Dispositivo NAC: Postura del mac OSX AV en el ejemplo de configuración de la versión 4.5 del NAC de Cisco

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Convenciones
Evaluación de la postura del mac con el antivirus de la almeja (ClamAV)
Paso 1. Configure una regla para marcar si ClamAV está instalado
Paso 2. Configure un requisito a los usuarios de Remediate si ClamAV no está instalado
Paso 3. Asocie el requisito de la distribución del link con la regla de la instalación AV
Paso 4. Configure una regla para marcar si ClamAV es actualizado
Paso 5. Configure un requisito a los usuarios de Remediate si ClamAV no es actualizado
Paso 6. Asocie el requisito de la actualización de la definición AV con la regla de la definición de virus
Paso 7. Asocie los requisitos a los papeles
Paso 8. Permita el acceso al sitio de la corrección en el papel temporal
Verifique la experiencia del usuario final
Troubleshooting
Información Relacionada

Introducción

Este documento describe cómo configurar la evaluación limpia de la postura del agente del acceso de Mac OS X vía la consola Web del administrador del Network Admission Control (NAC) para la versión 4.5.

La evaluación de la postura del mac en esta versión se limita al soporte AV/AS solamente. Refiera a los Release Note del Cisco NAC Appliance (Clean Access) para la lista de AV/AS que se soporten en el mac OSX.

prerrequisitos

Requisitos

Complete estos pasos antes de que usted intente esta configuración:

Este documento asume que usted está funcionando con la versión 4.5 del dispositivo NAC de Cisco y eso usted ha completado los pasos siguientes según las guías de consulta en el dispositivo NAC de Cisco – guía de instalación y configuración limpia del Access Manager, la versión 4.5:

1. Instale o actualice su administrador del NAC y servidor del NAC con la versión 4.5 del dispositivo NAC de Cisco según lo descrito en la guía de inicio rápido de la instalación del hardware del dispositivo NAC de Cisco, la versión 4.5.
2. Asegúrese de que los últimos paquetes del agente de Mac OS X (versión 4.5) y de soporte AV/AS estén disponibles en su administrador del NAC según lo descrito en las actualizaciones de la configuración y de la descarga.
3. Cree una página de registro del usuario predeterminado según lo descrito en la página del ingreso del usuario al sistema.
4. Requiera el uso del agente limpio 4.5 del acceso de Mac OS X como descrito adentro requiera el uso del agente.
5. Cree uno o más rol del usuario para los usuarios de Macintosh como descrito adentro cree los rol del usuario.

Nota: Refiera por favor a la sección de las restricciones del agente de MAC OS X para las versiones OS X y los Productos AV/AS y los tipos del requisito que se soportan para la evaluación de la postura del mac.

Componentes Utilizados

La información en este documento se basa en la versión 4.5 del NAC de Cisco.

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.

Evaluación de la postura del mac con el antivirus de la almeja (ClamAV)

La meta de este procedimiento es verificar que ClamAV 1.1.0 está instalado y puesto al día con las últimas definiciones de virus en la máquina del cliente.

Si ClamAV 1.1.0 no está instalado en la máquina del cliente, usted debe proporcionar al usuario con un link al sitio web de ClamAV para descargar y instalar el software. Después, usted debe verificar que ClamAV esté puesto al día con las últimas definiciones. Si no, el agente limpio del acceso puede comunicar con la almeja AV con una llamada API (con el tipo del requisito de la *actualización AV*) y solicitar ClamAV para ponerse al día.

Nota: A partir de la versión del NAC 4.5 de Cisco, soportan al tipo del requisito de la actualización AV solamente con ClamWin AV. Para el resto del AV/AS, una *distribución del link* o un tipo *local*

del control de requisito se puede configurar a los usuarios del remediate si sus definiciones de virus no son actualizadas.

Paso 1. Configure una regla para marcar si ClamAV está instalado

1. Va a la **Administración de dispositivos > limpia el acceso > limpia el agente > las reglas del acceso > la nueva regla AV**.
2. Teclee un nombre para la regla. Este ejemplo utiliza *Is_Clamwin_Installed_OSX*.**Nota:** Sea descriptivo de modo que usted pueda identificar fácilmente el propósito de la regla. Usted puede utilizar los dígitos y los caracteres de subrayado en el nombre, pero ningunos espacios.
3. Elija **ClamWin de la** lista desplegable del vendedor del antivirus.
4. Elija la **instalación del** descenso-abajo del tipo.
5. Elija el **mac OSX de la** lista desplegable del sistema operativo.La tabla en la parte inferior de la página se puebla con estos valores.
6. Marque la casilla de verificación de la **instalación** para 1.x.
7. Teclee una descripción en el campo de texto de la descripción de la regla, y haga clic la **regla de la salvaguardia**.

La nueva regla AV se agrega a la parte inferior de la lista de la regla.

Paso 2. Configure un requisito a los usuarios de Remediate si ClamAV no está instalado

Si el agente limpio del acceso detecta que ClamAV 1.1.0 no está instalado en la máquina del cliente, quarantines al usuario. En este momento, usted puede configurar un tipo del requisito de la *distribución del link* para proporcionar al usuario con un link para descargar ClamAV 1.1.0.

1. Haga clic la lengueta **limpia del agente del acceso**, y después haga clic los **requisitos**.
2. Haga clic el **nuevo requisito**.
3. Elija la **distribución del link de la** lista desplegable del tipo del requisito.
4. Elija **obligatorio de la** lista desplegable del tipo del aplicar.En este ejemplo, el usuario final es informado de este requisito y no puede proceder o tener acceso a la red a menos que el sistema del cliente cumpla el requisito.Refiera a configurar un requisito opcional/de auditoría para la información sobre otros tipos de implementación.
5. Elija el nivel de prioridad de la ejecución para este requisito en la máquina del cliente.Un prioritario (por ejemplo, 1) significa que este requisito está comprobado el sistema delante del resto de los requisitos (y aparece en los diálogos limpios del agente del acceso en esa orden). Este ejemplo asume que el control de la instalación de ClamWin es el primer requisito de la postura y establece la prioridad a un (1).**Nota:** El agente de Mac OS X no soporta la corrección automática. Por lo tanto, fijan al tipo de la corrección al manual. También, las funciones que aparecen en la nueva página de configuración del requisito (tipo, intervalo, y cuenta de reintentos de la corrección) no responden a ningún propósito cuando usted crea los tipos del requisito para la corrección del cliente Macintosh.
6. En el campo de texto del link de archivo URL, teclee el URL al cual los usuarios finales deben ser ordenados para descargar ClamAV 1.1.0.
7. En el nombre del requisito el texto clasifió, teclea un nombre único que transporta la acción al usuario final.Este nombre es visible a los usuarios en los diálogos limpios del agente del acceso. Este ejemplo utiliza la *descarga ClamAV*.

8. En el campo de texto de la descripción, teclee una descripción del requisito y de las instrucciones de dirigir a los usuarios que no pueden cumplir el requisito.
9. Haga clic la casilla de verificación del **Mac OS** enumerada en la sección del sistema operativo.
10. El tecleo **agrega el requisito** para agregar el requisito a la lista del requisito.

El nuevo requisito se agrega a la lista del requisito.

Paso 3. Asocie el requisito de la distribución del link con la regla de la instalación AV

1. Haga clic la lengueta **limpia del agente del acceso**, y después haga clic los **requisitos**.
2. Haga clic las Requisito-**reglas**.
3. De la lista desplegable del nombre del requisito, elija el requisito que usted creó en el paso 2.
4. Elija el **mac OSX de la** lista desplegable del sistema operativo.Las reglas creadas para el sistema operativo elegido se visualizan en la parte inferior de la página.
5. Haga clic la casilla de verificación para la regla que usted creó en el paso 1, y después haga clic la **actualización**.

Paso 4. Configure una regla para marcar si ClamAV es actualizado

1. Va a la **Administración de dispositivos > limpia el acceso > limpia el agente > las reglas del acceso > la nueva regla AV**.
2. Teclee un nombre para la regla. Este ejemplo utiliza *Is_ClamAV_Updated_OSX*.**Nota:** Sea descriptivo de modo que usted pueda identificar fácilmente el propósito de la regla. Usted puede utilizar los dígitos y los caracteres de subrayado en el nombre, pero ningunos espacios.
3. Elija **ClamWin de la** lista desplegable del vendedor del antivirus.
4. Elija la **definición de virus de la** lista desplegable del tipo.
5. Elija el **mac OSX de la** lista desplegable del sistema operativo.Las comprobaciones para de la definición de virus la tabla del mac OSX en la parte inferior de la página se pueblan.
6. Marque la casilla de verificación de la **instalación** para 1.x.
7. Teclee una descripción en el campo de texto de la descripción de la regla, y haga clic la **regla de la salvaguardia**.

La nueva regla AV se agrega a la parte inferior de la lista de la regla.

Paso 5. Configure un requisito a los usuarios de Remediate si ClamAV no es actualizado

Si el agente limpio del acceso detecta que ClamAV 1.1.0 no está puesto al día en la máquina del cliente, quarantines al usuario. En este momento, proporcionan el usuario un remediate del botón Update Button para.

Una vez que el usuario hace clic el botón Update Button, el agente limpio del acceso comunica con el software subyacente de ClamAV y pide ClamAV para ponerse al día.

Usted puede configurar un tipo del requisito de la actualización de la definición AV para implementar estas funciones.

1. Haga clic la lengueta **limpia del agente del acceso**, y después haga clic los **requisitos**.
2. Haga clic el **nuevo requisito**.
3. Elija la **actualización de la definición AV de la** lista desplegable del tipo del requisito.
4. Elija **obligatorio** el lista desplegable del tipo del aplicar.En este ejemplo, el usuario final es informado de este requisito y no puede proceder o tener acceso a la red a menos que el sistema del cliente cumpla el requisito.Refiera a configurar un requisito opcional/de auditoría para la información sobre otros tipos de implementación.
5. Elija el nivel de prioridad de la ejecución para este requisito en la máquina del cliente.Un prioritario (por ejemplo, 1) significa que este requisito está comprobado el sistema delante del resto de los requisitos (y aparece en los diálogos limpios del agente del acceso en esa orden). Este ejemplo asume que el control de la actualización de ClamWin es el segundo requisito de la postura y establece la prioridad a dos (2).**Nota:** El agente de Mac OS X no soporta la corrección automática. Por lo tanto, fijan al tipo de la corrección al manual. También, observe que las opciones del tipo, del intervalo, y de la cuenta de reintentos de la corrección que aparecen en la nueva página de configuración del requisito no responden a ningún propósito cuando usted crea los tipos del requisito para la corrección del cliente Macintosh.
6. Elija **ClamWin – (Mac OS) de la** lista desplegable del nombre del proveedor del antivirus.**Precaución:** Aseegurese le elegir el *ClamWin* – opción *(del Mac OS)*, no la opción de ClamWin.**Nota:** A partir de la versión del NAC 4.5 de Cisco, soportan al tipo del requisito de la actualización AV solamente con el mac OSX de ClamAVon. Para el resto del AV/AS en el mac OSX, una distribución del link o un tipo local del requisito del control se puede configurar a los usuarios del remediate si sus definiciones de virus no son actualizadas.
7. En el campo de texto del nombre del requisito, teclee un nombre único que transporte la acción al usuario final.Este nombre es visible a los usuarios en los diálogos limpios del agente del acceso. Este ejemplo utiliza la *actualización ClamAV*.
8. En el campo de texto de la descripción, teclee una descripción del requisito y de las instrucciones de dirigir a los usuarios que no pueden cumplir el requisito.
9. Haga clic la casilla de verificación del **Mac OS** enumerada en la sección del sistema operativo.
10. El tecleo **agrega el requisito** para agregar el requisito a la lista del requisito.

El nuevo requisito se agrega a la lista del requisito.

Paso 6. Asocie el requisito de la actualización de la definición AV con la regla de la definición de virus

1. Haga clic la lengueta **limpia del agente del acceso**, y después haga clic los **requisitos**.
2. Haga clic las Requisito-**reglas**.
3. De la lista desplegable del nombre del requisito, elija el requisito que usted creó en el paso 5.
4. Elija el **mac OSX de la** lista desplegable del sistema operativo.Las reglas creadas para el sistema operativo elegido se visualizan en la parte inferior de la página.
5. Haga clic la casilla de verificación para la regla que usted creó en el paso 4, y después haga clic la **actualización**.

Paso 7. Asocie los requisitos a los papeles

En este momento, usted puede conectar los requisitos de la postura (que se han asociado a las reglas) al papel en el cual colocan al usuario final.

1. Haga clic la lengueta **limpia del agente del acceso**, y después haga clic los Papel-**requisitos**.
2. Haga clic los Papel-**requisitos**.
3. Elija el **papel normal del login de la** lista desplegable del tipo del papel.
4. Del rol del usuario de la lista desplegable, elija el papel donde usted quiere los requisitos de la postura de ser aplicado. Este ejemplo aplica los requisitos de la postura al papel del *empleado*.Los requisitos creados anterior en este ejemplo se visualizan en la parte inferior de la página.
5. Marque las casillas de verificación para los requisitos que usted quiere aplicar a este papel, y haga clic la **actualización**.

Paso 8. Permita el acceso al sitio de la corrección en el papel temporal

Una vez que encuentran a los usuarios para ser no obedientes, quarantined y se colocan en el papel temporal. En este momento, los usuarios deben poder alcanzar los recursos de la corrección (servidor AV, sitios web, servidores de la corrección, etc.) de modo que puedan remediate ellos mismos.

Para este propósito, usted debe abrir el acceso apropiado en el papel temporal. En este ejemplo, los usuarios deben poder alcanzar http://www.clamxav.com para ambos los requisitos (actualización de la instalación y de la definición de virus).

1. Elija **User Management (Administración de usuario) > los rol del usuario**, y después haga clic la lengueta del **control de tráfico**.
2. Haga clic el **host**.
3. Elija el **papel temporal de la** lista desplegable, y navegue hacia abajo a la parte inferior de la lista.
4. Agregue **clamxav.com a la** lista permitida del host, y el haga click en AddEste paso se asegura de que el tráfico de los clientes a http://www.clamxav.com esté permitido a través de los servidores del NAC.**Nota:** Estas dos condiciones son importantes:El servidor del NAC utiliza la respuesta de DNS del servidor DNS para abrir dinámicamente el acceso. Por lo tanto, el tráfico de retorno del servidor DNS (respuesta de DNS) debe pasar a través del servidor del NAC.Usted debe tener un servidor DNS de confianza definido. Para las mejores prácticas, Cisco recomienda que usted agrega las entradas específicas del servidor DNS aquí en comparación con confiar en a todos los servidores DNS (*). Este ejemplo agrega el IP del servidor DNS (192.168.2.44) como servidor DNS de confianza. Usted puede agregar a los servidores DNS de confianza múltiples. Si usted no tiene un servidor DNS de confianza definido, el administrador del NAC le aconseja por consiguiente a través de un mensaje tal y como se muestra en de esta imagen:

Verifique la experiencia del usuario final

Use esta sección para confirmar que su configuración funciona correctamente.

Este escenario de la verificación de la postura del mac asume que su configuración inicial del NAC (administrador y servidor del NAC) es completa y que el servidor del NAC es accesible de las máquinas del cliente. El Agente de Acceso de Mantenimiento de Cisco 4.5.0.0 se debe instalar

en el mac que ejecuta OSX 10.4 o más alto. Este escenario asume que el mac no tiene ClamAV instalado antes de esta prueba.

1. Login a su agente limpio del acceso (versión 4.5.0.0).Le quarantined y se invita al remediate.**Nota:** Se marcan las casillas de verificación del FUNCIONAMIENTO, pero no editable, porque los requisitos son obligatorios. Si un requisito fuera configurado como *opcional*, la casilla de verificación del FUNCIONAMIENTO sería editable, y usted puede elegir saltar ese requisito.
2. Tecleo **Remediate**.Le reorientan al sitio web de ClamAV.
3. Descargue y instale ClamAV.A le puede ser que indiquen que funcione con el motor del antivirus de la almeja antes de que usted pueda utilizar ClamAV tal y como se muestra en de esta imagen:
4. Siga las instrucciones en pantalla para completar la instalación.El agente limpio del acceso visualiza el estatus del requisito de *ClamAV de la descarga* como acertado y se mueve encendido al segundo requisito (*actualización ClamAV*).Una vez que ClamAV es actualizado, el estatus del requisito de *ClamAV de la actualización* visualiza acertado.
5. Tecleo **completo** iniciar sesión a la red.Una vez que usted inicia sesión con éxito a la red, esta los mensajes aparecen.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

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