Dispositivo NAC (acceso limpio de Cisco): Configure y resuelva problemas las actualizaciones de la definición del antivirus

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Convenciones
Requisitos de la actualización de la definición de la configuración AV
Reglas AV
Verifique la información de servicio técnico AV
Cree la regla AV
Cree el requisito de la actualización de la definición AV
Asocie el requisito a las reglas
Aplique los requisitos al papel
Valide los requisitos
Reglas de Cisco
Controles de Cisco
Cisco preconfiguró las reglas (“pr_ ")
Troubleshooting
El acceso limpio de Cisco no pone al día la definición AV para los clientes
CCA incapaz de detectar el AV
Información Relacionada

Introducción

Este documento describe cómo configurar y resolver problemas los requisitos de la actualización de la definición del antivirus (AV) en el dispositivo del Cisco Network Admission Control (NAC), conocido antes como acceso limpio de Cisco.

prerrequisitos

Requisitos

Este documento asume que el acceso limpio de Cisco, que incluye limpie el Access Manager (CAM) y el servidor de acceso limpio (CAS), está instalado y trabaja correctamente.

Componentes Utilizados

La información en este documento se basa en el Cisco Clean Access 3.4 y posterior.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configure los requisitos de la actualización de la definición AV

El tipo del requisito de la **actualización de la definición AV** puede ser utilizado para poner al día los archivos de definición en un cliente para los Productos soportados del antivirus. Si el cliente no puede cumplir el requisito AV, el agente limpio del acceso comunica directamente con el Software anti virus instalado en el cliente y pone al día automáticamente los archivos de definición cuando el usuario hace clic el **botón Update Button** en el diálogo del agente.

Las reglas AV incorporan la lógica extensa para 24 vendedores del antivirus y se asocian a los requisitos de la actualización de la definición AV. Para los requisitos de la actualización de la definición AV, la configuración es similar a la de las disposiciones aduaneras, a menos que no haya necesidad de configurar los controles. Usted asocia los requisitos de la actualización de la definición AV a una o más reglas, a los rol del usuario y a los sistemas operativos AV y también configura las instrucciones limpias del diálogo del agente del acceso que usted quisiera que el usuario viera si el requisito AV falla.

Nota: En lo posible, se recomienda para utilizar las reglas AV asociadas a los requisitos de la actualización de la definición AV para marcar el Software anti virus en los clientes. En el caso de un producto NON-soportado AV, o si un producto o la versión AV no es reglas directas disponibles AV, usted tiene siempre la opción para utilizar Cisco proporcionó a los pc_checks y los pr_rules para el vendedor del antivirus o crear de sus propias comprobaciones personalizadas, reglas, y requisitos a través de la **Administración de dispositivos > limpian el acceso > limpian el agente del acceso**. Utilice el nuevo control, la nueva regla, y el nuevo archivo/el link/el requisito local del control.

Esta figura muestra el diálogo limpio del agente del acceso que aparece cuando un cliente no puede cumplir un requisito de la actualización de la definición AV.

El AV gobierna

Las reglas AV son tipos preconfigurados de la regla asociados a la matriz de los vendedores y los Productos originados en el producto soportado AV enumeran. No hay necesidad de configurar los controles con este tipo de regla.

Hay dos tipos básicos de reglas AV:

- **Reglas de la instalación AV** — Esta regla marca si el Software anti virus seleccionado está instalado para el OS cliente.
- **Reglas de la definición de virus AV** — Esta regla marca si los archivos de definición de virus son actualizados en el cliente. Las reglas de la definición de virus AV se pueden asociar en los requisitos de la actualización de la definición AV de modo que un usuario que falla el requisito pueda hacer clic el botón Update Button en el agente para ejecutar automáticamente la actualización.

Las reglas AV se asocian típicamente a los requisitos de la actualización de la definición AV. Estos pasos se requieren para crear los requisitos de la actualización de la definición AV:

1. Verifique la información de servicio técnico AV
2. Cree la regla AV
3. Cree el requisito de la actualización de la definición AV
4. Asocie el requisito a las reglas
5. Aplique los requisitos al papel
6. Valide los requisitos

Verifique la información de servicio técnico AV

El dispositivo NAC de Cisco permite que las versiones múltiples del agente limpio del acceso sean utilizadas en la red. Las nuevas actualizaciones al agente agregan el soporte para los últimos Productos del antivirus mientras que se liberan. El sistema escoge el mejor método, fecha del def o versión del def para ejecutar los controles de la definición AV basados en los Productos AV disponibles y la versión del agente. La página de la información de servicio técnico AV proporciona los detalles en la compatibilidad del agente con la última lista soportada del producto AV descargada al CAM. Esta página enumera la últimas versión y fecha de los archivos de definición para cada producto AV también la versión de la línea de fondo del agente necesario para el soporte de productos. Usted puede comparar la información AV del cliente contra la página de la información de servicio técnico AV para verificar que el archivo de definición que un cliente tiene es el más último. Si usted funciona con las versiones múltiples del agente en su red, esta página puede ayudar a resolver problemas qué versión se debe funcionar con para soportar un producto particular.

Complete estos pasos para ver los detalles del soporte de agente:

1. Elija la **Administración de dispositivos > limpian el acceso > limpian el agente del acceso > las reglas > la información de servicio técnico AV/AS**.
2. Elija el **antivirus del** menú desplegable de la categoría.
3. Elija a un **vendedor del antivirus del** menú desplegable.
4. Elija **Windows Vista/XP/2K** o **Windows 9x/ME del** menú desplegable del **sistema operativo** para ver la información de servicio técnico para esos sistemas del cliente. Esto puebla las tablas como se muestra:**Versión agente mínima requerida para soportar los Productos AV** — muestra la versión agente mínima requerida para soportar cada producto AV. Por ejemplo, un agente de 4.0.0.0 puede registrar en un papel que requiera la protección contra virus 1.x del centro de la seguridad de AOL, pero para 3.6.0.0 o un agente anterior, este control falla. Observe que si una versión de la fecha del def de los soportes de agente y de la versión del def marca, el control de la versión del def está utilizado.**La últimas versión/fecha de la definición de virus para el vendedor seleccionado** — visualiza la versión y la información más recientes de la fecha para el producto AV. El software AV para un cliente actualizado

debe visualizar los mismos valores.

Nota: El agente envía su información de la versión al CAM, y el CAM intenta siempre utilizar la versión de la definición de virus para los controles AV primero. Si la versión no está disponible, el CAM utiliza la fecha de la definición de virus en lugar de otro.

Consejo: Usted puede también ver la última versión del archivo de definición cuando usted elige a un vendedor AV de la **nueva** forma de la **regla AV**.

Cree la regla AV

Complete estos pasos para crear una regla AV:

1. Aseegurese le tener la última versión de la lista soportada del producto AV/AS.
2. Elija la **Administración de dispositivos > limpian el acceso > limpian el agente > las reglas del acceso > nueva regla AV**.
3. Teclee un **nombre de la regla**. Usted puede utilizar los dígitos y los caracteres de subrayado, pero ningunos espacios en el nombre.
4. Elija a un **vendedor del antivirus del** menú desplegable. Esto puebla las **comprobaciones para la** tabla **seleccionada de los sistemas operativos** en la parte inferior de la página con los productos admitidos y las versiones del producto de este vendedor para el **sistema operativo** seleccionado.
5. Del menú desplegable del **tipo**, elija la **instalación** o la **definición de virus**. Esto habilita las casillas de verificación para las columnas correspondientes de la instalación o de la definición de virus en la tabla.
6. Elija un **sistema operativo del** menú desplegable, Windows Vista/XP/2K o Windows ME/98. Esto visualiza las versiones del producto soportadas para este OS cliente en la tabla.
7. Teclee una **descripción** opcional de la **regla**.
8. En las **comprobaciones para los sistemas operativos seleccionados** presente, elija las versiones del producto que usted quiere comprobar para el cliente. Para hacer esto, marque una o más casillas de verificación en las columnas correspondientes de la **instalación** o de la **definición de virus**. **CUALQUIER** medios que usted quiera marcar para saber si hay cualquier producto y cualquier versión de este vendedor AV. **La instalación** marca si el producto está instalado, y la **definición de virus** marca si los archivos de definición de virus son actualizados en el cliente para el producto especificado.
9. El tecleo **agrega la regla**. La nueva regla AV se agrega en la parte inferior de la **lista de la regla** con el nombre que usted proporcionó.

Cree el requisito de la actualización de la definición AV

Estos pasos muestran cómo crear un nuevo requisito de la actualización de la definición AV para marcar el sistema del cliente para los Productos especificados y las versiones AV con un AV asociado gobiernan. Si los archivos de definición del antivirus del cliente no son actualizados, el usuario puede hacer clic simplemente el **botón Update Button** en el agente limpio del acceso, y el agente hace el software del residente AV poner en marcha su propio mecanismo de la actualización. Observe que el mecanismo real diferencia para diversos Productos AV, por ejemplo, las actualizaciones vivas contra el parámetro de la línea de comando.

1. En la lengueta **limpia del agente del acceso**, haga clic el link del submenú de los **requisitos**, y entonces el **nuevo requisito**.

2. Para el **tipo del requisito** elija la **actualización de la definición AV**.
3. **No aplique la** opción del **requisito** se marca por abandono, que señala el requisito de la actualización de la definición AV como **opcional**.**Nota:** Porque el proceso de Windows Update se ejecuta en el fondo, **no aplique el requisito** se fija por abandono para optimizar la experiencia del usuario. Se recomienda para dejar este requisito mientras que opcional si usted elige automáticamente el descargar y instala la opción. Una actualización forzada WSUS puede tardar un rato, y se inicia y funcionamiento en el fondo.
4. Elija la **prioridad de la** ejecución para este requisito en el cliente. Un prioritario, tal como 1, significa que este requisito está comprobado el sistema delante del resto de los requisitos y que aparece en los diálogos del agente en esa orden. Observe que si un requisito obligatorio falla, el agente no continúa el pasado esa punta hasta que ese requisito tenga éxito.
5. Elija un **nombre del proveedor del antivirus del** menú desplegable. **Los Productos** presentan las listas todas las versiones del producto de la definición de virus soportadas para cada OS cliente.
6. Para el **nombre del requisito**, teclee un nombre único para identificar este requisito del archivo de definición AV en el agente. El nombre es visible a los usuarios en los diálogos limpios del agente del acceso.
7. En el **campo Description (Descripción)**, teclee una descripción del requisito y de las instrucciones de dirigir a los usuarios que no pueden cumplir el requisito. Para un requisito de la actualización de la definición AV, usted debe incluir las instrucciones para que los usuarios hagan clic el **botón Update Button** para poner al día sus sistemas. Tenga esta información presente:**La actualización de la definición AV** visualiza el **botón Update Button** en el agente.**COMO la actualización de la definición** visualiza el **botón Update Button** en el agente.**Windows Update** visualiza el **botón Update Button** en el agente.
8. Marque uno o más de estas casillas de verificación para fijar los **sistemas operativos** para el requisito:**Windows todoWindows 2000Windows MEWindows 98Windows XP (todo) o uno o más de los sistemas operativos específicos de Windows XPWindows Vista (todo) o uno o más de los sistemas operativos específicos de Windows Vista**
9. El tecleo **agrega el requisito** para agregar el requisito a la lista del requisito.

Requisito del mapa a las reglas

Una vez que se crea el requisito y se especifican los links y las instrucciones de la corrección, asocie el requisito a una regla o a un conjunto de reglas. Una asignación de la requisito-a-regla asocia el ruleset que marca si el sistema del cliente cumple el requisito a la acción del requisito del usuario (botón del agente, instrucciones, links) necesaria para que cumpla el sistema del cliente.

1. En la lengueta **limpia del agente del acceso**, haga clic el submenú de los **requisitos**, y después abra la forma de las Requisito-**reglas**.
2. Del menú del **nombre del requisito**, elija el requisito de asociar.
3. Verifique el sistema operativo para el requisito en el menú del **sistema operativo**. **Las reglas para la** lista **seleccionada del sistema operativo** se pueblan con todas las reglas disponibles para el OS elegido.
4. Para las reglas de la definición de virus AV (fondo amarillo), usted puede configurar opcionalmente el CAM para permitir que los archivos de definición en el cliente sean varios días más viejo que lo que el CAM tiene disponible desde **actualizaciones**. Vea las **reglas > la información de servicio técnico AV-AS** para las últimas fechas del archivo del producto. Esto

permite que usted configure la deriva en un requisito de modo que si no se libera ningunos nuevos archivos de definición de virus de un proveedor de productos, sus clientes puedan todavía pasar el requisito. A tal efecto, complete estos pasos:Marque las **reglas de la definición de virus AV, permita que el archivo de definición sea días x más viejos que la** casilla de verificación.Teclee un número en el cuadro de texto. El valor por defecto es **0**, que indica que la fecha de la definición no puede ser más vieja que el archivo/la fecha del sistema.Seleccione una de estas opciones:**La última fecha del archivo** — Esto permite que el archivo de definición del cliente sea más viejo que la última fecha de la definición de virus en el CAM por el número de días que usted especifica.**Fecha del sistema actual** — Esto permite que el archivo de definición del cliente sea más viejo que la fecha del sistema CAM en que la **actualización** más reciente fue realizada por el número de días que usted especifica.

5. Navegue hacia abajo la página y marque la casilla de verificación **selecta** al lado de cada regla que usted quiere asociarse al requisito. Las reglas se aplican en su orden de prioridad, según lo descrito en esta tabla:
6. Para los **requisitos cumplidos si**, elija una de estas opciones:**Todas las reglas seleccionadas tienen éxito** — si todas las reglas se deben satisfacer para que el cliente sea considerado de acuerdo con el requisito**Cualquier regla seleccionada tiene éxito** — si por lo menos una regla seleccionada se debe satisfacer para que el cliente sea considerado de acuerdo con el requisito**Ninguna regla seleccionada tiene éxito** — si las reglas seleccionadas se deben todo el fall para que consideren el cliente de acuerdo con el requisitoSi los clientes no están de acuerdo con el requisito, deben instalar el software asociado al requisito o completar los pasos obligatorios.
7. Haga clic en **Update** (Actualizar).

Aplique los requisitos al papel

Una vez que se crean los requisitos, configurado con la corrección camina, y asociado a las reglas, necesitan ser asociados a los rol del usuario. Este paso aplica sus requisitos a los grupos de usuarios en el sistema.

Nota: Aseegurese le ya hacer los papeles de usuario que ingresa al sistema normales crear.

1. En la lengueta **limpia del agente del acceso**, haga clic el link del submenú de los Papel-**requisitos**.
2. Del menú del **tipo del papel**, elija el tipo del papel para configurar. En la mayoría de los casos, éste es **papel normal del login**.
3. Elija el nombre del papel del **rol del usuario del** menú.
4. Marque la casilla de verificación **selecta** para cada requisito que usted quiere aplicarse a los usuarios en el papel.
5. Haga clic en **Update** (Actualizar).
6. Antes de que usted acabe, aseegurese a los usuarios en el papel se requieren para utilizar el agente limpio del acceso.

Valide los requisitos

El Access Manager limpio valida automáticamente los requisitos y las reglas mientras que se crean. La columna de la **validez** bajo **Administración de dispositivos > acceso limpio > agente limpio del acceso > los requisitos > lista del requisito** visualiza la validez del requisito, como se

muestra:

- — El requisito es válido.
- — El requisito es inválido. Resalte este icono con su ratón en la visualización de la orden el mensaje de estado de la validez para este requisito. Los estados del mensaje de estado que gobiernan y que marcan las causas el requisito de ser inválidos, en este formato:`Invalid rule [rulename] in package [requirementname] (Rule verification error: Invalid check [checkname] in rule expression)`

El requisito debe ser corregido y ser hecho válido antes de que pueda ser utilizado. Típicamente, los requisitos y las reglas llegan a ser inválidos cuando hay una discordancía del sistema operativo.

Para corregir un requisito inválido, complete estos pasos:

1. Elija la **Administración de dispositivos > limpian el acceso > limpian el agente > los requisitos > las Requisito-reglas del acceso**.
2. Corrija cualesquiera reglas o control inválidas.
3. Elija el **nombre** inválido del **requisito del** menú desplegable.
4. Elija el **sistema operativo**.
5. Aseegurese el **requisito cumplido si**: la expresión se configura correctamente.
6. Aseegurese las reglas seleccionadas para el requisito son válido, que significa que él tiene una marca de tilde azul en la columna de la validez.

Reglas de Cisco

Una regla es una declaración condicional compuesta de uno o más controles. Una regla combina los controles con los operadores lógicos para formar una declaración boleana que pueda probar las características múltiples del sistema del cliente.

El dispositivo NAC de Cisco proporciona un conjunto de las reglas preconfiguradas y los controles a través de las actualizaciones conectan. Las reglas preconfiguradas tienen un prefijo de las `RRPP` en sus nombres, tales como `pr_AutoUpdateCheck_Rule`. Vea las reglas preconfiguradas Cisco (“pr_”) para más información.

Controles de Cisco

Un control es una declaración condicional que examina una característica del sistema del cliente, tal como un archivo, una clave de registro, un servicio, o una aplicación. Los controles preconfigurados tienen un prefijo de la `PC` en sus nombres, tales como `pc_Hotfix828035`. Esta tabla enumera los tipos de controles disponibles y qué él prueba.

Categoría del control	Tipo del control
Control del registro	• independientemente de si existe una clave de registro • valor de clave de registro
Control del archivo	• independientemente de si existe un archivo • fecha de la modificación o de la creación

	• versión del archivo
Mantenga el control	• independientemente de si un servicio se ejecuta
Control de la aplicación	• independientemente de si una aplicación se ejecuta

Cisco preconfiguró las reglas (“pr_ ")

El dispositivo NAC de Cisco proporciona un conjunto de las reglas preconfiguradas y los controles que se descargan al CAM a través de la página de las **actualizaciones** en la consola Web CAM, bajo **Administración de dispositivos > limpian el acceso > limpian el agente > las actualizaciones del acceso**.

Las reglas preconfiguradas tienen un prefijo de las `RRPP` en sus nombres, por ejemplo los `pr_XP_Hotfixes`, y se pueden copiar para el uso como plantilla, pero no pueden ser editadas o ser quitadas. Usted puede hacer clic el **botón Edit** para cualquier regla del `pr_` para ver la expresión de la regla que la define. La expresión de la regla para una regla preconfigurada se compone de los controles preconfigurados, tales como `pc_Hotfix835732`, y de los operadores boleanos. La expresión de la regla para las reglas preconfiguradas es actualizada a través de las actualizaciones de Cisco. Por ejemplo, cuando el nuevo hotfixes crítico del OS (Sistema operativo) Windows se libera para Windows XP, la regla de los `pr_XP_Hotfixes` se pone al día con los controles relacionados del hotfix.

Las reglas preconfiguradas son mencionadas bajo **Administración de dispositivos > limpian el acceso > limpian el agente del acceso > las reglas > la lista de la regla**. Los controles preconfigurados tienen un prefijo de la `PC` en sus nombres y son mencionados bajo **Administración de dispositivos > limpian el acceso > limpian el agente > las reglas > la lista de verificación del acceso**.

Nota: Cisco preconfiguró las reglas se piensa proporcionar el soporte para el hotfixes crítico del OS (Sistema operativo) Windows solamente.

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

El acceso limpio de Cisco no pone al día la definición AV para los clientes

Complete estos pasos para resolver este problema:

1. En el CAM, elija la **Administración de dispositivos > limpian el acceso > los requisitos > las Requisito-reglas**.
2. No reelija como candidato las reglas preconfiguradas (`pr_`), si ninguno.
3. Seleccione las reglas apropiadas AV.

CCA incapaz de detectar el AV

Si usted sospecha que CCA no detecta o reconocer el cierto AV marca, usted necesitan funcionar

con la herramienta de diagnóstico OESIS en el cliente.

Complete estos pasos:

1. Habilite el registro.Refiera al debug del permiso que abre una sesión al agente limpio del acceso para las instrucciones en cómo habilitar el debug que abre una sesión al cliente.
2. Intente iniciar sesión.
3. Funcione con la herramienta de diagnóstico OESIS.
4. Inhabilite el registro.

Nota: Si usted puede asir una exportación de la estructura de la clave de registro del producto AV, situada normalmente en el HKLM \ el software \ el <av_vendor>, que es útil también.

Información Relacionada

- Página de soporte del Cisco NAC Appliance (Clean Access)
- Soporte Técnico y Documentación - Cisco Systems