctionnement du module d'application Integrated Lucent Enforcer

Le module d'application Integrated Lucent Enforcer recherche sur un ordinateur client la présence de clients Symantec Endpoint Protection et Symantec Network Access Control gérés par Lucent VitalQIP Enterprise DHCP Server. Le module d'application Integrated Lucent Enforcer impose alors des politiques à ces clients, comme configuré dans Symantec Endpoint Protection Manager, agissant comme "serveur de gestion".

Le module d'application Integrated Lucent Enforcer authentifie les ordinateurs client en recherchant une réponse conformément aux critères suivants :

- L'un des clients Symantec Endpoint Protection ou Symantec Network Access Control s'exécute-il sur l'ordinateur client ?

- Le client Symantec Endpoint Protection ou Symantec Network Access Control dispose-t-il d'un identificateur unique (GUID) correct ?
  Le GUID est un nombre hexadécimal de 128 bits attribué à un ordinateur client qui exécute le client Symantec Endpoint Protection ou Symantec Network Access Control. Le serveur de gestion génère un GUID lors de l'installation initiale du client.
- Politique d'intégrité de l'hôte
  Une politique d'intégrité de l'hôte vérifie que l'ordinateur client exécute les applications et les fichiers de données requis quand l'ordinateur client essaye de se connecter au réseau.
- Le numéro de série de profil basé sur les dernières politiques de sécurité configurées, y compris la dernière politique d'intégrité de l'hôte.
  Le module d'application Integrated Lucent Enforcer vérifie que l'ordinateur client a reçu les dernières politiques de sécurité du serveur de gestion. Si le numéro de série de profil ne correspond pas, le module d'application Integrated Lucent Enforcer demande à l'ordinateur client de mettre à jour ses politiques de sécurité.

Remarque : Le module d'application Integrated Lucent Enforcer utilise un plug-in pour interagir avec Lucent VitalQIP Enterprise DHCP Server. Cependant, le module d'application Integrated Lucent Enforcer ne dépend pas de Lucent VitalQIP Enterprise DHCP Server.

Si vous arrêtez Lucent VitalQIP Enterprise DHCP Server, le module d'application Integrated Lucent Enforcer continue à fonctionner. De même, si vous arrêtez le module d'application Integrated Lucent Enforcer, Lucent VitalQIP Enterprise DHCP Server continue à fonctionner. En installant le module d'application Integrated Lucent Enforcer et Lucent VitalQIP Enterprise DHCP Server sur le même ordinateur, aucun matériel supplémentaire n'est requis.

Vous utilisez le serveur de gestion pour configurer les politiques de sécurité que le module d'application Integrated Lucent Enforcer impose. Avant d'autoriser un client à se connecter au réseau, Integrated Lucent Enforcer l'authentifie en vérifiant les conditions suivantes :

- L'ordinateur client doit avoir installé le client Symantec Endpoint Protection ou le client Symantec Network Access Control et il doit être en cours d'exécution.
- Le client possède un identifiant unique (GUID) correct.
- Le client est conforme aux dernières politiques d'intégrité de l'hôte par défaut ou à votre politique d'intégrité de l'hôte personnalisée.

- Le client a reçu la dernière politique de sécurité.
- Le client est certifié par Network Access Control Scanner, possède une adresse MAC approuvée ou exécute un système d'exploitation approuvé, si configuré.

Si le module d'application Integrated Lucent Enforcer ne peut pas authentifier le client, l'accès à une zone de quarantaine avec des ressources réseau limitées est fourni au client. La zone de quarantaine est configurée sur le même ordinateur que le module d'application Integrated Lucent Enforcer et Lucent VitalQIP Enterprise DHCP Server.

Vous pouvez également définir l'accès à un serveur de résolution. Le serveur de résolution fournit aux clients des liens vers des logiciels qui leur permettent de se conformer à la sécurité.

Où trouver plus d'informations sur la documentation apparentée pour un module d'application Integrated Lucent Enforcer

Le module d'application Integrated Lucent Enforcer Enforcer fait partie du logiciel Symantec Network Access Control.

Tableau 17-1 fournit des informations complémentaires sur les tâches que vous pouvez avoir besoin d'effectuer avant ou après l'installation d'un module d'application Integrated Lucent Enforcer.

Tableau 17-1 Documentation relative pour un module d'application Integrated Lucent Enforcer

Titre du document	Description
Guide d'installation pour Symantec Endpoint Protection et Symantec Network Access Control	Décrit l'installation des composants logiciels suivants : ■ Symantec Endpoint Protection Manager ■ Client Symantec Endpoint Protection ■ Client Symantec Network Access Control Il explique également l'installation et la configuration de la base de données Microsoft SQL intégrée, ainsi que la mise en place de la réplication.

Titre du document	Description
Guide d'administration pour Symantec Endpoint Protection et Symantec Network Access Control	Décrit la configuration et l'administration des composants logiciels suivants : ■ Symantec Endpoint Protection Manager ■ Client Symantec Endpoint Protection ■ Client Symantec Network Access Control Il décrit également la configuration des politiques d'intégrité de l'hôte utilisées par le module d'application Enforcer pour mettre en application la conformité sur les ordinateurs client.
Aide en ligne pour Symantec Endpoint Protection et Symantec Network Access Control	Explique l'utilisation de Symantec Endpoint Protection Manager.
fichiers sep_readme.txt et snac_readme.txt	Comprend les dernières informations sur les défauts critiques liés au module d'application Enforcer pouvant également affecter Symantec Endpoint Protection Manager. Consultez le fichier sep_readme.txt situé sur le CD d'installation nommé CD1 pour plus d'informations sur les défauts concernant Symantec Endpoint Protection. Consultez le fichier snac_readme situé sur le CD d'installation nommé CD2 pour plus d'informations sur les défauts concernant Symantec Network Access Control.
Guide client pour Symantec Endpoint Protection et Symantec Network Access Control	Décrit l'utilisation des composants logiciels suivants : ■ Client Symantec Endpoint Protection ■ Client Symantec Network Access Control
Aide en ligne pour les clients Symantec Endpoint Protection et Symantec Network Access Control	Décrit l'utilisation des composants logiciels suivants : ■ Client Symantec Endpoint Protection ■ Client Symantec Network Access Control
Aide en ligne pour un module d'application Integrated Lucent Enforcer	Décrit comment configurer un module d'application Integrated Lucent Enforcer.

Titre du document	Description
Aide en ligne pour Integrated Enforcer pour serveurs DHCP Microsoft	Décrit la configuration d'un module d'application Integrated Enforcer pour serveurs DHCP Microsoft.
Aide en ligne pour Integrated Enforcer pour Microsoft Network Access Protection (NAP)	Décrit la configuration d'un module d'application Integrated Enforcer pour Microsoft Network Access Protection.

Chapitre 18

Planifier l'installation de Symantec NAC Integrated Lucent Enforcer

Ce chapitre traite des sujets suivants :

A propos de la planification de l'installation d'un module d'application Integrated Lucent Enforcer

Vous devez répondre à un certain nombre d'exigences avant que le module d'application Integrated Lucent Enforcer puisse devenir opérationnel. Les conditions requises concernent le matériel et les logiciels, ainsi que d'autres composants logiciels, y compris des applications tierces.

Le type de boîtier Enforcer que vous pouvez mettre en œuvre dépend du type de produit Symantec Network Access Control dont vous avez fait l'acquisition.

Reportez-vous à votre accord de licence pour plus d'informations.

Eléments requis pour un module d'application Integrated Lucent Enforcer

Vous devez avoir déjà installé et configuré les composants suivants avant de pouvoir installer le module d'application Symantec Integrated Lucent Enforcer :

- Serveur DHCP d'entreprise Lucent VitalQIP 6.2
  Consultez la documentation fournie avec le serveur DHCP d'entreprise Lucent VitalQIP 6.2 pour plus d'informations sur son installation et sa configuration.
- Sybase Adaptive Server Enterprise Suite 12.5.2
  Consultez la documentation fournie avec Sybase pour plus d'informations sur l'installation et la configuration de la base de données Sybase.
- Symantec Endpoint Protection Manager, version 11.0.3
  Consultez le *Guide d'installation pour Symantec Endpoint Protection et Symantec Network Access Control* pour plus d'informations sur l'installation de Symantec Endpoint Protection Manager.
- Clients Symantec Network Access Control, version 11.0.3
  Consultez le *Guide d'installation pour Symantec Endpoint Protection et Symantec Network Access Control* pour plus d'informations sur l'installation des clients Symantec Network Access Control.
  Consultez le *Guide d'administration pour Symantec Endpoint Protection et Symantec Network Access Control* pour plus d'informations sur la mise à niveau des clients Symantec Network Access Control.
- Consultez le *Guide client pour Symantec Endpoint Protection et Symantec Network Access Control* pour plus d'informations sur l'utilisation des clients Symantec Network Access Control.

Tableau 18-1 doit être installé avant de pouvoir assurer la protection de clients.

Tableau 18-1 Eléments requis pour le module d'application Symantec NAC Integrated Lucent Enforcer

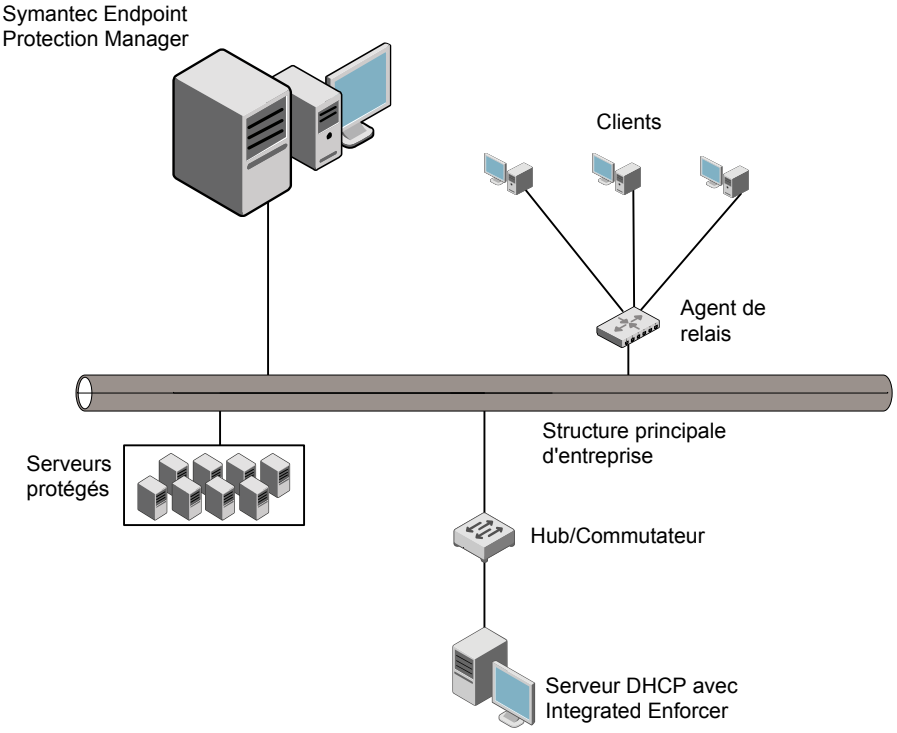
Nom du composant	Fonction du composant
Symantec Endpoint Protection Manager, version 11.0.3	Symantec Endpoint Protection Manager est requis pour la création de politiques de sécurité dans un emplacement centralisé et leur attribution aux clients Symantec Network Access Control.

Nom du composant	Fonction du composant
Client Symantec Network Access Control, version 11.0.3	Les clients Symantec doivent être installés et déployés sur les ordinateurs client avant que les politiques de sécurité puissent les protéger. Les politiques d'intégrité de l'hôte peuvent être configurées sur la console Symantec Endpoint Protection Manager.
Sybase Adaptive Server Enterprise Suite 12.5.2	Cette suite Sybase est requise.
Serveur DHCP d'entreprise Lucent VitalQIP 6.2	Le serveur DHCP d'entreprise Lucent VitalQIP 6.2 est requis pour les attributions des baux et des adresses IP DHCP.
Symantec NAC Integrated Lucent Enforcer	Symantec NAC Integrated Lucent Enforcer est requis pour authentifier les informations d'authentification d'un client et pour imposer la conformité d'un client à une politique de sécurité.

Planifier la disposition d'un module d'application Integrated Lucent Enforcer

Figure 18-1 illustre comment placer le module d'application Integrated Lucent Enforcer, Lucent VitalQIP Enterprise DHCP 6.2 Server et Symantec Endpoint Protection Manager, ainsi que les clients internes ou distants dans un réseau.

Figure 18-1 Disposition d'un module d'application Integrated Enforcer pour serveurs DHCP Alcatel-Lucent VitalQIP avec un serveur DHCP d'entreprise Lucent VitalQIP 6.2



Spécifications matérielles pour un module d'application Integrated Lucent Enforcer

La configuration matérielle requise par le module d'application Integrated Lucent Enforcer concerne la RAM, le processeur, l'espace de stockage, l'écran, l'adaptateur réseau et la carte d'interface réseau.

Pour des installations de 10 000 utilisateurs maximum, utilisez la configuration recommandée suivante :

- Pentium III 750 MHz
- 256 Mo de mémoire
- 120 Mo d'espace disque
- Adaptateurs réseau Fast Ethernet
- Une carte d'interface réseau (NIC) dotée de TCP/IP

Pour des installations de plus de 10 000 utilisateurs, utilisez la configuration recommandée suivante :

- Pentium 4 2.4 GHz
- 512 Mo de mémoire
- 512 Mo d'espace disque
- Adaptateurs réseau 1 Go
- Ecran de résolution 800 x 600, 256 couleurs (minimum)
- Une carte d'interface réseau (NIC) dotée de TCP/IP

Spécifications de système d'exploitation pour un module d'application Integrated Lucent Enforcer

Avant de pouvoir installer le module d'application Integrated Lucent Enforcer sur le même ordinateur que Lucent VitalQIP Enterprise DHCP 6.2 Server, vous devez installer l'un des systèmes d'exploitation suivants :

- Windows 2000 Advanced Server avec Service Pack 4 et serveur DHCP d'entreprise Lucent VitalQIP 6.2 ou version ultérieure
- Windows Server 2003 Standard Edition 32 bits et serveur DHCP d'entreprise Lucent VitalQIP 6.2 ou version ultérieure
- Windows Server 2003 Standard Edition 32 bits avec Service Pack 1 et serveur DHCP d'entreprise Lucent VitalQIP 6.2 ou version ultérieure

- Windows Server 2003 Standard Edition 32 bits avec Service Pack 2 et Lucent VitalQIP Enterprise DHCP 6.2 Server ou version ultérieure
- Windows Server 2003 Advanced Edition 32 bits et serveur DHCP d'entreprise Lucent VitalQIP 6.2 ou version ultérieure
- Windows Server 2003 Advanced Edition 32 bits avec Service Pack 1 et serveur DHCP d'entreprise Lucent VitalQIP 6.2 ou version ultérieure
- Windows Server 2003 Advanced Edition 32 bits avec Service Pack 2 et Lucent VitalQIP Enterprise DHCP 6.2 Server ou version ultérieure

Chapitre 19

Installer Symantec NAC Integrated Enforcer pour serveurs DHCP d'entreprise Alcatel-Lucent VitalQIP

Ce chapitre traite des sujets suivants :

Avant la première installation du module d'application Integrated Enforcer pour serveurs DHCP d'entreprise Alcatel-Lucent VitalQIP

Avant de commencer l'installation du module d'application Integrated Enforcer pour serveurs DHCP d'entreprise Alcatel-Lucent VitalQIP, vous devez avoir effectué les tâches suivantes :

- Terminer l'installation de Symantec Network Access Control, y compris Symantec Endpoint Protection Manager

Remarque : Symantec Endpoint Protection Manager doit être installé pour permettre le fonctionnement correct du module d'application Integrated Enforcer pour serveurs DHCP d'entreprise Alcatel-Lucent VitalQIP.

Consultez le *Guide d'installation pour Symantec Enterprise Protection et Symantec Network Access Control* pour plus d'informations sur l'installation de Symantec Endpoint Protection Manager.

- Terminer la configuration, le déploiement et l'installation du client Symantec Network Access Control
  Consultez le *Guide d'installation pour Symantec Enterprise Protection et Symantec Network Access Control* pour plus d'informations sur l'installation du client Symantec Network Access Control.
- Vérifier la configuration requise pour l'ordinateur sur lequel vous prévoyez d'installer les composants suivants :
  - Base de données Sybase
  - Serveur DHCP d'entreprise Lucent VitalQIP
  - Module d'application Integrated Enforcer pour serveurs DHCP d'entreprise Alcatel-Lucent VitalQIP

  Consultez la documentation qui accompagne la base de données Sybase pour plus d'informations sur l'installation et la configuration de la base de données.
  Consultez la documentation qui accompagne le serveur DHCP d'entreprise Lucent VitalQIP pour plus d'informations sur l'installation et la configuration du service DHCP.
  Se reporter à "Composants requis pour Integrated Enforcer pour serveurs DHCP Microsoft" à la page 338.

Installer un module d'application Integrated Enforcer pour serveurs DHCP d'entreprise Alcatel-Lucent VitalQIP

Vous devez installer le module d'application Integrated Enforcer pour serveurs DHCP d'entreprise Alcatel-Lucent VitalQIP sur l'ordinateur sur lequel vous avez déjà installé les logiciels suivants :

- Système d'exploitation Microsoft Windows Server
- Base de données Sybase
- Serveur DHCP d'entreprise Lucent VitalQIP 6.2

Vous devez vous connecter en tant qu'administrateur ou utilisateur du groupe d'administrateurs.

Remarque : Après avoir terminé l'installation du module d'application Integrated Enforcer pour serveurs DHCP d'entreprise Alcatel-Lucent VitalQIP, vous devez le configurer. Le module d'application Integrated Enforcer pour serveurs DHCP d'entreprise Alcatel-Lucent VitalQIP doit pouvoir établir une connexion au gestionnaire Symantec Endpoint Protection Manager, également nommé serveur de gestion.

Vous pouvez installer le module d'application Integrated Enforcer pour serveurs DHCP d'entreprise Alcatel-Lucent VitalQIP à l'aide des méthodes d'installation suivantes :

- Assistant d'installation
- Ligne de commande

Pour installer un module d'application Integrated Enforcer pour serveurs DHCP d'entreprise Alcatel-Lucent VitalQIP à l'aide d'un assistant

1. Insérez le CD d'installation nommé CD2.

   Si l'installation ne démarre pas automatiquement, cliquez deux fois sur **IntegratedEnforcerInstaller.exe**.

2. Si le serveur DHCP d'entreprise Lucent VitalQIP est déjà installé, dans le volet Welcome de l'assistant Symantec Integrated Lucent Enforcer Installation Wizard (volet Bienvenue de l'Assistant d'installation de Symantec Integrated Lucent Enforcer), cliquez sur **Next** (Suivant).
3. Dans le panneau License Agreement (Contrat de licence), cliquez sur **I accept the license agreement** (J'accepte le contrat de licence).
4. Cliquez sur **Next** (Suivant).
5. Dans le volet Destination Folder (Dossier de destination), effectuez l'une des opérations suivantes :
   - Pour accepter le dossier cible par défaut, cliquez sur **Next** (Suivant).
   - Pour modifier le dossier de destination, cliquez sur **Browse** (Parcourir), spécifiez un nouveau dossier cible, cliquez sur **OK**, puis cliquez sur **Next** (Suivant).

6 Si le volet Sélection du rôle s'affiche, sélectionnez **DHCP Enforcement for Alcatel-Lucent VitalQIP® DHCP Server** (Application DHCP pour serveur DHCP Alcatel-Lucent VitalQIP®) et cliquez sur **Next** (Suivant).

Le volet Role Selection (Sélection du rôle) ne s'affiche que si plus d'un type de module d'application Symantec NAC Integrated Enforcer peut être installé en fonction des services s'exécutant sur le serveur.

7 Dans le volet Ready to Install the Application (Prêt pour l'installation de l'application), cliquez sur **Next** (Suivant).

8 Lorsque vous êtes invité à redémarrer le serveur DHCP d'entreprise Lucent VitalQIP, effectuez une des tâches suivantes :

- Pour redémarrer le serveur DHCP d'entreprise Lucent VitalQIP immédiatement, cliquez sur **Yes** (Oui).
- Pour redémarrer le serveur DHCP d'entreprise Lucent VitalQIP manuellement plus tard (paramètre par défaut), cliquez sur **No** (Non). Si vous redémarrez le serveur DHCP d'entreprise Lucent VitalQIP ultérieurement, vous devez l'arrêter, puis le démarrer.

Vous devez redémarrer Lucent VitalQIP Enterprise DHCP Server pour que le module d'application Symantec Integrated Lucent Enforcer fonctionne.

Se reporter à "Arrêter et démarrer le serveur DHCP d'entreprise Lucent VitalQIP" à la page 366.

9 Cliquez sur **Finish** (Terminer).

Si vous devez réinstaller le module d'application Integrated Enforcer pour serveurs DHCP d'entreprise Alcatel-Lucent VitalQIP, vous devez d'abord le désinstaller.

Se reporter à "Désinstaller un module d'application Integrated Enforcer pour serveurs DHCP d'entreprise Alcatel-Lucent VitalQIP" à la page 365.

Pour installer un module d'application Integrated Enforcer pour serveurs DHCP d'entreprise Alcatel-Lucent VitalQIP depuis la ligne de commande

1. Pour commencer l'installation à partir de la ligne de commande, ouvrez une invite de commandes DOS.

   L'installation à partir de la ligne de commande fait uniquement appel aux paramètres par défaut.

2. Sur la ligne de commande, spécifiez le répertoire d'emplacement du programme d'installation d'Integrated Enforcer.

   C:\Program Files\Symantec\Integrated Enforcer est l'emplacement par défaut de l'installation.

3. Saisissez `IntegratedEnforcerInstaller.exe /qr` sur la ligne de commande et appuyez sur **Entrée**.

Désinstaller un module d'application Integrated Enforcer pour serveurs DHCP d'entreprise Alcatel-Lucent VitalQIP

Il peut s'avérer nécessaire de désinstaller le module d'application Integrated Enforcer pour serveurs DHCP d'entreprise Alcatel-Lucent VitalQIP. Vous pouvez désinstaller ce module d'application à l'aide de l'utilitaire du Panneau de configuration ou à partir de la ligne de commande.

Pour désinstaller un module d'application Integrated Enforcer pour serveurs DHCP d'entreprise Alcatel-Lucent VitalQIP

1. Dans la barre des tâches Windows, cliquez sur **Démarrer > Panneau de configuration > Ajout/Suppression de programmes**.
2. Cliquez sur **Symantec Integrated Enforcer**, puis sur **Supprimer**.
3. Lorsque vous êtes invité à supprimer le logiciel, cliquez sur **Oui**.
4. Lorsque vous êtes invité à redémarrer le serveur DHCP d'entreprise Lucent VitalQIP, effectuez une des tâches suivantes :

   - Pour redémarrer le serveur DHCP d'entreprise Lucent VitalQIP immédiatement, cliquez sur **Oui**.
   - Pour redémarrer le serveur DHCP d'entreprise Lucent VitalQIP manuellement plus tard (paramètre par défaut), cliquez sur **Non**. Pour redémarrer le serveur DHCP d'entreprise Lucent VitalQIP ultérieurement, vous devez l'arrêter, puis le démarrer.

Pour désinstaller complètement le module d'application Integrated Enforcer pour serveurs DHCP d'entreprise Alcatel-Lucent VitalQIP, vous devez redémarrer le serveur DHCP d'entreprise Lucent VitalQIP.

Pour désinstaller un module d'application Integrated Enforcer pour serveurs DHCP d'entreprise Alcatel-Lucent VitalQIP depuis la ligne de commande

1. Ouvrez une invite de commandes DOS.
2. A l'invite, tapez : **`MsiExec.exe /qn /X{A145EB45-0852-4E18-A9DC-9983A6AF2329}`**

Arrêter et démarrer le serveur DHCP d'entreprise Lucent VitalQIP

Il peut parfois être nécessaire d'arrêter et de démarrer le serveur DHCP d'entreprise Lucent VitalQIP.

Pour arrêter et démarrer le serveur DHCP d'entreprise Lucent VitalQIP

1. Sur la barre des tâches Windows, cliquez sur **Démarrer > Panneau de configuration > Outils d'administration > Services**.
2. Cliquez sur **Lucent DHCP Service**.
3. Cliquez avec le bouton droit de la souris, puis cliquez sur **Arrêter**.
4. Cliquez sur **Démarrer**.

Section 4

Configurer Symantec NAC Integrated Enforcer sur la console d'un boîtier Enforcer

Chapitre 20

Configurer Symantec NAC Integrated Enforcer sur la console d'un boîtier Enforcer

Ce chapitre traite des sujets suivants :

- Arrêter et démarrer les services de communication entre Integrated Enforcer et un serveur de gestion
- Déconnecter un module d'application Symantec NAC Lucent Integrated Enforcer d'un serveur de gestion sur une console Enforcer
- Se connecter aux serveurs Symantec Endpoint Protection Manager hérités

A propos de la configuration de Symantec NAC Integrated Enforcer sur une console Enforcer

Après l'installation de Symantec NAC Integrated Enforcer, la configuration s'effectue en deux étapes. D'abord, configurez les paramètres sur la console Integrated Enforcer. Ensuite, reportez-vous à la console de gestion de Symantec Endpoint Protection Manager pour apporter les modifications éventuelles aux paramètres de configuration du groupe auquel appartient Integrated Enforcer. Ces tâches sont présentées ci-dessous.

- Sur la console Enforcer d'Integrated Enforcer pour serveurs DHCP Microsoft, établissez la communication entre Integrated Enforcer et un serveur de gestion.
  Se reporter à "Etablir ou modifier la communication entre Integrated Enforcer et les serveurs Symantec Endpoint Protection Manager " à la page 371.
  Sur la console de gestion de Symantec Endpoint Protection Manager, configurez les paramètres de configuration de Symantec Integrated Enforcer.
- Installez le serveur DHCP avec une configuration de quarantaine.
  Vous devez configurer une classe d'utilisateurs de quarantaine et ajouter des ressources à la classe de quarantaine de chaque sous-réseau. Vous pouvez aussi utiliser l'option de configuration automatique de la quarantaine d'Integrated Enforcer. Elle permet à Integrated Enforcer pour serveurs DHCP Microsoft de configurer la classe d'utilisateurs et les ressources, uniquement si aucune classe de quarantaine n'a été configurée précédemment.
  Se reporter à "Configurer la quarantaine automatique" à la page 373.
- Si vous n'avez pas redémarré le service DHCP sur le serveur DHCP lors de l'installation d'Integrated Enforcer, arrêtez puis démarrez-le maintenant de façon manuelle.

Etablir ou modifier la communication entre Integrated Enforcer et les serveurs Symantec Endpoint Protection Manager

Vous devez spécifier une ou plusieurs consoles Symantec Endpoint Protection Manager auxquelles Integrated Enforcer peut se connecter. Après avoir configuré la liste de serveurs de gestion, vous devez configurer la connexion avec le mot de passe chiffré, le nom de groupe et le protocole de communication. Le mot de passe chiffré était précédemment connu en tant que clé partagée.

Après s'être connecté à un serveur de gestion, Integrated Enforcer s'enregistre automatiquement.

Consultez le *Guide d'administration pour Symantec Endpoint Protection et Symantec Network Access Control* pour plus d'informations sur des listes de serveurs de gestion.

Pour établir la communication entre Integrated Enforcer et un serveur Symantec Endpoint Protection Manager depuis la console Symantec NAC Integrated Enforcer

1. Dans la barre des tâches Windows de l'ordinateur Integrated Enforcer, cliquez sur **Démarrer > Programmes > Symantec Endpoint Protection > Symantec NAC Integrated Enforcer**.

   La console de configuration de Symantec Integrated Enforcer apparaît. Cette page principale affiche l'état de la connexion entre Integrated Enforcer et Symantec Endpoint Protection Manager. Une lumière verte indique qu'Integrated Enforcer est activement connecté au serveur de gestion. Une lumière rouge indique que la connexion est désactivée.

2. Dans le volet gauche, cliquez sur **Symantec Integrated Enforcer > Configure > Management Servers** (Configurer - Serveurs de gestion).

3. Dans le panneau Management Servers (Serveurs de gestion), cliquez sur **Add** (Ajouter) dans la colonne d'icône située à droite de la liste des serveurs de gestion.

4. Dans la boîte de dialogue Add/Edit Management Server , tapez l'adresse IP ou le nom Symantec Endpoint Protection Manager dans le champ de texte Server address.

   Vous pouvez taper une adresse IP, un nom d'hôte ou un nom de domaine. Si vous voulez utiliser un nom d'hôte ou un nom de domaine, vérifiez que le nom sera résolu correctement par le serveur DNS.

5. Dans la boîte de dialogue Add/Edit Management Server (Ajouter/Modifier un serveur de gestion), modifiez le numéro de port qu'Integrated Enforcer utilise pour communiquer avec Symantec Endpoint Protection Manager.

   Le numéro de port par défaut est 8006 pour le protocole HTTP et 443 pour le protocole HTTPS. Le protocole HTTPS doit être configuré de façon identique sur Symantec Endpoint Protection Manager et Integrated Enforcer.

6. Cliquez sur **OK**.

7. Cliquez sur la flèche **Move up** (Vers le haut) ou sur la flèche **Move down** (Vers le bas) de la colonne d'icône située à droite de la liste de serveurs de gestion pour modifier éventuellement l'ordre des serveurs de gestion que Symantec Integrated Enforcer utilise pour se connecter à Symantec Endpoint Protection Manager.

   La première fois qu'il se connecte à Symantec Endpoint Protection Manager, Symantec NAC Integrated Enforcer essaie de se connecter au premier serveur répertorié dans la liste de serveurs de gestion. Si le serveur de gestion n'est pas disponible, Symantec Integrated Enforcer se connecte au serveur de gestion suivant dans la liste des serveurs de gestion.

8. Dans la zone de texte Encrypted password (Mot de passe chiffré), saisissez le mot de passe de la console Symantec Endpoint Protection Manager de connexion.

   Symantec Endpoint Protection Manager et Integrated Enforcer doivent utiliser le même mot de passe chiffré pour la communication.

   Pour afficher les lettres et les numéros de la clé partagée au lieu des astérisques, sélectionnez **Unmask** (Révéler).

9. Dans la zone de texte Preferred group (Groupe préféré), tapez un nom pour le groupe Integrated Enforcer.

   Si vous ne spécifiez aucun nom de groupe, Symantec Endpoint Protection Manager attribue Symantec Integrated Enforcer à un groupe par défaut d'Enforcers dotés de paramètres par défaut. Le nom de groupe par défaut est I-DHCP. Toutefois, Symantec NAC Integrated Enforcer pour serveurs NAP Microsoft et les modules d'application Enforcer basés sur des boîtiers doivent être chacun dans un groupe distinct.

   Vous pouvez afficher les paramètres de groupe dans la console Symantec Endpoint Protection Manager à la page View Servers (Afficher les serveurs).

10 Pour spécifier le protocole que Symantec Integrated Enforcer utilise pour communiquer avec Symantec Endpoint Protection Manager, sélectionnez **HTTP** ou **HTTPS**.

Vous pouvez seulement utiliser le protocole HTTPS si Symantec Endpoint Protection Manager exécute SSL (Secure Sockets Layer).

Si vous avez sélectionné HTTPS et voulez requérir la vérification du certificat de Symantec Endpoint Protection Manager avec une autorité de certification tierce approuvée, cochez **Verify certificate when using HTTPs protocol** (Vérifier le certificat lors de l'utilisation du protocole HTTPS).

11 Cliquez sur **Save**.

Une fois Integrated Enforcer connecté à Symantec Endpoint Protection Manager, vous pouvez modifier la plupart des paramètres de configuration sur la console Symantec Endpoint Protection Manager. Cependant, le secret partagé ou mot de passe chiffré doit être le même sur Integrated Enforcer et Symantec Endpoint Protection Manager afin qu'ils puissent communiquer.

Configurer la quarantaine automatique

Les clients qui tentent de se connecter au réseau envoient une requête DHCP au serveur DHCP.

Soit Symantec NAC Integrated Enforcer peut effectuer la configuration de quarantaine en fonction des adresses IP autorisées, soit vous pouvez configurer une classe d'utilisateurs de quarantaine et lui ajouter des ressources pour chaque sous-réseau depuis le serveur DHCP. Integrated Enforcer ajoute la classe d'utilisateurs de quarantaine à tous les messages DHCP provenant de clients non conformes ou inconnus. Il renouvelle également les demandes du client au serveur DHCP. Les clients de confiance se voient immédiatement attribuer une adresse IP normale et ne sont pas mis en quarantaine. Les clients inconnus ou douteux sont mis en quarantaine, authentifiés, renouvelés si l'authentification réussit et une adresse IP normale leur est assignée.

L'accès est basé sur la politique d'intégrité de l'hôte et les paramètres de groupe définis dans Symantec Endpoint Protection Manager.

Entrez une liste d'adresses IP que vous souhaitez rendre accessibles aux ordinateurs mis en quarantaine, même en cas d'échec de l'authentification.

Pour configurer la quarantaine automatique pour Symantec NAC Integrated Enforcer

1. Dans la barre des tâches Windows de l'ordinateur Integrated Enforcer, cliquez sur **Démarrer > Programmes > Symantec Endpoint Protection > Symantec NAC Integrated Enforcer**.
2. Dans le volet gauche, cliquez sur **Symantec Integrated Enforcer > Configure > Automatic Quarantine Configuration** (Configuration de la quarantaine automatique).
3. Dans la page Automatic Quarantine Configuration d'Integrated Enforcer, cliquez sur **Add** (Ajouter) pour commencer à créer une liste d'adresses IP.
4. Entrez une adresse IP autorisée et cliquez sur **OK** pour l'ajouter à la liste.
5. Cliquez sur **Add** de nouveau pour continuer d'ajouter des adresses IP à la liste.
6. Modifiez la liste IP Address à l'aide des boutons **Edit, Remove, Remove all, Move Up** (Modifier, Supprimer, Supprimer tout, Déplacer vers le haut) ou **Move down** (Déplacer vers le bas).
7. Quand toutes les IP Addresses sont listées ou modifiées, cliquez sur **OK** en bas de la page pour enregistrer vos configurations.

Pour installer une configuration de quarantaine sur un serveur DHCP de Microsoft (tâche facultative avancée)

1. Sur le serveur DHCP, cliquez sur **Start > Administrative Tools > DHCP** (Démarrer Outils d'administration DHCP).

   Pour renouveler la demande avec une configuration de quarantaine, Integrated Enforcer ajoute dynamiquement une classe d'utilisateurs DHCP de quarantaine aux messages DHCP en provenance de clients non conformes. Vous définissez la classe d'utilisateurs de quarantaine en ajoutant un ID appelé : **`SYGATE_ENF`**. Ensuite, vous attribuez diverses ressources à la classe d'utilisateurs, notamment une adresse IP de passerelle, la durée du bail, un serveur DNS et un nombre suffisant d'itinéraires statiques pour la résolution.
2. Dans l'arborescence de la boîte de dialogue DHCP, cliquez avec le bouton droit de la souris sur le serveur DHCP et cliquez sur **Define User Classes** (Définir les classes d'utilisateurs).
3. Dans la boîte de dialogue DHCP User Classes (Classes d'utilisateurs DHCP), cliquez sur **Add** (Ajouter).

4 Dans la boîte de dialogue New Class (Nouvelle classe), tapez un nom d'affichage identifiant cette classe d'utilisateurs de quarantaine comme configuration de quarantaine, ainsi qu'une description facultative.

   Par exemple, vous pouvez identifier une classe d'utilisateurs de quarantaine, telle que QUARANTAINE.

5 Pour définir une nouvelle classe d'utilisateurs, cliquez sur la colonne ASCII et le type **SYGATE_ENF** en majuscules.

6 Cliquez sur **OK**.

7 Cliquez sur **Close** (Fermer).

Pour configurer des options de champ d'application sur un serveur DHCP de Microsoft (tâche facultative avancée)

1 Dans l'arborescence, cliquez avec le bouton droit de la souris sur **Server Options** (Options de serveur).

2 Cliquez sur **Configure Options...** (Configurer les options...).

3 Dans l'onglet Général, cochez **Routeur 003** et configurez l'adresse IP du routeur associé au client de relais DHCP.

4 Dans l'onglet Advanced (Avancé), dans la liste déroulante Vendor class (Classe de constructeur), cliquez sur **DHCP Standard Options** (Options standard DHCP).

5 Dans l'onglet Avancé, dans la liste déroulante Classe d'utilisateur, cliquez sur **QUARANTAINE**.

6 Cochez **Routeur 003**.

7 Dans le champ Adresse IP, tapez **127.0.0.1** (recommandé). Cependant, il incombe à l'administrateur de décider quel IP de routeur, le cas échéant, attribuer aux clients mis en quarantaine.

8 Cochez **Bail 051**.

9 Tapez la valeur hexadécimale de la durée de bail exprimée en secondes.

   Par exemple, pour 2 minutes, tapez 0x78.

10 Cliquez sur **OK**.

11 Cliquez sur **File > Exit** (Fichier > Quitter).

Configuration des paramètres de base de Symantec Integrated Enforcer

Vous pouvez ajouter ou modifier la description d'un module d'application Symantec Integrated Enforcer ou d'un groupe Integrated Enforcer dans la console Symantec Endpoint Protection Manager. Vous pouvez également les ajouter ou les modifier dans la console Integrated Enforcer.

Se reporter à "Ajout ou modification de la description d'un groupe d'Enforcer avec un module Symantec Integrated Enforcer" à la page 377.

Se reporter à "Ajout ou modification de la description d'un module Symantec Integrated Enforcer" à la page 377.

Toutefois, vous ne pouvez pas ajouter ou modifier le nom d'un groupe Integrated Enforcer dans la console Symantec Endpoint Protection Manager. Vous ne pouvez pas ajouter ou modifier l'adresse IP ou le nom d'hôte d'un module d'application Integrated Enforcer dans la console Symantec Endpoint Protection Manager. Au lieu de cela, vous devez effectuer ces tâches sur la console Enforcer.

Se reporter à "Ajout ou modification du nom d'un groupe Enforcer pour Symantec Integrated Enforcer" à la page 376.

Vous pouvez ajouter ou modifier l'adresse IP ou le nom d'hôte d'un module Integrated Enforcer dans une liste de serveurs de gestion.

Se reporter à "Ajout ou modification de l'adresse IP ou du nom d'hôte d'un module Symantec Integrated Enforcer" à la page 377.

Vous devez connecter le module Integrated Enforcer à Symantec Endpoint Protection Manager.

Se reporter à "Connexion de Symantec Integrated Enforcer à Symantec Endpoint Protection Manager" à la page 378.

Ajout ou modification du nom d'un groupe Enforcer pour Symantec Integrated Enforcer

Vous pouvez ajouter ou modifier le nom d'un groupe de modules d'application Enforcer dont un module Integrated Enforcer est membre. Effectuez ces tâches sur la console Enforcer pendant l'installation. Plus tard, si vous voulez modifier le nom d'un groupe Enforcer, vous pouvez le faire sur la console Enforcer.

Se reporter à "Etablir ou modifier la communication entre Integrated Enforcer et les serveurs Symantec Endpoint Protection Manager " à la page 371.

Tous les modules Enforcer d'un groupe partagent les mêmes paramètres de configuration.

Ajout ou modification de la description d'un groupe d'Enforcer avec un module Symantec Integrated Enforcer

Vous pouvez ajouter ou modifier le nom d'un groupe d'Enforcer dont un module Symantec Integrated Enforcer est membre. Vous pouvez effectuer cette tâche sur la console Symantec Endpoint Protection Manager au lieu de la console Integrated Enforcer.

Ajout ou modification de la description d'un groupe d'Enforcer avec un module Symantec Integrated Enforcer

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin, cliquez sur **Serveurs**.
3. Dans la page Admin, sous Afficher les serveurs, sélectionnez et développez le groupe d'Enforcer dont vous voulez ajouter ou modifier le nom.
4. Dans la page Admin, sous Tâches, cliquez sur **Modifier les propriétés du groupe**.
5. Dans la boîte de dialogue Settings (Paramètres), sous l'onglet General (Général), ajoutez ou modifiez une description pour le groupe de boîtiers Enforcer dans le champ Description.
6. Dans la boîte de dialogue Paramètres, cliquez sur **OK**.

Ajout ou modification de l'adresse IP ou du nom d'hôte d'un module Symantec Integrated Enforcer

Vous pouvez seulement changer l'adresse IP ou le nom d'hôte d'un module Integrated Enforcer sur la console d'Enforcer pendant l'installation. Si vous voulez modifier l'adresse IP ou le nom d'hôte du module Integrated Enforcer plus tard, vous pourrez le faire sur la console du module Integrated Enforcer.

Ajout ou modification de la description d'un module Symantec Integrated Enforcer

Vous pouvez ajouter ou modifier la description d'un module Symantec Integrated Enforcer. Vous pouvez effectuer cette tâche sur la console Symantec Endpoint Protection Manager au lieu de la console Integrated Enforcer. Après avoir terminé cette tâche, la description apparaît dans le champ Description du volet Gestion du serveur.

Pour ajouter ou modifier la description d'un module Symantec Integrated Enforcer

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin, cliquez sur **Serveurs**.
3. Sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe d'Enforcer qui inclut le module Integrated Enforcer dont vous souhaitez ajouter ou modifier la description.
4. Sélectionnez le module Integrated Enforcer dont vous souhaitez ajouter ou modifier la description.
5. Sous Tasks (Tâches), cliquez sur **Edit Enforcer Properties** (Modifier les propriétés d'Enforcer).
6. Dans la boîte de dialogue Enforcer Properties (Propriétés d'Enforcer), ajoutez ou modifiez une description pour le module d'application Integrated Enforcer dans le champ Description.
7. Cliquez sur **OK**.

Connexion de Symantec Integrated Enforcer à Symantec Endpoint Protection Manager

Les modules d'application Enforcer doivent pouvoir se connecter aux serveurs sur lesquels Symantec Endpoint Protection Manager est installé. Symantec Endpoint Protection Manager comprend un fichier qui aide à la gestion du trafic entre les clients, les gestionnaires Symantec Endpoint Protection Manager et les modules d'application Enforcer facultatifs tels qu'Integrated Enforcer. Ce fichier est appelé liste de serveurs de gestion.

La liste de serveurs de gestion spécifie à quel serveur Symantec Endpoint Protection Manager connecte un module d'application Integrated Enforcer. Elle spécifie également à quel serveur Symantec Endpoint Protection un module d'application Integrated Enforcer se connecte en cas de défaillance d'un serveur de gestion.

Une liste de serveurs de gestion par défaut est automatiquement créée pour chaque site pendant l'installation initiale. Tous les gestionnaires Symantec Endpoint Protection Manager disponibles sur le site sont automatiquement ajoutés à la liste de serveurs de gestion par défaut.

La liste de serveurs de gestion par défaut comprend les adresses IP ou les noms d'hôte du serveur de gestion auxquels les modules d'application Integrated Enforcer peuvent se connecter après l'installation initiale. Vous pouvez créer une liste de serveurs de gestion personnalisée avant de déployer des modules d'application Enforcer. Si vous créez une liste de serveurs de gestion personnalisée, vous pouvez

spécifier la priorité de connexion d'un module d'application Integrated Enforcer aux serveurs de gestion.

Vous pouvez sélectionner la liste de serveurs de gestion spécifique comprenant les adresses IP ou les noms d'hôte des serveurs de gestion auxquels vous voulez qu'Integrated Enforcer se connecte. Si le site ne comprend qu'un seul serveur de gestion, vous pouvez sélectionner la liste de serveurs de gestion par défaut.

Consultez le *Guide d'administration de Symantec Endpoint Protection et Symantec Network Access Control* pour plus d'informations sur la personnalisation des listes de serveurs de gestion.

Connexion de Symantec Integrated Enforcer à Symantec Endpoint Protection Manager

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.

   Le groupe Enforcer doit comprendre le module d'application Integrated Enforcer dont vous voulez modifier l'adresse IP ou le nom d'hôte dans une liste de serveurs de gestion.
4. Sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés de groupe).
5. Dans la boîte de dialogue Settings (Paramètres), dans l'onglet General (Général), sous Communication, sélectionnez la liste de serveurs de gestion à utiliser par ce module d'application Integrated Enforcer.
6. Dans l'onglet Général, sous Communication, cliquez sur **Sélectionner**.

   Vous pouvez afficher les adresses IP et les noms d'hôte de tous les serveurs de gestion disponibles, ainsi que les priorités qui leur ont été attribuées.
7. Dans la boîte de dialogue Management Server List (Listes de serveurs de gestion), cliquez sur **Close** (Fermer).
8. Dans la boîte de dialogue General (Général), cliquez sur **OK**.

Modifier une connexion Symantec Endpoint Protection Manager

Si nécessaire, vous pouvez mettre à jour l'adresse de serveur et les informations de port de Symantec Endpoint Protection Manager.

Pour modifier une connexion Symantec Endpoint Protection Manager

1. Dans la barre des tâches Windows de l'ordinateur Enforcer, cliquez sur **Démarrer > Programmes > Symantec Endpoint Protection > Symantec Integrated NAP Enforcer**.
2. Dans le volet de gauche, développez Symantec Integrated Enforcer.
3. Développez Configure (Configurer).
4. Cliquez sur **Management Servers** (Serveurs de gestion).
5. Dans le volet Management Servers, cliquez sur **Edit** (Modifier) dans la colonne d'icônes située à droite de la liste des serveurs de gestion.
6. Dans la boîte de dialogue Add/Edit Management Server , tapez l'adresse IP ou le nom Symantec Endpoint Protection Manager dans le champ de texte Server address.

   Vous pouvez taper une adresse IP, un nom d'hôte ou un nom de domaine. Si vous voulez utiliser un nom d'hôte ou un nom de domaine, Symantec Integrated Enforcer doit se connecter à un serveur DNS.
7. Cliquez sur **OK**.

Configurer une liste de fournisseurs approuvés

Les agents ne peuvent pas être installés sur certains périphériques réseau tels que les imprimantes ou les téléphones IP. Pour résoudre ces cas, vous pouvez configurer une liste de fournisseurs approuvés. Si le nom du fournisseur est considéré approuvé, alors le boîtier Symantec NAC Integrated Enforcer n'authentifiera pas le périphérique. Les périphériques obtiennent dans ce cas des adresses IP normales du serveur DHCP.

Pour configurer une liste de fournisseurs approuvés

1. Dans la barre des tâches Windows de l'ordinateur Integrated Enforcer, cliquez sur **Démarrer > Programmes > Symantec Endpoint Protection > Symantec NAC Integrated Enforcer**.
2. Dans le volet gauche, cliquez sur **Symantec Integrated Enforcer > Configure > DHCP Trusted Vendors Configuration** (Configuration des fournisseurs approuvés DHCP).
3. Pour activer la liste de fournisseurs approuvés, sélectionnez **Turn on Trusted Vendors** (Activer les fournisseurs approuvés).

   Lorsque la case à cocher Turn on Trusted Vendors (Activer les fournisseurs approuvés) est activée, l'intégrité de l'hôte ne sera pas appliquée pour le trafic DHCP provenant des fournisseurs approuvés sélectionnés.

4 Sélectionnez les fournisseurs que vous voulez qualifier d'approuvés.

5 Cliquez sur **Save** (Enregistrer).

Afficher les journaux Enforcer sur une console Enforcer

Symantec Integrated Enforcer consigne automatiquement des messages dans les journaux Enforcer Client (Client Enforcer) et Enforcer System (Système Enforcer). Ces journaux sont chargés dans Symantec Endpoint Protection Manager. Le journal client fournit des informations sur les connexions client et la communication avec Integrated Enforcer. Le journal système enregistre les informations associées à Integrated Enforcer, notamment les instances de démarrage et d'arrêt du service Enforcer.

Dans la console Symantec Endpoint Protection Manager, vous pouvez activer la journalisation et les paramètres de fichiers journaux pour Integrated Enforcer. Par défaut, tous les journaux sont activés et envoyés à Symantec Endpoint Protection Manager.

Pour afficher des journaux Enforcer sur une console Enforcer

1 Dans le volet gauche, développez **Symantec NAC Integrated Enforcer**.

2 Développez **View Logs** (Afficher les journaux) et cliquez sur **System Log** (Journal système) ou **Client Log** (Journal client).

3 Pour afficher toutes les modifications apportées au journal depuis sa dernière ouverture, cliquez sur **Refresh** (Actualiser).

4 Cliquez sur **OK**.

Configuration des journaux Symantec Integrated Enforcer

Les journaux Symantec Integrated Enforcer sont enregistrés sur l'ordinateur sur lequel vous avez installé Symantec Integrated Enforcer. Les journaux Enforcer sont générés par défaut.

Si vous voulez afficher des journaux Enforcer sur la console Symantec Endpoint Protection Manager, vous devez activer l'envoi de journaux sur la console Symantec Endpoint Protection Manager. Si cette option est activée, les données de journal sont envoyées depuis Integrated Enforcer vers Symantec Endpoint Protection Manager et enregistrées dans une base de données.

Vous pouvez modifier les paramètres de journal pour Integrated Enforcer sur la console Symantec Endpoint Protection Manager. Les activités sont enregistrées dans le même journal de serveur Enforcer pour tous les modules d'application Enforcer sur un site.

Vous pouvez configurer les paramètres pour les journaux suivants que le module Integrated Enforcer génère :

- Journal de serveur Enforcer
  Le journal de serveur Enforcer fournit les informations liées au fonctionnement d'un module Enforcer.
- Journal de client Enforcer
  Le journal Client fournit des informations sur les interactions entre Integrated Enforcer et les clients qui ont essayé de se connecter au réseau. Il affiche des informations sur l'authentification, les échecs d'authentification et les déconnexions.

Configuration des paramètres d'authentification de Symantec Integrated Enforcer

Vous pouvez spécifier un certain nombre de paramètres d'authentification pour une session d'authentification de module Integrated Enforcer. Lorsque vous appliquez ces modifications, elles sont envoyées automatiquement au module Integrated Enforcer sélectionné pendant le battement suivant.

A propos de l'utilisation des paramètres d'authentification

Vous pouvez mettre en application un certain nombre de paramètres d'authentification pour sécuriser davantage le réseau.

Tableau 20-1 fournit plus d'informations sur les options de l'onglet Authentification.

Tableau 20-1 Paramètres de configuration d'authentification pour Symantec Integrated Enforcer

Option	Description
Nombre maximal de paquets par session d'authentification	Nombre maximal de paquets de sollicitation qu'Integrated Enforcer envoie par session d'authentification. Le nombre par défaut est de 10. Se reporter à "Spécifier le nombre maximum de paquets pendant une session d'authentification" à la page 386.

Option	Description
Temps entre les paquets en session d'authentification	Temps (en secondes) entre les paquets de sollicitation envoyés par Enforcer. La valeur par défaut est 3 secondes. Se reporter à "Spécification de la fréquence des paquets de stimulation à envoyer aux clients" à la page 386.
Autoriser tous les clients, mais continuer à consigner les clients non authentifiés	Si cette option est activée, Enforcer authentifie tous les utilisateurs en vérifiant qu'ils exécutent un client. Il transfère alors la demande d'Integrated de recevoir une configuration réseau normale plutôt qu'une configuration réseau de quarantaine, indépendamment de l'échec ou de la réussite des vérifications. Le paramètre par défaut n'est pas activé. Se reporter à "Autorisation de tous les clients avec la connexion continue des clients non-authentifiés" à la page 387.
Autoriser tous les clients avec des systèmes d'exploitation non Windows	Si cette option est activée, Integrated Enforcer vérifie le système d'exploitation du client. Integrated Enforcer permet alors à tous les clients n'exécutant pas le système d'exploitation Windows de recevoir une configuration réseau normale sans être authentifié. Si cette option n'est pas activée, les clients reçoivent une configuration réseau de quarantaine. Le paramètre par défaut n'est pas activé. Se reporter à "Autorisation des clients non-Windows à se connecter à un réseau sans authentification" à la page 389.

Option	Description
Vérifier le numéro de série de politique du Client avant de permettre au client d'accéder au réseau	Si cette option est activée, Integrated Enforcer vérifie si le client a reçu les dernières politiques de sécurité du serveur de gestion. Si le numéro de série de politique n'est pas le plus récent, Integrated Enforcer informe le client de la nécessité de mise à jour de sa politique de sécurité. Le client transfère alors la demande d'Integrated de recevoir une configuration réseau de quarantaine. Si cette option n'est pas activée et si la vérification de l'intégrité de l'hôte réussit, Integrated Enforcer transfère la demande d'Integrated de recevoir une configuration réseau normale. Integrated Enforcer transfère la demande d'Integrated même si le client n'a pas la dernière politique de sécurité. Le paramètre par défaut n'est pas activé. Se reporter à "Faire vérifier le numéro de série de politique d'un client par Symantec Integrated Enforcer" à la page 389.
Activer le message instantané sur le client si le logiciel client ne s'exécute pas	Cette option est affichée mais actuellement indisponible pour Symantec Integrated Enforcer. Se reporter à "Envoi d'un message de Symantec Integrated Enforcer à un client à propos de non-conformité" à la page 391.

A propos des sessions d'authentification

Quand un client essaye d'accéder au réseau interne, Symantec Integrated Enforcer détecte d'abord si le client exécute un logiciel client. Si oui, le module d'application Enforcer transfère le message DHCP client au serveur DHCP pour obtenir une adresse IP de quarantaine restreinte. Ce processus est utilisé en interne par Integrated Enforcer pour son procédé d'authentification.

Integrated Enforcer commence alors sa session d'authentification avec le client. Une session d'authentification est un ensemble de paquets de sollicitation qu'Integrated Enforcer envoie à un client.

Pendant la session d'authentification, Enforcer envoie un paquet de sollicitation au client à une fréquence spécifiée. Le paramètre par défaut est toutes les trois secondes.

Integrated Enforcer continue à envoyer des paquets jusqu'à ce qu'une des conditions suivantes soit remplie :

- Le module Integrated Enforcer reçoit une réponse du client

- Integrated Enforcer a envoyé le nombre maximum de paquets spécifiés. Le paramètre par défaut est 10.

La fréquence (3 secondes) multipliée par le nombre de paquets (10) est la valeur utilisée pour le battement Enforcer. Le battement est l'intervalle pendant lequel Integrated Enforcer permet au client de rester connecté avant de démarrer une nouvelle session d'authentification. Le paramètre par défaut est de trois secondes.

Le client envoie des données à Integrated Enforcer, contenant les éléments suivants :

- Identificateur unique (UID)
- Son numéro de série de profil actuel
- Les résultats de la vérification d'intégrité de l'hôte

Integrated Enforcer vérifie l'identificateur UID et le numéro de série de politique du client auprès de Symantec Endpoint Protection Manager. Si le client a été mis à jour avec les dernières politiques de sécurité, son numéro de série de politique correspond à celui qu'Integrated Enforcer reçoit du serveur de gestion. Les résultats de vérification d'intégrité de l'hôte montrent si le client est conforme aux politiques de sécurité actuelles.

Si les données du client vérifient les conditions d'authentification, Symantec Integrated Enforcer fait suivre sa requête DHCP au serveur DHCP. Integrated Enforcer s'attend à recevoir une configuration réseau DHCP normale. Sinon, Integrated Enforcer transfère la requête au serveur DHCP de quarantaine pour recevoir une configuration réseau de quarantaine.

Vous pouvez installer un serveur DHCP sur un ordinateur et le configurer pour fournir une configuration réseau normale et une configuration réseau de quarantaine.

Après l'intervalle de battement ou toutes les fois que le client essaye de renouveler son adresse IP, Integrated Enforcer démarre une nouvelle session d'authentification. Le client doit répondre pour maintenir la connexion au réseau interne.

Integrated Enforcer déconnecte les clients qui ne répondent pas.

Pour les clients précédemment authentifiés mais qui échouent maintenant à l'authentification, Integrated Enforcer envoie un message au serveur DHCP. Le message est une demande de libérer l'adresse IP actuelle. Integrated Enforcer envoie alors un message DHCP au client. Le client envoie alors une demande de renouvellement de l'adresse IP et de la configuration réseau à Integrated Enforcer. Integrated Enforcer fait suivre cette demande au serveur DHCP de quarantaine.

Spécifier le nombre maximum de paquets pendant une session d'authentification

Pendant la session d'authentification, Integrated Enforcer envoie un paquet au client à une fréquence spécifiée.

Integrated Enforcer continue à envoyer des paquets jusqu'à ce que les conditions suivantes soient remplies :

- Integrated Enforcer reçoit une réponse du client.
- Integrated Enforcer a envoyé le nombre maximum spécifié de paquets.

Le paramètre par défaut pour le nombre maximum de paquets pour une session d'authentification est 10.

Pour spécifier le nombre maximum de paquets de stimulation pendant une session d'authentification

1. Dans la console Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administration).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.

   Le groupe de modules d'application Enforcer doit inclure le module d'application Integrated Enforcer pour lequel vous devez spécifier le nombre maximum de paquets de stimulation envoyés pendant une session d'authentification.
4. Sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés de groupe).
5. Sur l'onglet Authentification, saisissez le nombre maximum de paquets que vous voulez autoriser pendant une session d'authentification dans le champ **Maximum number of packets per authentication session** (Nombre maximal de paquets par session d'authentification).

   Le paramètre par défaut est 10.
6. Dans la boîte de dialogue Settings (Paramètres), sur l'onglet Authentication (Authentification), cliquez sur **OK**.

Spécification de la fréquence des paquets de stimulation à envoyer aux clients

Pendant la session d'authentification, le module Integrated Enforcer envoie un paquet de stimulation au client à une fréquence spécifiée.

Le module Integrated Enforcer continue d'envoyer des paquets jusqu'à ce que les conditions suivantes soient remplies :

- Le module Integrated Enforcer reçoit une réponse du client
- Le module Integrated Enforcer a envoyé le nombre de paquets maximum spécifié.

Le paramètre par défaut est toutes les 3 secondes.

Pour spécifier la fréquence des paquets de stimulation à envoyer aux clients

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin, cliquez sur **Serveurs**.
3. Sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.

   Le groupe de boîtiers Enforcer doit inclure le module d'application Integrated Enforcer pour lequel vous voulez spécifier la fréquence des paquets de stimulation à envoyer aux clients.
4. Sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Sous l'onglet Authentication (Authentification), sous Authentication Parameters (Paramètres d'authentification), tapez le nombre maximum de paquets de stimulation que le module Integrated Enforcer doit envoyer à un client pendant une session d'authentification dans le champ **Time between packets in authentication session** (Temps entre les paquets pendant la session d'authentification).

   Le paramètre par défaut est 10.
6. Dans la boîte de dialogue Paramètres, dans l'onglet Authentification, cliquez sur **OK**.

Autorisation de tous les clients avec la connexion continue des clients non-authentifiés

Déployer l'ensemble des logiciels client peut prendre un certain temps. Vous pouvez vouloir configurer le module Integrated Enforcer pour permettre à tous les clients de se connecter au réseau jusqu'à ce que vous ayez fini de distribuer le paquet client à tous les utilisateurs. Ces utilisateurs se connectent tous à un serveur Integrated à l'emplacement de ce module d'application Integrated Enforcer.

Le module Integrated Enforcer authentifie toujours tous les utilisateurs en vérifiant qu'ils exécutent un client, en vérifiant l'intégrité de l'hôte et en consignant les

résultats. Il fait suivre les requêtes DHCP pour recevoir la configuration réseau de serveur DHCP normale au lieu de la configuration réseau de quarantaine. Ce processus se produit indépendamment de l'échec ou de la réussite des vérifications de l'intégrité de l'hôte.

Le paramètre n'est pas activé par défaut.

Suivez les directives suivantes quand vous appliquez les paramètres de configuration :

- Ce paramètre doit être une mesure temporaire parce qu'il rend le réseau moins sécurisé.
- Lorsque ce paramètre est en vigueur, vous pouvez passer en revue les journaux Enforcer. Vous pouvez vous renseigner sur les types de clients qui essayent de se connecter au réseau à cet emplacement.

  Par exemple, vous pouvez passer en revue le journal d'activités client pour savoir si des clients ne disposent pas du logiciel client. Vous pouvez ensuite vérifier que le logiciel client est installé sur ces clients avant de désactiver cette option.

Pour autoriser tous les clients avec la connexion continue des clients non-authentifiés

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.

   Le groupe Enforcer doit inclure le module d'application Integrated Enforcer pour lequel vous voulez autoriser tous les clients tout en consignant les clients non-authentifiés.
4. Sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés de groupe).
5. Dans la boîte de dialogue Paramètres, dans l'onglet Authentification, cochez **Allow all clients, but continue to log which clients are not authenticated** (Autoriser tous les clients, mais continuer à consigner les clients non authentifiés).

   Le paramètre n'est pas activé par défaut.
6. Dans la boîte de dialogue Settings (Paramètres), sur l'onglet Authentication (Authentification), cliquez sur **OK**.

Autorisation des clients non-Windows à se connecter à un réseau sans authentification

Le module Integrated Enforcer ne peut pas authentifier un client qui prend en charge un système d'exploitation non-Windows. Par conséquent les clients non-Windows ne peuvent pas se connecter au réseau à moins que vous ne les autorisiez spécifiquement à se connecter au réseau sans authentification.

Le paramètre n'est pas activé par défaut.

Vous pouvez utiliser une des méthodes suivantes pour activer les clients qui prennent en charge une plate-forme non-Windows pour se connecter au réseau :

- Spécifiez chaque client non-Windows comme hôte approuvé.
- Autorisez tous les clients avec des systèmes d'exploitation non-Windows

Pour autoriser des clients non-Windows à se connecter à un réseau sans authentification

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.

   Le groupe Enforcer doit inclure le module d'application Integrated Enforcer pour lequel vous voulez autoriser l'ensemble des clients non-Windows à se connecter à un réseau.
4. Sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés de groupe).
5. Dans la boîte de dialogue Settings (Paramètres), dans l'onglet Authentication (Authentification), cochez **Allow all clients with non-Windows operating systems** (Autoriser tous les clients avec des systèmes d'exploitation non-Windows).

   Le paramètre n'est pas activé par défaut.
6. Dans la boîte de dialogue Settings (Paramètres), sur l'onglet Authentication (Authentification), cliquez sur **OK**.

Faire vérifier le numéro de série de politique d'un client par Symantec Integrated Enforcer

Symantec Endpoint Protection Manager met à jour le numéro de série de politique d'un client chaque fois que la politique de sécurité du client change. Lorsqu'un

client se connecte à Symantec Endpoint Protection Manager, il reçoit les dernières politiques de sécurité et le dernier numéro de série de politique.

Lorsqu'un client essaye de se connecter au réseau par Integrated Enforcer, Integrated Enforcer récupère le numéro de série de politique auprès de Symantec Endpoint Protection Manager. Integrated Enforcer compare alors le numéro de série de politique à celui qu'il reçoit du client. Si les numéros de série de politique correspondent, Integrated Enforcer confirme que le client exécute une politique de sécurité à jour.

La valeur par défaut pour ce paramètre n'est pas activée.

Les directives suivantes s'appliquent :

- Si l'option Check the Policy Serial Number on Client before allowing Client into network (Vérifier le numéro de série de politique du Client avant de permettre au client d'accéder au réseau) est activée, le client doit avoir la dernière politique de sécurité pour pouvoir se connecter au réseau par le serveur DHCP normal. Si le client ne dispose pas de la dernière politique de sécurité, il est informé qu'il doit télécharger la dernière politique. Integrated Enforcer fait alors suivre sa requête DHCP pour recevoir une configuration réseau de quarantaine.
- Si l'option Check the Policy Serial Number on Client before allowing Client into network (Vérifier le numéro de série de la politique du client avant d'autoriser l'accès au réseau) n'est pas cochée et si la vérification de l'intégrité de l'hôte est réussie, le client peut se connecter au réseau. Le client peut se connecter par le serveur DHCP normal même si sa politique de sécurité n'est pas à jour.

Pour faire vérifier le numéro de série de politique d'un client par Symantec Integrated Enforcer

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.

   Le groupe de modules d'application Enforcer doit inclure le module d'application Integrated Enforcer qui vérifie le numéro de série de politique des clients.
4. Sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés de groupe).

5 Dans la boîte de dialogue Settings (Paramètres), dans l'onglet Authentication (Authentification), cochez **Check the Policy Serial Number on the Client before allowing a Client into the network** (Vérifier le numéro de série de politique sur le client avant de permettre à un client d'accéder au réseau).

6 Dans la boîte de dialogue Settings (Paramètres), sur l'onglet Authentication (Authentification), cliquez sur **OK**.

Envoi d'un message de Symantec Integrated Enforcer à un client à propos de non-conformité

Bien que cette option soit affichée, elle est actuellement indisponible pour la configuration de Symantec Integrated Enforcer.

Etablissement de la communication entre Symantec Integrated Enforcer et Network Access Control Scanner sur une console Enforcer

Integrated Enforcer peut être configuré pour se connecter à des analyseurs Network Access Control Scanner. Lorsque Network Access Control Scanner est activé, il vérifie la sécurité des clients. Si l'analyseur détermine qu'aucun client n'est en cours d'exécution sur l'ordinateur client, la règle de politique est déclenchée. Le client est autorisé à accéder au réseau interne ou son accès est bloqué.

Remarque : Symantec Network Access Control Scanner ne prend pas en charge la connexion d'une imprimante à boîtier Symantec NAC Integrated Enforcer. Les imprimantes n'acceptent pas les itinéraires statiques configurés pour un boîtier Symantec Integrated Enforcer. Par conséquent, Symantec Network Access Control Scanner ne peut pas communiquer avec une imprimante connectée à un boîtier Integrated Enforcer.

Remarque : Le service Integrated Enforcer doit être redémarré lorsque l'analyseur est activé ou désactivé.

Pour établir la communication entre Symantec NAC Integrated Enforcer et Network Access Control Scanner sur la console Enforcer

1. Dans la barre des tâches Windows de l'ordinateur Integrated Enforcer, cliquez sur **Démarrer > Programmes > Symantec Endpoint Protection > Symantec NAC Integrated Enforcer**.
2. Dans le volet gauche, cliquez sur **Symantec Integrated Enforcer > Configure (Configurer) > Network Access Control Scanner**.
3. Pour activer des analyseurs Network Access Control Scanner, cochez la case **Turn on NAC scanner** (Activer l'analyseur NAC).
4. Pour ajouter ou modifier un analyseur Network Access Control Scanner, cliquez sur **Add** (Ajouter).
5. Entrez l'adresse, le nom d'hôte ou le nom DNS dans la boîte de dialogue Add/Edit management server (Ajouter/Modifier un serveur de gestion) de l'analyseur NAC et cliquez sur **OK**.
6. Entrez le mot de passe de chiffrement qui est configuré sur l'analyseur.

   Le secret partagé ou le mot de passe chiffré doit être le même que celui qui est défini sur l'analyseur.

   Pour afficher les lettres et les numéros de la clé partagée au lieu des astérisques, sélectionnez **Unmask** (Révéler).
7. Une fois que des adresses d'analyseur ont été ajoutées à la liste Address (Adresse), vous pouvez modifier celle-ci en cliquant sur les boutons **Edit (Modifier), Remove (Supprimer), Remove all (Supprimer tout), Move Up** (Déplacer vers le haut) ou **Move Down** (Déplacer vers le bas).

   Integrated Enforcer se connecte aux analyseurs NAC en fonction de leur ordre d'apparition dans la liste NAC Scanner Address (Adresses des analyseurs NAC).
8. Cliquez sur **OK** pour terminer la constitution de la liste des analyseurs NAC et leur configuration.

   Le service Integrated Enforcer doit être redémarré lorsque l'analyseur est activé ou désactivé.

Configuration des paramètres avancés de Symantec Integrated Enforcer

Vous pouvez configurer les paramètres de configuration avancés suivants d'Integrated Enforcer :

- paramètres de délai d'expiration, délai d'expiration d'authentification et délai d'expiration de message DHCP
  Bien que ces options soient affichées, elles sont actuellement indisponibles pour la configuration de Symantec Integrated Enforcer.
- Adresses MAC des hôtes approuvés qu'Integrated Enforcer autorise à se connecter au serveur DHCP normal sans authentification
  Se reporter à "Autorisation des serveurs, des clients et des périphériques à se connecter au réseau en tant qu'hôtes approuvés sans authentification" à la page 393.
- Activation d'authentification locale
  Se reporter à "Activation de l'authentification locale sur Integrated Enforcer" à la page 395.

Lorsque vous appliquez ces paramètres de configuration, les modifications sont envoyées au Symantec Integrated Enforcer sélectionné pendant le battement suivant.

Autorisation des serveurs, des clients et des périphériques à se connecter au réseau en tant qu'hôtes approuvés sans authentification

Un hôte approuvé est en général un serveur qui ne peut pas installer le logiciel client comme un serveur non Windows ou un périphérique comme une imprimante. Vous pouvez également vouloir identifier des clients non-Windows en tant qu'hôtes approuvés parce qu'Integrated Enforcer est incapable d'authentifier tous les clients qui n'exécutent pas le client Symantec Endpoint Protection ou le client Symantec Network Access Control.

Vous pouvez utiliser des adresses MAC pour spécifier certains serveurs, clients et périphériques comme hôtes approuvés.

Quand vous spécifiez des serveurs, des clients et des périphériques comme hôtes approuvés, Integrated Enforcer transmet tous les messages DHCP de l'hôte approuvé au serveur DHCP normal sans authentifier l'hôte approuvé.

Pour autoriser des serveurs, des clients et des périphériques à se connecter au réseau en tant qu'hôtes approuvés sans authentification

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Enforcer.

4. Sélectionnez le module Integrated Enforcer qui autorise les serveurs, les clients et les périphériques indiqués en tant qu'hôtes approuvés à se connecter au réseau sans authentification.
5. Sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés de groupe).
6. Dans la boîte de dialogue Paramètres, dans l'onglet Avancé, sous Hôtes approuvés, cliquez sur **Ajouter**.
7. Dans la boîte de dialogue Ajouter un hôte approuvé, tapez Adresse MAC pour le client ou l'hôte approuvé dans le champ Adresse MAC de l'hôte.

   Vous pouvez également copier un ensemble d'adresses MAC d'un fichier texte.

   Quand vous spécifiez une adresse MAC, vous pouvez utiliser un caractère générique si vous le tapez dans chacun des trois champs de droite.

   Par exemple, 11-22-23-*-*-* est un exemple d'utilisation correcte du caractère générique. Cependant, 11-22-33-44-*-66 ne représente pas une utilisation correcte du caractère générique.
8. Cliquez sur **OK**.
9. Dans la boîte de dialogue Paramètres, dans l'onglet Avancé, cliquez sur **OK**.

   L'adresse MAC de l'hôte approuvé que vous avez ajouté apparaît maintenant dans la zone Adresse MAC de la boîte de dialogue Paramètres.
10. Cliquez sur **OK**.

Autorisation d'un client hérité à se connecter au réseau avec Integrated Enforcer

Vous pouvez activer un Symantec Integrated Enforcer de sorte à ce qu'il se connecte à des clients hérités 5.1.x. Si votre réseau prend en charge une console Symantec Endpoint Protection Manager 11.0.2 ainsi qu'un boîtier Symantec Integrated Enforcer et qu'il doit prendre en charge des clients hérités 5.1.x, vous pouvez activer la prise en charge des clients hérités 5.1.x sur la console du serveur de gestion afin que le boîtier Symantec Integrated Enforcer ne les bloque pas.

Pour autoriser un client hérité à se connecter au réseau avec un boîtier Integrated Enforcer

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin, cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Integrated Enforcers.

4 Dans la page Admin, sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).

5 Dans la boîte de dialogue Settings (Paramètres), dans l'onglet Advanced (Avancés), sélectionnez **Allow legacy clients** (Autoriser les clients hérités).

6 Cliquez sur **OK**.

Activation de l'authentification locale sur Integrated Enforcer

L'authentification locale étant activée, si Integrated Enforcer perd sa connexion avec le client sur lequel Symantec Endpoint Protection Manager est installé, Integrated Enforcer authentifie les clients localement. Dans ce cas, Integrated Enforcer considère le client comme un utilisateur valide et ne vérifie que l'état d'intégrité de l'hôte du client.

Remarque : Si Integrated Enforcer ne perd pas sa connexion au serveur Symantec Endpoint Protection Manager server, il demande toujours à ce dernier de vérifier l'identificateur unique (UID) du client, que l'authentificaiton locale soit activée ou non.

Pour activer l'authentification locale sur Integrated Enforcer

1 Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).

2 Dans la page Admin (Admin), cliquez sur **Servers** (Serveurs).

3 Sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules Integrated Enforcer.

4 Sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés de groupe).

5 Dans la boîte de dialogue Settings (Paramètres), dans l'onglet Advanced (Avancé), sélectionnez **Enable Local Authentication** (Activer l'authentification locale).

6 Cliquez sur **OK**.

Arrêter et démarrer les services de communication entre Integrated Enforcer et un serveur de gestion

Pour le dépannage, vous pouvez arrêter et démarrer le service Enforcer ou le service (SNACLink.exe) qui communique avec Symantec Endpoint Protection Manager. Si vous arrêtez le service Enforcer, Integrated Enforcer supprime les

informations de conformité pour les clients existants. Il arrête également la collecte des informations pour les nouveaux clients. Cependant, il continue à communiquer avec Symantec Endpoint Protection Manager.

Si Symantec Endpoint Protection Manager est indisponible, Integrated Enforcer impose toujours la version de politique et le GUID pour tous les clients authentifiés. Le même processus est appliqué si vous arrêtez la connexion à Symantec Endpoint Protection Manager. Ces informations sont stockées dans le cache local (mais seulement si le cache est activé). Il authentifie automatiquement de nouveaux clients (en fonction de leur état d'intégrité d'hôte) mais ignore la vérification de politique et de GUID.

Dès que la communication à Symantec Endpoint Protection Manager est rétablie, Integrated Enforcer met à jour la version de politique. Il authentifie également les clients qui ont été ajoutés depuis que la connexion a été perdue.

Remarque : Vous pouvez configurer Symantec Integrated Enforcer pour mettre en quarantaine de nouveaux clients au lieu de les authentifier pendant que la connexion à Symantec Endpoint Protection Manager est indisponible. Pour cela, vous modifiez la valeur par défaut de la clé DetectEnableUidCache dans le registre.

L'arrêt d'Integrated Enforcer n'a pas d'incidence sur le serveur DHCP. En cas d'arrêt d'Integrated Enforcer, le serveur DHCP fonctionne comme si Enforcer n'était pas installé. Lorsque le serveur DHCP est indisponible, Integrated Enforcer arrête de collecter l'état de conformité des nouveaux clients. Cependant, il continue à communiquer avec les clients existants et continue à consigner les changements d'état. La maintenance et d'autres problèmes peuvent être sources d'indisponibilité du serveur DHCP.

Pour arrêter et démarrer les services de communication entre Integrated Enforcer et un serveur de gestion

1. Démarrez Symantec Integrated Enforcer.
2. Cliquez sur **Symantec NAC Integrated Enforcer**.
3. Effectuez l'une des tâches suivantes :
   - Dans la zone de groupe Enforcer service, cliquez sur **Stop**.
     L'option arrête le service Enforcer.
   - Dans la zone de groupe du Management server communication service, cliquez sur **Stop**.
     Cette option arrête le service Enforcer connecté à Symantec Endpoint Protection Manager.

Si l'état est défini sur Stopped, le service n'est pas exécuté.

4 Pour redémarrer le service, cliquez sur **Start**.

Si vous désactivez ou redémarrez l'ordinateur auquel Symantec Integrated Enforcer est connecté, le service Enforcer redémarre automatiquement au redémarrage de l'ordinateur.

Si le service de communication du serveur est arrêté, puis redémarré, Symantec Integrated Enforcer essaie de se connecter au dernier Symantec Endpoint Protection Manager auquel il était connecté. Si Symantec Endpoint Protection Manager est indisponible, Integrated Enforcer se connecte au premier serveur de gestion répertorié dans la liste de serveurs de gestion.

Déconnecter un module d'application Symantec NAC Lucent Integrated Enforcer d'un serveur de gestion sur une console Enforcer

Vous pouvez devoir déconnecter un module d'application Integrated Lucent Enforcer d'un serveur de gestion dans les circonstances suivantes :

- Dépanner un module d'application Integrated Lucent Enforcer.
- Dépanner un serveur de gestion.

Avertissement : Veillez à arrêter le service Enforcer avant d'essayer de déconnecter un module d'application Integrated Lucent Enforcer d'un serveur de gestion. Les clients ne pourront éventuellement plus se connecter au réseau à moins que vous ayez installé des serveurs de gestion de basculement.

Si vous voulez déconnecter un module d'application Integrated Lucent Enforcer d'un serveur de gestion, vous devez supprimer l'adresse IP, le nom d'hôte ou le nom de domaine de la liste du serveur de gestion indiquée.

Vous pouvez effectuer cette tâche sur une console Enforcer ou sur une console de serveur de gestion.

Pour déconnecter un module d'application Integrated Lucent Enforcer d'un serveur de gestion sur une console Enforcer

1 Dans la barre des tâches Windows de l'ordinateur Enforcer, cliquez sur **Démarrer > Programmes > Symantec Endpoint Protection > Symantec Integrated Lucent Enforcer**

2 Dans le volet gauche, développez Symantec Lucent Enforcer.

3 Développez Configure (Configurer).

4 Cliquez sur **Management Servers** (Serveurs de gestion).

5 Dans le volet Serveurs de gestion, sélectionnez le serveur de gestion que vous voulez déconnecter du module d'application Integrated Lucent Enforcer.

6 Dans la colonne d'icônes située à droite de la liste de serveurs de gestion, cliquez sur **Remove** (Supprimer) ou **Remove All** (Supprimer tout).

7 Cliquez sur **Save** (Enregistrer).

Se connecter aux serveurs Symantec Endpoint Protection Manager hérités

La page de configuration Integrated Enforcer Advanced Settings permet aux utilisateurs de contourner la quarantaine et de communiquer avec le serveur hérité 5.1.x Symantec Policy Manager.

Remarque : L'option de masque de sous-réseau sécurisé (255.255.255.255) est seulement disponible avec Lucent Integrated Enforcer.

Pour se connecter à un serveur Symantec Endpoint Protection Manager hérité

1 Cochez l'option **Use secure subnet mask (255.255.255.255) for quarantine IP address** (Utiliser le masque de sous-réseau sécurisé (255.255.255.255) pour l'adresse IP de quarantaine) ou décochez-la pour utiliser le sous-réseau par défaut 255.255.255.0

2 Cliquez sur **OK** pour enregistrer vos configurations.

Section 5

Installer et configurer Symantec NAC Integrated Enforcer pour Microsoft Network Access Protection

Chapitre 21

Présentation de Symantec NAC Integrated Enforcer pour Microsoft Network Access Protection

Ce chapitre traite des sujets suivants :

A propos du module d'application Integrated Enforcer pour Microsoft Network Access Protection

Integrated Enforcer pour Microsoft Network Access Protection (NAP) fonctionne en conjonction avec Microsoft Windows Network Policy Server (NPS) sur un serveur Microsoft Windows 2008. Symantec Integrated NAP Enforcer vérifie que les clients essayant de se connecter au réseau sont conformes aux politiques de sécurité configurées.

NAP restreint l'accès aux réseaux en créant un environnement contrôlé. Le module vérifie la politique de sécurité d'un client avant qu'il ne puisse se connecter au réseau d'entreprise. Si un client est non conforme, NAP corrige la politique de sécurité ou restreint l'accès des terminaux non conformes à la politique de sécurité d'une entreprise.

Network Access Protection est une technologie de création, d'application et de correction de politique d'état client incluse dans le système d'exploitation de Windows Server 2008. Les administrateurs système peuvent créer et appliquer

automatiquement des politiques d'état de sécurité. Ces politiques d'état de sécurité peuvent inclure les logiciels, mises à jour de sécurité, configurations de l'ordinateur et autres paramètres requis. Les ordinateurs client non conformes à une politique d'état de sécurité peuvent voir leur accès au réseau restreint jusqu'à ce que leur configuration soit mise à jour et respecte la politique. Selon le mode de déploiement de NAP choisi, les clients non conformes peuvent être automatiquement mis à jour de sorte que les utilisateurs retrouvent rapidement l'accès complet au réseau sans devoir mettre à jour ou reconfigurer manuellement leur ordinateur.

Si vous configurez un serveur Network Policy Server (NPS) en tant que serveur de politique Network Access Protection (NAP), le NPS évalue les rapports d'état (Statements of Health, SoH) envoyés par les ordinateurs client compatibles NAP tentant de se connecter au réseau. Vous pouvez configurer des politiques NAP sur NPS pour permettre à des ordinateurs client de mettre à jour leur configuration pour être conformes à la politique réseau de votre société.

NAP peut vous aider à résoudre ces problèmes de la façon suivante :

- En vérifiant la conformité avec les politiques de sécurité de terminal client
- En contrôlant l'accès des clients invités
- En authentifiant les utilisateurs finaux

Chapitre 22

Planifier l'installation de Symantec NAC Integrated Enforcer pour Microsoft Network Access Protection

Ce chapitre traite des sujets suivants :

A propos de la planification de l'installation de Symantec Integrated NAP Enforcer

Vous devez remplir un certain nombre de conditions requises avant qu'Integrated Enforcer pour Microsoft Network Access Protection (NAP) puisse devenir opérationnel. Les conditions requises s'appliquent au matériel et aux logiciels, ainsi qu'à d'autres composants logiciels, y compris des applications tierces.

Le type de boîtier Enforcer mis en œuvre dépend du type de produit Symantec Network Access Control dont vous avez fait l'acquisition.

Reportez-vous à votre accord de licence pour plus d'informations.

Composants requis pour Symantec Integrated NAP Enforcer

Le module d'application Symantec Integrated NAP Enforcer fonctionne avec Microsoft DHCP Server, Symantec Endpoint Protection Manager et le client Symantec Network Access Control avec Network Access Protection activée. Symantec Integrated NAP Enforcer vérifie que les clients sont conformes aux politiques de sécurité configurées avant qu'ils ne puissent se connecter à un réseau.

Les composants requis suivants doivent être installés avant de pouvoir utiliser Symantec Integrated NAP Enforcer :

Version 11.0.2 de Symantec Endpoint Protection Manager	Requise pour créer des politiques de sécurité dans un emplacement centralisé et les attribuer aux clients.
Windows 2008 server Le service DHCP Server ainsi que le service Network Policy Server (NPS) doivent également être installés sur le même ordinateur.	Installation requise de Microsoft Windows Server avec les services DHCP Server et Network Policy Server. Ces deux services doivent être installés et configurés pour que vous puissiez installer le module d'application Symantec Integrated NAP Enforcer.
Contrôleur de domaine	Installation requise du contrôleur de domaine sur l'ordinateur sur lequel est installé Symantec Endpoint Protection Manager ou sur un autre ordinateur qui prend en charge Microsoft Windows Server 2003.
Symantec Integrated NAP Enforcer	Requis pour authentifier des clients et appliquer des politiques de sécurité.
Client Symantec Network Access Control	Installation requise du client Symantec Network Access Control.

Configuration matérielle requise pour Symantec Integrated NAP Enforcer

La configuration matérielle requise du module d'application Symantec Integrated NAP Enforcer concerne la RAM, le processeur, l'espace de stockage, l'écran, l'adaptateur réseau et la carte d'interface réseau.

Pour les installations concernant jusqu'à 10 000 utilisateurs, utilisez la configuration recommandée suivante :

- Pentium III 750 MHz
- 256 Mo de mémoire
- 120 Mo d'espace disque
- Adaptateurs réseau Fast Ethernet
- Une carte d'interface réseau (NIC) dotée de TCP/IP

Pour des installations concernant 10 000 utilisateurs ou plus, utilisez la configuration recommandée suivante :

- Pentium 4 2.4 GHz
- 512 Mo de mémoire
- 512 Mo d'espace disque
- Adaptateurs réseau 1 Go
- Ecran de résolution 800 x 600, 256 couleurs (minimum)
- Une carte d'interface réseau (NIC) dotée de TCP/IP

Système d'exploitation requis pour Symantec Integrated NAP Enforcer

Symantec Integrated NAP Enforcer requiert l'installation du système d'exploitation et des services suivants :

- Windows 2008 server Standard Edition et Windows 2008 server Enterprise Edition
- Vous pouvez sélectionner l'une des configurations suivantes :
  - Service DHCP de Windows Server 2008 si vous prévoyez d'utiliser l'application DHCP
    Le service DHCP de Windows 2008 doit être situé sur le même ordinateur que Windows Server 2008 Network Policy Server.
  - Service DHCP de Windows si vous prévoyez d'utiliser l'application 802.1x
    Le service DHCP de Windows peut être situé sur le même ordinateur que Windows Server 2008 Network Policy Server. Vous pouvez également configurer le service DHCP sur un ordinateur distinct que vous avez configuré en tant que serveur DHCP de Windows 2008 ou serveur DHCP de Windows 2003.

- Service Windows Server 2008 Network Policy Server (NPS)

Système d'exploitation requis pour le client Symantec Network Access Control

Le client Symantec Network Access Control nécessite que l'un des systèmes d'exploitation suivants soit installé sur l'ordinateur client :

- Windows Vista (x86) Edition Familiale Basique, Edition Familiale Premium, Edition Professionnelle, Edition Entreprise, Edition Intégrale
- Windows Vista Edition Familiale Basique x64, Edition Familiale Premium x64, Edition Professionnelle x64 , Edition Entreprise x64, Edition Intégrale x64
- Windows Vista (x86) avec Service Pack 1 Edition Familiale Basique, Edition Familiale Premium, Edition Professionnelle, Edition Entreprise, Edition Intégrale
- Windows Vista avec Service Pack 1 Edition Familiale Basique x64, Edition Familiale Premium x64, Edition Professionnelle x64, Edition Entreprise x64, Edition Intégrale x64
- XP Professionnel avec Service Pack 3

Chapitre 23

Installer Symantec NAC Integrated Enforcer pour Microsoft Network Access Protection

Ce chapitre traite des sujets suivants :

Avant d'installer Symantec Integrated NAP Enforcer

Avant d'installer Symantec Integrated Enforcer, vous devez avoir terminé les tâches d'installation et de configuration suivantes :

- Installation de Symantec Endpoint Protection Manager

Remarque : Nous vous recommandons d'installer Symantec Endpoint Protection Manager avant d'installer Symantec Integrated NAP Enforcer. Symantec Endpoint Protection Manager doit être installé pour que le module Symantec Integrated NAP Enforcer fonctionne correctement.

Consultez le *Guide d'installation pour Symantec Enterprise Protection et Symantec Network Access Control* pour obtenir des instructions sur l'installation de Symantec Endpoint Protection Manager.

- Vérification des conditions matérielles et logicielles requises pour l'ordinateur sur lequel vous prévoyez d'installer les composants suivants :
  - Service de serveur DHCP
  - Service Network Access Protection Server
  - Contrôleur de domaine
  - Symantec Integrated NAP Enforcer

  Se reporter à "Composants requis pour Symantec Integrated NAP Enforcer" à la page 404.

Installation de Symantec Integrated NAP Enforcer

Vous devez installer le module d'application Symantec Integrated NAP Enforcer sur l'ordinateur sur lequel vous avez déjà installé le système d'exploitation Microsoft Windows Server. Le service DHCP Server et le service Network Access Protection Server devraient déjà être installés et configurés sur le même ordinateur. Vous devez vous connecter en tant qu'administrateur ou utilisateur du groupe d'administrateurs.

Remarque : Une fois que vous avez finalisé l'installation de Symantec Integrated NAP Enforcer, vous devez vous connecter à la console Symantec Endpoint Protection Manager.

Vous pouvez installer Symantec Integrated NAP Enforcer en utilisant l'Assistant d'installation.

Se reporter à "Pour installer Symantec Integrated NAP Enforcer avec l'Assistant d'installation" à la page 408.

Pour installer Symantec Integrated NAP Enforcer avec l'Assistant d'installation

1. Insérez le CD d'installation de Symantec Network Access Control dans le lecteur de CD-ROM pour lancer automatiquement l'installation.

   Si l'installation ne démarre pas, cliquez sur **IntegratedEnforcerInstaller.exe**.

   Vous devez quitter l'installation et installer le serveur NAP si ce n'est pas encore le cas.

   Si le service NAP Server est déjà installé, Welcome to Symantec Integrated NAP Enforcer Installation Wizard (Bienvenue dans l'assistant d'installation de Symantec Integrated Enforcer) s'affiche.

2. Dans l'écran Welcome (Bienvenue), cliquez sur **Next** (Suivant).

3 Dans le panneau License Agreement (Contrat de licence), cliquez sur **I accept the license agreement** (J'accepte le contrat de licence).

4 Cliquez sur **Next**.

5 Dans le panneau Destination Folder (Dossier de destination), effectuez l'une des tâches suivantes :

- Pour accepter le dossier de destination par défaut, cliquez sur **Next**. L'application est automatiquement installée dans le dossier C:\Program Files\Symantec\Integrated Enforcer\.
- Cliquez sur **Browse** (Parcourir) pour localiser et sélectionner un dossier de destination, cliquez sur **OK**, puis cliquez sur **Next**.

6 Si le volet Role Selection (Sélection du rôle) s'affiche, sélectionnez **NAP Enforcement** (Application NAP) et cliquez sur **Next** (Suivant).

Le volet Role Selection (Sélection du rôle) ne s'affiche que si plus d'un type de module d'application Symantec NAC Integrated Enforcer peut être installé en fonction des services s'exécutant sur le serveur.

7 Dans le panneau Ready to Install the Application (Prêt pour l'installation de l'application), cliquez sur **Next**.

Si vous devez modifier des paramètres précédents, cliquez sur **Back** (Retour).

8 Cliquez sur **Finish** (Terminer).

Si vous devez réinstaller Symantec Integrated NAP Enforcer, vous devez d'abord le désinstaller.

Se reporter à "Pour désinstaller le module d'application Symantec Integrated NAP Enforcer" à la page 409.

Se reporter à "Pour désinstaller le module d'application Symantec Integrated NAP Enforcer à partir de la ligne de commande" à la page 410.

9 Cliquez sur **Démarrer > Programmes > Symantec Enterprise Protection > Symantec Integrated Enforcer**.

Pour désinstaller le module d'application Symantec Integrated NAP Enforcer

1 Dans la barre des tâches Windows, cliquez sur **Démarrer > Panneau de configuration > Ajout/Suppression de programmes**.

2 Cliquez sur **Symantec Integrated Enforcer**, puis sur **Supprimer**.

3 Lorsque vous êtes invité à supprimer le logiciel, cliquez sur **Oui**.

4 Lorsque vous êtes invité à redémarrer le serveur NAP, effectuez l'une des tâches suivantes :

- Pour redémarrer le serveur NAP immédiatement, cliquez sur **Oui**.

- Pour redémarrer le service NAP manuellement plus tard (par défaut), cliquez sur **Non**.
  Si vous redémarrez le service NAP plus tard, vous devez l'arrêter, puis le démarrer.
  Vous devez redémarrer le serveur NAP pour désinstaller complètement Symantec Integrated Enforcer.

Pour désinstaller le module d'application Symantec Integrated NAP Enforcer à partir de la ligne de commande

1. Ouvrez une invite de commandes DOS.
2. A l'invite, tapez : **`MsiExec.exe /qn /X{A145EB45-0852-4E18-A9DC-9983A6AF2329}`**
3. Redémarrez le serveur NAP

Pour arrêter et démarrer manuellement le serveur NAP

1. Sur la barre des tâches Windows, cliquez sur **Démarrer > Panneau de configuration > Outils d'administration > Services**.
2. Cliquez sur **NAP Server** (Serveur NAP).
3. Cliquez avec le bouton droit puis sélectionnez **Stop**.
4. Cliquez sur **Start**.

Chapitre 24

Configurer Symantec NAC Integrated Enforcer pour Microsoft Network Access Protection sur une console Enforcer

Ce chapitre traite des sujets suivants :

A propos de la configuration d'un boîtier Symantec Integrated NAP Enforcer sur une console Enforcer

Après avoir terminé l'installation du boîtier Symantec Integrated NAP Enforcer, vous devez effectuer les tâches suivantes avant qu'il puisse devenir opérationnel :

- Spécifiez au moins un gestionnaire Symantec Endpoint Protection Manager auquel le boîtier Symantec Integrated NAP Enforcer peut se connecter.
  Cela inclut l'ajout du nom d'hôte ou de l'adresse IP du Symantec Endpoint Protection Manager au fichier appelé liste de serveurs de gestion. Le boîtier Symantec Network Access Control Integrated NAP Enforcer doit se connecter à une adresse IP ou un nom d'hôte de gestionnaire Symantec Endpoint Protection Manager. Autrement la configuration échoue.
  Se reporter à "Connecter un boîtier Symantec Integrated NAP Enforcer à un serveur de gestion sur une console Enforcer" à la page 412.
- Ajoutez un mot de passe chiffré ou un secret partagé configuré pendant l'installation de Symantec Endpoint Protection Manager.
  Le mot de passe chiffré était auparavant une clé partagée.
  Se reporter à "Chiffrer la communication entre un boîtier Symantec Integrated NAP Enforcer et un serveur de gestion" à la page 414.
- Définissez un nom de groupe Enforcer.
  Se reporter à "Configurer un nom de groupe d'Enforcer sur la console Symantec Integrated NAP Enforcer" à la page 415.
- Configurez un protocole de communication HTTP.
  Se reporter à "Configurer un protocole de communication HTTP sur la console Symantec Integrated NAP Enforcer" à la page 416.

Connecter un boîtier Symantec Integrated NAP Enforcer à un serveur de gestion sur une console Enforcer

Vous devez connecter Symantec Integrated Network Access Protection Enforcer à un serveur de gestion sur une console Network Access Protection Enforcer.

Pour connecter un boîtier Symantec Integrated NAP Enforcer à un serveur de gestion sur une console Enforcer

1. Dans la barre des tâches Windows de l'ordinateur Enforcer, cliquez sur **Démarrer > Programmes > Symantec Endpoint Protection > Symantec Integrated NAP Enforcer**.

   La console Symantec Integrated NAP Enforcer apparaît. La page principale affiche l'état de la connexion entre Symantec Integrated NAP Enforcer et le gestionnaire Symantec Endpoint Protection Manager. Une lumière verte indique que Symantec Integrated NAP Enforcer est activement connecté au serveur de gestion. Une lumière rouge indique que la connexion a échoué.

2. Dans le volet gauche, développez Symantec NAP Enforcer.
3. Dans le volet gauche, développez Configure (Configurer).
4. Dans le volet gauche, cliquez sur **Management Servers** (Serveurs de gestion).
5. Dans le volet Management Servers, cliquez sur **Add** (Ajouter) dans la colonne d'icône située à droite de la liste des serveurs de gestion.
6. Dans la boîte de dialogue Add/Edit Management Server (Ajouter/Modifier un serveur de gestion), tapez l'adresse IP ou le nom de Symantec Endpoint Protection Manager dans la zone de texte Server address (Adresse du serveur).

   Vous pouvez taper une adresse IP, un nom d'hôte ou un nom de domaine. Si vous voulez utiliser un nom de domaine, Symantec Integrated NAP Enforcer doit se connecter à un serveur DNS.

7. Dans la boîte de dialogue Add/Edit Management Server, modifiez le numéro de port que Symantec Integrated NAP Enforcer utilise pour communiquer avec Symantec Endpoint Protection Manager.

   Le numéro de port par défaut est 80 pour le protocole HTTP et 443 pour le protocole HTTPS. Vous pouvez uniquement utiliser le protocole HTTPS s'il est configuré de la même manière que sur Symantec Endpoint Protection Manager.

8. Cliquez sur **OK**.
9. Dans la boîte de dialogue Add/Edit management server, sélectionnez un autre serveur de gestion.

   Vous pouvez modifier l'ordre des serveurs de gestion que Symantec Integrated NAP Enforcer utilise pour se connecter à Symantec Endpoint Protection Manager.

10 Cliquez sur les flèches **Move up** (Vers le haut) ou **Move down** (Vers le bas) de la colonne d'icône située à droite de la liste de serveurs de gestion.

   Lorsqu'un boîtier Symantec Integrated NAP Enforcer se connecte à Symantec Endpoint Protection Manager pour la première fois, il tente de se connecter au premier serveur de gestion présenté dans la liste de serveurs de gestion. Si le serveur de gestion n'est pas disponible, le boîtier Symantec Integrated NAP Enforcer se connecte au serveur de gestion suivant dans la liste des serveurs de gestion.

11 Pour modifier un serveur de gestion, cliquez sur **Edit** (Modifier) dans la colonne d'icône et modifiez l'adresse du serveur de gestion ou les informations de port.

Pour supprimer Symantec Endpoint Protection Manager d'une liste de serveurs de gestion sur une console Symantec Integrated NAP Enforcer

1 Dans la barre des tâches Windows de l'ordinateur Enforcer, cliquez sur **Démarrer > Programmes > Symantec Endpoint Protection > Symantec Integrated NAP Enforcer**.

2 Dans le volet gauche, développez Symantec NAP Enforcer.

3 Développez Configure.

4 Cliquez sur **Management Servers**.

5 Pour supprimer un gestionnaire Symantec Endpoint Protection Manager, cliquez sur **Remove** (Supprimer) ou **Remove All** (Supprimer tout) dans la colonne d'icône.

Chiffrer la communication entre un boîtier Symantec Integrated NAP Enforcer et un serveur de gestion

Si vous voulez ajouter une couche de sécurité supplémentaire, vous pouvez protéger la communication entre le boîtier Symantec Integrated NAP Enforcer et le gestionnaire Symantec Endpoint Protection Manager grâce au chiffrement. La communication chiffrée requiert l'utilisation du protocole HTTPS au lieu du protocole HTTP. Vous devez également acheter un certificat tiers auprès d'un fournisseur.

Vous configurez généralement un mot de passe chiffré pendant la première installation de Symantec Endpoint Protection Manager. Le même mot de passe doit être configuré sur le module d'application Symantec Integrated NAP Enforcer. Si les mots de passe chiffrés ne correspondent pas, la communication entre Symantec Integrated NAP Enforcer et Symantec Endpoint Protection Manager échoue.

Pour chiffrer la communication entre un boîtier Symantec Integrated NAP Enforcer et un serveur de gestion

1. Dans la barre des tâches Windows de l'ordinateur Enforcer, cliquez sur **Démarrer > Programmes > Symantec Endpoint Protection > Symantec Integrated NAP Enforcer**.
2. Dans le volet gauche, développez Symantec NAP Enforcer.
3. Développez Configure (Configurer).
4. Cliquez sur **Management Servers** (Serveurs de gestion).
5. Saisissez le mot de passe chiffré dans la zone de texte Encrypted Password (Mot de passe chiffré) sur la console Symantec Integrated NAP Enforcer.

   Symantec Integrated NAP Enforcer doit utiliser le même mot de passe chiffré pour la communication avec Symantec Endpoint Protection Manager. Le mot de passe chiffré est toujours configuré pendant l'installation de Symantec Endpoint Protection Manager.
6. Activez l'option **Unmask** (Révéler).

   Les lettres et les chiffres du mot de passe chiffré apparaissent maintenant à la place des astérisques.
7. Cliquez sur **OK**.

Configurer un nom de groupe d'Enforcer sur la console Symantec Integrated NAP Enforcer

Vous devez ajouter un nom pour le groupe d'Enforcer. Dès lors que Symantec Integrated NAP Enforcer se connecte à Symantec Endpoint Protection Manager, il enregistre automatiquement le nom du groupe de boîtiers Enforcer sur le serveur de gestion.

Pour configurer un nom de groupe d'Enforcer sur la console Symantec Integrated NAP Enforcer

1. Dans la barre des tâches Windows de l'ordinateur Enforcer, cliquez sur **Démarrer > Programmes > Symantec Endpoint Protection > Symantec Integrated NAP Enforcer**.
2. Dans le volet gauche, développez Symantec NAP Enforcer.
3. Développez Configure (Configurer).
4. Cliquez sur **Management Servers** (Serveurs de gestion).

5 Dans le volet droit, tapez le nom du groupe de boîtiers Enforcer dans la zone de texte Preferred group (Groupe préféré) sur la console Symantec Integrated NAP Enforcer.

Si vous n'ajoutez pas de nom au groupe Integrated Enforcer sur la console Enforcer, tous les Integrated Enforcers appartiennent automatiquement au groupe Temporary (Temporaire) du serveur de gestion. Si vous ajoutez le nom du groupe Integrated Enforcer sur la console Enforcer, le nom du groupe Enforcer est automatiquement enregistré sur le serveur de gestion.

6 Cliquez sur **OK**.

Configurer un protocole de communication HTTP sur la console Symantec Integrated NAP Enforcer

Vous devez établir un protocole de communication entre Symantec Integrated NAP Enforcer et Symantec Endpoint Protection Manager. Autrement la communication échoue entre Symantec Integrated NAP Enforcer et Symantec Endpoint Protection Manager.

Vous pouvez configurer un protocole HTTP ou HTTPS. Si vous sélectionnez le protocole HTTPS, vous devez acheter un certificat d'un fournisseur tiers.

Pour configurer un protocole de communication HTTP sur la console Symantec Integrated NAP Enforcer

1 Dans la barre des tâches Windows de l'ordinateur Enforcer, cliquez sur **Démarrer > Programmes > Symantec Endpoint Protection > Symantec Integrated NAP Enforcer**.

2 Dans le volet gauche, développez Symantec NAP Enforcer.

3 Développez Configure (Configurer).

4 Cliquez sur **Management Servers** (Serveurs de gestion).

5 Dans le volet droit de la console Symantec Integrated NAP Enforcer, cliquez sur HTTP.

Si vous voulez configurer une communication chiffrée entre Symantec Integrated NAP Enforcer et la console Symantec Endpoint Protection Manager, vous devez utiliser le protocole HTTPS.

6 Si vous devez vérifier le certificat étant donné que vous utilisez le protocole HTTPS, cochez la case **Verify certificate when using HTTPS protocol** (Vérifier certificat lors de l'utilisation du protocole HTTPS).

7 Cliquez sur **OK**.

Chapitre 25

Configurer Symantec NAC Integrated Enforcer pour Microsoft Network Access Protection sur une console Symantec Endpoint Protection Manager

Ce chapitre traite des sujets suivants :

A propos de la configuration d'un boîtier Symantec Integrated NAP Enforcer sur la console Symantec Endpoint Protection Manager

Pour permettre la prise en charge du module d'application Symantec Integrated NAP Enforcer dans un environnement réseau, vous devez activer l'application NAP sur Symantec Endpoint Protection Manager. Sinon, le module d'application Enforcer ne fonctionnera pas correctement.

Vous devez également définir un ou plusieurs critères requis pour la politique Security Health Validator (Validation d'état de sécurité). Vous pouvez par exemple vérifier si la politique Security Health Validator du client est la dernière à avoir été installée sur un client. Si ce n'est pas le cas, alors le client est bloqué et la connexion au réseau est impossible.

Activer l'application NAP pour les clients

Vous devez activer l'application NAP pour Symantec Endpoint Protection et les clients Symantec Network Access Control. Si vous n'activez pas l'application Network Access Protection (NAP) pour les clients, le module d'application Symantec Integrated NAP Enforcer ne peut mettre en application aucune politique Security Health Validator.

Pour activer l'application NAP pour les clients

1. Dans la console Symantec Endpoint Protection Manager, cliquez sur **Clients**.
2. Dans la page Clients, sous View Groups (Afficher les groupes), sélectionnez le groupe pour lequel vous voulez activer l'application NAP.
3. Dans l'onglet Policies (Politiques), cliquez sur **General Settings** (Paramètres généraux).
4. Dans la boîte de dialogue Settings (Paramètres), cliquez sur **Security Settings** (Paramètres de sécurité).
5. Dans l'onglet des paramètres de sécurité, dans la zone Enforce Client (Client d'exécution), sélectionnez **Enable NAP Enforcement** (Activer l'application NAP).

   Ce paramètre est désactivé par défaut.
6. Cliquez sur **OK**.

Vérifier que le serveur de gestion gère le client

Vous pouvez définir un contrôle de vérification pour vous assurer que Symantec Endpoint Protection Manager gère le client Symantec Endpoint Protection ou le client Symantec Network Access Control.

Pour vérifier que le serveur de gestion gère le client

1. Dans la console Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administration).
2. Dans la page Admin, cliquez sur **Servers** (Serveurs).
3. Toujous dans la page Admin, sous View (Afficher), sélectionnez le groupe Enforcer pour lequel vous voulez vérifier que le serveur de gestion gère le client.
4. Cliquez avec le bouton droit de la souris sur le groupe Enforcer et sélectionnez Edit Properties (Modifier les propriétés).
5. Dans la boîte de dialogue I-DHCP Settings (Paramètres I-DHCP), dans la zone Client Information (Informations clients) de l'onglet NAP, sélectionnez **Verify that the management server manages the client** (Vérifier que le serveur de gestion gère le client).

   Ce paramètre est désactivé par défaut.
6. Dans la boîte de dialogue I-DHCP Settings (Paramètres I-DHCP), dans la zone Client Information (Informations clients) de l'onglet NAP Setting (Paramètres NAP), cliquez sur **OK**.

Vérifier les politiques Security Health Validator

Vous pouvez vérifier que les politiques Security Health Validator (Validation d'état de sécurité) sont installées sur les clients Symantec Endpoint Protection et Symantec Network Access Control.

Pour vérifier les politiques Security Health Validator

1. Dans la console Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administration).
2. Dans la page Admin, cliquez sur **Servers** (Serveurs).
3. Toujours dans cette page, sous View (Afficher), sélectionnez le groupe pour lequel vous voulez configurer les politiques Security Health Validator.
4. Cliquez avec le bouton droit de la souris sur le groupe Enforcer et sélectionnez Edit Properties (Modifier les propriétés).

5 Dans la boîte de dialogue I-DHCP Settings (Paramètres I-DHCP), dans la zone Client Information (Informations client) de l'onglet NAP Setting (Paramètre NAP), sélectionnez **Verify that the security Health Validator policy is current** (Vérifier que la politique Security Health Validator est actuelle).

   Ce paramètre est désactivé par défaut.

6 Cliquez sur **OK**.

Vérifier que les clients passent la vérification de l'intégrité de l'hôte

Vous pouvez définir un contrôle de conformité pour les clients de Symantec Endpoint Protection Manager.

Pour vérifier que les clients réussissent l'étape de vérification d'intégrité d'hôte

1 Dans la console Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administration).

2 Dans la page Admin, cliquez sur **Servers** (Serveurs).

3 Dans la page Admin, sous View (Afficher), sélectionnez le groupe Enforcer pour lequel vous voulez vous assurer que le client a passé la vérification de l'intégrité de l'hôte.

4 Cliquez avec le bouton droit sur le groupe Enforcer et sélectionnez **Edit Properties** (Modifier les propriétés).

5 Dans la boîte de dialogue I-DHCP (Paramètres I-DHCP), dans la zone Host Integrity Satus (Etat d'intégrité de l'hôte) de l'onglet NAP Setting (Paramètres NAP), sélectionnez **Verify that the client passes the Host Integrity check** (Vérifier que le client passe la vérification de l'intégrité de l'hôte).

   Ce paramètre est désactivé par défaut.

6 Cliquez sur **OK**.

Activer l'authentification locale sur le module d'application Symantec Integrated NAP Enforcer

L'authentification locale étant activée, si le module d'application Symantec Integrated NAP Enforcer perd sa connexion avec le client sur lequel Symantec Endpoint Protection Manager est installé, Symantec Integrated NAP Enforcer authentifie les clients localement. Dans ce cas, le module d'application Symantec

Integrated NAP Enforcer considère le client comme un utilisateur valide et ne vérifie que l'état d'intégrité d'hôte du client.

Remarque : Si le module d'application Symantec Integrated NAP Enforcer ne perd pas sa connexion au serveur Symantec Endpoint Protection Manager, il demande toujours à ce dernier de vérifier l'identificateur unique (UID) du client, que l'authentificaiton locale soit activée ou non.

Pour activer l'authentification locale sur le module d'application Symantec Integrated NAP Enforcer

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin, cliquez sur **Servers** (Serveurs).
3. Sous View Servers (Afficher les serveurs), sélectionnez et développez le groupe de modules d'application Symantec Integrated NAP Enforcer.
4. Sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés de groupe).
5. Dans la boîte de dialogue Settings (Paramètres), dans l'onglet Advanced (Avancé), sélectionnez **Enable Local Authentication** (Activer l'authentification locale).
6. Cliquez sur **OK**.

Configurer des journaux pour le module d'application Symantec Integrated NAP Enforcer

Les journaux pour le module d'application Symantec Integrated NAP Enforcer sont enregistrés sur l'ordinateur sur lequel vous avez installé le module d'application Symantec Integrated NAP Enforcer. Les journaux Enforcer sont générés par défaut.

Si vous voulez afficher des journaux Enforcer sur la console Symantec Endpoint Protection Manager, vous devez activer l'envoi de journaux sur la console Symantec Endpoint Protection Manager. Si cette option est activée, les données de journal sont envoyées depuis le module d'application Symantec Integrated NAP Enforcer vers Symantec Endpoint Protection Manager et enregistrées dans une base de données.

Vous pouvez modifier les paramètres de journal pour le module d'application Symantec Integrated NAP Enforcer sur la console Symantec Endpoint Protection

Manager. Les activités sont enregistrées dans le même journal Enforcer Server pour tous les modules d'application Enforcer sur un site.

Vous pouvez configurer des paramètres pour les journaux suivants générés par le module d'application Symantec Integrated NAP Enforcer :

- Journal Enforcer Server
- Journal Enforcer Client
  Le journal Client fournit des informations sur les interactions entre Integrated Enforcer et les clients qui ont essayé de se connecter au réseau. Il fournit des informations sur l'authentification, les échecs d'authentification et les déconnexions.

Section 6

Administration des modules d'application Enforcer depuis la console Symantec Endpoint Protection Manager

Chapitre 26

Gestion des modules d'application Enforcer depuis la console Symantec Endpoint Protection Manager

Ce chapitre traite des sujets suivants :

A propos de la gestion des modules Enforcer sur la console de serveur de gestion

Les paramètres de Symantec Enforcer sur la console du serveur de gestion vous aident à configurer Enforcer, ses interactions d'authentification et ses interactions d'application avec les clients. Avant de configurer les paramètres Enforcer sur la console, vous devez finaliser l'installation et paramétrer Enforcer sur le boîtier ou l'ordinateur.

Les paramètres de module d'application sur la console Symantec Endpoint Protection Manager dépendent du type de module Enforcer configuré : Boîtier Gateway, LAN ou DHCP. Par conséquent, les paramètres pour chacun sont couverts séparément.

Vous effectuez la majeure partie de la configuration et de l'administration d'Enforcer depuis la console. La plupart des paramètres de configuration d'Enforcer peuvent seulement être modifiés sur la console. Cependant, quelques paramètres d'Enforcer exigent de modifier un fichier d'Enforcer sur l'ordinateur d'Enforcer plutôt que sur la console. Presque tous les paramètres pour des modules d'application Enforcer sont configurés sur la page Serveurs de la console. Certains paramètres supplémentaires requis pour LAN Enforcer figurent sur la page Politiques.

Si vous administrez plusieurs modules d'application Enforcer et que vous êtes responsable d'autres tâches, il est généralement plus commode de les administrer depuis un emplacement centralisé. La console fournit cette possibilité. Vous pouvez ouvrir une session sur une console pour afficher des informations sur tous les modules d'application Enforcer.

Vous devez effectuer quelques tâches sur l'ordinateur sur lequel Enforcer est installé. Les tâches incluent l'utilisation de la console Enforcer locale plutôt que les tâches de maintenance de la console de gestion et du matériel. Par exemple, vous dépannez Enforcer et une connexion de console sur Enforcer lui-même. Pour définir le problème, vous pouvez devoir vérifier physiquement l'état du matériel d'Enforcer ou modifier sa connexion réseau.

Ce chapitre n'inclut pas d'informations sur la façon de configurer le client Symantec Enforcement, qui est un composant séparé d'Enforcer.

A propos de la gestion des modules d'application Enforcer depuis la page Serveurs

La page Servers (Serveurs) de la console de gestion présente tous les modules Enforcer qui sont installés, avec les consoles et serveurs connectés, dans le volet View Servers (Afficher les serveurs). Chaque Enforcer est listé sous un nom de groupe. Vous modifiez des propriétés d'Enforcer au niveau du groupe.

Se reporter à "Modifier le nom et la description d'un module d'application Enforcer" à la page 430.

Vous avez besoin des privilèges d'administrateur système pour afficher la page Serveurs.

A propos des groupes d'Enforcer

La configuration d'Enforcer sur la console est faite au niveau du groupe d'Enforcer plutôt qu'au niveau individuel d'Enforcer. Les modules d'application Enforcer sont listés sous un nom de groupe sur la page Serveurs de la console.

Les groupes d'Enforcer constituent une manière de synchroniser les paramètres d'Enforcer. Tous les modules d'application Enforcer d'un groupe partagent les mêmes paramètres (propriétés). Pour mettre à jour les propriétés d'Enforcer, vous devez sélectionner le nom de groupe dans le volet Afficher les serveurs et modifier les propriétés de groupe.

Comment la console détermine le nom de groupe d'Enforcer

Quand vous installez la connexion de console sur la console locale Enforcer, vous pouvez spécifier un nom de groupe. Enforcer s'enregistre auprès de la console après établissement de la connexion. La console attribue automatiquement Enforcer au groupe spécifié et liste Enforcer sous le nom de groupe dans le volet Afficher les serveurs de la console. Si vous ne spécifiez pas de nom pendant la configuration, la console attribue Enforcer à un groupe d'Enforcer par défaut. La console utilise le nom de l'ordinateur d'Enforcer comme nom de groupe.

A propos des groupes d'Enforcer de basculement

Un nouvel Enforcer s'identifie à la console comme Enforcer de basculement de réserve. Cette identification se produit si vous ajoutez un DHCP Enforcer de basculement ou un Gateway Enforcer qui se connecte par un hub ou un commutateur au même sous-réseau. La console attribue alors le nouveau Enforcer de basculement de réserve au même groupe que l'Enforcer actif. L'affectation se

produit que vous ayez ou non spécifié un nom de groupe pendant l'installation sur la console locale. Cette action garantit que le DHCP Enforcer ou Gateway Enforcer de basculement a exactement les mêmes paramètres que l'Enforcer principal.

Pour les modules d'application LAN Enforcer, le basculement est pris en charge par le commutateur plutôt que par Enforcer, donc l'affectation automatique au même groupe ne se produit pas. Vous pouvez vous assurer que les modules d'application LAN Enforcer multiples partagent des paramètres. Spécifiez le même nom de groupe dans la console locale Enforcer dans la boîte de dialogue Paramètres de la console.

A propos de la modification d'un nom de groupe

Vous ne pouvez pas modifier un nom de groupe d'Enforcer depuis la console. Cependant, vous pouvez spécifier un nouveau nom de groupe depuis la console locale Enforcer. Enforcer entre alors dans le nouveau groupe. Vous pouvez devoir actualiser l'écran de la console pour voir la modification.

A propos de la création d'un nouveau groupe d'Enforcer

Habituellement, vous devez seulement créer un nouveau groupe d'Enforcer si vous ajoutez un Enforcer qui requiert des paramètres différents des modules d'application Enforcer existants.

Vous pouvez créer un nouveau groupe d'Enforcer sur la console locale Enforcer en spécifiant le nouveau nom dans la boîte de dialogue Paramètres de la console. Le nouveau groupe a les paramètres par défaut d'Enforcer.

Vous pouvez laisser vide la zone de nom de groupe quand vous connectez le nouvel Enforcer depuis la console locale. Dans ce cas, la console attribue Enforcer à un nouveau groupe. Ce groupe prend le nom de l'ordinateur d'Enforcer et ses paramètres par défaut.

Vous pouvez utiliser la même méthode pour déplacer Enforcer vers un autre groupe. Spécifiez le nom de groupe désiré depuis la console locale Enforcer. Enforcer prend les paramètres du groupe vers lequel il est déplacé.

Informations Enforcer apparaissant sur la console Enforcer

Vous pouvez afficher des informations sur Enforcer dans la console.

Vous pouvez uniquement modifier les paramètres des cartes d'interface réseau sur le boîtier Enforcer et non sur la console. Si vous modifiez la configuration de

carte d'interface réseau sur le bôitier Enforcer, les nouveaux paramètres sont chargés sur la console de gestion lors du battement suivant.

Vous pouvez afficher des informations similaires sur Enforcer sur la console Enforcer.

Tableau 26-1 décrit le type d'informations que vous pouvez afficher.

Tableau 26-1 Informations au sujet du boîtier Enforcer sur la console Enforcer

Champ	Description
Nom	Identique au champ Hostname (Nom d'hôte).
Description	Brève description du module Enforcer. La description représente la seule information que vous pouvez modifier sur la console de gestion.
Version	Version du logiciel Enforcer exécuté sur l'ordinateur Enforcer sélectionné.
Nom d'hôte	Nom de l'ordinateur sur lequel Enforcer est installé.
Système d'exploitation	Système d'exploitation de l'ordinateur sur lequel le module Enforcer sélectionné est installé.
Etat en ligne	En ligne : Le service est exécuté, il est le module Enforcer actif principal. Hors ligne : Le service est interrompu.
Etat de basculement	(Gateway et DHCP Enforcer uniquement) Indique si le module Enforcer est actif ou en veille.
IP interne	Adresse IP de la carte d'interface de réseau interne.
IP externe	(Gateway et DHCP Enforcer uniquement) Adresse IP de la carte d'interface de réseau externe.
MAC interne	Adresse MAC de la carte d'interface réseau interne
MAC externe	(Gateway et DHCP Enforcer uniquement) Adresse MAC de la carte d'interface de réseau externe.
Carte d'interface réseau interne	Constructeur et modèle de la carte d'interface réseau interne.
Carte d'interface réseau externe	(Gateway et DHCP Enforcer uniquement) Fabricant et modèle de la carte d'interface de réseau externe.

Affichage des informations sur le module Enforcer sur la console de gestion

Vous pouvez afficher des informations sur Enforcer à partir d'une console.

Se reporter à Tableau 26-1 à la page 429.

Pour afficher des informations sur le module Enforcer sur la console de gestion

1. Dans la console Symantec Endpoint Protection Manager, dans la page Admin, cliquez sur **Servers** (Serveurs).
2. Sous View Servers (Afficher les serveurs), cliquez sur le nom du module Enforcer au sujet duquel vous voulez afficher des informations.

   Aucune information sur le boîtier LAN Enforcer n'apparaît dans les champs se rapportant à la carte d'interface réseau externe car le boîtier LAN Enforcer ne requiert qu'une carte d'interface réseau interne. Aucun état de basculement ne s'affiche car un commutateur gère le basculement LAN Enforcer.

Modifier le nom et la description d'un module d'application Enforcer

Le nom Enforcer est toujours le nom d'hôte du boîtier ou de l'ordinateur sur lequel il est installé. Vous pouvez seulement modifier le nom Enforcer en modifiant le nom d'hôte de l'ordinateur.

Vous pouvez modifier la description d'Enforcer depuis la console. Par exemple, vous pouvez vouloir entrer une description pour identifier l'emplacement d'Enforcer.

Pour modifier la description d'un module d'application Enforcer

1. Dans la console, sur la page Admin (Admin), cliquez sur **Servers** (Serveurs).
2. Sous View Servers (Afficher les serveurs), cliquez sur le nom d'Enforcer, puis sous Tasks (Tâches), cliquez sur **Edit Enforcer Properties** (Modifier les propriétés d'Enforcer). La boîte de dialogue de propriétés apparaît. La zone de nom n'est pas modifiable.
3. Entrez le texte désiré dans la zone de texte Description.
4. Cliquez sur **OK**.

   Vous pouvez également modifier la description d'Enforcer en cliquant avec le bouton droit de la souris sur le nom d'Enforcer et en sélectionnant Propriétés.

Suppression d'un Enforcer ou un groupe d'Enforcer

Vous pouvez supprimer un Enforcer de la console de gestion. Quand vous supprimez un Enforcer, il libère une licence parce que l'ordinateur utilisé n'exécute plus Enforcer. Vous ne pouvez pas supprimer Enforcer de la console quand Enforcer est en ligne. Vous pouvez désactiver Enforcer puis le supprimer. Quand vous redémarrez l'ordinateur d'Enforcer, Enforcer se reconnecte à la console. Enforcer s'enregistre de nouveau et réapparaît sur la page Serveurs. Pour supprimer Enforcer de manière permanente de la console, désinstallez d'abord Enforcer de l'ordinateur d'Enforcer.

Pour supprimer un groupe Enforcer après avoir désinstallé Enforcer de l'ordinateur Enforcer

1. Désactivez ou désinstallez Enforcer sur l'ordinateur d'Enforcer.
2. Dans la console, sur la page Admin (Admin), cliquez sur **Servers** (Serveurs).
3. Sous View Servers (Afficher les serveurs), cliquez sur le nom du module Enforcer, puis sous Tasks (Tâches), cliquez sur **Delete Enforcer** (Supprimer Enforcer). Une zone de texte de message vous demande de confirmer la suppression.
4. Pour confirmer la suppression, cliquez sur **Yes** (Oui).

   Si aucun Enforcer n'est listé dans un groupe et que vous ne voulez plus utiliser le groupe en question, vous pouvez supprimer ce dernier. Le groupe ne doit plus contenir de noms de modules Enforcer avant que vous ne le supprimiez. Lorsque vous supprimez un groupe Enforcer, vous supprimez tous ses paramètres personnalisés.

Pour supprimer un groupe d'Enforcer

1. Dans la console Symantec Endpoint Protection, cliquez sur **Admin**.

   Dans la page Admin, cliquez sur **Servers** (Serveurs).
2. Sous View Servers (Afficher les serveurs), cliquez sur le nom de groupe de module Enforcer.
3. Cliquez sur **Delete Group** (Supprimer groupe).

   Une zone de texte de message vous demande de confirmer la suppression.
4. Pour confirmer la suppression, cliquez sur **Yes** (Oui).

Exportation et importation des paramètres de groupe d'Enforcer

Vous pouvez vouloir exporter ou importer des paramètres pour un groupe d'Enforcer. Les paramètres sont exportés vers un fichier dans le format .xml. Quand vous importez des paramètres, vous devez les importer dans un groupe existant d'Enforcer, ce qui remplace les paramètres du groupe sélectionné.

Pour exporter des paramètres de groupe d'Enforcer

1. Dans la console de gestion, sur la page Admin, cliquez sur **Servers** (Serveurs).
2. Sous View Servers (Afficher les serveurs), cliquez sur le nom de groupe d'Enforcer, puis cliquez sur **Export Group Properties** (Exporter les propriétés de groupe).
3. Sélectionnez un emplacement dans lequel enregistrer le fichier et spécifiez un nom de fichier.
4. Cliquez sur **Save** (Enregistrer).

Quand vous importez des paramètres, vous devez les importer dans un groupe existant d'Enforcer, ce qui remplace les paramètres du groupe sélectionné.

Pour importer des paramètres de groupe d'Enforcer

1. Dans la console de gestion, sur la page Admin, cliquez sur **Servers** (Serveurs).
2. Sous View Servers (Afficher les serveurs), cliquez sur le nom de groupe d'Enforcer dont vous voulez remplacer les paramètres, puis cliquez sur **Import Group Properties** (Importer les propriétés de groupe).
3. Sélectionnez le fichier que vous souhaitez importer, puis cliquez sur **Open** (Ouvrir).

   Vous êtes invité à confirmer le remplacement des propriétés de groupe d'Enforcer actuelles.
4. Cliquez sur **Yes** (Yes).

Fenêtres contextuelles pour les clients bloqués

Quand Enforcer bloque un client qui essaye de se connecter au réseau, les deux types suivants de messages instantanés peuvent être configurés :

- Message pour les ordinateurs qui exécutent un client
- Message pour les ordinateurs Windows qui n'exécutent pas un client (Gateway Enforcer ou DHCP Enforcer seulement)

Messages pour les ordinateurs qui exécutent le client

Si Enforcer bloque des ordinateurs bien qu'ils exécutent un client, il peut y avoir plusieurs causes. Un blocage peut se produire à cause d'un échec de vérification d'intégrité d'hôte ou si la politique client n'est pas à jour. Quand ces événements se produisent, vous pouvez spécifier qu'un message instantané s'affiche sur le client. Ce message informe l'utilisateur qu'Enforcer a bloqué tout le trafic du client et pourquoi il l'a bloqué. Par exemple, le message suivant s'affiche si le client a échoué lors de la vérification d'intégrité d'hôte :

```
Symantec Enforcer a bloqué tout le trafic du client parce que
la vérification de l'intégrité de l'hôte a échoué pour le client.
```

Vous pouvez ajouter un texte au message par défaut. Par exemple, vous pouvez vouloir dire à l'utilisateur de l'ordinateur quoi faire pour remédier à la situation. Vous configurez ce message en tant que paramètre de politique de groupe de clients plutôt que comme paramètre d'Enforcer.

Messages pour les ordinateurs Windows qui n'exécutent pas le client (Gateway Enforcer ou DHCP Enforcer seulement)

Dans certains cas, les clients essayent de se connecter au réseau d'entreprise sans exécuter le client. Les modules d'application Gateway Enforcer et DHCP Enforcer fournissent un message instantané pour informer les utilisateurs d'ordinateurs Windows de la nécessité d'installer le logiciel client. Le message indique aux clients qu'ils ne peuvent accéder au réseau parce que le client Symantec ne s'exécute pas. Vous pouvez configurer le contenu du message dans l'onglet Authentification de la boîte de dialogue Paramètres d'Enforcer. Utilisez l'option Activer le message instantané sur le client si le client ne s'exécute pas.

Remarque : Pour Gateway Enforcer seulement, une alternative au message instantané est l'option Rediriger HTTP. L'option Rediriger HTTP connecte le client à un site Web avec des instructions ou des fonctions de résolution.

Pour qu'Enforcer affiche un message sur le client, les ports UDP 137 et 138 doivent être ouverts pour transmettre le message.

Windows Messaging (également appelé Messenger) doit s'exécuter sur les systèmes Windows NT (Windows NT 4.0, 2000, XP et Windows Server 2003) pour que l'ordinateur affiche les messages instantanés. Si le client s'exécute, Windows Messaging n'est pas requis pour afficher un message instantané du client.

Configuration des messages d'Enforcer

Vous pouvez configurer les messages d'Enforcer qui apparaissent sur les clients quand Enforcer bloque les clients.

Remarque : Vous ne pouvez modifier les paramètres que pour les groupes qui n'héritent pas des paramètres d'un groupe parent.

Pour configurer des messages d'Enforcer

1. Dans la console, dans la page Clients (Clients), sélectionnez l'onglet Policies (Politiques).
2. Sous View Policies (Afficher les politiques), sélectionnez le groupe pour lequel vous voulez spécifier un message contextuel.
3. Sous Settings (Paramètres), sélectionnez **General Settings** (Paramètres généraux). La boîte de dialogue Group Settings (Paramètres de groupe) apparaît avec l'onglet General Settings (Paramètres généraux) sélectionné.
4. Dans l'onglet Security Settings (Paramètres de sécurité), sélectionnez **Display a message when a client is blocked by a Symantec Enforcer** (Afficher un message lorsqu'un client est bloqué par Symantec Enforcer).
5. Si vous voulez ajouter du texte au message par défaut, cliquez sur **Set Additional Text** (Définir un texte supplémentaire), puis tapez le texte et cliquez sur **OK**.
6. Cliquez sur **OK**.

A propos des paramètres de client et d'Enforcer

Les clients Symantec fonctionnent avec Enforcer sans configuration particulière. L'exception porte sur quelques paramètres d'authentification 802.1x requis pour LAN Enforcer. En outre, il existe une situation que vous devez connaître quand vous configurez des clients. Si un utilisateur final arrête le client pendant qu'il s'exécute, un problème peut se poser.

Configuration des clients pour utiliser un mot de passe afin d'arrêter le service client

Le client peut passer l'authentification d'Enforcer au commencement, alors que le client s'exécute, et recevoir une configuration réseau et une adresse IP normales. Si l'authentification du client échoue ultérieurement, Enforcer envoie un message

au client. Du fait de cet échec, le client doit effectuer une publication et renouveler l'adresse IP. Cependant, si l'utilisateur final arrête le client sur l'ordinateur client, Enforcer ne peut pas imposer la publication et la renouveler. Pour s'assurer qu'Enforcer peut continuer à mettre en quarantaine ou à bloquer des clients, vous pouvez restreindre les utilisateurs autorisés à arrêter un client. Vous pouvez restreindre des utilisateurs en demandant un mot de passe pour que l'utilisateur final arrête le client.

Pour configurer des clients pour utiliser un mot de passe afin d'arrêter le service client

1. Dans la console, sur la page Clients, sélectionnez le groupe de clients.
2. Dans l'onglet Policies (Politiques), sous Settings (Paramètres), cliquez sur **General Settings** (Paramètres généraux).
3. Dans l'onglet Security Settings (Paramètres de sécurité), sous Client Password Protection (Protection du client par mot de passe), sélectionnez **Require a password to stop the client service** (Exiger un mot de passe pour arrêter le service client) et spécifiez le mot de passe.
4. Cliquez sur **OK**.

Section 7

Utilisation des rapports et des journaux du module d'application Enforcer

Chapitre 27

Gestion des rapports et des journaux du module Enforcer

Ce chapitre traite des sujets suivants :

Rapports Enforcer

La page Reports (Rapports) de la console Symantec Endpoint Protection Manager fournit les rapports prédéfinis et les rapports personnalisés. Vous pouvez afficher les rapports rapides prédéfinis contenant des informations sur les modules d'application Enforcer à la page Rapports.

Les rapports suivants d'Enforcer sont disponibles :

- Le rapport System (Système) intitulé Top Enforcers That Generate Errors (Enforcer générant des erreurs) contient des informations sur les modules Enforcer générant des erreurs et des avertissements.
- Le rapport System (Système) intitulé Site Status (Etat du site) contient des informations sur le système Enforcer, le trafic et le débit de journal des paquets.
- Le rapport Compliance (Conformité) contient des informations sur l'état de conformité des clients.

Consultez le *Guide d'administration pour Symantec Endpoint Protection Manager et Symantec Network Access Control* pour plus d'informations au sujet des rapports Enforcer.

Se reporter à "A propos des journaux Enforcer" à la page 440.

A propos des journaux Enforcer

Les modules d'application Enforcer fournissent les journaux suivants, que vous pouvez utiliser pour contrôler et dépanner l'activité du système :

- Journal de serveur Enforcer
  Se reporter à "A propos du journal de serveur Enforcer" à la page 440.
- Journal de client Enforcer
  Se reporter à "A propos du journal de client Enforcer" à la page 441.
- Journal de trafic Enforcer (Gateway Enforcer uniquement)
  Se reporter à "A propos du journal du trafic de Gateway Enforcer" à la page 442.

Par défaut, les journaux Enforcer sont stockés sur l'ordinateur d'installation du logiciel ou sur le boîtier Enforcer lui-même. Vous pouvez décider que les journaux soient automatiquement envoyés depuis le boîtier Enforcer ou l'ordinateur sur lesquels vous avez installé Integrated Enforcer vers la console Symantec Endpoint Protection Manager. Cependant, vous devez activer l'option d'envoi des journaux sur la console Symantec Endpoint Protection Manager.

Les données journal sont envoyées depuis Enforcer vers la console Symantec Endpoint Protection Manager, puis stockées dans la base de données. Vous pouvez modifier les paramètres de journal Enforcer, afficher des journaux et générer des rapports sur Enforcer depuis la console Symantec Endpoint Protection Manager. Les activités sont enregistrées dans le même journal de serveur Enforcer pour tous les modules d'application Enforcer sur un site.

Remarque : Un journal système intitulé Enforcer Activity (Activité Enforcer) est également disponible sur la console Symantec Endpoint Protection Manager. Il contient des informations sur des événements tels que le moment où les modules d'application Enforcer démarrent et celui où ils se connectent à Symantec Endpoint Protection Manager.

A propos du journal de serveur Enforcer

Le journal de serveur Enforcer fournit les informations liées au fonctionnement d'un module Enforcer.

Tableau 27-1 décrit les informations disponibles dans le journal Enforcer Server (Serveur Enforcer).

Tableau 27-1 Informations de journal de serveur Enforcer

Nom de colonne du journal	Description
Heure	Date et heure de l'événement consigné. Vous devriez garder l'heure du journal de serveur Enforcer synchronisée avec l'heure de système Linux sur le boîtier Enforcer. Vous pouvez modifier manuellement l'heure du boîtier Enforcer pour respecter l'heure d'été.
Type d'événement	Type d'événement. Par exemple, Enforcer registered (Enforcer enregistré) ou Server received Enforcer log (Le serveur a reçu le journal du module Enforcer) sont des types d'événements.
Enforcer Name (Nom Enforcer)	Nom du module Enforcer que cet événement implique.
Site	Nom du site que cet événement implique.
Server (Serveur)	Nom du serveur que cet événement implique.

A propos du journal de client Enforcer

Un journal de client Enforcer fournit des informations au sujet des interactions entre un module Enforcer et un client qui a essayé de se connecter au réseau. Il affiche des informations sur l'authentification, les échecs d'authentification et les déconnexions.

Dans un scénario d'authentification point à point, le journal de client Enforcer affiche également des informations sur l'authentification, les échecs d'authentification et les déconnexions. Les informations concernent les interactions entre les clients qui agissent en tant que modules Enforcer et clients distants. Les clients distants essayent de se connecter au réseau en passant par les clients agissant en tant que modules Enforcer.

Le Tableau 27-2 décrit les informations disponibles dans le journal de client Enforcer.

Tableau 27-2 Informations de journal de client Enforcer

Nom de colonne du journal	Description
Time (Heure)	Date et heure auxquelles s'est produite l'interaction avec le client.
Enforcer Name (Nom Enforcer)	Nom d'hôte du boîtier Enforcer que cet événement implique.
Enforcer Type (Type Enforcer)	Type d'Enforcer que cet événement implique, boîtier Gateway Enforcer, boîtier DHCP Enforcer ou boîtier LAN Enforcer.
Site	Nom du site que cet événement implique.
Remote Host (Hôte distant)	Le nom d'hôte du client que cet événement fait participer (le cas échéant).
Action	Action effectuée par le module Enforcer. Cette colonne peut contenir les actions suivantes : ■ Authenticated (Authentifié) L'identificateur unique du client (UID) était correct. ■ Rejected (Rejeté) L'UID du client était incorrect ou aucun client n'était en cours d'exécution. ■ Disconnected (Déconnecté) Le client s'est déconnecté de l'Enforcer ou le service Enforcer a été interrompu. ■ Passed (Réussi) Le client a réussi la vérification de l'intégrité de l'hôte. ■ Failed (Echec) La vérification de l'intégrité de l'hôte a échoué pour le client.
Remote MAC (MAC distant)	Adresse MAC du client.

A propos du journal du trafic de Gateway Enforcer

Le journal du trafic enregistre tout le trafic qui entre par l'adaptateur externe d'un boîtier Gateway Enforcer et sort par l'adaptateur interne.

Remarque : Les journaux du trafic sont disponibles sur les boîtiers Gateway Enforcer uniquement. Le contenu dépend du filtre de journal de trafic qui est défini dans la boîte de dialogue Paramètres de Gateway Enforcer.

Le Tableau 27-3 décrit les informations disponibles dans le journal du trafic de Gateway Enforcer.

Tableau 27-3 Informations de journal de trafic du boîtier Gateway Enforcer

Nom de colonne du journal	Description
Time (Heure)	Date et heure de l'événement de trafic.
Enforcer Name (Nom Enforcer)	Nom du boîtier Gateway Enforcer que cet événement implique.
Enforcer Type (Type Enforcer)	Nom du type Enforcer que cet événement implique, Gateway Enforcer, DHCP Enforcer ou LAN Enforcer.
Site	Nom du site que cet événement implique.
Port local	Le port TCP ou le port UDP de la destination de paquet.
IP d'hôte local	Adresse IP de la source de paquet.
IP de l'hôte distant	Adresse IP de la destination de paquet.
Direction	Direction du trafic : entrant, qui entre dans le boîtier Gateway Enforcer ou sortant, qui quitte le boîtier Gateway Enforcer.
Action	Opération effectuée. Par exemple, authentification ou blocage.
Nombre	Nombre de fois où le même paquet a été reçu.

Configurer les paramètres du journal Enforcer

Vous pouvez configurer les paramètres pour les journaux Enforcer dans la boîte de dialogue Settings *nom d'Enforcer* (Paramètres de "nom d'Enforcer") dans l'onglet Logging (Consignation). Les modifications sont envoyées au module d'application Enforcer sélectionné lors du battement suivant.

Désactiver la consignation des évènements Enforcer sur la console Symantec Endpoint Protection Manager

Par défaut, la consignation Enforcer est activée. Vous pouvez la désactiver sur la console Symantec Endpoint Protection Manager. Si vous désactivez la consignation, vous pourrez l'activer du même emplacement.

Pour désactiver la consignation Enforcer sur la console Symantec Endpoint Protection Manager

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin, cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez le groupe Enforcer dont vous voulez désactiver la consignation.
4. Dans la page Admin, sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans la boîte de dialogue *nom_Enforcer* Settings (Paramètres nom_Enforcer), dans l'onglet Logging (Consignation), décochez la case **Enable logging** (Activer la consignation) pour chaque journal que vous souhaitez désactiver.
6. Cliquez sur **OK**.

Activation de l'envoi des journaux d'un boîtier Enforcer à Symantec Endpoint Protection Manager

Par défaut, tous les journaux sont automatiquement envoyés du boîtier Enforcer ou de l'ordinateur sur lequel vous avez installé Integrated Enforcer basé sur logiciel vers Symantec Endpoint Protection Manager. Dès que vous activez l'envoi de journaux, vous pouvez afficher tous les journaux Symantec dans un emplacement central sur la console Symantec Endpoint Protection Manager.

Pour activer l'envoi des journaux Enforcer depuis un module d'application Enforcer vers Symantec Endpoint Protection Manager

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin, cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Administration), sous View Servers (Afficher les serveurs), sélectionnez le groupe Enforcer pour lequel vous voulez activer l'envoi des journaux Enforcer depuis un module d'application Enforcer vers Symantec Endpoint Protection Manager.
4. Dans la page Admin, sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).

5 Dans la boîte de dialogue *nom_Enforcer* (Paramètres nom_Enforcer), dans l'onglet Logging (Consignation), cochez la case **Send the log to the management server** (Envoyer le journal au serveur de gestion).

Vous pouvez activer l'envoi de chaque type de journal d'un boîtier Enforcer ou de l'ordinateur sur lequel vous avez installé Integrated Enforcer basé sur logiciel vers Symantec Endpoint Protection Manager.

6 Cliquez sur **OK**.

Paramétrage de la taille et de l'âge des journaux Enforcer

Vous pouvez spécifier la taille maximale des fichiers journaux Enforcer et le nombre de jours pendant lesquels les entrées du journal sont stockées.

Pour paramétrer la taille et l'âge des journaux Enforcer

1 Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).

2 Dans la page Admin, cliquez sur **Servers** (Serveurs).

3 Dans la page Admin (Admin), sous View Servers (Afficher les serveurs), sélectionnez le groupe Enforcer dont vous voulez paramétrer la taille et l'âge des journaux Enforcer.

4 Dans la page Admin, sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).

5 Dans la boîte de dialogue *nom_Enforcer* Settings (Paramètres nom_Enforcer), dans l'onglet Logging (Consignation), spécifiez le nombre de kilo-octets maximal de données à maintenir pour chaque journal dans chaque champ de taille de fichier journal Maximum.

Le paramètre par défaut est 512 Ko.

6 Dans le champ Log entry will expire after (L'entrée du journal expire après), indiquez le nombre de jours pendant lesquels l'entrée reste dans la base de données avant d'être supprimée.

La plage est de 1 jour à 365 jours, avec une plage par défaut de 30 jours.

7 Cliquez sur **OK**.

Filtrage des journaux de trafic pour un boîtier Enforcer

Si vous avez plusieurs clients se connectant via un boîtier Enforcer, vous pouvez obtenir un journal de trafic de taille importante. Vous pouvez filtrer le type de données qu'un boîtier Enforcer consigne dans un journal de trafic dans le but de

réduire la taille du fichier journal. La liste de filtre vous permet de filtrer le trafic qu'un boîtier Enforcer consigne avant de conserver les données.

Pour filtrer les journaux de trafic pour un boîtier Enforcer

1. Dans la console de Symantec Endpoint Protection Manager, cliquez sur **Admin** (Administrateur).
2. Dans la page Admin, cliquez sur **Servers** (Serveurs).
3. Dans la page Admin (Administration), sous View Servers (Afficher les serveurs), sélectionnez le groupe Enforcer pour lequel vous voulez filtrer les journaux de trafic.
4. Dans la page Admin, sous Tasks (Tâches), cliquez sur **Edit Group Properties** (Modifier les propriétés du groupe).
5. Dans la boîte de dialogue *nom_Enforcer* Settings (Paramètres nom_Enforcer), dans l'onglet Logging (Consignation), dans la liste de filtre de journal Traffic (Trafic), sélectionnez l'une des options de filtre suivantes :

All traffic (Tout le trafic)	Consigne l'intégralité du trafic, y compris ce qui est autorisé et laissé
Only blocked traffic (Uniquement le trafic bloqué)	Consigne uniquement les clients bloqués par Enforcer
Only allowed traffic (Uniquement le trafic autorisé)	Consigne uniquement les clients autorisés par Enforcer

6. Cliquez sur **OK**.

Index

Symboles

A

B

C

D

E

F

G

H

I

J

L

Q

R

S

T

U

V