Ejemplo de Configuración de Autenticación LDAP para UCS Central

Contenido

Introducción

Este documento proporciona una configuración de ejemplo para la autenticación LDAP (protocolo ligero de acceso a directorios) para Cisco Unified Computing System (UCS) Central. Los procedimientos utilizan la interfaz gráfica de usuario (GUI) de UCS Central, un dominio de ejemplo de bglucs.com y un nombre de usuario de ejemplo de testuser.

En la versión 1.0 del software UCS Central, LDAP es el único protocolo de autenticación remota admitido. La versión 1.0 tiene soporte muy limitado para la autenticación remota y la configuración LDAP para el propio UCS Central. Sin embargo, puede utilizar UCS Central para configurar todas las opciones para los dominios UCS Manager administrados por UCS Central.

Las limitaciones de la autenticación remota de UCS Central incluyen:

- RADIUS y TACACS no son compatibles.

- No se soporta la asignación de pertenencia a grupos LDAP para la asignación de roles y grupos de proveedores LDAP para múltiples controladores de dominio.
- LDAP utiliza solamente el atributo CiscoAVPair o cualquier atributo sin utilizar para pasar la función. La función pasada es una de las funciones predefinidas de la base de datos local de UCS Central.
- No se admiten varios dominios/protocolos de autenticación.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- UCS Central está implementado.
- Microsoft Active Directory está implementado.

Componentes Utilizados

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

- UCS Central versión 1.0
- Microsoft Active Directory

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Recopilar información

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

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

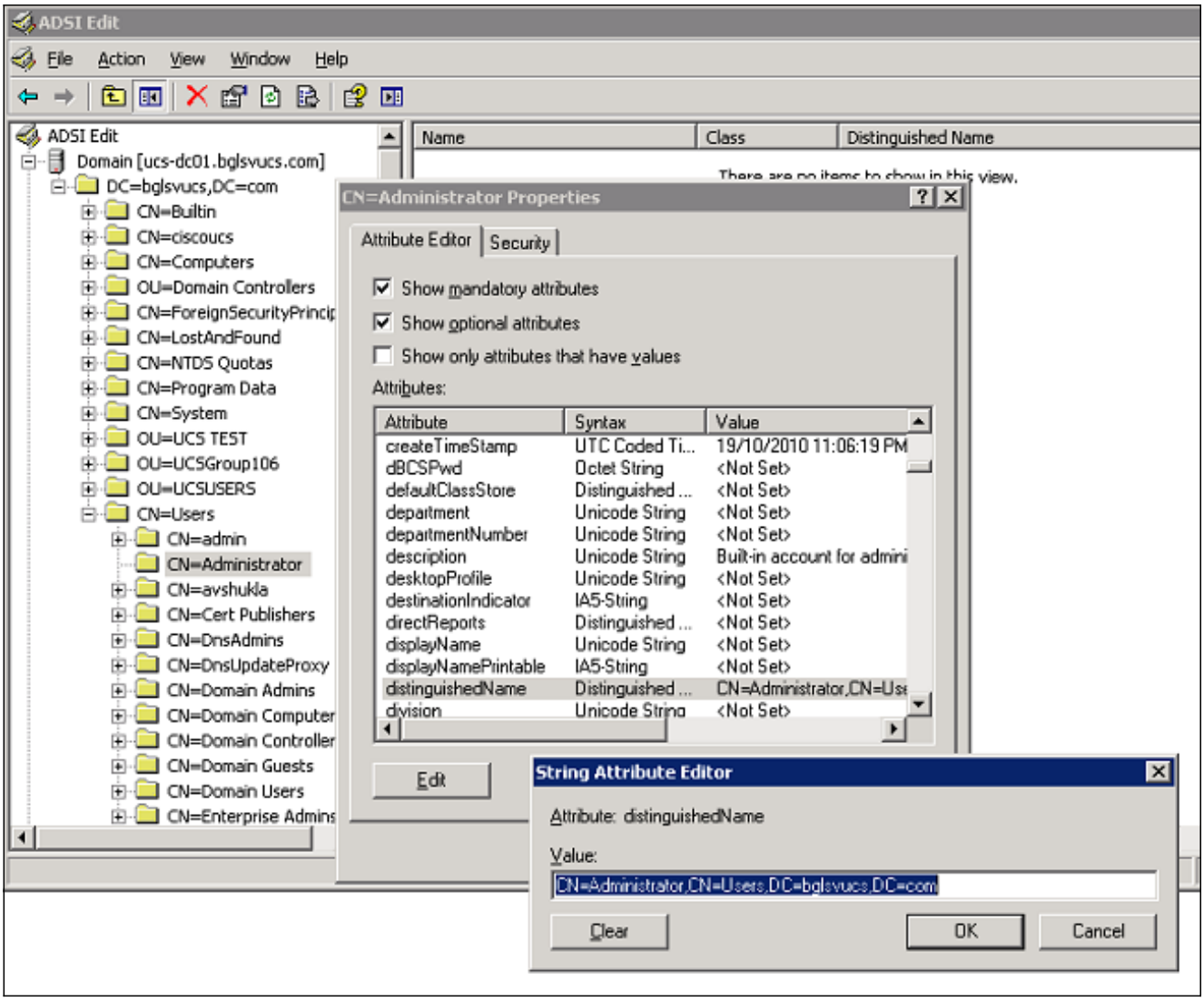
Enlazar detalles del usuario

El usuario de enlace puede ser cualquier usuario LDAP en el dominio que tenga acceso de lectura al dominio; se requiere un usuario de enlace para la configuración LDAP. UCS Central utiliza el nombre de usuario y la contraseña del usuario de enlace para conectar y consultar Active Directory (AD) para la autenticación de usuario, etc. En este ejemplo se utiliza la cuenta de administrador como usuario de enlace.

Este procedimiento describe cómo un administrador LDAP puede utilizar el Editor de interfaces de

servicio de Active Directory (ADSI) para encontrar el DN.

1. Abra el Editor ADSI.
2. Busque el usuario de enlace. El usuario se encuentra en la misma ruta que en AD.
3. Haga clic con el botón derecho del ratón en el usuario y elija **Propiedades**.
4. En el cuadro de diálogo Propiedades, haga doble clic en **nombre** distinguido.
5. Copie el DN del campo
   Valor.



6. Haga clic en **Cancelar** para cerrar todas las ventanas.

Para obtener la contraseña del usuario de enlace, póngase en contacto con el administrador de AD.

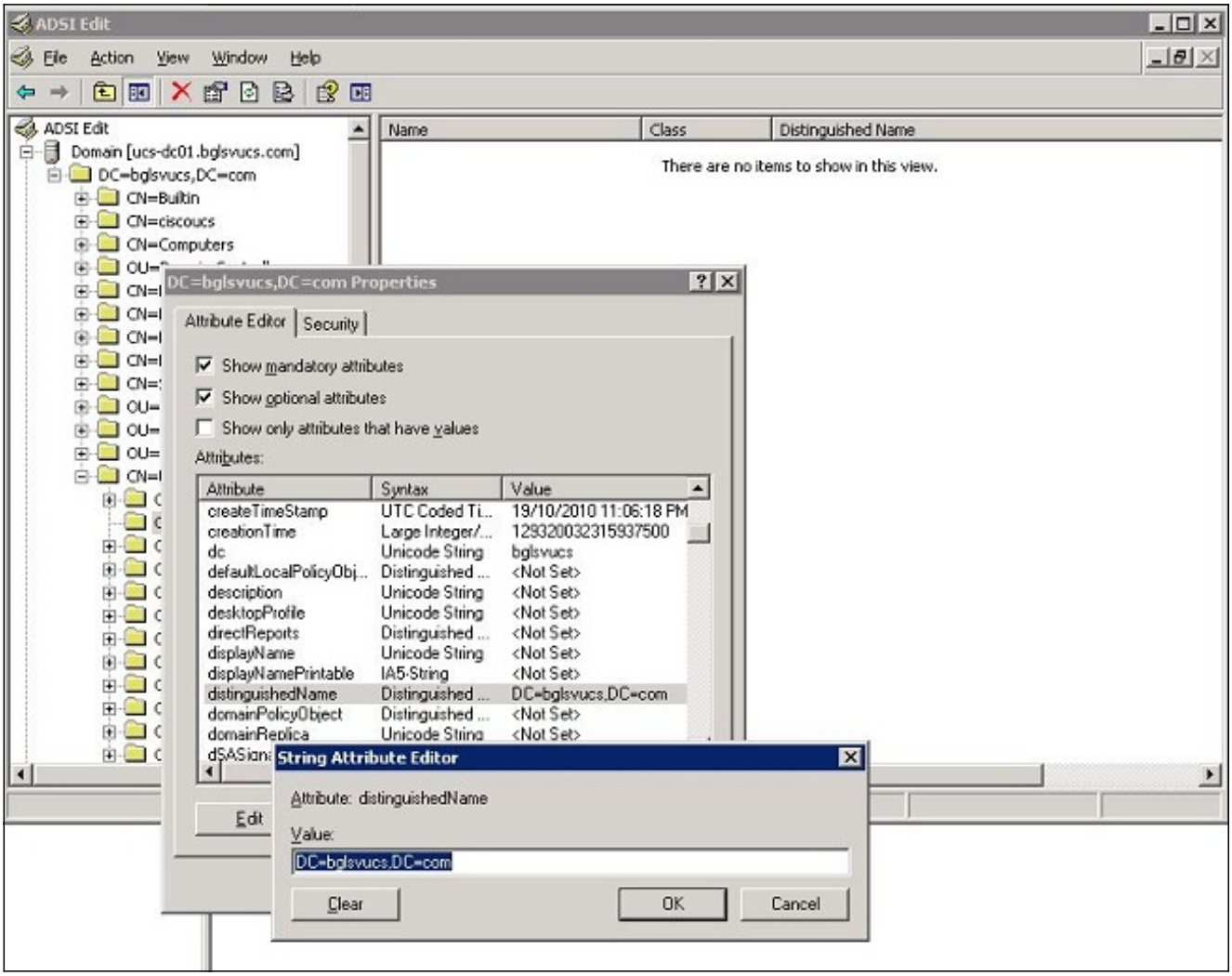
Detalles de DN base

DN base es el DN de la unidad organizativa (OU) o el contenedor donde comienza la búsqueda de los detalles del usuario y usuario. Puede utilizar el DN de una OU creada en AD para UCS o UCS Central. Sin embargo, puede que le resulte más sencillo utilizar el DN para la raíz del dominio en sí.

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

1. Abra el Editor ADSI.

2. Busque la OU o el contenedor que se utilizará como DN base.
3. Haga clic con el botón derecho del ratón en la OU o en el contenedor y elija **Propiedades**.
4. En el cuadro de diálogo Propiedades, haga doble clic en **nombre** distinguido.
5. Copie el DN del campo de valor y observe cualquier otro detalle que necesite.



6. Haga clic en **Cancelar** para cerrar todas las ventanas.

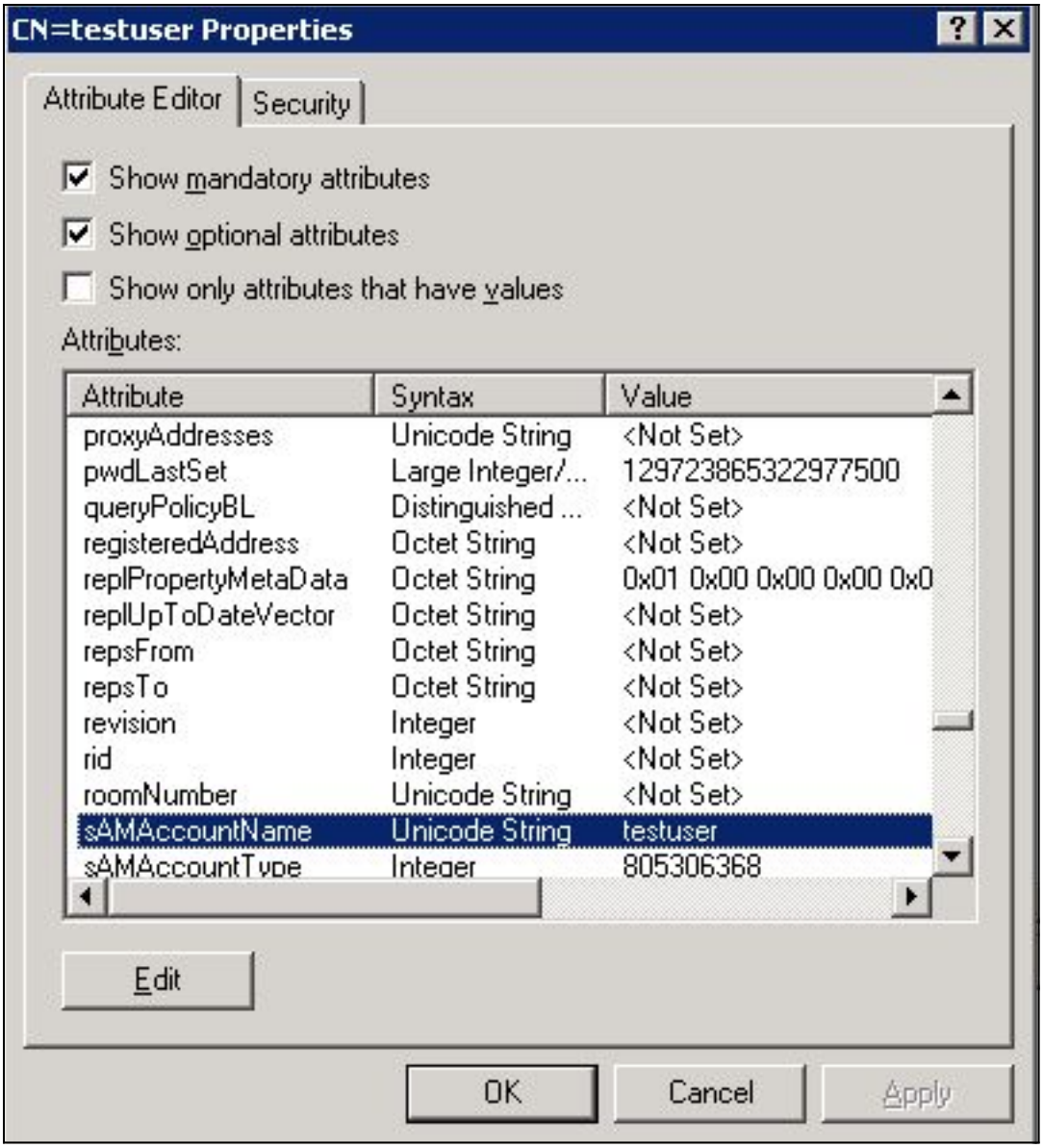
Detalles del proveedor

El proveedor desempeña un papel clave en la autenticación y autorización LDAP en UCS Central. El proveedor es uno de los servidores AD que UCS Central consulta para buscar y autenticar al usuario y para obtener detalles del usuario, como información de rol. Asegúrese de recopilar el nombre de host o la dirección IP del servidor de AD del proveedor.

Propiedad de filtro

El campo o la propiedad de filtro se utiliza para buscar la base de datos de AD. La ID de usuario ingresada al inicio de sesión se devuelve al AD y se compara con el filtro.

Puede utilizar sAMAccountName=$userid como valor de filtro. sAMAccountName es un atributo en AD y tiene el mismo valor que el ID de usuario de AD, que se utiliza para iniciar sesión en la GUI de UCS Central.



Agregar y configurar atributos

Esta sección resume la información que necesita para agregar el atributo CiscoAVPair (si es necesario) y actualizar el atributo CiscoAVPair u otro atributo predefinido antes de iniciar la configuración LDAP.

El campo de atributo especifica el atributo AD (en la propiedad de usuario), que devuelve la función que se va a asignar al usuario. En la versión 1.0a del software UCS Central, el atributo personalizado CiscoAVPair o cualquier otro atributo no utilizado en AD se puede unificar para pasar esta función.

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

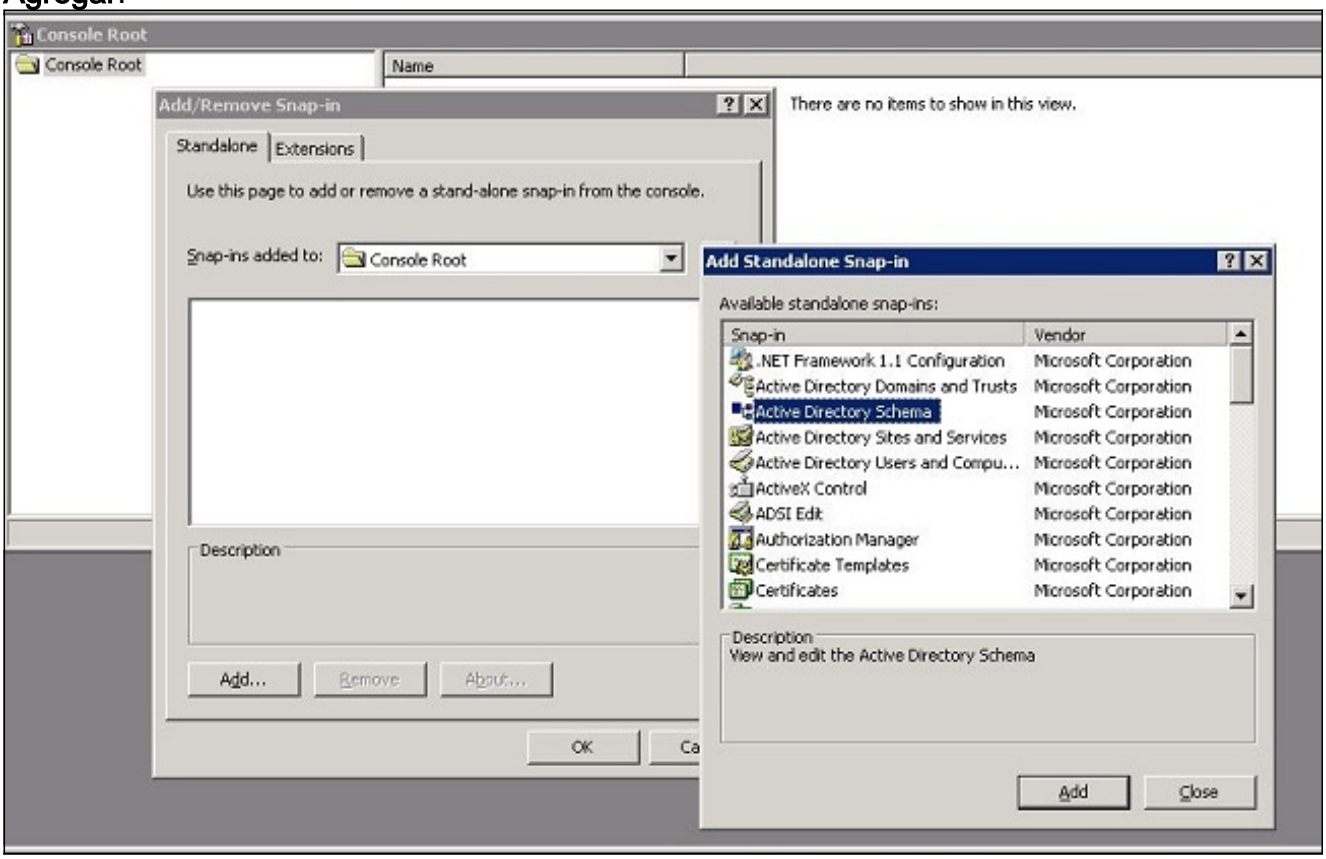
Agregar atributo CiscoAVPair

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

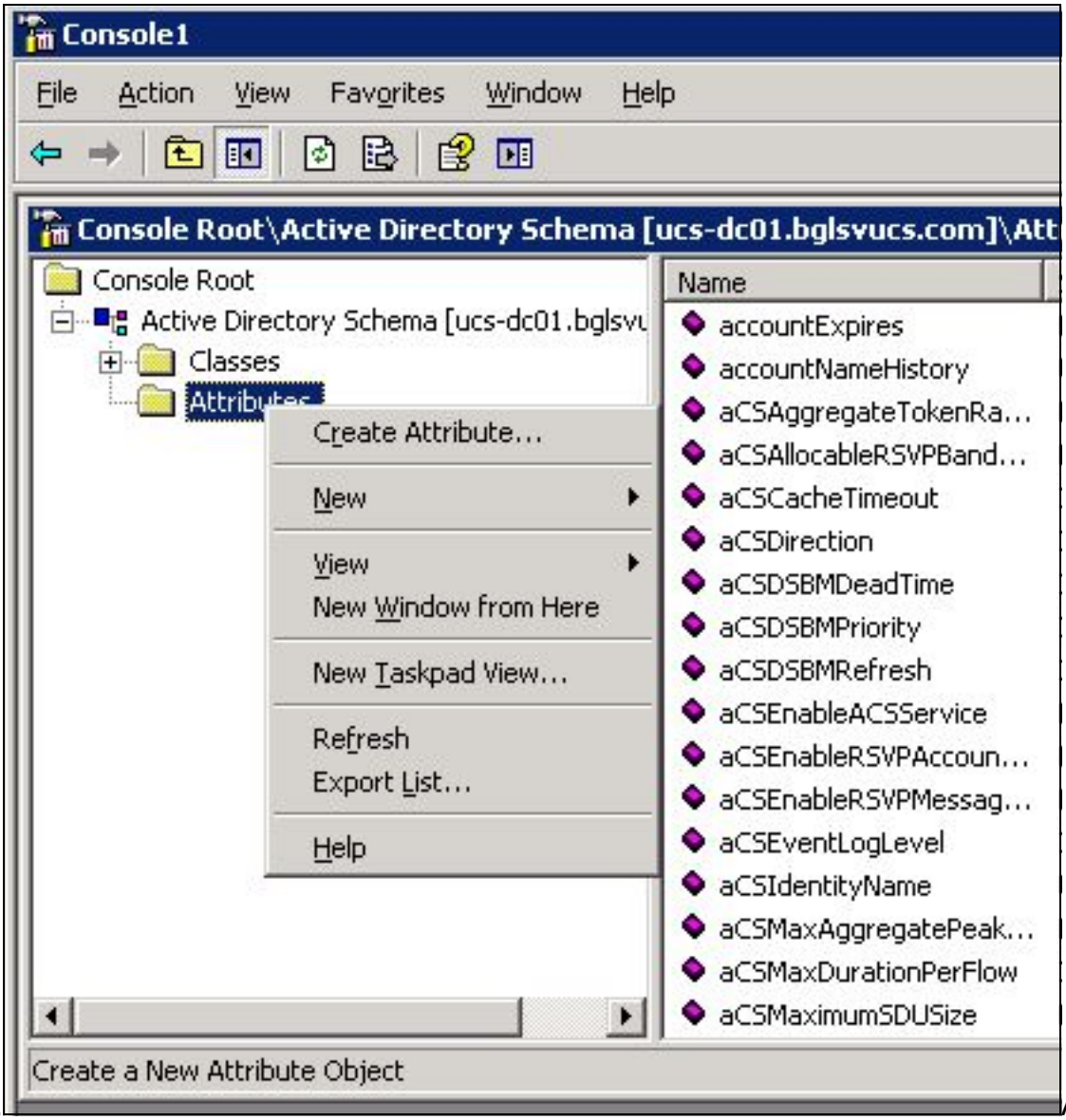
Este procedimiento describe cómo expandir el esquema en un servidor de Windows AD y agregar

el atributo CiscoAVPair.

1. Inicie sesión en un servidor AD.
2. Haga clic en **Inicio > Ejecutar**, escriba **mmc** y presione **Intro** para abrir una consola vacía de Microsoft Management Console (MMC).
3. En el MMC, haga clic en **Archivo > Agregar o quitar complemento > Agregar**.
4. En el cuadro de diálogo Agregar complemento independiente, seleccione el **esquema de Active Directory** y haga clic en **Agregar**.

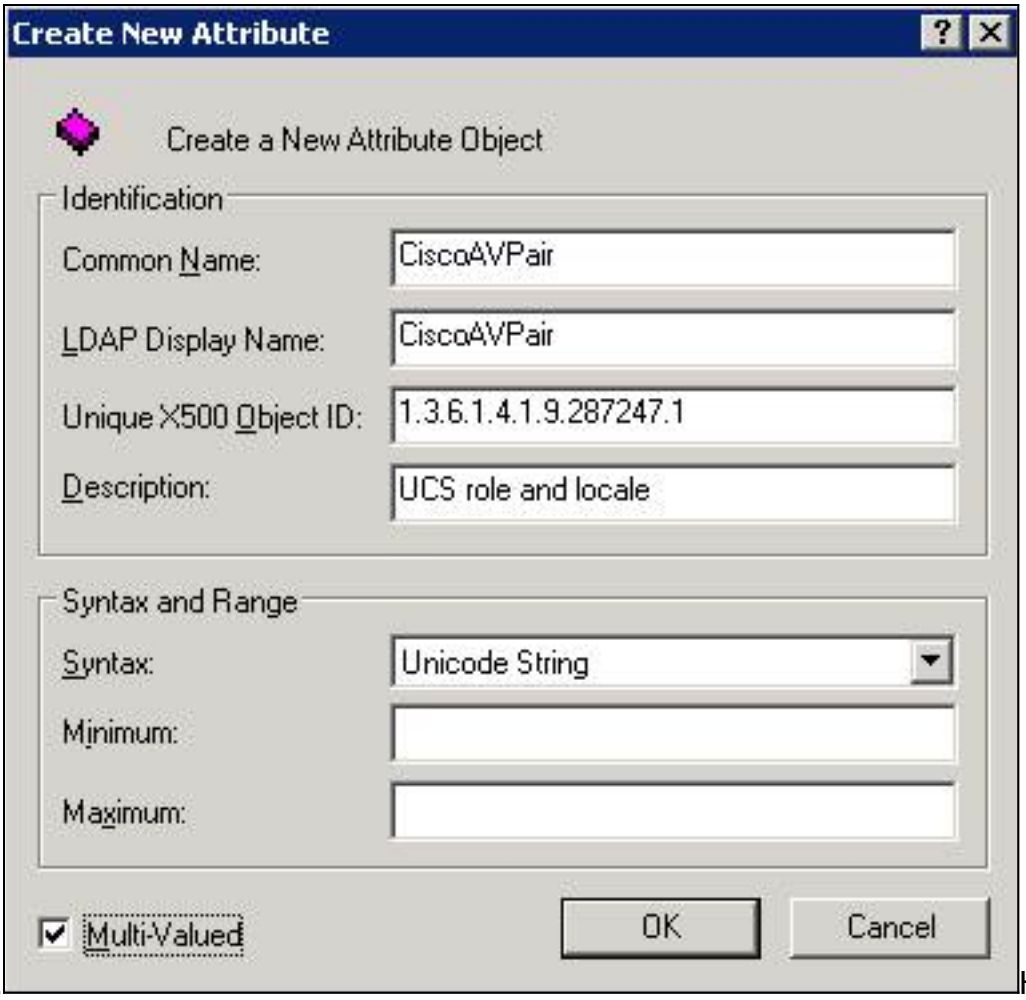


5. En el MMC, expanda **Esquema de Active Directory**, haga clic con el botón derecho en **Atributos** y elija **Crear**



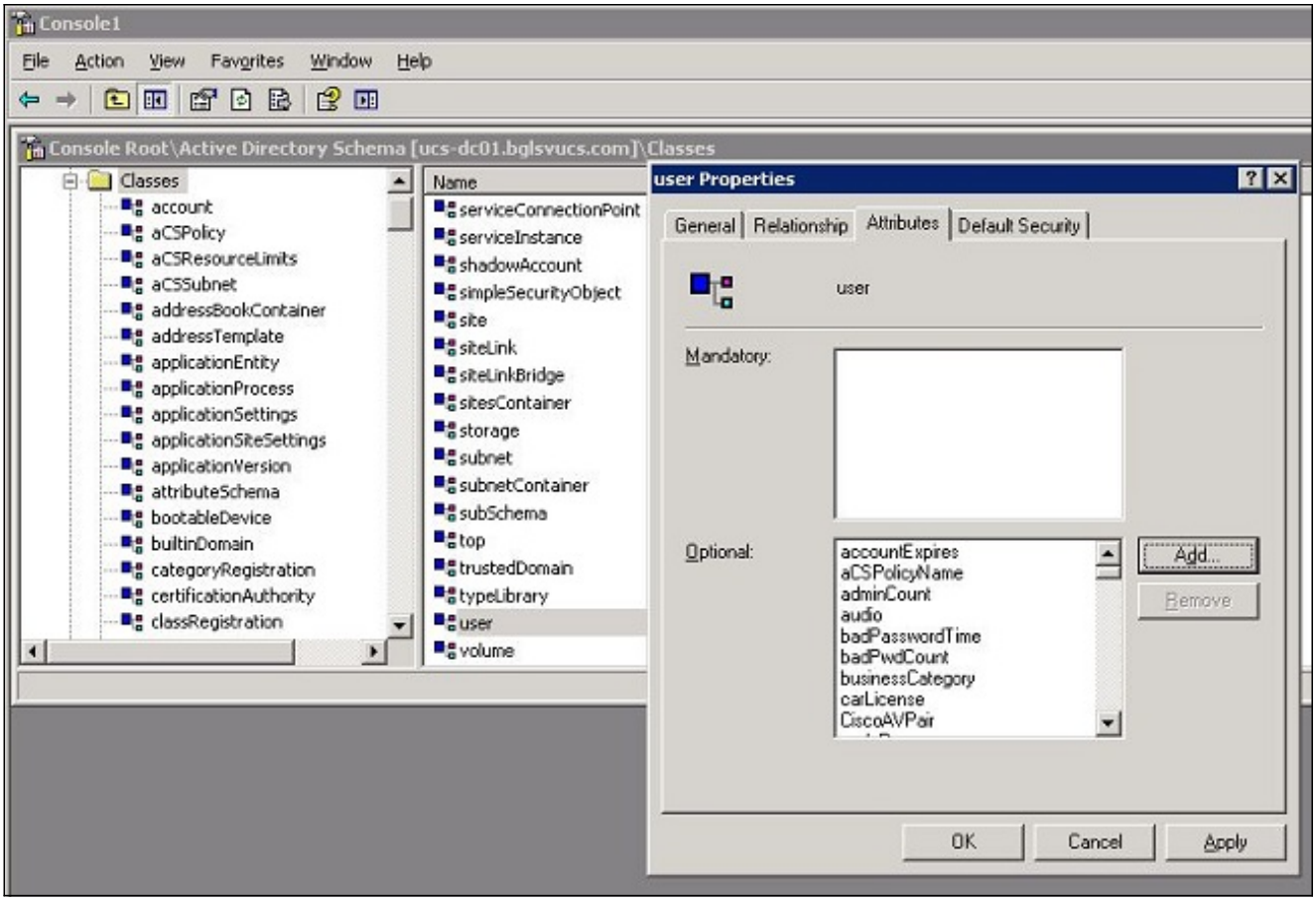
atributo.Aparecerá el cuadro de diálogo Crear nuevo atributo

6. Cree un atributo denominado CiscoAVPair en el servicio de autenticación remota.En los campos Nombre común y Nombre de visualización LDAP, ingrese **CiscoAVPair**.En el campo Identificador de objeto único 500, introduzca **1.3.6.1.4.1.9.287247.1**.En el campo Description (Descripción), introduzca **UCS role and locale**.En el campo Sintaxis, seleccione **Cadena Unicode** en la lista

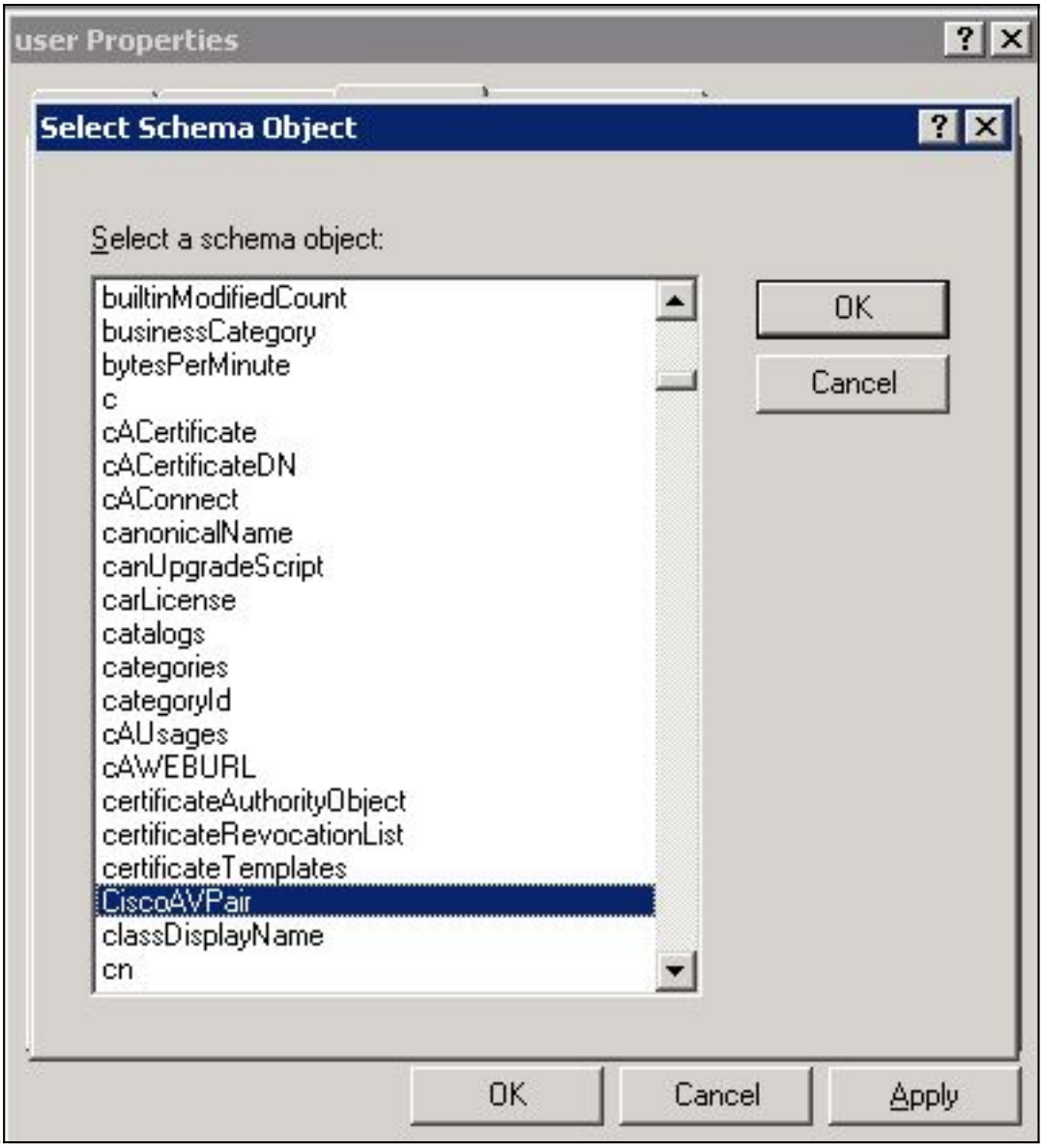


desplegable.Haga clic en **Aceptar** para guardar el atributo y cerrar el cuadro de diálogo.Una vez agregado el atributo al esquema, se debe asignar o incluir en la clase de usuario. Esto permite editar la propiedad de usuario y especificar el valor de la función que se va a pasar.

7. En el mismo MMC utilizado para la expansión del esquema de AD, expanda **Clases**, haga clic con el botón derecho en **usuario** y elija **Propiedades**.
8. En el cuadro de diálogo Propiedades del usuario, haga clic en la ficha **Atributos** y haga clic en
Agregar.

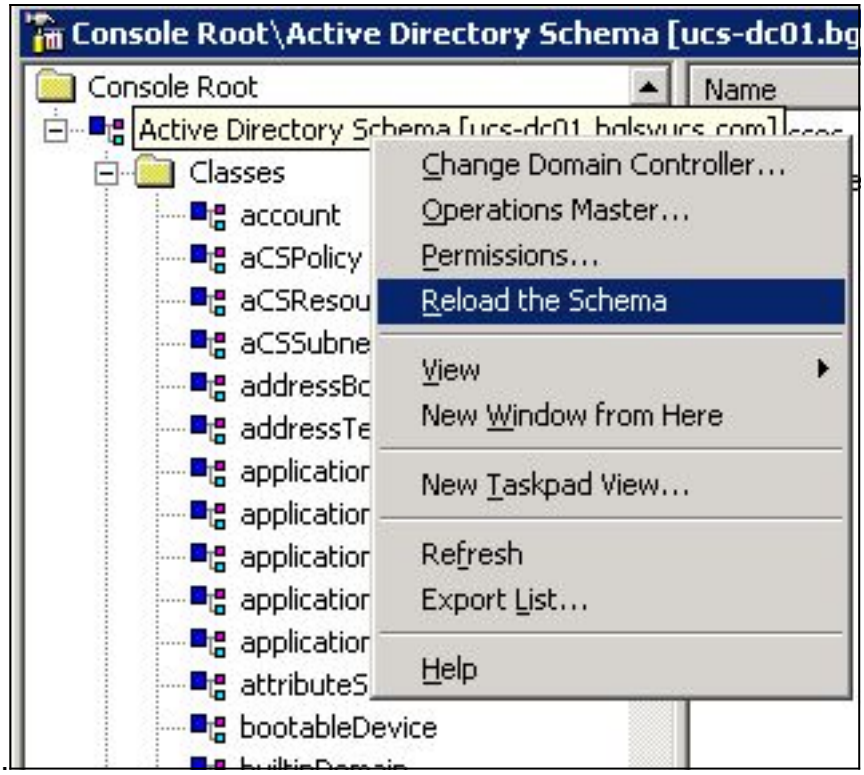


9. En el cuadro de diálogo Seleccionar objeto de esquema, haga clic en **CiscoAVPair** y haga

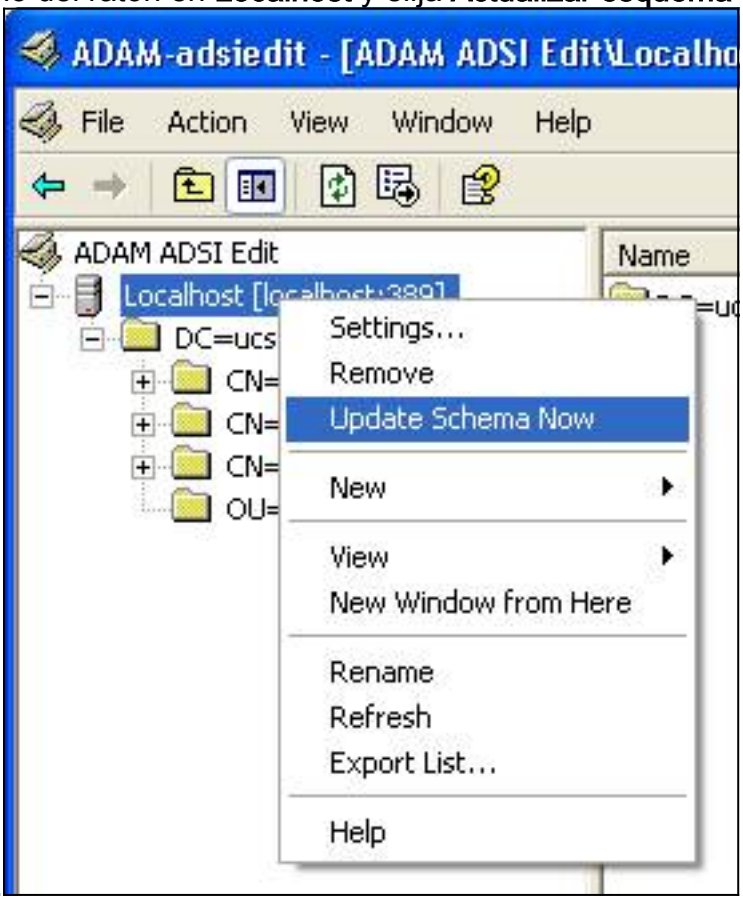


clic en **Aceptar**.

10. En el cuadro de diálogo Propiedades del usuario, haga clic en **Aplicar**.
11. Haga clic con el botón derecho en **Esquema de Active Directory** y elija **Recargar el Esquema** para incluir los nuevos

cambios. 

12. Si es necesario, utilice el Editor ADSI para actualizar el esquema. Haga clic con el botón derecho del ratón en **Localhost** y elija **Actualizar esquema**

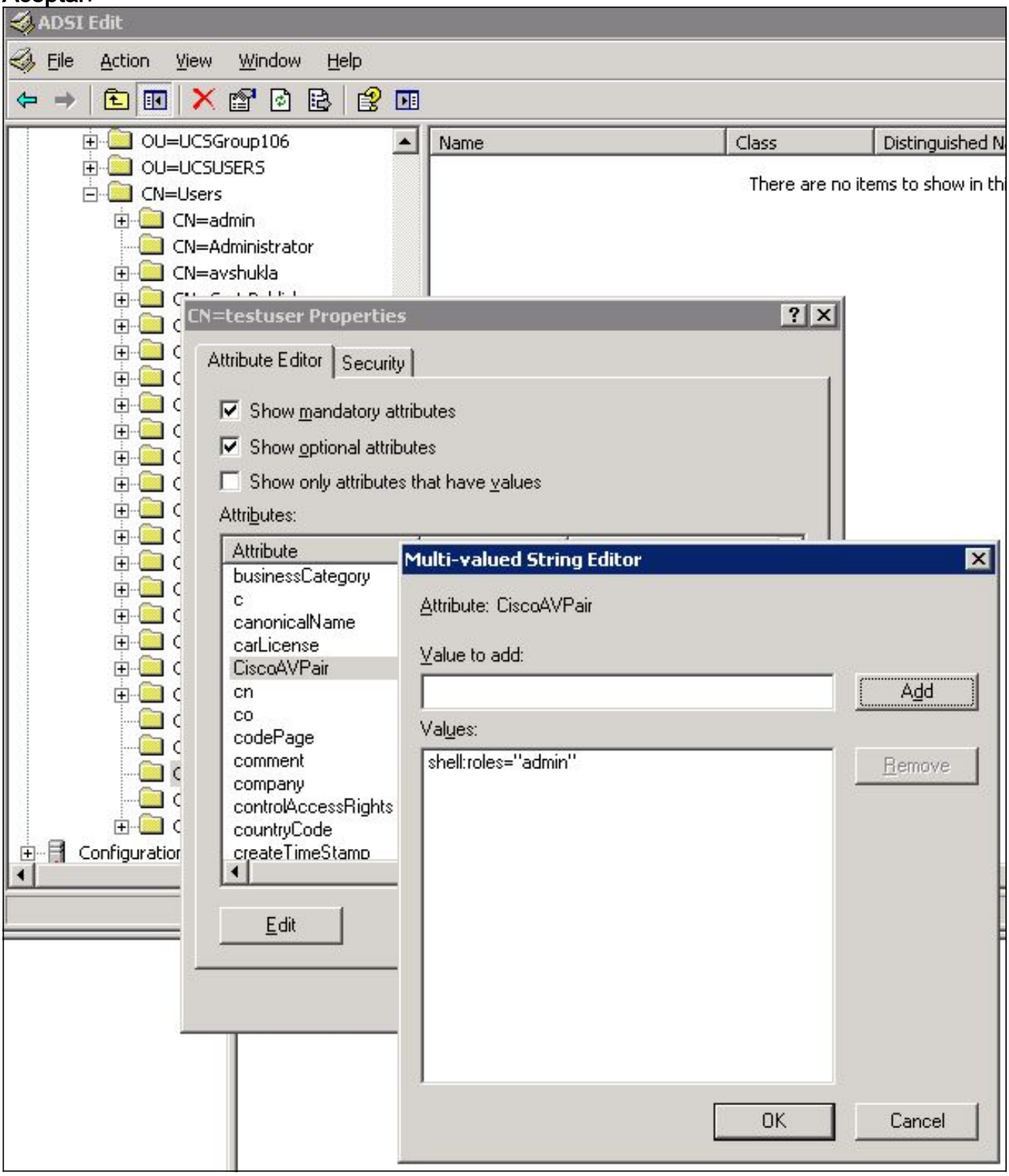
ahora. 

Actualizar atributo CiscoAVPair

Este procedimiento describe cómo actualizar el atributo CiscoAVPair. La sintaxis es `shell:roles="<role>"`.

1. En el cuadro de diálogo Editar ADSI, busque el usuario que necesita acceso a UCS Central.

2. Haga clic con el botón derecho del ratón en el usuario y elija **Propiedades**.
3. En el cuadro de diálogo Propiedades, haga clic en la ficha **Editor de atributos**, haga clic en **CiscoAVPair** y haga clic en **Editar**.
4. En el cuadro de diálogo Editor de cadenas multivaloradas, introduzca el valor **shell:roles="admin"** en el campo Valores y haga clic en **Aceptar**.



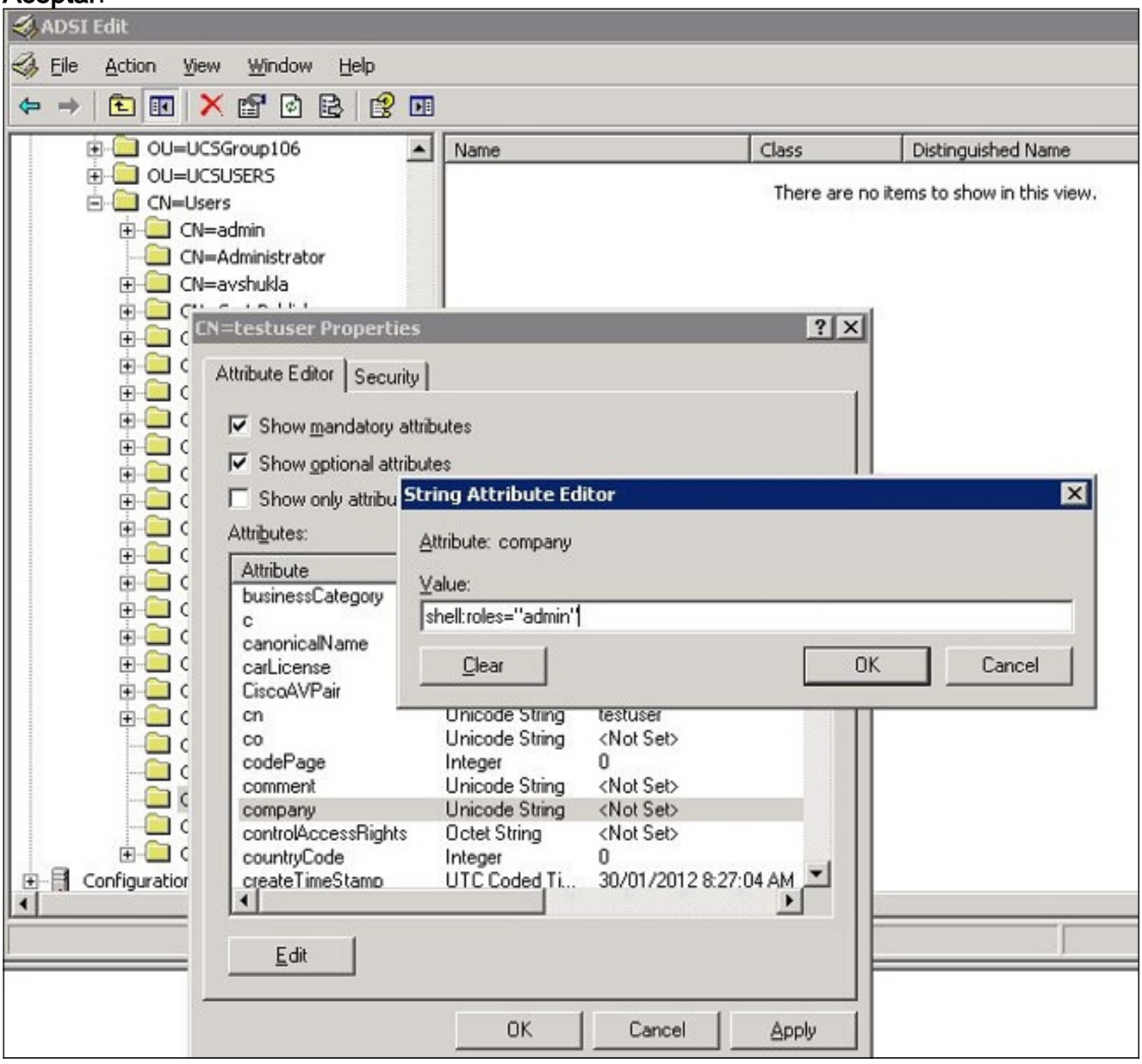
5. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo Propiedades.

Actualizar atributo predefinido

Este procedimiento describe cómo actualizar un atributo predefinido, donde la función es una de las funciones de usuario predefinidas en UCS Central. Este ejemplo utiliza la *compañía* de

atributos para pasar la función. La sintaxis es `shell:roles="<role>"`.

1. En el cuadro de diálogo Editar ADSI, busque el usuario que necesita acceso a UCS Central.
2. Haga clic con el botón derecho del ratón en el usuario y elija **Propiedades**.
3. En el cuadro de diálogo Propiedades, haga clic en la ficha **Editor de atributos**, haga clic en **compañía** y haga clic en **Editar**.
4. En el cuadro de diálogo Editor de atributos de cadena, introduzca el valor **shell:roles="admin"** en el campo Valor y haga clic en **Aceptar**.

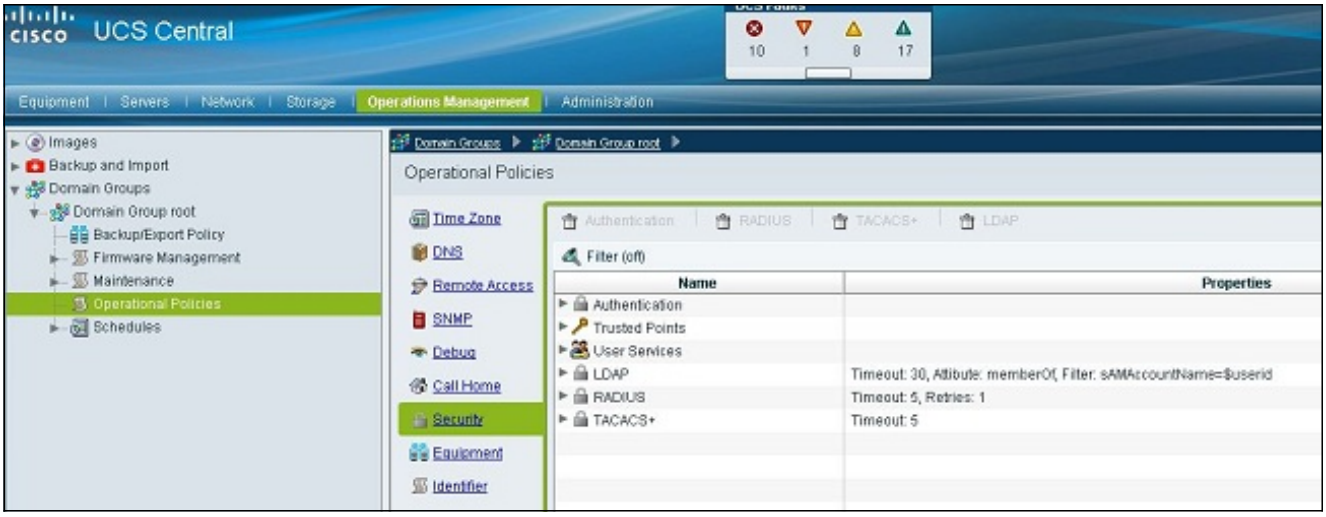


5. Haga clic en **Aceptar** para guardar los cambios y cerrar el cuadro de diálogo Propiedades.

Configuración de la autenticación LDAP en UCS Central

La configuración LDAP en UCS Central se completa en Operations Management.

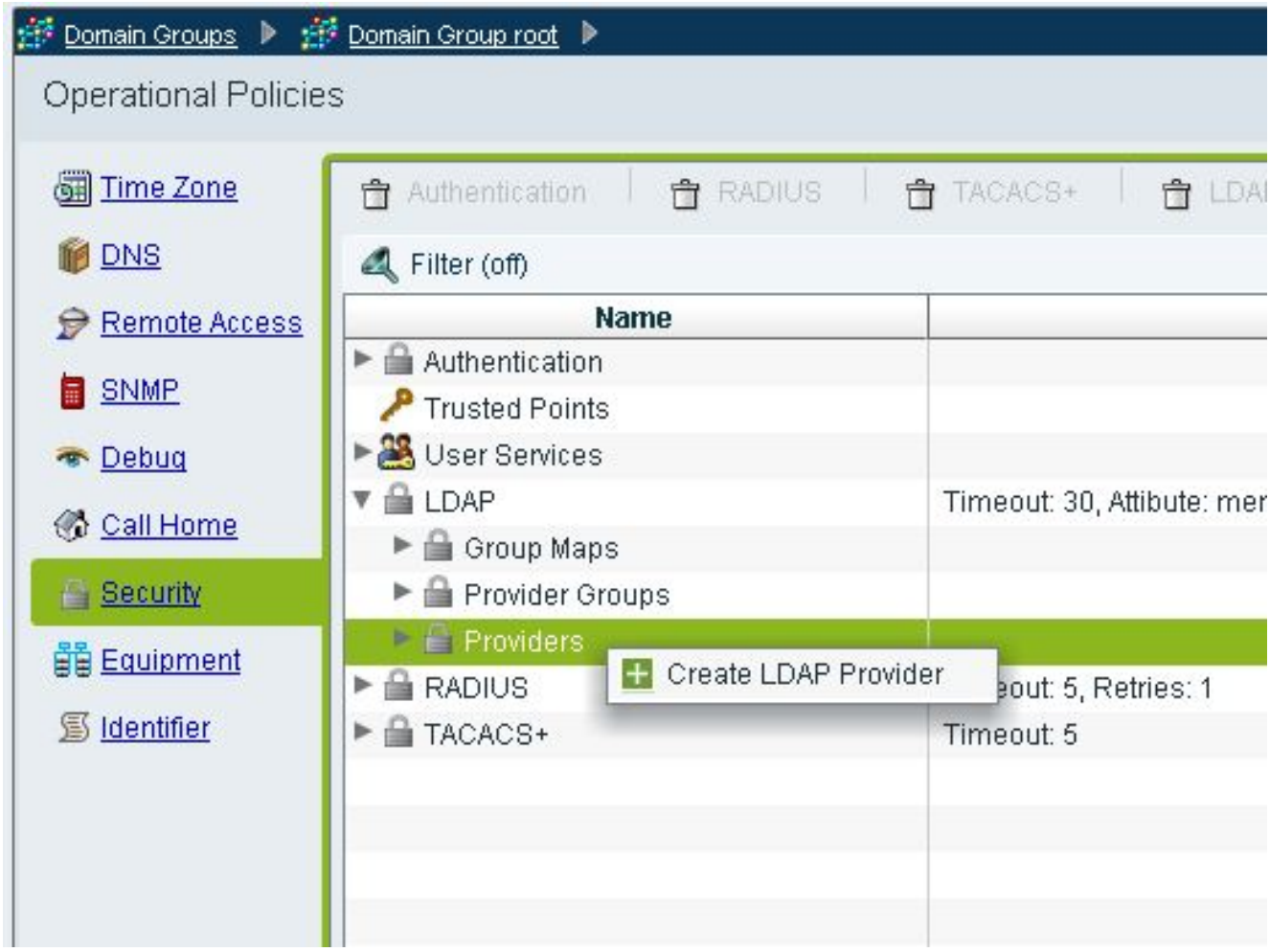
1. Inicie sesión en UCS Central en una cuenta local.
2. Haga clic en **Operations Management**, expanda **Domain Groups** y haga clic en **Operational Policies** > **Security**.



3. Para configurar la autenticación LDAP, siga estos pasos:Configure el proveedor LDAP.Configure el grupo de proveedores LDAP (no disponible en la versión 1.0a).Cambie la regla de autenticación nativa.

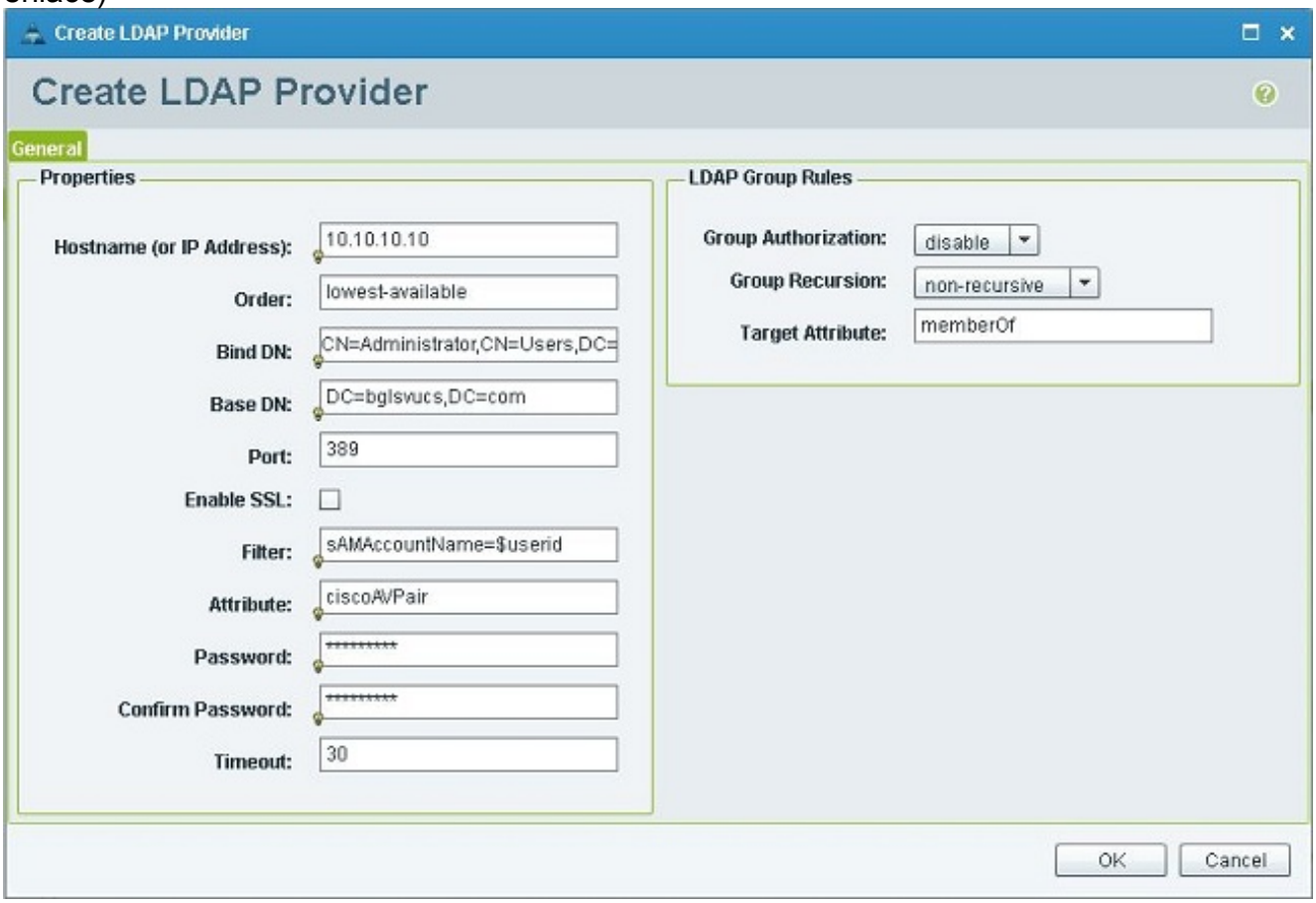
Configurar proveedor LDAP

1. Haga clic en **LDAP**, haga clic con el botón derecho en **Proveedores** y elija **Crear proveedor LDAP**.



2. En el cuadro de diálogo Crear proveedor LDAP, agregue estos detalles, que se recopilaron anteriormente.Nombre de host o IP del proveedorEnlazar DNDN baseFiltroAtributo (CiscoAVPair o un atributo predefinido como la empresaContraseña (contraseña del usuario utilizada en el DN de

enlace)



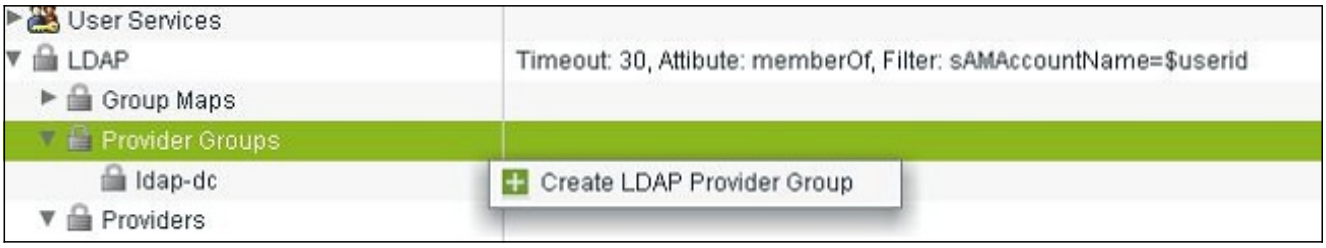
3. Haga clic en **Aceptar** para guardar la configuración y cerrar el cuadro de diálogo.

Nota: No es necesario modificar ningún otro valor en esta pantalla. Las reglas del grupo LDAP no son compatibles con la autenticación de UCS Central en esta versión.

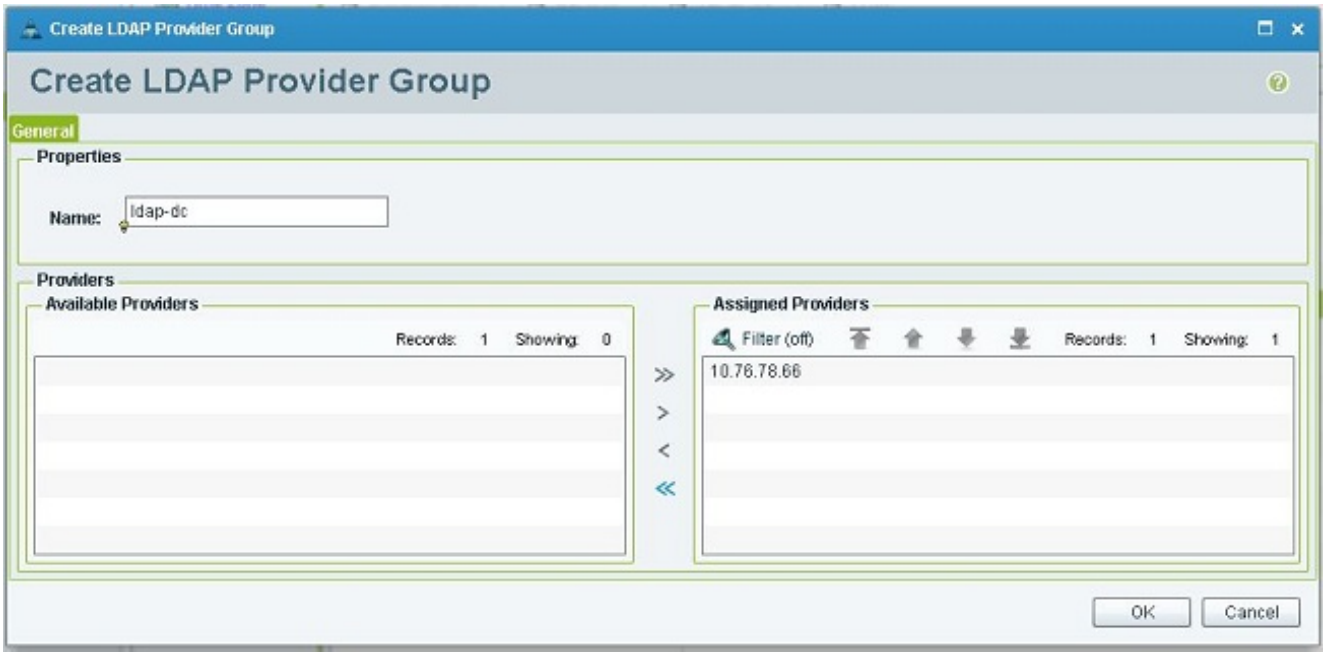
Configurar grupo de proveedores LDAP

Nota: En la versión 1.0a, no se admiten grupos de proveedores. Este procedimiento describe cómo configurar un grupo de proveedores ficticio para que lo use más adelante en la configuración.

1. Haga clic en **LDAP**, haga clic con el botón derecho del mouse en **Grupo de Proveedores** y elija **Crear Grupo de Proveedores LDAP**.



2. En el cuadro de diálogo Crear grupo de proveedores LDAP, introduzca el nombre del grupo en el campo Nombre.
3. En la lista de proveedores disponibles a la izquierda, seleccione el proveedor y haga clic en el símbolo mayor que (**>**) para mover ese proveedor a Proveedores asignados a la derecha.



4. Haga clic en **Aceptar** para guardar los cambios y cerrar la pantalla.

Cambiar regla de autenticación nativa

La versión 1.0a no admite varios dominios de autenticación como en UCS Manager. Para solucionar esto, debe modificar la regla de autenticación nativa.

La autenticación nativa tiene la opción de modificar la autenticación para los inicios de sesión o inicios de sesión de consola predeterminados. Dado que no se soportan varios dominios, puede utilizar la cuenta local o una cuenta LDAP, pero no ambos. Cambie el valor de rango para utilizar local o LDAP como origen de autenticación.

1. Haga clic en **Authentication**, haga clic con el botón derecho en **Native Authentication** y elija **Properties**.
2. Determine si desea autenticación predeterminada, autenticación de consola o ambas. Utilice la autenticación predeterminada para la interfaz gráfica de usuario y la interfaz de línea de comandos (CLI). Utilice la autenticación de consola para la vista de máquina virtual (KVM) basada en kernel de máquina virtual (VM).
3. Elija **ldap** en la lista desplegable Rango. El valor de rango determina si local o LDAP es el origen de la
autenticación.

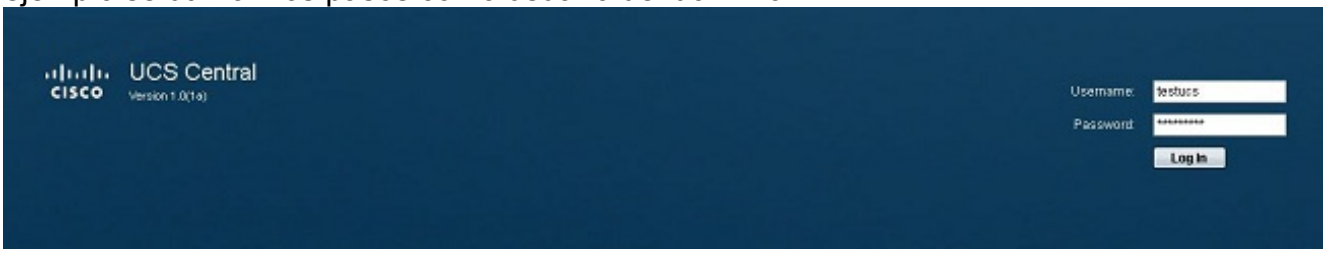
4. Haga clic en **Aceptar** para cerrar la página.
5. En la página Políticas, haga clic en **Guardar** si es necesario para guardar los cambios.

Nota: No cierre la sesión actual ni modifique la autenticación de la consola hasta que verifique que la autenticación LDAP funcione correctamente. La autenticación de consola proporciona una manera de volver a la configuración anterior. Consulte la sección Verificación.

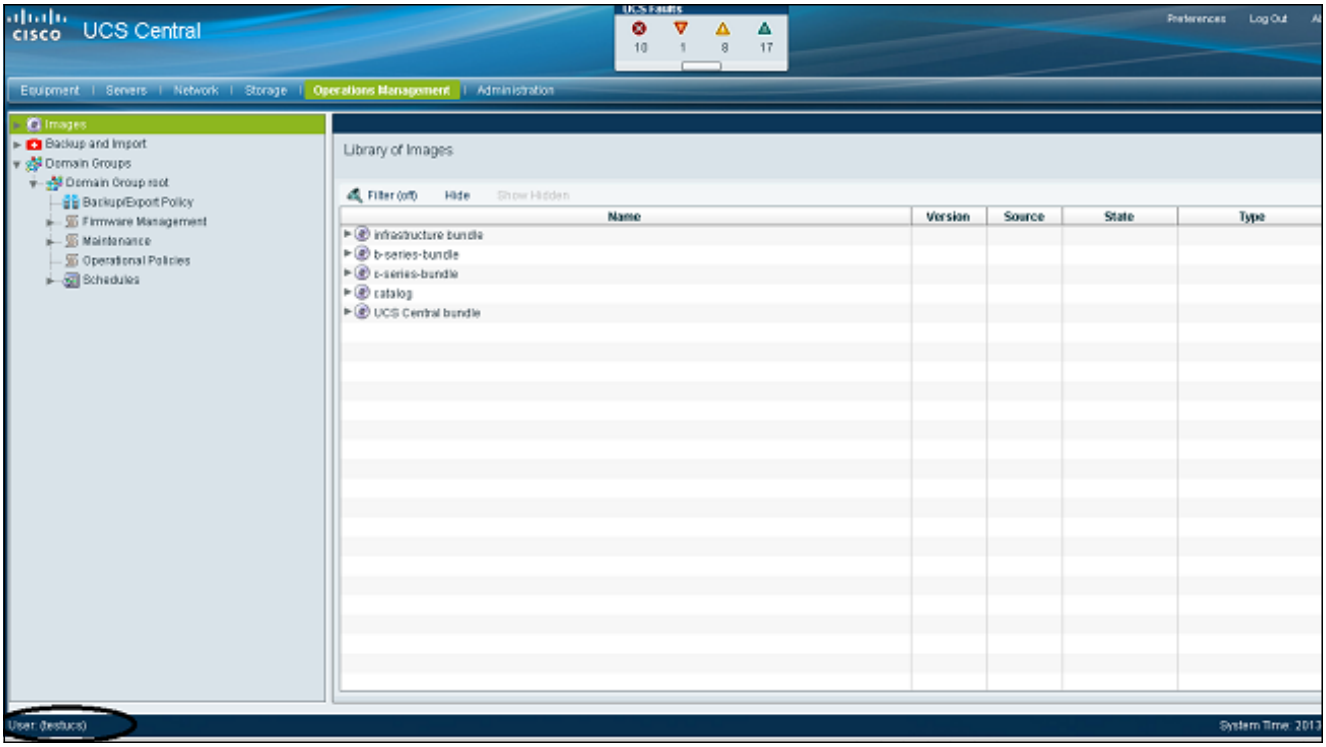
Verificación

Este procedimiento describe cómo probar la autenticación LDAP.

1. Abra una nueva sesión en UCS Central e introduzca el nombre de usuario y la contraseña. No es necesario incluir un dominio o un carácter antes del nombre de usuario. En este ejemplo se utilizan los pasos como usuario del dominio.



2. La autenticación LDAP es correcta si ve el panel de UCS Central. El usuario se muestra en la parte inferior de la
página.



Troubleshoot

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

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems