

SOPHOS

simple + secure

Sophos NAC Advanced Guide de résolution des problèmes

Version du produit : 3.2

Date du document : avril 2011



Table des matières

1 Problèmes d'installation.....	3
2 Problèmes du Compliance Manager.....	4
3 Problèmes de journalisation.....	7
4 Problèmes de communication serveur (depuis l'agent).....	8
5 Problèmes avec le client VPN.....	11
6 Problèmes de stratégies.....	12
7 Problèmes d'enregistrement.....	19
8 Problèmes de rapports.....	21
9 Problèmes relatifs aux alertes.....	23
10 Problèmes de serveur.....	24
11 Problèmes d'application.....	26
12 Problèmes relatifs aux applications tierces.....	34
13 Support technique.....	35
14 Mentions légales.....	36

1 Problèmes d'installation

Cette section contient des informations pour résoudre les problèmes d'installation de Sophos NAC Advanced.

1.1 Installation des bases de données de conformité

L'installation des bases de données de conformité échoue

Cause : le compte utilisé pour l'installation ne dispose pas des droits d'administrateur local sur les bases de données de conformité.

Solution : ouvrez une session à l'aide d'un compte disposant des droits administrateur.

Cause : au cours de l'installation, une fenêtre affiche les messages suivants : "Failed to load the test rule file" avec un nom de fichier XML et "Cursor operation conflict." Ce message apparaît parce que l'attribut "No count" est activé pour les connexions au serveur SQL.

Solution :

1. Ouvrez Microsoft SQL Server Enterprise Manager et recherchez le serveur SQL sur lequel l'installation a échoué.
2. Cliquez avec le bouton droit de la souris sur le serveur SQL et sélectionnez **Properties**.
3. Cliquez sur l'onglet **Connections**.
4. Dans la liste **Attribute**, recherchez l'attribut "No count" et désélectionnez la case à cocher.
5. Cliquez sur **OK**.

1.2 Déploiement de l'agent

L'installation de l'agent échoue

Cause : le compte utilisé pour l'installation ne dispose pas des droits d'administrateur local.

Résolution : assurez-vous que le compte permettant d'installer l'agent dispose des droits d'administrateur local.

2 Problèmes du Compliance Manager

Cette section contient des informations pour résoudre les problèmes relatifs au Compliance Manager.

2.1 Connexion ou installation

Connexion impossible au Compliance Manager

Cause : l'administrateur ne peut pas ouvrir de session sur le Compliance Manager.

Solution :

1. Assurez-vous d'être en mesure de contacter le Serveur d'applications de conformité.
2. Si des comptes sont gérés dans le Compliance Manager et pas dans une banque d'utilisateurs externe, assurez-vous que le nom et le mot de passe du compte sont valides.

Remarque : utilisez **admin** et un mot de passe de votre choix la première fois que vous ouvrez une session sur le Compliance Manager.

3. Si vous utilisez une banque d'utilisateurs externe pour la gestion des comptes, vérifiez que celui utilisé pour le compte Compliance Manager est du même type que celui utilisé pour l'authentification de l'agent. S'ils ne sont pas du même type, créez une stratégie de demande de connexion et classez-la en priorité. Pour plus d'informations, reportez-vous au *Guide d'installation de Sophos NAC Advanced*.
4. Il se peut que les droits n'aient pas été configurés correctement pour les applications Sophos dans les bases de données de conformité. Pour plus d'informations, reportez-vous au problème "Échec de connexion de tous les composants du Serveur d'applications de conformité ou du serveur RADIUS aux bases de données de conformité" de la section [Serveur SQL](#) à la page 25.

Cause : le service d'état ASP.NET ne fonctionne pas.

Solution : paramétrez le service d'état ASP.NET sur automatique et démarrez-le.

2.2 Compliance Manager

Certaines fenêtres n'apparaissent pas dans le Compliance Manager

Cause : si le bloqueur de fenêtres intempestives est activé, certaines tâches, telles que l'impression d'un rapport ou la consultation de l'aide en ligne, sont limitées dans le Compliance Manager.

Solution : désactivez le bloqueur de fenêtres intempestives pendant l'utilisation du Compliance Manager.

Des pages n'apparaissent pas correctement dans le Compliance Manager

Cause : le Compliance Manager est utilisé avec Internet Explorer 6.x et n'a pas été ajouté comme site Web de confiance.

Solution : ajoutez le Compliance Manager comme site Web de confiance dans Internet Explorer. Ce paramètre n'est pas nécessaire pour Internet Explorer 7.x.

Impossible d'exécuter les fonctions de création, de modification ou de configuration dans le Compliance Manager

Cause : les bases de données de conformité sont indisponibles.

Solution :

1. Assurez-vous que les bases de données de conformité fonctionnent correctement.
2. Assurez-vous que le service du serveur SQL est démarré correctement et que le mot de passe du compte de service de Sophos NAC Advanced utilisé pour lancer l'instance du serveur SQL est le même que celui créé avant l'installation de Sophos NAC Advanced.

Cause : l'installation du Serveur d'applications de conformité ne s'est pas terminée avec succès.

Solution : recherchez dans le journal des événements du Serveur d'applications de conformité toute erreur d'installation et terminez l'installation du Serveur d'applications de conformité.

Aucun correctif n'est disponible

Cause : si aucun correctif ne figure dans la page de liste des correctifs du Compliance Manager, c'est que la tâche Patch Loader n'est pas parvenue à charger les correctifs.

Solution : à l'aide de la commande Server Task Status sur la page d'accueil du Compliance Manager, vérifiez que la tâche Patch Loader a bien échoué et consultez-en la raison. Les causes les plus vraisemblables de cet échec sont soit que le Serveur d'applications de conformité n'a pas d'accès en sortie à Internet (ce qui est nécessaire pour Patch Loader) soit que le serveur proxy n'est pas configuré ou pas configuré correctement. Exécutez manuellement la tâche Patch Loader sur le Serveur d'applications de conformité pour télécharger et mettre à jour les informations sur les correctifs. Configurez votre serveur proxy. Pour plus d'informations, reportez-vous au *Guide d'installation de Sophos NAC Advanced*.

Les dates des fichiers signatures des applications antivirus ou antispywares semblent être obsolètes

Cause : le dernier fichier de signatures n'a pas été récupéré par la tâche Current Definition Loader.

Solution : à l'aide de la commande Server Task Status sur la page d'accueil du Compliance Manager, vérifiez que la tâche Current Definition Loader a bien échoué et consultez-en la raison. Les causes les plus vraisemblables de cet échec sont soit que le Serveur d'applications de conformité n'a pas d'accès en sortie à Internet (ce qui est nécessaire pour Current Definition Loader) soit que le serveur proxy n'est pas configuré ou pas configuré correctement. Exécutez manuellement la tâche Current Definition Loader sur le Serveur d'applications de conformité pour télécharger et mettre à jour les informations sur la date des signatures de l'application. Configurez Sophos NAC Advanced en tant que serveur proxy RADIUS. Pour plus d'informations, reportez-vous au *Guide d'installation de Sophos NAC Advanced*.

Les noms des applications n'apparaissent pas de manière appropriée dans le Compliance Manager

Cause : la prise en charge des langues d'Asie de l'Est n'est pas installée.

Solution : assurez-vous d'avoir bien installé les fichiers de prise en charge des langues d'Asie Orientale (via le Panneau de configuration > Options régionales et linguistiques) sur la machine depuis laquelle vous consultez le Compliance Manager.

L'utilisation des boutons du navigateur produit une erreur

Cause : vous utilisez les boutons du navigateur Web pour naviguer.

Solution : l'utilisation des boutons du navigateur Web pour naviguer dans le Compliance Manager n'est **pas** prise en charge. La navigation et les fonctions doivent être exécutées à l'aide des options de menu, des liens et des boutons disponibles sur chaque page.

Vous ne voyez pas toutes les fonctionnalités ou toutes les actions d'actualisation d'une application.

Cause : les fonctionnalités ou actions d'actualisation ne sont pas prises en charge pour cette version de l'application ou pour tous les systèmes d'exploitation.

Solution : la disponibilité des fonctionnalités d'une application et des actions d'actualisation dépend de la conception du logiciel de cette application. Il se peut que certaines fonctionnalités et actions d'actualisation ne soient pas disponibles pour certains systèmes d'exploitation prenant en charge l'application ou pour toutes les versions d'une application. Si une fonctionnalité n'est pas prise en charge, elle n'apparaît pas. Si une fonctionnalité est prise en charge sur certains systèmes d'exploitation mais pas sur d'autres, seuls les systèmes d'exploitation pris en charge apparaissent. Si une action d'actualisation est prise en charge sur certains systèmes d'exploitation mais pas sur d'autres, les systèmes d'exploitation non pris en charge apparaissent avec un x.

Avant de déployer la stratégie, nous vous conseillons de la tester pour vous assurer que l'application, les règles de détection des applications, les paramètres du profil et de la stratégie que vous avez sont corrects.

Vous ne voyez pas toutes les fonctionnalités d'un profil

Cause : toutes les fonctionnalités ne tiennent pas sur la page du Compliance Manager.

Solution : développez l'arborescence située près de l'en-tête pour voir les fonctionnalités sur la page Web.

3 Problèmes de journalisation

Cette section contient des informations pour résoudre les problèmes relatifs à la journalisation.

3.1 Journalisation de l'agent

Les fichiers journaux de l'agent ne sont pas présents pour l'Agent de quarantaine

Cause : la journalisation n'est pas activée.

Solution : activez la journalisation sur l'agent en sélectionnant la case à cocher Activer la journalisation dans la boîte de dialogue A propos de. Si elle n'est pas spécifiée dans le modèle de configuration d'agent appliqué à la stratégie de l'ordinateur d'extrémité, la journalisation est automatiquement définie au niveau 1 (messages d'erreur et d'avertissement).

Remarque : la journalisation affecte les performances. Nous conseillons par conséquent d'activer la journalisation uniquement pour la résolution des problèmes et de la désactiver lorsque la résolution des problèmes est terminée. Les fichiers journaux de Windows 2000 et Windows XP sont placés dans le répertoire <lecteur>:\Documents and Settings\All Users\Application Data\Sophos\Sophos NAC\Logs et ceux de Windows Vista et Windows 7 dans le répertoire <lecteur>:\ProgramData\Sophos\Sophos NAC\Logs.

3.2 Journalisation de l'agent temporaire

Les fichiers journaux de l'agent ne sont pas présents pour l'agent temporaire

Cause : la journalisation n'est pas activée.

Solution : activez la journalisation de l'agent temporaire. Sélectionnez la case à cocher Activer la journalisation dans la boîte de dialogue A propos de. Pour plus d'informations, reportez-vous au *Guide de configuration de l'agent de Sophos NAC Advanced*.

Remarque : la journalisation affecte les performances. Nous conseillons par conséquent d'activer la journalisation uniquement pour la résolution des problèmes et de la désactiver lorsque la résolution des problèmes est terminée. Les fichiers journaux sont placés dans le répertoire <lecteur>:\Sophos\SDA<numéro aléatoire>\Logs.

4 Problèmes de communication serveur (depuis l'agent)

Cette section contient des informations pour résoudre les problèmes de communication serveur sur ou depuis l'agent.

4.1 Récupération de stratégies, enregistrement ou création de rapports

Échec de récupération de stratégies, de l'enregistrement ou de la création de rapports

Important : pour d'autres problèmes relatifs aux stratégies, à l'enregistrement ou aux rapports, reportez-vous aux chapitres [Problèmes de stratégies](#) à la page 12, [Problèmes d'enregistrement](#) à la page 19 ou [Problèmes de rapports](#) à la page 21.

Cause : l'adresse du Serveur d'applications de conformité n'était pas correcte lorsque l'agent a été déployé ou l'adresse du serveur a été changée après le déploiement de l'agent. L'adresse du serveur utilisée pour la connexion au Serveur d'applications de conformité apparaît dans le fichier journal.

Si l'adresse IP ou le nom DNS n'est **pas** correct ou si le Serveur d'applications de conformité ne fonctionne plus, l'erreur suivante apparaît dans la boîte de dialogue ou la page Résultats : "L'agent n'a pas pu effectuer l'opération de <>. Si ce problème persiste, veuillez contacter votre administrateur et lui signaler le problème. (Raison : serveur introuvable. Code: 700)".

Si l'adresse IP ou le nom DNS est correct mais le chemin URL n'est **pas** correcte, l'erreur suivante apparaît dans la boîte de dialogue ou la page Résultats : "L'agent n'a pas pu effectuer l'opération de <>. Si ce problème persiste, veuillez contacter votre administrateur et lui signaler le problème. (Raison : URL incorrecte. Code: 404)".

Solution :

1. Assurez-vous que le Serveur d'applications de conformité ne peut pas être contacté en lançant une vérification de conformité disponible via l'option de menu Vérifier la conformité associée à l'icône de l'Agent de quarantaine de la zone de notification.
2. Activez la journalisation sur l'agent en sélectionnant la case à cocher Activer la journalisation dans la boîte de dialogue A propos de, puis vérifiez l'adresse du serveur (adresse IP ou nom DNS) et le mode du serveur (http/https) du Serveur d'applications de conformité en ouvrant le fichier journal API de l'agent nommé <GUID>_trace.log. Pour l'agent de conformité, ce fichier journal s'affiche si le paramètre Logging Agent du modèle de configuration d'agent est défini sur Log All Messages and Brief Trace. Pour l'agent temporaire, Log All Messages and Brief Trace sont spécifiés lorsque la journalisation est activée. Pour l'agent de conformité, les fichiers journaux de Windows 2000 et Windows XP sont placés dans le répertoire <lecteur>:\Documents and Settings\All Users\Application Data\Sophos\Sophos NAC\Logs et ceux de Windows Vista et Windows 7 dans le répertoire <lecteur>:\ProgramData\Sophos\Sophos NAC\Logs. Pour l'agent temporaire, Les fichiers journaux sont placés dans le répertoire <lecteur>:\Sophos\SDA<numéro aléatoire>\Logs.
3. Réinstallez l'agent avec l'adresse correcte du Serveur d'applications de conformité. Lors de l'installation, le format de l'adresse du serveur (< Serveur d'applications de conformité> sur lequel les services web Registration Interface, Policy Interface et Reporting Interface

sont installés) doit uniquement être le nom DNS ou l'adresse IP, comme "www.sophos.fr" ou "10.0.0.160".

Important : si le certificat Web sur le Serveur d'applications de conformité est configuré pour utiliser une adresse IP, cette dernière doit être utilisée lors de l'installation de l'agent. De même, si le certificat Web est configuré pour utiliser un nom DNS, un nom DNS doit être utilisé lors de l'installation de l'agent.

Cause : l'enregistrement de l'agent a été supprimé. Le message d'erreur suivant apparaît dans la boîte de dialogue ou sur la page Résultats : "L'agent n'a pas pu effectuer l'opération de <>. Si ce problème persiste, veuillez contacter votre administrateur et lui signaler le problème. (Raison : le serveur a rejeté la demande de l'agent. Code : 500)".

Solution : enregistrez de nouveau l'agent. Sur l'ordinateur d'extrémité, cliquez avec le bouton droit de la souris sur l'icône de l'agent de la zone de notification et sélectionnez **Enregistrer**.

Cause : l'ordinateur d'extrémité n'a pas d'accès Internet.

Solution : assurez-vous que l'ordinateur d'extrémité accède à Internet.

Cause : le certificat SSL n'est pas installé sur l'agent ou sur le Serveur d'applications de conformité.

Solution :

1. Assurez-vous que le certificat numérique de l'autorité de certification est installé dans le magasin de l'autorité de certification de confiance de la machine locale (non pas de l'utilisateur). Ceci est nécessaire pour https.

Remarque : pour valider correctement les certificats sur les ordinateurs d'extrémité fonctionnant sous d'anciens systèmes d'exploitation Microsoft Windows[®], y compris Windows 2000, installez le "Root Certificate Update" depuis le site Web de Microsoft.

2. Assurez-vous qu'un certificat numérique est installé sur le Serveur d'applications de conformité et qu'il a été émis par une Autorité de certification de confiance comme VeriSign. Ceci est nécessaire pour https.

Remarque : si vous utilisez HTTP pour les tests, les URL utiliseront aussi HTTP.

Cause : le Serveur d'applications de conformité n'est pas joignable.

Solution :

1. Assurez-vous que le logiciel de pare-feu sur l'ordinateur d'extrémité ne bloque pas le trafic vers le Serveur d'applications de conformité et vérifiez qu'un pare-feu ne bloque pas le trafic vers l'ordinateur d'extrémité. Si un pare-feu bloque le trafic, ouvrez le cas échéant le pare-feu pour l'autoriser.
2. Assurez-vous que l'adresse appropriée du Serveur d'applications de conformité est opérationnelle en testant l'URL du Serveur d'applications de conformité dans un navigateur Web. Si une erreur des services Web apparaît, l'adresse du serveur est correcte. Vous pouvez tester l'une des URL suivantes :

[http\(s\)://< Serveur d'applications de conformité>/RegistrationInterface/RegistrationInterface310.aspx](http(s)://< Serveur d'applications de conformité>/RegistrationInterface/RegistrationInterface310.aspx)

[http\(s\)://< Serveur d'applications de conformité>/ServerStatusInterface/ServerStatusInterface310.aspx](http(s)://< Serveur d'applications de conformité>/ServerStatusInterface/ServerStatusInterface310.aspx)

3. Assurez-vous que le Serveur d'applications de conformité a été ajouté comme ressource réseau autorisée dans les modèles d'accès appropriés du Compliance Manager.
4. Dans le cas où l'ordinateur d'extrémité est à un emplacement distant, il doit se connecter au VPN, puis effectuer une vérification de conformité lancée par l'utilisateur via l'agent sur l'ordinateur d'extrémité.

Cause : l'agent utilise un serveur proxy Web pour se connecter au Serveur d'applications de conformité et les paramètres du serveur proxy Web sont incorrects.

Solution : accédez aux paramètres proxy Web dans Internet Explorer et assurez-vous que les paramètres sont corrects :

1. Cliquez sur **Outils > Options Internet** .
2. Cliquez sur l'onglet **Connections**.
3. Cliquez sur **Paramètres et/ou Paramètres réseau** et spécifiez les paramètres appropriés du proxy.

Assurez-vous que l'adresse appropriée du Serveur d'applications de conformité est opérationnelle en testant l'URL du Serveur d'applications de conformité dans un navigateur Web. Si une erreur des services Web apparaît, l'adresse du serveur est correcte. Vous pouvez tester l'une des URL suivantes :

[http\(s\)://<Compliance Application Server>/RegistrationInterface/RegistrationInterface310.asmx](http(s)://<Compliance Application Server>/RegistrationInterface/RegistrationInterface310.asmx)

[http\(s\)://<Compliance Application Server>/ServerStatusInterface/ServerStatusInterface310.asmx](http(s)://<Compliance Application Server>/ServerStatusInterface/ServerStatusInterface310.asmx)

Cause : l'agent utilise un serveur proxy Web pour se connecter au Serveur d'applications de conformité, mais les paramètres du serveur proxy Web ne sont pas définis pour l'utilisateur en cours.

Solution : étant donné que les paramètres sont définis séparément par utilisateur, assurez-vous que les paramètres du proxy Web dans Internet Explorer sont définis pour l'utilisateur en cours. Pour plus d'informations, reportez-vous au problème précédent.

Cause : une entrée DNS a changé et l'ordinateur d'extrémité n'a pas fait l'objet d'un redémarrage ou le processus AgentAPI.exe n'a pas été arrêté et redémarré.

Solution : redémarrez chaque ordinateur d'extrémité ou quittez l'agent, puis arrêtez et démarrez le processus AgentAPI.exe sur chaque ordinateur d'extrémité. Ceci efface les entrées DNS obsolètes.

Cause : la clé serveur ne correspond pas. L'erreur suivante apparaît dans la boîte de dialogue ou la page Résultats : Échec de la validation du serveur. Code : 701" (si les messages d'erreur détaillés sont activés).

Solution : si une nouvelle clé de serveur est générée dans le Compliance Manager, la même clé de serveur doit être importée sur tous les serveurs d'applications de conformité afin que ceux-ci soient synchronisés.

Assurez-vous d'utiliser le bon fichier de clé serveur ServerKey.xml et la même clé serveur sur tous les serveurs d'applications de conformité (en cas d'utilisation de plusieurs serveurs).

5 Problèmes avec le client VPN

Cette section contient des informations pour résoudre les problèmes relatifs au client VPN.

5.1 VPN

VPN ou toute autre application tierce n'appelle pas l'agent correctement

Cause : l'Agent de quarantaine n'est pas appelé depuis le VPN ou depuis toute autre application tierce.

Solution : assurez-vous que les applications tierces appellent le vérificateur de conformité "Compliance Checker" (Cmpchk.exe) pour que l'agent puisse lancer une vérification intégrale de la conformité. Pour plus d'informations, reportez-vous au *Guide de configuration de l'agent de Sophos NAC Advanced*.

Cause : l'agent n'est pas en cours d'exécution.

Solution : assurez-vous que l'agent est bien en cours d'exécution avant son appel par une application tierce.

VPN ne se connecte pas

Cause : d'après l'Agent Policy Update Threshold, la dernière récupération de stratégie par l'ordinateur d'extrémité n'a pas eu lieu dans le temps imparti.

Solution : assurez-vous que la dernière récupération de stratégie pour l'ordinateur d'extrémité a eu lieu dans le temps imparti défini dans le champ Agent Policy Update Threshold du Compliance Manager (**Configure System** > **Enforcer Settings**).

Cause : les codes de retour sont incorrects lors de l'appel du vérificateur de conformité (Cmpchk.exe).

Solution : assurez-vous que les codes de retour sont corrects et gérés correctement lors de l'appel du vérificateur de conformité (Cmpchk.exe). Pour plus d'informations sur les codes de retour, reportez-vous au *Guide de configuration de l'agent de Sophos NAC Advanced*.

Échec de l'authentification VPN

Cause : le nom utilisateur utilisé pour l'authentification RADIUS ne correspond pas au nom utilisateur utilisé pour l'authentification VPN.

Solution : assurez-vous que le format de la chaîne du nom utilisateur correspond exactement à ce qui a été saisi dans l'agent pour l'authentification RADIUS et l'application client VPN (le nom utilisateur n'est pas sensible aux majuscules).

Cause : l'ordinateur d'extrémité se voit affecter un modèle d'accès RADIUS Enforcer qui refuse l'accès sans aucune raison valable.

Solution : consultez le rapport du RADIUS Enforcer du Compliance Manager pour savoir quel modèle d'accès est affecté à l'ordinateur d'extrémité et la raison pour laquelle il a été affecté.

Assurez-vous que les bons modèles d'accès RADIUS Enforcer sont appliqués aux bons états d'accès et de conformité dans la stratégie et dans les paramètres Enforcer et vérifiez que les modèles d'accès contiennent les bons paramètres ou les bonnes ressources réseau.

6 Problèmes de stratégies

Cette section contient des informations pour résoudre les problèmes relatifs aux stratégies.

6.1 Récupération des stratégies

Échec de récupération des stratégies

Important : pour plus d'informations, reportez-vous à la section [Problèmes de communication serveur \(depuis l'agent\)](#) à la page 8.

Cause : l'enregistrement de l'agent de l'utilisateur a expiré. Le message d'erreur suivant apparaît dans la boîte de dialogue ou sur la page Résultats : "Échec de l'opération de récupération de la stratégie dû à l'expiration de l'enregistrement de l'utilisateur. Enregistrez l'agent."

Solution : l'utilisateur doit enregistrer l'agent à l'aide de l'option de menu Enregistrer.

6.2 Évaluation et application des stratégies

L'agent n'est pas en mesure d'évaluer/d'appliquer la stratégie

Important : pour plus d'informations, reportez-vous à la section [Problèmes de communication serveur \(depuis l'agent\)](#) à la page 8.

Cause : l'enregistrement de l'agent de l'utilisateur a expiré. Le message d'erreur suivant apparaît dans la boîte de dialogue ou sur la page Résultats : "Échec de l'opération d'application de la stratégie dû à l'expiration de l'enregistrement de l'utilisateur. Enregistrez l'agent."

Solution : l'utilisateur doit enregistrer l'agent à l'aide de l'option de menu Enregistrer.

L'ordinateur d'extrémité ne reçoit pas de stratégie (l'utilisateur est en cours d'authentification)

Cause : aucune stratégie par défaut n'est définie et l'utilisateur est membre d'un groupe qui n'est pas associé à une stratégie dans le Compliance Manager ou l'utilisateur ne peut pas être mappé sur un groupe.

Solution : utilisez le Compliance Manager pour associer le groupe à une stratégie ou créer une stratégie par défaut.

Cause : le groupe d'utilisateur a changé entre le moment où l'agent a enregistré l'utilisateur pour la dernière fois et le moment où la stratégie a été récupérée.

Solution : terminez l'enregistrement de l'utilisateur dans la zone **Manage > Endpoints** du Compliance Manager afin que l'agent puisse ré-enregistrer l'utilisateur et récupérer la bonne stratégie.

Cause : le groupe de l'utilisateur n'est pas créé dans le Compliance Manager.

Solution : créez le groupe dans le Compliance Manager. Pour plus d'informations, reportez-vous à l'Aide du Compliance Manager.

Cause : si vous utilisez l'Agent de quarantaine, l'intervalle de rafraîchissement des stratégies (Policy Refresh Interval) n'a pas été atteint et donc, l'agent n'a pas récupéré la stratégie mise à jour.

Solution : récupérez la stratégie via une vérification de conformité lancée par l'utilisateur, disponible à l'aide de l'option de menu Vérifier la conformité associée à l'icône de l'Agent de quarantaine de la zone de notification.

L'ordinateur d'extrémité ne reçoit pas de stratégie correcte

Cause : le groupe d'utilisateur a changé entre le moment où l'agent a enregistré l'utilisateur pour la dernière fois et le moment où la stratégie a été récupérée.

Solution : terminez l'enregistrement de l'utilisateur dans la zone **Manage > Endpoints** du Compliance Manager afin que l'agent puisse ré-enregistrer l'utilisateur et récupérer la bonne stratégie.

Cause : l'utilisateur est un membre du groupe, en revanche, le groupe n'est pas associé à la bonne stratégie dans le Compliance Manager.

Solution : assurez-vous que le groupe est associé à la bonne stratégie dans le Compliance Manager.

Cause : les groupes ne sont pas correctement classés par ordre de priorité dans le Compliance Manager.

Solution : assurez-vous que les groupes sont correctement classés par ordre de priorité dans le Compliance Manager. Si plusieurs groupes s'appliquent à un ordinateur d'extrémité particulier, le premier groupe associé à ce système sera utilisé. Si l'utilisateur reçoit la stratégie par défaut, assurez-vous que les noms du groupe sont également corrects.

Cause : l'utilisateur n'est pas membre du groupe attendu dans la banque d'utilisateurs.

Solution : assurez-vous que l'utilisateur est associé au bon groupe dans la banque d'utilisateurs et assurez-vous que le nom du groupe est correct. Pour être authentifié correctement, le nom du groupe dans le Compliance Manager doit correspondre soit à un nom de groupe de sécurité dans l'archive utilisateur (Active Directory ou Windows NT) soit à une valeur retournée par le serveur RADIUS (proxy RADIUS).

Cause : le groupe de l'utilisateur n'est pas créé dans le Compliance Manager.

Solution : créez le groupe dans le Compliance Manager. Pour plus d'informations, reportez-vous à l'Aide du Compliance Manager.

Cause : l'utilisateur reçoit la stratégie par défaut plutôt que la bonne stratégie.

Solution : assurez-vous que l'utilisateur est associé au bon groupe dans la banque d'utilisateurs. Assurez-vous que le nom du groupe est créé et qu'il est correct dans le Compliance Manager. Assurez-vous que le groupe est associé à la bonne stratégie dans le Compliance Manager.

Si vous utilisez le paramètre d'enregistrement Use Computer Logon, l'utilisateur doit ouvrir une session sur son ordinateur d'extrémité en utilisant ces codes d'accès de domaine ; autrement, il recevra la stratégie par défaut.

L'ordinateur d'extrémité n'effectue pas l'évaluation par rapport à une stratégie mise à jour

Important : pour plus d'informations, reportez-vous à la section [Problèmes de communication serveur \(depuis l'agent\)](#) à la page 8.

Cause : si vous utilisez l'Agent de quarantaine, l'intervalle de rafraîchissement des stratégies (Policy Refresh Interval) n'a pas été atteint et donc, l'agent n'a pas récupéré la stratégie mise à jour.

Solution : récupérez la stratégie via une vérification de conformité lancée par l'utilisateur, disponible à l'aide de l'option de menu Vérifier la conformité associée à l'icône de l'Agent de quarantaine de la zone de notification.

Les paramètres ou les fonctionnalités de l'agent sont incorrectement appliqués sur l'ordinateur d'extrémité

Cause : ce problème peut être un effet secondaire au problème "Le système d'extrémité ne reçoit pas la stratégie correcte" ou "Le système d'extrémité n'évalue pas par rapport à une stratégie mise à jour".

Solution : assurez-vous que l'ordinateur d'extrémité reçoit la stratégie correcte et mise à jour (utilisez le rapport Agent Session pour confirmer). Sinon, suivez les étapes de résolution des problèmes "Le système d'extrémité ne reçoit pas la stratégie correcte" ou "Le système d'extrémité ne reçoit pas la stratégie mise à jour". Si l'ordinateur d'extrémité reçoit la stratégie correcte et à jour, passez aux autres étapes de ce chapitre.

Cause : un modèle de configuration d'agent incorrect a été ajouté à la stratégie de l'ordinateur d'extrémité ou les paramètres sont incorrects dans le modèle de configuration d'agent.

Solution : vérifiez que le modèle de configuration d'agent appliqué à la stratégie de l'ordinateur d'extrémité est correct et que le modèle contient des paramètres d'agent corrects.

Cause : l'agent n'affiche pas le paramètre régional attendu de l'habillage.

Solution : l'habillage d'agent apparaît dynamiquement en fonction du paramètre régional de l'utilisateur par défaut, quelle que soit la langue du système d'exploitation installé sur le système d'extrémité.

L'activation de l'action d'actualisation pour les profils Windows Update ne fonctionne pas.

Cause : la stratégie de groupe ne permet pas l'activation des Mises à jour automatiques.

Solution : si la stratégie de groupe ne permet pas l'activation des Mises à jour automatiques, vous ne pouvez pas la remplacer dans la stratégie de conformité. Assurez-vous que la stratégie de groupe est telle que vous la souhaitez et que la stratégie de conformité est synchrone avec la stratégie de groupe.

L'application n'est pas détectée sur l'ordinateur d'extrémité ou l'application échappe à la détection

Cause : l'application que vous détectez peut être inexacte.

Solution : vérifiez que vous disposez du nom approprié de l'application associée au profil qui a été ajouté à la stratégie. Les applications sont répertoriées dans le Compliance Manager sous le nom du produit principal. Parfois, l'application est commercialisée sous un nom différent. Vérifiez le produit effectivement installé pour déterminer le nom du produit principal ou contactez l'éditeur pour vérifier ce nom.

Avant de déployer la stratégie, nous vous conseillons de la tester pour vous assurer que l'application, les règles de détection des applications, les paramètres du profil et de la stratégie que vous avez sont corrects.

Cause : les règles de détection des fonctions installées pour l'application personnalisée sont incorrectes.

Solution : avant de déployer la stratégie, nous vous conseillons de la tester pour vous assurer que l'application, les règles de détection des applications, les paramètres du profil et de la stratégie dont vous disposez sont corrects.

Activez la fonction de journalisation Brief Trace sur l'agent en sélectionnant la case Activer la journalisation dans la boîte de dialogue A propos de et assurez-vous que le modèle de configuration de l'agent appliqué à la stratégie du système d'extrémité a le paramètre Logging Agent spécifié en tant qu'erreur, avertissement, informations et messages de suivi. Consultez le journal API de l'agent (<GUID>_trace.log) pour résoudre les problèmes de détection.

Remarque : la journalisation affecte les performances. Nous conseillons par conséquent d'activer la journalisation uniquement pour la résolution des problèmes et de la désactiver lorsque la résolution des problèmes est terminée. Les fichiers journaux de Windows 2000 et Windows XP sont placés dans le répertoire <lecteur>:\Documents and Settings\All Users\Application Data\Sophos\Sophos NAC\Logs et ceux de Windows Vista et Windows 7 dans le répertoire <lecteur>:\ProgramData\Sophos\Sophos NAC\Logs.

Cause : la date de la règle de détection du registre de l'application n'est pas au bon format.

Solution : si vous utilisez une date dans une détection de registre, assurez-vous que l'application est détectée sur l'ordinateur d'extrémité à l'aide du format de date correct. Vous pouvez sélectionner soit le paramètre régional du système qui détermine le format de date d'après la langue du système soit Anglais (États-Unis). Pour déterminer quel format utiliser, nous vous conseillons d'installer l'application sur les systèmes d'exploitation internationaux que vous avez l'intention de prendre en charge, d'exécuter l'application de l'éditeur et de déterminer comment les dates changent ou sont stockées pour chaque système d'exploitation, car elles peuvent être différentes.

Cause : le numéro de version défini dans la fonctionnalité d'application ou dans la règle de détection d'applications ne contient pas un nombre correct de valeurs significatives pour l'évaluation prévue des ordinateurs d'extrémité.

Solution : la version est évaluée sur l'ordinateur d'extrémité à l'aide du nombre de valeurs significatives spécifiées dans la condition ou dans la règle de détection. Par conséquent, si vous définissez une fonctionnalité de version ou créez une règle de détection avec une version, veillez à ce que le numéro de version contienne le nombre correct de valeurs significatives pour l'évaluation prévue des systèmes d'extrémité.

Par exemple, si vous créez une condition qui spécifie == 8 et si la version de l'ordinateur d'extrémité est 8.1, le logiciel compare 8.1 à 8 dans la condition (une valeur significative), et la condition est remplie. En revanche, si vous créez une condition qui spécifie == 8.0 et si la version de l'ordinateur d'extrémité est 8.1, le logiciel compare 8.1 à 8 dans la condition (deux valeurs significatives), et la condition n'est pas remplie.

Cause : le format de date défini dans la fonctionnalité ne correspond pas exactement au format renvoyé depuis l'évaluation de conformité.

Solution : si vous définissez un profil pour une application antivirus ou antispyware standard et si vous spécifiez une fonctionnalité de date (Last Scan Date et Signature Date) à l'aide de l'opérateur == (Egal à), veillez à ce que la date renvoyé de l'ordinateur d'extrémité soit au format MM/JJ/AAAA. Si l'application renvoie une date au format MM/JJ/AAAA HH:MM:SS, la détection peut échouer même si la date sur l'ordinateur d'extrémité est identique à la valeur spécifiée dans la condition. Pour éviter ce problème, vous pouvez utiliser l'opérateur >= (supérieur ou égal à) ou <= (inférieur ou égal à) au lieu de == lors de la définition des dates ou tester une stratégie avant de la déployer pour vous assurer que l'opérateur == ne fait pas échouer la détection.

6.3 Messages ou actions d'actualisation

Les messages n'apparaissent pas et les actions d'actualisation ne sont pas exécutées sur l'ordinateur d'extrémité

Cause : le message ne s'affiche pas pour les utilisateurs.

Résolution :

1. Vérifiez que la stratégie est en mode Remediate ou Enforce. Si elle est en mode Report Only, les messages ne s'afficheront pas.
2. Vérifiez qu'un message est créé, que le message est associé à la condition correcte du profil et que la condition a été remplie sur l'ordinateur d'extrémité. Utilisez le Compliance Manager pour consulter le rapport Agent Session et voir le lien Assessment Details vers les détails du profil et les messages affichées aux utilisateurs.

Cause : le message ne s'affiche pas pour les utilisateurs sur des systèmes d'exploitation en langue étrangère.

Résolution : assurez-vous que les messages de tous les profils dans la stratégie de l'ordinateur d'extrémité sont créés en anglais, qui est la langue par défaut, et que ces profils créent ensuite des messages identiques dans toutes les langues étrangères appropriées.

Cause : l'action d'actualisation n'est pas effectuée sur l'ordinateur d'extrémité.

Résolution :

1. Vérifiez que la stratégie est en mode Remediate ou Enforce. Si elle est en mode Report Only, les actions d'actualisation ne seront pas exécutées.
2. Vérifiez que l'action d'actualisation est sélectionnée pour la condition correcte du profil et que la condition a été remplie sur l'ordinateur d'extrémité. Utilisez le Compliance Manager pour consulter le rapport Agent Session et voir le lien Assessment Details vers les détails du profil et les actions d'actualisation exécutées sur l'ordinateur d'extrémité.
3. Si vous avez une stratégie qui exige que le logiciel mette automatiquement à jour un fichier signature antivirus ou antispyware, vérifiez que le modèle d'accès approprié autorise l'accès à l'emplacement du serveur des fichiers signatures afin que la mise à jour puisse être effectuée.
4. Si vous avez vérifié les étapes 1 à 3 et si l'action d'actualisation n'est toujours pas exécutée, il est possible que cette dernière ne soit pas prise en charge sur ce système d'exploitation. Si une action d'actualisation est prise en charge sur certains systèmes d'exploitation mais pas sur d'autres, les systèmes d'exploitation non pris en charge apparaissent avec un x. Assurez-vous que l'utilisateur peut corriger l'application d'une autre façon et qu'un message

est créé pour cette fonctionnalité d'application afin de conseiller des instructions d'actualisation à l'utilisateur.

6.4 Correctifs

Les correctifs les plus récents ne sont pas récupérés par l'agent

Important : pour plus d'informations, reportez-vous à la section [Journal des événements](#) à la page 25.

Cause : Sophos NAC Advanced ne télécharge pas les correctifs les plus récents.

Solution : à l'aide de la commande Server Task Status sur la page d'accueil du Compliance Manager, vérifiez que la tâche Patch Loader a bien échoué et consultez la raison de cet échec. La cause d'échec la plus probable est que le Serveur d'applications de conformité ne dispose pas de l'accès sortant à Internet, qui est requis par Patch Loader. Exécutez manuellement la tâche Patch Loader sur le Serveur d'applications de conformité pour télécharger et mettre à jour les informations sur les correctifs. Pour plus d'informations, reportez-vous au *Guide d'installation de Sophos NAC Advanced*.

Cause : les correctifs sont obsolètes pour les anciens agents (3.0.x).

Solution : si le Serveur d'applications de conformité n'a pas accès à Internet, assurez-vous que le fichier CAB utilisé pour la détection des correctifs est publié manuellement sur le Serveur d'applications de conformité. Pour plus d'informations, reportez-vous au problème "Affichage d'erreurs Patch Loader dans le journal des événements du Serveur d'applications de conformité". Pour plus d'informations, reportez-vous à la section [Journal des événements](#) à la page 25.

Cause : l'utilisateur se sert de l'agent temporaire tout en ayant un accès restreint à l'ordinateur d'extrémité.

Solution : l'agent temporaire n'évalue pas les correctifs si l'utilisateur est connecté en tant qu'utilisateur avec restrictions. Modifiez l'utilisateur afin qu'il s'exécute en tant qu'administrateur et exécutez de nouveau l'agent temporaire. Si ce changement n'est pas possible, nous vous recommandons de créer une stratégie distincte pour les utilisateurs de l'agent temporaire. Ces utilisateurs sont généralement des invités. 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.

6.5 Dates des fichiers signatures

Les dates les plus récentes des fichiers signatures pour les logiciels antivirus et antispyware ne sont pas récupérées par l'agent

Important : pour plus d'informations, reportez-vous à la section [Journal des événements](#) à la page 25.

Cause : Sophos NAC Advanced ne télécharge pas les fichiers signatures les plus récents.

Résolution : à l'aide de la commande Server Task Status sur la page d'accueil du Compliance Manager, vérifiez que la tâche Current Definition Loader a bien échoué et consultez la raison de cet échec. La cause d'échec la plus probable est que le serveur ne dispose pas de l'accès

sortant à Internet, qui est requis par Current Definition Loader. Exécutez manuellement la tâche Current Definition Loader sur le serveur pour télécharger et mettre à jour les informations sur la date des signatures de l'application. Pour plus d'informations, reportez-vous au *Guide d'installation de Sophos NAC Advanced* .

7 Problèmes d'enregistrement

Cette section contient des informations pour résoudre les problèmes d'enregistrement des ordinateurs d'extrémité.

7.1 Enregistrement

Échec de l'enregistrement

Important : pour plus d'informations, reportez-vous à la section [Problèmes de communication serveur \(depuis l'agent\)](#) à la page 8.

Échec de l'authentification

Cause : un nom utilisateur/mot de passe incorrects ont été envoyés à l'agent.

Solution : assurez-vous que le nom utilisateur/mot de passe utilisés pour exécuter l'agent sont corrects. Les nom utilisateur/mot de passe proviennent soit directement de l'utilisateur qui les saisit dans la boîte de dialogue Enregistrement ou Codes d'accès, soit de la ligne de commande via un script ou une autre application telle qu'un "dialer".

Cause : l'utilisateur n'est pas configuré dans la banque d'utilisateurs du client.

Solution : configurez les nom utilisateur/mot de passe correctement dans la banque d'utilisateurs du client (c'est à dire, Active Directory, Domaine NT, etc.).

Cause : le secret partagé du Service d'authentification Internet ne correspond pas.

Remarque : pour plus d'informations sur l'utilisation de l'outil de test d'authentification (Authentication Test) afin de diagnostiquer les problèmes, reportez-vous au *Guide des outils de Sophos NAC Advanced*.

Solution : pour déterminer un problème de correspondance du secret partagé du Service d'authentification Internet, récupérez la valeur du secret partagé à l'aide de l'outil de chiffrement des secrets (Secret Encryption) et procédez à un test à l'aide de l'outil d'authentification. Un secret partagé non correspondant affiche une erreur de réponse non valide semblable à :

"Completed Attempt (1): To server 127.0.0.1:1812. Status: InvalidResponse In 2578.1085 mS. Radius request failed after all attempts. Last Reason: InvalidResponse"

Pour résoudre ce problème :

Utilisez l'outil de cryptage des secrets pour définir le secret partagé du Service d'authentification Internet dans l'interface des stratégies (Policy Interface) ainsi que le secret partagé du Service d'authentification Internet sur le client RADIUS.

Cause : le type d'authentification ne correspond pas.

Remarque : pour plus d'informations sur l'utilisation de l'outil de test d'authentification (Authentication Test) afin de diagnostiquer les problèmes, reportez-vous au *Guide des outils de Sophos NAC Advanced*.

Solution : pour déterminer un problème de correspondance du type d'authentification, récupérez la valeur du type d'authentification depuis le fichier Registration Interface Web.config (l'installation par défaut est MS-CHAP v2) et exécutez-le dans l'outil de test d'authentification.

Un type d'authentification non correspondant affiche une erreur de refus d'accès semblable à :

"Results: Completed Attempt (1): To server 127.0.0.1:1812. Status: Succeeded Received: AccessReject In 156.249 mS."

Si vous n'exécutez pas de serveur proxy RADIUS, un message semblable au suivant apparaît dans le journal des événements du système (System Event Log) :

"Resolution/more info - System event log - local authentication method used doesn't match remote access policy. Reason-Code = 66 Reason = The user attempted to use an authentication method that is not enabled on the matching remote access policy."

Pour résoudre ce problème :

- Changez le type d'authentification dans le fichier Registration Interface Web.config (généralement dans le sous-répertoire Inetpub\wwwroot\RegistrationInterface sur le Serveur d'applications de conformité) pour faire correspondre un des types d'authentification sur le serveur RADIUS procédant à l'authentification.
- Si vous exécutez des serveurs proxy RADIUS, consultez le journal ou vérifiez la configuration du serveur RADIUS procédant à l'authentification afin de déterminer quelles méthodes d'authentification sont utilisées et modifiez le type d'authentification dans le fichier Policy Interface Web.config afin qu'il corresponde à l'un des types d'authentification du serveur RADIUS procédant à l'authentification.

Des erreurs de l'interface d'enregistrement apparaissent dans le journal des événements du Serveur d'applications de conformité

Cause : l'interface d'enregistrement ne peut pas communiquer avec RADIUS Enforcer.

Solution : consultez le journal des événements du Serveur d'applications de conformité pour voir les erreurs. Si une erreur indique que toutes les tentatives de contacter le RADIUS Enforcer ont échoué, vérifiez l'adresse IP du RADIUS Enforcer, les protocoles et le secret partagé dans l'interface d'enregistrement à l'aide de l'outil de cryptage des secrets. Pour plus d'informations, reportez-vous au *Guide des outils de Sophos NAC Advanced*.

8 Problèmes de rapports

Cette section contient des informations pour résoudre les problèmes relatifs aux rapports.

8.1 Agent

L'agent ne peut pas créer de rapports

Important : pour plus d'informations, reportez-vous à la section [Problèmes de communication serveur \(depuis l'agent\)](#) à la page 8.

Cause : l'enregistrement de l'agent de l'utilisateur a expiré. Le message d'erreur suivant apparaît dans la boîte de dialogue ou sur la page Résultats : "Échec de l'opération de création de rapports dû à l'expiration de l'enregistrement de l'utilisateur. Enregistrez l'agent."

Solution : l'utilisateur doit enregistrer l'agent à l'aide de l'option de menu Enregistrer.

8.2 Compliance Manager

Des données sont manquantes dans le rapport Agent Session

Cause : si vous utilisez l'Agent de quarantaine, l'intervalle d'édition de rapports de la stratégie (Reporting Interval) n'a pas été atteint, l'agent n'a donc pas mis à jour les données du rapport.

Solution : procédez à la mise à jour des données du rapport via une vérification de conformité lancée par l'utilisateur, disponible à l'aide de l'option de menu Vérifier la conformité associée à l'icône de la zone de notification de l'Agent de quarantaine.

Les rapports semblent incomplets ou il y manque des informations

Cause : le service de transfert de stratégie (Policy Transfer Service) ne fonctionne pas.

Solution : démarrez Policy Transfer Service sur le Serveur d'applications de conformité et assurez-vous qu'il est défini sur "Automatic".

L'exécution d'un rapport avec des données archivées ne produit aucun résultat

Cause : la tâche Report Warehouse Loader SQL n'a jamais été exécutée.

Solution : dans ce cas, le rapport affichera "No Data Available" près de son nom. À l'aide de la commande Server Task Status de la page d'accueil du Compliance Manager, vérifiez quand la tâche Report Warehouse Loader a été exécutée et s'il y a eu des erreurs. Confirmez que le SQL Server Agent fonctionne sur l'instance hébergeant les bases de données de conformité. Chaque nuit à 2h30 (à moins que l'heure soit manuellement modifiée), le SQL Server Agent exécute la tâche Report Warehouse Loader, ce qui déplace les données de la base de données ReportStore dans la base de données ReportStoreWH. En guise de bon usage, les propriétés du SQL Server Agent doivent être changées pour automatiquement redémarrer le SQL Server Agent s'il s'arrête subitement. En outre, le service SQLAgent (nom de l'instance) doit être en cours d'exécution. En guise de bon usage, le SQLAgent (nom de l'instance) doit être paramétré sur Automatic.

Pour plus d'informations sur l'exécution de la tâche Sophos NAC - Load WH, reportez-vous au *Guide d'installation de Sophos NAC Advanced*.

L'exécution d'un rapport avec des données archivées produit des résultats qui sont obsolètes

Cause : la tâche Report Warehouse Loader SQL n'a pas été exécutée récemment.

Solution : dans ce cas, le rapport affichera "Use Data from the Last Archive (mm/jj/aaaa hh:mm:ss)" près de son nom avec une date antérieure aux dernières 24 heures. À l'aide de la commande Server Task Status de la page d'accueil du Compliance Manager, vérifiez quand la tâche Report Warehouse Loader a été exécutée et s'il y a eu des erreurs. Confirmez que le SQL Server Agent fonctionne sur l'instance hébergeant les Compliance Databases. Chaque nuit à 2h30 (à moins que l'heure soit manuellement modifiée), le SQL Server Agent exécute la tâche Report Warehouse Loader SQL, ce qui déplace les données de la base de données ReportStore dans la base de données ReportStoreWH. En guise de bon usage, les propriétés du SQL Server Agent doivent être changées pour automatiquement redémarrer le SQL Server Agent s'il s'arrête subitement. En outre, le service SQLAgent (nom de l'instance) doit être en cours d'exécution. En guise de bon usage, le SQLAgent (nom de l'instance) doit être paramétré sur Automatic.

Pour plus d'informations sur l'exécution de la tâche Sophos NAC - Load WH, reportez-vous au installation guide *de* Sophos NAC Advanced.

L'exécution d'un rapport avec des données courantes produit des résultats qui semblent obsolètes

Cause : si vous utilisez l'Agent de quarantaine, l'intervalle d'édition de rapports de la stratégie (Reporting Interval) n'a pas été atteint, l'agent n'a donc pas mis à jour les données du rapport.

Solution : procédez à la mise à jour des données du rapport via une vérification de conformité lancée par l'utilisateur, disponible à l'aide de l'option de menu Vérifier la conformité associée à l'icône de la zone de notification de l'Quarantine Agent.

Cause : il se peut que l'Agent Report Service ne fonctionne pas.

Solution : démarrez Agent Report Service sur le Serveur d'applications de conformité et assurez-vous qu'il est défini sur "Automatic".

L'exécution d'un rapport avec des données archivées produit des résultats incomplets

Cause : la tâche Sophos NAC - Load WH n'a pas été exécutée récemment ou échoue.

Solution : dans ce cas, le rapport affichera "Use Data from the Last Archive (mm/jj/aaaa hh:mm:ss)" près de son nom avec une date antérieure aux dernières 24 heures. À l'aide de la commande Server Task Status de la page d'accueil du Compliance Manager, vérifiez si la tâche Report Warehouse Loader a échoué et consultez la raison de cet échec. Confirmez que le SQL Server Agent fonctionne sur l'instance hébergeant les bases de données de conformité. Chaque nuit à 2h30 (à moins que l'heure soit manuellement modifiée), le SQL Server Agent exécute la tâche Report Warehouse Loader, ce qui déplace les données de la base de données ReportStore dans la base de données ReportStoreWH. En guise de bon usage, les propriétés du SQL Server Agent doivent être changées pour automatiquement redémarrer le SQL Server Agent s'il s'arrête subitement. En outre, le service SQLAgent (nom de l'instance) doit être en cours d'exécution. En guise de bon usage, le SQLAgent (nom de l'instance) doit être paramétré sur Automatic.

Pour plus d'informations sur l'exécution de la tâche Report Warehouse Loader, reportez-vous au *Guide d'installation de Sophos NAC Advanced*.

9 Problèmes relatifs aux alertes

Cette section contient des informations pour résoudre les problèmes relatifs aux alertes.

9.1 Compliance Manager

Les alertes ne sont pas reçues

Cause : le journal des événements du Serveur d'applications de conformité est plein.

Solution : assurez-vous d'avoir assez d'espace disque disponible pour le journal des événements du Serveur d'applications de conformité.

Cause : le serveur de messagerie n'est pas configuré correctement.

Solution : recherchez les erreurs dans le journal des événements du Serveur d'applications de conformité. Assurez-vous que le trafic SMTP (port TCP 25) est ouvert entre le Serveur d'applications de conformité et le serveur de messagerie. Assurez-vous aussi que le bon serveur de messagerie est configuré dans le Compliance Manager (**Configure System** > **Alerts** , **paramètre Alert E-mail Server**).

Cause : il se peut qu'Alert Service ne fonctionne pas.

Solution : démarrez Alert Service sur le Serveur d'applications de conformité et assurez-vous qu'il est défini sur "Automatic".

Cause : l'alerte n'est pas configurée correctement dans le Compliance Manager.

Solution : nous vous conseillons de tester vos stratégies et vos alertes à l'aide d'un groupe de test avant de les déployer afin de vous assurer d'avoir les paramètres corrects.

10 Problèmes de serveur

Cette section contient des informations pour résoudre les problèmes de serveur **autres que** des problèmes liés à l'agent.

10.1 Serveur d'applications de conformité

La machine serveur SQL n'est pas accessible par Sophos depuis le Serveur d'applications de conformité par Sophos NAC Advanced

Cause : le Serveur d'applications de conformité n'est pas connecté correctement pour communiquer avec les bases de données de conformité.

Solution : pour vérifier la connectivité, effectuez les étapes suivantes sur le Serveur d'applications de conformité, à l'aide d'un compte de service Sophos NAC Advanced ayant accès aux bases de données de conformité :

1. Créez un nouveau fichier .txt sur le bureau du Serveur d'applications de conformité.
2. Renommez le fichier conn.udl. Vous **devez** avoir l'extension .udl.
3. Une fois créé, cliquez deux fois sur le fichier conn.udl.
4. Depuis la fenêtre Data Link Properties, cliquez sur l'onglet **Provider**.
5. Sélectionnez **Microsoft OLE DB Provider for SQL Server**, puis cliquez sur **Suivant**.
6. Sélectionnez ou saisissez le nom ou l'instance du serveur SQL. Ce nom **doit** être le même que celui que vous avez utilisé pour l'installation du Serveur d'applications de conformité.
7. Sélectionnez le bouton d'option **Utiliser la sécurité intégrée de Windows NT**.
8. Sélectionnez le bouton d'option **Sélectionner la base de données sur le serveur**.
9. Sélectionnez **PolicyStore** dans la liste déroulante.
10. Cliquez sur **Tester la connexion**.

Pour plus d'informations sur les raisons potentielles des problèmes de connectivité et les solutions, reportez-vous à la section [Installation des bases de données de conformité](#) à la page 3 et au problème "Échec de connexion de tous les composants du Serveur d'applications de conformité ou du serveur RADIUS aux bases de données de conformité" de la section [Serveur SQL](#) à la page 25.

10.2 Serveur RADIUS

Le serveur SQL n'est pas accessible depuis le serveur RADIUS

Cause : le serveur RADIUS n'est pas connecté correctement pour communiquer aux bases de données de conformité

Solution : pour vérifier la connectivité, effectuez les étapes suivantes sur le serveur RADIUS, à l'aide d'un compte de service Sophos NAC Advanced ayant accès aux bases de données de conformité :

1. Créez un nouveau fichier .txt sur le bureau du serveur RADIUS.
2. Renommez le fichier conn.udl. Vous **devez** avoir l'extension .udl.
3. Une fois créé, cliquez deux fois sur le fichier conn.udl.
4. Depuis la fenêtre Data Link Properties, cliquez sur l'onglet **Provider**.

5. Sélectionnez **Microsoft OLE DB Provider for SQL Server**, puis cliquez sur **Suivant**.
6. Sélectionnez ou saisissez le nom ou l'instance du serveur SQL. Ce nom **doit** être le même que celui que vous avez utilisé pour l'installation du serveur RADIUS.
7. Sélectionnez le bouton d'option **Utiliser la sécurité intégrée de Windows NT**.
8. Sélectionnez le bouton d'option **Sélectionner la base de données sur le serveur**.
9. Sélectionnez **PolicyStore** dans la liste déroulante.
10. Cliquez sur **Tester la connexion**.

Pour plus d'informations sur les raisons potentielles des problèmes de connectivité et les solutions, reportez-vous à la section [Installation des bases de données de conformité](#) à la page 3 et au problème "Échec de connexion de tous les composants du Serveur d'applications de conformité ou du serveur RADIUS aux bases de données de conformité" de la section [Serveur SQL](#) à la page 25.

10.3 Serveur SQL

Aucun des composants du Serveur d'applications de conformité ou du serveur RADIUS ne parvient à se connecter aux bases de données de conformité

Cause : il se peut que les droits n'aient pas été configurés correctement pour les applications Sophos NAC Advanced dans les bases de données de conformité.

Résolution :

1. Ouvrez le Services Snap-in sur le Serveur d'applications de conformité.
2. Observez le Sophos NAC Host Service pour identifier sous quelle identité de compte le service fonctionne.
3. Vérifiez que l'identité de compte a les droits d'accès aux bases de données de conformité.

10.4 Journal des événements

Des erreurs de Patch Loader ou de Current Definition Loader apparaissent dans le journal des événements du Serveur d'applications de conformité

Cause : le Serveur d'applications de conformité n'a pas d'accès Internet.

Solution :

1. Assurez-vous que le Serveur d'applications de conformité dispose d'un accès Internet.
2. Si vous utilisez un serveur proxy, celui-ci doit être configuré dans le Compliance Manager. Cliquez sur **Configure System > Server Settings**. Cliquez sur le nom du serveur et saisissez les détails du proxy dans le volet **Server Details**.
3. Si vous avez des erreurs de Patch Loader ou de Current Definition Loader, veuillez contacter le [support technique](#) à la page 35.

Remarque : la mise à jour manuelle de Current Definition Loader peut être très compliquée lorsque le Serveur d'applications de conformité ne dispose pas d'un accès Internet. Ce fichier est mis à jour toutes les heures et les données peuvent par conséquent être très rapidement obsolètes. Ce fichier contient les dates les plus récentes des signatures pour les applications antivirus et antispyswares.

11 Problèmes d'application

Cette section contient des informations pour résoudre les problèmes d'application réseau.

11.1 Accès réseau

L'accès est refusé à l'ordinateur d'extrémité alors qu'il devrait être autorisé (ou vice versa), l'ordinateur d'extrémité est placé en quarantaine alors qu'il ne devrait pas, ou l'utilisateur voit un ou des messages incorrects dans la boîte de dialogue Agent Results

Cause : ce problème peut être un effet secondaire au problème "Le système d'extrémité ne reçoit pas la stratégie correcte" ou "Le système d'extrémité n'évalue pas par rapport à une stratégie mise à jour". Pour plus d'informations, reportez-vous à la section [Évaluation et application des stratégies](#) à la page 12.

Solution : assurez-vous que l'ordinateur d'extrémité reçoit la stratégie correcte et mise à jour (utilisez le rapport Agent Session du Compliance Manager pour confirmer). Sinon, suivez les étapes de résolution des problèmes "Le système d'extrémité ne reçoit pas la stratégie correcte" ou "Le système d'extrémité ne reçoit pas la stratégie mise à jour". Si l'ordinateur d'extrémité reçoit la stratégie correcte et à jour, passez aux autres étapes de ce chapitre.

Cause : Agent Enforcer, RADIUS Enforcer ou DHCP Enforcer refuse l'accès à l'ordinateur d'extrémité.

Solution : utilisez le Compliance Manager pour consulter le rapport Agent Enforcer, RADIUS Enforcer ou DHCP Enforcer et voir la raison pour laquelle Enforcer a refusé l'accès à l'ordinateur d'extrémité. Il est possible que le RADIUS Enforcer ait échoué à authentifier l'utilisateur.

Cause : des modèles d'accès Agent Enforcer incorrects ou avec des paramètres incorrects sont associés à la stratégie.

Solution : utilisez le Compliance Manager afin de vous assurer que les modèles d'accès Agent Enforcer corrects sont appliqués aux états d'agent et aux états de conformité dans la stratégie et vérifiez que les modèles d'accès Agent Enforcer utilisés dans la stratégie incluent les ressources réseau appropriées. Aussi, assurez-vous que les ressources réseau ont des noms d'exécutables, des ports/protocoles ou, le cas échéant, des adresses IP corrects.

Le modèle d'accès Agent Enforcer appliqué par défaut à l'état de conformité Non-Compliant dans la stratégie permet l'accès à tous les produits Sophos et à Internet pour les réseaux internes qui utilisent des adresses IP privées, et refuse tout autre trafic sortant. Vous pouvez changer ces paramètres en créant un nouveau modèle d'accès Agent Enforcer et en l'appliquant à l'état de conformité Non-Compliant dans la stratégie du système d'extrémité.

Si vous appliquez un modèle d'accès Enforcer qui empêche l'accès au réseau en modes Report Only ou Remediate, tous les systèmes d'extrémité seront interdits d'accès quel que soit l'état en cours de leur conformité. Pour appliquer un état de conformité, changez le mode de stratégie sur Enforce.

Cause : des modèles d'accès RADIUS Enforcer ou DHCP Enforcer incorrects ou des modèles d'accès RADIUS Enforcer ou DHCP Enforcer avec des paramètres incorrects sont associés à la stratégie ou aux paramètres Enforcer.

Solution : utilisez le Compliance Manager pour vous assurer que des modèles d'accès RADIUS Enforcer ou DHCP Enforcer corrects sont appliqués aux états d'accès et de conformité corrects dans la stratégie et dans les paramètres Enforcer et vérifiez que les modèles d'accès RADIUS Enforcer ou DHCP Enforcer contiennent les paramètres corrects.

Si vous appliquez un modèle d'accès Enforcer qui empêche l'accès au réseau en modes Report Only ou Remediate, tous les systèmes d'extrémité seront interdits d'accès quel que soit l'état en cours de leur conformité. Pour appliquer un état de conformité, changez le mode de stratégie sur Enforce.

Cause : les modèles d'accès RADIUS Enforcer ou DHCP Enforcer ne sont pas classés correctement par ordre de priorité.

Solution : utilisez le Compliance Manager pour vous assurer que les modèles d'accès RADIUS Enforcer ou DHCP Enforcer sont classés correctement par ordre de priorité dans la stratégie ou dans les paramètres Enforcer. Classez par ordre de priorité les modèles d'accès les plus spécifiques/stricts, puis les moins spécifiques/stricts. Les modèles d'accès les plus spécifiques/stricts fournissent une adresse IP spécifique ou une plage d'adresses IP plus limitée tandis que les modèles d'accès moins spécifiques/stricts fournissent une plage d'adresses IP plus étendue.

Cause : une ressource réseau exécutable n'est pas détectée par le logiciel.

Solution : le nom du processus exécutable doit être le nom qui apparaît dans l'onglet Processus du Gestionnaire des tâches Windows.

Le logiciel détecte seulement les exécutables qui s'exécutent au niveau Winsock. Si l'application ne fonctionne pas au niveau Winsock, elle ne sera pas détectée.

Cause : les ressources réseau ne sont pas classées correctement par ordre de priorité.

Solution : utilisez le Compliance Manager pour vous assurer que les ressources réseau sont classées correctement dans le modèle d'accès Agent Enforcer. Classez par ordre de priorité tout d'abord les ressources réseau les plus spécifiques/strictes, puis les moins spécifiques/strictes. Si plusieurs ressources réseau s'appliquent à un ordinateur d'extrémité, la première qui correspond déterminera l'accès réseau pour la session des ordinateurs d'extrémité. Les ressources réseau exécutables sont évaluées avant les ressources réseau de ports/protocoles.

Cause : l'ordinateur d'extrémité est exempté et ne devrait pas l'être ou n'est pas exempté et devrait l'être.

Solution : utilisez le Compliance Manager pour vous assurer que l'ordinateur d'extrémité n'est **pas** une exemption s'il doit faire l'objet d'une évaluation pour sa conformité. De même, assurez-vous que l'ordinateur d'extrémité est une exemption s'il ne doit **pas** faire l'objet d'une évaluation pour sa conformité.

Assurez-vous que les modèles d'accès RADIUS Enforcer ou DHCP Enforcer appropriés sont appliqués aux exemptions.

Aussi, assurez-vous que les exemptions sont classées correctement par ordre de priorité dans la page de liste Exemptions. Classez par ordre de priorité les exemptions les plus spécifiques/strictes en premier, puis les moins spécifiques/strictes. Si plusieurs exemptions s'appliquent à un ordinateur d'extrémité, la première correspondante détermine l'accès réseau pour la session des ordinateurs d'extrémité. De plus, si plusieurs modèles d'accès s'appliquent à une exemption particulière, le premier modèle contenant l'adresse IP correspondante du client RADIUS, du serveur DHCP ou du relais DHCP est utilisé.

Cause : les règles de détection d'application personnalisées sont définies de manière incorrecte dans le Compliance Manager.

Solution :

1. Vérifiez que les règles de détection personnalisées des applications sont correctement définies dans le Compliance Manager. Pour plus d'informations, reportez-vous au problème "L'application n'est pas détectée sur le système d'extrémité ou l'application échappe à la détection" de la section [Évaluation et application des stratégies](#) à la page 12.
2. Activez la fonction de journalisation Brief Trace sur l'agent en sélectionnant la case Activer la journalisation dans la boîte de dialogue A propos de et assurez-vous que le modèle de configuration de l'agent appliqué à la stratégie du système d'extrémité a le paramètre Logging Agent spécifié en tant qu'erreur, avertissement, informations et messages de suivi. Consultez le journal API de l'agent (<GUID>_trace.log) pour résoudre les problèmes de détection.

Remarque : la journalisation affecte les performances. nous conseillons par conséquent d'activer la journalisation uniquement pour la résolution des problèmes et de la désactiver lorsque la résolution des problèmes est terminée. Les fichiers journaux de Windows 2000 et Windows XP sont placés dans le répertoire <lecteur>:\Documents and Settings\All Users\Application Data\Sophos\Sophos NAC\Logs et ceux de Windows Vista et Windows 7 dans le répertoire <lecteur>:\ProgramData\Sophos\Sophos NAC\Logs.

Cause : il se peut que les profils ou les applications personnalisées associés à la stratégie ne contiennent pas le système d'exploitation de l'ordinateur d'extrémité et ne soient donc pas correctement évalués.

Solution :

1. À l'aide du Compliance Manager, assurez-vous que le système d'exploitation de l'ordinateur d'extrémité est ajouté comme profil de système d'exploitation dans la stratégie affectée et que toutes les applications personnalisées associées à la stratégie (via les profils d'applications) contiennent aussi le système d'exploitation de l'ordinateur d'extrémité.
2. Utilisez le Compliance Manager pour consulter le rapport Non-Compliance Detail ou Agent Session et voir le lien Assessment Details pour assurer que l'agent évalue les applications.

Cause : d'après l'Agent Policy Update Threshold, la dernière récupération de stratégie par l'ordinateur d'extrémité n'a pas eu lieu dans le temps imparti.

Solution : assurez-vous que la dernière récupération de stratégie pour l'ordinateur d'extrémité a eu lieu dans le temps imparti défini dans le champ Agent Policy Update Threshold du Compliance Manager (**Configure System** > **Enforcer Settings**). Récupérez la stratégie via une vérification de conformité lancée par l'utilisateur, disponible à l'aide de l'option de menu Vérifier la conformité associée à l'icône de l'Agent de quarantaine de la zone de notification.

Cause : la case à cocher Override Enforcers du Compliance Manager (**Configure System** > **Enforcer Settings**) est sélectionnée.

Solution : désélectionnez la case à cocher Override DHCP Enforcers et assurez-vous que l'état d'accès par défaut dispose des modèles d'accès corrects affectés pour le type d'application RADIUS ou DHCP.

Cause : l'agent de conformité ne fonctionne pas sur l'ordinateur d'extrémité.

Remarque : ce problème s'applique seulement à l'Agent de quarantaine.

Solution :

1. Assurez-vous que l'agent de conformité fonctionne.
2. Assurez-vous que le service Agent API fonctionne.

Cause : le paramètre Agent Enforcement Action dans la stratégie (section paramètres d'agent DHCP) est défini sur None, et l'ordinateur d'extrémité utilise encore une adresse IP non conforme.

Remarque : ce problème s'applique seulement à l'application DHCP.

Solution : si le paramètre DHCP Agent Enforcement Action dans la stratégie est défini sur None et si l'ordinateur d'extrémité est passé d'un état non conforme à un état conforme, il se peut que l'ordinateur ne reçoive pas une adresse IP conforme. Changez le paramètre Agent Enforcement Action sur Release Renew, enregistrez la stratégie et exécutez une vérification de conformité lancée par l'utilisateur sur l'ordinateur d'extrémité.

Cause : le paramètre Agent Enforcement Action dans la stratégie (section Paramètres d'agent 802.1x) est défini sur None, et l'ordinateur d'extrémité se voit toujours affecter une adresse VLAN en quarantaine.

Remarque : ce problème s'applique seulement à l'application 802.1x.

Solution : si le paramètre 802.1x Agent Enforcement Action dans la stratégie est défini sur None et si l'ordinateur d'extrémité est passé d'un état non conforme à un état conforme, il se peut que le système ne soit pas réauthentié et affecté à une adresse VLAN conforme. Changez le paramètre Agent Enforcement Action sur Reauthenticatation, enregistrez la stratégie et exécutez une vérification de conformité lancée par l'utilisateur sur l'ordinateur d'extrémité.

Cause : aucun message n'apparaît pour l'utilisateur même si l'ordinateur d'extrémité est interdit d'accès ou mis en quarantaine.

Solution :

1. Vérifiez qu'un message est créé, que le message est associé à la condition correcte du profil et que la condition a été remplie sur l'ordinateur d'extrémité. Utilisez le Compliance Manager pour consulter le rapport Non-Compliance Detail ou Agent Session et voir le lien Assessment Details indiquant les détails de profil et les messages affichés aux utilisateurs et comprendre pourquoi l'ordinateur d'extrémité a été interdit d'accès ou mis en quarantaine et pourquoi il n'a reçu aucun message.
2. Vérifiez que la stratégie est en mode Remediate ou Enforce. Si elle est en mode Report Only, les messages ne s'afficheront pas. Si vous appliquez un modèle d'accès Enforcer qui empêche l'accès au réseau en modes Report Only ou Remediate, l'accès sera refusé à tous les systèmes d'extrémité quel que soit l'état actuel de leur conformité.
3. Assurez-vous que les modèles d'accès corrects sont appliqués aux états d'accès et de conformité corrects de la stratégie et vérifiez que les modèles d'accès contiennent les paramètres ou les ressources réseau corrects.

Cause : il y a un problème d'installation d'une ou de plusieurs applications de sécurité sur l'ordinateur d'extrémité.

Solution :

1. Utilisez le Compliance Manager pour consulter le rapport Non-Compliance Detail ou Agent Session et voir le lien Assessment Details indiquant les détails d'évaluation de conformité pour déterminer quels problèmes sont rencontrés par l'agent.
2. Vérifiez que vous disposez du nom approprié de l'application associée au profil qui a été ajouté à la stratégie. Les applications sont répertoriées dans le Compliance Manager sous le nom du produit principal. Parfois, l'application est commercialisée sous un nom différent. Vérifiez le produit effectivement installé pour déterminer le nom du produit principal ou contactez l'éditeur pour vérifier ce nom.
3. Assurez-vous que les applications de sécurité voulues fonctionnent comme prévu sur le système d'extrémité. Pour plus d'informations, reportez-vous au site Web de l'application de sécurité, aux informations sur la résolution des problèmes et, si nécessaire, consultez le support clients.

Cause : problèmes d'accès réseau indéterminés.

Solution :

1. Assurez-vous que la stratégie est correcte.
2. Utilisez le Compliance Manager pour consulter le rapport Non-Compliance ou Agent Session et voir le lien Assessment Details indiquant les détails d'évaluation de la conformité.
3. Utilisez le Compliance Manager pour consulter le rapport Agent Session et vous assurer que l'agent reçoit la stratégie prévue avec la bonne version.
4. Utilisez le Compliance Manager pour consulter les rapports Agent Enforcer, RADIUS Enforcer, DHCP Enforcer, RADIUS Exemption ou DHCP Exemption pour résoudre les problèmes liés à l'accès réseau et aux exemptions.

11.2 802.1x

Le contrôleur d'accès/commutateur 802.1x ne peut pas authentifier l'utilisateur

Solution : consultez l'entrée du Service d'authentification Internet (IAS) de cet utilisateur dans le journal des événements système du Serveur d'applications de conformité. Si l'erreur suivante apparaît, il se peut que l'utilisateur ait un problème d'accès réseau : "The request was rejected by a third-party extension DLL file."

Important : pour plus d'informations, reportez-vous à la section [Accès réseau](#) à la page 26.

Solution : consultez l'entrée du Service d'authentification Internet (IAS) de cet utilisateur dans le journal des événements système du Serveur d'applications de conformité. Si l'une des erreurs suivantes apparaît, il se peut que l'utilisateur ait un problème d'authentification : "The connection attempt did not match any remote access policy." OU "The remote RADIUS (Remote Authentication Dial-In User Service) server did not process the authentication request."

Important : pour plus d'informations, reportez-vous à la section [Paramètres de configuration RADIUS Enforcer](#) à la page 31.

Le Service d'authentification Internet ne peut pas authentifier l'ordinateur d'extrémité

Cause : une erreur système sur le Serveur d'applications de conformité indique que le protocole EAP (Extensible Authentication Protocol) est un protocole non valide ; par conséquent, la

stratégie d'accès à distance du Service d'authentification Internet n'est pas configurée pour le protocole EAP.

Solution : consultez l'entrée du Service d'authentification Internet (IAS) de cet utilisateur dans le journal des événements système du Serveur d'applications de conformité. Si une erreur apparaît indiquant qu'EAP est un protocole non valide, modifiez le profil de la stratégie d'accès à distance sur le Serveur d'applications de conformité et ajoutez les types EAP appropriés pour l'ordinateur d'extrémité (**Authentication > EAP Methods**).

Le contrôleur d'accès/commutateur 802.1x affecte un VLAN incorrect

Cause : le paramètre Agent Enforcement Action dans la stratégie (section Paramètres d'agent 802.1x) est défini sur None, et l'ordinateur d'extrémité se voit toujours affecter une adresse VLAN en quarantaine.

Solution : si le paramètre 802.1x Agent Enforcement Action dans la stratégie est défini sur None et si l'ordinateur d'extrémité est passé d'un état non conforme à un état conforme, il se peut que le système ne soit pas réauthentifié et affecté à une adresse VLAN conforme. Changez le paramètre Agent Enforcement Action sur Reauthentification, enregistrez la stratégie et exécutez une vérification de conformité lancée par l'utilisateur sur l'ordinateur d'extrémité.

Cause : les paramètres du modèle d'accès RADIUS définis dans le Compliance Manager sont incorrects.

Solution : les attributs RADIUS sont spécifiques au fournisseur de périphériques. Pour plus d'informations sur les attributs RADIUS nécessaires pour un périphérique particulier, reportez-vous à la documentation sur le périphérique.

Cause : assurez-vous que les paramètres du modèle d'accès RADIUS définis dans le Compliance Manager incluent l'adresse IP dans la liste des adresses IP correspondant au contrôleur d'accès/commutateur 802.1x.

Solution : assurez-vous que les paramètres du modèle d'accès RADIUS incluent l'adresse IP dans la liste des adresses IP correspondant au contrôleur d'accès/commutateur 802.1x.

Cause : les VLAN qui sont configurés via le Compliance Manager n'existent pas sur le contrôleur d'accès/commutateur 802.1x.

Solution : ajoutez le VLAN approprié au contrôleur d'accès/commutateur 802.1x.

Impossible d'utiliser l'agent sur le VLAN invité du contrôleur d'accès/commutateur 802.1x

Cause : le VLAN invité du contrôleur d'accès/commutateur 802.1x n'autorise peut être pas l'accès au Serveur d'applications de conformité.

Solution : vérifiez que le VLAN invité du contrôleur d'accès/commutateur 802.1x autorise l'accès au Serveur d'applications de conformité.

11.3 Paramètres de configuration RADIUS Enforcer

L'utilisateur ne peut pas s'authentifier sur le périphérique de réseau (VPN)

Cause : l'ordinateur d'extrémité se voit affecter un modèle d'accès RADIUS Enforcer qui, à tort, lui refuse l'accès.

Solution : consultez le rapport du RADIUS Enforcer pour savoir quel modèle d'accès est attribué au système d'extrémité et la raison pour laquelle il a été attribué.

Assurez-vous que les bons modèles d'accès RADIUS Enforcer sont appliqués aux bons états d'accès et de conformité dans la stratégie et dans les paramètres Enforcer et vérifiez que les modèles d'accès contiennent les bons paramètres ou les bonnes ressources réseau.

Cause : la stratégie d'accès à distance est peut-être configurée incorrectement ou elle peut être configurée correctement mais l'utilisateur n'a pas été ajoutée au magasin d'utilisateurs.

Solution :

1. Utilisez le Compliance Manager pour consulter le rapport RADIUS Enforcer pour visualiser la raison pour laquelle l'opération d'authentification de l'utilisateur a échoué.
2. Passez en revue les stratégies d'accès à distance. Vous pouvez vérifier ceci dans le journal des événements système par l'entrée du journal des événements IAS de cet utilisateur et la raison suivante : "The connection attempt did not match any remote access policy." Pour un exemple de stratégie d'accès à distance, reportez-vous au *Guide d'installation de Sophos NAC Advanced*.

Cause : le serveur RADIUS (proxy) distant a rejeté la demande.

Solution :

1. Utilisez le Compliance Manager pour consulter le rapport RADIUS Enforcer pour visualiser la raison pour laquelle l'opération d'authentification de l'utilisateur a échoué.
2. Assurez-vous que tous les paramètres sont corrects sur le serveur RADIUS d'authentification. Vous pouvez vérifier ceci dans le journal des événements système par l'entrée du journal des événements IAS de cet utilisateur et la raison suivante : "The remote RADIUS (Remote Authentication Dial-In User Service) server did not process the authentication request." En outre, l'adresse IP du serveur d'authentification sera celle du serveur RADIUS distant qui a rejeté la demande d'authentification de l'utilisateur. Si c'est le cas, consultez les journaux du serveur RADIUS distant pour plus d'informations.

Cause : les types d'authentification entre la stratégie d'accès à distance IAS et le périphérique réseau ne correspondent pas.

Le périphérique réseau peut être un RAC (Remote Access Concentrator), un concentrateur VPN ou tout autre périphérique réseau demandant l'authentification.

Remarque : pour plus d'informations sur l'utilisation de l'outil de test d'authentification (Authentication Test) pour diagnostiquer les problèmes, reportez-vous au *Guide des outils de Sophos NAC Advanced*.

Solution : exécutez un test à l'aide du test d'authentification. Sélectionnez la méthode d'authentification utilisée par le périphérique réseau. Un type d'authentification non correspondant affiche une erreur de refus d'accès semblable à :

"Results: Completed Attempt (1): To server 127.0.0.1:1812. Status: Succeeded Received: AccessReject In 156.249 mS."

Si vous n'exécutez pas de serveur proxy RADIUS, un message semblable au suivant apparaît dans le journal des événements du système (System Event Log) :

"Resolution/more info - System event log - local authentication method used doesn't match remote access policy. Reason-Code = 66 Reason = The user attempted to use an authentication method that is not enabled on the matching remote access policy."

Pour résoudre ce problème :

- Changez la configuration du périphérique réseau pour qu'il prenne en charge le type d'authentification ou changez la stratégie d'accès à distance IAS pour qu'elle prenne en charge le type d'authentification du périphérique réseau.
- Si vous exécutez des serveurs proxy RADIUS, changez la configuration du périphérique réseau pour qu'il prenne en charge le type d'authentification utilisé par le serveur RADIUS distant ou changez la configuration sur le serveur RADIUS distant pour qu'il prenne en charge la méthode d'authentification utilisée par le périphérique réseau.

12 Problèmes relatifs aux applications tierces

Cette section contient des informations pour résoudre les problèmes relatifs aux applications tierces.

12.1 Applications tierces

Une autre application ne fonctionne pas

Cause : le modèle d'accès Agent Enforcer empêche une autre application de fonctionner.

Solution : assurez-vous que le modèle d'accès Agent Enforcer associé à la stratégie de l'ordinateur d'extrémité est correct. Tentez de remplacer la quarantaine sur l'ordinateur d'extrémité. Si l'application fonctionne lorsque la quarantaine est remplacée sur l'ordinateur d'extrémité, assurez-vous que les ressources réseau de l'application sont incluses dans le modèle d'accès Agent Enforcer associé à la stratégie de l'ordinateur d'extrémité. Aussi, assurez-vous que les ressources réseau ont des noms d'exécutables, des ports/protocoles ou, le cas échéant, des adresses IP corrects.

13 Support technique

Vous pouvez obtenir du support technique pour les produits Sophos 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.

14 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 licence conformément à ses termes 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.