NAC(CCA) 4.x: Usuarios del mapa a ciertos papeles usando el ejemplo de la Configuración LDAP

Contenido

Introducción

Este documento describe el Lightweight Directory Access Protocol (LDAP) que asocia la característica para asociar a los usuarios a ciertos papeles en el dispositivo del Network Admission Control (NAC) o el acceso limpio de Cisco (CCA).

El dispositivo NAC de Cisco (antes acceso limpio de Cisco) es un producto fácilmente desplegado del NAC que utiliza la infraestructura de red para aplicar la conformidad de la política de seguridad en todos los dispositivos que busquen a los recursos de computación de la red de acceso. Con el dispositivo NAC, los administradores de la red pueden autenticar, autorizan, evalúan, y remediate atado con alambre, Tecnología inalámbrica, y los usuarios remotos y sus máquinas antes del acceso a la red. Identifica si los dispositivos conectados a la red tales como laptopes, Teléfonos IP, o videoconsolas son obedientes con las políticas de seguridad de su red y repara cualquier vulnerabilidad antes de permitir el acceso a la red.

prerrequisitos

Requisitos

Este documento asume que CCA el administrador, CCA servidor y servidor LDAP está instalado y trabaja correctamente.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- 3300 Series del dispositivo NAC de Cisco - Limpie el Access Manager 4.0
- 3300 Series del dispositivo NAC de Cisco - Limpie el servidor de acceso 4.0

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 TécnicosCisco para obtener más información sobre las convenciones del documento.

Autenticación contra el Active Directory backend

Varios tipos de proveedores de la autenticación en el Access Manager limpio pueden ser utilizados para autenticar a los usuarios contra un servidor del Active Directory (AD), el servicio de directorio propietario de Microsoft. Éstos incluyen Windows NT(NTLM), el Kerberos y el LDAP (preferidos).

Si usted utiliza el LDAP para conectar con el AD, el Nombre distintivo (DN) completo de Search(Admin) tiene que ser fijado típicamente al DN de una cuenta con los privilegios administrativos o los privilegios básicos del usuario. La primera entrada del Common Name (CN) debe ser administrador del AD, o usuario con los privilegios leídos. Observe que el filtro de la búsqueda, SAMAccountName, es el nombre de ingreso del usuario al sistema en el esquema del valor por defecto AD.

Ejemplo de configuración AD/LDAP

Esto ilustra una configuración de muestra usando el LDAP para comunicar con el Active Directory backend:

1. Cree a un Usuario administrador del dominio dentro de los usuarios de directorio activo y computadora. Coloque a este usuario en la carpeta del usuario.
2. Dentro de los usuarios de directorio activo y computadora, seleccione el **hallazgo del** menú Actions (menú Acciones).Aseegurese que sus resultados muestran la columna de la membresía del grupo para el usuario creado. Sus resultados de la búsqueda deben mostrar el **usuario** y la **membresía del grupo** asociada dentro del Active Directory. Ésta es la información que usted necesitará transferir en el Access Manager limpio.
3. De la consola Web limpia del Access Manager, van al **User Management (Administración de usuario) > los servidores de autenticación > nueva** forma del **servidor**.
4. Elija el **LDAP** como el tipo de servidor.
5. Para el **Search(Admin) los campos bajos completos del contexto DN** y de la **búsqueda**, entraron los resultados del hallazgo dentro de los usuarios de directorio activo y computadora.

6. Estos campos son todos que son necesarios configurar correctamente a este servidor de autenticación dentro del CAM:**ServerURL**: ldap://192.168.137.10:389 - Éste es el puerto de escucha de la dirección IP y LDAP del controlador de dominio.**Search(Admin) DN lleno**: Muir de CN=sheldon, cn=Users, DC=domainname, dc=com**Contexto bajo de la búsqueda**: DC=domainname, dc=com**Papel predeterminado**: Seleccione el papel predeterminado que pondrán a un usuario en autenticado una vez.Descripción: Utilizado apenas para la referencia.**Nombre del proveedor**: Éste es el nombre del servidor LDAP usado para la configuración de página del usuario en el CAM.**Contraseña de la búsqueda**: la contraseña de dominio de los muir del sheldon**Filtro de la búsqueda**: SAMAccountName=$user$
7. El tecleo **agrega el servidor**.En este momento, su prueba del auth debe trabajar.
8. Para prueba de la autentificación:**De User Management (Administración de usuario) > los servidores de autenticación > el auth prueban la lengueta**, seleccionan el proveedor contra el cual usted quiere probar las credenciales en la lista del **proveedor**. Si no aparece el proveedor, aseegurese lo se configura correctamente en la **lista de** lengueta de los **servidores**.Ingrese el nombre de usuario y contraseña para el usuario y si está necesitado un valor VLAN ID.El tecleo **autentica**.Los resultados de la prueba aparecen en la parte inferior de la ventana.**Autenticación acertada:**Para cualquier tipo de proveedor, resultado: La autenticación acertada y el papel del usuario se visualizan cuando la prueba del auth tiene éxito.Para los servidores LDAP/RADIUS, cuando la autenticación es acertada y las reglas se configura de la asignación, los atributos/los valores especificados en la regla de la asignación también se visualizan si el servidor de autenticación (LDAP/RADIUS) vuelve esos valores. Por ejemplo:`Result: Authentication successful`
`Role: <role name>`
`Attributes for Mapping:`
`<Attribute Name>=<Attribute value>` **Autenticación fallada:**Cuando la autenticación falla, las presentaciones del mensaje junto con la autenticación fallaron el resultado como se muestra.

Usuarios del mapa a los papeles usando los atributos o las identificaciones de VLAN

Las formas de las reglas de la **asignación** se pueden utilizar para asociar a los usuarios en el rol del usuario basado en estos parámetros:

- El VLAN ID del tráfico de usuarios que origina del lado untrusted del CAS (todos los tipos de servidor de autenticación)
- Atributos de la autenticación pasajeros de los servidores de autenticación LDAP y RADIUS (y atributos de RADIUS pasajeros de los Concentradores VPN de Cisco)

Por ejemplo, si usted tiene dos conjuntos de los usuarios en la misma subred IP pero con diversos privilegios de acceso a la red, tales como empleados inalámbricos y estudiantes, usted puede utilizar un atributo de un servidor LDAP para asociar un conjunto de los usuarios en un papel de usuario determinado. Usted puede entonces crear las políticas de tráfico para permitir el acceso a la red a un papel y para negar el acceso a la red a otros papeles.

El dispositivo NAC de Cisco realiza la secuencia de la asignación como se muestra:

El dispositivo NAC de Cisco permite que el administrador especifique las expresiones boleanas complejas al definir la asignación gobierna para el Kerberos, LDAP y los servidores de autenticación de RADIUS. Asociando las reglas se analizan en las condiciones y usted puede

utilizar las expresiones boleanas para combinar los atributos y el VLAN múltiple ID del usuario múltiple para asociar a los usuarios en los rol del usuario. Asociar las reglas se puede crear para un rango de las identificaciones de VLAN, y las coincidencias del atributo se pueden hacer sin diferenciación entre mayúsculas y minúsculas. Esto permite que las condiciones múltiples sean configuradas fexiblemente para una regla de la asignación.

Una regla de la asignación comprende un tipo de proveedor del auth, una expresión de la regla, y el rol del usuario en la cual para asociar al usuario. La expresión de la regla comprende uno o una combinación de condiciones que los parámetros de usuario deben hacer juego para ser asociado en el papel de usuario específicado. Una condición se comprende de un tipo de la condición, de un nombre del atributo de la fuente, de un operador, y del valor de atributo contra el cual se corresponde con el atributo determinado.

Para crear una regla de la asignación, usted primero agrega las condiciones (de la salvaguardia) para configurar una expresión de la regla. Entonces, una vez que se crea una expresión de la regla, usted puede agregar la regla de la asignación al servidor de autenticación para el papel de usuario específicado.

Asociar las reglas puede conectar en cascada. Si una fuente tiene más de una regla que asocia, las reglas se evalúan en la orden en la cual aparecen en la lista de las reglas de la asignación. El papel de la primera regla positiva de la asignación se utiliza. Una vez que se resuelve una regla, otras reglas no se prueban. Si no hay regla verdad, el papel predeterminado de esa fuente de la autenticación se utiliza.

Regla de la asignación de la configuración

Complete estos pasos:

1. Van a **User Management (Administración de usuario) > los servidores de autenticación > las reglas de la asignación** y hacen clic el link de la **regla de la asignación del agregar** para el servidor de autenticación.La forma de la **regla de la asignación del agregar** aparece.
2. Condiciones de la configuración para asociar la regla (a):**Nombre del proveedor** — El nombre del proveedor fija los campos de la forma de las reglas de la asignación para ese tipo de servidor de autenticación. Por ejemplo, la forma permite solamente la configuración de la regla de la asignación VLAN ID para los tipos de servidor de autenticación del Kerberos, del Windows NT, del NetBios SSO de Windows, y S/Ident. La forma permite el VLAN ID o la configuración de la regla de la asignación del atributo para el RADIUS, LDAP, y el auth del Cisco VPN SSO teclea.**Tipo de la condición** — Configure y agregue las condiciones primero (camina **A** en la figura) antes de agregar la regla de la asignación. Elija uno de éstos del menú desplegable para fijar los campos de la forma de la condición:**Atributo** — Para el LDAP, RADIUS, proveedores del auth del Cisco VPN SSO solamente.**VLAN ID** — Todos los tipos de servidor de autenticación.Para un tipo de la condición de VLAN ID (véase la figura), este campo se llama **Nombre de propiedad**. Por abandono, esto se puebla con el “VLAN ID” (y inhabilitado para editar).**Nombre del atributo** — Para los servidores LDAP (véase la figura), el **nombre del atributo** es un campo de texto en el cual usted ingresa el atributo de la fuente que usted quiere probar. El nombre debe ser idéntico (caso sensible) al nombre del atributo pasajero por la fuente de la autenticación, a menos que usted elija los **iguales ignore al** operador del **caso** para crear la condición.**Valor de atributo** — Ingrese el valor que se probará contra el **nombre del atributo de la** fuente.**Operador (atributo)** — Elija al operador que define la prueba de la cadena del atributo de la fuente:**iguales** — Verdad si el

valor del **nombre del atributo** hace juego el **valor de atributo**.**no iguales** — Verdad si el valor del **nombre del atributo** no hace juego el **valor de atributo**.**contiene** — Verdad si el valor del **nombre del atributo** contiene el **valor de atributo**.**comienza con** — Verdad si el valor del **nombre del atributo** comienza con el **valor de atributo**.**extremos con** — Verdad si el valor del **nombre del atributo** termina con el **valor de atributo**.**los iguales ignoran el caso** — Verdad si el valor del **nombre del atributo** hace juego la cadena del **valor de atributo**. No importa si la cadena sea mayúscula o minúscula.**Operador (VLAN ID)** — Si usted elige el VLAN ID como el **tipo de la condición**, elija a uno de estos operadores para definir una condición esa las pruebas contra los números enteros VLAN ID:**iguales** — Verdad si el VLAN ID hace juego el VLAN ID en el campo de **valor de propiedad**.**no iguales** — Verdad si el VLAN ID no hace juego el VLAN ID en el campo de **valor de propiedad**.**pertenece a** — Verdad si el VLAN ID baja dentro del rango de los valores configurados para el campo de **valor de propiedad**. El valor debe ser una o más identificaciones de VLAN separadas coma. Los rangos de las identificaciones de VLAN se pueden especificar por el guión (-), por ejemplo, [2,5,7,100-128,556-520]. Solamente los números enteros se pueden ingresar, no las cadenas. Observe que los corchetes son opcionales.**Ejemplo:Agregue la condición (la condición de la salvaguardia)** — Aseegurese configurar la condición, después haga clic **agregan la condición** para agregar la condición a la expresión de la regla (si no su configuración no se guarda).

3. Agregue la regla de la asignación al papel (b): Agregue la regla de la asignación (paso **B** en la figura) después de que usted haya configurado y haya agregado las condiciones.**Nombre de la función** — Después de que usted haya agregado por lo menos una condición, elija el rol del usuario al cual usted aplicará la asignación del menú desplegable.**Prioridad** — Seleccione una prioridad del dropdown para determinar la orden en la cual asociando las reglas se prueban. La primera regla que evalúa para verdad se utiliza para asignar al usuario un papel.**Expresión de la regla** — Para ayudar en configurar las declaraciones condicionales para la regla de la asignación, este campo visualiza el contenido de la condición más reciente que se agregará. Después de agregar las condiciones, usted debe hacer clic **agrega la regla de la asignación** para salvar todas las condiciones a la regla.**Descripción** — Una descripción opcional de la regla de la asignación.**Agregue la asignación (la asignación de la salvaguardia)** — Haga clic este botón cuando el agregar hecho condiciona para crear la regla de la asignación para el papel. Usted tiene que agregar o salvar la asignación para un papel especificado, o su configuración y sus condiciones no serán guardadas.

Edite las reglas de la asignación

- **Prioridad** — Para cambiar la prioridad de una regla de la asignación más adelante, haga clic la flecha arriba/abaja al lado de la entrada en **User Management (Administración de usuario) > los servidores de autenticación > lista de servidores**. La prioridad determina la orden en la cual se prueban las reglas. La primera regla que evalúa para verdad se utiliza para asignar al usuario a un papel.
- **Edite** — Haga clic el botón Edit al lado de la regla para modificar la regla de la asignación, o borre las condiciones de la regla. Observe que al editar una condición compuesta, las condiciones debajo (creado más adelante) no están visualizadas. Éste es evitar los loopes.
- **Cancelación** — Haga clic el botón Delete Button al lado de la entrada de la regla de la asignación para que un servidor de autenticación borre esa regla individual de la asignación.

Haga clic el botón Delete Button al lado de una condición en la forma de la regla de la asignación del editar para quitar esa condición de la regla de la asignación. Observe que usted no puede quitar una condición que sea dependiente en otra regla en una declaración compuesta. Para borrar una condición individual, usted tiene que borrar la condición compuesta primero.

Troubleshooting

Si el asociar del usuario AD CCA al rol del usuario no está trabajando, después aseegurese que usted asocia a los usuarios a un papel basado en los atributos con el memberof, Operator=contains, y el atributo Value= (nombre del grupo) de Names= del atributo.

Información Relacionada

- Página de soporte del dispositivo NAC de Cisco
- Soporte Técnico y Documentación - Cisco Systems