Dispositif NAC (Cisco Clean Access) : Configurer et dépanner les mises à jour des définitions d'antivirus

Contenu

Introduction

Ce document décrit comment configurer et dépanner les conditions requises de mise à jour de définition de l'antivirus (poids du commerce) dans l'appliance du Cisco Network Admission Control (NAC), autrefois connue sous le nom de Cisco Clean Access.

Conditions préalables

Conditions requises

Ce document suppose que Cisco Clean Access, qui inclut Clean Access Manager (CAM) et Clean Access Server (CAS), est installé et fonctionne correctement.

Composants utilisés

Les informations dans ce document sont basées sur le Cisco Clean Access 3.4 et plus tard.

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.

Configurez les conditions requises de mise à jour de définition poids du commerce

Le type de condition requise de **mise à jour de définition poids du commerce** peut être utilisé afin de mettre les dossiers à jour de définition sur un client pour les Produits pris en charge d'antivirus. Si le client n'arrive pas à atteindre la condition requise poids du commerce, Clean Access Agent communique directement avec le logiciel anti-virus installé sur le client et met automatiquement les dossiers à jour de définition quand l'utilisateur clique sur le bouton de **mise à jour** sur le dialogue d'agent.

Les règles poids du commerce incorporent la logique étendue pour 24 constructeurs d'antivirus et sont associées avec des conditions requises de mise à jour de définition poids du commerce. Pour des conditions requises de mise à jour de définition poids du commerce, la configuration est semblable à celle des dispositions douanières, à moins qu'il n'y ait aucun besoin de configurer des contrôles. Vous associez des conditions requises de mise à jour de définition poids du commerce avec un ou plusieurs règles, rôles de l'utilisateur et systèmes d'exploitation poids du commerce et configurez également les instructions de dialogue de Clean Access Agent que vous voulez que l'utilisateur voie si la condition requise poids du commerce échoue.

Remarque: Dans la mesure du possible, il est recommandé pour utiliser des règles poids du commerce tracées aux conditions requises de mise à jour de définition poids du commerce afin de vérifier le logiciel anti-virus sur des clients. Dans le cas d'un produit non-pris en charge poids du commerce, ou si un produit ou la version poids du commerce n'est pas des règles traversantes disponibles poids du commerce, vous avez toujours l'option d'utiliser Cisco avez fourni des pc_checks et des pr_rules pour le constructeur d'antivirus ou de créer de leurs propres contrôles, règles, et conditions requises faits sur commande par la **Gestion de périphériques > le Clean Access > le Clean Access Agent**. Utilisez le nouveau contrôle, la nouvelle règle, et le nouveau fichier/lien/condition requise locale de contrôle.

Cette figure affiche le dialogue de Clean Access Agent qui apparaît quand un client n'arrive pas à atteindre une condition requise de mise à jour de définition poids du commerce.

Règles poids du commerce

Les règles poids du commerce sont les types préconfigurés de règle tracés à la matrice des constructeurs et des Produits originaires dans la liste des produits prise en charge poids du

commerce. Il n'y a aucun besoin de configurer des contrôles avec ce type de règle.

Il y a deux types de base de règles poids du commerce :

- **Règles poids du commerce d'installation** — Cette règle vérifie si le logiciel anti-virus sélectionné est installé pour le SYSTÈME D'EXPLOITATION de client.
- **Règles poids du commerce de définition de virus** — Cette règle vérifie si les fichiers de définition de virus sont à jour sur le client. Des règles poids du commerce de définition de virus peuvent être tracées dans des conditions requises de mise à jour de définition poids du commerce de sorte qu'un utilisateur qui échoue la condition requise puisse cliquer sur le bouton de mise à jour dans l'agent afin d'exécuter automatiquement la mise à jour.

Des règles poids du commerce sont typiquement associées avec des conditions requises de mise à jour de définition poids du commerce. Ces étapes sont exigées afin de créer des conditions requises de mise à jour de définition poids du commerce :

1. Vérifiez les informations de support poids du commerce
2. Créez la règle poids du commerce
3. Créez la condition requise de mise à jour de définition poids du commerce
4. Condition requise de carte aux règles
5. Appliquez-vous les conditions requises au rôle
6. Validez les conditions requises

Vérifiez les informations de support poids du commerce

L'appliance de Cisco NAC permet des plusieurs versions de Clean Access Agent à utiliser sur le réseau. Les nouvelles mises à jour à l'agent ajoutent le soutien des derniers Produits d'antivirus pendant qu'elles sont sorties. Le système sélectionne la meilleure méthode, date de Def ou version de Def afin d'exécuter des contrôles de définition poids du commerce basés sur les Produits poids du commerce disponibles et la version de l'agent. La page des informations de support poids du commerce fournit des détails sur la compatibilité d'agent en plus défunte liste des produits prise en charge poids du commerce téléchargée au CAM. Cette page répertorie la dernières version et date des fichiers de définition pour chaque produit poids du commerce aussi bien la version de spécification de base de l'agent requis pour le support produit. Vous pouvez comparer les informations poids du commerce du client contre la page des informations de support poids du commerce afin de vérifier que le fichier de définition qu'un client a est le plus tardif. Si vous exécutez des plusieurs versions de l'agent sur votre réseau, cette page peut aider à dépanner quelle version doit être exécutée afin de prendre en charge un produit particulier.

Terminez-vous ces étapes afin de visualiser des détails de support d'agent :

1. Choisissez la **Gestion de périphériques > le Clean Access > le Clean Access Agent > les règles > les informations de support AV/AS**.
2. Choisissez l'**antivirus du** menu déroulant de catégorie.
3. Choisissez un **constructeur d'antivirus du** menu déroulant.
4. Choisissez **Windows Vista/XP/2K** ou **Windows 9x/ME du** menu déroulant **du système d'exploitation** afin de visualiser les informations de support pour ces systèmes client. Ceci remplit tables comme affichées :**Version minimum d'agent requise pour prendre en charge des Produits poids du commerce** — affiche la version minimum d'agent requise afin de prendre en charge chaque produit poids du commerce. Par exemple, un agent de 4.0.0.0 peut se connecter dans un rôle qui exige la protection antivirus 1.x de centre de protection et

sécurité d'AOL, mais pour 3.6.0.0 ou un agent plus tôt, ce contrôle échoue. Notez que si une version de l'agent prend en charge la date de Def et les contrôles de version de Def, le contrôle de version de Def est utilisé.**La plus défuntes version/date de définition de virus pour le constructeur Selected** — affiche la dernières version et informations de date pour le produit poids du commerce. Le logiciel poids du commerce pour un client à jour doit afficher les mêmes valeurs.

Remarque: L'agent envoie ses informations de version au CAM, et de CAM les tentatives toujours d'utiliser la version de définition de virus pour le poids du commerce vérifie d'abord. Si la version n'est pas disponible, le CAM utilise la date de définition de virus à la place.

Conseil : Vous pouvez également visualiser la dernière version du fichier de définition quand vous choisissez un constructeur poids du commerce de la **nouvelle** forme de **règle poids du commerce**.

Créez la règle poids du commerce

Terminez-vous ces étapes afin de créer une règle poids du commerce :

1. Veillez-vous pour avoir la dernière version de la liste des produits prise en charge AV/AS.
2. Choisissez la **Gestion de périphériques > le Clean Access > le Clean Access Agent > les règles > nouvelle règle poids du commerce**.
3. Introduisez un **nom de règle**. Vous pouvez n'utiliser des chiffres et des traits de soulignement, mais aucun espace dans le nom.
4. Choisissez un **constructeur d'antivirus du** menu déroulant. Ceci remplit **vérifie la** table **sélectionnée de systèmes d'exploitation au** bas de page avec les Produits et les versions du produit pris en charge de ce constructeur pour le **système d'exploitation** sélectionné.
5. Du menu déroulant de **type**, choisissez l'**installation** ou la **définition de virus**. Ceci active les cases pour les colonnes correspondantes de définition d'installation ou de virus dans la table.
6. Choisissez un **système d'exploitation du** menu déroulant, Windows Vista/XP/2K ou Windows ME/98. Ceci affiche les versions du produit prises en charge pour ce SYSTÈME D'EXPLOITATION de client dans la table.
7. Tapez une **description** facultative de **règle**.
8. Dans **vérifie la** table **sélectionnée de systèmes d'exploitation**, choisissent les versions du produit que vous voulez vérifier sur le client. Afin de faire ceci, vérifiez un ou plusieurs cases dans les colonnes correspondantes de **définition d'installation** ou de **virus**. **TOUS** moyens que vous voulez vérifier n'importe quel produit et n'importe quelle version de ce constructeur poids du commerce. **L'installation** vérifie si le produit est installé, et la **définition de virus** vérifie si les fichiers de définition de virus sont à jour sur le client pour le produit spécifié.
9. Cliquez sur Add la **règle**. La nouvelle règle poids du commerce est ajoutée au bas de la **liste de règle** avec le nom que vous avez fourni.

Créez la condition requise de mise à jour de définition poids du commerce

Ces étapes affichent comment créer une nouvelle condition requise de mise à jour de définition poids du commerce afin de vérifier le système client pour les Produits spécifiés et des versions poids du commerce avec un poids du commerce associé ordonnent. Si les fichiers de définition d'antivirus du client ne sont pas à jour, l'utilisateur peut simplement cliquer sur le bouton de **mise à jour** sur Clean Access Agent, et l'agent fait lancer le logiciel poids du commerce de résident son propre mécanisme de mise à jour. Notez que le mécanisme réel diffère pour différents Produits

poids du commerce, par exemple, des modifications direct contre le paramètre de la ligne de commande.

1. Sur l'onglet de **Clean Access Agent**, cliquez sur le lien de sous-menu de **conditions requises**, et puis la **nouvelle condition requise**.
2. Pour le **type de condition requise** choisissez la **mise à jour de définition poids du commerce**.
3. **N'imposez pas l'**option de **condition requise** est vérifié par défaut, qui indique la condition requise de mise à jour de définition poids du commerce comme **facultative**.**Remarque:** Puisque le processus de Windows Update fonctionne à l'arrière-plan, **n'imposez pas la condition requise** est placé par défaut afin d'optimiser l'expérience utilisateur. Il est recommandé pour laisser cette condition requise pendant que facultatif si vous choisissez automatiquement le télécharger et installez l'option. Une mise à jour forcée par WSUS peut prendre un moment, et est lancée et passage à l'arrière-plan.
4. Choisissez la **priorité de l'**exécution pour cette condition requise sur le client. Une haute priorité, telle que 1, signifie que cette condition requise est vérifiée le système en avant de toutes autres conditions requises et apparaît dans les dialogues d'agent dans cette commande. Notez que si une condition obligatoire échoue, l'agent ne continue pas le passé ce point jusqu'à ce que cette condition requise réussisse.
5. Choisissez un **nom de constructeur d'antivirus du** menu déroulant. Le tableau de **Produits** présente toutes les versions du produit de définition de virus prises en charge pour chaque SYSTÈME D'EXPLOITATION de client.
6. Pour le **nom de condition requise**, introduisez un nom unique pour identifier cette condition requise de fichier de définition poids du commerce dans l'agent. Le nom est visible aux utilisateurs sur les dialogues de Clean Access Agent.
7. Dans le **champ description**, tapez une description de la condition requise et des instructions de guider les utilisateurs qui n'arrivent pas à atteindre la condition requise. Pour une condition requise de mise à jour de définition poids du commerce, vous devez inclure des instructions pour que les utilisateurs cliquent sur le bouton de **mise à jour** afin de mettre à jour leurs systèmes. Maintenez ces informations dans l'esprit :**La mise à jour de définition poids du commerce** affiche le bouton de **mise à jour** sur l'agent.**COMME la mise à jour de définition** affiche le bouton de **mise à jour** sur l'agent.**Les Windows Update** affichent le **bouton de mise à jour** sur l'agent.
8. Vérifiez un ou plusieurs de ces cases afin de placer les **systèmes d'exploitation** pour la condition requise :**Windows toutWindows 2000Windows MEWindows 98Windows XP (tous) ou un ou plusieurs des systèmes d'exploitation spécifiques de Windows XPWindows Vista (tous) ou un ou plusieurs des systèmes d'exploitation spécifiques de Windows Vista**
9. Cliquez sur Add la **condition requise** afin d'ajouter la condition requise à la liste de condition requise.

Condition requise de carte aux règles

Une fois que la condition requise est créée et les liens et les instructions de correction sont spécifiés, tracez la condition requise à une règle ou à un ensemble de règles. Une cartographie de condition requise-à-règle associe le ruleset qui vérifie si le système client répond à l'exigence à l'action d'exigence de l'utilisateur (bouton d'agent, instructions, liens) requise pour que le système client se conforme.

1. Sur l'onglet de **Clean Access Agent**, cliquez sur le sous-menu de **conditions requises**, et puis

ouvrez la forme de Condition requise-**règles**.
2. Du menu de **nom de condition requise**, choisissez la condition requise de tracer.
3. Vérifiez le système d'exploitation pour la condition requise dans le menu **du système d'exploitation**. **Les règles pour la** liste **du système d'exploitation Selected** est remplies avec toutes les règles disponibles pour le SYSTÈME D'EXPLOITATION choisi.
4. Pour des règles de définition de virus poids du commerce (fond jaune), vous pouvez sur option configurer le CAM pour permettre à des fichiers de définition sur le client pour être un certain nombre de jours plus que ce qui le CAM a fourni par des **mises à jour**. Voir des **règles > les informations de support AV-AS** pour les dernières dates de fichier de produit. Ceci te permet pour configurer la marge de sécurité dans une condition requise de sorte que si aucun nouveau fichier de définition de virus n'est sorti d'un constructeur du produit, vos clients puissent encore passer la condition requise. Pour ce faire, suivez ces étapes :Cochez les **règles de définition de virus poids du commerce, permettez au fichier de définition pour être des jours x plus que la** case.Tapez un nombre dans la zone de texte. Le par défaut est **0**, qui indique que la date de définition ne peut pas être plus ancienne que le fichier/date du système.Sélectionnez une de ces options :**La dernière date de fichier** — Ceci permet au fichier de définition de client pour être plus ancien que la dernière date de définition de virus sur le CAM par le nombre de jours où vous spécifiez.**Date du système en cours** — Ceci permet au fichier de définition de client pour être plus ancien que la date du système de CAM où la dernière modification a été exécutée par le nombre de jours où vous spécifiez.
5. Faites descendre l'écran la page et cochez la case **choisie** à côté de chaque règle que vous voulez associer avec la condition requise. Les règles sont appliquées dans leur ordre de priorité, comme décrit dans cette table :
6. Pour des **exigences répondues si**, choisissez une de ces options :**Toutes les règles sélectionnées réussissent** — si toutes les règles doivent être satisfaites pour que le client soit considéré conformément à la condition requise**N'importe quelle règle sélectionnée réussit** — si au moins une règle sélectionnée doit être satisfaite pour que le client soit considéré conformément à la condition requise**Aucune règle sélectionnée ne réussit** — si les règles sélectionnées doivent tout échouer pour que le client soit considéré conformément à la condition requiseSi les clients ne sont pas conformément à la condition requise, ils doivent installer le logiciel associé avec la condition requise ou se terminer les étapes priées.
7. Cliquez sur **Update**.

Appliquez-vous les conditions requises au rôle

Une fois que des conditions requises sont créées, configuré avec la correction fait un pas, et associé avec des règles, elles doivent être tracées aux rôles de l'utilisateur. Cette étape s'applique vos conditions requises aux groupes d'utilisateurs dans le système.

Remarque: Veillez-vous déjà pour faire créer des rôles d'utilisateur de connexion normaux.

1. Sur l'onglet de **Clean Access Agent**, cliquez sur le lien de sous-menu de Rôle-**conditions requises**.
2. **Du menu Type de rôle**, choisissez le type du rôle pour configurer. Dans la plupart des cas, c'est **rôle normal de procédure de connexion**.
3. Choisissez le nom du rôle du **rôle de l'utilisateur de** menu.
4. Cochez la case **choisie** pour chaque condition requise que vous voulez s'appliquer aux utilisateurs dans le rôle.

5. Cliquez sur **Update**.
6. Avant que vous terminiez, assurez-vous que des utilisateurs dans le rôle sont requis d'utiliser Clean Access Agent.

Validez les conditions requises

Clean Access Manager valide automatiquement des conditions requises et des règles pendant qu'elles sont créées. La colonne de **validité** sous la **Gestion de périphériques > le Clean Access > le Clean Access Agent > les conditions requises > la liste de condition requise** affiche la validité de condition requise, comme affiché :

- — La condition requise est valide.
- — La condition requise est non valide. Mettez en valeur cette icône avec votre souris dans l'affichage de commande le message d'état de validité pour cette condition requise. Les états de message d'état qui ordonnent et qui vérifient des causes la condition requise d'être non valides, dans ce format :`Invalid rule [rulename] in package [requirementname] (Rule verification error:
Invalid check [checkname] in rule expression)`

L'exigence doit être corrigée et être prévue valide avant qu'elle puisse être utilisée. Typiquement, les conditions requises et les règles deviennent non valides quand il y a une non-concordance du système d'exploitation.

Afin de corriger une condition requise non valide, terminez-vous ces étapes :

1. Choisissez la **Gestion de périphériques > le Clean Access > le Clean Access Agent > les conditions requises > les Condition requise-règles**.
2. Corrigez tous les règles ou contrôles non valides.
3. Choisissez le **nom** non valide de **condition requise du** menu déroulant.
4. Choisissez le **système d'exploitation**.
5. Assurez-vous l'**exigence répondue si** : l'expression est correctement configurée.
6. Assurez-vous les règles sélectionnées pour la condition requise sont valides, qui signifie qu'elles ont un coche bleu dans la colonne de validité.

Règles de Cisco

Une règle est une déclaration conditionnelle composée d'un ou plusieurs contrôles. Une règle combine des contrôles avec les opérateurs logiques afin de former une déclaration booléenne qui peut tester de plusieurs caractéristiques du système client.

L'appliance de Cisco NAC fournit un ensemble de règles préconfigurées et les contrôles par les mises à jour joignent. Les règles préconfigurées ont un préfixe des `RP` dans leurs noms, tels que le `pr_AutoUpdateCheck_Rule`. Voir pour en savoir plus de règles préconfiguré par Cisco (le « pr_ »).

Contrôles de Cisco

Un contrôle est une déclaration conditionnelle qui examine une caractéristique du système client, tel qu'un fichier, une clé de registre, un service, ou une application. Les contrôles préconfigurés ont un préfixe de `PC` dans leurs noms, tels que `pc_Hotfix828035`. Ce tableau présente les types de contrôles disponibles et ce qu'elles testent.

Catégorie de contrôle	Type de contrôle
Contrôle de registre	• si une clé de registre existe • valeur de clé de registre
Contrôle de fichier	• si un fichier existe • date de modification ou de création • version du fichier
Entretenez le contrôle	• si un service fonctionne
Contrôle d'application	• si une application fonctionne

Cisco a préconfiguré des règles (« pr_ ")

L'appliance de Cisco NAC fournit un ensemble de règles et de contrôles préconfigurés qui sont téléchargés au CAM par la page de **mises à jour** sur la console Web de CAM, sous la **Gestion de périphériques > le Clean Access > le Clean Access Agent > les mises à jour**.

Les règles préconfigurées ont un préfixe des `RP` dans leurs noms, par exemple des `pr_XP_Hotfixes`, et peuvent être copiées pour l'usage comme modèle, mais ne peuvent pas être éditées ou retirées. Vous pouvez cliquer sur le bouton d'**éditer** pour n'importe quelle règle de `pr_` afin de visualiser l'expression de règle qui la définit. L'expression de règle pour une règle préconfigurée se compose de contrôles préconfigurés, tels que `pc_Hotfix835732`, et d'opérateurs booléens. L'expression de règle pour des règles préconfigurées est mise à jour par des mises à jour de Cisco. Par exemple, quand de nouveaux correctifs essentiels de système d'exploitation windows sont relâchés pour Windows XP, la règle de `pr_XP_Hotfixes` est mise à jour avec les contrôles relatifs de correctif.

Des règles préconfigurées sont répertoriées sous la **Gestion de périphériques > le Clean Access > le Clean Access Agent > les règles > la liste de règle**. Les contrôles préconfigurés ont un préfixe de `PC` dans leurs noms et sont répertoriés sous la **Gestion de périphériques > le Clean Access > le Clean Access Agent > les règles > la liste de contrôle**.

Remarque: Cisco a préconfiguré des règles sont destinés pour fournir le support pour des correctifs essentiels de système d'exploitation windows seulement.

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Cisco Clean Access ne met pas à jour la définition poids du commerce pour des clients

Procédez comme suit pour résoudre ce problème :

1. Dans le CAM, choisissez la **Gestion de périphériques > le Clean Access > les conditions requises > les Condition requise-règles**.
2. En désélectionnez les règles préconfigurées (`pr_`), si.

3. Sélectionnez les règles appropriées poids du commerce.

CCA incapable de détecter le poids du commerce

Si vous suspectez le CCA ne le détecte pas ou identifier le certain poids du commerce vérifie, vous doivent exécuter l'outil de diagnostic OESIS dans le client.

Procédez comme suit :

1. Se connecter d'enable.Référez-vous au debug d'enable ouvrant une session Clean Access Agent pour des instructions sur la façon dont activer mettent au point ouvrir une session le client.
2. Tentative d'ouvrir une session.
3. Exécutez l'outil de diagnostic OESIS.
4. Se connecter de débronchement.

Remarque: Si vous pouvez saisir une exportation de la structure de clé de registre du produit poids du commerce, normalement située à HKLM \ à logiciel \ à <av_vendor>, qui est utile aussi.

Informations connexes

- Page de support de Dispositif Cisco NAC (Clean Access)
- Support et documentation techniques - Cisco Systems