PEAP bajo redes inalámbricas unificadas con ACS 5.1 y el servidor de Windows 2003

Contenido

Introducción

Este documento describe cómo configurar el acceso inalámbrico seguro mediante controladores

LAN inalámbricos, el software Microsoft Windows 2003 y Cisco Secure Access Control Server (ACS) 5.1 a través de Protected Extensible Authentication Protocol (PEAP) con Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) versión 2.

Nota: Para la información sobre el despliegue de asegure la Tecnología inalámbrica, refiera al modelo de la Tecnología inalámbrica del sitio web y del Cisco SAFE del Wi-Fi de Microsoft.

prerrequisitos

Requisitos

Hay una suposición que el instalador tiene la instalación de Windows 2003 del conocimietno básico e instalación del controlador LAN de la tecnología inalámbrica de Cisco mientras que este documento cubre solamente las configuraciones específicas para facilitar las pruebas.

Para la instalación inicial y la información de la configuración para los reguladores de las Cisco 5508 Series, refiera a la guía de instalación del controlador inalámbrica de las Cisco 5500 Series. Para la instalación inicial y la información de la configuración para los reguladores de las Cisco 2100 Series, refiera a la guía de inicio rápido: Regulador del Wireless LAN de las Cisco 2100 Series.

Microsoft Windows 2003 guías de instalación y configuración se puede encontrar en instalar el r2 2003 del Servidor Windows .

Antes de que usted comience, instale el Microsoft Windows server 2003 con el sistema operativo SP1 en cada uno de los servidores en el laboratorio de prueba y ponga al día todo el Service Packs. Instale los reguladores y los Puntos de acceso ligeros (revestimientos) y asegúrese de que las actualizaciones de último software están configuradas.

Utilizan al Servidor Windows 2003 con el SP1, Enterprise Edition, para poder configurar el Autoregistro de los Certificados del usuario y del puesto de trabajo para la autenticación PEAP. El Autoregistro del certificado y autorenewal hacen más fácil desplegar los Certificados y mejorar la Seguridad automáticamente la expiración y renovando los Certificados.

Componentes Utilizados

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

- Regulador de las Cisco o? Series que funcionamientos 7.0.98.0
- Cisco protocolo de 1142 Lightweight Access Point (LWAPP) AP
- Empresa de Windows 2003 con el Internet Information Server (IIS), el Certificate Authority (CA), el DHCP, y el Domain Name System (DNS) instalado
- Dispositivo del sistema de control de acceso seguro de Cisco 1121 (ACS) 5.1
- Profesional de Windows XP con el SP (y Service Packs actualizado) y Wireless Network Interface Card (NIC) (con CCX el soporte del v3) o supplicant del otro vendedor.
- Cisco 3750 Switch

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.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Cisco asegura la Topología de laboratorio inalámbrica
El propósito primario de este documento es proporcionarle el procedimiento paso a paso para implementar el PEAP bajo redes inalámbricas unificadas con ACS 5.1 y el Servidor de Enterprise de Windows 2003. El énfasis principal está en el Autoregistro del cliente de modo que el cliente auto-aliste y tome el certificado del servidor.

Nota: Para agregar el Wi-Fi protegió el acceso (WPA)/WPA2 con la norma de encripción del Temporal Key Integrity Protocol (TKIP) /Advanced (AES) al profesional de Windows XP con el SP, refieren a la actualización del elemento de información de los servicios del aprovisionamiento WPA2/Wireless (WPS IE) para Windows XP con el Service Pack 2.

Empresa 2003 de Windows puesta con el IIS, Certificate Authority, DNS, DHCP (CA)

CA (democa)

CA es un ordenador que funciona con al Servidor Windows 2003 con el SP2, Enterprise Edition, y realiza estos papeles:

- Un controlador de dominio para el **dominio demo.local** que ejecuta el IIS
- Un servidor DNS para el **dominio DNS demo.local**
- Un servidor DHCP
- Empresa raíz CA para el **dominio demo.local**

Realice estos pasos para configurar CA para estos servicios:

1. Realice una instalación básica y una configuración.
2. Configure el ordenador como controlador de dominio.
3. Aumente el nivel funcional del dominio.
4. Instale y configure el DHCP.

5. Instale los servicios de certificados.
6. Verifique los permisos del administrador para los Certificados.
7. Agregue los ordenadores al dominio.
8. Permita el acceso de red inalámbrica a los ordenadores.
9. Agregue a los usuarios al dominio.
10. Permita el acceso de red inalámbrica a los usuarios.
11. Agregue a los grupos al dominio.
12. Agregue a los usuarios al grupo de los wirelessusers.
13. Agregue las computadoras cliente al grupo de los wirelessusers.

Realice la instalación básica y la configuración

Siga estos pasos:

1. Instale al Servidor Windows 2003 con el SP2, Enterprise Edition, como servidor independiente.
2. Configure el protocolo TCP/IP con la dirección IP de *10.0.10.10* y la máscara de subred de *255.255.255.0*.

Configure la Computadora como controlador de dominio

Siga estos pasos:

1. Para comenzar al Asisitente de instalación de Active Directory, elija el **Start (Inicio) > Run (Ejecutar)**, **teclee dcpromo.exe, y** haga clic la AUTORIZACIÓN**.**
2. En la recepción a la página del Asisitente de instalación de Active Directory, haga clic **después**.
3. En la página de la compatibilidad del sistema operativo, haga clic **después**.
4. En la página de tipo del controlador de dominio, el **controlador de dominio** selecto **para un nuevo dominio** y el tecleo **después**.
5. En la nueva página del dominio del crear, el **dominio** selecto **en un nuevo bosque** y el tecleo **después**.
6. En la página del instalar o de la configuración DNS, seleccione **ningún, apenas instale y configure el DNS en este ordenador** y haga clic **después**.
7. En la nuevos página del Domain Name, tipo **demo.local y** tecleo después**.**
8. En la página del Domain Name del NetBios, ingrese el nombre de NETBIOS del dominio como **versión parcial de programa** y haga clic **después**.
9. En las carpetas de la base de datos y del registro que las ubicaciones paginan, que valide los directorios predeterminados de las carpetas de la base de datos y del registro y que haga clic **después**.
10. En System Volume (Volumen del sistema) la página compartida, verifique que la ubicación de la carpeta predeterminada está correcta y haga clic **después**.
11. En los permisos pagine, verifique que los **permisos compatibles solamente con los sistemas operativos del Windows 2000 o del Servidor Windows 2003** están seleccionados y tecleo **después**.
12. En la página de la contraseña de administración del modo del Restore de los servicios de directorio, deje el espacio en blanco de casillas de verificación de contraseña y haga clic **después**.

13. Revise la información sobre la página de resumen y haga clic **después**.
14. Cuando le hacen con la instalación de Active Directory, clic en Finalizar.
15. Cuando se le pregunte para recomenzar el ordenador, el tecleo **ahora recomienza**.

Aumente el nivel funcional del dominio

Siga estos pasos:

1. Abra los **dominios de Active Directory y las confianzas broche-**en de la carpeta de las **herramientas administrativas** (**Start (Inicio) > Programs (Programas) > Administrative Tools (Herramientas administrativas) > dominios de Active Directory y confianzas**), y después haga clic con el botón derecho del ratón la computadora dominio **CA.demo.local.**
2. Haga clic el **nivel funcional del dominio del aumento**, y después seleccione al **Servidor Windows 2003** en la página del nivel funcional del dominio del aumento.
3. Haga clic el **aumento**, haga clic la **AUTORIZACIÓN**, y después haga clic la **AUTORIZACIÓN** otra vez.

Instale y configure el DHCP

Siga estos pasos:

1. Instale el **Protocolo de configuración dinámica de host (DHCP)** como componente de **servicio de red** usando **agregan o quitan los programas** en el panel de control.
2. Abra el **DHCP broche-**en de la carpeta de las **herramientas administrativas** (**Start (Inicio) > Programs (Programas) > Administrative Tools (Herramientas administrativas) > DHCP**), y después resalte al servidor DHCP, **CA.demo.local.**
3. Haga clic la **acción**, y después haga clic **autorizan** para autorizar el servicio del DHCP.
4. En el árbol de la consola, haga clic con el botón derecho del ratón **CA.demo.local, y después haga clic el** nuevo alcance.
5. En la página de Bienvenida del nuevo asistente de alcance, haga clic **después**.
6. En la página del nombre del alcance, teclee **CorpNet** en el campo de nombre.
7. Haga clic **después** y complete estos parámetros:Comience a la dirección IP 10.0.20.1Termine a la dirección IP 10.0.20.200Longitud - **24**Máscara de subred - **255.255.255.0**
8. Haga clic **después** y ingrese *10.0.20.1* para el IP Address del comienzo y *10.0.20.100* para que el IP Address del extremo sea excluido. Luego haga clic en Next (Siguiente). Esto reserva los IP Addresses en el rango de 10.0.20.1 a 10.0.20.100. Éstos reservan los IP Addresses no son asignados por el servidor DHCP.
9. En la página del tiempo de validez, haga clic **después**.
10. En la configuración las opciones DHCP paginan, eligen **sí, quiero ahora configurar estas opciones** y hacer clic **después**.
11. En la página del router (default gateway) agregue a la dirección del router predeterminada de *10.0.20.1* y haga clic **después**.
12. En el Domain Name y los servidores DNS pagine, teclee *demo.local en el* campo del dominio del padre, teclee 10.0.10.10 *en el* campo de la dirección IP, y después haga clic el tecleo de Addand después**.**
13. En los TRIUNFOS que los servidores paginan, que haga clic **después**.
14. En la página del alcance del activar, elija **sí, quiero ahora activar este alcance** y hacer clic

después.
15. Cuando usted acaba con la nueva página del asistente de alcance, clic en Finalizar.

Instale los servicios de certificados

Siga estos pasos:

Nota: El IIS debe ser instalado antes de que usted instale los servicios de certificados y el usuario debe ser parte de la empresa Admin OU.

1. En el panel de control, abierto **agregue o quite los programas**, y después haga clic **agregan/quitan a los componentes de Windows**.
2. En la página del Asistente de componentes de Windows, elija los servicios de certificados, y después haga clic después.
3. En la página de tipo de CA, elija la empresa raíz CA y haga clic después.
4. En CA que identifica la página de información, teclee el *democa* en el Common Name para este cuadro de CA. Usted puede también ingresar los otros detalles opcionales. Entonces haga clic **después** y valide los valores por defecto en la página de las configuraciones de la base de datos del certificado.
5. Haga clic en Next (Siguiente). Al completar la instalación, clic en Finalizar.
6. Haga Click en OK después de que usted leyera el mensaje de advertencia sobre instalar el IIS.

Verifique los permisos del administrador para los Certificados

Siga estos pasos:

1. Elija el **Start (Inicio) > Administrative Tools (Herramientas administrativas)** > las **autoridades de certificación**.
2. Haga clic con el botón derecho del ratón el **democa CA** y después haga clic las **propiedades**.
3. En la ficha de seguridad, haga clic a los **administradores** en la lista del grupo o de Nombres de usuario.
4. En los permisos para administradores enumere, verifique que estas opciones están fijadas **para permitir**:Publique y maneje los CertificadosManeje CAPida los CertificadosSi ninguno de estos se fijan para negar o no se seleccionan, fije los permisos **para permitir**.
5. Haga Click en OK para cerrar el cuadro de diálogo Propiedades de CA del democa, y después para cerrar las autoridades de certificación.

Agregue las Computadoras al dominio

Siga estos pasos:

Nota: Si el ordenador se agrega ya al dominio, proceda a agregar a los usuarios al dominio.

1. Abra a los **usuarios de directorio activo y computadora broche-**en.
2. En el árbol de la consola, amplíe **demo.local.**
3. Haga clic con el botón derecho del ratón las **Computadoras**, haga clic **nuevo**, y después haga clic la **Computadora**.

4. En el nuevo objeto – El cuadro de diálogo de la Computadora, teclea el nombre del ordenador en el campo de nombre de la computadora y hace clic **después**. Este ejemplo utiliza al *cliente del* nombre de computadora.
5. En el cuadro de diálogo manejado, haga clic **después**.
6. En el nuevo objeto – Cuadro de diálogo de la Computadora, clic en Finalizar.
7. Relance los pasos 3 a 6 para crear las cuentas de la computadora adicional.

Permita el acceso de red inalámbrica a las Computadoras

Siga estos pasos:

1. En el árbol de la consola de los usuarios de directorio activo y computadora, haga clic la carpeta de las **Computadoras** y haga clic con el botón derecho del ratón en el ordenador para el cual usted quiere asignar el acceso de red inalámbrica. Este ejemplo muestra el procedimiento con la computadora cliente cuál usted agregó en las **propiedades del** tecleo del paso 7., y después va al **dial-in tab**.
2. En el Permiso de acceso remoto, elija **permiten el acceso** y hacen clic la **AUTORIZACIÓN**.

Agregue a los usuarios al dominio

Siga estos pasos:

1. En el árbol de la consola de los usuarios de directorio activo y computadora, haga clic con el botón derecho del ratón a los **usuarios**, haga clic **nuevo**, y después haga clic al **usuario**.
2. En el nuevo objeto – El cuadro de diálogo del usuario, teclea el nombre del usuario de red inalámbrica. Este ejemplo utiliza el *wirelessuser del* nombre en el campo de primer nombre, y el *wirelessuser* en el campo de nombre de inicio de usuario. Haga clic en Next (Siguiente).
3. En el nuevo objeto – El cuadro de diálogo del usuario, teclea una contraseña de su opción en la contraseña y confirma los campos de contraseña. Borre al **usuario debe cambiar la contraseña en la** casilla de verificación **siguiente del inicio**, y hace clic **después**.
4. En el nuevo objeto – Cuadro de diálogo del usuario, clic en Finalizar.
5. Relance los pasos 2 a 4 para crear las cuentas de usuario adicionales.

Permita el acceso de red inalámbrica a los usuarios

Siga estos pasos:

1. En el árbol de la consola de los usuarios de directorio activo y computadora, haga clic la **carpeta del usuario**, haga clic con el botón derecho del ratón el **wirelessuser**, haga clic las **propiedades**, y después vaya al **dial-in tab**.
2. En el Permiso de acceso remoto, elija **permiten el acceso** y hacen clic la **AUTORIZACIÓN**.

Agregue a los grupos al dominio

Siga estos pasos:

1. En el árbol de la consola de los usuarios de directorio activo y computadora, haga clic con el botón derecho del ratón a los **usuarios**, haga clic **nuevo**, y después haga clic al **grupo**.

2. En el nuevo objeto – Agrupe el cuadro de diálogo, teclee el nombre del grupo en el campo de nombre del grupo y haga clic la **AUTORIZACIÓN**. Este documento utiliza los *wirelessusers del* nombre del grupo.

Agregue a los usuarios al grupo de los wirelessusers

Siga estos pasos:

1. En el panel de detalles de los usuarios de directorio activo y computadora, haga doble clic en el grupo *WirelessUsers*.
2. Vaya a la lengueta y al haga click en Add de los miembros
3. En los usuarios selectos, los contactos, cuadro de diálogo de las Computadoras, o de los grupos, teclean el nombre de los usuarios que usted quiere agregar al grupo. Este ejemplo muestra cómo agregar el *wirelessuser del* usuario al grupo. Haga clic en OK.
4. En el múltiplo los nombres encontraron el cuadro de diálogo, **AUTORIZACIÓN del** tecleo. La cuenta de usuario del wirelessuser se agrega al grupo de los wirelessusers.
5. Haga Click en OK para salvar los cambios al grupo de los wirelessusers.
6. Relance este procedimiento para agregar a más usuarios al grupo.

Agregue las computadoras cliente al grupo de los wirelessusers

Siga estos pasos:

1. Relance los pasos 1 y 2 en los usuarios del agregar a la sección de grupo de los wirelessusers de este documento.
2. En los usuarios selectos, el cuadro de diálogo de los contactos, o de las Computadoras, teclea el nombre del ordenador que usted quiere agregar al grupo. Este ejemplo muestra cómo agregar el ordenador nombrado *cliente al* grupo.
3. Haga clic los **tipos de objeto**, borre la casilla de verificación de los **usuarios**, y después marque las **Computadoras**.
4. Haga clic en OK dos veces. La cuenta de la computadora cliente se agrega al grupo de los wirelessusers.
5. Relance el procedimiento para agregar más ordenadores al grupo.

Secure ACS 5.1 de Cisco 1121

Instalación usando el dispositivo de la serie CSACS-1121

El dispositivo CSACS-1121 se instala previamente con el software ACS 5.1. Esta sección le da una descripción del proceso de instalación y de las tareas que usted debe realizar antes de instalar el ACS.

1. Conecte el CSACS-1121 con la consola de la red y del dispositivo. Vea el capítulo 4, los “cables de conexión.”
2. Accione para arriba el dispositivo CSACS-1121. Vea el capítulo 4, “accionando para arriba el dispositivo de la serie CSACS-1121.”
3. Funcione con el **comando setup** en el prompt CLI de configurar las configuraciones iniciales

para el servidor ACS. Vea funcionar con el programa de configuración.

Instale al servidor ACS

Esta sección describe el proceso de instalación para el servidor ACS en el dispositivo de la serie CSACS-1121.

- Funcione con el programa de configuración
- Verifique el proceso de instalación
- Tareas de la Poste-instalación

Para información detallada sobre la instalación del servidor del Cisco Secure ACS refiera a la instalación y al guía de actualización para el Cisco Secure Access Control System 5.1.

Configuración de controlador de Cisco WLC5508

Cree la configuración necesaria para WPAv2/WPA

Siga estos pasos:

Nota: La suposición es que el regulador tiene conectividad básica a la red y el alcance IP a la interfaz de administración es acertado.

1. Hojee a **https://10.0.1.10** para iniciar sesión al regulador.
2. Haga clic en Login (Conexión).
3. Inicie sesión con el usuario predeterminado *admin* y la contraseña predeterminada *admin*.
4. Cree una nueva interfaz para la asignación del VLA N bajo menú del **regulador**.
5. Haga clic las **interfaces**.
6. Haga clic en **New**.
7. En el campo de nombre de la interfaz, ingrese al *empleado*. (Este campo puede ser cualquier valor que usted tenga gusto.)
8. En el campo VLAN ID, ingrese *20*. (Este campo puede ser cualquier VLA N que se lleve adentro la red.)
9. Haga clic en Apply (Aplicar).
10. Configure la información como esto interconecta > edita las demostraciones de la ventana:Interconecte a la dirección IP 10.0.20.2Netmask - **255.255.255.0**Gateway - **10.0.10.1**DHCP primario - **10.0.10.10**
11. Haga clic en Apply (Aplicar).
12. Haga clic la lengueta **WLAN**.
13. Elija **crean nuevo**, y el tecleo **va**.
14. Ingrese un nombre del perfil, y, en el campo WLAN SSID, ingrese al *empleado*.
15. Elija un ID para la red inalámbrica (WLAN), y el tecleo **se aplica**.
16. Configure la información para esta red inalámbrica (WLAN) cuando aparecen los WLAN > editan la ventana.**Nota:** WPAv2 es el método de encripción elegido de la capa 2 para este laboratorio. Para permitir que el WPA con los clientes TKIP-MIC se asocie a este SSID, usted puede también marcar al **modo de compatibilidad WPA** y **no prohibir los clientes WPA2 TKIP los** cuadros o a esos clientes que no soportan el método de encripción AES 802.11i.
17. En los WLAN > editan la pantalla, hacen clic la **ficha general**.

18. Aseegurese que el cuadro del estatus está marcado para saber si hay **habilitado** y la **interfaz** apropiada (empleado) está elegida. También, aseegurese marcar la casilla de verificación **habilitada** para el broadcast SSID.
19. Haga clic en la ficha Security (Seguridad).
20. Conforme al submenú de la capa 2, marque **WPA + WPA2** para la Seguridad de la capa 2. Para el cifrado WPA2, marque **AES + TKIP** para permitir a los clientes TKIP.
21. Elija el **802.1x** como el método de autentificación.
22. Salte el submenú de la capa 3 pues no se requiere. Una vez que configuran al servidor de RADIUS, el servidor apropiado se puede elegir del menú de la autenticación.
23. **El QoS** y las **fichas Avanzadas** se pueden dejar en el valor por defecto a menos que se requiera cualquier configuración especial.
24. Haga clic el **menú de seguridad** para agregar al servidor de RADIUS.
25. Conforme al submenú RADIUS, haga clic la **autenticación**. Entonces, haga clic **nuevo**.
26. Agregue la dirección IP del servidor de RADIUS (10.0.10.20) que es el servidor ACS configurado anterior.
27. Aseegurese que la clave compartida hace juego al cliente AAA configurado en el servidor ACS. Aseegurese que el cuadro del **usuario de la red** está marcado y el tecleo **se aplica**.
28. La configuración básica es completa ahora y usted puede comenzar a probar el PEAP.

Autenticación PEAP

El PEAP con la versión MS-CHAP 2 requiere los Certificados en los servidores ACS pero no en los clientes de red inalámbrica. La inscripción auto de los Certificados del ordenador para los servidores ACS se puede utilizar para simplificar un despliegue.

Para configurar el servidor de CA para proporcionar el Autoregistro para el ordenador y los Certificados de usuario, complete los procedimientos en esta sección.

Nota: Microsoft ha cambiado la plantilla del servidor Web con la versión de la empresa CA de Windows 2003 de modo que las claves sean no más exportables y la opción sea grayed hacia fuera. No hay otros Certificate Template plantilla de certificado suministrados los servicios de certificados que están para la autenticación de servidor y dan la capacidad de marcar las claves pues exportable que están disponibles en el descenso-abajo así que usted tiene que crear una nueva plantilla que lo haga tan.

Nota: El Windows 2000 permite las claves exportables y estos procedimientos no necesitan ser seguidos si usted utiliza el Windows 2000.

Instale los Certificate Template plantilla de certificado Broche-en

Siga estos pasos:

1. Elija el **Start (Inicio) > Run (Ejecutar)**, ingrese el *mmc*, y haga clic la **AUTORIZACIÓN**.
2. En el menú de archivos, el tecleo **agrega/quita Broche-en**, y entonces haga click en Add
3. Bajo Broche-en, los **Certificate Template plantilla de certificado del** clic doble, **cierre del** tecleo, y entonces hacen clic la **AUTORIZACIÓN**.
4. En el árbol de la consola, **Certificate Template plantilla de certificado del** tecleo. Todos los Certificate Template plantilla de certificado aparecen en el panel de detalles.
5. Para desviar los pasos 2 a 4, ingrese *certtmpl.msc broche*-en *el cual* abra los Certificate

Template plantilla de certificado.

Cree el Certificate Template plantilla de certificado para el servidor Web ACS

Siga estos pasos:

1. En el panel de detalles de los Certificate Template plantilla de certificado broche-en, haga clic la plantilla del **servidor Web**.
2. En el Menú Action (Acción), haga clic la **plantilla duplicado**.
3. En el campo de nombre de la visualización de la plantilla, ingrese el *ACS*.
4. Vaya a la lengueta de la **dirección de petición** y el control **permite que la clave privada sea exportada**. También asegúrese de que la **firma y el cifrado** esté seleccionada del menú desplegable del propósito.
5. Elija las **peticiones debe utilizar uno de los CSP siguientes** y marcar el **v1.0 del Proveedor criptográfico de la base de Microsoft**. Desmarque cualquier otro CSP se marque que, y haga clic la **AUTORIZACIÓN**.
6. Vaya a la lengueta del **asunto**, elija la **fuente** en la petición, y haga clic la **AUTORIZACIÓN**.
7. Vaya a la **ficha de seguridad**, resalte el **grupo de Admins del dominio**, y aseegurese que la opción del **alistar** está marcada bajo permitido.**Nota:** Si usted elige construir de este control de la información del Active Directory solamente el **nombre principal de usuario (UPN)** y desmarcar el **nombre del email del incluido** en el asunto y el email nombre porque un nombre del email no fue ingresado para la cuenta de usuario de red inalámbrica en los usuarios de directorio activo y computadora broche-en. Si usted no inhabilita estas dos opciones, el Autoregistro intenta utilizar el email, que da lugar a un error del Autoregistro.
8. Hay medidas de seguridad complementaria si es necesario para evitar que los Certificados sean eliminados automáticamente. Éstos se pueden encontrar bajo lengueta de los requisitos de la emisión. Esto no se discute más lejos en este documento.
9. Haga Click en OK para salvar la plantilla y moverse sobre la publicación de esta plantilla desde el Certificate Authority broche-en.

Habilite el nuevo Certificate Template plantilla de certificado del servidor Web ACS

Siga estos pasos:

1. Abra las autoridades de certificación broche-en. Realice los pasos 1 a 3 en el crear el Certificate Template plantilla de certificado para la sección del servidor Web ACS, elija la opción del **Certificate Authority**, elija la **computadora local**, y el clic en Finalizar.
2. En el árbol de la consola del Certificate Authority, amplíe **ca.demo.local, y después haga clic con el botón derecho del ratón los** Certificate Template plantilla de certificado**.**
3. Va a **nuevo** > el **Certificate Template plantilla de certificado a publicar**.
4. Haga clic el **Certificate Template plantilla de certificado ACS**.
5. El Haga Click en OK y abre a los **usuarios de directorio activo y computadora broche-en**.
6. En el árbol de la consola, los **usuarios de directorio activo y computadora del** clic doble, el click derecho **demo.local, y** entonces hacen clic las propiedades**.**
7. En la lengueta de la directiva del grupo, la **directiva del Default Domain del** tecleo, y entonces hace clic **edita**. Esto abre el editor del objeto de la directiva del grupo broche-en.
8. En el árbol de la consola, amplíe el **Computer Configuration (Configuración de la computadora) > Windows Settings (Configuración de Windows) > Security Settings**

(**Configuración de seguridad**) > las **directivas de la clave pública**, y después elija las **configuraciones automáticas del pedido de certificado**.
9. Haga clic con el botón derecho del ratón las **configuraciones automáticas del pedido de certificado**, y elija el **nuevo > automático pedido de certificado**.
10. En la recepción a la página automática del asistente para la configuración del pedido de certificado, haga clic **después**.
11. En la página del Certificate Template plantilla de certificado, haga clic la **Computadora**, y después haga clic **después**.
12. Cuando usted completa la página automática del asistente para la configuración del pedido de certificado, clic en Finalizar. El tipo de certificado de la Computadora ahora aparece en el panel de detalles del editor del objeto de la directiva del grupo broche-en.
13. En el árbol de la consola, amplíe la **configuración de usuario** > las **configuraciones del** > Security (Seguridad) de las **configuraciones de Windows** > las **directivas de la clave pública**.
14. En el panel de detalles, haga doble clic las **configuraciones del Autoregistro**.
15. Elija **alistan los Certificados automáticamente** y el control **renueva los certificados vencidos, se pone al día hasta que finalicen los Certificados y quita los Certificados revocados** y los **Certificados de la actualización que utilizan los Certificate Template plantilla de certificado**.
16. Haga clic en OK.

Configuración del certificado ACS 5.1

Certificado exportable de la configuración para el ACS

Nota: El servidor ACS debe obtener un certificado de servidor del servidor de la empresa raíz CA para autenticar a un cliente PEAP de la red inalámbrica (WLAN).

Nota: Aseegurese que el Administrador IIS no está abierto durante el proceso de configuración del certificado como problemas de las causas con la información guardada en memoria caché.

1. Inicie sesión al servidor ACS con las derechas de una administración de cuenta.
2. Vaya a la **administración del sistema** > a la **configuración** > a los **Certificados de servidor local**. Haga clic en Add (Agregar).
3. Cuando usted elige un método de la creación del certificado de servidor, elija **generan el pedido de firma de certificado**. Haga clic en Next (Siguiente).
4. Ingrese un tema y una longitud de clave del certificado como el ejemplo, después haga clic el **final**:Tema del certificado - **CN=acs.demo.local**Longitud de clave - **1024**
5. El ACS indicará que se haya generado un pedido de firma de certificado. Haga clic en OK.
6. Bajo administración del sistema, van a la **configuración** > a los **Certificados de servidor local** > las **solicitudes de firma excepcionales**.**Nota:** La razón de este paso es que Windows 2003 no permite las claves exportables y usted necesita generar un pedido de certificado basado en el certificado ACS que usted creó eso lo hace anterior.
7. Elija la entrada del **pedido de firma de certificado**, y haga clic la **exportación**.
8. Salve el archivo del **.pem del** certificado ACS al escritorio.

Instale el certificado en el software ACS 5.1

Siga estos pasos:

1. Abra a un navegador y conecte con CA el servidor URL **http://10.0.10.10/certsrv**.
2. La ventana de los servicios de certificados de Microsoft aparece. Elija la **petición un certificado**.
3. Haga clic para presentar un **pedido de certificado avanzado**.
4. En el pedido avanzado, el tecleo **presenta un pedido de certificado usando un base-64-encoded…**
5. En el campo del Saved Request, si los permisos de la Seguridad del navegador, hojean al archivo y al separador de millares anteriores del pedido de certificado ACS.
6. Los ajustes de seguridad del navegador pueden no permitir el acceder del archivo en un disco. Si es así **AUTORIZACIÓN del** tecleo para realizar una goma manual.
7. Localice el archivo ACS *.pem de la exportación anterior ACS. Abra el archivo usando un editor de textos (por ejemplo, libreta).
8. Resalte el contenido entero del archivo, y haga clic la **copia**.
9. Vuelva a la ventana del pedido de certificado de Microsoft. **Pegue el** contenido copiado en el campo del Saved Request.
10. Elija el **ACS** como el Certificate Template plantilla de certificado, y el tecleo **somete**.
11. Una vez que se publica el certificado, elija el **base 64 codificado**, y haga clic el **certificado de la descarga**.
12. Haga clic la **salvaguardia** para salvar el certificado al escritorio.
13. Van al **ACS > la administración del sistema > la configuración > los Certificados de servidor local**. Elija el **certificado firmado de CA del lazo**, y haga clic **después**.
14. El tecleo **hojea**, y localiza el certificado guardado.
15. Elija el certificado ACS que fue publicado por el servidor de CA, y haga clic **abierto**.
16. También, marque el cuadro del protocolo para el **EAP**, y el clic en Finalizar.
17. El certificado CA-publicado ACS aparecerá en el certificado del local ACS.

Almacén de la identidad de la configuración ACS para el Active Directory

Siga estos pasos:

1. Conecte con el ACS y inicie sesión con la cuenta de administración.
2. Vaya a los **usuarios y la identidad salva > identidad externa salva > Active Directory**.
3. Ingrese el dominio *demo.local del* Active Directory*, ingrese la* contraseña del servidor, y haga clic TestConnection**. Haga clic la** orden OKIN para continuar.
4. Haga clic los **cambios de la salvaguardia**.**Nota:** Para más información sobre el procedimiento de la integración ACS 5.x refiera a ACS 5.x y posterior: Integración con el ejemplo de configuración del Microsoft Active Directory.

Agregue un regulador al ACS como cliente AAA

Siga estos pasos:

1. Conecte con el ACS, y vaya a los **recursos de red** > a los **dispositivos de red y a los clientes AAA**. El tecleo **crea**.
2. Ingrese en estos campos:Nombre - **wlc**IP - **10.0.1.10**Checkbox RADIUS - **Marcado**Secreto compartido - **Cisco**

3. El tecleo **somete** cuando está acabado. El regulador aparecerá pues una entrada en la lista de dispositivos de red ACS.

Políticas de acceso de la configuración ACS para la Tecnología inalámbrica

Siga estos pasos:

1. En el ACS, vaya a las **políticas de acceso** > a los **servicios del acceso**.
2. En la ventana de los servicios del acceso, el tecleo **crea**.
3. Cree un servicio del acceso, y ingrese un nombre (por ejemplo WirelessAD). Elija **basado en la plantilla del servicio**, y haga clic **selecto**.
4. En el diálogo de la página web, elija el **acceso a la red – simple**. Haga clic en OK.
5. En el diálogo de la página web, elija el **acceso a la red – simple**. Haga clic en OK. Una vez que se selecciona la plantilla, haga clic **después**.
6. Bajo protocolos permitidos, marque los cuadros para **Allow MS-CHAPv2** y **permita el PEAP**. Haga clic en Finish (Finalizar).
7. Cuando el ACS le indica a que active el nuevo servicio, haga clic **sí**.
8. En el nuevo acceso mantenga acaba de activan que fue creado/, amplíe y elija la **identidad**. Para la fuente de la identidad, haga clic **selecto**.
9. Elija **AD1** para el Active Directory que fue configurado en el ACS, **AUTORIZACIÓN del** tecleo.
10. Confirme la fuente de la identidad está AD1, y la **salvaguardia del** tecleo **cambia**.

Cree la política de acceso ACS y la regla del servicio

Siga estos pasos:

1. Vaya a las **políticas de acceso** > a las **reglas de selección del servicio**.
2. El tecleo **crea** en la ventana de la política de la selección del servicio. Dé a nueva regla un nombre (por ejemplo, *WirelessRule*). Marque el cuadro para el **protocolo** para hacer juego el **radio**.
3. Elija el **radio**, y haga clic la **AUTORIZACIÓN**.
4. Bajo resultados, elija **WirelessAD** para el servicio (creado en el paso anterior).
5. Una vez que se crea la nueva regla inalámbrica, elija y **mueva** esta regla al top, que será la primera regla para identificar la autenticación de RADIUS inalámbrica usando el Active Directory.

Configuración del cliente para el PEAP usando Windows cero tacto

En nuestro ejemplo, el CLIENTE es un ordenador que funciona con al profesional de Windows XP con el SP que actúa como cliente de red inalámbrica y obtiene el acceso a los recursos del Intranet a través de la Tecnología inalámbrica AP. Complete los procedimientos en esta sección para configurar al CLIENTE como cliente de red inalámbrica.

Realice una instalación básica y una configuración

Siga estos pasos:

1. Conecte al CLIENTE con el segmento de red del Intranet usando un cable Ethernet conectado con el concentrador.
2. En el CLIENTE, instale al profesional de Windows XP con el SP2 como ordenador del miembro nombrado CLIENT del dominio demo.local.
3. Instale al profesional de Windows XP con el SP2. Esto se debe instalar para tener soporte PEAP.**Nota:** Firewall de Windows se gira automáticamente en el profesional de Windows XP con el SP2. No apague el Firewall.

Instale el adaptador de red inalámbrica

Siga estos pasos:

1. Apague la computadora cliente.
2. Desconecte la computadora cliente del segmento de red del Intranet.
3. Recomience la computadora cliente, y después abra una sesión usando la cuenta del administrador local.
4. Instale el adaptador de red inalámbrica.**Nota:** No instale el software de configuración del fabricante para el adaptador de red inalámbrica. Instale los drivers del adaptador de red inalámbrica que usan al asistente de hardware del agregar. También, cuando está indicado, proporcione el CD proporcionado por el fabricante o un disco de los drivers actualizados para el uso del profesional de Windows XP el SP2.

Configure la conexión de red inalámbrica

Siga estos pasos:

1. Termine una sesión y después inicie sesión usando la cuenta de **WirelessUser** en el **dominio demo.local**.
2. Elija el **comienzo** > al **panel de control**, haga doble clic las **conexiones de red**, y después haga clic con el botón derecho del ratón la **conexión de red inalámbrica**.
3. Haga clic las **propiedades**, vaya a la lengueta de las **redes inalámbricas**, y aseegurese el **uso Windows de configurar mis configuraciones de la red inalámbrica** se marca.
4. Haga clic en Add (Agregar).
5. Bajo lengueta de la asociación, ingrese al *empleado* en el campo del nombre de red (SSID).
6. Elija el **WPA** para la autenticación de red, y aseegurese que la encripción de datos está fijada al **TKIP**.
7. Haga clic la lengueta de la **autenticación**.
8. Valide que configuran al tipo EAP para utilizar **EAP protegido (PEAP)**. Si no es, elíjalo del menú desplegable.
9. Si usted quisiera que la máquina fuera autenticada antes del login (que permite los scripts del login o directiva del grupo avanza para ser aplicado), el control **autentica como ordenador cuando información acerca de la computadora está disponible**.
10. Haga clic en Properties (Propiedades).
11. Como el PEAP implica la autenticación del servidor del cliente, asegúrese de que el **certificado de servidor del validar** esté marcado. También, aseegurese CA que publicó el certificado ACS se marca bajo menú de los Trusted Root Certification Authority.

12. Elija la **contraseña asegurada (v2 EAP-MSCHAP)** bajo método de autentificación como se utiliza para la autenticación interna.
13. Aseegurese el **permiso rápido volver a conectar la** casilla de verificación se marca. Entonces, **AUTORIZACIÓN del** tecleo tres veces.
14. Haga clic con el botón derecho del ratón el icono de la conexión de red inalámbrica en systray, y después haga clic las **redes inalámbricas disponibles de la visión**.
15. Haga clic la red inalámbrica del empleado, y después haga clic **conectan**. El cliente de red inalámbrica mostrará **conectado** si la conexión es acertada.
16. Después de que la autenticación sea acertada, marque la configuración TCP/IP para el adaptador de red inalámbrica usando las conexiones de red. Debe tener un intervalo de direcciones de 10.0.20.100-10.0.20.200 del alcance de DHCP o del alcance creado para los clientes de red inalámbrica de CorpNet.
17. Para probar las funciones, abra a un navegador y hojee a **http://10.0.10.10** (o a la dirección IP del servidor de CA).

Resuelva problemas la autenticación inalámbrica con el ACS

Siga estos pasos:

1. Van al **ACS >** la **supervisión y los informes**, y hacen clic la **supervisión del lanzamiento y señalan el Visualizador**.
2. Una ventana ACS separada se abrirá. **Panel del** tecleo.
3. En la mi sección de informes preferida, **autenticaciones del** tecleo **– RADIUS – hoy**.
4. Un registro mostrará todas las autenticaciones de RADIUS pues paso o fall. Dentro de una entrada registrada, haga clic en el **icono de la lupa** en la columna de los detalles.
5. El detalle de la autenticación de RADIUS proporcionará mucha información sobre las tentativas registradas.
6. La cuenta del golpe del servicio ACS puede proporcionar una descripción de las tentativas que corresponden con las reglas creadas en el ACS. Van al **ACS >** las **políticas de acceso >** los **servicios del acceso**, y hacen clic las **reglas de selección del servicio**.

La autenticación PEAP falla con el servidor ACS

Cuando su cliente falla la autenticación PEAP con un servidor ACS, marque si usted encuentra el mensaje de error `duplicado NAS del intento de autenticación` en la opción de los **intentos fallidos** bajo menú del **informe y de la actividad del** ACS.

Usted puede ser que reciba este mensaje de error cuando el Microsoft Windows XP SP2 está instalado en la máquina del cliente y Windows XP SP2 autentica contra un servidor del otro vendedor con excepción de un servidor del Microsoft IAS. Particularmente, el servidor del RADIUS de Cisco (ACS) utiliza un método distinto para calcular el tipo de protocolo extensible authentication: Longitud: Formato del valor (EAP-TLV) ID que las aplicaciones de Windows XP del método. Microsoft ha identificado esto como defecto en el supplicant de XP SP2.

Para un hotfix, el contacto Microsoft y refiere a la autenticación PEAP del artículo no es acertado cuando usted conecta con un servidor de RADIUS de tercera persona . El problema subyacente es ése en el lado del cliente, con la utilidad de Windows, el rápido vuelve a conectar la opción se inhabilita para el PEAP por abandono. Sin embargo, esta opción se habilita por abandono en el lado del servidor (ACS). Para resolver este problema, desmarque el rápido vuelven a conectar la

opción en el servidor ACS (bajo las opciones del sistema global). Alternativamente, usted puede habilitar el rápido vuelve a conectar la opción en el lado del cliente para resolver el problema.

Perorm estos pasos para habilitar rápidamente vuelve a conectar en el cliente que ejecuta Windows XP usando la utilidad de Windows:

1. Vaya al **Start (Inicio)> Settings (Configuración) > Control panel (Panel de control)**.
2. Haga doble clic el icono de las **conexiones de red**.
3. Haga clic con el botón derecho del ratón el icono de la **conexión de red inalámbrica**, y después haga clic las **propiedades**.
4. Haga clic la lengueta de las **redes inalámbricas**.
5. Elija el **uso Windows de configurar mi opción Settings de la red inalámbrica** para permitir a las ventanas para configurar el adaptador del cliente.
6. Si usted ha configurado ya un SSID, elija el SSID y haga clic las **propiedades**. Si no, haga clic **nuevo** para agregar una nueva red inalámbrica (WLAN).
7. Ingrese el SSID bajo asociación cuadro se aseeguran que la autenticación de red está **abierta** y la encripción de datos está fijada al **WEP**.
8. Haga clic la **autenticación**.
9. Elija la **autenticación del IEEE 802.1X del permiso para esta opción de red**.
10. Elija el **PEAP** como el tipo EAP, y haga clic las **propiedades**.
11. Elija el **permiso rápidamente vuelven a conectar la** opción en la parte inferior de la página.

Información Relacionada

- PEAP bajo redes inalámbricas unificadas con ACS 4.0 y Windows 2003
- Controlador LAN de la tecnología inalámbrica de Cisco (WLC) y ejemplo de configuración de Cisco ACS 5.x (TACACS+) para la autenticación Web
- Instalación y guía de actualización para el Cisco Secure Access Control System 5.1
- Soporte Técnico y Documentación - Cisco Systems