

Dispositif NAC : Exemple de configuration de la posture AV Mac OSX sur Cisco NAC version 4.5

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Estimation de posture de MAC avec l'antivirus de palourde \(ClamAV\)](#)

[Étape 1. Configurez une règle de vérifier si ClamAV est installé](#)

[Étape 2. Configurez une condition requise aux utilisateurs de Remediate si ClamAV n'est pas installé](#)

[Étape 3. Tracez la condition requise de distribution de lien avec la règle d'installation poids du commerce](#)

[Étape 4. Configurez une règle de vérifier si ClamAV est mis à jour](#)

[Étape 5. Configurez une condition requise aux utilisateurs de Remediate si ClamAV n'est pas mis à jour](#)

[Étape 6. Tracez la condition requise de mise à jour de définition poids du commerce avec la règle de définition de virus](#)

[Étape 7. Tracez les conditions requises aux rôles](#)

[Étape 8. Permettez Access au site de correction dans le rôle provisoire](#)

[Vérifiez l'expérience utilisateur](#)

[Dépannez](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer l'estimation de posture de Clean Access Agent de Mac OS X par l'intermédiaire de la console Web de gestionnaire de Contrôle d'admission au réseau (NAC) pour la version 4.5.

L'estimation de posture de MAC dans cette release est limitée au support AV/AS seulement. Référez-vous aux [notes de mise à jour en Dispositif Cisco NAC \(Clean Access\)](#) pour la liste d'AV/AS qui sont pris en charge sur le MacOSX.

Conditions préalables

Conditions requises

Terminez-vous ces étapes avant que vous tentiez cette configuration :

Ce document suppose que vous exécutez la version 4.5 d'appareils de Cisco NAC et cela vous vous êtes terminé les étapes suivantes selon les instructions dans l'[appliance de Cisco NAC – guide d'installation et de configuration de Clean Access Manager, version 4.5](#) :

1. Installez ou promouvez votre gestionnaire NAC et serveur NAC avec la version 4.5 d'appareils de Cisco NAC comme décrit dans le [guide de démarrage rapide d'installation de matériel d'appareils de Cisco NAC, version 4.5](#).
2. Assurez-vous que le plus récent agent de Mac OS X (version 4.5) et les modules de support AV/AS sont disponibles sur votre gestionnaire NAC comme décrit dedans [configurez et téléchargez les mises à jour](#).
3. Créez une page par défaut d'ouverture de session utilisateur comme décrit en [page d'ouverture de session utilisateur](#).
4. Exigez l'utilisation du Mac OS X Clean Access Agent 4.5 comme décrit dedans [exigez l'utilisation de l'agent](#).
5. Créez un ou plusieurs rôles de l'utilisateur pour des utilisateurs de Macintosh comme décrit dedans [créez les rôles de l'utilisateur](#).

Remarque: Veuillez se référer à la section de [restrictions d'agent de MAC OS X](#) pour des versions de OS X et des Produits AV/AS et des types de condition requise qui sont pris en charge pour l'estimation de posture de MAC.

[Composants utilisés](#)

Les informations dans ce document sont basées sur la version 4.5 de Cisco NAC.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

[Conventions](#)

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

[Estimation de posture de MAC avec l'antivirus de palourde \(ClamAV\)](#)

Le but de cette procédure est de vérifier que ClamAV 1.1.0 est installé et mis à jour avec les dernières définitions de virus sur la machine cliente.

Si ClamAV 1.1.0 n'est pas installé sur la machine cliente, vous devez fournir à l'utilisateur un lien au site Web de ClamAV afin de télécharger et installer le logiciel. Ensuite, vous devez vérifier que ClamAV est mis à jour avec les dernières définitions. Sinon, l'agent de Clean Access peut communiquer avec la palourde poids du commerce par un appel API (avec le type de condition requise de *mise à jour poids du commerce*) et inviter ClamAV pour se mettre à jour.

Remarque: En date de la release du Cisco NAC 4.5, le type de condition requise de mise à jour poids du commerce est pris en charge seulement avec ClamWin poids du commerce. Pour tout autre AV/AS, une *distribution de lien* ou un type *local de contrôle* de condition requise peut être

configurée aux utilisateurs de remEDIATE si leurs définitions de virus ne sont pas mises à jour.

Étape 1. Configurez une règle de vérifier si ClamAV est installé

1. Allez à la **Gestion de périphériques > au Clean Access > au Clean Access Agent > aux règles > nouvelle règle poids du commerce.**
2. Introduisez un nom pour la règle. Cet exemple utilise *Is_Clamwin_Installed_OSX*. **Remarque:** Soyez descriptif de sorte que vous puissiez facilement identifier le but de la règle. Vous pouvez n'utiliser des chiffres et des traits de soulignement dans le nom, mais aucun espace.
3. Choisissez **ClamWin de la** liste déroulante de constructeur d'antivirus.
4. Choisissez l'**installation du** déroulant de type.
5. Choisissez le **MacOSX de la** liste déroulante du système d'exploitation. La table au bas de page est remplie avec ces valeurs.
6. Cochez la case d'**installation** pour 1.x.
7. Tapez une description dans le champ texte de description de règle, et cliquez sur la **règle de sauvegarde**.

La nouvelle règle poids du commerce est ajoutée au bas de la liste de règle.

Étape 2. Configurez une condition requise aux utilisateurs de Remediate si ClamAV n'est pas installé

Si Clean Access Agent le détecte que ClamAV 1.1.0 n'est pas installé sur la machine cliente, il met en quarantaine l'utilisateur. En ce moment, vous pouvez configurer un type de condition requise de *distribution de lien* afin de fournir à l'utilisateur un lien pour télécharger ClamAV 1.1.0.

1. Cliquez sur l'onglet de **Clean Access Agent**, et puis cliquez sur les **conditions requises**.
2. Cliquez sur New la **condition requise**.
3. Choisissez la **distribution de lien de la** liste déroulante de type de condition requise.
4. Choisissez **obligatoire de la** liste déroulante de type d'exécution. Dans cet exemple, l'utilisateur final est au courant de cette condition requise et ne peut pas poursuivre ou avoir l'accès au réseau à moins que le système client réponde à l'exigence. Référez-vous à [configurer une exigence facultative/audit](#) pour des informations sur d'autres types d'application.
5. Choisissez le niveau de priorité d'exécution pour cette condition requise sur la machine cliente. Une haute priorité (par exemple, 1) signifie que cette condition requise est vérifiée le système en avant de toutes autres conditions requises (et apparaît dans les dialogues de Clean Access Agent dans cette commande). Cet exemple suppose que le contrôle d'installation de ClamWin est la première condition requise de posture et fixe la priorité à un (1). **Remarque:** L'agent de Mac OS X ne prend en charge pas la correction automatique. Par conséquent, le type de correction est placé au manuel. En outre, les fonctions qui apparaissent à la nouvelle page de configuration de condition requise (type, intervalle, et nombre de tentatives de correction) n'atteignent aucun objectif quand vous créez des types de condition requise pour la correction de client de Macintosh.
6. Dans le champ texte URL de lien de fichier, tapez l'URL vers lequel les utilisateurs finaux devraient être dirigés afin de télécharger ClamAV 1.1.0.
7. Dans le nom de condition requise le texte a classé, introduit un nom unique qui donne l'action à l'utilisateur final. Ce nom est visible aux utilisateurs dans les dialogues de Clean

Access Agent. Cet exemple utilise le *téléchargement ClamAV*.

8. Dans le champ texte de description, tapez une description de la condition requise et des instructions de guider les utilisateurs qui n'arrivent pas à atteindre la condition requise.
9. Cliquez sur la case de **Mac OS** répertoriée dans la section du système d'exploitation.
10. Cliquez sur Add la **condition requise** afin d'ajouter la condition requise à la liste de condition requise.

La nouvelle condition requise est ajoutée à la liste de condition requise.

[Étape 3. Tracez la condition requise de distribution de lien avec la règle d'installation poids du commerce](#)

1. Cliquez sur l'onglet de **Clean Access Agent**, et puis cliquez sur les **conditions requises**.
2. **Condition requise-règles de clic**.
3. De la liste déroulante de nom de condition requise, choisissez la condition requise que vous avez créée dans l'[étape 2](#).
4. Choisissez le **MacOSX** de la liste déroulante du système d'exploitation. Des règles créées pour le système d'exploitation choisi sont affichées au bas de page.
5. Cliquez sur la case pour la règle que vous avez créée dans l'[étape 1](#), et puis cliquez sur la **mise à jour**.

[Étape 4. Configurez une règle de vérifier si ClamAV est mis à jour](#)

1. Allez à la **Gestion de périphériques > au Clean Access > au Clean Access Agent > aux règles > nouvelle règle poids du commerce**.
2. Introduisez un nom pour la règle. Cet exemple utilise *Is_ClamAV_Updated_OSX*. **Remarque:** Soyez descriptif de sorte que vous puissiez facilement identifier le but de la règle. Vous pouvez n'utiliser des chiffres et des traits de soulignement dans le nom, mais aucun espace.
3. Choisissez **ClamWin** de la liste déroulante de constructeur d'antivirus.
4. Choisissez la **définition de virus** de la liste déroulante de type.
5. Choisissez le **MacOSX** de la liste déroulante du système d'exploitation. Le virus que la définition vérifie la table de MacOSX au bas de page est rempli.
6. Cochez la case d'**installation** pour 1.x.
7. Tapez une description dans le champ texte de description de règle, et cliquez sur la **règle de sauvegarde**.

La nouvelle règle poids du commerce est ajoutée au bas de la liste de règle.

[Étape 5. Configurez une condition requise aux utilisateurs de Remediate si ClamAV n'est pas mis à jour](#)

Si Clean Access Agent le détecte que ClamAV 1.1.0 n'est pas mis à jour sur la machine cliente, il met en quarantaine l'utilisateur. En ce moment, l'utilisateur est équipé de remediate de bouton de mise à jour.

Une fois que l'utilisateur clique sur le bouton de mise à jour, l'agent de Clean Access communique avec le logiciel sous-jacent de ClamAV et demande à ClamAV pour se mettre à jour.

Vous pouvez configurer un type de condition requise de mise à jour de définition poids du

commerce afin d'implémenter cette fonctionnalité.

1. Cliquez sur l'onglet de **Clean Access Agent**, et puis cliquez sur les **conditions requises**.
2. Cliquez sur New la **condition requise**.
3. Choisissez la **mise à jour de définition poids du commerce de la** liste déroulante de type de condition requise.
4. Choisissez **obligatoire** la de la liste déroulante de type d'exécution. Dans cet exemple, l'utilisateur final est au courant de cette condition requise et ne peut pas poursuivre ou avoir l'accès au réseau à moins que le système client réponde à l'exigence. Référez-vous à [configurer une exigence facultative/audit](#) pour des informations sur d'autres types d'application.
5. Choisissez le niveau de priorité d'exécution pour cette condition requise sur la machine cliente. Une haute priorité (par exemple, 1) signifie que cette condition requise est vérifiée le système en avant de toutes autres conditions requises (et apparaît dans les dialogues de Clean Access Agent dans cette commande). Cet exemple suppose que le contrôle de mise à jour de ClamWin est la deuxième condition requise de posture et fixe la priorité à deux (2). **Remarque:** L'agent de Mac OS X ne prend en charge pas la correction automatique. Par conséquent, le type de correction est placé au manuel. En outre, notez que les options de type, d'intervalle, et de nombre de tentatives de correction qui apparaissent à la nouvelle page de configuration de condition requise n'atteignent aucun objectif quand vous créez des types de condition requise pour la correction de client de Macintosh.
6. Choisissez **ClamWin – (Mac OS) de la** liste déroulante de nom de constructeur d'antivirus. **Attention :** Veillez-vous pour choisir le *ClamWin – option (de Mac OS)*, pas l'option de ClamWin. **Remarque:** En date de la release du Cisco NAC 4.5, le type de condition requise de mise à jour poids du commerce est pris en charge seulement avec le MacOSX de ClamAVon. Pour tout autre AV/AS sur le MacOSX, une distribution de lien ou un type local de condition requise de contrôle peut être configurée aux utilisateurs de remédiate si leurs définitions de virus ne sont pas mises à jour.
7. Dans le champ texte de nom de condition requise, introduisez un nom unique qui donne l'action à l'utilisateur final. Ce nom est visible aux utilisateurs dans les dialogues de Clean Access Agent. Cet exemple utilise la *mise à jour ClamAV*.
8. Dans le champ texte de description, tapez une description de la condition requise et des instructions de guider les utilisateurs qui n'arrivent pas à atteindre la condition requise.
9. Cliquez sur la case de **Mac OS** répertoriée dans la section du système d'exploitation.
10. Cliquez sur Add la **condition requise** afin d'ajouter la condition requise à la liste de condition requise.

La nouvelle condition requise est ajoutée à la liste de condition requise.

[Étape 6. Tracez la condition requise de mise à jour de définition poids du commerce avec la règle de définition de virus](#)

1. Cliquez sur l'onglet de **Clean Access Agent**, et puis cliquez sur les **conditions requises**.
2. **Condition requise-règles de clic**.
3. De la liste déroulante de nom de condition requise, choisissez la condition requise que vous avez créée dans l'[étape 5](#).
4. Choisissez le **MacOSX de la** liste déroulante du système d'exploitation. Des règles créées pour le système d'exploitation choisi sont affichées au bas de page.
5. Cliquez sur la case pour la règle que vous avez créée dans l'[étape 4](#), et puis cliquez sur la

mise à jour.

Étape 7. Tracez les conditions requises aux rôles

En ce moment, vous pouvez lier les conditions requises de posture (qui ont été tracées aux règles) au rôle dans lequel l'utilisateur final est placé.

1. Cliquez sur l'onglet de **Clean Access Agent**, et puis cliquez sur les **Rôle-conditions requises**.
2. **Rôle-conditions requises de clic**.
3. Choisissez le **rôle normal de procédure de connexion de la** liste déroulante de type de rôle.
4. Du rôle de l'utilisateur de liste déroulante, choisissez le rôle où vous voulez les conditions requises de posture d'être appliqué. Cet exemple s'applique les conditions requises de posture au rôle des *employés*. Les conditions requises créées plus tôt dans cet exemple sont affichées au bas de page.
5. Vérifiez les cases pour les conditions requises que vous voulez s'appliquer à ce rôle, et cliquez sur la **mise à jour**.

Étape 8. Permettez Access au site de correction dans le rôle provisoire

Une fois que des utilisateurs s'avèrent non-conformes, ils sont mis en quarantaine et placés dans le rôle provisoire. En ce moment, les utilisateurs doivent pouvoir atteindre les ressources en correction (serveur poids du commerce, sites Web, serveurs de correctif, etc.) de sorte qu'elles puissent remédiate elles-mêmes.

À cet effet, vous devez ouvrir l'accès approprié dans le rôle provisoire. Dans cet exemple, les utilisateurs doivent pouvoir atteindre <http://www.clamxav.com> pour les les deux les conditions requises (mise à jour de définition d'installation et de virus).

1. Choisissez la **gestion des utilisateurs > les rôles de l'utilisateur**, et puis cliquez sur l'onglet de **contrôle de trafic**.
2. **Hôte de clic**.
3. Choisissez le **rôle provisoire de la** liste déroulante, et le faites descendre l'écran au bas de la liste.
4. Ajoutez **clamxav.com** à la liste permise d'hôte, et cliquez sur Add. Cette étape s'assure qu'on permet le trafic des clients à <http://www.clamxav.com> par les serveurs NAC. **Remarque:** Ces deux conditions sont importantes : Le serveur NAC emploie la réponse de DN du serveur DNS pour ouvrir dynamiquement l'accès. Par conséquent, le trafic de retour du serveur DNS (réponse de DN) doit passer par le serveur NAC. Vous devez faire définir un serveur DNS de confiance. Pour des pratiques recommandées, Cisco recommande que vous ajoutiez les entrées spécifiques de serveur DNS ici par opposition à faire confiance à tous les serveurs DNS (*). Cet exemple ajoute l'IP de serveur DNS (192.168.2.44) en tant que serveur DNS de confiance. Vous pouvez ajouter les serveurs DNS de confiance par multiple. Si vous ne faites pas définir un serveur DNS de confiance, le gestionnaire NAC vous informe en conséquence par un message suivant les indications de cette image :

Vérifiez l'expérience utilisateur

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Ce scénario de vérification de posture de MAC suppose que votre installation de l'initiale NAC (gestionnaire et serveur NAC) est complète et que le serveur NAC est accessible des machines cliente. Cisco Clean Access Agent 4.5.0.0 devrait être installé sur le MAC qui exécute OSX 10.4 ou plus élevé. Ce scénario suppose que le MAC n'a pas ClamAV installé avant ce test.

1. Procédure de connexion à votre Clean Access Agent (version 4.5.0.0).T'êtes mis en quarantaine et invité au remEDIATE.**Remarque:** Les cases de PASSAGE sont vérifiées, mais non editable, parce que les conditions requises sont obligatoires. Si une condition requise était configurée comme *facultative*, la case de PASSAGE serait editable, et vous pouvez choisir d'ignorer cette condition requise.
2. Clic **Remediate**.Vous êtes réorienté au site Web de ClamAV.
3. Téléchargez et installez ClamAV.Vous pourriez être incité à exécuter l'engine d'antivirus de palourde avant que vous puissiez utiliser ClamAV suivant les indications de cette image :
4. Suivez les instructions à l'écran afin de se terminer l'installation.L'agent de Clean Access affiche le statut de la condition requise de *ClamAV de téléchargement* en tant que réussi et passe à la deuxième condition requise (*mise à jour ClamAV*).Une fois que ClamAV est mis à jour, le statut de la condition requise de *ClamAV de mise à jour* affiche réussi.
5. Clic **complet** pour ouvrir une session au réseau.Une fois que vous ouvrez une session avec succès au réseau, ce les messages apparaît.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- [Support produit de Dispositif Cisco NAC \(Clean Access\)](#)
- [Support et documentation techniques - Cisco Systems](#)