Ejemplo de configuración de la autenticación ldap para la central UCS

Contenido

Introducción

Este documento proporciona una configuración de muestra para la autenticación del Lightweight Directory Access Protocol (LDAP) para la central del Cisco Unified Computing System (UCS). Los procedimientos utilizan el Interfaz gráfica del usuario (GUI) central UCS, un dominio del ejemplo de bglucs.com, y un nombre de usuario de ejemplo del testuser.

En la versión 1.0 del software central UCS, el LDAP es el único protocolo de autenticación remota soportado. La versión 1.0 tiene soporte muy limitado para la autenticación remota y la Configuración LDAP para la central UCS sí mismo. Sin embargo, usted puede utilizar la central UCS para configurar todas las opciones para los dominios del administrador UCS manejados por la central UCS.

Las limitaciones de la autenticación remota central UCS incluyen:

- El RADIUS y el TACACS no se soportan.
- Los grupos de la asignación de la membresía del grupo LDAP para la asignación del papel y del proveedor LDAP para los reguladores del dominio múltiple no se soportan.
- El LDAP utiliza solamente el atributo de CiscoAVPair o cualquier atributo inusitado para pasar el papel. El papel pasajero es uno de los papeles predefinidos en la base de datos local de la central UCS.
- Los dominios/los protocolos de la autenticación múltiple no se soportan.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Se despliega la central UCS.
- Se despliega el Microsoft Active Directory.

Componentes Utilizados

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

- Versión 1.0 de la central UCS
- Microsoft Active Directory

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.

Recopile la información

Esta sección resume la información que usted necesita recopilar antes de que usted comience la configuración.

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

Ate a los detalles del usuario

El usuario del lazo puede ser cualquier usuario LDAP en el dominio que tiene acceso de lectura al dominio; requieren a un usuario del lazo para la Configuración LDAP. La central UCS utiliza el nombre de usuario y contraseña del usuario del lazo para conectar y preguntar el Active Directory (AD) para la autenticación de usuario y así sucesivamente. Este ejemplo utiliza la cuenta del

administrador como el usuario del lazo.

Este procedimiento describe cómo un administrador LDAP puede utilizar el editor de las interfaces del Active Directory Service (ADSI) para encontrar el DN.

1. Abra el editor ADSI.
2. Encuentre al usuario del lazo. El usuario está en la misma trayectoria que en el AD.
3. Haga clic con el botón derecho del ratón al usuario, y elija las **propiedades**.
4. En el cuadro de diálogo Propiedades, haga doble clic el **distinguishedName**.
5. Copie el DN del campo de valor.
6. Haga clic la **cancelación** para cerrar todas las ventanas.

Para obtener la contraseña para el usuario del lazo, entre en contacto al administrador AD.

Base los detalles DN

La base DN es el DN de la unidad organizativa (OU) o del envase donde la búsqueda para el usuario y los detalles del usuario comienza. Usted puede utilizar el DN de un OU creado en el AD para la central UCS o UCS. Sin embargo, usted puede encontrarla más simple utilizar el DN para la raíz del dominio sí mismo.

Este procedimiento describe cómo un administrador LDAP puede utilizar el editor ADSI para encontrar la base DN.

1. Abra el editor ADSI.
2. Encuentre el OU o el envase que se utilizarán como la base DN.
3. Haga clic con el botón derecho del ratón el OU o el envase, y elija las **propiedades**.
4. En el cuadro de diálogo Propiedades, haga doble clic el **distinguishedName**.
5. Copie el DN del campo de valor, y observe cualquier otro detalle que usted necesite.
6. Haga clic la **cancelación** para cerrar todas las ventanas.

Detalles del proveedor

El proveedor juega una función fundamental en la autenticación Idap y la autorización en la central UCS. El proveedor es uno de los servidores AD que las interrogaciones centrales UCS para buscar y autenticar al usuario y para conseguir a los detalles del usuario tales como información del papel. Esté seguro de recolectar el nombre de host o la dirección IP del servidor del proveedor AD.

Filtre la propiedad

El campo o la propiedad del filtro se utiliza para buscar la base de datos AD. La identificación del usuario ingresada en el login se devuelve al AD y se compara contra el filtro.

Usted puede utilizar sAMAccountName=$userid como el valor del filtro. el sAMAccountName es un atributo en el AD y tiene el mismo valor que la identificación del usuario AD, que se utiliza para iniciar sesión al UCS GUI central.

Agregue y configure los atributos

Esta sección resume la información que usted necesita para agregar el atributo de CiscoAVPair (si procede) y poner al día el atributo u otro de CiscoAVPair, atributo predefinido antes de que usted comience la Configuración LDAP.

El campo del atributo especifica el atributo AD (bajo propiedad del usuario), que devuelve el papel que se asignará al usuario. En la versión 1.0a del software central UCS, el atributo personalizado CiscoAVPair o cualquier otro atributo inusitado en el AD se puede poner en unidades para pasar este papel.

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

Agregue el atributo de CiscoAVPair

Para agregar un nuevo atributo al dominio, ampliar el esquema del dominio, y agregar el atributo a la clase (que, en este ejemplo, es usuario).

Este procedimiento describe cómo ampliar el esquema en un servidor de Windows AD y agregar el atributo de CiscoAVPair.

1. Login a un servidor AD.
2. Haga clic el **Start (Inicio) > Run (Ejecutar)**, el tipo **mmc**, y el Presione ENTER para abrir una consola vacía del Microsoft Management Console (MMC).
3. En el MMC, el clic en Archivo > Add**/quita Broche-en** > Add.
4. En el agregar independiente Broche-en el cuadro de diálogo, seleccione el **esquema del Active Directory**, y el haga click en Add
5. En el MMC, amplíe el **esquema del Active Directory**, haga clic con el botón derecho del ratón los **atributos**, y elija **crean el atributo**.El nuevo cuadro de diálogo del atributo del crear aparece
6. Cree un atributo nombrado CiscoAVPair en el servicio de autenticación remota.En los campos de nombre del Common Name y de la visualización del LDAP, ingrese **CiscoAVPair**.En el campo único del ID del objeto 500, ingrese **1.3.6.1.4.1.9.287247.1**.En el campo Description (Descripción), ingrese el **papel y la escena UCS**.En el campo del sintaxis, seleccione la **cadena de Unicode de la** lista desplegable.Haga Click en OK para salvar el atributo y cerrar el cuadro de diálogo.El atributo se agrega una vez al esquema, debe ser asociado o ser incluido en la clase de usuario. Esto permite que usted edite la propiedad del usuario y que especifique el valor el papel que se pasará.
7. En el mismo MMC usado para la extensión del esquema AD, amplíe las **clases**, haga clic con el botón derecho del ratón al **usuario**, y elija las **propiedades**.
8. En el cuadro de diálogo de las propiedades del usuario, haga clic la lengueta de los **atributos**, y el haga click en Add
9. En el cuadro de diálogo selecto del objeto de esquema, haga clic **CiscoAVPair**, y haga clic la **AUTORIZACIÓN**.
10. En el cuadro de diálogo de las propiedades del usuario, el tecleo **se aplica**.
11. Haga clic con el botón derecho del ratón el **esquema del Active Directory**, y elija la **recarga el esquema** para incluir los nuevos cambios.
12. En caso necesario, utilice el editor ADSI para poner al día el esquema. Haga clic con el botón derecho del ratón el **localhost**, y **ahora** elija el **esquema de la actualización**.

Ponga al día el atributo de CiscoAVPair

Este procedimiento describe cómo poner al día el atributo de CiscoAVPair. El sintaxis es `shell: roles= " <role>”.`

1. En el ADSI edite el cuadro de diálogo, localizan al usuario que necesita el acceso a la central UCS.
2. Haga clic con el botón derecho del ratón al usuario, y elija las **propiedades**.
3. En el cuadro de diálogo Propiedades, haga clic la lengueta del **editor del atributo**, hacen clic **CiscoAVPair**, y el tecleo **edita**.
4. En el cuadro de diálogo polivalente del editor de la cadena, ingrese el **shell del** valor**: roles= " admin”** en la **AUTORIZACIÓN del** campo y del tecleo de valores.
5. Haga Click en OK para salvar los cambios y cerrar el cuadro de diálogo Propiedades.

Atributo predefinido actualización

Este procedimiento describe cómo poner al día un atributo predefinido, donde está uno el papel de los rol del usuario predefinidos en la central UCS. Este ejemplo utiliza a la *compañía del* atributo para pasar el papel. El sintaxis es `shell: roles= " <role>”.`

1. En el ADSI edite el cuadro de diálogo, localizan al usuario que necesita el acceso a la central UCS.
2. Haga clic con el botón derecho del ratón al usuario, y elija las **propiedades**.
3. En el cuadro de diálogo Propiedades, haga clic la lengueta del **editor del atributo**, hacen clic a la **compañía**, y el tecleo **edita**.
4. En el cuadro de diálogo del editor del atributo de la cadena, ingrese el **shell del** valor**: roles= " admin”** en el campo de valor, y **AUTORIZACIÓN del** tecleo.
5. Haga Click en OK para salvar los cambios y cerrar el cuadro de diálogo Propiedades.

Autenticación ldap de la configuración en la central UCS

La Configuración LDAP en la central UCS se completa bajo Administración de operaciones.

1. Login a la central UCS conforme a una cuenta local.
2. Haga clic la **Administración de operaciones**, amplíe a los **grupos de dominio**, y haga clic el **>** Security (Seguridad) **operativo de las directivas**.
3. Para configurar la autenticación ldap, tome estas medidas:Configure el proveedor LDAP.Configure el grupo del proveedor LDAP (no disponible en la versión 1.0a).Cambie la regla nativa de la autenticación.

Configure el proveedor LDAP

1. Haga clic el **LDAP**, haga clic con el botón derecho del ratón los **proveedores**, y elija **crean el proveedor LDAP**.
2. En el cuadro de diálogo del proveedor del crear LDAP, agregue estos detalles, que fueron recolectados anterior.Nombre de host o IP del proveedorLazo DNBase DNFiltroAtributo (CiscoAVPair o un atributo predefinido tal como compañíaContraseña (contraseña del

usuario usado en el lazo DN)
3. Haga Click en OK para salvar la configuración y cerrar el cuadro de diálogo.

Nota: Ningún otro valor necesita ser modificado en esta pantalla. Las reglas del grupo LDAP no se soportan para la autenticación central UCS en esta versión.

Grupo del proveedor de la configuración LDAP

Nota: En la versión 1.0a, los grupos del proveedor no se soportan. Este procedimiento describe cómo configurar un grupo simulado del proveedor para utilizar en la configuración más adelante.

1. Haga clic el **LDAP**, haga clic con el botón derecho del ratón el **grupo del proveedor**, y elija **crean el grupo del proveedor LDAP**.
2. En el cuadro de diálogo del grupo del proveedor del LDAP del crear, ingrese el nombre para el grupo en el campo de nombre.
3. De la lista de proveedores disponibles a la izquierda, seleccione el proveedor, y haga clic el mayor que el símbolo (**>**) para mover ese proveedor a los proveedores asignados a la derecha.
4. Haga Click en OK para salvar los cambios y cerrar la pantalla.

Cambie la regla nativa de la autenticación

La versión 1.0a no soporta los dominios de la autenticación múltiple como en el administrador UCS. Para trabajar alrededor de esto, usted necesita modificar la regla nativa de la autenticación.

La autenticación nativa tiene la opción para modificar la autenticación para los logines predeterminados o los accesos a la consola. Puesto que los dominios múltiples no se soportan, usted puede utilizar la cuenta local o una cuenta LDAP, pero no ambas. Cambie el valor del reino para utilizar el local o el LDAP como la fuente de autenticación.

1. Haga clic la **autenticación**, haga clic con el botón derecho del ratón la **autenticación nativa**, y elija las **propiedades**.
2. Determine si usted quiere la autenticación predeterminada, la autenticación de la consola, o ambas. Utilice la autenticación predeterminada para el GUI y el comando line interface(cli). Utilice la autenticación de la consola para la opinión corazón-basada virtual de la máquina virtual de la máquina (VM) (KVM).
3. Elija el **ldap de la** lista desplegable del reino. El valor del reino determina si el local o el LDAP es la fuente de autenticación.
4. Haga Click en OK para cerrar la página.
5. En las directivas pagine, haga clic la **salvaguardia** si procede para salvar los cambios.

Nota: No hace el logout de su sesión en curso o modificar la autenticación de la consola hasta que usted verifique que la autenticación ldap trabaje correctamente. La autenticación de la consola proporciona una manera de invertir a la configuración previa. Refiera a la sección del verificar.

Verificación

Este procedimiento describe cómo probar la autenticación ldap.

1. Abra una nueva sesión en la central UCS, y ingrese el nombre de usuario y contraseña. Usted no necesita incluir un dominio o un carácter antes del nombre de usuario. Este ejemplo utiliza los testucs como el usuario del dominio.
2. La autenticación ldap es acertada si usted ve el panel de la central UCS. Visualizan al usuario en la parte inferior de la página.

Troubleshooting

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

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems