

SOPHOS

simple + secure

Sophos NAC Advanced Guide d'installation

Version du produit : 3.2

Date du document : septembre 2011



Table des matières

1	À propos de ce document.....	3
2	Configuration requise.....	5
3	Liste de contrôle de l'installation.....	6
4	Liste de contrôles postérieurs à l'installation.....	7
5	Installation pour serveur autonome.....	14
6	Installation pour plusieurs serveurs.....	16
7	Mises à niveau du logiciel.....	20
8	Désinstallation du logiciel.....	24
9	Configuration requise suite à l'installation.....	25
10	Installation de l'agent temporaire.....	53
11	Désinstallation de l'agent temporaire du serveur Web.....	55
12	Déploiement de l'agent.....	56
13	Désinstallation de l'agent.....	58
14	Paramètres optionnels.....	59
15	Support technique.....	63
16	Mentions légales.....	64

1 À propos de ce document

Ce document vous aide à installer et à configurer Sophos NAC Advanced. Ce document contient les informations suivantes :

- Configuration requise
- Listes de contrôle de l'installation et des tâches postérieures à l'installation
- Installation du logiciel
- Désinstallation du logiciel
- Configuration requise suite à l'installation
- Configuration requise de l'agent temporaire
- Installation de l'agent temporaire
- Désinstallation de l'agent temporaire
- Configuration requise de l'agent
- Déploiement de l'agent
- Désinstallation de l'agent
- Paramètres optionnels (installations multi-serveurs uniquement)

1.1 À qui s'adresse ce document ?

Ce document s'adresse aux généralistes en informatique travaillant au sein de petites et moyennes entreprises. Ce document peut également intéresser les spécialistes de l'informatique travaillant au sein d'entreprises disposant de plus de 25 000 ordinateurs d'extrémité. Si vous avez plus de 1000 ordinateurs d'extrémité, nous vous recommandons d'utiliser les Sophos Professional Services. Nos consultants Professional Services travaillent en collaboration avec votre équipe de sécurité informatique pour mettre au point et mettre en place un plan de déploiement de vos logiciels.

1.2 Documentation

La documentation de Sophos NAC Advanced s'installe avec Sophos NAC Advanced et elle est disponible sous le menu **Démarrer > Sophos > Compliance Manager**. Installez Adobe® Acrobat® Reader pour pouvoir accéder et utiliser la documentation.

1.3 Nom et mot de passe du compte Compliance Manager

Pour accéder au Compliance Manager, utilisez un nom et un mot de passe de compte.

Utilisez le nom et le mot de passe de compte suivants pour accéder au Compliance Manager pour la première fois :

- **Nom du compte** = admin
- **Mot de passe** = un mot de passe de votre choix

Conservez une trace de ce mot de passe car il est le seul moyen dont vous disposez pour accéder au Compliance Manager tant que vous n'avez pas créé d'autres comptes utilisateurs. Pour plus d'informations, reportez-vous à la section [Accès au Compliance Manager](#) à la page 28.

2 Configuration requise

L'assistant d'installation de Sophos NAC Advanced vous guide tout au long de l'installation de la configuration système requise de Sophos NAC Advanced. Certains éléments requis pour la configuration du système doivent être installés depuis un CD-ROM système d'exploitation. Vous devez avoir à disposition le CD-ROM système d'exploitation approprié.

Les éléments suivants doivent être installés depuis un CD-ROM système d'exploitation s'ils ne sont pas déjà installés sur le(s) serveur(s) :

- Service d'authentification Internet (IAS) (Windows Server 2003) ou serveur NPS (Network Policy Server) (Windows Server 2008)
- Microsoft Messaging Queue (MSMQ)
- Gestionnaire des services Internet (IIS) version 6.0 ou supérieure
- ASP.NET

Configuration requise pour le contrôleur de domaine

Créez manuellement un compte de domaine standard sur le contrôleur de domaine, puis précisez que le mot de passe n'expire jamais et que l'utilisateur ne peut pas changer le mot de passe. Pour terminer cette tâche, vous devez impérativement disposer d'un compte d'administrateur de domaine sur le contrôleur de domaine. L'installation de Sophos NAC Advanced ajoute ce compte de service au groupe d'administrateurs locaux sur l'agent de conformité afin que Sophos NAC Advanced puisse accéder aux bases de données du serveur SQL. Ce compte de service doit impérativement disposer d'un accès en **lecture** à l'attribut **Membre de** des utilisateurs.

Configuration requise du certificat Web

L'interface des stratégies, l'interface d'édition de rapports et l'interface d'enregistrement sont des services Web qui nécessitent l'utilisation du certificat HTTPS pour pouvoir communiquer avec l'agent de conformité installé sur chaque ordinateur d'extrémité. Pour que Sophos NAC Advanced fonctionne correctement, installez un certificat Web pour ces composants sur le serveur d'applications de conformité. Ces composants peuvent partager un certificat Web. Si vous générez votre propre certificat Web, assurez-vous que tous les ordinateurs d'extrémité acceptent ce certificat Web généré comme valide. Si vous testez ou évaluez Sophos NAC Advanced et que HTTPS n'est pas activé, le certificat Web n'est pas nécessaire.

Remarque : si vous avez plusieurs serveurs d'applications de conformité et prévoyez d'utiliser un logiciel d'équilibrage de charge, le certificat Web doit correspondre à l'URL "pool de serveurs" qui sera également configurée sur tous les agents.

Pour voir la configuration requise, allez sur la page des différentes configurations requises sur le site Web de Sophos (<http://www.sophos.fr/products/all-sysreqs.html>).

3 Liste de contrôle de l'installation

Utilisez cette liste de contrôle de l'installation pour vérifier que vous avez effectué toutes les tâches nécessaires à l'installation de Sophos NAC Advanced.

Tâche	Description	Terminée
1.	Recherchez vos CD-ROM du système d'exploitation Windows Server. L'assistant d'installation de Sophos NAC Advanced vous guide tout au long de l'installation de la configuration système requise. Lors de l'installation, il se peut qu'il vous soit demandé d'installer la configuration requise depuis un CD-ROM du système d'exploitation.	
2.	Créez un compte de service Sophos NAC Advanced sur le contrôleur de domaine.	
3.	Installez un certificat Web sur le serveur d'applications de conformité de Sophos. Sophos utilise HTTPS pour protéger les noms utilisateur, mots de passe et toutes autres données sensibles dans un environnement de production. Vous pouvez désactiver HTTPS à des fins de tests ou d'évaluations. Pour plus d'informations, reportez-vous à la section Désactivation de HTTPS pour tests en environnements hors production à la page 61. Si vous testez ou évaluez Sophos NAC Advanced et que HTTPS n'est pas activé, le certificat Web n'est pas nécessaire.	
4.	Installez le serveur de base de données de conformité de Sophos. Pour des petites mises en place et évaluations, installez Sophos NAC Advanced sur un serveur autonome.	
5.	Installez le serveur d'applications de conformité de Sophos. Les mises en place de grande ampleur peuvent nécessiter l'utilisation de serveurs d'applications de conformité de Sophos supplémentaires.	
6.	Installez RADIUS Enforcer sur les serveurs appropriés. (Tâche facultative) RADIUS Enforcer s'installe automatiquement dans le cadre de l'installation du serveur d'applications de conformité. Vous avez aussi la possibilité d'installer RADIUS Enforcer séparément sur des serveurs supplémentaires.	

4 Liste de contrôles postérieurs à l'installation

Une fois l'installation terminée, configurez Sophos NAC Advanced. Utilisez cette liste de contrôles postérieurs à l'installation pour vérifier que vous avez effectué toutes les tâches nécessaires à la configuration de Sophos NAC Advanced. La configuration DHCP de Sophos NAC Advanced est facultative et dépend de votre choix à utiliser l'application du DHCP.

Liste de contrôles postérieurs à l'installation en cas d'utilisation de Windows Server 2003

Tâche	Description	Terminée
Configuration de Sophos NAC Advanced		
1.	Démarrez le SQL Server Agent et vérifiez/modifiez les paramètres par défaut d'édition de rapports. Pour plus d'informations, reportez-vous à la section Démarrage de l'agent SQL Server et vérification/modification des paramètres par défaut d'édition de rapports à la page 25.	
2.	Définissez la taille des bases de données de conformité et des journaux des transactions. Pour plus d'informations, reportez-vous à la section Taille des bases de données et des journaux des transactions du serveur SQL à la page 26.	
3.	Configurez une banque d'utilisateurs externe pour accéder au Compliance Manager. (Tâche facultative) Pour plus d'informations, reportez-vous à la section Configuration d'une banque d'utilisateurs externe pour accéder au Compliance Manager (Tâche facultative) à la page 29.	
4.	Accédez au Sophos Compliance Manager. Remarque : à l'aide du Compliance Manager, créez ou utilisez les modèles d'accès, les profils, les stratégies et les groupes préconfigurés. Pour plus d'informations, reportez-vous à la section Accès au Compliance Manager à la page 28.	
5.	Installez l'agent temporaire sur un serveur Web. Remarque : ce serveur peut être le même serveur sur lequel vous avez installé le Sophos Compliance Manager. Pour plus d'informations, reportez-vous à la section Installation de l'agent temporaire sur un serveur Web à la page 53.	
Paramètres du Service d'authentification Internet (IAS) (Windows Server 2003)		
6.	Attribuez au Service d'authentification Internet l'accès à Active Directory. Remarque : pour les mises en place LDAP ou si vous utilisez Sophos NAC Advanced en tant que proxy RADIUS (pour une configuration de Sophos	

Tâche	Description	Terminée
	<p>NAC Advanced en mode proxy devant un autre serveur RADIUS), vous n'avez pas besoin d'effectuer cette tâche.</p> <p>Pour plus d'informations, reportez-vous à la section Accès du Service d'authentification Internet à Active Directory à la page 31.</p>	
7.	<p>Configurez une stratégie d'accès à distance.</p> <p>Pour plus d'informations, reportez-vous à la section Configuration d'une Stratégie d'accès à distance à la page 32.</p>	
8.	<p>Désactivez la journalisation du Service d'authentification Internet pour assurer le succès des requêtes d'authentification. (Tâche facultative)</p> <p>Pour plus d'informations, reportez-vous à la section Désactivation de la journalisation du Service d'authentification Internet pour des demandes d'authentification réussies (tâche facultative) à la page 34.</p>	
9.	<p>Ajoutez les clients RADIUS pour chaque périphérique d'accès au réseau. (Tâche facultative)</p> <p>Remarque : effectuez cette tâche uniquement lorsque vous prévoyez de mettre en application RADIUS. L'application de RADIUS est utilisée avec VPN, 802.1x, Cisco NAC et avec les mises en place RADIUS étendues. Pour chaque concentrateur VPN, ajoutez une entrée client RADIUS au Service d'authentification Internet.</p> <p>Pour plus d'informations, reportez-vous à la section Ajout de clients RADIUS pour chaque périphérique d'accès au réseau (tâche facultative) à la page 34.</p>	
<p>Sophos NAC Advanced en tant que proxy RADIUS (Windows Server 2003) (tâches facultatives)</p> <p>Remarque : ces tâches sont uniquement requises lorsque vous configurez Sophos NAC Advanced en mode proxy devant un autre serveur RADIUS.</p>		
10.	<p>Ajoutez un groupe de serveur d'accès distant.</p> <p>Pour plus d'informations, reportez-vous à la section Ajout d'un groupe de serveurs RADIUS distant à la page 39.</p>	
11.	<p>Créez une stratégie de demande de connexion.</p> <p>Pour plus d'informations, reportez-vous à la section Création d'une Stratégie de demande de connexion à la page 40.</p>	
12.	<p>Vérifiez les conditions de la stratégie.</p> <p>Pour plus d'informations, reportez-vous à la section Vérification des conditions de la stratégie à la page 41.</p>	
13.	<p>Changez les ports d'authentification RADIUS.</p> <p>Pour plus d'informations, reportez-vous à la section Modification des ports d'authentification et de gestion RADIUS à la page 41.</p>	

Tâche	Description	Terminée
14.	<p>Changez le protocole d'authentification d'enregistrement dans l'interface d'enregistrement de Sophos NAC Advanced.</p> <p>Pour plus d'informations, reportez-vous à la section Modification du protocole d'authentification RADIUS dans l'interface d'enregistrement à la page 42.</p>	
15.	<p>Configurez le serveur RADIUS pour les réorientations/profils de groupes. (Tâche facultative)</p> <p>Pour plus d'informations, reportez-vous à la section Configuration du serveur RADIUS pour les réorientations/profils de groupes (tâche facultative) à la page 42.</p>	
<p>Mise en place de Microsoft LDAP (tâche facultative)</p> <p>Remarque : cette tâche est uniquement requise lorsque vous utilisez des répertoires LDAP existants avec RADIUS Enforcer.</p>		
16.	<p>Reportez-vous au <i>Guide de mise en place de LDAP de Sophos NAC Advanced</i> pour voir une liste de contrôle de toutes les tâches LDAP.</p>	
<p>Configuration de plusieurs serveurs d'applications de conformité Sophos</p> <p>Remarque : installez et configurez tous les serveurs d'applications de conformité afin qu'ils soient identiques au serveur d'applications de conformité principal. Pour les mises en place de LDAP, si vous voulez réutiliser un fichier de configuration sur plusieurs serveurs, exécutez l'outil de chiffrement de mots de passe sur chaque serveur pour mettre à jour et chiffrer le mot de passe bind. Pour plus d'informations, reportez-vous au <i>Guide des outils de Sophos NAC Advanced</i> .</p>		
17.	<p>Exportez la clé du serveur depuis le serveur d'applications de conformité principal et importez la clé du serveur vers les serveurs d'applications de conformité supplémentaires.</p> <p>Pour plus d'informations, reportez-vous à la section Exportation et importation de la clé du serveur sur des serveurs d'applications de conformité supplémentaires. à la page 51.</p>	
18.	<p>Configurez le Round Robin DNS sur Windows Server 2003. Effectuez cette tâche sur le serveur Windows exécutant le service de nom de domaine lorsque d'autres logiciels ou appliances d'équilibrage de charge ne sont pas utilisés.</p> <p>Pour plus d'informations, reportez-vous à la section Configuration du Round Robin DNS sur Windows Server 2003 et supérieur à la page 52.</p>	
<p>Mise en place du protocole DHCP (tâche facultative)</p>		
19.	<p>Reportez-vous au <i>Guide de mise en application de DHCP de Sophos NAC Advanced</i> pour voir une liste de contrôle de toutes les tâches LDAP.</p>	
<p>Déploiement du Sophos Compliance Agent</p>		

Tâche	Description	Terminée
20.	Déployez l'agent de conformité sur les ordinateurs d'extrémité. Pour plus d'informations, reportez-vous à la section Déploiement de l'agent à la page 56.	

Liste de contrôles postérieurs à l'installation en cas d'utilisation de Windows Server 2008

Tâche	Description	Terminée
Configuration de Sophos NAC Advanced		
1.	Démarrez le SQL Server Agent et vérifiez/modifiez les paramètres par défaut d'édition de rapports. Pour plus d'informations, reportez-vous à la section Démarrage de l'agent SQL Server et vérification/modification des paramètres par défaut d'édition de rapports à la page 25.	
2.	Définissez la taille des bases de données de conformité et des journaux des transactions. Pour plus d'informations, reportez-vous à la section Taille des bases de données et des journaux des transactions du serveur SQL à la page 26.	
3.	Configurez une banque d'utilisateurs externe pour accéder au Compliance Manager. (Tâche facultative) Pour plus d'informations, reportez-vous à la section Configuration d'une banque d'utilisateurs externe pour accéder au Compliance Manager (Tâche facultative) à la page 29.	
4.	Accédez au Sophos Compliance Manager. Remarque : à l'aide du Compliance Manager, créez ou utilisez les modèles d'accès, les profils, les stratégies et les groupes préconfigurés. Pour plus d'informations, reportez-vous à la section Accès au Compliance Manager à la page 28.	
5.	Installez l'agent temporaire sur un serveur Web. Remarque : ce serveur peut être le même serveur sur lequel vous avez installé le Sophos Compliance Manager. Pour plus d'informations, reportez-vous à la section Installation de l'agent temporaire sur un serveur Web à la page 53.	
Paramètres de la stratégie réseau (Windows Server 2008)		

Tâche	Description	Terminée
6.	<p>Attribuez au Serveur de stratégie réseau (NPS) l'accès à Active Directory.</p> <p>Remarque : pour les mises en place LDAP ou si vous utilisez Sophos NAC Advanced en tant que proxy RADIUS (pour une configuration de Sophos NAC Advanced en mode proxy devant un autre serveur RADIUS), vous n'avez pas besoin d'effectuer cette tâche.</p> <p>Pour plus d'informations, reportez-vous à la section Attribution au Serveur de stratégie réseau (NPS) de l'accès à Active Directory à la page 36.</p>	
7.	<p>Configurez une stratégie réseau.</p> <p>Pour plus d'informations, reportez-vous à la section Configuration d'une stratégie réseau à la page 36.</p>	
8.	<p>Désactivez la journalisation du Serveur de stratégie réseau pour que les demandes d'authentification s'effectuent avec succès. (Tâche facultative)</p> <p>Pour plus d'informations, reportez-vous à la section Désactivation de la journalisation du Serveur de stratégie réseau pour que les demandes d'authentification s'effectuent avec succès (tâche facultative) à la page 38.</p>	
9.	<p>Ajoutez les clients RADIUS pour chaque périphérique d'accès au réseau. (Tâche facultative)</p> <p>Remarque : effectuez cette tâche uniquement lorsque vous prévoyez de mettre en application RADIUS. L'application de RADIUS est utilisée avec VPN, 802.1x, Cisco NAC et avec les mises en place RADIUS étendues. Pour chaque concentrateur VPN, ajoutez une entrée client RADIUS au Serveur de stratégie réseau.</p> <p>Pour plus d'informations, reportez-vous à la section Ajout de clients RADIUS pour chaque périphérique d'accès au réseau (tâche facultative) à la page 38.</p>	
<p>Sophos NAC Advanced en tant que proxy RADIUS (Windows Server 2008) (tâches facultatives)</p> <p>Remarque : ces tâches sont uniquement requises lorsque vous configurez Sophos NAC Advanced en mode proxy devant un autre serveur RADIUS.</p>		
10.	<p>Ajoutez un groupe de serveur d'accès distant.</p> <p>Pour plus d'informations, reportez-vous à la section Ajout d'un groupe de serveurs RADIUS distant à la page 45.</p>	
11.	<p>Créez une stratégie de demande de connexion.</p> <p>Pour plus d'informations, reportez-vous à la section Création d'une Stratégie de demande de connexion à la page 46.</p>	
12.	<p>Vérifiez les conditions de la stratégie.</p> <p>Pour plus d'informations, reportez-vous à la section Vérification des conditions de la stratégie à la page 47.</p>	

Tâche	Description	Terminée
13.	<p>Changez le protocole d'authentification d'enregistrement dans l'interface d'enregistrement de Sophos NAC Advanced.</p> <p>Pour plus d'informations, reportez-vous à la section Modification du protocole d'authentification RADIUS dans l'interface d'enregistrement à la page 47.</p>	
14.	<p>Configurez le serveur RADIUS pour les réorientations/profils de groupes. (Tâche facultative)</p> <p>Pour plus d'informations, reportez-vous à la section Configuration du serveur RADIUS pour les réorientations/profils de groupes (tâche facultative) à la page 48.</p>	
<p>Mise en place de Microsoft LDAP (tâche facultative)</p> <p>Remarque : cette tâche est uniquement requise lorsque vous utilisez des répertoires LDAP existants avec RADIUS Enforcer.</p>		
15.	Reportez-vous au <i>Guide de mise en place de LDAP de Sophos NAC Advanced</i> pour voir une liste de contrôle de toutes les tâches LDAP.	
<p>Configuration de plusieurs serveurs d'applications de conformité Sophos</p> <p>Remarque : installez et configurez tous les serveurs d'applications de conformité afin qu'ils soient identiques au serveur d'applications de conformité principal. Pour les mises en place de LDAP, si vous voulez réutiliser un fichier de configuration sur plusieurs serveurs, exécutez l'outil de chiffrement de mots de passe sur chaque serveur pour mettre à jour et chiffrer le mot de passe bind. Pour plus d'informations, reportez-vous au <i>Guide des outils de Sophos NAC Advanced</i>.</p>		
16.	<p>Exportez la clé du serveur depuis le serveur d'applications de conformité principal et importez la clé du serveur vers les serveurs d'applications de conformité supplémentaires.</p> <p>Pour plus d'informations, reportez-vous à la section Exportation et importation de la clé du serveur sur des serveurs d'applications de conformité supplémentaires, à la page 51.</p>	
17.	<p>Configurez le Round Robin DNS sur Windows Server 2003. Effectuez cette tâche sur le serveur Windows exécutant le service de nom de domaine lorsque d'autres logiciels ou appliances d'équilibrage de charge ne sont pas utilisés.</p> <p>Pour plus d'informations, reportez-vous à la section Configuration du Round Robin DNS sur Windows Server 2003 et supérieur à la page 52.</p>	
<p>Mise en place du protocole DHCP (tâche facultative)</p>		
18.	Reportez-vous au <i>Guide de mise en application de DHCP de Sophos NAC Advanced</i> pour voir une liste de contrôle de toutes les tâches LDAP.	
<p>Déploiement du Sophos Compliance Agent</p>		

Tâche	Description	Terminée
19.	Déployez l'agent de conformité sur les ordinateurs d'extrémité. Pour plus d'informations, reportez-vous à la section Déploiement de l'agent à la page 56.	

5 Installation pour serveur autonome

Lors de l'installation de Sophos NAC Advanced sur un serveur autonome, les bases de données de conformité Sophos sont installées en premier suivies par le serveur d'applications de conformité.

L'installation de Sophos NAC Advanced nécessite l'utilisation d'un compte de domaine avec les droits d'administrateur local. Le compte qui installe NAC doit être défini en tant qu'utilisateur de SQL Server ou doit faire partie d'un groupe défini en tant qu'utilisateur de SQL Server. De même, l'utilisateur du SQL Server doit être affecté au rôle de serveur sysadmin dans SQL.

1. Sur le contrôleur de domaine, créez manuellement un compte de domaine standard et précisez que le mot de passe n'expire jamais et que l'utilisateur ne peut pas changer le mot de passe.

L'installation ajoute ce compte de service au groupe d'administrateurs locaux sur le serveur de conformité afin que le serveur de conformité de Sophos puisse accéder aux bases de données du serveur SQL. Ce compte de service doit impérativement disposer d'un accès en **lecture** de l'attribut **Membre de** des utilisateurs.

2. Téléchargez Sophos NAC Advanced depuis le site Web de Sophos.
3. Cliquez deux fois sur le fichier d'installation pour lancer l'installation.

Nous vous conseillons d'activer le suivi de la journalisation lors de l'installation de Sophos NAC Advanced. À partir d'une invite de commandes, saisissez le nom du fichier d'installation de Sophos NAC Advanced suivi d'une espace puis de /trace (par exemple, nac_xx_sfx.exe /trace). Lorsque le message d'installation apparaît, cliquez sur **OK** pour confirmer l'installation. Le journal d'installation de l'agent se trouve dans le dossier %temp%.

4. Cliquez sur **Next** pour continuer.
5. Lisez le Contrat de licence Utilisateur Final, sélectionnez le bouton **I Accept the terms of the License Agreement**, et cliquez sur **Next** pour continuer.
6. Sélectionnez le bouton **Sophos Compliance Application Server, Compliance Databases, and RADIUS Enforcer**. Cliquez sur **Next** pour continuer.
7. Saisissez les informations du compte de service dans les champs appropriés. Cliquez sur **Next** pour continuer.

Il s'agit du compte de domaine standard requis par les serveurs SQL et par le serveur d'applications de conformité. Ce compte de service a été créé à l'étape 1.

8. Si nécessaire, précisez les paramètres du proxy Internet de ce serveur en sélectionnant la case **Use Proxy**. Cliquez sur **Next** pour continuer.

L'adresse et le port du serveur proxy sont des champs obligatoires. Le nom utilisateur, le mot de passe et le mot de passe de confirmation sont nécessaires seulement lors de l'utilisation d'un proxy authentifié.

9. Saisissez vos Détails du compte de téléchargement Sophos dans les champs appropriés. Cliquez sur **Next** pour continuer.

Les détails du compte de téléchargement Sophos vous sont fournis à l'achat de Sophos NAC Advanced. Le nom utilisateur et le mot de passe sont requis pour mettre à jour les correctifs et récupérer les dernières mises à jour des signatures virales à destination des applications antivirus et antispywares. Si vous saisissez le nom d'utilisateur ou le mot de passe de manière incorrecte lors de l'installation, vous pouvez les corriger à l'aide du Compliance Manager. Pour plus d'informations, reportez-vous à l'Aide de Compliance Manager.

10. Si nécessaire, modifiez le répertoire des composants NAC IIS du Compliance Manager. Cliquez sur **Next** pour continuer.

11. Cliquez sur **Install** pour commencer l'installation.

Le serveur d'applications de conformité de Sophos et le Compliance Manager sont configurés et une barre de progression de l'installation apparaît. Une partie de l'installation peut durer plusieurs minutes au cours desquelles il se peut que l'indicateur de progression ne bouge pas. N'annulez pas l'installation et celle-ci continuera à progresser.

12. Cliquez sur **Finish**.

Remarque :

- En cas d'erreurs lors de l'installation, consultez le journal des événements pour obtenir plus d'informations. En cas d'échec de l'installation de la base de données, supprimez les bases de données suivantes si elles ont été créées : AlertStore, AuditStore, GeneralStore, PolicyStore, ReportStore, ReportStoreCache, ReportStoreWH et SecurityStore. Dès que vous avez supprimé les bases de données, essayez de relancer l'installation.
- Une fois l'installation terminée, vous devez terminer les tâches de configuration postérieures à l'installation. Pour plus d'informations, reportez-vous à la section [Configuration requise suite à l'installation](#) à la page 25.

6 Installation pour plusieurs serveurs

Pour de plus grandes installations, Sophos vous demande d'installer les bases de données du serveur SQL et l'application sur des serveurs séparés. Installez impérativement les bases de données du serveur SQL avant d'installer l'application.

6.1 Installation des bases de données

Lorsque vous installez les bases de données du serveur SQL et l'application sur des serveurs séparés, ceux-ci doivent être connectés au même domaine. De plus, vous devez utiliser un compte avec les droits d'administrateur local pour procéder à l'installation des bases de données du serveur SQL. Le compte qui installe NAC doit être défini en tant qu'utilisateur de SQL Server ou doit faire partie d'un groupe défini en tant qu'utilisateur de SQL Server. De même, l'utilisateur du SQL Server doit être affecté au rôle de serveur sysadmin dans SQL.

1. Sur le contrôleur de domaine, créez manuellement un compte de domaine standard et précisez que le mot de passe n'expire jamais et que l'utilisateur ne peut pas changer le mot de passe.

L'installation ajoute ce compte de service au groupe d'administrateurs locaux sur le serveur d'applications de conformité afin que le serveur d'applications de conformité de Sophos puisse accéder aux bases de données du serveur SQL. Ce compte de service doit impérativement disposer d'un accès en **lecture** de l'attribut **Membre de** des utilisateurs.

Remarque : cette étape n'est pas requise pour les mises à niveau de Sophos NAC Advanced.

2. Téléchargez Sophos NAC Advanced depuis le site Web de Sophos.
3. Cliquez deux fois sur le fichier d'installation pour lancer l'installation.
Nous vous conseillons d'activer le suivi de la journalisation lors de l'installation de Sophos NAC Advanced. À partir d'une invite de commandes, saisissez le nom du fichier d'installation de Sophos NAC Advanced suivi d'une espace puis de /trace (par exemple, nac_xx_sfx.exe /trace). Lorsque le message d'installation apparaît, cliquez sur **OK** pour confirmer l'installation. Le journal d'installation de l'agent se trouve dans le dossier %temp%.
4. Cliquez sur **Next** pour continuer.
5. Lisez le Contrat de licence Utilisateur Final, sélectionnez le bouton **I Accept the terms of the License Agreement**, et cliquez sur **Next** pour continuer.
6. Procédez de l'une des manières suivantes :
 - Si vous installez les bases de données de conformité Sophos sur Windows Server 2003, sélectionnez le bouton **Sophos Compliance Database Server Only**. Cliquez sur **Next** pour continuer.
 - Si vous installez les bases de données de conformité de Sophos sur Windows Server 2000 SP3 ou sur Windows Server 2003 64 bits, lorsque le programme d'installation détecte que vous pouvez uniquement installer les bases de données SQL, cliquez sur le bouton **OK**.

7. Saisissez les informations du compte de service dans les champs appropriés. Cliquez sur **Next** pour continuer.
Il s'agit du compte de domaine standard requis par les serveurs SQL et par le serveur d'applications de conformité. Ce compte de service a été créé à l'étape 1. Si vous exécutez une mise à niveau, utilisez les informations du même compte que celui utilisé dans l'installation originale.
8. Procédez de l'une des manières suivantes :
 - Si vous avez plus d'une instance de la base de données locale sur ce serveur, sélectionnez l'instance de la base de données appropriée. Cliquez sur **Next** pour continuer.
 - Si vous n'avez pas plus d'une instance de la base de données, passez à l'étape suivante.
9. Cliquez sur **Install** pour commencer l'installation.
Les bases de données de conformité de Sophos sont configurées et une barre de progression de l'installation apparaît. Une partie de l'installation peut durer plusieurs minutes au cours desquelles il se peut que l'indicateur de progression ne bouge pas. N'annulez pas l'installation et celle-ci continuera à progresser.
10. Cliquez sur **Finish**.
Important : en cas d'erreurs lors de l'installation, consultez le journal des événements pour obtenir plus d'informations. En cas d'échec de l'installation de la base de données, supprimez les bases de données suivantes si elles ont été créées : AlertStore, AuditStore, GeneralStore, PolicyStore, ReportStore, ReportStoreCache, ReportStoreWH et SecurityStore. Dès que vous avez supprimé les bases de données, essayez de relancer l'installation.

6.2 Installation de l'application

Lorsque vous installez les bases de données et l'application sur des serveurs séparés, ceux-ci doivent être connectés au même domaine. De plus, vous devez utiliser un compte avec les droits d'administrateur local pour procéder à l'installation de l'application.

Important : installez et configurez correctement tous les serveurs d'applications de conformité supplémentaires afin qu'ils soient identiques au serveur d'applications de conformité principal. Pour plus d'informations, reportez-vous à la section [Configuration de plusieurs serveurs d'applications \(tâches facultatives\)](#) à la page 51.

1. Téléchargez Sophos NAC Advanced depuis le site Web de Sophos.
2. Cliquez deux fois sur le fichier d'installation pour lancer l'installation.
Nous vous conseillons d'activer le suivi de la journalisation lors de l'installation de Sophos NAC Advanced. À partir d'une invite de commandes, saisissez le nom du fichier d'installation de Sophos NAC Advanced suivi d'une espace puis de /trace (par exemple, nac_xx_sfx.exe /trace). Lorsque le message d'installation apparaît, cliquez sur **OK** pour confirmer l'installation. Le journal d'installation de l'agent se trouve dans le dossier %temp%.
3. Cliquez sur **Next** pour continuer.
4. Lisez le Contrat de licence Utilisateur Final, sélectionnez le bouton **I Accept the terms of the License Agreement**, et cliquez sur **Next** pour continuer.

5. Sélectionnez le bouton **Sophos Compliance Application Server and RADIUS Enforcer**. Cliquez sur **Next** pour continuer.
6. Saisissez les informations du compte de service dans les champs appropriés. Cliquez sur **Next** pour continuer.
Il s'agit du compte de domaine standard requis par les serveurs SQL et par le serveur d'applications de conformité. Les informations de ce compte de service doivent correspondre aux informations du compte de service que vous avez saisies lorsque vous avez installé les bases de données de conformité de Sophos.
7. Si nécessaire, précisez les paramètres du proxy Internet de ce serveur en sélectionnant la case **Use Proxy**. Cliquez sur **Next** pour continuer.
L'adresse et le port du serveur proxy sont des champs obligatoires. Le nom utilisateur, le mot de passe et le mot de passe de confirmation sont nécessaires seulement lors de l'utilisation d'un proxy authentifié.
8. Saisissez le nom de la serveur de base de données de conformité de Sophos. Cliquez sur **Next** pour continuer.
Lorsque vous n'utilisez pas l'instance SQL par défaut, le serveur et le nom de l'instance doivent apparaître au format serveur\nominstance. L'installation procède à la vérification de la connexion entre le serveur que vous êtes en train d'installer et la serveur de base de données de conformité.
9. Saisissez vos Détails du compte de téléchargement Sophos dans les champs appropriés. Cliquez sur **Next** pour continuer.
Les détails du compte de téléchargement Sophos vous sont fournis à l'achat de Sophos NAC Advanced. Le nom utilisateur et le mot de passe sont requis pour mettre à jour les correctifs et récupérer les dernières mises à jour des signatures virales à destination des applications antivirus et antispywares. Si vous saisissez le nom d'utilisateur ou le mot de passe de manière incorrecte lors de l'installation, vous pouvez les corriger à l'aide du Compliance Manager. Pour plus d'informations, reportez-vous à l'Aide de Compliance Manager.
10. Si nécessaire, modifiez le répertoire des composants NAC IIS du Compliance Manager. Cliquez sur **Next** pour continuer.
11. Cliquez sur **Install** pour commencer l'installation.
Le serveur d'applications de conformité de Sophos est configuré et une barre de progression de l'installation apparaît. Une partie de l'installation peut durer plusieurs minutes au cours desquelles il se peut que l'indicateur de progression ne bouge pas. N'annulez pas l'installation et celle-ci continuera à progresser.
12. Cliquez sur **Finish**.

Remarque :

- En cas d'erreurs lors de l'installation, consultez le journal des événements pour obtenir plus d'informations.
- Une fois l'installation terminée, vous devez terminer les tâches de configuration postérieures à l'installation. Pour plus d'informations, reportez-vous à la section [Configuration requise suite à l'installation](#) à la page 25. Si vous exécutez une mise à niveau, revenez aux instructions de [Mises à niveau du logiciel](#) à la page 20 au lieu de terminer les opérations requises d'après installation.

6.3 Installation de RADIUS Enforcer

RADIUS Enforcer s'installe automatiquement dans le cadre de l'installation du serveur d'applications de conformité. Vous avez aussi la possibilité d'installer RADIUS Enforcer séparément sur des serveurs supplémentaires. Pour des raisons d'extensibilité, de configuration réseau, ou de spécifications réseau, il se peut que vous ayez à installer RADIUS Enforcer sur plusieurs serveurs. Pour de plus grandes installations, installez RADIUS Enforcer sur un autre serveur afin de séparer l'activité de mise en application et l'activité de l'agent sur le serveur d'applications de conformité.

Remarque: Sophos collabore directement avec chaque entreprise pour déterminer si RADIUS Enforcer doit être installé ou non sur des serveurs séparés.

1. Téléchargez Sophos NAC Advanced depuis le site Web de Sophos.

2. Cliquez deux fois sur le fichier d'installation pour lancer l'installation.

Nous vous conseillons d'activer le suivi de la journalisation lors de l'installation de Sophos NAC Advanced. À partir d'une invite de commandes, saisissez le nom du fichier d'installation de Sophos NAC Advanced suivi d'une espace puis de /trace (par exemple, `nac_xx_sfx.exe /trace`). Lorsque le message d'installation apparaît, cliquez sur **OK** pour confirmer l'installation. Le journal d'installation de l'agent se trouve dans le dossier %temp%.

3. Cliquez sur **Next** pour continuer.

4. Lisez le Contrat de licence Utilisateur Final, sélectionnez le bouton **I Accept the terms of the License Agreement**, et cliquez sur **Next** pour continuer.

5. Sélectionnez le bouton **Sophos RADIUS Enforcer Only**. Cliquez sur **Next** pour continuer.

6. Saisissez les informations du compte de service dans les champs appropriés. Cliquez sur **Next** pour continuer.

Il s'agit du compte de domaine standard requis par les serveurs SQL et par le serveur d'applications de conformité. Les informations de ce compte de service doivent correspondre aux informations du compte de service que vous avez saisies lorsque vous avez installé les bases de données de conformité de Sophos.

7. Saisissez le nom du serveur de base de données de conformité de Sophos. Cliquez sur **Next** pour continuer.

Lorsque vous n'utilisez pas l'instance SQL par défaut, le serveur et le nom de l'instance doivent apparaître au format `serveur\nominstance`. L'installation procède à la vérification de la connexion entre le serveur que vous êtes en train d'installer et le serveur de base de données de conformité.

8. Cliquez sur **Install** pour commencer l'installation.

RADIUS Enforcer est configuré et une barre de progression de l'installation apparaît.

9. Cliquez sur **Finish**.

Remarque: en cas d'erreurs lors de l'installation, consultez le journal des événements pour obtenir plus d'informations.

7 Mises à niveau du logiciel

Sophos NAC Advanced version 3.2.x peut être mise à niveau à partir de la version 3.0.x et 3.2 de Sophos NAC Advanced. Sophos NAC pour Endpoint Security and Control intégré dans Sophos Endpoint Security and Control ne peut pas être mis à niveau à Sophos NAC Advanced.

Important : pour mettre à niveau le logiciel, saisissez ou sélectionnez les informations dans la prochaine installation qui sont identiques à celles que vous avez saisies ou sélectionnées lors de l'installation originale.

1. Avant la mise à niveau, rendez-vous sur le Compliance Manager et configurez un agent de test qui utilise l'adresse IP d'un des serveurs d'applications de conformité.

Important : l'adresse IP du serveur d'applications de conformité qui est utilisée à cette étape doit correspondre à celle du premier serveur d'applications de conformité sur lequel vous effectuez la mise à niveau.

2. Faites une copie de sauvegarde de la clé du serveur d'applications de conformité et de toutes les bases de données.

Remarque : faites une copie de sauvegarde de ces bases de données : AlertStore, AuditStore, GeneralStore, PolicyStore, ReportStore, ReportStoreCache, ReportStoreWH et SecurityStore.

3. Mettez tous les serveurs d'applications de conformité en mode maintenance à l'aide de l'outil Mode de maintenance. Exécutez l'outil à partir d'une invite de commande sur chaque serveur d'applications de conformité.

- Si vous procédez à la mise à niveau à partir de la version 3.0.x, utilisez l'invite de commandes pour vous rendre dans le répertoire Program Files\Endforce\Support Tools et saisissez **MaintMode.exe /start**.

- Si vous procédez à la mise à niveau à partir de la version 3.2, utilisez l'invite de commandes pour vous rendre dans le répertoire Program Files\Sophos\NAC\Support Tools et saisissez **MaintMode.exe /start**.

Remarque : lorsque le logiciel est en mode maintenance, l'agent reconnaît le mode et fonctionne sans erreur, interruption ou indication du mode maintenance aux utilisateurs. L'agent enregistre toutes les informations d'évaluation et de rapport localement jusqu'à ce que le logiciel revienne en mode production. Pour plus d'informations, reportez-vous au *Guide des outils de Sophos NAC Advanced* .

4. Installez la mise à niveau des bases de données sur le serveur SQL en suivant les instructions de la section [Installation des bases de données](#) à la page 16.

Remarque : Sophos NAC Advanced dispose d'un fichier d'installation que vous devez exécuter sur le serveur de base de données de conformité et sur les serveurs d'applications de conformité. Lorsque vous exécutez le fichier d'installation, vous pouvez spécifier les options d'installation appropriées pour chaque serveur. Vous devez mettre à niveau les bases de données en premier. En cas d'erreurs lors de l'installation, consultez le journal des événements pour obtenir plus d'informations.

Remarque : les mises à niveau à partir de SQL Server 2000 sont prises en charge. Procédez d'abord à la mise à niveau de Sophos NAC Advanced et ensuite à la mise à niveau à une version prise en charge de SQL Server.

En cas d'échec de la mise à niveau des bases de données, supprimez les bases de données suivantes si elles ont été créées : AlertStore, AuditStore, GeneralStore, PolicyStore, ReportStore, ReportStoreCache, ReportStoreWH et SecurityStore. Une fois les bases de données supprimées, utilisez les copies de sauvegarde des bases de données NAC que vous avez effectuées auparavant. Vous pouvez ensuite tenter une nouvelle installation.

5. Sur le serveur SQL, procédez de la manière suivante :
 - a) Démarrez l'agent SQL Server s'il n'est pas déjà démarré. Pour plus d'informations, reportez-vous à la section [Démarrage de l'agent SQL Server et vérification/modification des paramètres par défaut d'édition de rapports](#) à la page 25.
 - b) Vérifiez/modifiez le temps d'exécution de la tâche Report Warehouse Loader. Ce paramètre planifie le moment auquel les données du rapport en cours sont déplacées vers les rapports archivés. Pour plus d'informations, reportez-vous à la section [Vérification/modification de la tâche Report Warehouse Loader](#) à la page 60.
 - c) Vérifiez/modifiez les paramètres par défaut des rapports. Pour plus d'informations, reportez-vous à la section [Démarrage de l'agent SQL Server et vérification/modification des paramètres par défaut d'édition de rapports](#) à la page 25.
6. Supprimez le serveur d'applications de conformité que vous prévoyez de mettre à niveau en premier dans le groupe d'équilibrage de charge.

Remarque : l'adresse IP de ce serveur doit correspondre à l'agent de test que vous avez configuré à l'étape 1. Cette étape est obligatoire uniquement si Sophos NAC Advanced est installé dans un environnement d'équilibrage de charge.

7. Installez la mise à niveau de l'application sur ce serveur d'applications de conformité en suivant les instructions de la section [Installation de l'application](#) à la page 17.

Remarque : en cas d'erreurs lors de l'installation, consultez le journal des événements pour obtenir plus d'informations.
8. Remettez le serveur d'applications de conformité en mode production à l'aide de l'outil mode de maintenance. À partir de l'invite de commandes, rendez-vous dans le répertoire Program Files\Sophos\NAC\Support Tools et saisissez **MaintMode.exe /stop**.
9. Assurez-vous que l'agent de test que vous avez configuré peut effectuer avec succès les opérations d'enregistrement, de récupération, de vérification, d'application, d'actualisation et d'édition de rapports.

10. Remettez le serveur d'applications de conformité en mode de maintenance à l'aide de l'outil mode de maintenance. À partir de l'invite de commandes, rendez-vous dans le répertoire Program Files\Sophos\NAC\Support Tools et saisissez **MaintMode.exe /start**.

11. Ajoutez de nouveau le serveur d'applications de conformité dans le groupe d'équilibrage de charge.

Remarque : cette étape est obligatoire uniquement si Sophos NAC Advanced est installé dans un environnement d'équilibrage de charge.

12. Installez la mise à niveau de l'application sur tous les serveurs d'applications de conformité supplémentaires en suivant les instructions de la section [Installation de l'application](#) à la page 17 .

13. Sur tous les serveurs d'applications de conformité, procédez de la manière suivante :

- Vérifiez/modifiez le temps d'exécution de la tâche Patch Loader sur tous les serveurs d'applications de conformité. Pour plus d'informations, reportez-vous à la section [Vérification/modification de la tâche Patch Loader](#) à la page 59.
- Pour tester le logiciel en environnements hors production, désactivez HTTPS. Pour plus d'informations, reportez-vous à la section [Désactivation de HTTPS pour tests en environnements hors production](#) à la page 61.

14. Remettez tous les serveurs d'applications de conformité en mode production à l'aide de l'outil mode de maintenance. À partir de l'invite de commandes de chaque serveur d'applications de conformité, rendez-vous dans le répertoire Program Files\Sophos\NAC\Support Tools et saisissez **MaintMode.exe /stop**.

15. Installez la mise à niveau de l'agent sur un ordinateur d'extrémité de test et assurez-vous qu'il peut effectuer les opérations d'enregistrement, de récupération, de vérification, d'application, d'actualisation et d'édition de rapports.

16. Installez la mise à niveau de l'agent sur les ordinateurs d'extrémité appropriés.

17. Installez l'agent temporaire sur le serveur web approprié à l'aide des instructions de la section [Installation de l'agent temporaire sur un serveur Web](#) à la page 53.

Remarque : l'agent temporaire remplace désormais l'agent Web. L'installation de l'agent temporaire désinstalle l'agent Web et installe l'agent temporaire.

Remarque : les restrictions d'accès aux répertoires utilisés par Sophos NAC Advanced sont supprimées lors de la mise à niveau de votre logiciel. Appliquez de nouveau les restrictions d'accès une fois la mise à niveau terminée.

La mise à niveau de Sophos NAC Advanced à partir de la version 3.0.x :

- Configure les nouvelles fonctions de la version publiée. Pour bénéficier des nouvelles fonctionnalités des stratégies, vous devez mettre à jour les stratégies existantes.
- Met à jour le Compliance Manager avec les profils, applications, fonctions et actions prédéfinis. La mise à niveau procède aussi à la suppression des profils, applications, fonctions et actions qui ne sont plus prises en charge. Ces modifications peuvent affecter certaines des stratégies que vous avez créées.
- Convertit les modèles de déploiement de l'agent en modèles de configuration de l'agent. Les modèles de configuration de l'agent contiennent les paramètres de l'agent qui sont identiques aux paramètres que contenaient les modèles de déploiement de l'agent. Les

modèles de configuration de l'agent vous permettent de mettre à jour les paramètres de l'agent par le biais des stratégies.

- Ne prend plus en charge Windows 98, par conséquent, toutes les références à Windows 98 sont supprimées. Seules les données de rapports de Windows 98 sont conservées.
- Met à jour les noms de la Vue SQL. Les Vues SQL sont désormais préfacées avec NACVP plutôt que EFVP. Les demandes SQL utilisant EFVP doivent être mises à jour.

Remarque : si vous procédez à la mise à niveau de la version 3.2 à la version 3.2.x, ces modifications ne sont pas applicables car elles ont été effectuées lors de la mise à niveau à la version 3.2.

8 Désinstallation du logiciel

Lorsque vous désinstallez Sophos NAC Advanced, désinstallez d'abord l'application, puis les bases de données. Autrement l'application va générer des erreurs parce que les bases de données ont été désinstallées.

8.1 Désinstallation de l'application

La désinstallation de l'application ne supprime pas tous les éléments que vous avez créés dans le Compliance Manager. Tous les éléments, par exemple les stratégies et les informations de compte utilisateur, sont archivées dans les bases de données de conformité.

1. Depuis le menu Démarrer, cliquez sur **Panneau de configuration > Ajouter ou supprimer des programmes**.
2. Sélectionnez **Sophos Compliance Application Server** et cliquez sur **Supprimer**.
3. Cliquez sur **Oui** pour confirmer la suppression du serveur d'applications de conformité. L'application est supprimée.

8.2 Désinstallation de la base de données

La désinstallation des bases de données supprime uniquement les fichiers utilisés pour créer les bases de données et pas les bases de données elles-mêmes.

1. Depuis le menu Démarrer, cliquez sur **Panneau de configuration > Ajouter ou supprimer des programmes**.
2. Sélectionnez **Sophos Compliance Database Server** et cliquez sur **Supprimer**.
3. Cliquez sur **Oui** pour confirmer la suppression des fichiers serveur utilisés pour créer les bases de données. Les fichiers serveur sont supprimés et les bases de données demeurent intactes.

8.3 Désinstallation de RADIUS Enforcer

La désinstallation de RADIUS Enforcer est uniquement requise lorsque vous avez installé RADIUS Enforcer sur un serveur séparé depuis l'application Sophos NAC Advanced.

1. Depuis le menu Démarrer, cliquez sur **Panneau de configuration > Ajouter ou supprimer des programmes**.
2. Sélectionnez **Sophos RADIUS Enforcer** et cliquez sur **Supprimer**.
3. Cliquez sur **Oui** pour confirmer la suppression de RADIUS Enforcer. RADIUS Enforcer a été supprimé.

9 Configuration requise suite à l'installation

La configuration requise suite à l'installation consiste à accomplir des tâches de configuration supplémentaires nécessaires au bon fonctionnement de Sophos NAC Advanced.

9.1 Démarrage de l'agent SQL Server et vérification/modification des paramètres par défaut d'édition de rapports

Sophos NAC Advanced génère des rapports qui vous aide à identifier la conformité des systèmes d'extrémité aux stratégies de sécurité et les risques pour l'entreprise. Ces rapports génèrent des informations pouvant vous aider à résoudre des problèmes. Pour que la génération de rapports réussisse, assurez-vous que l'Agent SQL Server est démarré.

Les rapports sont disponibles soit en version résumée soit en version détaillée et incluent les données actuelles ou archivées. Les paramètres des rapports indiquent depuis combien de temps les données sont conservées dans le rapport en cours et quand elles sont archivées. Nous vous conseillons de ne changer aucun autre paramètre de rapports.

Les paramètres par défaut pour tous les rapports sont :

- Purger les données d'audit tous les **90** jours. Cette valeur correspond à la valeur `auditStorePurgeDays`. Si la valeur est paramétrée sur **-1**, la purge des données est désactivée.
- Purger les données des rapports actuels tous les **2** jours. Cette valeur correspond à la valeur `reportStorePurgeDays`.
- Purger les données des rapports archivés tous les **30** jours. Cette valeur correspond à la valeur `reportStoreWHPurgeDays`.

Remarque : la valeur `reportStoreWHPurgeDays` doit être plus grande que la valeur `reportStorePurgeDays` et que la valeur de déplacement des données.

- Déplacement des données vers les rapports archivés **1** fois par jour pour tous les rapports à 02:30 du matin. Cette valeur se trouve dans la tâche Report Warehouse Loader. Pour plus d'informations sur la modification de la fréquence d'archivage, reportez-vous à la section [Vérification/modification de la tâche Report Warehouse Loader](#) à la page 60.

1. Depuis le menu Démarrer du serveur SQL, procédez de l'une des manières suivantes :

- Si vous utilisez SQL Server 2000, cliquez sur **Microsoft SQL Server > Enterprise Manager**. SQL Enterprise Manager s'ouvre.
- Si vous utilisez SQL Server 2005 ou supérieur, cliquez sur **Microsoft SQL Server (version) > SQL Server Management Studio**. SQL Server Management Studio s'ouvre.

2. Pour démarrer l'Agent SQL Server, procédez de l'une des manières suivantes :

- Si vous utilisez SQL Server 2000, dans le dossier Gestion, recherchez **Agent SQL Server**, cliquez dessus avec le bouton droit de la souris et sélectionnez **Démarrer**.
- Si vous utilisez SQL Server 2005 ou supérieur, recherchez l'**Agent SQL Server**, cliquez avec le bouton droit de la souris dessus et sélectionnez **Démarrer**.

Important : pour vous assurer que l'Agent SQL Server démarre automatiquement au redémarrage du serveur SQL, ouvrez le Gestionnaire de contrôle des services Windows et

modifiez le type de démarrage du service SQLSERVERAGENT (SQL Server 2000) ou de l'Agent SQL Server (SQL Server 2005 ou supérieur) sur automatique.

3. Pour modifier les valeurs de purge, recherchez la base de données **ReportStore** et la table **LoadParam**.
4. Pour ouvrir la table **LoadParam**, procédez de l'une des manières suivantes :
 - Si vous utilisez SQL Server 2000, cliquez avec le bouton droit de la souris sur la table **LoadParam** et sélectionnez **Ouvrir une table > Renvoyer toutes les lignes**.
 - Si vous utilisez SQL Server 2005 ou supérieur, cliquez avec le bouton droit de la souris sur la table **LoadParam** et sélectionnez **Ouvrir une table**.
5. Pour modifier la valeur de purge des données d'audit, saisissez une nouvelle valeur sur la ligne **auditStorePurgeDays** dans la colonne **paramValue**.
Si le paramètre de la valeur est sur -1, la purge des données d'audit est désactivée.
6. Pour changer la valeur des données de purge pour les rapports actuels, saisissez une nouvelle valeur sur la ligne **reportStorePurgeDays** de la colonne **paramValue**.
7. Pour changer la valeur des données de purge pour les rapports archivés, saisissez une nouvelle valeur dans la rangée **reportStoreWHPurgeDays** de la colonne **paramValue**.
Remarque : la valeur reportstoreWHPurgeDays doit être plus grande que la valeur reportStorePurgeDays et que la valeur de déplacement des données.
8. Quittez SQL Enterprise Manager ou SQL Server Management Studio.

9.2 Taille des bases de données et des journaux des transactions du serveur SQL

Au cours de l'installation, les bases de données sont créées afin de permettre leur croissance automatique, d'empêcher la réduction automatique et de mettre à jour automatiquement les statistiques. Nous vous conseillons de ne pas modifier les propriétés de ces bases de données.

Pour des performances optimales de la base de données, nous vous conseillons de :

- Définir une taille assez grande pour les bases de données et pour leurs journaux des transactions respectifs afin d'éviter qu'ils grossissent trop régulièrement.
- Fixer une taille et non un pourcentage d'extension des bases de données et de leurs journaux des transactions respectifs.

9.2.1 Recommandations pour la taille des bases de données

Nom de la base de données	Taille recommandée	Taille maximale recommandée
ReportStore	.4 Ko x (nombre de profils dans la stratégie) x (nombre de systèmes d'extrémité)	500 Mo

Nom de la base de données	Taille recommandée	Taille maximale recommandée
ReportStoreWH Remarque : par défaut, la valeur de vidage des données est de 30 jours.	1.5 Ko x (nombre de profils dans la stratégie) x (nombre de systèmes d'extrémité) x (valeur de vidage des données en jours)	500 Mo
PolicyStore	Pour une entreprise ayant des milliers d'utilisateurs et une stratégie contenant moins de 100 applications, paramétrez la base de données PolicyStore sur 500 Mo.	100 Mo

9.2.2 Recommandations pour la taille des journaux des transactions

Nom du journal des transactions	Taille recommandée	Taille maximale recommandée
ReportStore	500 Mo	100 Mo
ReportStoreWH	2 Go	250 Mo
PolicyStore	Conserver la taille par défaut	100 Mo

9.2.3 Modification de la taille des bases de données et des journaux des transactions SQL (SQL Server 2000)

Pour déterminer la taille des bases de données SQL et des journaux des transactions, reportez-vous aux sections [Recommandations pour la taille des bases de données](#) à la page 26 et [Recommandations pour la taille des journaux des transactions](#) à la page 27. Les instructions suivantes s'appliquent au SQL Server 2000.

1. Depuis le menu Start du serveur SQL, cliquez sur **Microsoft SQL Server > Enterprise Manager**.
SQL Enterprise Manager s'ouvre.
2. Pour changer la taille de ReportStore, dans le dossier Bases de données, recherchez **ReportStore**, cliquez dessus avec le bouton droit de la souris et sélectionnez **Propriétés**.
3. Cliquez sur l'onglet **Fichiers de données**.
4. Sélectionnez le champ **Taille initiale (Mo)** et saisissez une taille raisonnable pour ReportStore.

5. Sélectionnez le bouton radio **En méga-octets** et saisissez une taille raisonnable pour la croissance du fichier de ReportStore.
6. Cliquez sur l'onglet **Journal des transactions**.
7. Sélectionnez le champ **Taille initiale (Mo)** et saisissez une taille raisonnable pour le journal des transactions de ReportStore.
8. Sélectionnez le bouton radio **En méga-octets** et saisissez une taille raisonnable pour le journal des transactions de ReportStore.
9. Cliquez sur **OK**.
10. Répétez les étapes 2 à 9 pour ReportStoreWH et PolicyStore.
11. Quittez SQL Enterprise Manager.

9.2.4 Modification de la taille des bases de données et des journaux des transactions de SQL (SQL Server 2005 et supérieur)

Pour déterminer la taille des bases de données SQL et des journaux des transactions, reportez-vous aux sections [Recommandations pour la taille des bases de données](#) à la page 26 et [Recommandations pour la taille des journaux des transactions](#) à la page 27. Les instructions suivantes s'appliquent à SQL Server 2005 et supérieur.

1. Depuis le menu Start du serveur SQL, cliquez sur **Microsoft SQL Server (version) > SQL Server Management Studio**.
2. Depuis la boîte de dialogue SQL Server Management Studio, recherchez la base de données **ReportStore** dans le dossier Databases et cliquez dessus avec le bouton droit de la souris, puis, sélectionnez **Properties**.
3. Depuis la boîte de dialogue Properties, sélectionnez **Files**.
4. Recherchez le fichier **ReportStore_Data**, sélectionnez le champ **Initial Size (MB)** et saisissez une taille appropriée pour la base de données.
5. Recherchez le fichier **ReportStore_Log**, sélectionnez le champ **Initial Size (MB)** et saisissez une taille appropriée pour le fichier journal.
6. Cliquez sur **OK**.
7. Répétez les étapes 2 à 6 pour ReportStoreWH et PolicyStore.
8. Quittez SQL Server Management Studio.

9.3 Accès au Compliance Manager

Le Compliance Manager est un emplacement centralisé permettant d'administrer Sophos NAC Advanced. Le Compliance Manager s'installe en tant que site Web par défaut à l'emplacement suivant : <LecteurLocal>\Inetpub\wwwroot\SophosNAC.

Important : pour que le Compliance Manager affiche et sauvegarde les informations et pour qu'il affiche les images correctement :

- Ajoutez le Compliance Manager comme site Web de confiance dans Internet Explorer. Ce paramètre n'est pas nécessaire pour Internet Explorer 7.x.
- Désactivez le blocage des fenêtres intempestives lors de l'accès au Compliance Manager.

Important : pour un fonctionnement correct de Sophos NAC Advanced avec HTTPS, installez un certificat Web pour les composants de l'interface Web, de l'interface des stratégies, de l'interface des rapports et de l'interface d'enregistrement. Ces composants peuvent partager le même certificat Web. Si vous générez votre propre certificat Web, assurez-vous que tous les ordinateurs d'extrémité acceptent ce certificat Web généré comme valide. Si vous testez ou évaluez Sophos NAC Advanced et que HTTPS n'est pas activé, le certificat Web n'est pas nécessaire.

1. Ouvrez Internet Explorer.
2. Saisissez l'adresse suivante : `https://<adresse ip/DNS du serveur Sophos>/SophosComplianceManager`. La page de connexion au Compliance Manager apparaît.

Remarque : pour désactiver HTTPS, reportez-vous à la section [Désactivation de HTTPS pour tests en environnements hors production](#) à la page 61. Dès que HTTPS est désactivé, vous pouvez accéder au Compliance Manager en utilisant l'adresse suivante : `https://<adresse ip/DNS du serveur Sophos>/SophosComplianceManager`.

3. Saisissez **Admin** dans le champ **Account Name** et le mot de passe de votre choix dans le champ **Password**.
4. Cliquez sur **OK**.

Remarque :

- Conservez une trace de ce mot de passe car c'est le seul moyen dont vous disposez pour accéder au Compliance Manager tant que vous n'avez pas créé d'autres comptes utilisateurs.
- Avec le Compliance Manager, créez ou utilisez les modèles d'accès, profils, groupes et stratégies préconfigurés.

9.4 Configuration d'une banque d'utilisateurs externe pour accéder au Compliance Manager (Tâche facultative)

Lorsque vous créez des comptes utilisateur pour accéder au Compliance Manager, précisez que ces comptes utilisent une banque d'utilisateurs externe. Si cette banque d'utilisateurs est du même type que celle utilisée par le Compliance Manager pour procéder à l'authentification, alors aucune configuration supplémentaire n'est requise. Si les comptes utilisateur Compliance Manager sont différents de ceux des agents de conformité, créez une stratégie de demande de connexion séparée.

Remarque : Sophos collabore directement avec les entreprises disposant de comptes utilisateur Compliance Manager qui utilisent un type de banque d'utilisateurs différent de celui des utilisateurs de l'agent. Cette collaboration directe garantit une mise en place correcte de la configuration.

9.4.1 Création d'une Stratégie de demande de connexion pour une banque d'utilisateurs externe (Windows Server 2003)

Si les comptes utilisateur du Compliance Manager vont utiliser un type de banque d'utilisateurs différent de celui des agents de conformité, créez une Stratégie de demande de connexion

séparée avec un type de service administratif. Cette Stratégie de demande de connexion doit avoir la priorité.

1. À partir du menu Démarrer du serveur d'applications de conformité, cliquez sur **Outils d'administration > Service d'authentification Internet**.

Le service d'authentification Internet s'ouvre.

2. Cliquez deux fois sur **Demande de connexion en cours de traitement**.
3. Cliquez avec le bouton droit de la souris sur **Stratégies de demande de connexion** puis cliquez sur **Nouvelle > Stratégie de demande de connexion**.

L'assistant Stratégie de demande de nouvelle connexion apparaît.

4. Cliquez sur **Suivant** pour continuer.
5. Sélectionnez l'option **Une stratégie personnalisée**. Saisissez un nom pour la stratégie de demande de connexion dans le champ à disposition. Cliquez sur **Suivant** pour continuer.
6. Cliquez sur **Ajouter** pour spécifier les conditions appropriés de la stratégie.
7. Sélectionnez la condition de stratégie **Type de service** pour la stratégie et cliquez sur **Ajouter**.
8. Sélectionnez **Administration** depuis la liste **Types disponibles** et cliquez sur **Ajouter**. Cliquez sur **OK** pour continuer.
9. Cliquez sur **Suivant** pour continuer.
10. Cliquez sur **Suivant** pour continuer.
11. Vérifiez les informations concernant la stratégie de demande de connexion et cliquez sur **Terminer**.

Cette Stratégie de demande de connexion doit avoir la priorité. Pour donner une plus grande priorité à la stratégie, cliquez avec le bouton droit de la souris sur le nom de la stratégie et sélectionnez **Monter**.

9.4.2 Création d'une Stratégie de demande de connexion pour une banque d'utilisateurs externe (Windows Server 2008)

Si les comptes utilisateur du Compliance Manager vont utiliser un type de banque d'utilisateurs différent de celui des agents de conformité, créez une Stratégie de demande de connexion séparée avec un type de service administratif. Cette Stratégie de demande de connexion doit avoir la priorité.

1. À partir du menu Démarrer du serveur d'applications de conformité, cliquez sur **Outils d'administration > Serveur de stratégie réseau**.

Le Serveur de stratégie du réseau s'ouvre.

2. Sous Stratégies, cliquez avec le bouton droit de la souris sur **Stratégies de demande de connexion**, puis cliquez sur **Nouvelle**.

L'assistant Stratégie de demande de nouvelle connexion apparaît.

3. Saisissez un nom de stratégie et laissez **Non spécifié** comme méthode de connexion réseau.
4. Cliquez sur **Suivant** pour continuer.
5. Cliquez sur **Ajouter** pour spécifier les conditions appropriés de la stratégie.

6. Sélectionnez la condition de stratégie **Type de service** et cliquez sur **Ajouter**.
7. Sélectionnez **Administration** et cliquez sur **OK**.
8. Cliquez sur **Suivant** pour continuer.
9. Dans la section **Authentification**, sélectionnez le bouton **Accepter les utilisateurs sans valider les informations d'identification**.
10. Cliquez sur **Suivant** pour continuer.
11. Cliquez sur **Suivant** pour continuer. Il n'est pas nécessaire de définir des attributs pour cette stratégie.
12. Vérifiez les informations concernant la stratégie de demande de connexion et cliquez sur **Terminer**.

Cette Stratégie de demande de connexion doit avoir la priorité. Pour donner une plus grande priorité à la stratégie, cliquez avec le bouton droit de la souris sur le nom de la stratégie et sélectionnez **Monter**.

9.5 Paramètres du Service d'authentification Internet (IAS) (Windows Server 2003)

Le Service d'authentification Internet (IAS) est utilisé pour la recherche et l'authentification de groupes et pour l'application de RADIUS.

La majorité des mises en place Sophos NAC Advanced nécessitent la recherche et l'authentification de groupes. Vous allez devoir effectuer les étapes suivantes :

- Attribuez au Service d'authentification Internet l'accès à Active Directory.

Remarque : pour les mises en place LDAP ou si vous utilisez Sophos NAC Advanced en tant que proxy RADIUS (pour une configuration de Sophos NAC Advanced en mode proxy devant un autre serveur RADIUS), vous n'avez **pas** besoin d'effectuer cette tâche.

- Créez une stratégie d'accès à distance.

Si vous utilisez RADIUS Enforcement avec un réseau privé virtuel (VPN), 802.1x, Cisco NAC, ou des mises en place avancées de RADIUS, vous allez devoir effectuer les étapes suivantes :

- Attribuez au Service d'authentification Internet l'accès à Active Directory.
- Configurez une stratégie d'accès à distance.
- Ajoutez les clients RADIUS pour chaque périphérique d'accès au réseau, tel que les concentrateurs VPN.

9.5.1 Accès du Service d'authentification Internet à Active Directory

Par défaut, il se peut que le Service d'authentification Internet n'ait **pas** l'autorisation d'authentifier les utilisateurs dans Active Directory. Le serveur du Service d'authentification Internet doit avoir l'autorisation d'authentifier les utilisateurs dans Active Directory.

Important :

- Pour les mises en place LDAP ou si vous utilisez Sophos NAC Advanced en tant que proxy RADIUS (pour une configuration de Sophos NAC Advanced en mode proxy devant un autre serveur RADIUS), vous n'avez **pas** besoin d'effectuer cette tâche.

- Répétez ces instructions sur tous les serveurs d'applications de conformité ainsi que sur tous les serveurs RADIUS Enforcer.
- 1. Ouvrez une session sur un serveur d'applications de conformité ou sur un serveur RADIUS Enforcer en utilisant un compte avec les autorisations d'administrateur de domaine.
- 2. Depuis le menu Démarrer du serveur d'applications de conformité ou du serveur RADIUS Enforcer, cliquez sur **Outils d'administration > Service d'authentification Internet**.
Le service d'authentification Internet s'ouvre.
- 3. Cliquez avec le bouton droit de la souris sur **Service d'authentification Internet** et sélectionnez **Inscrire le serveur dans Active Directory**.
- 4. Cliquez sur **Oui** pour confirmer l'accès du Service d'authentification Internet à Active Directory.
Si le Service d'authentification Internet peut accéder à Active Directory, vous recevez un message le confirmant. Aucune autre étape n'est nécessaire.
- 5. Quittez le Service d'authentification Internet.
- 6. Répétez ces instructions sur tous les serveurs d'applications de conformité et sur tous les serveurs RADIUS Enforcer.

9.5.2 Configuration d'une Stratégie d'accès à distance

Créez une Stratégie d'accès à distance pour la majorité des mises en place de Sophos NAC Advanced. Ce document fournit uniquement une stratégie d'accès à distance fréquemment utilisée pour VPN. Les mises en place de Sophos NAC Advanced pour réseau local (LAN) nécessite une stratégie d'accès à distance pour la recherche et l'authentification des groupes.

Important :

- Si vous utilisez Sophos NAC Advanced en tant que proxy RADIUS (configuration de Sophos NAC Advanced en mode proxy devant un autre serveur RADIUS), vous n'avez **pas** besoin de configurer les stratégies d'accès à distance.
- Répétez ces instructions sur tous les serveurs d'applications de conformité ainsi que sur tous les serveurs RADIUS Enforcer.
- 1. Depuis le menu Démarrer du serveur d'applications de conformité ou du serveur RADIUS Enforcer, cliquez sur **Outils d'administration > Service d'authentification Internet**.
Le service d'authentification Internet s'ouvre.
- 2. Cliquez sur **Stratégies d'accès distant**.
- 3. Supprimez les deux stratégies intégrées : Connexions à d'autres serveurs d'accès et Connexions aux serveurs d'accès à distance et de routage Microsoft. Cliquez avec le bouton droit de la souris sur chaque nom de stratégie et sélectionnez **Supprimer**.
- 4. Cliquez avec le bouton droit de la souris sur **Stratégies d'accès distant** puis cliquez sur **Nouvelle stratégie d'accès distant**.
L'assistant Nouvelle stratégie d'accès distant apparaît.
- 5. Cliquez sur **Suivant** pour continuer.

6. Cliquez sur le bouton **Installer une stratégie personnalisée**. Saisissez un nom pour la stratégie d'accès distant dans le champ à disposition. Par exemple, utilisez Accorde l'accès aux utilisateurs VPN comme nom de stratégie d'accès distant. Cliquez sur **Suivant** pour continuer.
7. Cliquez sur **Ajouter** pour spécifier les conditions appropriés de la stratégie.
8. Procédez de l'une des manières suivantes :
 - Si tous les utilisateurs nécessitent l'accès quel que soit leurs groupes de domaine, passez à l'étape suivante.
 - Si des groupes de domaine spécifiques nécessitent l'accès plutôt que tous les utilisateurs, passez à l'étape 11.
9. Sélectionnez la condition de stratégie **Restrictions relatives aux jours et aux heures** si tous les utilisateurs nécessitent l'accès quel que soit leurs groupes de domaine. Cliquez sur **Ajouter**.

Remarque : la condition de stratégie Restrictions relatives aux jours et aux heures permet l'accès à tous les utilisateurs tandis que la condition de stratégie Groupes Windows permet de restreindre l'accès par groupe de domaine.
10. Sélectionnez le bouton **Autorisés**, puis cliquez sur **OK**. Passez à l'étape 15.
11. Sélectionnez la condition de stratégie **Groupes Windows** si les groupes de domaine spécifiques nécessitent l'accès plutôt que tous les utilisateurs. Cliquez sur **Ajouter**.

Remarque : la condition de stratégie Groupes Windows permet de restreindre l'accès au groupe de domaine tandis que la condition de stratégie Restrictions relatives aux jours et aux heures permet l'accès à tous les utilisateurs.
12. Cliquez sur **Ajouter** pour ajouter les groupes de domaine auxquels vous souhaitez appliquer cette stratégie d'accès à distance.
13. Saisissez les noms des groupes de domaine. Par exemple, Utilisateurs DOCLAB\VPN est un groupe de domaine valide. Cliquez sur **OK**.

Répétez les étapes 12 et 13 pour ajouter des groupes de domaine supplémentaires.
14. Cliquez sur **OK** lorsque vous avez terminé de spécifier les groupes de domaine.

La fenêtre Groupes affiche tous les groupes de domaine que vous avez ajouté.
15. Cliquez sur **Suivant** pour continuer.

Remarque : les conditions de la stratégie apparaissent selon la condition de stratégie Restrictions relatives aux jours et aux heures ou la condition de stratégie Groupes Windows que vous avez spécifiée.
16. Cliquez sur le bouton **Accorder l'autorisation d'accès distant**. Cliquez sur **Suivant** pour continuer.
17. Cliquez sur **Modifier le profil**.

18. Cliquez sur l'onglet **Authentification**. Sélectionnez les méthodes d'authentification que vous souhaitez utiliser. Cliquez sur **OK**.

Remarque :

- Pour une mise en place de LDAP, sélectionnez la case Authentification non chiffrée (PAP, SPAP).
- Si vous sélectionnez les cases Authentification non chiffrée (CHAP) ou Authentification non chiffrée (PAP, SPAP), une boîte de dialogue s'ouvre et vous demande si vous souhaitez voir la rubrique d'aide correspondante. Cliquez sur **Non** pour continuer.

19. Cliquez sur l'onglet **Avancé**. Cliquez sur **Ajouter**.
20. Sélectionnez **Ignore-User-Dialin-Properties** dans la liste déroulante des attributs. Cliquez sur **Ajouter**.
21. Sélectionnez le bouton **True**. Cliquez sur **OK**.
22. Cliquez sur **Fermer**. Cliquez sur **OK**.
23. Cliquez sur **Suivant** pour continuer.
24. Vérifiez les informations concernant la stratégie d'accès distant et cliquez sur **Terminer**.

9.5.3 Désactivation de la journalisation du Service d'authentification Internet pour des demandes d'authentification réussies (tâche facultative)

Pour réduire le nombre de messages du Journal des événements, Sophos vous suggère de désactiver la journalisation pour des demandes d'authentification réussies.

Remarque : répétez ces instructions sur tous les serveurs d'applications de conformité et sur tous les serveurs RADIUS Enforcer.

1. Depuis le menu Démarrer du serveur d'applications de conformité ou du serveur RADIUS Enforcer, cliquez sur **Outils d'administration > Service d'authentification Internet**.
Le service d'authentification Internet s'ouvre.
2. Cliquez avec le bouton droit de la souris sur **Service d'authentification Internet** et sélectionnez **Propriétés**.
3. Deselectionnez la case **Demandes d'authentification réussies** et cliquez sur **Appliquer**.
4. Quittez le Service d'authentification Internet.
5. Répétez ces instructions sur tous les serveurs d'applications de conformité et sur tous les serveurs RADIUS Enforcer.

9.5.4 Ajout de clients RADIUS pour chaque périphérique d'accès au réseau (tâche facultative)

Les instructions suivantes sont requises uniquement pour l'application de RADIUS. L'application de RADIUS est utilisée avec VPN, 802.1x, Cisco NAC et avec les mises en place RADIUS étendues. Pour chaque concentrateur VPN, ajoutez une entrée client RADIUS au

Service d'authentification Internet. Répétez ces instructions sur tous les serveurs d'applications de conformité et sur tous les serveurs RADIUS Enforcer.

1. Depuis le menu Démarrer du serveur d'applications de conformité ou du serveur RADIUS Enforcer, cliquez sur **Outils d'administration > Service d'authentification Internet**.

Le service d'authentification Internet s'ouvre.

2. Cliquez avec le bouton droit de la souris sur **Clients RADIUS** et sélectionnez **Nouveau client RADIUS**.

La fenêtre Ajouter un client RADIUS apparaît.

3. Saisissez un nom et une adresse IP ou un nom DNS que le concentrateur VPN va utiliser pour contacter le serveur d'applications de conformité. Cliquez sur **Suivant** pour continuer.
4. Saisissez et confirmez le secret partagé du concentrateur VPN dans les champs appropriés. Le secret partagé est le même que celui utilisé lors de la configuration du concentrateur VPN.

Remarque : dans le champ Client-Fournisseur, conservez l'option RADIUS Standard.

5. Assurez-vous que la case **Les requêtes doivent contenir l'attribut de l'authentificateur de message** n'est **pas** sélectionnée.
6. Cliquez sur **Terminer**.

Répétez ces instructions pour chaque concentrateur VPN que vous allez utiliser avec Sophos NAC Advanced. Répétez ces instructions sur tous les serveurs d'applications de conformité et sur tous les serveurs RADIUS Enforcer.

9.6 Paramètres du Serveur de stratégie réseau (NPS) (Windows Server 2008)

Le Serveur de stratégie réseau (NPS) est utilisé pour la recherche et l'authentification de groupes et pour l'application de RADIUS.

La majorité des mises en place Sophos NAC Advanced nécessitent la recherche et l'authentification de groupes. Vous allez devoir effectuer les étapes suivantes :

- Attribuez au Serveur de stratégie réseau (NPS) l'accès à Active Directory.

Remarque : pour les mises en place LDAP ou si vous utilisez Sophos NAC Advanced en tant que proxy RADIUS (pour une configuration de Sophos NAC Advanced en mode proxy devant un autre serveur RADIUS), vous n'avez **pas** besoin d'effectuer cette tâche.

- Créez une stratégie réseau.

Si vous utilisez RADIUS Enforcement avec un réseau privé virtuel (VPN), 802.1x, Cisco NAC, ou des mises en place avancées de RADIUS, vous allez devoir effectuer les étapes suivantes :

- Attribuez au Serveur de stratégie réseau (NPS) l'accès à Active Directory.
- Configurez une stratégie réseau.
- Ajoutez les clients RADIUS pour chaque périphérique d'accès au réseau, tel que les concentrateurs VPN.

9.6.1 Attribution au Serveur de stratégie réseau (NPS) de l'accès à Active Directory

Par défaut, il se peut que le Serveur de stratégie réseau n'ait **pas** l'autorisation d'authentifier les utilisateurs dans Active Directory. Le Serveur de stratégie réseau doit avoir l'autorisation d'authentifier les utilisateurs dans Active Directory.

Important :

- Pour les mises en place LDAP ou si vous utilisez Sophos NAC Advanced en tant que proxy RADIUS (pour une configuration de Sophos NAC Advanced en mode proxy devant un autre serveur RADIUS), vous n'avez **pas** besoin d'effectuer cette tâche.
- Répétez ces instructions sur tous les serveurs d'applications de conformité ainsi que sur tous les serveurs RADIUS Enforcer.

1. Ouvrez une session sur un serveur d'applications de conformité ou sur un serveur RADIUS Enforcer en utilisant un compte avec les autorisations d'administrateur de domaine.
2. Depuis le menu Démarrer du serveur d'applications de conformité ou du serveur RADIUS Enforcer, cliquez sur **Outils d'administration > Serveur de stratégie réseau**.

Le Serveur de stratégie du réseau s'ouvre.

3. Cliquez avec le bouton droit de la souris sur **NPS (Local)** et sélectionnez **Inscrire le serveur dans Active Directory**.
4. Cliquez sur **OK** pour confirmer l'accès du Serveur de stratégie réseau à Active Directory.

Si le Serveur de stratégie réseau peut accéder à Active Directory, vous recevez un message de confirmation. Aucune autre étape n'est nécessaire.

5. Quittez le Serveur de stratégie réseau.
6. Répétez ces instructions sur tous les serveurs d'applications de conformité et sur tous les serveurs RADIUS Enforcer.

9.6.2 Configuration d'une stratégie réseau

Créez une stratégie réseau pour la majorité de vos mises en place de Sophos NAC Advanced. Ce document fournit uniquement une stratégie réseau fréquemment utilisée pour VPN. Les mises en place de Sophos NAC Advanced pour réseau local (LAN) nécessite une stratégie réseau pour la recherche et l'authentification des groupes.

Important :

- Si vous utilisez Sophos NAC Advanced en tant que proxy RADIUS (configuration de Sophos NAC Advanced en mode proxy devant un autre serveur RADIUS), vous n'avez **pas** besoin de configurer les stratégies réseau.
- Répétez ces instructions sur tous les serveurs d'applications de conformité ainsi que sur tous les serveurs RADIUS Enforcer.

1. Depuis le menu Démarrer du serveur d'applications de conformité ou du serveur RADIUS Enforcer, cliquez sur **Outils d'administration > Serveur de stratégie réseau**.

Le Serveur de stratégie du réseau s'ouvre.

2. Sous Stratégies, cliquez sur **Stratégies réseau**.
3. Supprimez les deux stratégies intégrées : Connexions à d'autres serveurs d'accès et Connexions aux serveurs d'accès à distance et de routage Microsoft. Cliquez avec le bouton droit de la souris sur chaque nom de stratégie et sélectionnez **Supprimer**.
4. Cliquez avec le bouton droit de la souris sur **Stratégies réseau** et sélectionnez **Nouvelle**.
L'assistant Nouvelle stratégie réseau apparaît.
5. Saisissez un nom de stratégie et laissez **Non spécifié** comme méthode de connexion réseau. Par exemple, utilisez Accorde l'accès aux utilisateurs VPN comme nom de stratégie réseau. Cliquez sur **Suivant** pour continuer.
6. Cliquez sur **Ajouter** pour spécifier les conditions appropriés de la stratégie.
7. Procédez de l'une des manières suivantes :
 - Si tous les utilisateurs nécessitent l'accès quel que soit leurs groupes de domaine, passez à l'étape suivante.
 - Si des groupes de domaine spécifiques nécessitent l'accès plutôt que tous les utilisateurs, passez à l'étape 10.
8. Sélectionnez la condition de stratégie **Restrictions relatives aux jours et aux heures** si tous les utilisateurs nécessitent l'accès quel que soit leurs groupes de domaine. Cliquez sur **Ajouter**.
Remarque : la condition de stratégie Restrictions relatives aux jours et aux heures permet l'accès à tous les utilisateurs tandis que la condition de stratégie Groupes Windows permet de restreindre l'accès par groupe de domaine.
9. Sélectionnez le bouton **Autorisés**, puis cliquez sur **OK**. Passez à l'étape 14.
10. Sélectionnez la condition de stratégie **Groupes Windows** si les groupes de domaine spécifiques nécessitent l'accès plutôt que tous les utilisateurs. Cliquez sur **Ajouter**.
Remarque : la condition de stratégie Groupes Windows permet de restreindre l'accès au groupe de domaine tandis que la condition Restrictions relatives aux jours et aux heures permet l'accès à tous les utilisateurs.
11. Cliquez sur **Ajouter des groupes** pour ajouter les groupes de domaine auxquels vous souhaitez appliquer cette stratégie réseau.
12. Saisissez les noms des groupes de domaine. Par exemple, Utilisateurs DOCLAB\VPN est un groupe de domaine valide. Cliquez sur **OK**.
Répétez les étapes 11 et 12 pour ajouter des groupes de domaine supplémentaires.
13. Cliquez sur **OK** lorsque vous avez terminé de spécifier les groupes de domaine.
La fenêtre Groupes Windows affiche tous les groupes de domaine que vous avez ajouté.
14. Cliquez sur **Suivant** pour continuer.
Remarque : les conditions de la stratégie apparaissent selon la condition de stratégie Restrictions relatives aux jours et aux heures ou Groupes Windows que vous avez spécifiée.
15. Cliquez sur le bouton **Accès accordé**. Cliquez sur **Suivant** pour continuer.

16. Sélectionnez les cases correspondant aux méthodes d'authentification que vous souhaitez utiliser. Cliquez sur **Suivant** pour continuer.

Remarque :

- Pour une mise en place de LDAP, sélectionnez la case Authentification non chiffrée (PAP, SPAP).
 - Si vous sélectionnez les cases Authentification non chiffrée (CHAP) ou Authentification non chiffrée (PAP, SPAP), une boîte de dialogue s'ouvre et vous demande si vous souhaitez voir la rubrique d'aide correspondante. Cliquez sur **Non** pour continuer.
17. Cliquez sur **Suivant** pour continuer. Il n'est pas nécessaire de configurer des contraintes pour cette stratégie.
 18. Cliquez sur **Suivant** pour continuer. Il n'est pas nécessaire de configurer des paramètres supplémentaires pour cette stratégie.
 19. Vérifiez les informations concernant la stratégie réseau et cliquez sur **Terminer**.

9.6.3 Désactivation de la journalisation du Serveur de stratégie réseau pour que les demandes d'authentification s'effectuent avec succès (tâche facultative)

Pour réduire le nombre de messages du Journal des événements, Sophos vous suggère de désactiver la journalisation pour des demandes d'authentification réussies.

Remarque : répétez ces instructions sur tous les serveurs d'applications de conformité et sur tous les serveurs RADIUS Enforcer.

1. Depuis le menu Démarrer du serveur d'applications de conformité ou du serveur RADIUS Enforcer, cliquez sur **Outils d'administration > Serveur de stratégie réseau**.
Le Serveur de stratégie du réseau s'ouvre.
2. Cliquez avec le bouton droit de la souris sur **NPS (Local)** et sélectionnez **Propriétés**.
3. Deselectionnez la case **Demandes d'authentification réussies** et cliquez sur **Appliquer**.
4. Quittez le Serveur de stratégie réseau.
5. Répétez ces instructions sur tous les serveurs d'applications de conformité et sur tous les serveurs RADIUS Enforcer.

9.6.4 Ajout de clients RADIUS pour chaque périphérique d'accès au réseau (tâche facultative)

Les instructions suivantes sont requises uniquement pour l'application de RADIUS.

L'application de RADIUS est utilisée avec VPN, 802.1x, Cisco NAC et avec les mises en place RADIUS étendues. Pour chaque concentrateur VPN, ajoutez une entrée client RADIUS au Serveur de stratégie réseau. Répétez ces instructions sur tous les serveurs d'applications de conformité et sur tous les serveurs RADIUS Enforcer.

1. Depuis le menu Démarrer du serveur d'applications de conformité ou du serveur RADIUS Enforcer, cliquez sur **Outils d'administration > Serveur de stratégie réseau**.
Le Serveur de stratégie du réseau s'ouvre.

2. Sous Clients et serveurs RADIUS, cliquez avec le bouton droit de la souris sur **Clients RADIUS** et cliquez sur **Nouveau client RADIUS**.

La fenêtre Ajouter un client RADIUS apparaît.

3. Saisissez un nom et une adresse IP ou un nom DNS que le concentrateur VPN va utiliser pour contacter le serveur d'applications de conformité. Cliquez sur **Next** pour continuer.
4. Saisissez et confirmez le secret partagé du concentrateur VPN dans les champs appropriés. Le secret partagé est le même que celui utilisé lors de la configuration du concentrateur VPN.

Remarque : dans le champ Client-Fournisseur, conservez l'option RADIUS Standard.

5. Assurez-vous que la case **Les messages de demande d'accès doivent contenir l'attribut de l'authentificateur de message** n'est pas sélectionnée.
6. Cliquez sur **OK**.

Répétez ces instructions pour chaque concentrateur VPN que vous allez utiliser avec Sophos NAC Advanced. Répétez ces instructions sur tous les serveurs d'applications de conformité et sur tous les serveurs RADIUS Enforcer.

9.7 Sophos NAC Advanced en tant que proxy RADIUS (Windows Server 2003) (tâches facultatives)

Pour utiliser Sophos NAC Advanced en tant que proxy RADIUS (configuration de Sophos NAC Advanced en mode proxy devant un autre serveur RADIUS), modifiez la configuration du Service d'authentification Internet. L'utilisation de Sophos NAC Advanced en tant que proxy RADIUS ne nécessite pas la création d'une stratégie d'accès distant. Créez plutôt une stratégie de demande de connexion et utilisez un groupe de serveurs RADIUS à distance.

Remarque : répétez ces instructions sur tous les serveurs d'applications de conformité ainsi que sur tous les serveurs RADIUS Enforcer.

9.7.1 Ajout d'un groupe de serveurs RADIUS distant

1. Depuis le menu Démarrer du serveur d'applications de conformité ou du serveur RADIUS Enforcer, cliquez sur **Outils d'administration > Service d'authentification Internet**.

Le service d'authentification Internet s'ouvre.

2. Cliquez sur **Requête de connexion en cours de traitement**.
3. Cliquez avec le bouton droit de la souris sur **Groupes de serveurs RADIUS distants** et sélectionnez **Nouveau groupe de serveurs RADIUS distants**.

L'assistant Nouveau groupe de serveurs RADIUS distants apparaît.

4. Cliquez sur **Suivant** pour continuer.
5. Sélectionnez l'option **Standard** et saisissez un nom de groupe de serveurs dans le champ approprié.
6. Cliquez sur **Suivant** pour continuer.
7. Saisissez l'adresse IP de votre serveur RADIUS distant principal dans le champ disponible.

8. Saisissez l'adresse IP de votre serveur RADIUS distant de sauvegarde ou dessélectionnez la case **Paramétrer un serveur de sauvegarde pour ce groupe**.
9. Saisissez et confirmez le secret partagé du groupe de serveurs.
10. Cliquez sur **Suivant** pour continuer.
11. Assurez-vous que la case **Démarrer l'Assistant Stratégie de demande de nouvelle connexion à la fermeture de cet Assistant** est sélectionnée.
12. Vérifiez les informations concernant le groupe de serveurs RADIUS distant et cliquez sur **Terminer**.
13. Rendez-vous sur [Création d'une Stratégie de demande de connexion](#) à la page 40.

9.7.2 Création d'une Stratégie de demande de connexion

Créez une Stratégie de demande de connexion lorsque vous utilisez Sophos NAC Advanced en tant que proxy RADIUS.

1. Procédez de l'une des manières suivantes :
 - Si vous démarrez l'assistant comme indiqué à la section [Ajout d'un groupe de serveurs RADIUS distant](#) à la page 39, passez à l'étape suivante.
 - Depuis le menu Démarrer du serveur d'applications de conformité ou du serveur RADIUS Enforcer, cliquez sur **Outils d'administration > Service d'authentification Internet**. Le service d'authentification Internet s'ouvre. Cliquez deux fois sur **Demande de connexion en cours de traitement**. Cliquez avec le bouton droit de la souris sur **Stratégies de demande de connexion** puis cliquez sur **Nouvelle > Stratégie de demande de connexion**.

L'assistant Stratégie de demande de nouvelle connexion apparaît.

2. Cliquez sur **Suivant** pour continuer.
3. Sélectionnez l'option **Une stratégie typique pour un scénario commun**.
4. Saisissez un nom pour la stratégie de demande de connexion.
5. Cliquez sur **Suivant** pour continuer.
6. Sélectionnez l'option **Transfère les demandes de connexion à un serveur RADIUS distant pour authentification**.
7. Cliquez sur **Suivant** pour continuer.
8. Saisissez le(s) nom(s) de domaine que vous allez utiliser en tant que proxy ou un caractère joker .* si vous prévoyez d'utiliser tous les domaines en tant que proxy.
9. Dessélectionnez la case **Avant l'authentification, supprimer le nom de domaine du nom utilisateur**.
10. Sélectionnez le groupe de serveurs que vous avez créé dans la liste déroulante.
11. Cliquez sur **Suivant** pour continuer.
12. Cliquez sur **Terminer**.
13. Rendez-vous sur [Vérification des conditions de la stratégie](#) à la page 41.

9.7.3 Vérification des conditions de la stratégie

1. Dans la liste **Stratégie de demande de connexion du Service d'authentification Internet**, cliquez avec le bouton droit de la souris sur la stratégie que vous venez de créer et sélectionnez **Propriétés**.

La fenêtre des Propriétés apparaît.

2. Vérifiez les conditions de la stratégie que vous avez créée.
3. Si les conditions de la stratégie sont incorrectes ou incomplètes, cliquez sur **Ajouter** ou sur **Modifier** pour effectuer des changements.

Remarque : si vous devez créer une condition de la stratégie pour que tous les utilisateurs soient mis en proxy, vous pouvez utiliser l'heure du jour en tant que condition et la définir sur 24x7.

4. Cliquez sur **OK**.
5. Rendez-vous à la section [Modification des ports d'authentification et de gestion RADIUS](#) à la page 41.

9.7.4 Modification des ports d'authentification et de gestion RADIUS

Par défaut, les ports d'authentification et de gestion RADIUS sont définis sur 1812 et 1813. Si vous utilisez d'autres ports d'authentification et de gestion, les ports d'authentification et de gestion doivent être modifiés.

Remarque : le port d'authentification le plus fréquemment utilisé est le port 1645 tandis que le port de gestion le plus fréquemment utilisé est le port 1646.

1. Dans la liste Groupes de serveurs RADIUS distants dans le Service d'authentification Internet, cliquez avec le bouton droit de la souris sur le groupe de serveurs que vous venez de créer et sélectionnez **Propriétés**.

La fenêtre des Propriétés apparaît.

2. Sélectionnez le premier serveur dans la liste des serveurs que vous avez ajoutés à ce groupe et cliquez sur **Propriétés**.
3. Cliquez sur l'onglet **Authentification/Gestion des comptes**.

4. Si nécessaire, modifiez le port d'authentification, le secret partagé et le port de gestion.

Remarque : le port d'authentification le plus fréquemment utilisé est le port 1645 tandis que le port de gestion le plus fréquemment utilisé est le port 1646.

5. Si nécessaire, répétez les étapes 2 à 5 pour paramétrer les ports d'authentification et de gestion pour des serveurs supplémentaires dans le groupe de serveurs.
6. Cliquez sur **OK**.
7. Rendez-vous à la section [Modification du protocole d'authentification RADIUS dans l'interface d'enregistrement](#) à la page 42.

9.7.5 Modification du protocole d'authentification RADIUS dans l'interface d'enregistrement

Par défaut, Sophos NAC Advanced utilise MSchapV2 RADIUS comme protocole d'authentification par défaut. Si votre serveur RADIUS distant n'utilise pas ce protocole d'authentification, modifiez le protocole d'authentification RADIUS dans l'interface d'enregistrement.

1. Recherchez le fichier Registration Interface Web.config pour l'interface d'enregistrement sur le serveur d'applications de conformité ou sur le serveur RADIUS Enforcer. Si vous avez installé le logiciel Sophos NAC Advanced dans l'emplacement par défaut, le fichier est disponible à l'emplacement suivant : *<lecteur local>*\inetpub\wwwroot\RegistrationInterface\web.config.
2. Ouvrez le fichier Web.config dans le Bloc-notes.
3. Recherchez la section **authInterface** et la sous-section **radius**.
4. Modifiez la valeur **mschapv2** sur cette ligne `<add key="authType" value="mschapv2" />` pour celle du protocole d'authentification RADIUS utilisé par votre serveur RADIUS distant.

La sous-section radius modifiée du fichier Registration Interface web.config doit apparaître ainsi :

```
<radius>

<add key="authType" value="votre protocole d'authentification
RADIUS distant" />
<add key="serverRetries" value="1" />
<add key="listRetries" value="1" />
</radius>
```

5. Enregistrez et fermez le fichier.
6. Vous pouvez aussi choisir de vous rendre à la section [Configuration du serveur RADIUS pour les réorientations/profils de groupes \(tâche facultative\)](#) à la page 42.

9.7.6 Configuration du serveur RADIUS pour les réorientations/profils de groupes (tâche facultative)

Vous pouvez utiliser Sophos NAC Advanced ou le serveur RADIUS pour la réorientation de groupes. Pour ces deux configurations, créez des groupes à l'aide de Sophos NAC Advanced. Pour plus d'informations, reportez-vous à l'Aide de Compliance Manager.

Pour utiliser les réorientations/profils de groupes du serveur RADIUS avec Sophos NAC Advanced, envoyez les informations sur le groupe par le biais d'un paquet RADIUS vers Sophos NAC Advanced à l'aide d'un attribut spécifique d'un fournisseur (VSA). Pour de plus amples informations, reportez-vous à la documentation utilisateur de RADIUS pour savoir comment renvoyer un attribut spécifique d'un fournisseur.

Attribut spécifique d'un fournisseur Sophos (VSA)

La syntaxe d'un attribut spécifique d'un fournisseur repose sur les instructions décrites à la section 5.26 du document (URL RFC2685) "Remote Authentication Dial In User Service (RADIUS)" disponible sur Internet à <http://www.rfc-archive.org/getrfc.php?rfc=2865>.

Identifiant Fournisseur Sophos

L'identifiant Fournisseur identifie le fournisseur. L'identifiant du fournisseur Sophos est 5428 (décimal) ou 0x00001534 (hexadécimal, dans l'ordre du réseau).

Attribut EF-GroupID

L'attribut spécifique d'un fournisseur EF-GroupID indique quel groupe est utilisé pour mettre en place les paramètres de la session pour un utilisateur identifié.

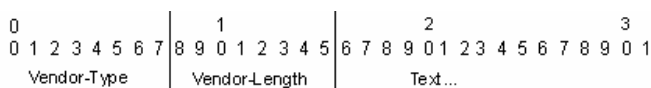
Les modèles d'accès RADIUS Enforcer déterminent l'accès réseau ; toutefois les exemptions sont considérées en priorité. Lorsqu'une requête est exemptée, l'accès au réseau est autorisé quel que soit le groupe. Le tableau suivant décrit les scénarios de spécification ou de non spécification d'une stratégie par défaut dans le Compliance Manager :

Scénarios	Stratégie par défaut spécifiée	Stratégie par défaut non spécifiée
L'attribut spécifique d'un fournisseur EF-GroupID n'est pas présent	La stratégie par défaut est appliquée. L'accès au réseau est déterminé lorsqu'un modèle d'accès RADIUS Enforcer correspond à la requête. Les modèles d'accès RADIUS Enforcer associés à la stratégie sont évalués en priorité. Si aucune correspondance n'est trouvée, les modèles d'accès RADIUS Enforcer par défaut sont évalués. Si aucune correspondance n'est trouvée, l'accès au réseau est refusé.	L'utilisateur ne reçoit pas la stratégie. L'accès au réseau est déterminé lorsqu'un modèle d'accès RADIUS Enforcer correspond à la requête. Les modèles d'accès RADIUS Enforcer par défaut sont évalués en priorité. Si aucune correspondance n'est trouvée, l'accès au réseau est refusé.
L'attribut spécifique d'un fournisseur EF-GroupID n'existe pas ou n'est pas défini.	La stratégie par défaut est appliquée. L'accès au réseau est déterminé lorsqu'un modèle d'accès RADIUS Enforcer correspond à la requête. Les modèles d'accès RADIUS Enforcer associés à la stratégie sont évalués en priorité. Si aucune correspondance n'est trouvée, les modèles d'accès RADIUS Enforcer par défaut sont évalués. Si aucune correspondance n'est trouvée, l'accès au réseau est refusé.	L'utilisateur ne reçoit pas la stratégie. L'accès au réseau est déterminé lorsqu'un modèle d'accès RADIUS Enforcer correspond à la requête. Les modèles d'accès RADIUS Enforcer par défaut sont évalués en priorité. Si aucune correspondance n'est trouvée, l'accès au réseau est refusé.
L'attribut spécifique d'un fournisseur EF-GroupID est valide	L'utilisateur est placé dans un groupe spécifié et la stratégie associée est appliquée. L'accès au réseau est déterminé lorsqu'un modèle d'accès RADIUS Enforcer	L'utilisateur est placé dans un groupe spécifié et la stratégie associée est appliquée. L'accès au réseau est déterminé lorsqu'un modèle d'accès RADIUS Enforcer correspond à la

Scénarios	Stratégie par défaut spécifiée	Stratégie par défaut non spécifiée
	correspond à la requête. Les modèles d'accès RADIUS Enforcer associés à la stratégie sont évalués en priorité. Si aucune correspondance n'est trouvée, les modèles d'accès RADIUS Enforcer par défaut sont évalués. Si aucune correspondance n'est trouvée, l'accès au réseau est refusé.	requête. Les modèles d'accès RADIUS Enforcer associés à la stratégie sont évalués en priorité. Si aucune correspondance n'est trouvée, les modèles d'accès RADIUS Enforcer par défaut sont évalués. Si aucune correspondance n'est trouvée, l'accès au réseau est refusé.

Format de l'attribut EF-GroupID

Le format des informations sur la valeur de l'attribut spécifique d'un fournisseur EF-GroupID est décrit dans le diagramme et le tableau ci-dessous. Les champs sont transmis de la gauche vers la droite.



Type de fournisseur	Longueur du fournisseur	Texte
20 (14 hex) pour EF-User-Group	>2	<p>Le champ de texte est compris entre un ou plusieurs octets de caractères lisibles par l'œil humain. Il ne doit pas se terminer par un zéro. La valeur de ce champ de texte détermine un Groupe d'utilisateurs particulier pour la session de l'utilisateur identifié.</p> <p>Paramètres du texte de l'identifiant du Groupe d'utilisateurs :</p> <ul style="list-style-type: none"> ■ Maximum de 253 caractères pouvant contenir une combinaison de chiffres et de lettres. Aucun autre caractère n'est autorisé. ■ Non sensible aux majuscules. ■ Espaces non autorisés.

Exemple d'attribut EF-User-Group

Si, par exemple, l'attribut spécifique d'un fournisseur est paramétré sur EF-User-Group = "WestCoastSales", il comprend des chiffres hexadécimaux (ordre du réseau) décrit dans le tableau suivant :

Description	Chiffres hexadécimaux
Informations d'en-tête	
Saisissez : attribut RADIUS 26 (déc.)	1A
Longueur : incluant les octets de type et de longueur	16
MSB (octet le plus significatif) de l'identifiant Fournisseur est toujours 00	00
Identifiant Fournisseur Sophos	00 15 34
Type de fournisseur : EF-User-Group	14
Informations sur la valeur	
Longueur du fournisseur : incluant les octets du type de fournisseur et de la longueur du fournisseur	0E
Texte : "WestCoastSales" (sans guillemets)	57 65 73 74 43 6F 61 73 74 53 61 6C 65 73

9.8 Sophos NAC Advanced en tant que proxy RADIUS (Windows Server 2008) (tâches facultatives)

Si vous utilisez Sophos NAC Advanced en tant que proxy RADIUS (configuration de Sophos NAC Advanced en mode proxy devant un autre serveur RADIUS), modifiez la configuration du Serveur de stratégie réseau (NPS). L'utilisation de Sophos NAC Advanced en tant que proxy RADIUS ne nécessite pas la création d'une stratégie réseau. Créez plutôt une stratégie de demande de connexion et utilisez un groupe de serveurs RADIUS à distance.

Remarque : répétez ces instructions sur tous les serveurs d'applications de conformité ainsi que sur tous les serveurs RADIUS Enforcer.

9.8.1 Ajout d'un groupe de serveurs RADIUS distant

1. Depuis le menu Démarrer du serveur d'applications de conformité ou du serveur RADIUS Enforcer, cliquez sur **Outils d'administration > Serveur de stratégie réseau**.

Le Serveur de stratégie du réseau s'ouvre.

2. Sous Clients et serveurs RADIUS, cliquez avec le bouton droit de la souris sur **Groupes de serveurs RADIUS distants** et cliquez sur **Nouveau**.

L'assistant Nouveau groupe de serveurs RADIUS distants apparaît.

3. Saisissez un nom de groupe de serveurs dans le champ approprié.
4. Cliquez sur **Ajouter**.
5. Saisissez l'adresse IP de votre serveur RADIUS distant dans le champ disponible.
6. Cliquez sur l'onglet **Authentification/Gestion des comptes**.
7. Saisissez et confirmez le secret partagé RADIUS dans les champs appropriés.
8. Si nécessaire, modifiez le port d'authentification et le port de gestion.

Remarque : par défaut, les ports d'authentification et de gestion RADIUS sont définis sur 1812 et 1813. Si vous utilisez d'autres ports d'authentification et de gestion, les ports d'authentification et de gestion doivent être modifiés. le port d'authentification le plus fréquemment utilisé est le port 1645 tandis que le port de gestion le plus fréquemment utilisé est le port 1646.

9. Cliquez sur l'onglet **Équilibrage de la charge**.
10. Définissez la priorité de votre serveur RADIUS distant dans le champ disponible.
11. Cliquez sur **OK**.
12. Répétez les étapes 4 à 11 pour créer des serveurs RADIUS supplémentaires pour le groupe.
13. Vérifiez les informations concernant le groupe de serveurs RADIUS distant et cliquez sur **OK**.
14. Rendez-vous sur [Création d'une Stratégie de demande de connexion](#) à la page 46.

9.8.2 Création d'une Stratégie de demande de connexion

Créez une Stratégie de demande de connexion lorsque vous utilisez Sophos NAC Advanced en tant que proxy RADIUS.

1. Depuis le menu Démarrer du serveur d'applications de conformité ou du serveur RADIUS Enforcer, cliquez sur **Outils d'administration > Serveur de stratégie réseau**.

Le Serveur de stratégie du réseau s'ouvre.

2. Sous Stratégies, cliquez avec le bouton droit de la souris sur **Stratégies de demande de connexion**, puis cliquez sur **Nouvelle**.

L'assistant Stratégie de demande de nouvelle connexion apparaît.

3. Saisissez un nom de stratégie et laissez **Non spécifié** comme méthode de connexion réseau.
4. Cliquez sur **Suivant** pour continuer.
5. Cliquez sur **Ajouter** pour spécifier les conditions appropriés de la stratégie.
6. Sélectionnez la condition appropriée, puis cliquez sur **Ajouter**.
7. Définissez la valeur de la condition et cliquez sur **OK**.

Remarque : par exemple, vous pouvez sélectionner le Nom utilisateur à l'étape précédente et définir qu'il contienne "mondomaine.com" à cette étape.

8. Cliquez sur **Suivant** pour continuer.
9. Dans la section **Authentification**, sélectionnez le bouton **Transfère les demandes de connexion à un groupe de serveurs RADIUS distant pour être authentifiée**.
10. Sélectionnez le groupe de serveurs RADIUS que vous avez créé dans la liste déroulante.

11. Cliquez sur **Suivant** pour continuer.
12. Dans la section **Attribut** sous **Spécifier un nom de domaine**, sélectionnez **Nom utilisateur** depuis la liste déroulante et cliquez sur **Ajouter**.
13. Dans le champ **Rechercher**, saisissez le(s) nom(s) de domaine que vous allez utiliser en tant que proxy ou un caractère joker .* si vous prévoyez d'utiliser tous les domaines en tant que proxy.
14. Ne remplissez pas le champ **Remplacer par**.
15. Cliquez sur **OK**.
16. Cliquez sur **Suivant** pour continuer.
17. Cliquez sur **Terminer**.
18. Rendez-vous sur [Vérification des conditions de la stratégie](#) à la page 47.

9.8.3 Vérification des conditions de la stratégie

1. Dans le Serveur de stratégie réseau, sous Stratégies, cliquez sur **Stratégies de demande de connexion**. Dans la liste des stratégies, cliquez avec le bouton droit de la souris sur la stratégie que vous venez de créer et sélectionnez **Propriétés**.

La fenêtre des Propriétés apparaît.

2. Cliquez sur l'onglet **Conditions** pour passer en revue les conditions de la stratégie que vous avez créée.
3. Si les conditions de la stratégie sont incorrectes ou incomplètes, cliquez sur **Ajouter** ou sur **Modifier** pour effectuer des changements.

Remarque : si vous devez créer une condition de stratégie pour que tous les utilisateurs soient mis en proxy, vous pouvez ajouter une condition Restrictions relatives aux jours et aux heures et la définir sur 24x7.

4. Cliquez sur **OK**.
5. Passez à la section [Modification du protocole d'authentification RADIUS dans l'interface d'enregistrement](#) à la page 47.

9.8.4 Modification du protocole d'authentification RADIUS dans l'interface d'enregistrement

Par défaut, Sophos NAC Advanced utilise MSchapV2 RADIUS comme protocole d'authentification par défaut. Si votre serveur RADIUS distant n'utilise pas ce protocole d'authentification, vous devez impérativement modifier le protocole d'authentification RADIUS dans l'interface d'enregistrement.

1. Recherchez le fichier Registration Interface Web.config pour l'interface d'enregistrement sur le serveur d'applications de conformité ou sur le serveur RADIUS Enforcer. Si vous avez installé le logiciel Sophos NAC Advanced dans l'emplacement par défaut, le fichier est disponible à l'emplacement suivant : *<lecteur local>*\inetpub\wwwroot\RegistrationInterface\web.config.
2. Ouvrez le fichier Web.config dans le Bloc-notes.
3. Recherchez la section **authInterface** et la sous-section **radius**.

4. Modifiez la valeur **mschapv2** sur cette ligne `<add key="authType" value="mschapv2" />` pour celle du protocole d'authentification RADIUS utilisé par votre serveur RADIUS distant.

La sous-section radius modifiée du fichier Registration Interface web.config doit apparaître ainsi :

```
<radius>

<add key="authType" value="votre protocole d'authentification
RADIUS distant"/>
<add key="serverRetries" value="1"/>
<add key="listRetries" value="1"/>
</radius>
```

5. Enregistrez et fermez le fichier.
6. Vous pouvez aussi choisir de vous rendre à la section [Configuration du serveur RADIUS pour les réorientations/profils de groupes \(tâche facultative\)](#) à la page 48.

9.8.5 Configuration du serveur RADIUS pour les réorientations/profils de groupes (tâche facultative)

Vous pouvez utiliser Sophos NAC Advanced ou le serveur RADIUS pour la réorientation de groupes. Pour ces deux configurations, créez des groupes à l'aide de Sophos NAC Advanced. Pour plus d'informations, reportez-vous à l'Aide de Compliance Manager.

Pour utiliser les réorientations/profils de groupes du serveur RADIUS avec Sophos NAC Advanced, envoyez les informations sur le groupe par le biais d'un paquet RADIUS vers Sophos NAC Advanced à l'aide d'un attribut spécifique d'un fournisseur (VSA). Pour de plus amples informations, reportez-vous à la documentation utilisateur de RADIUS pour savoir comment renvoyer un attribut spécifique d'un fournisseur.

Attribut spécifique d'un fournisseur Sophos (VSA)

La syntaxe d'un attribut spécifique d'un fournisseur repose sur les instructions décrites à la section 5.26 du document (URL RFC2685) "Remote Authentication Dial In User Service (RADIUS)" disponible sur Internet à <http://www.rfc-archive.org/getrfc.php?rfc=2865>.

Identifiant Fournisseur Sophos

L'identifiant Fournisseur identifie le fournisseur. L'identifiant du fournisseur Sophos est 5428 (décimal) ou 0x00001534 (hexadécimal, dans l'ordre du réseau).

Attribut EF-GroupID

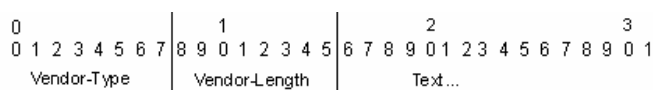
L'attribut spécifique d'un fournisseur EF-GroupID indique quel groupe est utilisé pour mettre en place les paramètres de la session pour un utilisateur identifié.

Les modèles d'accès RADIUS Enforcer déterminent l'accès réseau ; toutefois les exemptions sont considérées en priorité. Lorsqu'une requête est exemptée, l'accès au réseau est autorisé quel que soit le groupe. Le tableau suivant décrit les scénarios de spécification ou de non spécification d'une stratégie par défaut dans le Compliance Manager :

Scénarios	Stratégie par défaut spécifiée	Stratégie par défaut non spécifiée
L'attribut spécifique d'un fournisseur EF-GroupID n'est pas présent	La stratégie par défaut est appliquée. L'accès au réseau est déterminé lorsqu'un modèle d'accès RADIUS Enforcer correspond à la requête. Les modèles d'accès RADIUS Enforcer associés à la stratégie sont évalués en priorité. Si aucune correspondance n'est trouvée, les modèles d'accès RADIUS Enforcer par défaut sont évalués. Si aucune correspondance n'est trouvée, l'accès au réseau est refusé.	L'utilisateur ne reçoit pas la stratégie. L'accès au réseau est déterminé lorsqu'un modèle d'accès RADIUS Enforcer correspond à la requête. Les modèles d'accès RADIUS Enforcer par défaut sont évalués en priorité. Si aucune correspondance n'est trouvée, l'accès au réseau est refusé.
L'attribut spécifique d'un fournisseur EF-GroupID n'existe pas ou n'est pas défini.	La stratégie par défaut est appliquée. L'accès au réseau est déterminé lorsqu'un modèle d'accès RADIUS Enforcer correspond à la requête. Les modèles d'accès RADIUS Enforcer associés à la stratégie sont évalués en priorité. Si aucune correspondance n'est trouvée, les modèles d'accès RADIUS Enforcer par défaut sont évalués. Si aucune correspondance n'est trouvée, l'accès au réseau est refusé.	L'utilisateur ne reçoit pas la stratégie. L'accès au réseau est déterminé lorsqu'un modèle d'accès RADIUS Enforcer correspond à la requête. Les modèles d'accès RADIUS Enforcer par défaut sont évalués en priorité. Si aucune correspondance n'est trouvée, l'accès au réseau est refusé.
L'attribut spécifique d'un fournisseur EF-GroupID est valide	L'utilisateur est placé dans un groupe spécifié et la stratégie associée est appliquée. L'accès au réseau est déterminé lorsqu'un modèle d'accès RADIUS Enforcer correspond à la requête. Les modèles d'accès RADIUS Enforcer associés à la stratégie sont évalués en priorité. Si aucune correspondance n'est trouvée, les modèles d'accès RADIUS Enforcer par défaut sont évalués. Si aucune correspondance n'est trouvée, l'accès au réseau est refusé.	L'utilisateur est placé dans un groupe spécifié et la stratégie associée est appliquée. L'accès au réseau est déterminé lorsqu'un modèle d'accès RADIUS Enforcer correspond à la requête. Les modèles d'accès RADIUS Enforcer associés à la stratégie sont évalués en priorité. Si aucune correspondance n'est trouvée, les modèles d'accès RADIUS Enforcer par défaut sont évalués. Si aucune correspondance n'est trouvée, l'accès au réseau est refusé.

Format de l'attribut EF-GroupID

Le format des informations sur la valeur de l'attribut spécifique d'un fournisseur EF-GroupID est décrit dans le diagramme et le tableau ci-dessous. Les champs sont transmis de la gauche vers la droite.



Type de fournisseur	Longueur du fournisseur	Texte
20 (14 hex) pour EF-User-Group	>2	<p>Le champ de texte est compris entre un ou plusieurs octets de caractères lisibles par l'œil humain. Il ne doit pas se terminer par un zéro. La valeur de ce champ de texte détermine un Groupe d'utilisateurs particulier pour la session de l'utilisateur identifié.</p> <p>Paramètres du texte de l'identifiant du Groupe d'utilisateurs :</p> <ul style="list-style-type: none"> ■ Maximum de 253 caractères pouvant contenir une combinaison de chiffres et de lettres. Aucun autre caractère n'est autorisé. ■ Non sensible aux majuscules. ■ Espaces non autorisés.

Exemple d'attribut EF-User-Group

Si, par exemple, l'attribut spécifique d'un fournisseur est paramétré sur EF-User-Group = "WestCoastSales", il comprend des chiffres hexadécimaux (ordre du réseau) décrit dans le tableau suivant :

Description	Chiffres hexadécimaux
Informations d'en-tête	
Saisissez : attribut RADIUS 26 (déc.)	1A
Longueur : incluant les octets de type et de longueur	16
MSB (octet le plus significatif) de l'identifiant Fournisseur est toujours 00	00
Identifiant Fournisseur Sophos	00 15 34
Type de fournisseur : EF-User-Group	14
Informations sur la valeur	

Description	Chiffres hexadécimaux
Longueur du fournisseur : incluant les octets du type de fournisseur et de la longueur du fournisseur	0E
Texte : "WestCoastSales" (sans guillemets)	57 65 73 74 43 6F 61 73 74 53 61 6C 65 73

9.9 Configuration de plusieurs serveurs d'applications (tâches facultatives)

La présence de plusieurs serveurs d'applications de conformité permet à Sophos NAC Advanced de s'adapter. Installez et configurez correctement tous les serveurs d'applications de conformité supplémentaires afin que ceux-ci soient identiques au serveur d'applications de conformité principal. Pour LDAP, si vous voulez réutiliser un fichier de configuration sur plusieurs serveurs, exécutez l'outil de chiffrement de mots de passe sur chaque serveur pour mettre à jour et chiffrer le mot de passe Bind. Le chiffrement du mot de passe Bind est spécifique au serveur.

Les tâches suivantes sont requises en présence de plusieurs serveurs d'applications de conformité :

- Exportation et importation de la clé serveur sur des serveurs d'applications de conformité supplémentaires. Pour plus d'informations, reportez-vous à la section [Exportation et importation de la clé du serveur sur des serveurs d'applications de conformité supplémentaires](#), à la page 51.
- Configuration du Round Robin DNS sur Microsoft Windows[®] Server 2003 lorsque d'autres logiciels ou appliances d'équilibrage de charge ne sont pas utilisés. Pour plus d'informations, reportez-vous à la section [Configuration du Round Robin DNS sur Windows Server 2003 et supérieur](#) à la page 52.

9.9.1 Exportation et importation de la clé du serveur sur des serveurs d'applications de conformité supplémentaires.

Si vous avez plusieurs serveurs d'applications de conformité, la paire de clés publique/privée doit être synchronisée sur tous les serveurs d'applications de conformité participants. Pour plus d'informations, reportez-vous à l'Aide du Compliance Manager.

1. Sur le serveur d'applications de conformité principal, ouvrez une session sur le Compliance Manager.
2. Cliquez sur **Configure System > Server Key**.
3. Exportez la paire de clés publique/privée.
4. Sur un autre serveur d'applications de conformité, ouvrez une session sur le Compliance Manager et cliquez sur **Configure System > Server Key**.
5. Importez la paire de clés publique/privée.
6. Répétez les étapes 4 et 5 pour tous les serveurs d'applications de conformité supplémentaires.

9.9.2 Configuration du Round Robin DNS sur Windows Server 2003 et supérieur

La configuration du Round Robin DNS sur Microsoft Windows Server 2003 et supérieur permet de répartir les évaluations sur plusieurs serveurs tout en maintenant une structure unique de groupes, de stratégies et d'applications dans Sophos NAC Advanced. Le Round Robin DNS est une fonction d'équilibrage de charge des serveurs DNS qui permet la distribution de ressources par plusieurs serveurs. La présente section donne un exemple simple de configuration de la fonction Round Robin du service de nom de domaine (DNS) de Microsoft Windows Server. Les autres serveurs de nom de domaine prenant en charge le Round Robin doivent fonctionner de la même manière.

Remarque : cette tâche n'est pas nécessaire en cas d'utilisation d'un logiciel d'équilibrage de charge.

1. Depuis le menu Démarrer du serveur Windows exécutant le service de nom de domaine, cliquez sur **Outils d'administration > DNS**
La fenêtre de gestion de DNS apparaît.
2. Développez l'arborescence DNS.
3. Cliquez avec le bouton droit de la souris sur le nom du serveur et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Avancé**.
5. Sélectionnez la case à cocher **Activer la fonction Round Robin**.
6. Cliquez sur **OK** pour enregistrer vos modifications.
7. Développez le dossier **Zones de recherche directes**, cliquez avec le bouton droit de la souris sur le domaine dans lequel les serveurs d'applications de conformité sont configurés et sélectionnez **Nouvel hôte (A)...**
8. Saisissez le nom d'hôte et l'adresse IP du serveur d'applications de conformité principal que vous avez installé et configuré et cliquez sur **Ajouter un hôte**.
Remarque : le nom d'hôte que vous saisissez devient une partie de l'hôte de l'URL que vous voulez que les agents utilisent. Par exemple, si vous ajoutez sophosapp en tant que nouvel hôte, le nom de domaine pleinement qualifié devient `sophosapp.endpointsoftware.info`.
9. Cliquez sur **OK** pour confirmer l'ajout du nom d'hôte et de l'adresse IP.
10. Répétez l'étape 8 pour chaque serveur d'applications de conformité supplémentaire.
Remarque : pour un bon fonctionnement du Round Robin DNS, le nom d'hôte doit être identique pour tous les serveurs d'applications de conformité. Par exemple, le nom d'hôte du serveur d'applications de conformité principal est `sophosapp`. Par conséquent, tous les serveurs d'applications de conformité supplémentaires doivent avoir `sophosapp` comme nom d'hôte.
11. Cliquez sur **Terminé** pour revenir à la fenêtre de gestion de DNS.

Par exemple, la demande d'un nom de domaine entièrement qualifié `sophosapp.endpointsoftware.info` retourne une des trois adresses IP du serveur d'applications de conformité suivantes : 10.0.224.102, 10.0.224.103 ou 63.110.105.174. Un agent configuré avec ce domaine pourra communiquer avec tous les serveurs d'applications de conformité.

10 Installation de l'agent temporaire

L'agent temporaire s'adresse aux utilisateurs qui n'ont pas installé ou ne peuvent pas installer l'agent sur un ordinateur d'extrémité, comme les sous-traitants ou les invités. Pour plus d'informations sur la personnalisation de l'agent temporaire, reportez-vous au *Guide de configuration de l'agent de Sophos NAC Advanced*.

10.1 Configuration requise de l'agent temporaire

Pour voir la configuration requise, allez sur la page des différentes configurations requises sur le site Web de Sophos (<http://www.sophos.fr/products/all-sysreqs.html>).

10.2 Installation de l'agent temporaire sur un serveur Web

Pour pouvoir utiliser l'agent temporaire, vous devez d'abord installer l'agent temporaire sur un serveur Web Windows accessible aux utilisateurs. L'agent temporaire peut être installé sur le même serveur que le serveur d'applications de conformité. Dès qu'il est installé, les utilisateurs peuvent télécharger l'agent temporaire à l'aide d'un navigateur.

1. Téléchargez l'Sophos Compliance Dissolvable Agent depuis le site Web de Sophos. Autrement, insérez le CD-ROM Sophos Install CD. Le CD-ROM doit se lancer automatiquement.
2. Cliquez deux fois sur le fichier d'installation de l'Sophos Compliance Dissolvable Agent pour lancer l'installation de l'agent temporaire.
3. Cliquez sur **Next** pour continuer.
4. Lisez le Contrat de licence Utilisateur Final, sélectionnez le bouton **I Accept the terms of the License Agreement**, et cliquez sur **Next** pour continuer.
5. Cliquez sur **Change** pour sélectionner le bon répertoire d'installation ou continuez avec le répertoire par défaut : c:\Inetpub\wwwroot. Cliquez sur **Next** pour continuer.
6. Saisissez l'adresse IP ou le nom DNS du serveur d'applications de conformité Sophos.

Remarque : si Sophos NAC Advanced a été installé sur plusieurs serveurs, l'adresse du serveur est soit l'adresse IP, soit le nom DNS du serveur d'applications de conformité mais pas le serveur de base de données de conformité. Si vous avez plusieurs serveur d'applications de conformité, saisissez le nom d'hôte qui représente l'ensemble des serveurs d'applications de conformité. Si vous modifiez l'adresse du serveur après avoir installé l'agent temporaire, vous devez réinstaller l'agent temporaire sur le serveur Web et précisez la nouvelle adresse du serveur d'applications de conformité Sophos au cours de l'installation.

7. Si vous testez ou évaluez Sophos NAC Advanced, désélectionnez la case **Secure Sophos Server (use HTTPS)**.
8. La case **Always register agent with server** n'est pas sélectionnée par défaut. Si vous souhaitez que vos utilisateurs s'enregistrent lorsqu'ils utilisent l'agent temporaire, sélectionnez-la. Cliquez sur **Next** pour continuer.

Remarque : si vous désélectionnez la case Always register agent with server, vous devez modifier le paramètre d'enregistrement de l'agent temporaire sur On dans le Compliance Manager.

9. Cliquez sur **Install** pour commencer l'installation.
10. Cliquez sur **Finish** pour finir l'installation.

Remarque :

- En cas d'erreurs lors de l'installation, consultez le journal des événements (Event Log) sur le serveur Web pour obtenir plus d'informations.
- Les ordinateurs d'extrémité ont accès à l'agent temporaire par le biais de l'URL `http(s)://<adresse ip/nom DNS>/dissolvableagent` si vous installez l'agent temporaire dans le répertoire par défaut. L'adresse IP ou le nom DNS correspond au serveur Web sur lequel vous avez installé l'agent temporaire.

Important : l'agent temporaire ne peut pas effectuer l'évaluation des correctifs si l'utilisateur est connecté en tant qu'utilisateur avec restrictions. Connectez-vous en tant qu'administrateur. Si ce changement n'est pas possible, Sophos vous conseille de créer une stratégie distincte pour les utilisateurs de l'agent temporaire. Cette stratégie ne doit pas contenir de correctifs, en revanche, elle doit contenir le profil Windows Update. Ce profil garantit que l'outil Windows Update est installé et que les Mises à jour automatiques sont activées.

11 Désinstallation de l'agent temporaire du serveur Web

Utilisez ces étapes pour désinstaller le composant serveur de l'agent temporaire depuis un serveur Web. Si vous désinstallez l'agent temporaire du serveur Web, les utilisateurs ne pourront pas télécharger l'agent temporaire.

1. Depuis le menu Démarrer, sélectionnez **Panneau de configuration > Ajouter ou supprimer des programmes**.
2. Sélectionnez **Sophos Compliance Dissolvable Agent**, puis cliquez sur **Supprimer**.
3. Cliquez sur **Oui** pour confirmer la suppression du agent temporaire.

12 Déploiement de l'agent

Dès que vous terminés avec les instructions de la section *Configuration requise suite à l'installation* du présent document, vous pouvez installer les agents de conformité sur les ordinateurs d'extrémité.

12.1 Configuration requise

Pour voir la configuration requise, allez sur la page des différentes configurations requises sur le site Web de Sophos (<http://www.sophos.fr/products/all-sysreqs.html>).

12.2 Installation de l'agent

L'installation de l'agent utilise toutes les valeurs d'une installation précédente si cette installation existe. Les droits administratifs sont nécessaires sur l'ordinateur d'extrémité pour pouvoir installer l'agent ; toutefois, après l'installation, l'interface de l'agent fonctionne sous n'importe quel mode utilisateur, y compris le mode utilisateur restreint. Suite à l'installation, l'agent apparaît dans la fenêtre Ajouter ou Supprimer des programmes depuis le Panneau de configuration de Microsoft Windows, en revanche, il n'apparaît pas dans le menu Démarrer de Microsoft Windows.

Options de configuration de l'installation de l'agent

Vous pouvez configurer l'installation de l'agent grâce à des options par lignes de commande spécifiques.

- Pour installer l'Agent de quarantaine et préciser le mode d'enregistrement, utilisez la commande suivante : `msiexec /i "<chemin complet du fichier d'installation de l'agent>" AGENT_SETTINGS="Register=<mode d'enregistrement>"`. Si le mode d'enregistrement n'est pas spécifié, la demande est utilisée par défaut.

Remarque : les modes d'enregistrement disponibles de l'agent sont `always`, `demand`, `nopassword` et `usecomputerlogon`. Pour plus d'informations, reportez-vous au *Guide de bon usage de Sophos NAC Advanced*.

- Pour configurer l'adresse IP ou le nom DNS et le mode (HTTP ou HTTPS) du serveur d'applications de conformité avec lequel l'agent communique, utilisez la commande suivante : `msiexec /i "<chemin complet du fichier d'installation de l'agent>" AGENT_SERVER=<Adresse IP ou nom DNS> AGENT_SERVERMODE=<http ou https>`. Si le mode n'est pas spécifié, HTTPS est utilisé par défaut.
- Pour configurer une classe utilisateur DHCP, utilisez la commande suivante : `msiexec /i "<chemin complet du fichier d'installation de l'agent>" AGENT_DHCPCLASS=<classe utilisateur>`. La classe utilisateur DHCP est utilisée pour l'application du protocole DHCP lorsque vous n'utilisez pas le DHCP Enforcer de NAC.

Par exemple, `msiexec /i "c:\SophosComplianceAgent.msi" AGENT_INSTALLTYPE=quarantine AGENT_SETTINGS="Register=usecomputerlogon" AGENT_SERVER=appserver AGENT_SERVERMODE=https` installe l'Agent de quarantaine à l'aide du paramètre d'enregistrement Use Computer Logon à partir du fichier d'installation de l'agent se trouvant sur le lecteur C et indique que l'agent va communiquer via HTTPS avec le serveur d'applications de conformité dont le nom DNS est "appserver".

Pour installer l'agent :

1. Téléchargez Sophos Compliance Agent depuis le site Web de Sophos.
Autrement, insérez le CD-ROM Sophos Install CD. Le CD-ROM doit se lancer automatiquement.
2. Cliquez deux fois sur le fichier d'installation de Sophos Compliance Agent.
3. Cliquez sur **Next** pour lancer l'assistant.
4. Lisez le Contrat de licence Utilisateur Final, sélectionnez le bouton **I Accept the terms of the License Agreement**, et cliquez sur **Next** pour continuer.
5. Saisissez l'adresse IP ou le nom DNS du serveur d'applications de conformité.
6. Si vous testez ou évaluez Sophos NAC Advanced, désélectionnez la case **Secure Sophos Server (use HTTPS)**. Cliquez sur **Next** pour continuer.

Remarque : si Sophos NAC Advanced a été installé sur plusieurs serveurs, l'adresse du serveur est soit l'adresse IP, soit le nom DNS du serveur d'applications de conformité mais pas le serveur de base de données de conformité. Si vous avez plus d'un serveur d'applications de conformité, saisissez le nom d'hôte qui représente l'ensemble des serveurs d'applications de conformité.

7. Cliquez sur **Change** pour sélectionner le bon répertoire d'installation ou continuez avec le répertoire par défaut et cliquez sur **Next** pour continuer.
8. Cliquez sur **Install** pour commencer l'installation. Pour annuler l'installation, cliquez sur **Cancel**.

Remarque : sur les installations Windows 2000, la boîte de dialogue Pilote non signé apparaît sauf si le Service Pack 3 ou supérieur est installé. Ce comportement est dû à la manière dont est générée la signature par le laboratoire Windows Hardware Quality Lab (WHQL). Sur les installations Windows XP, la boîte de dialogue Pilote non signé peut apparaître si le Service Pack 1 est installé, en revanche, elle ne devrait pas apparaître si le Service Pack 1a, Service Pack 2 ou aucun Service pack n'est installé.

9. Cliquez sur **Finish** pour finir l'installation.
Suite à l'installation de l'agent, il se peut que vous deviez redémarrer le système d'extrémité pour les raisons suivantes.
 - Au cours de l'installation, vous avez été invité à fermer les applications qui utilisaient des ressources partagées, comme XMLDOM, et vous avez décidé de ne pas fermer ces applications.
 - Vous mettez à niveau l'Agent de quarantaine et cette mise à niveau utilise une nouvelle version (pilote du noyau) du Gestionnaire de l'agent de quarantaine.

13 Désinstallation de l'agent

Important : au cours de la désinstallation de l'agent, il se peut qu'une boîte de dialogue de l'Explorateur Windows apparaisse et vous demande de fermer certaines applications, comme un client de messagerie, avant de procéder à la désinstallation de l'agent. Nous vous conseillons de fermer les applications pour que la désinstallation se déroule avec succès. La désinstallation de l'agent nécessite également le redémarrage de l'ordinateur d'extrémité.

1. Depuis le menu Démarrer, sélectionnez **Panneau de configuration > Ajouter ou supprimer des programmes**.
2. Sélectionnez **Sophos Compliance Agent**, puis cliquez sur **Supprimer**.
3. Cliquez sur **Oui** pour confirmer la suppression de l'agent.

14 Paramètres optionnels

Cette section contient les paramètres optionnels pour Sophos NAC Advanced. La mise en place de Sophos NAC Advanced peut nécessiter d'effectuer toutes les tâches suivantes ou certaines d'entre elles.

14.1 Vérification/modification de la tâche Patch Loader

La tâche Patch Loader est planifiée par défaut pour s'exécuter tous les jours et de manière aléatoire. Cette tâche récupère les définitions des correctifs les plus récents depuis Sophos et exige l'accès à Internet.

1. Depuis le menu Démarrer du serveur d'applications de conformité, cliquez sur **Panneau de configuration** > **Tâches planifiées** .

La fenêtre Tâches planifiées apparaît.

2. Cliquez deux fois sur **Sophos NAC PatchLoader**. La fenêtre des Propriétés apparaît.
3. Cliquez sur l'onglet **Planification**.
4. Modifiez l'heure de la tâche planifiée à votre convenance et cliquez sur **OK**.
5. Cliquez sur **OK** pour enregistrer vos modifications.
6. Quittez les Tâches planifiées.

14.2 Exécution manuelle de la tâche Patch Loader

La tâche Patch Loader est planifiée par défaut pour s'exécuter tous les jours de manière aléatoire. Toutefois, vous pouvez exécuter manuellement la tâche Patch Loader. Cette tâche récupère les définitions des correctifs les plus récents depuis Sophos et exige l'accès à Internet.

1. Depuis le menu Démarrer du serveur d'applications de conformité, cliquez sur **Panneau de configuration** > **Tâches planifiées** .

La fenêtre Tâches planifiées apparaît.

2. Cliquez avec le bouton droit de la souris sur **Sophos NAC PatchLoader** et sélectionnez **Exécuter**.
3. Quittez les Tâches planifiées.

14.3 Vérification/modification de la tâche Current Definition Loader

La tâche Current Definition Loader est planifiée pour s'exécuter toutes les heures. L'installation de Sophos NAC Advanced planifie cette tâche pour qu'elle s'exécute de manière aléatoire. Celle-ci se déroule en quelques minutes et nécessite l'accès à Internet. Cette tâche récupère depuis Sophos les mises à jour les plus récentes des signatures virales à destination des applications antivirus et antispywares.

1. Depuis le menu Démarrer du serveur d'applications de conformité, cliquez sur **Panneau de configuration** > **Tâches planifiées** .

La fenêtre Tâches planifiées apparaît.

2. Cliquez deux fois sur **Sophos NAC CurrentDefsLoader**. La fenêtre des Propriétés apparaît.
3. Cliquez sur l'onglet **Planification**.
4. Cliquez sur **Avancé**.
5. Modifiez l'heure de la tâche planifiée et cliquez sur **OK**.
6. Cliquez sur **OK** pour enregistrer vos modifications.
7. Quittez les Tâches planifiées.

14.4 Exécution manuelle de la tâche Current Definition Loader

La tâche Current Definition Loader est planifiée pour s'exécuter toutes les heures ; toutefois, vous pouvez aussi exécuter manuellement la tâche Current Definition Loader. L'installation de Sophos NAC Advanced planifie cette tâche pour qu'elle s'exécute de manière aléatoire. Celle-ci se déroule en quelques minutes et nécessite l'accès à Internet. Cette tâche récupère depuis Sophos les mises à jour les plus récentes des signatures virales à destination des applications antivirus et antispywares.

1. Depuis le menu Démarrer du serveur d'applications de conformité, cliquez sur **Panneau de configuration > Tâches planifiées**.

La fenêtre Tâches planifiées apparaît.

2. Cliquez avec le bouton droit de la souris sur **Sophos NAC CurrentDefsLoader** et sélectionnez **Exécuter**.
3. Quittez les Tâches planifiées.

14.5 Vérification/modification de la tâche Report Warehouse Loader

La tâche Report Warehouse Loader est planifiée par défaut pour s'exécuter à 02:30 du matin tous les jours ; toutefois, vous pouvez aussi exécuter manuellement cette tâche. Cette tâche contrôle l'heure à laquelle les données de rapports sont archivées et purgées des données des rapports.

1. Depuis le menu Démarrer du SQL Server, procédez de l'une des manières suivantes :
 - Si vous utilisez SQL Server 2000, cliquez sur **Microsoft SQL Server > Enterprise Manager**. SQL Enterprise Manager s'ouvre.
 - Si vous utilisez SQL Server 2005 ou supérieur, cliquez sur **Microsoft SQL Server (version) > SQL Server Management Studio**. SQL Server Management Studio s'ouvre.
2. Recherchez l'**Agent SQL Server**.

Remarque : si vous utilisez SQL Server 2000, l'Agent SQL Server est sous le dossier Gestion.
3. Sous l'Agent SQL Server, sélectionnez **Travaux**.
4. Cliquez deux fois sur la tâche **Sophos NAC - LoadWH**. La fenêtre des Propriétés apparaît.
5. Procédez de l'une des manières suivantes :
 - Si vous utilisez SQL Server 2000, cliquez sur l'onglet **Planification**.
 - Si vous utilisez SQL Server 2005 ou supérieur, cliquez sur **Planification**.

6. Procédez de l'une des manières suivantes :
 - Cliquez sur **Nouvelle planification** (SQL Server 2000) ou sur **Nouveau** (SQL Server 2005 ou supérieur) pour ajouter une nouvelle planification, et une fois que vous l'avez ajoutée, cliquez sur **OK**.
 - Cliquez sur **Modifier** pour modifier la planification existante et cliquez sur **OK**.

Remarque : vous pouvez modifier l'heure à laquelle les données des rapports sont déplacées dans les rapports archivés et/ou vous pouvez définir d'autres tâches pour déplacer plusieurs fois par jour les données des rapports dans les rapports archivés.
7. Cliquez sur **OK** pour enregistrer vos modifications.
8. Quittez SQL Enterprise Manager ou SQL Server Management Studio.

14.6 Exécution manuelle de la tâche Report Warehouse Loader

La tâche Report Warehouse Loader contrôle le moment auquel les données de rapports sont archivées et purgées. Elle est paramétrée par défaut pour s'exécuter tous les jours à 2:30 du matin. Toutefois, vous pouvez également exécuter manuellement la tâche Report Warehouse Loader.

1. Depuis le menu Démarrer du SQL Server, procédez de l'une des manières suivantes :
 - Si vous utilisez SQL Server 2000, cliquez sur **Microsoft SQL Server > Enterprise Manager**. SQL Enterprise Manager s'ouvre.
 - Si vous utilisez SQL Server 2005 ou supérieur, cliquez sur **Microsoft SQL Server (version) > SQL Server Management Studio**. SQL Server Management Studio s'ouvre.
2. Recherchez l'**Agent SQL Server**.

Remarque : si vous utilisez SQL Server 2000, l'Agent SQL Server est sous le dossier Gestion.
3. Sous l'Agent SQL Server, sélectionnez **Travaux**.
4. Cliquez avec le bouton droit de la souris sur **Sophos NAC - LoadWH** et sélectionnez **Démarrer le travail**.

Remarque : le temps d'exécution manuelle de la tâche Sophos NAC - LoadWH est approximativement le même que celui de l'exécution automatique toutes les nuits.
5. Quittez SQL Enterprise Manager ou SQL Server Management Studio.

14.7 Désactivation de HTTPS pour tests en environnements hors production

Sophos NAC Advanced utilise HTTPS pour protéger les noms utilisateur, mots de passe et toutes autres données sensibles dans un environnement de production. Dans certains cas, tout particulièrement à des fins de tests et d'évaluations, il se peut qu'il soit nécessaire de désactiver HTTPS.

1. Depuis le menu Démarrer du serveur d'applications de conformité, cliquez sur **Outils d'administration > Gestionnaire des services Internet (IIS)**.
Le Gestionnaire des services Internet s'ouvre.

2. Ouvrez le dossier **Sites Web** et ouvrez le dossier **Site Web par défaut**.
3. Cliquez avec le bouton droit de la souris sur **RegistrationInterface** et sélectionnez **Propriétés**.
La fenêtre des Propriétés de RegistrationInterface apparaît.
4. Cliquez sur l'onglet **Sécurité de répertoire**.
5. Dans la zone **Communications sécurisées**, cliquez sur **Modifier**.
La fenêtre Communications sécurisées apparaît.
6. Dessélectionnez la case **Requérir un canal sécurisé (SSL)**.
7. Cliquez sur **OK** pour retourner dans la fenêtre des Propriétés de RegistrationInterface et cliquez sur **OK** pour retourner dans le Gestionnaire des services Internet (IIS).
8. Répétez les étapes 2 à 6 pour PolicyInterface et ReportInterface, et ServerStatusInterface.
9. Quittez le Gestionnaire des services Internet (IIS).

15 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.

16 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.

OpenSSL cryptographic toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL license

Copyright © 1998-2011 The OpenSSL Project. Tous droits réservés.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)”

4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,

PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”

The word “cryptographic” can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

“This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER

IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]