

SOPHOS

Sophos NAC Advanced Guide de mise en place de LDAP

Version du produit : 3.2

Date du document : mars 2011



Table des matières

1	À propos de ce document.....	3
2	Liste de contrôle de la mise en place de LDAP.....	4
3	Mise en place de LDAP.....	5
4	Résolutions des problèmes relatifs à LDAP.....	18
5	Support technique.....	20
6	Mentions légales.....	21

1 À propos de ce document

Ce document contient les informations suivantes à propos de Sophos NAC Advanced :

- Liste de contrôle de la mise en place de LDAP
- Informations sur la mise en place de LDAP
- Résolutions des problèmes relatifs à LDAP

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 conjointement avec votre équipe de sécurité informatique pour mettre au point et mettre en place un plan de déploiement de vos logiciels.

2 Liste de contrôle de la mise en place de LDAP

Pour configurer LDAP (Lightweight Directory Access Protocol), exécutez toutes les tâches présentes dans cette liste de contrôle. Sauf mention contraire, toutes les tâches sont effectuées conformément aux instructions du présent document.

Tâche	Description	Terminée
Mise en place de LDAP		
1.	Installez et configurez Sophos NAC Advanced à l'aide de la liste de contrôle d'installation du <i>Guide d'installation de Sophos NAC Advanced</i> . Lorsque vous arrivez à la tâche de mise en place de LDAP, utilisez ce <i>Guide de mise en place de LDAP</i> .	
2.	Créez un fichier de configuration LDAP.	
3.	Configurez les paramètres du registre sur le serveur d'applications de conformité pour qu'il reconnaisse le fichier de configuration LDAP.	
4.	Exécutez l'outil de chiffrement de mots de passe pour chiffrer le mot de passe bind dans le fichier de configuration LDAP.	
5.	Changez en PAP (Password Authentication Protocol) le protocole d'authentification dans l'interface d'enregistrement. Important : PAP force l'envoi des mots de passe en texte en clair. Aussi, nous vous conseillons d'utiliser LDAP plutôt que SSL. Pour utiliser LDAP plutôt que SSL, installez un certificat sur votre contrôleur de domaine ou sur votre serveur répertoire. Pour plus d'informations sur cette configuration, reportez-vous à la documentation de votre éditeur.	
6.	Spécifiez l'authentification PAP dans la stratégie d'accès distant (Windows Server 2003) ou dans la stratégie réseau (Windows Server 2008).	
7.	Créez une stratégie de demande de connexion.	
Mise en place de Microsoft LDAP (tâche facultative)		
8.	Vérifiez que le compte de service que vous avez spécifié dans le fichier de configuration LDAP dispose des autorisations correctes Active Directory. Remarque : LDAP s'authentifie auprès d'Active Directory à l'aide de la stratégie de demande de connexion précédemment créée.	

3 Mise en place de LDAP

Pour utiliser les répertoires LDAP existants avec le mécanisme d'application du RADIUS Enforcer, exécutez les tâches suivantes :

1. Créez un fichier de configuration LDAP.
2. Configurez les paramètres du registre sur le serveur d'applications de conformité pour qu'il reconnaisse le fichier de configuration.
3. Exécutez l'outil de chiffrement de mots de passe pour chiffrer le mot de passe bind dans le fichier de configuration LDAP.
4. Changez en PAP (Password Authentication Protocol) le protocole d'authentification dans l'interface d'enregistrement.
5. Spécifiez l'authentification PAP dans la stratégie d'accès à distance (Remote Access Policy).
6. Créez une stratégie de demande de connexion.

3.1 Création d'un fichier de configuration LDAP

Pour que la mise en place de LDAP fonctionne correctement avec Sophos NAC Advanced, créez un fichier de configuration LDAP avec des paramètres adaptés à votre répertoire LDAP.

1. À l'aide d'un éditeur de texte, créez un fichier de configuration LDAP avec des paramètres LDAP appropriés.

Remarque : en guise de référence, utilisez les exemples de fichiers de configuration LDAP. Pour plus d'informations, reportez-vous à la section [Paramètres du fichier de configuration LDAP](#) à la page 8.

2. Enregistrez le fichier de configuration LDAP avec un nom de votre choix et une extension .config. Par exemple, LDAPconfiguration.config.
3. Copiez le fichier de configuration LDAP sur tous les serveurs d'applications de conformité.

Remarque : nous vous conseillons de placer le fichier de configuration LDAP dans le dossier c:\Program Files\Sophos\NAC\Authgateway.

3.1.1 Exemples de fichiers de configuration

Les fichiers de configuration suivants sont des exemples. Une copie du fichier LDAPsample.config est disponible dans l'emplacement par défaut suivant : c:\Program Files\Sophos\NAC\Authgateway sur le serveur d'applications de conformité.

Pour plus d'informations sur les paramètres spécifiques du fichier de configuration, reportez-vous à la section [Paramètres du fichier de configuration LDAP](#) à la page 8.

Exemple de configuration 1 - Mise en place standard

L'exemple du fichier de configuration suivant fonctionne avec les mises en place de LDAP standard comme OpenLDAP™ ou Novell® eDirectory™.

```
<? xml version="1.0" encoding="utf-8"?>
<configuration>
```

```

<ldapSettings>
  <ldapGroupLookup value="All" />
  <ldapComplianceCheck value="All" />
  <lookupSettings value="All">
    <method type="GroupObject" />
    <hosts>
      <host address="10.0.1.2" port="389" ssl="no" />
      <host address="brasslite" port="389" />
      <host address="MyLDAP" port="636" ssl="yes" />
    </hosts>
    <BaseDN>
      <DN type="user" value="dc=example,dc=com" />
      <DN type="group" value="ou=mygroups,dc=example,dc=com" />
    </BaseDN>
    <ssl certstore="MY" />
    <bindDN value="cn=manager,dc=example,dc=com" />
    <bindPW value="AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAAYtMu5iWVl0
66Z678F74kuAQAAAACAAAAAADZgAAqAAAABAAAABSekDd9Kq3SRHwvaY
yewMwAAAAAASAAACgAAAAEAAAAITxtlveN79033PeYldTOS4I_u65?AAb
MniR1N1FZIUAAAABfM6mmt62tTxcwm66ikA8laRM9M=" />
    <timeout value="5" />
    <userAttribute value="uid" />
    <userFilter value="objectClass=Person" />
    <groupAttribute value="cn" />
    <groupFilter value="objectClass=GroupOfUniqueNames" />
    <groupAttributeName value="UniqueMember" />
  </lookupSettings>
  <ldapAttributes>
    <attribute name="carlicense" />
    <attribute name="homepostaladdress" />
    <attribute name="businesscategory" />
  </ldapAttributes>
  <radiusAttributeMaps>
    <map ldapattr="carlicense" radiusattrnumber="25"
attrtype="String" replace="ou=$1,ou=Engineering">
      <![CDATA[ ( . + )]]></map>
    <map ldapattr="homepostaladdress" radiusattrnumber="11"
attrtype="String" replace="$1"><![CDATA[ ( . + )]]></map>
    <map ldapattr="businesscategory" radiusattrnumber="26"
vsaname="5428" vsanumber="200" vsatype="Text"
replace="$1"><![CDATA[ ( . + )]]></map>
  </radiusAttributeMaps>
</ldapSettings>
</configuration>

```

Exemple de configuration 2 - LDAP utilisant la mise en place Active Directory

L'exemple du fichier de configuration suivant fonctionne avec les mises en place de LDAP se connectant à Active Directory.

Remarque : cet exemple de configuration est principalement fourni à des fins de test. Nous vous conseillons d'utiliser la fonctionnalité de groupe par défaut de Sophos NAC Advanced

lorsque vous utilisez Active Directory. S'il vous est impossible de procéder ainsi, utilisez la mise en place suivante.

```
<? xml version ="1.0" encoding ="utf-8"?>
<configuration>
  <ldapSettings>
    <ldapGroupLookup value="All" />
    <ldapComplianceCheck value="All" />
    <lookupSettings value="All">
      <method type="GroupObject" />
      <hosts>
        <host address="10.0.1.2" port="389" ssl="no" />
        <host address="brasslite" port="389" />
        <host address="MyLDAP" port="636" ssl="yes" />
      </hosts>
      <BaseDN>
        <DN type="user" value="dc=example,dc=com" />
        <DN type="group" value="ou=mygroups,dc=example,dc=com" />
      </BaseDN>
      <ssl certstore="MY" />
      <bindDN value="cn=manager,dc=example,dc=com" />
      <bindPW value="AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAAYtMu5iWVl0
66Z678F74kuAQAAAACAAAAAADZgAAqAAAABAAAABSeKdd9Kq3SRHwvaY
yewMwAAAAAASAAACgAAAAEAAAAITxtlveN79033PeYldTOS4I_u65?AAb
MniR1N1FZIUAAAABfM6mmt62tTxcwm66ikA8laRM9M=" />
      <timeout value="5" />
      <userAttribute value="samaccountname" />
      <userFilter value="objectClass=Person" />
      <groupAttribute value="cn" />
      <groupFilter value="objectClass=Group" />
      <groupAttributeName value="Member" />
    </lookupSettings>
    <ldapAttributes>
      <attribute name="carlicense" />
      <attribute name="homepostaladdress" />
      <attribute name="businesscategory" />
    </ldapAttributes>
    <radiusAttributeMaps>
      <map ldapattr="carlicense" radiusattrnumber="25"
attrtype="String" replace="ou=$1,ou=Engineering">
      </map>
      <map ldapattr="homepostaladdress" radiusattrnumber="11"
attrtype="String" replace="$1"></map>
      <map ldapattr="businesscategory" radiusattrnumber="26"
vsaname="5428" vsanumber="200" vsatype="Text"
replace="$1"></map>
    </radiusAttributeMaps>
  </ldapSettings>
</configuration>
```

3.1.2 Paramètres du fichier de configuration LDAP

Le tableau suivant contient les éléments, les attributs, les descriptions et les valeurs possibles du fichier de configuration LDAP.

Élément	Attribut	Description et valeurs possibles
<configuration>		
ldapSettings		Section contenant tous les paramètres du répertoire LDAP.
<ldapSettings>		
ldapGroupLookup	value	Valeur indiquant quelle section lookupSettings doit être référencée dans le fichier de configuration lorsque le RADIUS Enforcer exécute une consultation de groupe.
ldapComplianceCheck	value	Valeur indiquant quelle section lookupSettings doit être référencée dans le fichier de configuration lorsque le RADIUS Enforcer exécute une vérification de conformité de stratégie.
lookupSettings		Section contenant les paramètres sur où et comment rechercher des informations dans le répertoire LDAP lorsque le RADIUS Enforcer exécute une consultation du groupe d'utilisateurs ou une vérification de conformité de stratégie.
ldapAttributes		Section identifiant les attributs LDAP à récupérer du répertoire à mapper aux attributs RADIUS lors d'une vérification de conformité de stratégie.
radiusAttributeMaps		Section identifiant les attributs RADIUS auxquels les attributs LDAP sont mappés lors d'une vérification de conformité de stratégie.
<lookupSettings> (plusieurs sections lookupSettings peuvent être définies, le cas échéant)		
method	Type	<p>Méthode dans laquelle le RADIUS Enforcer consulte le groupe d'un utilisateur dans le répertoire LDAP. Les valeurs prises en charge sont :</p> <ul style="list-style-type: none"> ■ GroupObject : indique que les noms de groupes sont stockés sous la forme d'objets dans le répertoire LDAP et que le RADIUS Enforcer doit chercher les objets groupe dont l'utilisateur est membre. ■ UserAttribute : indique que les noms de groupes sont contenus dans les attributs d'un utilisateur et que le RADIUS Enforcer doit rechercher les objets utilisateur pour déterminer de quels groupes un utilisateur est membre.

Élément	Attribut	Description et valeurs possibles
hosts		Section contenant les paramètres de la machine hôte du répertoire LDAP.
host	address	Adresse IP ou nom d'hôte de la machine hôte du répertoire LDAP.
	port	Port utilisé lors de la connexion à la machine hôte du répertoire LDAP.
	ssl	Lorsque la valeur=Yes, SSL sert à accéder à la machine hôte du répertoire LDAP.
BaseDN		Section contenant le DN (Distinguished Name ou nom absolu) de base du répertoire LDAP.
DN	Type	Désigne le type de DN pour déterminer l'emplacement lorsque le RADIUS Enforcer effectue une recherche dans le répertoire LDAP. Cette valeur doit être supérieure à toutes les unités d'organisation possibles pour les groupes et les utilisateurs dans la hiérarchie du répertoire. Les valeurs prises en charge sont : <ul style="list-style-type: none"> ■ User : cette valeur est utilisée à la fois pour les recherches de groupes d'utilisateurs et les vérifications de conformité de stratégie lors de la recherche d'un objet utilisateur correspondant dans le répertoire LDAP. ■ Group : cette valeur est utilisée lors de la recherche d'objets groupe dont l'utilisateur est membre. Cette valeur est seulement utilisée lorsque le type de méthode est GroupObject.
	value	Désigne le DN effectivement utilisé comme emplacement de départ lorsque le RADIUS Enforcer effectue une recherche dans le répertoire LDAP. Cette valeur doit être supérieure à toutes les unités d'organisation possibles pour les groupes et les utilisateurs dans la hiérarchie du répertoire.
ssl	certstore	Chaîne de caractères désignant le nom du magasin de certificats. Actuellement, cette valeur doit seulement contenir "MY". <p>Remarque : cette valeur est nécessaire seulement si vous avez configuré SSL pour l'un des hôtes spécifiés.</p>
bindDN	value	Identifiant utilisateur utilisé pour effectuer toutes les recherches LDAP. Laissez ce champ vierge pour les binds anonymes. <p>Remarque : lors de l'utilisation de LDAP pour une authentification à Active Directory, ce compte de service dispose du droit de lecture pour la sous-arborescence</p>

Élément	Attribut	Description et valeurs possibles
		CN ou unité d'organisation où les comptes utilisateurs du domaine résident et du droit de lecture pour l'appartenance au groupe.
bindPW	value	Mot de passe compte bindDN associé. Laissez ce champ vierge pour les binds non authentifiés. Important : ce champ est chiffré et doit être défini à l'aide de l'outil de chiffrement de mots de passe. Pour plus d'informations, reportez-vous à la section Exécution de l'outil de chiffrement de mots de passe pour chiffrer le mot de passe bind à la page 13.
timeout	value	Désigne en secondes le temps que le RADIUS Enforcer attend pour recevoir des données du répertoire LDAP avant de passer à son processus suivant.
userAttribute	value	Désigne le nom de l'attribut contenant le nom utilisateur dans le répertoire LDAP. Cette valeur est combinée avec userFilter (ci-dessous) pour former un filtre de recherche LDAP. Cette valeur est utilisée lorsque le type de méthode est GroupObject ou UserAttribute.
userFilter	value	Chaîne de caractères facultative du filtre utilisée avec l'attribut userAttribute (ci-dessus) pour former une chaîne de caractères de recherche LDAP lors de la recherche d'un objet utilisateur correspondant. Le filtre de recherche obtenu prend la forme suivante : ($\&$ (userFilter)(userAttribute=<nom utilisateur>)) Cette valeur est utilisée lorsque le type de méthode est GroupObject ou UserAttribute.
groupAttribute	value	Désigne le nom de l'attribut contenant le nom du groupe sur un objet utilisateur ou groupe correspondant. La valeur de cet attribut se comporte différemment selon la méthode de recherche de groupes utilisée. Pour les recherches de groupes de type UserAttribute, cet attribut sera placé sur l'objet utilisateur correspondant. Pour les recherches de groupes de type GroupObject, cet attribut sera placé sur les objets groupe correspondants dont l'utilisateur est membre.
groupAttributeName	value	Désigne le nom de l'attribut contenant la liste des utilisateurs appartenant à ce groupe dans le répertoire LDAP. Cette valeur est combinée avec groupFilter (ci-dessous) pour former un filtre de recherche LDAP. Cette valeur est seulement utilisée lorsque le type de méthode est GroupObject.

Élément	Attribut	Description et valeurs possibles
groupFilter	value	Chaîne de caractères facultative du filtre utilisée conjointement à groupAttributeName (ci-dessus) pour former une chaîne de caractères de recherche LDAP complète. Le filtre de recherche obtenu prend la forme suivante : (&(groupFilter)(groupAttributeName=<DN de l'utilisateur>)) Cette valeur est seulement utilisée lorsque le type de méthode est GroupObject.
groupSearchMax	value	Nombre maximum de groupes renvoyés pour chaque utilisateur du répertoire LDAP vers le RADIUS Enforcer lors de l'exécution des consultations de groupe de type GroupObject. La valeur par défaut est 100. Remarque : ce champ n'est pas inclus dans le fichier de configuration exemple. Si vous avez des utilisateurs qui sont dans plus de 100 groupes, vous pouvez avoir besoin d'ajouter ce champ à votre fichier de configuration et soit spécifier une valeur supérieure à 100 soit choisir 0 comme valeur pour renvoyer tous les groupes.
<ldapAttributes>		
attribute	name	Nom de l'attribut de l'utilisateur que vous voulez mapper sur un attribut RADIUS lors d'une vérification de conformité de stratégie.
<radiusAttributeMaps>		
map	ldapattr	Nom d'un attribut LDAP que vous avez identifié dans la section ldapAttributes que vous voulez mapper sur un attribut RADIUS.
	radiusattrnumber	Numéro de l'attribut RADIUS que vous voulez mapper sur l'attribut LDAP correspondant. Exemple : la classe de l'attribut RADIUS est 25. L'identifiant du filtre de l'attribut RADIUS est 11. Remarque : pour spécifier un attribut spécifique à un fournisseur, cet attribut doit être défini sur 26.
	attrtype	Type de données de l'attribut RADIUS que vous voulez mapper sur l'attribut LDAP correspondant. Les valeurs prises en charge sont : String ou Integer .
	vsaname	Numéro d'identification de l'attribut RADIUS spécifique au fournisseur que vous voulez mapper sur l'attribut LDAP correspondant. Cette valeur est uniquement utilisée pour les attributs spécifiques à un fournisseur.

Élément	Attribut	Description et valeurs possibles
	vsanumber	Numéro de l'attribut RADIUS spécifique au fournisseur que vous voulez mapper sur l'attribut LDAP correspondant. Cette valeur est uniquement utilisée pour les attributs spécifiques à un fournisseur.
	vsatype	Type de données de l'attribut RADIUS spécifique au fournisseur que vous voulez mapper sur l'attribut LDAP correspondant. Les valeurs prises en charge sont : Text ou Integer . Cette valeur est uniquement utilisée pour les attributs spécifiques à un fournisseur.
	replace	Valeur de remplacement d'une expression régulière utilisée pour mapper l'attribut LDAP sur l'attribut RADIUS. La chaîne de remplacement est utilisée conjointement avec l'expression régulière dans la section cdata pour rechercher des chaînes de caractères dans l'attribut LDAP et les convertir au format souhaité. Le texte de l'élément mappé est la partie de recherche de l'expression régulière et doit être formaté comme suit : " <code><![CDATA[MyFindExpression]]></code> " Pour plus d'informations sur les expressions régulières, consultez http://msdn2.microsoft.com/en-us/library/az24scfc(vs.71).aspx .

3.2 Configuration des paramètres du registre sur les serveurs d'applications et serveurs RADIUS

Si vous voulez configurer RADIUS Enforcer pour qu'il utilise LDAP, configurez les paramètres suivants du registre sur tous les serveurs d'applications de conformité et sur tous les serveurs RADIUS Enforcer. Ces paramètres du registre doivent être manuellement configurés car ils ne sont pas spécifiés par l'installation du serveur d'applications de conformité de Sophos.

HKEY_LOCAL_MACHINE\SOFTWARE\Sophos\NAC\AuthGateway		
Nom du paramètre de registre	Type	Description de la valeur
LDAPConfigFilename	String	Chaîne de caractères spécifiant le chemin intégral et le nom du fichier de configuration LDAP que vous créez. Le RADIUS Enforcer et le fichier AuthGatewayConfig.exe utilisent ce paramètre pour localiser le fichier de configuration.

HKEY_LOCAL_MACHINE\SOFTWARE\Sophos\NAC\AuthGateway		
UseLDAPAuthAuthZ	DWORD	<p>Spécifie que l'authentification et l'autorisation LDAP seront utilisés au lieu de RADIUS.</p> <p>Important : pour que ce changement soit introduit, vous devez redémarrer le service d'authentification Internet (IAS) ou le service de stratégie réseau et le package Sophos COM+.</p> <ul style="list-style-type: none"> ■ 0 = LDAP est désactivé ■ 1 = LDAP est activé

3.3 Exécution de l'outil de chiffrement de mots de passe pour chiffrer le mot de passe bind

Pour chiffrer le mot de passe bind dans le fichier de configuration, vous devez exécuter l'outil de chiffrement de mots de passe depuis une invite de commande avec les paramètres appropriés.

Remarque : si vous voulez réutiliser un fichier de configuration sur plusieurs serveurs, vous devez exécuter l'outil de chiffrement de mots de passe sur chaque serveur pour mettre à jour et chiffrer le mot de passe bind car le chiffrement du mot de passe est spécifique au serveur.

1. Recherchez l'outil de chiffrement de mots de passe ou AuthGatewayConfig.exe sur le serveur d'applications de conformité. L'emplacement par défaut de cet outil est c:\Program Files\Sophos\NAC\Authgateway.
2. Assurez-vous que le paramètre du registre LDAPConfigFilename pointe vers le fichier de configuration que vous avez créé.
3. Depuis une invite de commande, allez dans le répertoire où le fichier AuthGatewayConfig.exe se trouve.
4. Saisissez **AuthGatewayConfig.exe <bindDN><bindPW>**, où <bindDN> et <bindPW> sont remplacés par l'identifiant de l'utilisateur bind et les valeurs du mot de passe bind appropriés, et appuyez sur **Enter**. Un message apparaît indiquant que le mot de passe bind a été mis à jour avec succès.

Important : le bindDN doit être saisi exactement tel qu'il apparaît dans le fichier de configuration que vous avez créé.

3.4 Changement en PAP du protocole d'authentification dans l'interface d'enregistrement

Sophos NAC Advanced utilise par défaut le protocole d'authentification MSchapV2 RADIUS. Pour les mises en place LDAP, modifiez le protocole d'authentification dans l'interface d'enregistrement sur PAP.

Important : PAP force l'envoi des mots de passe en texte en clair. Aussi, nous vous conseillons d'utiliser LDAP plutôt que SSL. Pour ce faire, vous devez installer un certificat sur votre

contrôleur de domaine ou sur votre serveur répertoire. Pour plus d'informations sur cette configuration, reportez-vous à la documentation de votre éditeur.

1. Recherchez le fichier Web.config pour l'interface d'enregistrement sur le serveur d'applications de conformité. Si vous avez installé le logiciel Sophos NAC Advanced dans l'emplacement par défaut, le fichier est disponible à l'emplacement suivant :
c:\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. Changez dans la ligne `<add key="authType" value="mschap2" />` **mschap2** en **pap**.
5. Enregistrez et fermez le fichier.

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

```
<radius>
  <add key="authType" value="pap" />
  <add key="serverRetries" value="1" />
  <add key="listRetries" value="1" />
</radius>
```

6. Répétez ces étapes sur tous les serveurs d'applications de conformité.

3.5 Spécification de l'authentification PAP dans la stratégie d'accès à distance (Windows Server 2003)

Créez une stratégie d'accès à distance pour les mises en place VPN (Virtual Private Network ou réseau privé virtuel) et LAN (Local Area Network ou réseau local). Pour qu'une mise en place de LDAP fonctionne correctement avec Sophos NAC Advanced, spécifiez une authentification PAP dans les stratégies d'accès à distance du service d'authentification Internet (IAS).

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 sur **Stratégies d'accès distant**.
3. Cliquez avec le bouton droit de la souris sur le nom de la Stratégie d'accès à distance utilisée avec Sophos NAC Advanced, puis sélectionnez **Propriétés**.
4. Cliquez sur **Modifier le profil**.
5. Cliquez sur l'onglet **Authentification**.
6. Sélectionnez la case à cocher **Authentification non cryptée (PAP, SPAP)** si elle n'est pas sélectionnée, puis cliquez sur **OK**.
7. Cliquez sur **OK** pour revenir à la fenêtre principale du Service d'authentification Internet.
8. Répétez ces étapes sur tous les serveurs d'applications de conformité.

3.6 Spécification de l'authentification PAP dans la stratégie réseau (Windows Server 2008)

Créez une stratégie réseau pour les mises en place VPN (Virtual Private Network ou réseau privé virtuel) et LAN (Local Area Network ou réseau local). Pour qu'une mise en place de LDAP fonctionne correctement avec Sophos NAC Advanced, spécifiez une authentification PAP dans la stratégie réseau du serveur de stratégie réseau.

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 sur **Stratégies réseau**.
3. Cliquez avec le bouton droit de la souris sur le nom de la stratégie réseau utilisée avec Sophos NAC Advanced, puis sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Contraintes**.
5. Dans la section **Méthodes d'authentification**, sélectionnez la case à cocher **Authentification non cryptée (PAP, SPAP)** si elle n'est pas sélectionnée, puis cliquez sur **OK**.
6. Répétez ces étapes sur tous les serveurs d'applications de conformité.

3.7 Création d'une stratégie de demande de connexion (Windows Server 2003)

Pour qu'une mise en place de LDAP fonctionne correctement avec Sophos NAC Advanced, spécifiez une stratégie de demande de connexion sur tous les serveurs d'applications de conformité.

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. 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**. Cliquez sur **Nouvelle** > **Stratégie de demande de connexion** .
2. Cliquez sur **Suivant** pour continuer.
3. Sélectionnez l'option **Une stratégie personnalisée**.
4. Saisissez un nom de stratégie.
5. Cliquez sur **Suivant** pour continuer.
6. Cliquez sur **Ajouter** pour ajouter des attributs.
7. Sélectionnez l'attribut approprié, puis cliquez sur **Ajouter**.

Remarque : généralement, l'attribut Restrictions relatives aux jours et aux heures est spécifié.

8. Spécifiez les contraintes heure du jour appropriées, puis cliquez sur **OK**.

Remarque : généralement, les contraintes heure du jour sont définies sur 24 heures/7 jours par semaine permises. Pour obtenir cette contrainte, sélectionnez le bouton d'option Autorisé.

9. Cliquez sur **Suivant** pour continuer.
10. Cliquez sur **Modifier le profil**.
11. Cliquez sur le bouton d'option **Accepter les utilisateurs sans valider les informations d'identification**, puis cliquez sur **OK**.
12. Cliquez sur **Suivant** pour continuer.
13. Cliquez sur **Terminer**.

Remarque : si d'autres stratégies de demande de connexion existent sur le serveur d'applications de conformité, assurez-vous que cette stratégie de demande de connexion est spécifiée comme ayant une priorité inférieure.

14. Répétez ces étapes sur tous les serveurs d'applications de conformité.

3.8 Création d'une stratégie de demande de connexion (Windows Server 2008)

Pour qu'une mise en place de LDAP fonctionne correctement avec Sophos NAC Advanced, spécifiez une stratégie de demande de connexion sur tous les serveurs d'applications de conformité.

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 Stratégie de demande de connexion**.
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 ajouter des conditions.
6. Sélectionnez la condition appropriée, puis cliquez sur **Ajouter**.

Remarque : généralement, l'attribut Restrictions relatives aux jours et aux heures est spécifié.

7. Spécifiez les contraintes heure du jour appropriées, puis cliquez sur **OK**.

Remarque : généralement, les contraintes heure du jour sont définies sur 24 heures/7 jours par semaine permises. Pour obtenir cette contrainte, sélectionnez le bouton d'option Autorisé.

8. Cliquez sur **Suivant** pour continuer.
9. Dans la section **Authentification**, sélectionnez le bouton d'option **Accepter les utilisateurs sans valider les informations d'identification**, puis cliquez sur **Suivant**.
10. Cliquez sur **Suivant** pour continuer. Il n'est pas nécessaire de définir des attributs pour cette stratégie.

11. Cliquez sur **Terminer**.

Remarque : si d'autres stratégies de demande de connexion existent sur le serveur d'applications de conformité, assurez-vous que cette stratégie de demande de connexion est spécifiée comme ayant une priorité inférieure.

12. Répétez ces étapes sur tous les serveurs d'applications de conformité.

3.9 Utilisation de LDAP pour authentification sur Active Directory

Certaines entreprises utilisent LDAP ET Active Directory. Pour utiliser LDAP pour authentification sur Active Directory :

- Vérifiez que le compte de service que vous avez spécifié dans le fichier de configuration LDAP dispose des autorisations correctes Active Directory.
- Utilisez la stratégie de demande de connexion précédemment créée.

3.9.1 Vérification des autorisations du compte de service requis

Le compte de service que vous avez spécifié dans le fichier de configuration LDAP doit avoir les autorisations suivantes :

- Autorisation en lecture pour la sous-arborescence CN ou unité d'organisation où les comptes utilisateur du domaine résident.
- Autorisation en lecture pour l'appartenance au groupe.

Remarque : ce compte de service est spécifié dans l'élément bindDN du fichier de configuration LDAP.

4 Résolutions des problèmes relatifs à LDAP

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

4.1 Problèmes de communication serveur

Cette section contient des informations pour résoudre les problèmes de communication serveur.

Cause	Résolution
Problèmes du journal d'événements d'applications	
<p>Problème :</p> <p>Message d'erreur du journal d'événements contenant : "LDAPDataAgent: BSB, unable to authenticate search user, XXX. YYY"</p> <p>OU</p> <p>Message d'erreur du journal d'événements contenant : "LDAPDataAgent: GetUserGroup, unable to re-authenticate search user, XXX. YYY", où XXX est l'utilisateur de recherche défini dans le fichier de configuration LDAP et YYY est le message d'erreur reçu depuis le serveur LDAP.</p>	
Bad bindDN	Confirmer que la valeur bindDN est correcte dans le fichier de configuration LDAP.
Bad bindPW (mot de passe associé au compte bindDN)	Réinitialiser la valeur bindPW à l'aide de l'outil de chiffrement de mots de passe (AuthGatewayConfig.exe).
<p>Problème : message d'information du journal d'événements contenant : "LDAPDataAgent: BSB, error search for user, XXX, using filter, YYY. No such object. Invalid BaseDN?", où XXX est l'uid de l'utilisateur et YYY est un filtre de recherche LDAP.</p>	
Le DN de base utilisateur est non valide ou incorrect.	Confirmer que la valeur DN de base de type "utilisateur" est correcte dans le fichier de configuration LDAP.
<p>Problème : message d'erreur du journal d'événements contenant : "LDAPDataAgent: ZZZ, Exception while loading LDAP Config.", où ZZZ est un nom de fonction.</p>	
Impossible de localiser le fichier de configuration LDAP.	Confirmer que la valeur spécifiée dans le chemin du registre HKLM\Software\Sophos\AuthGateway\LDAPConfigFilename (REG_SZ) est correcte.
Fichier de configuration LDAP non valide.	Pour plus d'informations, voir le message d'événement détaillé plus en bas dans le même événement ou voir l'entrée précédente du journal d'événements.
<p>Problème : message d'erreur ou d'avertissement du journal d'événements contenant : "LDAPDataAgent: ZZZ, LDAP Exception (AAA). BBB. Lors de la tentative de connexion au serveur, CCC", où ZZZ est un nom de fonction, AAA le numéro d'erreur, BBB la description de l'erreur et CCC est le nom ou l'adresse IP du serveur LDAP.</p>	

Cause	Résolution
Le serveur CCC LDAP est en panne.	Confirmer que le serveur CCC fonctionne correctement OU modifier le fichier de configuration LDAP pour qu'il utilise un autre serveur LDAP.
Délai imparti dépassé pour la recherche en cours sur le serveur CCC.	Effectuer l'une des opérations suivantes, dans aucun ordre particulier : <ul style="list-style-type: none"> ■ Spécifier un filtre de recherche plus réduit dans le fichier de configuration LDAP. ■ Augmenter la valeur de temporisation dans le fichier de configuration LDAP. ■ Changer la liste serveur LDAP du fichier de configuration pour une utilisation des serveurs LDAP soumis à moins de charge.
Echec(s) SSL.	Effectuer l'une des opérations suivantes, dans aucun ordre particulier : <ul style="list-style-type: none"> ■ Vérifier que CCC correspond au sujet (Subject) du certificat SSL du serveur LDAP. ■ Vérifier que l'autorité de certification (AC) émettrice apparaît dans la liste Trusted Root Authorities dans la magasin des certificats du serveur d'applications de conformité. ■ Vérifier que le certificat envoyé au serveur CCC est valide (par exemple : n'a pas expiré, a le nom correct, est une source fiable, etc.).
Problème : message d'avertissement du journal d'événements contenant : "LDAPDataAgent: LDAP Disconnect (AAA). BBB. From server, CCC"	
Le serveur CCC LDAP a de façon inattendue terminé la connexion LDAP.	Confirmer que le serveur CCC fonctionne correctement OU modifier le fichier de configuration LDAP pour qu'il utilise un autre serveur LDAP.

5 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.

6 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.