Admisiones IP ISR y LDAP para el cambio de dirección de la red a ScanSafe/al ejemplo de la Configuración de seguridad de la red de la nube

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Antecedentes
Configurar
Diagrama de la red
Configuración LDAP
Configuración AAA
Admisión IP de la configuración
Admisión IP del permiso
Host interiores exentos de la autenticación
Habilite al servidor HTTP en el ISR
Configure el cambio de dirección del CWS
Ejemplo de Configuración Completo
LDAP
AAA
Admisión IP
Servidor HTTP
Contenido-exploración y CWS
Determine los objetos DN en el AD - ADSI editan
Métodos de autentificación
NTLM activo
NTLM transparente
Autenticación básica (vía el HTTP en el texto claro)
NTLM pasivo
Secuencia de mensaje para la autenticación NTLM activa
Verificación
Troubleshooting
Comandos show
Comandos de Debug
Problemas comunes
La admisión IP no intercepta los pedidos de HTTP
Soluciones posibles

[Los usuarios reciben un error *no encontrado 404*](#)
[Soluciones posibles](#)
[La autenticación de usuario falla Cuando se le pregunte](#)
[Causas comunes](#)
[Troubleshooting LDAP](#)
[Pasos de alto nivel para la autenticación ldap](#)
[Análisis de la salida de los debugs LDAP](#)
[RFC 4511](#)

Introducción

Este documento describe cómo configurar al Routers de los Servicios integrados de las G2 Series de Cisco (ISR). Mientras que la configuración de la admisión y del Lightweight Directory Access Protocol (LDAP) IP se puede utilizar simplemente para el Proxy de autenticación en el ISR, se utiliza típicamente conjuntamente con la función de redirección de la Seguridad de la red de la nube de Cisco (CWS). Como tal, este documento se piensa para ser una referencia para complementar la documentación de la configuración y del troubleshooting del cambio de dirección del CWS en los ISR.

Prerrequisitos

Requisitos

Cisco recomienda que su reunión del sistema estos requisitos antes de que usted intente las configuraciones que se describen en este documento:

- El ISR debe funcionar con la versión del código 15.2(1)T1 o más adelante.
- Su sistema debe tener las imágenes con la licencia fijada función de seguridad (SEC) que están disponibles en el ® del Cisco IOS (universal).
- La estación de trabajo del cliente en el dominio del Active Directory (AD) debe tener la capacidad para realizar la autenticación activa vía un buscador Web.
- Usted debe tener una suscripción del CWS.

Componentes Utilizados

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

- Internet Explorer, Google Chrome, Mozilla Firefox (requiere la configuración adicional para la autenticación transparente del administrador de LAN de NT (NTLM))
- Cisco G2 800, 1900, 2900, y 3900 Series ISR.

- Controlador de dominio de Microsoft Windows AD (ADDC)

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.

> Nota: Cisco G1 1800, 2800, y 3800 Series Router no se soporta.

Antecedentes

Muchos administradores que instalan las G2 Series ISR de Cisco que no tienen dispositivos de seguridad adaptantes de Cisco (ASA) en sus redes eligen utilizar las funciones del cambio de dirección del CWS ISR (antes ScanSafe) para aprovecharse de la solución del CWS para la filtración de la red. Como parte de esa solución, la mayoría de los administradores también quieren utilizar la infraestructura actual AD para enviar la información de la Identificación del usuario a las torres del CWS con objeto de la aplicación de políticas del usuario o basada en el grupo para las políticas de filtrado de la red en el portal del CWS.

El concepto global es similar a la integración entre el ASA y el agente de directorio del contexto (CDA), con algunas diferencias. La mayoría de las diferencias notables son que el ISR no mantiene realmente un usuario-a-IP pasivo que asocia la base de datos, así que los usuarios deben pasar con algún tipo de autenticación para transitar el ISR y enviar la información del usuario o del grupo al portal del CWS.

> Consejo: Refiera a la sección de los **métodos de autentificación de** este documento para más información sobre las diferencias entre los diversos métodos de autentificación que están disponibles.

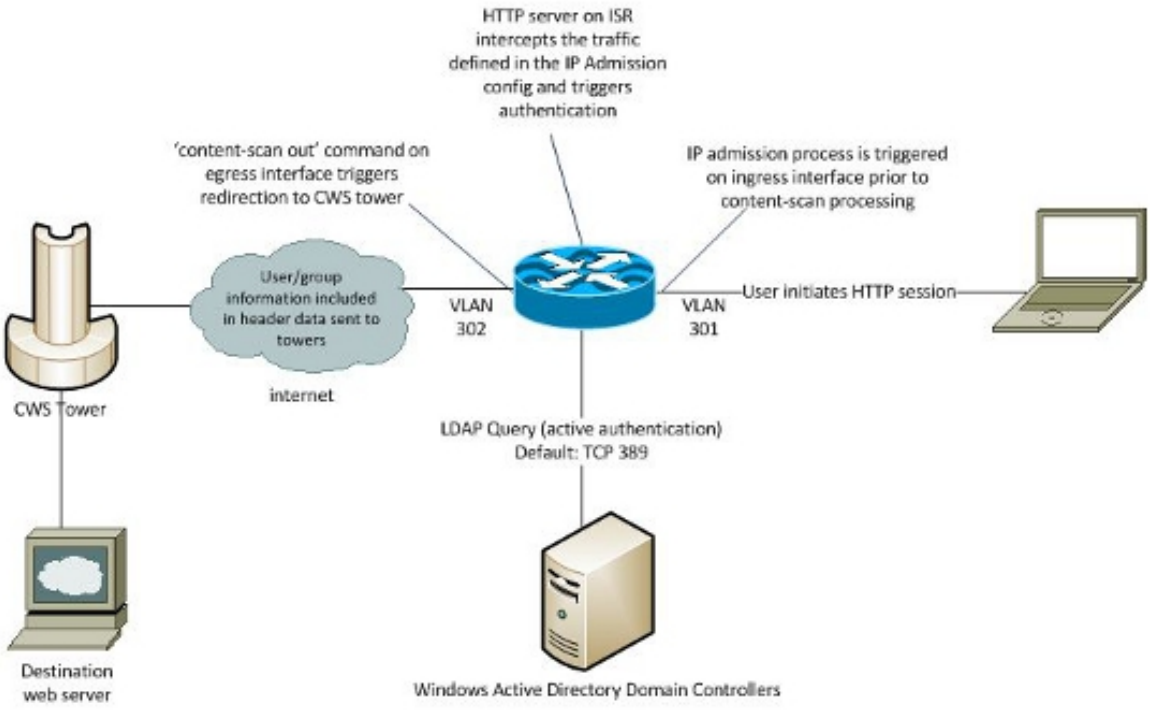
Mientras que la porción del cambio de dirección del CWS de la configuración que se describe en este documento es relativamente directa, algunos administradores pudieron encontrar la dificultad con las tentativas de configurar la porción de la autenticación. Esta porción trabaja con el comando de la **admisión del IP** que se refiere a las sentencias de autenticación de los servidores LDAP y del Authentication, Authorization, and Accounting (AAA) que deben también ser configuradas. El propósito de este documento es proporcionar a los operadores de la red con una fuente de referencia completa para configurar o resolver problemas las admisiones IP y las porciones LDAP de esta configuración en las G2 Series ISR de Cisco.

Configurar

Utilice la información que se describe en esta sección para configurar Cisco ISR.

> Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red



Configuración LDAP

Complete estos pasos para configurar las propiedades LDAP de los servidores AAA:

1. Configure una correspondencia del atributo del LDAP para forzar el nombre de usuario que es ingresado por el usuario para corresponder con la propiedad del **sAMAccountName** en el AD:
   ```
   C-881(config)#ldap attribute-map ldap-username-map map type sAMAccountName
    username
   C-881(config-attr-map)#map type sAMAccountName username
   ```
   Nota: Se requiere esta configuración porque el atributo del **sAMAccountName** es un valor único en el AD, a diferencia del atributo del Common Name (CN), que se utiliza de otra manera para hacer juego por abandono. Por ejemplo, puede haber instancias múltiples de *John Smith* en el AD, pero puede solamente haber un usuario con el **sAMAccountName del** *jsmith*, que es también el inicio de la cuenta de usuario. Otras cuentas de *John Smith* tienen **sAMAccountNames** tales como *jsmith1* o *jsmith2*.
   El comando de los **atributos del ldap de la demostración** se puede también utilizar para ver una lista de los atributos LDAP y de los atributos asociados AAA.

2. Configure al grupo de servidor LDAP:
   ```
   C-881(config)#aaa group server ldap LDAP_GROUP
   C-881(config-ldap-sg)#server DC01
   ```
3. Configure a los servidores LDAP:
   ```
   C-881(config)#ldap server DC01
   C-881(config-ldap-server)# ipv4 10.10.10.150
   C-881(config-ldap-server)#attribute map ldap-username-map
   C-881(config-ldap-server)# bind authenticate root-dn CN=Csco_Service,CN=Users,
   DC=lab,DC=cisco,DC=com password Cisco12345!

   C-881(config-ldap-server)#base-dn DC=lab,DC=cisco,DC=com
   ```

```
C-881(config-ldap-server)#search-filter user-object-type top
C-881(config-ldap-server)#authentication bind-first
```

Esta configuración no requiere generalmente la modificación, a menos que haya una necesidad de implementar un búsqueda-filtro de encargo. Solamente los administradores que están versados en el LDAP y saben entrar correctamente esta información deben utilizar los filtros de encargo de la búsqueda. Si usted es incierto sobre el filtro de la búsqueda que debe ser utilizado, utilice simplemente el filtro descrito; localiza a los usuarios en un entorno normal AD.

Otra porción de la Configuración LDAP que también requiere la atención apropiada detallar es los nombres distintivos (DN) que se requieren en los comandos lazo-autenticar-raíz-**dn** y base-**dn**. Éstos deben ser ingresados exactamente mientras que aparecen en el servidor LDAP, o las interrogaciones del LDAP fallan. Además, el comando base-**dn** debe ser la parte de más baja el árbol LDAP, donde residen todos los usuarios se autentican que.

Considere el escenario en el cual el comando base-**dn** en la configuración previa se modifica por ejemplo esto:

```
base-dn OU=TestCompany,DC=lab,DC=cisco,DC=com
```

En este caso, la interrogación para los usuarios que se incluyen en el **cn=Users, DC=lab, dc=cisco, dc=com** no vuelve ningún resultado, puesto que el servidor LDAP busca solamente la unidad organizativa de TestCompany (OU) y los objetos del niño dentro de ella. Como consecuencia, la autenticación falla siempre para esos usuarios hasta que se trasladen al TestCompany OU o a su sub-estructura, o si el comando base-**dn** se altera para incluirla en la interrogación.

> Consejo: Refiera al **determinar que el DN se opone en el AD - ADSI edita la** sección de este documento para más información sobre cómo determinar los DN apropiados para la base y los comandos root.

Configure el AAA

Ahora que configuran a los servidores LDAP, usted debe referirse a ellos a las sentencias AAA correspondientes que son utilizadas por el proceso de la admisión IP:

```
C-881(config)#aaa authentication login SCANSAFE_AUTH group LDAP_GROUP
C-881(config)#aaa authorization network SCANSAFE_AUTH group LDAP_GROUP
```

> Nota: Si estos comandos no están disponibles, después el **comando aaa new-model** pudo necesitar ser ingresado para habilitar estas funciones AAA porque no se habilitan por abandono.

Admisión IP de la configuración

La porción de la admisión IP acciona un proceso que indique al usuario para la autenticación (o realiza la autenticación transparente) y después realiza las interrogaciones LDAP basadas en los credenciales de usuario y los servidores de AAA que se definen en la configuración. Si autentican a los usuarios con éxito, la información de la Identificación del usuario después es tirada por el proceso de la contenido-exploración y enviada al CWS las torres, junto con el flujo reorientado. El proceso de la admisión IP no se activa hasta que ingresen al ***comando name de la*** **admisión del IP** en la interfaz de ingreso del router. Por lo tanto, esta porción de la configuración se puede

implementar sin ningún impacto del tráfico.

```
C-881(config)#ip admission virtual-ip 1.1.1.1 virtual-host ISR_PROXY
C-881(config)#ip admission name SCANSAFE_ADMISSION ntlm
C-881(config)#ip admission name SCANSAFE_ADMISSION method-list authentication
 SCANSAFE_AUTH authorization SCANSAFE_AUTH
```

Admisión IP del permiso

Aquí está la configuración que se utiliza para habilitar la admisión IP:

> Nota: El fuerza a los usuarios a ser autenticado, que causa la interrupción del flujo de tráfico si la autenticación falla.

```
C-881(config)#int vlan301 (internal LAN-facing interface)
C-881(config-if)#ip admission SCANSAFE_ADMISSION
```

Host interiores exentos de la autenticación

Algunos administradores pudieron desear de eximir algunos host interiores del proceso de autenticación por las diversas razones. Por ejemplo, puede ser que sea indeseable para los servidores internos o los dispositivos que no son capaces del NTLM o de la autenticación básica que se afectarán por el proceso de las admisiones IP. En estos casos, una lista de control de acceso (ACL) se puede aplicar a la configuración de la admisión IP para evitar que el host específico IP o las subredes accione la admisión IP.

En este ejemplo, el host interior **10.10.10.150** está exento del requisito de la autenticación, mientras que la autenticación todavía se requiere para el resto de los host:

```
C-881(config)#ip access-list extended NO_ADMISSION
C-881(config-ext-nacl)#deny ip host 10.10.10.150 any
C-881(config-ext-nacl)#permit ip any any
C-881(config)#ip admission name SCANSAFE_ADMISSION ntlm list NO_ADMISSION
```

Habilite al servidor HTTP en el ISR

Se requiere que usted permite al servidor HTTP para interceptar a las sesiones HTTP e iniciar el proceso de autenticación:

```
Ip http server
Ip http secure-server
```

> Nota: **Ip http el servidor seguro** es solamente necesario si el cambio de dirección al HTTPS para la autenticación se requiere.

Cambio de dirección del CWS de la configuración

Aquí está una configuración sumaria básica para el cambio de dirección del CWS:

```
Ip http server
Ip http secure-server
```

Ejemplo de Configuración Completo

Esta sección proporciona los ejemplos de configuración completos para las secciones anteriores.

LDAP

```
Ip http server
Ip http secure-server
```

AAA

```
Ip http server
Ip http secure-server
```

Admisión IP

```
Ip http server
Ip http secure-server
```

Servidor HTTP

```
Ip http server
Ip http secure-server
```

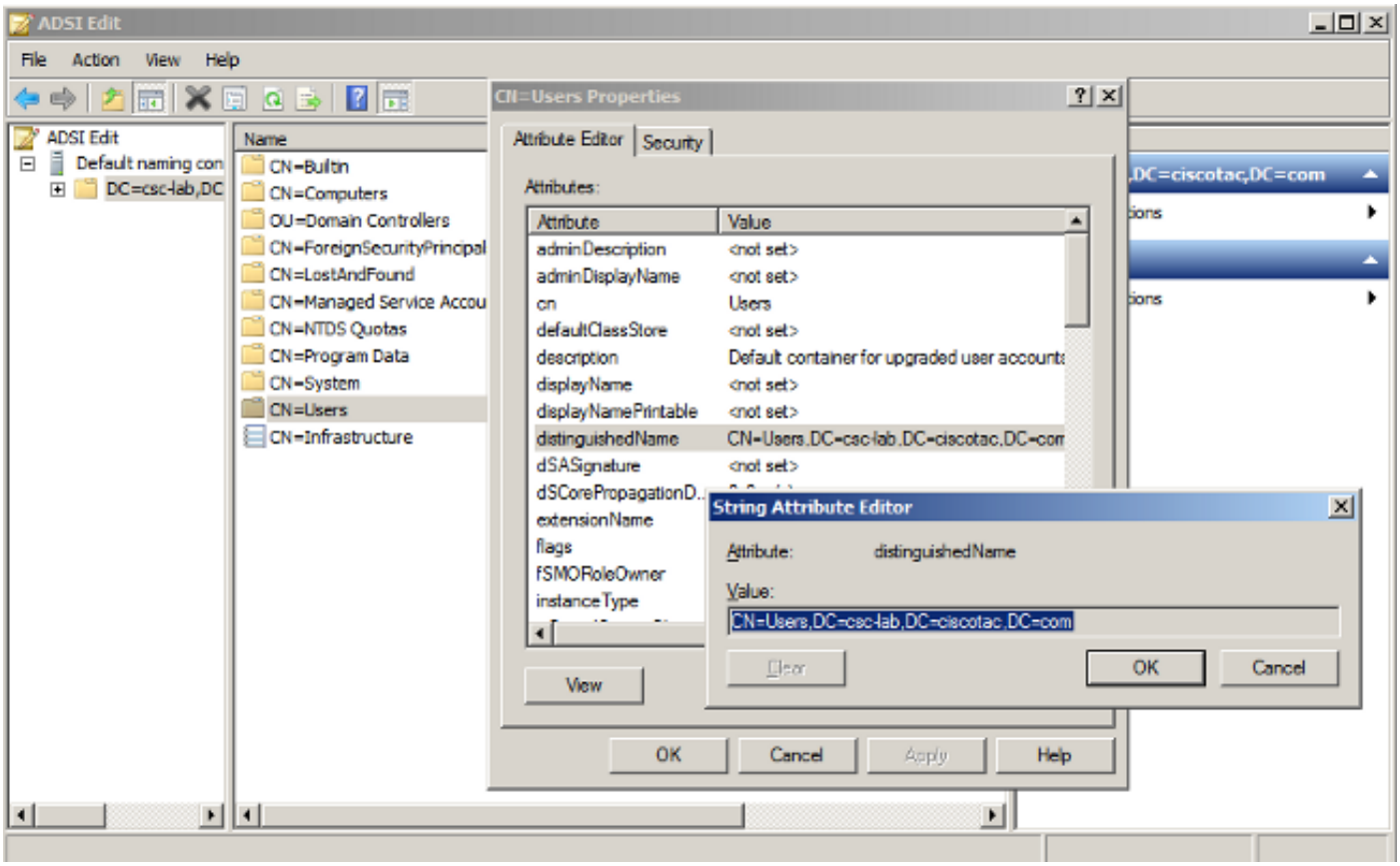
Contenido-exploración y CWS

```
Ip http server
Ip http secure-server
```

Determine los objetos DN en el AD - ADSI editan

Si es necesario, es posible hojear una estructura AD para mirar para arriba los DN para el uso con la base del usuario o de la búsqueda del grupo. Los administradores pueden utilizar una herramienta llamada el *ADSI editan* que se incorpora a los controladores de dominio AD. Para abrir el ADSI edite, elija el **Start (Inicio) > Run (Ejecutar)** en el controlador de dominio AD y ingrese **adsiedit.msc.**

Una vez que el ADSI Edit está abierto, haga clic con el botón derecho del ratón cualquier objeto, tal como un OU, grupo, o usuario, y elija las **propiedades** para ver el DN de ese objeto. La cadena DN se puede entonces copiar y pegar fácilmente a la configuración del router para evitar cualquier error tipográfico. Esta imagen ilustra el proceso:



Métodos de autentificación

Hay cuatro diversos tipos de métodos de autentificación disponibles que utilicen la admisión IP, y se entienden mal a menudo, especialmente la diferencia entre el NTLM transparente y pasivo. Las siguientes secciones describen las diferencias entre estos tipos de autenticación.

NTLM activo

El método de autenticación NTLM activo indica a los usuarios para la autenticación cuando la autenticación NTLM transparente falla. Esto es generalmente debido al hecho de que el buscador del cliente no soporta la autenticación integrada de Microsoft Windows o porque el usuario registrado en el puesto de trabajo con las credenciales locales (del NON-dominio). La autenticación NTLM activa realiza las interrogaciones LDAP al controlador de dominio para asegurarse de que las credenciales proporcionadas están correctas.

> Nota: Con todos los tipos de autenticación NTLM, las credenciales no se pasan vía el texto claro. Sin embargo, la versión 1 (NTLMv1) NTLM tiene vulnerabilidades bien documentadas. El ISR es NTLMv2-capable, aunque por abandono, las versiones anteriores de Microsoft Windows pudieran negociar vía el NTLMv1. Este comportamiento es dependiente sobre las políticas de autenticación AD.

NTLM transparente

La autenticación NTLM transparente ocurre cuando registran a un usuario en el puesto de trabajo

con las credenciales del dominio, y esas credenciales son pasadas transparente por el navegador al router IOS. El router IOS entonces realiza una interrogación LDAP para validar los credenciales de usuario. Ésta es generalmente la forma de autenticación deseada para esta característica.

Autenticación básica (vía el HTTP en el texto claro)

Esta forma de autenticación se utiliza típicamente como mecanismo de repliegue cuando la autenticación NTLM falla o no es posible para los clientes tales como Macintosh, dispositivos Linux-basados, o dispositivos móviles. Con este método, si no habilitan al servidor seguro HTTP, después estas credenciales se pasan vía el HTTP en el texto claro (muy inseguro).

NTLM pasivo

Las credenciales pasivas de las peticiones de la autenticación NTLM de los usuarios pero no autentican realmente al usuario contra el controlador de dominio. Mientras que esto puede evitar los problemas LDAP-relacionados donde las interrogaciones fallan contra el controlador de dominio, también expone a los usuarios en el entorno a un riesgo de seguridad. Si la autenticación transparente falla o no es posible, después indican a los usuarios para las credenciales. Sin embargo, el usuario puede ingresar cualquier credencial que ella elija, que se pasan a la torre del CWS. Como consecuencia, las directivas no se pudieron aplicar apropiadamente.

Por ejemplo, el usuario A puede utilizar Firefox (que por abandono no permita el NTLM transparente sin la configuración adicional) y ingresar el nombre de usuario del usuario B con cualquier contraseña, y las directivas para el usuario B se aplican al usuario A. La exposición del riesgo puede ser atenuada si fuerzan a los usuarios todos a utilizar a los navegadores que soportan la autenticación NTLM transparente, pero en la mayoría de los casos, el uso de la autenticación pasiva no se recomienda.

Secuencia de mensaje para la autenticación NTLM activa

Aquí está la secuencia del mensaje Complete para el método de autenticación NTLM activo:

```
Browser -->  ISR : GET / google.com
Browser <--  ISR : 302 Page moved http://1.1.1.1/login.html
Browser -->  ISR : GET /login.html 1.1.1.1
Browser <--  ISR : 401 Unauthorized..Authenticate using NTLM
Browser -->  ISR : GET /login.html + NTLM Type-1 msg
ISR     -->  AD  : LDAP Bind Request + NTLM Type-1 msg
```

El ISR copia el mensaje del tipo 1 del HTTP al LDAP, byte-por-byte sin ninguna alteración de los datos.

```
ISR     <--  AD  : LDAP Bind Response + NTLM Type-2 msg
Browser <--  ISR : 401 Unauthorized + NTLM Type-2 msg
```

El mensaje del Tipo 2 también se copia byte-por-byte del LDAP al HTTP. Así, en el PCAP, aparece originar de **1.1.1.1**, pero el contenido real es del AD.

```
Browser -->  ISR : GET /login.html + NTLM Type-3 msg
ISR     -->  AD  : LDAP Bind Request + NTLM Type-3 msg
ISR     <--  AD  : LDAP Bind response - Success
Browser <--  ISR : 200OK + redirect to google.com
```

Cuando se configura el NTLM activo, el ISR no interfiere durante el intercambio NTLM. Sin embargo, si se configura el NTLM pasivo, después el ISR genera su propio mensaje del Tipo 2.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

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

Comandos show

> Nota: La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

Usted puede utilizar estos **comandos show** para resolver problemas su configuración:

- **muestre el caché de la admisión del IP**
- **muestre el estatus de la admisión del IP**
- **muestre las estadísticas de la admisión del IP**
- **muestre al servidor LDAP todo**

Comandos de Debug

> Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

Aquí están algunos comandos debug útiles que usted puede utilizar para resolver problemas su configuración:

- **ldap todo del debug** - Este comando se puede utilizar para descubrir la razón que la autenticación falla.
- **detalle de la admisión del IP del debug** - Este comando es muy prolijo y Uso intensivo de la CPU. Cisco recomienda que usted lo utiliza solamente con los solos probares cliente que accionan la admisión IP.
- **ntlm de la admisión del IP del debug** - Este comando se puede utilizar para descubrir la razón que el proceso de la admisión IP está accionado.
- **httpd de la admisión del IP del debug**

- **transacción del debug ip http**
- **debug aaa authorization de la autenticación aaa del debug**

Problemas comunes

Esta sección describe algunos problemas frecuentes que se encuentren con la configuración descrita en este documento.

La admisión IP no intercepta los pedidos de HTTP

Este problema se pone de manifiesto cuando usted ve la salida del **comando statistics de la admisión del IP de la demostración**. La salida no muestra la interceptación de ninguna pedidos de HTTP:

```
C-881#show ip admission statistics
Webauth HTTPd statistics:

HTTPd process 1
Intercepted HTTP requests: 0
```

Soluciones posibles

Hay dos Soluciones posibles a este problema. El primer es verificar que **ip http el servidor** está habilitado.

Si no habilitan al servidor HTTP para el ISR, después los activadores de la admisión IP pero interceptan nunca realmente HTTP session. Por lo tanto, indica para la autenticación. En esta situación, no hay salida para el **comando cache de la admisión del IP de la demostración**, pero muchas repeticiones de estas líneas se consideran en la salida del **comando detail de la admisión del IP del debug**:

```
C-881#show ip admission statistics
Webauth HTTPd statistics:

HTTPd process 1
Intercepted HTTP requests: 0
```

La segunda solución a este problema es verificar que la dirección IP del usuario no está exenta del ACL en la configuración de la admisión IP.

Los usuarios reciben un error *no encontrado 404*

Se observa este problema cuando reorientan a los usuarios para la autenticación, y un error **no encontrado 404** ocurre en el navegador.

Soluciones posibles

Asegúrese de que el nombre en el virtual-**host ISR_PROXY de 1.1.1.1 de la admisión del IP IP**

virtual pueda resolver con éxito con el servidor del Domain Name System (DNS) del cliente. En este caso, el cliente realiza una interrogación DNS para ISR_PROXY.lab.cisco.com puesto que lab.cisco.com es el nombre de dominio completo (FQDN) del dominio al cual se une al puesto de trabajo. Si la interrogación DNS falla, el cliente envía una interrogación de la resolución de nombre del Multicast del local de la conexión (LLMNR), seguida por una interrogación NETBIOS que se transmita a la subred local.

Si todas estas tentativas de la resolución fallan, después 404 no encontrados o el Internet Explorer no pueden visualizar el error de la página web se visualiza en el navegador.

La autenticación de usuario falla Cuando se le pregunte

Esto se puede causar por las diversas razones pero se relaciona generalmente con la Configuración LDAP en el ISR, o la comunicación entre el ISR y el servidor LDAP. En el ISR, el síntoma se observa generalmente cuando pegan a los usuarios en el estado de Init que la admisión IP se acciona una vez:

```
C-881(config)#do show ip admi cac
Authentication Proxy Cache
Client Name N/A, Client IP 10.10.10.152, Port 56674, timeout 60,
 Time Remaining 2, state INIT
```

Causas comunes

Éstas son las causas comunes para este problema:

- Un nombre de usuario y/o una contraseña inválidos es ingresado por el usuario para la autenticación activa.
- Un base-dn inválido se utiliza en la Configuración LDAP, que da lugar a las búsquedas que no vuelven ningún resultado.
- Una autenticación inválida raíz-dn del lazo se configura para el nombre de usuario o la contraseña, que hacen el lazo LDAP fallar.
- La comunicación entre el ISR y el servidor LDAP falla. Verifique que el servidor LDAP escuche en el puerto TCP especificado la comunicación de LDAP y que todos los Firewall entre los dos permiten el tráfico.
- Un filtro inválido de la búsqueda no causa ningún resultado para la búsqueda LDAP.

Troubleshooting LDAP

La mejor manera de determinar la razón que la autenticación falla es utilizar los comandos debug del LDAP en el ISR. Tenga presente que los debugs pueden ser costosos y peligrosos ejecutarse en un ISR si hay resultado en exceso, y pueden hacer al router colgar y requerir un ciclo duro del poder. Esto es especialmente verdad para las Plataformas más bajas.

Para resolver problemas, Cisco recomienda que usted aplica un ACL a la regla de la admisión IP para sujetar solamente un solo puesto de trabajo de la prueba en la red a la autenticación. Esta

manera, los debugs se puede habilitar con un riesgo mínimo de impacto negativo a la capacidad del router de pasar el tráfico.

> Consejo: Refiera a los **host interiores exentos de la** sección de la **autenticación de** este documento para más información sobre la aplicación de un ACL a la configuración de las admisiones IP.

Cuando usted resuelve problemas los problemas LDAP-relacionados, es útil entender los pasos en los cuales el LDAP procesa las peticiones del ISR.

Pasos de alto nivel para la autenticación ldap

Aquí están los pasos de alto nivel para la autenticación ldap:

1. Abra la conexión al servidor LDAP en el puerto especificado. El puerto predeterminado es **TCP 389**.
2. El lazo al servidor LDAP con el lazo autentica el usuario raíz-**dn** y la contraseña.
3. Realice la búsqueda LDAP, con el uso del base-**dn** y de los búsqueda-filtros que se definen en la Configuración LDAP, para el usuario que intenta autenticar.
4. Obtenga los resultados LDAP del servidor LDAP y cree una entrada de caché de la admisión IP para el usuario si la autenticación es acertada, o el reprompt para las credenciales en caso de falla de autenticación.

Análisis de la salida de los debugs LDAP

Estos procesos se pueden ver en la salida del **comando all del ldap del debug**. Esta sección proporciona un ejemplo de la salida de los debugs LDAP para una autenticación que falle debido a un base-**dn** inválido. Revise la salida de los debugs y los comentarios asociados, que describen las porciones de la salida que muestran donde los pasos ya mencionados pudieron encontrar el error.

```
*Jan 30 20:51:50.818: LDAP: LDAP: Queuing AAA request 23 for processing
*Jan 30 20:51:50.818: LDAP: Received queue event, new AAA request
*Jan 30 20:51:50.818: LDAP: LDAP authentication request
*Jan 30 20:51:50.818: LDAP: Username sanity check failed
*Jan 30 20:51:50.818: LDAP: Invalid hash index 512, nothing to remove
*Jan 30 20:51:50.818: LDAP: New LDAP request
*Jan 30 20:51:50.818: LDAP: Attempting first next available LDAP server
*Jan 30 20:51:50.818: LDAP: Got next LDAP server :DC01
*Jan 30 20:51:50.818: LDAP: Free connection not available. Open a new one.
*Jan 30 20:51:50.818: LDAP: Opening ldap connection
( 10.10.10.150, 389 )ldap_open
```

La porción de la salida mostrada en intrépido indica que esto no es un problema de la capa de red, puesto que el conexión se abre con éxito.

```
*Jan 30 20:51:50.822: LDAP: Root Bind on CN=Csco_Service,CN=Users,DC=lab,
DC=cisco,DC=com initiated.
*Jan 30 20:51:51.330: LDAP: Ldap Result Msg: SUCCESS, Result code =0
```

```
*Jan 30 20:51:51.330: LDAP: Root DN bind Successful on :CN=Csco_Service,
CN=Users,DC=lab,DC=cisco,DC=com
```

El lazo autenticar-dn está correcto en esta salida. Si la configuración es incorrecta para esto, después consideran a los errores del lazo.

```
*Jan 30 20:51:50.822: LDAP: Root Bind on CN=Csco_Service,CN=Users,DC=lab,
DC=cisco,DC=com initiated.
*Jan 30 20:51:51.330: LDAP: Ldap Result Msg: SUCCESS, Result code =0
*Jan 30 20:51:51.330: LDAP: Root DN bind Successful on :CN=Csco_Service,
CN=Users,DC=lab,DC=cisco,DC=com
```

La porción de la salida mostrada en intrépido indica que todas las operaciones del lazo son acertadas y procede a buscar para el usuario real.

```
*Jan 30 20:51:51.854: LDAP: SASL NTLM authentication done..Execute search
*Jan 30 20:51:51.854: LDAP: Next Task: Send search req
*Jan 30 20:51:51.854: LDAP: Transaction context removed from list[ldap reqid=15]
*Jan 30 20:51:51.854: LDAP: Dynamic map configured
*Jan 30 20:51:51.854: LDAP: Dynamic map found for aaa type=username
*Jan 30 20:51:51.854: LDAP: Ldap Search Req sent
ld 2293572544
base dn     dc=lab1,dc=cisco,dc=comscope       2
filter (&(objectclass=top)(sAMAccountName=testuser5))
ldap_req_encode
put_filter "(&(objectclass=top)(sAMAccountName=testuser5))"
put_filter: AND
put_filter_list "(objectclass=top)(sAMAccountName=testuser5)"
put_filter "(objectclass=top)"
put_filter: simple
put_filter "(sAMAccountName=testuser5)"
put_filter: simple
Doing socket write
*Jan 30 20:51:51.854: LDAP: lctx conn index = 2
```

La primera línea (mostrada en intrépido) indica que la salida de los debugs de la búsqueda LDAP comienza. También, note que el controlador de dominio base-**dn** se debe configurar para el **laboratorio**, no **lab1**.

```
*Jan 30 20:51:52.374: LDAP: LDAP Messages to be processed: 1
*Jan 30 20:51:52.374: LDAP: LDAP Message type: 101
*Jan 30 20:51:52.374: LDAP: Got ldap transaction context from reqid
16ldap_parse_result
*Jan 30 20:51:52.374: LDAP: resultCode: 10 (Referral)
*Jan 30 20:51:52.374: LDAP: Received Search Response resultldap_parse_result
ldap_err2string
*Jan 30 20:51:52.374: LDAP: Ldap Result Msg: FAILED:Referral, Result code =10
*Jan 30 20:51:52.374: LDAP: LDAP Search operation result : failedldap_msgfree
*Jan 30 20:51:52.374: LDAP: Closing transaction and reporting error to AAA
*Jan 30 20:51:52.374: LDAP: Transaction context removed from list
[ldap reqid=16]
*Jan 30 20:51:52.374: LDAP: Notifying AAA: REQUEST FAILED
```

La porción de la salida mostrada en intrépido indica que la búsqueda no volvió ningún resultado, que en este caso es debido a un base-**dn** inválido.

RFC 4511

RFC 4511 (**Lightweight Directory Access Protocol (LDAP): El protocolo**) proporciona la información sobre los mensajes del código de resultado para el LDAP y la otra información protocolo-relacionada LDAP, que se pueden referir vía el sitio web IETF.