

Sophos NAC DHCP Guide de configuration

Version du produit : 3.9

Date du document : décembre 2011



Table des matières

1 À propos de ce guide.....	3
2 Aperçu de la mise en application de DHCP.....	4
3 Installation de la mise en application de DHCP.....	5
4 Mise à niveau de la mise en application de DHCP.....	18
5 Annexe : utilisation de l'utilitaire de configuration de DHCP Enforcer.....	24
6 Support technique.....	27
7 Mentions légales.....	28

1 À propos de ce guide

Ce guide vous aide à configurer la mise en application de DHCP afin que vous puissiez identifier les ordinateurs d'extrémité inconnus se connectant à votre réseau, évaluer leurs niveaux de sécurité et contrôler leur accès au réseau. Il décrit comment configurer NAC DHCP Enforcer et le serveur NAC. Ce document contient également des informations à propos de votre logiciel de mise en application de DHCP.

Il contient, en particulier, des informations sur :

- L'installation et la configuration du logiciel DHCP Enforcer pour la première fois.
- La configuration de DHCP à l'aide du NAC Manager.
- La mise à niveau de la mise en application de DHCP.

Ce guide s'adresse à vous si :

- Vous utilisez la Sophos Enterprise Console.
- Vous utilisez la version de Sophos NAC intégrée à l'Enterprise Console.
- Vous souhaitez installer et configurer la mise en application de DHCP ou mettre à niveau la mise en application de DHCP.

Consultez le *Guide de démarrage rapide de Sophos Enterprise Console* avant de lire ce guide.

La documentation Sophos est disponible sur <http://www.sophos.fr/support/docs/>.

1.1 Configuration requise pour le logiciel DHCP Enforcer

Pour utiliser la mise en application de DHCP avec Sophos NAC, vous devez installer le logiciel Sophos DHCP Enforcer sur votre serveur DHCP.

Configuration requise pour le logiciel DHCP Enforcer	
Système d'exploitation	<p>Les versions suivantes de Windows Server sont prises en charge :</p> <ul style="list-style-type: none"> ■ Windows Server 2003 standard et supérieur (32 bits) ■ Windows Server 2003 SP2 et supérieur (64 bits) ■ Windows Server 2003 R2 standard et supérieur (32 bits et 64 bits) ■ Windows Server 2008 standard et supérieur (32 et 64 bits) ■ Windows Server 2008 R2 standard et supérieur (32 et 64 bits) <p>Remarque : les éditions Web et Core de Windows Server 2008 ne sont pas prises en charge.</p>
Logiciel DHCP	Logiciel Dynamic Host Configuration Protocol (DHCP) de Microsoft®

2 Aperçu de la mise en application de DHCP

Sophos NAC contient les paramètres par défaut de la mise en application de DHCP. Ces paramètres par défaut concernent la mise en place la plus usuelle de DHCP afin qu'une configuration minimale soit requise dès que Sophos NAC est installé. Toutefois, les mises en place du protocole DHCP sont très variables, aussi, il se peut qu'une configuration supplémentaire soit nécessaire.

Remarque : la liste de contrôle de la mise en application de DHCP fournit une liste des tâches requises pour implémenter la mise en application de DHCP. Déterminez les instructions dont vous avez besoin :

- Si vous utilisez la mise en application de DHCP pour la première fois, reportez-vous à la section [Liste de contrôle de l'installation de la mise en application de DHCP](#) à la page 5.
- Si vous installez la mise en application de DHCP pour la première fois dans la version 3.3 ou 3.7 de Sophos NAC et que vous procédez à la mise à niveau à la version 3.9, reportez-vous à la section [Liste de contrôle de la mise à niveau de la mise en application de DHCP](#) à la page 18.

Paramètres par défaut prédéfinis de la mise en application de DHCP

Si nécessaire, utilisez le NAC Manager pour modifier les paramètres par défaut.

- Les ordinateurs d'extrémité inconnus sont autorisés à accéder au réseau. Les ordinateurs d'extrémité inconnus ne sont pas administrés par la Sophos Enterprise Console, ne disposent pas de l'agent de conformité, ne sont pas exemptés et n'ont pas exécuté l'agent temporaire. Par défaut, les serveurs DHCP sont paramétrés sur Report Only. Pour activer la mise en application de DHCP et mettre en quarantaine les ordinateurs d'extrémité inconnus, changez le mode Unknown Endpoint sur Enforce.

Remarque : lorsque la mise en application de DHCP est activée, les ordinateurs d'extrémité inconnus sont interdits d'accès aux adresses IP privées et au réseau local (LAN).

- Les ordinateurs d'extrémité connus sont autorisés à accéder au réseau. Les ordinateurs d'extrémité connus sont administrés par la Sophos Enterprise Console, disposent de l'agent de conformité et l'exécutent. Les stratégies NAC sont paramétrées sur Report Only. Pour activer la mise en application de DHCP pour les ordinateurs d'extrémité connus, modifiez le mode de la stratégie sur Enforce pour chaque stratégie que vous souhaitez utiliser.

Remarque : lorsque la mise en application de DHCP est activée, les ordinateurs d'extrémité conformes et partiellement conformes exécutant l'agent sont autorisés à accéder au réseau. Les ordinateurs d'extrémité non conformes exécutant l'agent sont interdits d'accès au réseau.

Nous vous conseillons d'utiliser la mise en application de DHCP pour les ordinateurs d'extrémité inconnus et la mise en application de l'agent pour les ordinateurs d'extrémité connus. Toutefois, Sophos NAC ne vous permet pas d'utiliser la mise en application de DHCP pour les ordinateurs d'extrémité connus. Pour plus d'informations sur la mise en application de l'agent, reportez-vous au Guide de configuration de Sophos Compliance Agent.

3 Installation de la mise en application de DHCP

Vous pouvez installer la mise en application de DHCP de Sophos NAC pour la première fois en suivant les étapes de cette section.

3.1 Liste de contrôle de l'installation de la mise en application de DHCP

La liste de contrôle de l'installation de la mise en application de DHCP fournit une liste des tâches requises pour implémenter la mise en application de DHCP. Sauf mention contraire, toutes les tâches sont effectuées conformément aux instructions du présent document.

Tâche	Description	Terminée
Installation de Sophos NAC et de l'agent de conformité		
1.	Installez et configurez Sophos NAC. Pour plus d'informations, reportez-vous au <i>Guide de démarrage rapide de Sophos Endpoint Security and Control</i> .	
2.	Installez l'agent de conformité sur les ordinateurs d'extrémité à l'aide de la Sophos Enterprise Console. Pour plus d'informations, reportez-vous au <i>Guide de démarrage rapide de Sophos Endpoint Security and Control</i> .	
Tâches du serveur DHCP		
3.	Installez le logiciel DHCP Enforcer sur chaque serveur DHCP.	
Tâches du NAC Manager de Sophos		
4.	Exécutez l'assistant de configuration de DHCP pour configurer les serveurs proxy, d'actualisation, de l'agent temporaire et DHCP à utiliser avec la mise en place de DHCP de Sophos NAC.	
5.	Exécutez le rapport DHCP Enforcer pour : <ul style="list-style-type: none"> ■ Déterminer si les ordinateurs d'extrémité connus vont recevoir l'accès réseau approprié lorsque la mise en application de DHCP sera activée. ■ Rechercher les ordinateurs d'extrémité nécessitant une exemption. 	
6.	Créez des exemptions pour les ordinateurs d'extrémité qui ne sont pas en mesure d'exécuter l'agent de conformité, tels que les ordinateurs d'extrémité avec systèmes d'exploitation non Windows. Les exemptions s'appliquent également aux ordinateurs d'extrémité ne nécessitant pas la vérification de leur conformité, tels que les serveurs, les routeurs et les imprimantes.	
7.	Activez la mise en application de DHCP.	

3.2 Installation du logiciel DHCP Enforcer

Installez le logiciel DHCP Enforcer sur chaque serveur Microsoft DHCP. Le logiciel DHCP Enforcer inclut DHCP Enforcer et l'utilitaire de configuration DHCP Enforcer Configuration Utility. Le serveur DHCP est configuré lors de l'installation. Si vous devez modifier les paramètres du serveur DHCP qui ont été définis lors de l'installation de DHCP Enforcer, utilisez l'utilitaire de configuration DHCP Enforcer Configuration Utility. Pour plus d'informations, reportez-vous à la section [Annexe : utilisation de l'utilitaire de configuration de DHCP Enforcer](#) à la page 24.

1. Rendez-vous sur <http://www.sophos.fr/support/updates/>.
2. Saisissez votre nom utilisateur et mot de passe MySophos.
3. Sur la page Web des téléchargements **Enterprise**, téléchargez le programme d'installation de NAC DHCP Enforcer.
4. Exécutez le programme d'installation.

L'assistant d'installation vous guide tout au long de l'installation. Acceptez les options par défaut.

Conservez un enregistrement de la clé partagée que vous entrez sur la page **Sophos DHCP Enforcer**. La clé partagée sert à sécuriser le trafic entre le serveur NAC et le serveur DHCP. La même clé partagée doit être saisie lorsque vous lancez l'assistant DHCP Configuration Wizard à l'aide du NAC Manager.

Remarque : suite à l'installation du logiciel DHCP Enforcer, vérifiez que le service DHCP fonctionne sur chaque serveur DHCP.

3.3 Exécution de tâches NAC Manager

Dès que vous avez installé DHCP Enforcer sur chaque serveur DHCP, utilisez le NAC Manager pour configurer vos serveurs DHCP afin qu'ils fonctionnent avec Sophos NAC. La mise en application de DHCP nécessite une configuration minimale à l'aide du NAC Manager. La mise en application de DHCP est paramétrée par défaut sur Report Only. Vous devez activer la mise en application.

- Les **ordinateurs d'extrémité inconnus** ne sont pas administrés par la Sophos Enterprise Console, ne disposent pas de l'agent de conformité, ne sont pas exemptés et n'ont pas exécuté l'agent temporaire.
- Les **ordinateurs d'extrémité connus** sont administrés par la Sophos Enterprise Console, disposent de l'agent de conformité et l'exécutent.

Remarque : vous devez créer des exemptions pour les ordinateurs d'extrémité qui ne sont pas en mesure d'exécuter l'agent de conformité, tels que les ordinateurs d'extrémité avec systèmes d'exploitation non Windows. Les exemptions s'appliquent également aux ordinateurs d'extrémité ne nécessitant pas la vérification de leur conformité, tels que les serveurs, les routeurs et les imprimantes. Les ordinateurs d'extrémité recevant une adresse IP affectée de manière dynamique via DHCP sont les seuls ordinateurs d'extrémité devant être exemptés.

Procédez aux tâches du NAC Manager suivantes :

1. Exécutez l'assistant de configuration de DHCP pour configurer les serveurs proxy, d'actualisation, de l'agent temporaire et DHCP à utiliser avec la mise en application de DHCP de Sophos NAC.
2. Exécutez le rapport DHCP Enforcer du NAC Manager pour déterminer si les ordinateurs d'extrémité connus vont recevoir l'accès réseau approprié lorsque la mise en application de DHCP sera activée. Recherchez également les ordinateurs d'extrémité nécessitant une exemption.
3. Créez des exemptions pour les ordinateurs d'extrémité qui ne sont pas en mesure d'exécuter l'agent de conformité ou qui ne nécessitent pas la vérification de conformité.
4. Activez la mise en application de DHCP.

3.3.1 Exécution de l'assistant de configuration de DHCP

L'assistant de configuration DHCP vous aide à identifier les serveurs proxy, de correction, de l'agent temporaire et DHCP à utiliser avec les mises en place de Sophos NAC DHCP et configure automatiquement les modèles d'accès DHCP Enforcer par défaut avec vos définitions de serveurs.

Procédure

1. Connectez-vous au NAC Manager.
2. Cliquez sur **Enforce > DHCP Configuration Wizard**. Cliquez sur **Suivant** pour continuer.
3. Procédez de l'une des manières suivantes :

- Si vous utilisez des serveurs proxy, cliquez sur **Yes** et cliquez sur **Next**. Passez à l'étape suivante.
- Si vous n'utilisez **pas** de serveurs proxy, cliquez sur **No** et cliquez sur **Next**. Passez à l'étape 5.

Important : si vous ne définissez pas de serveur proxy pour l'accès Internet, les utilisateurs n'auront pas d'accès Internet et le modèle d'accès par défaut DHCP - Internet Access DHCP Enforcer aura seulement un accès pour correction.

4. Définissez les serveurs proxy requis pour autoriser l'accès Internet et cliquez sur **Next**. Procédez de l'une des manières suivantes :
 - Dessélectionnez les cases des serveurs que vous ne souhaitez **pas** inclure en tant que serveur proxy.
 - Cliquez sur **Add** pour ajouter de nouveaux serveurs, saisissez les informations du serveur proxy et cliquez sur **OK**. Répétez cette étape autant de fois que nécessaire pour ajouter d'autres serveurs. Dès qu'ils sont créés, ces serveurs peuvent être administrés sur la page **Enforce > Network Resources** .

Remarque : les serveurs proxy sélectionnés remplaceront les serveurs en cours d'utilisation dans le modèle d'accès DHCP - Internet Access DHCP Enforcer par défaut.

5. Définissez les serveurs d'actualisation requis pour autoriser l'accès aux opérations de correction, tels que les contrôleurs de domaine, et cliquez sur **Next**.

Procédez de l'une des manières suivantes :

- Dessélectionnez les cases des serveurs que vous ne souhaitez **pas** inclure en tant que serveur de correction.
- Cliquez sur **Add** pour ajouter de nouveaux serveurs, puis saisissez les informations du serveur d'actualisation et cliquez sur **OK**. Répétez cette étape autant de fois que nécessaire pour ajouter d'autres serveurs. Dès qu'ils sont créés, ces serveurs peuvent être administrés sur la page **Enforce > Network Resources** .

Remarque : les serveurs proxy sélectionnés remplaceront les serveurs en cours d'utilisation dans le modèle d'accès DHCP - Remediation Access DHCP Enforcer par défaut.

6. Procédez de l'une des manières suivantes :

- Si vous avez installé l'agent temporaire, cliquez sur **Yes**, puis sur **Next**. Passez à l'étape suivante.
- Si vous n'avez **pas** installé l'agent temporaire, cliquez sur **No**, puis sur **Next**. Passez à l'étape 8.

Remarque : si vous avez installé l'agent temporaire sur le même serveur que Sophos NAC, il n'est pas nécessaire de créer un serveur de l'agent temporaire supplémentaire.

7. Définissez les serveurs hébergeant l'agent temporaire afin que DHCP Enforcer puisse autoriser leur accès. Cet accès est requis afin que les ordinateurs d'extrémité inconnus, tels que les invités, puissent être connus du réseau. Cliquez sur **Add** pour ajouter de nouveaux serveurs, saisissez les informations du serveur de l'agent temporaire et cliquez sur **OK**. Puis cliquez sur **Next**. Dès qu'ils sont créés, ces serveurs peuvent être administrés sur la page **Configure System > Server Settings** .

8. Définissez les serveurs DHCP sur lesquels le logiciel DHCP Enforcer est installé. Cliquez sur **Add** pour ajouter de nouveaux serveurs, puis, saisissez les informations du serveur DHCP Enforcer et cliquez sur **OK**. Répétez cette étape autant de fois que nécessaire pour ajouter d'autres serveurs. Puis cliquez sur **Next**. Dès qu'ils sont créés, ces serveurs peuvent être administrés sur la page **Configure System > Server Settings** .

Remarque : la clé partagée doit correspondre à ce que vous avez saisi lors de l'installation de DHCP Enforcer sur le serveur. La clé partagée sert à sécuriser le trafic entre le serveur NAC et le serveur DHCP.

9. Cliquez sur **Finish**.

3.3.2 Exécution du rapport DHCP Enforcer

Exécutez le rapport Sophos NAC DHCP Enforcer pour déterminer l'état de conformité des ordinateurs d'extrémité avant d'activer la mise en application de DHCP. Les stratégies NAC prédéfinies sont paramétrées sur Report Only. Le rapport DHCP Enforcer peut être utilisé pour déterminer si le bon modèle d'accès sera appliqué lorsque la mise en application sera activée. Vous pouvez exempter des périphériques et accéder aux détails de l'évaluation depuis le rapport DHCP Enforcer.

Procédure

1. Connectez-vous au NAC Manager.
2. Cliquez sur **Report > Troubleshooting**.

3. Cliquez sur la liste **Report Type** et sélectionnez **DHCP Enforcer**.
4. Le cas échéant, cliquez sur le **signe plus** se trouvant à côté de **Report Criteria** et saisissez ou sélectionnez les options de recherche appropriées. Vous pouvez aussi cliquer sur le lien **Custom Sort** pour étendre vos options de triage. Les options de tri personnalisées du rapport sont modifiées temporairement lors de son exécution.

Remarque : vous pouvez utiliser le symbole * ou % pour effectuer une recherche avec un caractère joker sur la plupart des champs. Par exemple, si vous saisissez M% dans le champ Returned User Class, toutes les classes d'utilisateur qui commencent par un M s'affichent. De même, si vous saisissez M sans le symbole % dans le champ Returned User Class, seules les classes d'utilisateur qui s'appellent M s'affichent.

5. Cliquez sur **Run**.

Champs et descriptions

Champ	Description
Entrée du rapport Summary	
Date/Time	Date et heure de la tentative d'accès réseau. Remarque : la date et l'heure proviennent du fuseau horaire du navigateur Web accédant au NAC Manager.
MAC Address	Adresse MAC du périphérique tentant de se connecter au réseau. L'adresse MAC qui apparaît est affectée au NIC associé à la requête DHCP du client.
Computer Name	Nom du périphérique tentant de se connecter au réseau. Le nom de l'ordinateur est dérivé de la requête du client.
Compliance State	État de conformité de l'ordinateur d'extrémité, affecté lors de l'évaluation de la conformité. Les états de conformité disponibles sont Compliant (conforme), Partially Compliant (partiellement conforme) et Non-Compliant (non conforme). Trois tirets (---) signifient que l'agent n'a pas signalé d'état de conformité. Les modèles d'accès DHCP Enforcer associés à l'état de conformité de stratégie déterminent l'accès réseau.
Template Name (Version)	Nom et version du modèle d'accès qui détermine l'action prise par le DHCP Enforcer. Le modèle d'accès utilisé est basé sur la raison. Les modèles d'accès disponibles incluent les modèles par défaut suivants ainsi que tous les modèles d'accès que vous avez créés : <ul style="list-style-type: none"> ■ DHCP - Full Access : autorise l'accès intégral au réseau. ■ DHCP - Internet Access : permet l'accès à Internet et refuse l'accès aux adresses IP privées et au réseau local (LAN). <p>Important : si vous ne définissez pas de serveur proxy pour l'accès Internet comme ressource réseau, les utilisateurs n'auront pas d'accès Internet et ce modèle fournira uniquement l'accès à des fins d'actualisation.</p>

Champ	Description
	<ul style="list-style-type: none"> ■ DHCP - Remediation Access : refuse tout accès réseau sauf aux serveurs d'actualisation, au serveur NAC et au serveur de l'agent temporaire.
Reason	<p>Raison pour laquelle un modèle d'accès particulier a été affecté par le DHCP Enforcer. Les conditions disponibles sont :</p> <ul style="list-style-type: none"> ■ Assessment : l'évaluation effectuée par l'agent a déterminé l'état de conformité. Les modèles d'accès DHCP Enforcer associés à l'état de conformité de stratégie déterminent l'accès réseau. Un lien apparaît vers les informations concernant l'évaluation de conformité associée à cette entrée DHCP Enforcer. ■ Default Template : l'ordinateur d'extrémité peut avoir une stratégie associée ou être une exemption désignée, mais aucun modèle d'accès associé n'a été trouvé. Les modèles d'accès par défaut désignés dans la zone Configure System > Enforcer Settings déterminent l'accès réseau. ■ Enforcer Override : la mise en application n'a pas été vérifiée. Si la case à cocher Override DHCP Enforcer est sélectionnée dans la zone Configure System > Enforcer Settings, les modèles d'accès Maintenance Mode/Enforcer Override aussi désignés dans cette zone déterminent l'accès réseau. ■ Exempted : l'ordinateur d'extrémité est exempté selon les critères d'exemption définis dans la zone Enforce > Exemptions. Les modèles d'accès associés aux critères d'exemption déterminent l'accès réseau. Les sous-raisons Exempted apparaissent entre parenthèses : <ul style="list-style-type: none"> ■ User Class : la classe d'utilisateur a été spécifiée comme une exemption. ■ Vendor Class : la classe du fournisseur a été spécifiée comme une exemption. ■ MAC : l'adresse MAC a été spécifiée comme une exemption. ■ IP Scope : l'étendue IP a été spécifiée comme une exemption. ■ Maintenance Mode : le logiciel est en mode de maintenance. Les modèles d'accès Maintenance Mode/Enforcer Override désignés dans la zone Configure System > Enforcer Settings déterminent l'accès réseau. ■ Policy Retrieval Error : l'état de conformité de l'ordinateur d'extrémité est obsolète d'après le champ DHCP Policy Update Threshold configuré dans la zone Configure System > Enforcer Settings. Les modèles d'accès DHCP Enforcer de la stratégie associés à l'état Policy Retrieval Error déterminent l'accès réseau. ■ Remediate : la stratégie est en mode Remediate. Les modèles d'accès DHCP Enforcer associés au mode de stratégie Remediate déterminent l'accès réseau. ■ Report Only : la stratégie est en mode Report Only. Les modèles d'accès DHCP Enforcer associés au mode de stratégie Report Only déterminent l'accès réseau. ■ Reserved : l'adresse MAC du périphérique demandant l'accès réseau est réservé pour un périphérique particulier sur le serveur DHCP.

Champ	Description
	<ul style="list-style-type: none"> ■ System Error : Enforcer a rencontré une erreur qui a empêché le succès de l'opération. Le paramètre du registre SystemErrors dans le serveur NAC est défini par défaut pour refuser l'accès réseau. ■ Template Error : un modèle d'accès associé était introuvable et les modèles d'accès par défaut désignés dans la zone Configure System > Enforcer Settings n'ont pas pu être utilisés. Si cette erreur survient, l'accès réseau est déterminé par le serveur DHCP, lequel ne renverra pas de classe d'utilisateur et refusera l'accès à l'utilisateur. ■ Unknown Endpoint : aucun enregistrement de conformité n'existe. Les modèles d'accès Unknown Endpoint désignés dans la zone Configure System > Enforcer Settings déterminent l'accès réseau.
Returned User Class	Classe d'utilisateur DHCP renvoyée au serveur DHCP par le DHCP Enforcer pour application.
DHCP Server	Adresse IP du serveur DHCP demandant l'accès réseau depuis le DHCP Enforcer. Il s'agit du serveur DHCP sur lequel le logiciel DHCP Enforcer est installé.
Entrée du rapport Detailed	
Agent Enforcement Action	<p>Action prise par l'ordinateur d'extrémité concernant l'affectation des adresses IP. L'ordinateur d'extrémité initialise la publication et le renouvellement des adresses IP d'après l'action d'application d'agents spécifiée dans la stratégie. L'agent obtient de nouvelles adresses IP lorsqu'il démarre et lance une évaluation de conformité, lorsque l'état de conformité de l'ordinateur d'extrémité change, lorsque le mode de stratégie change et lorsque les modèles d'accès DHCP Enforcer définis dans la stratégie de l'ordinateur d'extrémité changent. Les valeurs disponibles incluent :</p> <ul style="list-style-type: none"> ■ None : les adresses IP de l'ordinateur d'extrémité ne sont ni publiées ni renouvelées. ■ Release Renew : les adresses IP de l'ordinateur d'extrémité sont publiées, puis renouvelées à l'aide du serveur DHCP. Les adresses IP courantes sont laissées de côté avant l'obtention de nouvelles. ■ Trois tirets (---) : l'agent n'a pas signalé d'action.
Vendor Class	Classe du fournisseur du client DHCP.
DHCP Relay	Adresse IP du relais DHCP (s'il est présent dans la requête DHCP originale) utilisé par le DHCP Enforcer pour sélectionner un modèle d'accès DHCP Enforcer. 0.0.0.0 apparaît si un relais DHCP n'est pas utilisé.
Transaction ID	Identifiant de transaction renvoyé depuis le serveur DHCP. L'identifiant de transaction associe les messages du client DHCP avec les réponses du serveur.

3.3.3 Création d'exemptions DHCP

Les ordinateurs d'extrémité exemptés ne sont pas en mesure d'exécuter l'agent de conformité, tels que les ordinateurs d'extrémité avec systèmes d'exploitation non Windows. Les exemptions s'appliquent également aux ordinateurs d'extrémité ne nécessitant pas la vérification de leur conformité, tels que les serveurs, les routeurs et les imprimantes. Les ordinateurs d'extrémité recevant une adresse IP affectée de manière dynamique via DHCP sont les seuls ordinateurs d'extrémité devant être exemptés. Créez les exemptions DHCP pour ces ordinateurs d'extrémité sinon, ils seront interdits d'accès au réseau lorsque vous activerez la mise en application de DHCP.

À l'aide du NAC Manager, vous pouvez créer deux types d'exemptions DHCP :

- **Exemptions par critères DHCP** : exemptions créées par l'adresse MAC, la classe d'utilisateur et la classe du fournisseur.
- **Exemptions par étendues IP** : exemptions créées pour des segments du réseau.

3.3.3.1 Création d'exemptions par critères DHCP

Utilisez la page Exemptions du NAC Manager pour créer des exemptions par critères DHCP. Les critères d'exemption et les modèles d'accès DHCP Enforcer sont utilisés conjointement les uns avec les autres pour identifier les exemptions et indiquer des actions. Une fois que le critère d'exemption défini est trouvé, les modèles d'accès DHCP Enforcer déterminent l'action d'accès réseau appropriée à prendre.

Procédure

1. Connectez-vous au NAC Manager.
2. Cliquez sur **Enforce > Exemptions**. Puis cliquez sur **Create Exemption** dans la section inférieure gauche de la page.
3. Saisissez un nom et une description d'exemption.
4. Cliquez sur la zone de liste **Exemption Type** et sélectionnez **DHCP Criteria**.
5. Sous Exemption Criteria, sélectionnez l'option **MAC Address**, **User Class** ou **Vendor Class** pour spécifier les critères d'exemption que vous voulez définir, saisissez l'adresse MAC (ou le préfixe) appropriée, la classe d'utilisateur ou la classe de fournisseur dans le champ prévu, puis cliquez sur **Add**.

Répétez cette opération autant que nécessaire pour ajouter des critères d'exemption supplémentaires.

Remarque : vous pouvez utiliser le symbole * pour spécifier des exemptions avec des caractères joker à partir du moment où le symbole * est en dernier. Par exemple, si vous spécifiez AA* comme adresse MAC, toutes les adresses MAC commençant par AA seront exemptées. Si vous spécifiez une adresse MAC sans le symbole *, vous devez spécifier l'adresse MAC exacte que vous voulez exempter.

6. Cliquez sur **Select** pour ajouter des modèles d'accès DHCP Enforcer à l'exemption, sélectionnez le modèle d'accès **DHCP - Full Access** et cliquez sur **OK**.

Le modèle d'accès **DHCP - Full Access** est prédéfini dans Sophos NAC pour permettre l'accès au réseau. Vous avez configuré cette exemption pour accéder au réseau sans évaluation de la conformité par Sophos NAC.

7. Cliquez sur **Save**.

3.3.3.2 Création d'exemptions par étendues IP

Les ordinateurs d'extrémité recevant une adresse IP affectée de manière dynamique via DHCP sont les seuls ordinateurs d'extrémité devant être exemptés. Utilisez la page Exemptions du NAC Manager pour créer des exemptions par étendues IP. Les exemptions par étendues IP sont des exemptions créées pour des segments du réseau. Les exemptions par étendues IP sont utiles lors d'un déploiement par phases de l'application dans toute l'entreprise, vous pouvez exempter des segments de réseau que vous ne souhaitez pas encore appliquer.

Procédure

1. Connectez-vous au NAC Manager.
2. Cliquez sur **Enforce > Exemptions**. Puis cliquez sur **Create Exemption** dans la section inférieure gauche de la page.
3. Saisissez un nom et une description d'exemption.
4. Cliquez sur la liste **Exemption Type** et sélectionnez **IP Scope**.
5. Sous Exempted IP Scopes, cliquez sur **Select** pour ajouter des étendues IP existantes à l'exemption, sélectionnez les étendues appropriées et cliquez sur **OK**.

Si vous ne voyez pas l'étendue IP dont vous avez besoin, vous pouvez en créer une. Pour cela, créez un nouveau modèle d'accès DHCP Enforcer ou mettez à jour un des modèles d'accès DHCP Enforcer prédéfinis.

6. Si nécessaire, utilisez les flèches pour classer les étendues par ordre de priorité.

Si plusieurs étendues IP s'appliquent à une exemption particulière, la première étendue IP rencontrée sera utilisée. Nous vous recommandons de classer par ordre de priorité les étendues les plus spécifiques/strictes, puis les moins spécifiques/strictes.

7. Cliquez sur **Save**.

Important : une fois que vous avez créé des exemptions, vous pouvez les classer par ordre de priorité sur la page de liste **Exemptions**. Si plusieurs exemptions s'appliquent à un ordinateur d'extrémité particulier, la première exemption associée à cet ordinateur sera utilisée. Nous vous conseillons de classer par ordre de priorité les exemptions les plus spécifiques/strictes, puis les moins spécifiques/strictes.

3.3.4 Activation de la mise en application de DHCP

Vous pouvez activer la mise en application de DHCP pour les ordinateurs d'extrémité inconnus et connus. Nous vous conseillons d'utiliser la mise en application de DHCP pour les ordinateurs d'extrémité inconnus et la mise en application de l'agent pour les ordinateurs d'extrémité connus. Toutefois, Sophos NAC ne vous permet pas d'utiliser la mise en application de DHCP pour les ordinateurs d'extrémité connus.

3.3.4.1 Activation de la mise en application de DHCP pour les ordinateurs d'extrémité inconnus

Vous pouvez activer la mise en application de DHCP pour les ordinateurs d'extrémité inconnus sur chaque serveur DHCP. Ainsi, vous pouvez spécifier les serveurs DHCP qui mettront en quarantaine les ordinateurs d'extrémité inconnus. Utilisez cette fonction pour effectuer un déploiement par étapes de la mise en application de DHCP.

Avant d'activer la mise en application de DHCP pour les ordinateurs d'extrémité inconnus, créez des exemptions. Les ordinateurs d'extrémité recevant une adresse IP affectée de manière dynamique via DHCP sont les seuls ordinateurs d'extrémité devant être exemptés.

Procédure

1. Connectez-vous au NAC Manager.
2. Cliquez sur **Configure System > Server Settings**.
3. Cliquez sur le nom du serveur DHCP pour lequel vous souhaitez activer la mise en application de DHCP.
4. Cliquez sur la liste **Unknown Endpoint Mode** et sélectionnez **Enforce**. Le mode Enforce utilise le modèle d'accès DHCP - Internet Access pour mettre en quarantaine les ordinateurs d'extrémité inconnus et autoriser l'accès à Internet ou aux serveurs d'actualisation.

Remarque : si vous avez défini un serveur proxy lorsque vous avez lancé l'assistant de configuration de DHCP, les ordinateurs d'extrémité ont accès à Internet. Si vous n'avez pas défini un serveur proxy, les ordinateurs d'extrémité accèdent aux serveurs d'actualisation que vous avez définis dans l'assistant de configuration de DHCP. Vous pouvez changer le modèle d'accès dans la zone **Configure System > Enforcer Settings**.

5. Cliquez sur **Save**.

3.3.4.2 Activation de la mise en application de DHCP pour les ordinateurs d'extrémité connus

Vous pouvez activer la mise en application de DHCP pour les ordinateurs d'extrémité connus dans les stratégies. Si vous envisagez d'utiliser la mise en application de DHCP ou l'application de l'agent pour les ordinateurs d'extrémité connus, changez le mode des stratégies dans Policy Mode de Report Only sur Enforce.

Important : toutes les stratégies et changements de stratégies s'appliquent immédiatement, en revanche, une stratégie ne s'applique pas à l'ordinateur d'extrémité tant que l'agent ne la récupère pas.

Procédure

1. Connectez-vous au NAC Manager.
2. Cliquez sur **Manage > Policies**. Puis cliquez sur le nom de la stratégie que vous voulez mettre à jour.
3. Cliquez sur la liste **Policy Mode** et sélectionnez **Enforce**.
 - **Enforce :** le mode de stratégie Enforce spécifie que les ordinateurs d'extrémité sont évalués par rapport à la stratégie affectée et que les informations relatives au rapport sont générées dans le NAC Manager. Les messages apparaissent, les actions d'actualisation sont effectuées et des actions d'application sont prises à travers l'utilisation de modèles d'accès pour l'état d'accès approprié. Le mode Enforce utilise les modèles d'accès affectés à l'étape 5.
4. Cliquez sur la liste **Agent Enforcement Action** et sélectionnez **Release Renew**. Vous devez sélectionner Release Renew lors de l'utilisation de la mise en application de DHCP pour les ordinateurs d'extrémité connus.

5. Dans la zone de navigation gauche Network Access, cliquez sur **DHCP**. Cliquez sur l'onglet **Enforcer** et vérifiez les affectations des modèles d'accès.

Remarque : par défaut, chaque stratégie est automatiquement chargée avec les modèles d'accès. Assurez-vous que les modèles d'accès corrects sont appliqués. Conservez les affectations des modèles d'accès Report Only et Remediate.

Affectations du modèle d'accès DHCP Enforcer prédéfini

- **Policy Retrieval Error :** l'état de conformité de l'ordinateur d'extrémité est obsolète d'après le champ DHCP Policy Update Threshold configuré dans la zone **Configure System > Enforcer Settings** . Le modèle d'accès DHCP - Remediation Access refuse l'accès au réseau sauf aux serveurs de correction que vous avez définis lors de l'exécution de l'assistant de configuration de DHCP.
 - **Compliant :** l'ordinateur d'extrémité est conforme. Le modèle d'accès DHCP - Full Access autorise l'accès au réseau lorsque l'ordinateur d'extrémité est conforme.
 - **Partially Compliant :** l'ordinateur d'extrémité est partiellement conforme. Le modèle d'accès DHCP - Full Access autorise l'accès au réseau lorsque l'ordinateur d'extrémité est conforme.
 - **Non-Compliant :** l'ordinateur d'extrémité n'est pas conforme. Le modèle d'accès DHCP - Remediation Access refuse l'accès au réseau sauf aux serveurs de correction que vous avez définis lors de l'exécution de l'assistant de configuration de DHCP.
6. Si nécessaire, utilisez les flèches pour classer par ordre de priorité les modèles d'accès DHCP Enforcer.
Si plusieurs modèles s'appliquent à un état particulier, le premier modèle correspondant à l'état est utilisé. Nous vous recommandons d'attribuer d'abord les modèles d'accès les plus spécifiques/stricts et ensuite les modèles d'accès les moins spécifiques/stricts.
 7. Cliquez sur **Save**.

3.3.4.2.1 Utilisation des stratégies prédéfinies

Vous pouvez utiliser les stratégies prédéfinies pour appliquer la stratégie de conformité à la sécurité aux ordinateurs d'extrémité administrés et non administrés.

- **Default :** cette stratégie est affectée si l'agent de conformité est installé sur un ordinateur d'extrémité et si aucune stratégie n'a été affectée. Par défaut, le mode de stratégie est paramétré sur Report Only. Cette stratégie effectue des actions d'actualisation sur l'ordinateur d'extrémité si le mode de stratégie est paramétré sur Remediate ou Enforce.
- **Managed :** cette stratégie peut être utilisée pour les ordinateurs d'extrémité qui sont administrés avec la Sophos Enterprise Console et sur lesquels un agent de conformité est installé. Par défaut, le mode de stratégie est paramétré sur Report Only. Cette stratégie effectue des actions d'actualisation sur l'ordinateur d'extrémité si le mode de stratégie est paramétré sur Remediate ou Enforce.
- **Unmanaged :** cette stratégie peut être utilisée pour les ordinateurs d'extrémité situés hors de l'entreprise. Cette stratégie n'effectue pas d'actions d'actualisation sur l'ordinateur d'extrémité. L'agent temporaire utilise la stratégie Unmanaged.

Remarque : si l'agent de conformité n'est pas installé sur un ordinateur d'extrémité et si ce dernier n'utilise pas l'agent temporaire, les paramètres Enforcer déterminent l'accès réseau.

3.3.4.3 Expérience utilisateur de la mise en application de DHCP

Dès que vous avez activé la mise en application de DHCP, l'expérience utilisateur de la mise en application de DHCP dépend de l'état inconnu ou connu de l'ordinateur d'extrémité. En outre, les invités peuvent exécuter l'agent temporaire de conformité pour obtenir l'accès au réseau.

- Les **ordinateurs d'extrémité inconnus** ne sont pas administrés par la Sophos Enterprise Console, ne disposent pas de l'agent de conformité, ne sont pas exemptés et n'ont pas exécuté l'agent temporaire.
- Les **ordinateurs d'extrémité invités** peuvent utiliser l'agent temporaire de conformité pour le contrôle d'accès réseau.
- Les **ordinateurs d'extrémité connus** sont administrés par la Sophos Enterprise Console, disposent de l'agent de conformité et l'exécutent.

Expérience utilisateur de la mise en application de DHCP pour ordinateurs d'extrémité inconnus

Lorsque la mise en application de DHCP est activée, les utilisateurs des ordinateurs d'extrémité inconnus sont soumis à l'expérience suivante :

1. L'ordinateur d'extrémité démarre.
2. Lorsque la mise en application de DHCP pour les ordinateurs d'extrémité inconnus est activée, les ordinateurs d'extrémité disposent d'un accès au réseau limité. Ces ordinateurs d'extrémité accèdent à Internet ou aux serveurs d'actualisation. Si vous avez défini un serveur proxy lorsque vous avez lancé l'assistant de configuration de DHCP, les ordinateurs d'extrémité ont accès à Internet. Si vous n'avez pas défini un serveur proxy, les ordinateurs d'extrémité accèdent aux serveurs d'actualisation que vous avez définis dans l'assistant de configuration de DHCP.

Expérience utilisateur de la mise en application de DHCP pour ordinateurs d'extrémité invités

Lorsque la mise en application de DHCP est activée et que les ordinateurs d'extrémité invités doivent utiliser l'agent temporaire de conformité, les utilisateurs invités sont soumis à l'expérience suivante :

1. L'ordinateur d'extrémité démarre.
2. L'utilisateur ouvre Internet Explorer, navigue vers l'URL de l'agent temporaire de conformité et exécute l'agent temporaire de conformité.
3. L'agent temporaire de conformité effectue une évaluation et détermine si l'ordinateur d'extrémité est conforme, partiellement conforme ou non conforme à la stratégie NAC.
4. Lorsque la mise en application de DHCP est configurée et activée, il se passe ce qui suit :
 - Les ordinateurs d'extrémité conformes sont autorisés à accéder au réseau.
 - Les ordinateurs d'extrémité partiellement conformes sont autorisés à accéder au réseau. L'agent temporaire de conformité affiche des messages à l'utilisateur afin que celui-ci puisse actualiser son ordinateur d'extrémité et le mettre en conformité. Si la stratégie NAC est configurée pour actualiser automatiquement l'ordinateur d'extrémité, l'actualisation de l'ordinateur d'extrémité a lieu. Par défaut, l'actualisation est désactivée. Nous vous conseillons de ne pas corriger l'ordinateur d'extrémité d'un utilisateur invité.

- Les ordinateurs d'extrémité non conformes sont interdits d'accès au réseau. Ces ordinateurs d'extrémité accèdent à Internet ou aux serveurs d'actualisation. Si vous avez défini un serveur proxy lorsque vous avez lancé l'assistant de configuration de DHCP, les ordinateurs d'extrémité ont accès à Internet. Si vous n'avez pas défini un serveur proxy, les ordinateurs d'extrémité accèdent aux serveurs d'actualisation que vous avez définis dans l'assistant de configuration de DHCP. L'agent temporaire de conformité affiche des messages à l'utilisateur afin que celui-ci puisse actualiser son ordinateur d'extrémité afin qu'il soit conforme. Si la stratégie NAC est configurée pour actualiser automatiquement l'ordinateur d'extrémité, l'actualisation de l'ordinateur d'extrémité a lieu. Par défaut, l'actualisation est désactivée. Nous vous conseillons de ne pas corriger l'ordinateur d'extrémité d'un utilisateur invité.


Expérience utilisateur de la mise en application de DHCP pour les ordinateurs d'extrémité connus

Lorsque la mise en application de DHCP est activée, les ordinateurs d'extrémité connus sont soumis à l'expérience DHCP suivante :

1. L'ordinateur d'extrémité démarre et l'agent de conformité s'exécute.
2. L'agent de conformité effectue une évaluation et détermine si l'ordinateur d'extrémité est conforme, partiellement conforme ou non conforme à la stratégie NAC.
3. Lorsque la mise en application de DHCP est configurée et activée, il se passe ce qui suit :
 - Les ordinateurs d'extrémité conformes sont autorisés à accéder au réseau.
 - Les ordinateurs d'extrémité partiellement conformes sont autorisés à accéder au réseau. L'agent de conformité affiche des messages à l'utilisateur afin que celui-ci puisse actualiser son ordinateur d'extrémité afin qu'il soit conforme. Si la stratégie NAC est configurée pour actualiser automatiquement l'ordinateur d'extrémité, l'actualisation a lieu.
 - Les ordinateurs d'extrémité non conformes sont interdits d'accès au réseau. Ces ordinateurs d'extrémité ont accès à Internet et à tous les serveurs d'actualisation que vous avez définis lors de l'exécution de l'assistant de configuration de DHCP. L'agent de conformité affiche des messages à l'utilisateur afin que celui-ci puisse actualiser son ordinateur d'extrémité afin qu'il soit conforme. Si la stratégie NAC est configurée pour actualiser automatiquement l'ordinateur d'extrémité, l'actualisation de l'ordinateur d'extrémité a lieu.

4 Mise à niveau de la mise en application de DHCP

Pour utiliser la mise en application de DHCP dans la version 3.9 de Sophos NAC, procédez à la mise à niveau de votre logiciel de mise en application de DHCP. Pour procéder à la mise à niveau, désinstallez votre logiciel DHCP existant, puis installez le nouveau logiciel. Désactivez également la mise en application de DHCP avant de désinstaller le logiciel et activez-la suite à l'installation du nouveau logiciel.

 **Attention :** pour procéder à la mise à niveau, désactivez la mise en application de DHCP. nous vous conseillons de mettre à niveau la mise en application de DHCP à une heure faisant encourir un risque minimal pour votre réseau.

4.1 Liste de contrôle de la mise à niveau de la mise en application de DHCP

La liste de contrôle de la mise à niveau de la mise en application de DHCP contient une liste de tâches requises pour mettre à niveau la mise en application de DHCP à la version 3.9 de Sophos NAC. Sauf mention contraire, toutes les tâches sont effectuées conformément aux instructions du présent document.

Tâche	Description	Terminée
Mise à niveau de Sophos NAC		
1.	Procédez à la mise à niveau de Sophos NAC. Pour plus d'informations, allez dans le Centre de mise à niveau d'Endpoint Security and Control à l'adresse http://www.sophos.fr/support/upgrades/ .	
Tâches du Sophos NAC Manager, partie 1		
2.	Désactivez la mise en application de DHCP.	
Tâches du serveur DHCP		
3.	Désinstallez le logiciel DHCP Enforcer existant sur chaque serveur DHCP.	
4.	<p>Installez le nouveau logiciel DHCP Enforcer sur chaque serveur DHCP.</p> <p>Important : lorsque vous installez le logiciel DHCP Enforcer sur un serveur DHCP, saisissez de nouveau la clé partagée. Si possible, utilisez la clé partagée de la version précédente, car elle correspondra à la clé partagée du même serveur DHCP dans le NAC Manager. Si vous ne savez pas quelle clé partagée était utilisée dans la version précédente, créez-en une nouvelle pendant l'installation du logiciel. Toutefois, vous devrez ensuite mettre à jour la clé partagée de ce serveur DHCP dans le NAC Manager pour que ces clés correspondent.</p> <p>Remarque : suite à l'installation du logiciel DHCP Enforcer, vérifiez que le service DHCP fonctionne sur chaque serveur DHCP.</p>	

Tâche	Description	Terminée
Tâches du Sophos NAC Manager, partie 2		
5.	Mettez à jour la clé partagée pour chaque serveur DHCP. (Tâche facultative)	
6.	Activez la mise en application de DHCP.	

4.2 Désactivation de la mise en application de DHCP

Désactivez la mise en application de DHCP des ordinateurs d'extrémité inconnus et connus lors de la mise à niveau de la mise en application de DHCP. Nous vous conseillons d'utiliser la mise en application de DHCP pour les ordinateurs d'extrémité inconnus et la mise en application de l'agent pour les ordinateurs d'extrémité connus. Toutefois, Sophos NAC ne vous permet pas d'utiliser la mise en application de DHCP pour les ordinateurs d'extrémité connus.

4.2.1 Désactivation de la mise en application de DHCP pour les ordinateurs d'extrémité inconnus

Pour désactiver la mise en application de DHCP pour les ordinateurs d'extrémité inconnus, modifiez le mode Unknown Endpoint sur chaque serveur DHCP de Enforce à Report Only.

Procédure

1. Cliquez sur **Configure System > Server Settings**.
2. Cliquez sur le nom du serveur DHCP pour lequel vous souhaitez désactiver la mise en application de DHCP.
3. Cliquez sur la liste **Unknown Endpoint Mode** et sélectionnez **Report Only**. Le mode Report Only utilise le modèle d'accès DHCP - Full Access afin d'autoriser l'accès au réseau aux ordinateurs d'extrémité inconnus.
4. Cliquez sur **Save**.

4.2.2 Désactivation de la mise en application de DHCP pour les ordinateurs d'extrémité connus

Pour désactiver la mise en application de DHCP, modifiez le mode de stratégie de Enforce à Report Only dans les stratégies appropriées.

Important : toutes les stratégies et changements de stratégies s'appliquent immédiatement, en revanche, une stratégie ne s'applique pas à l'ordinateur d'extrémité tant que l'agent ne la récupère pas.

Remarque : si vous utilisez la mise en application de l'agent plutôt que la mise en application de DHCP pour les ordinateurs d'extrémité connus, cette tâche n'est pas nécessaire.

Procédure

1. Connectez-vous au NAC Manager.

2. Cliquez sur **Manage > Policies**. Puis cliquez sur le nom de la stratégie que vous voulez mettre à jour.
3. Cliquez sur la liste **Policy Mode** et sélectionnez **Report Only**.
 - **Report Only** : le mode de stratégie Report Only spécifie que les ordinateurs d'extrémité sont évalués par rapport à la stratégie affectée et que les informations relatives au rapport sont générées dans le NAC Manager. Aucun message n'apparaît, aucune action d'actualisation n'est effectuée et aucune action d'application n'est prise. Le mode Report Only utilise le modèle d'accès DHCP - Full Access afin d'autoriser l'accès au réseau aux ordinateurs d'extrémité connus.
4. Cliquez sur **Save**.

4.3 Désinstallation du logiciel DHCP Enforcer

Désinstallez le logiciel DHCP Enforcer sur chaque serveur Microsoft DHCP. Le logiciel DHCP Enforcer inclut DHCP Enforcer et l'outil de configuration DHCP Enforcer Configuration Utility.

1. Dans le menu Démarrer, sélectionnez **Panneau de configuration > Ajout/Suppression de programmes**.
2. Sélectionnez **Sophos DHCP Enforcer Software**, puis cliquez sur **Supprimer**.
3. Cliquez sur **Oui** pour confirmer la suppression du logiciel DHCP Enforcer.

4.4 Installation du logiciel DHCP Enforcer

Installez le logiciel DHCP Enforcer sur chaque serveur Microsoft DHCP. Le logiciel DHCP Enforcer inclut DHCP Enforcer et l'utilitaire de configuration DHCP Enforcer Configuration Utility. Le serveur DHCP est configuré lors de l'installation. Si vous devez modifier les paramètres du serveur DHCP qui ont été définis lors de l'installation de DHCP Enforcer, utilisez l'utilitaire de configuration DHCP Enforcer Configuration Utility. Pour plus d'informations, reportez-vous à la section [Annexe : utilisation de l'utilitaire de configuration de DHCP Enforcer](#) à la page 24.

1. Rendez-vous sur <http://www.sophos.fr/support/updates/>.
2. Saisissez votre nom utilisateur et mot de passe MySophos.
3. Sur la page Web des téléchargements **Enterprise**, téléchargez le programme d'installation de NAC DHCP Enforcer.
4. Exécutez le programme d'installation.

L'assistant d'installation vous guide tout au long de l'installation. Acceptez les options par défaut.

Conservez un enregistrement de la clé partagée que vous entrez sur la page **Sophos DHCP Enforcer**. La clé partagée sert à sécuriser le trafic entre le serveur NAC et le serveur DHCP. La même clé partagée doit être saisie lorsque vous lancez l'assistant DHCP Configuration Wizard à l'aide du NAC Manager.

Remarque : suite à l'installation du logiciel DHCP Enforcer, vérifiez que le service DHCP fonctionne sur chaque serveur DHCP.

4.5 Mise à jour de la clé partagée du serveur DHCP

La clé partagée sert à sécuriser le trafic entre le serveur NAC et le serveur DHCP.

Lorsque vous installez le logiciel DHCP Enforcer sur un serveur DHCP, saisissez de nouveau la clé partagée. Si possible, utilisez la clé partagée de la version précédente, car elle correspond à la clé partagée du même serveur DHCP dans le NAC Manager. Si vous ne savez pas quelle clé partagée était utilisée dans la version précédente, créez-en une nouvelle pendant l'installation du logiciel. Toutefois, vous devrez ensuite mettre à jour la clé partagée de ce serveur DHCP dans le NAC Manager pour que ces clés correspondent.

Remarque : si vous avez utilisé la clé partagée de la version précédente pendant l'installation du logiciel DHCP Enforcer, cette tâche n'est pas nécessaire.

Procédure

1. Cliquez sur **Configure System > Server Settings**.
2. Cliquez sur le nom du serveur DHCP dont la clé partagée doit être mise à jour.
3. Saisissez et confirmez la clé partagée du serveur.

Important : la clé partagée doit correspondre à ce que vous avez saisi lors de l'installation du logiciel DHCP Enforcer sur le serveur DHCP.

4. Cliquez sur **Save**.

4.6 Activation de la mise en application de DHCP

Vous pouvez activer la mise en application de DHCP pour les ordinateurs d'extrémité inconnus et connus. Nous vous conseillons d'utiliser la mise en application de DHCP pour les ordinateurs d'extrémité inconnus et la mise en application de l'agent pour les ordinateurs d'extrémité connus. Toutefois, Sophos NAC ne vous permet pas d'utiliser la mise en application de DHCP pour les ordinateurs d'extrémité connus.

4.6.1 Activation de la mise en application de DHCP pour les ordinateurs d'extrémité inconnus

Vous pouvez activer la mise en application de DHCP pour les ordinateurs d'extrémité inconnus sur chaque serveur DHCP. Ainsi, vous pouvez spécifier les serveurs DHCP qui mettront en quarantaine les ordinateurs d'extrémité inconnus. Utilisez cette fonction pour effectuer un déploiement par étapes de la mise en application de DHCP.

Avant d'activer la mise en application de DHCP pour les ordinateurs d'extrémité inconnus, créez des exemptions. Les ordinateurs d'extrémité recevant une adresse IP affectée de manière dynamique via DHCP sont les seuls ordinateurs d'extrémité devant être exemptés.

Procédure

1. Connectez-vous au NAC Manager.
2. Cliquez sur **Configure System > Server Settings**.
3. Cliquez sur le nom du serveur DHCP pour lequel vous souhaitez activer la mise en application de DHCP.

4. Cliquez sur la liste **Unknown Endpoint Mode** et sélectionnez **Enforce**. Le mode Enforce utilise le modèle d'accès DHCP - Internet Access pour mettre en quarantaine les ordinateurs d'extrémité inconnus et autoriser l'accès à Internet ou aux serveurs d'actualisation.

Remarque : si vous avez défini un serveur proxy lorsque vous avez lancé l'assistant de configuration de DHCP, les ordinateurs d'extrémité ont accès à Internet. Si vous n'avez pas défini un serveur proxy, les ordinateurs d'extrémité accèdent aux serveurs d'actualisation que vous avez définis dans l'assistant de configuration de DHCP. Vous pouvez changer le modèle d'accès dans la zone **Configure System > Enforcer Settings** .

5. Cliquez sur **Save**.

4.6.2 Activation de la mise en application de DHCP pour les ordinateurs d'extrémité connus

Vous pouvez activer la mise en application de DHCP pour les ordinateurs d'extrémité connus dans les stratégies. Si vous envisagez d'utiliser la mise en application de DHCP ou l'application de l'agent pour les ordinateurs d'extrémité connus, changez le mode des stratégies dans Policy Mode de Report Only sur Enforce.

Important : toutes les stratégies et changements de stratégies s'appliquent immédiatement, en revanche, une stratégie ne s'applique pas à l'ordinateur d'extrémité tant que l'agent ne la récupère pas.

Procédure

1. Connectez-vous au NAC Manager.
2. Cliquez sur **Manage > Policies**. Puis cliquez sur le nom de la stratégie que vous voulez mettre à jour.
3. Cliquez sur la liste **Policy Mode** et sélectionnez **Enforce**.
 - **Enforce :** le mode de stratégie Enforce spécifie que les ordinateurs d'extrémité sont évalués par rapport à la stratégie affectée et que les informations relatives au rapport sont générées dans le NAC Manager. Les messages apparaissent, les actions d'actualisation sont effectuées et des actions d'application sont prises à travers l'utilisation de modèles d'accès pour l'état d'accès approprié. Le mode Enforce utilise les modèles d'accès affectés à l'étape 5.
4. Cliquez sur la liste **Agent Enforcement Action** et sélectionnez **Release Renew**. Vous devez sélectionner Release Renew lors de l'utilisation de la mise en application de DHCP pour les ordinateurs d'extrémité connus.

5. Dans la zone de navigation gauche Network Access, cliquez sur **DHCP**. Cliquez sur l'onglet **Enforcer** et vérifiez les affectations des modèles d'accès.

Remarque : par défaut, chaque stratégie est automatiquement chargée avec les modèles d'accès. Assurez-vous que les modèles d'accès corrects sont appliqués. Conservez les affectations des modèles d'accès Report Only et Remediate.

Affectations du modèle d'accès DHCP Enforcer prédéfini

- **Policy Retrieval Error :** l'état de conformité de l'ordinateur d'extrémité est obsolète d'après le champ DHCP Policy Update Threshold configuré dans la zone **Configure System > Enforcer Settings** . Le modèle d'accès DHCP - Remediation Access refuse l'accès au réseau sauf aux serveurs de correction que vous avez définis lors de l'exécution de l'assistant de configuration de DHCP.
 - **Compliant :** l'ordinateur d'extrémité est conforme. Le modèle d'accès DHCP - Full Access autorise l'accès au réseau lorsque l'ordinateur d'extrémité est conforme.
 - **Partially Compliant :** l'ordinateur d'extrémité est partiellement conforme. Le modèle d'accès DHCP - Full Access autorise l'accès au réseau lorsque l'ordinateur d'extrémité est conforme.
 - **Non-Compliant :** l'ordinateur d'extrémité n'est pas conforme. Le modèle d'accès DHCP - Remediation Access refuse l'accès au réseau sauf aux serveurs de correction que vous avez définis lors de l'exécution de l'assistant de configuration de DHCP.
6. Si nécessaire, utilisez les flèches pour classer par ordre de priorité les modèles d'accès DHCP Enforcer.
Si plusieurs modèles s'appliquent à un état particulier, le premier modèle correspondant à l'état est utilisé. Nous vous recommandons d'attribuer d'abord les modèles d'accès les plus spécifiques/stricts et ensuite les modèles d'accès les moins spécifiques/stricts.
 7. Cliquez sur **Save**.

5 Annexe : utilisation de l'utilitaire de configuration de DHCP Enforcer

Si vous devez modifier les paramètres de DHCP Enforcer qui ont été définis lors de l'installation de DHCP Enforcer, utilisez l'outil de configuration DHCP Enforcer Configuration Utility. Cet outil est installé sur le serveur DHCP lors de l'installation de DHCP Enforcer. Si vous avez plusieurs serveurs DHCP, vous devez modifier les paramètres de DHCP Enforcer sur chaque serveur DHCP.

5.1 Mise à jour de la clé partagée

Procédure

La clé partagée doit correspondre à ce que vous avez saisi lors de l'installation de DHCP Enforcer sur le serveur. La clé partagée sert à sécuriser le trafic entre le serveur NAC et le serveur DHCP.

1. Dans le menu Démarrer du serveur DHCP, sélectionnez **Sophos > NAC > Support Tools > DHCP Enforcer Configuration Utility**.

La boîte de dialogue **DHCP Enforcer Configuration Utility** apparaît avec l'onglet **Enforcer** sélectionné.

2. Dans la boîte de dialogue **DHCP Enforcer Configuration Utility**, cliquez sur le bouton **Édit**.
3. Dans la boîte de dialogue **DHCP Enforcer RADIUS Enforcer Server Settings**, saisissez et confirmez la nouvelle clé partagée et cliquez sur **OK**.

5.2 Mise à jour des paramètres avancés

Cette section vous décrit comment mettre à jour les paramètres avancés de DHCP Enforcer à l'aide de l'outil DHCP Enforcer Configuration Utility. Dans la majorité des cas, ces paramètres ne devraient pas nécessiter de mise à jour.

Procédure

1. Dans le menu Démarrer du serveur DHCP, sélectionnez **Sophos > NAC > Support Tools > DHCP Enforcer Configuration Utility**.

La boîte de dialogue **DHCP Enforcer Configuration Utility** apparaît avec l'onglet **Enforcer** sélectionné.

2. Dans la boîte de dialogue **DHCP Enforcer Configuration Utility**, cliquez sur l'icône **Advanced**.
3. Si nécessaire, modifiez les paramètres DHCP Enforcer.
4. Cliquez sur **OK**.

Répétez ces instructions sur tous les serveurs DHCP auxquelles elles s'appliquent.

5.2.1 Champs et descriptions de l'outil DHCP Configuration Utility

Champs	Descriptions
Onglet Enforcer	
Access for Multiple Servers	Ce bouton d'option ne s'applique pas à Sophos Endpoint Security and Control.
Boîte de dialogue DHCP Enforcer RADIUS Enforcer Server Settings Cliquez sur l'icône Edit pour accéder à cette boîte de dialogue. Remarque : les champs présents dans cette fenêtre sont en rapport avec le serveur NAC.	
Enable	Indique si le serveur NAC est activé. Lorsqu'il est activé, le serveur NAC est utilisé pour les activités de conformité à la stratégie et d'édition de rapports.
IP Address	Désigne l'adresse IP du serveur NAC.
Authentication Port	Désigne le port d'authentification du serveur NAC.
Accounting Port	Désigne le port de gestion de compte du serveur NAC.
Shared Key	Identifie la clé partagée du serveur DHCP. La clé partagée est la même que celle utilisée lors de l'installation de DHCP Enforcer.
Confirm Shared Key	Confirme la clé partagée du serveur DHCP.
Boîte de dialogue DHCP Enforcer Resolve IP	
Hostname	Identifie le nom d'hôte, si l'adresse IP n'est pas connue, du serveur NAC. Lorsque vous saisissez le nom d'hôte, vous pouvez résoudre le nom d'hôte en adresse IP.
Onglet Advanced	
Enable Policy Compliance	Lorsque ce champ est sélectionné, les activités de conformité à la stratégie et d'édition de rapports sont activées pour tous les paquets de requêtes DHCP, sauf pour ceux qui sont identifiés par le code d'option réservée.
Attempts	Indique la fréquence d'exécution de la conformité à la stratégie pour un paquet de requêtes DHCP.
Timeout	Indique, en secondes, combien de temps le serveur DHCP attend avant de lancer une nouvelle vérification de conformité à la stratégie.
Default User Class	Identifie la classe d'utilisateur à utiliser s'il est impossible d'obtenir la classe d'utilisateur définie dans la stratégie en raison d'une erreur au cours d'une évaluation de la conformité à la stratégie.

Champs	Descriptions
Error	Lorsque cette option est sélectionnée, elle enregistre les messages d'erreur Microsoft dans le journal des événements de l'application (Application Event Log).
Warning	Lorsque cette option est sélectionnée, elle enregistre les messages d'avertissement Microsoft dans le journal des événements de l'application (Application Event Log).
Information	Lorsque cette option est sélectionnée, elle enregistre les messages d'information Microsoft dans le journal des événements de l'application (Application Event Log).
Trace	Lorsque cette option est sélectionnée, la journalisation du suivi Microsoft est activée et enregistrée dans le journal des événements de l'application (Application Event Log).
Subnet Mask Override	Spécifie le masque de sous-réseau disponible aux utilisateurs non conformes à la stratégie et annule le sous-réseau du serveur DHCP pour restreindre l'accès au réseau.
Black Hole IP Address	Adresse IP factice utilisée par DHCP Enforcer pour éliminer/exclure le trafic des ressources bloquées.
Boîte de dialogue DHCP Enforcer Informs IP Address	
IP Address	Indique l'adresse IP associée au client, comme un concentrateur d'accès à distance (RAC : remote access concentrator) pour lequel vous souhaitez contourner les activités de vérification de la conformité et d'édition de rapports pour les paquets d'informations DHCP. Par défaut, les activités de vérification de la conformité et d'édition de rapports sont effectuées pour les paquets d'informations DHCP. Lorsqu'une adresse IP est spécifiée, la vérification de la conformité et l'édition de rapports ne sont pas effectuées pour les paquets d'informations DHCP depuis ce client.
Boîte de dialogue DHCP Enforcer Resolve IP	
Hostname	Identifie le nom d'hôte, lorsque l'adresse IP n'est pas connue, du client pour lequel vous souhaitez contourner la vérification de la conformité et l'édition de rapports. Lorsque vous saisissez le nom d'hôte, vous pouvez résoudre le nom d'hôte en adresse IP.

6 Support technique

Le support technique pour les produits Sophos est disponible de l'une des manières suivantes :

- Rendez-vous sur le forum de la communauté SophosTalk en anglais sur <http://community.sophos.com/> et recherchez d'autres utilisateurs rencontrant le même problème que le vôtre.
- Rendez-vous sur la base de connaissances du support de Sophos sur <http://www.sophos.fr/support/>.
- Téléchargez la documentation des produits sur <http://www.sophos.fr/support/docs/>.
- Envoyez un courriel à support@sophos.fr, y compris le ou les numéros de version du logiciel Sophos, le ou les systèmes d'exploitation et le ou les niveaux de correctif ainsi que le texte du ou des messages d'erreur.

7 Mentions légales

Copyright © 2011 Sophos Limited. Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre sauf si vous possédez une licence valide, auquel cas vous pouvez reproduire la documentation conformément aux termes de cette licence ou si vous avez le consentement préalable écrit du propriétaire du copyright.

Sophos et Sophos Anti-Virus sont des marques déposées de Sophos Limited. Tous les autres noms de produits et de sociétés mentionnés sont des marques ou des marques déposées appartenant à leurs propriétaires respectifs.