Configuración de LDAP seguro en servidores UCS C-Series

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Antecedentes

Configuración en el lado del servidor de la serie C de UCS

Verificación

Introducción

Este documento describe cómo configurar SecureLDAP en servidores de la serie C.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos de Cisco UCS y CIMC.

Componentes Utilizados

- Servidor de la serie C de Cisco UCS en modo independiente.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

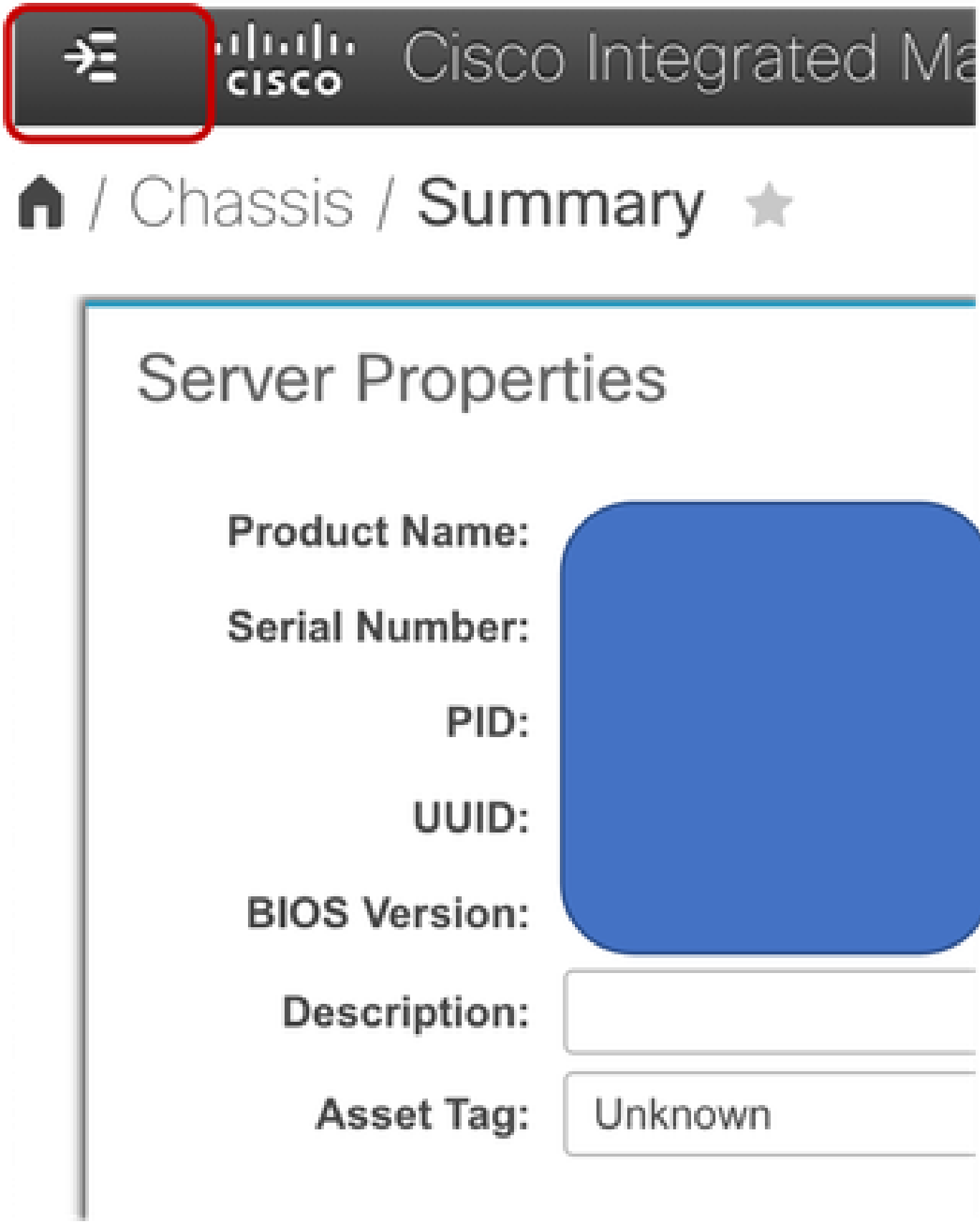
El ejemplo de esta guía muestra la configuración LDAP segura en los servidores de la serie C de UCS:

- Configure un servidor DNS, permitiendo el uso de nombres de dominio para el servidor LDAP en lugar de una dirección IP en el servidor UCS. Asegúrese de que se han configurado los registros A adecuados para que señalen a las direcciones IP del servidor

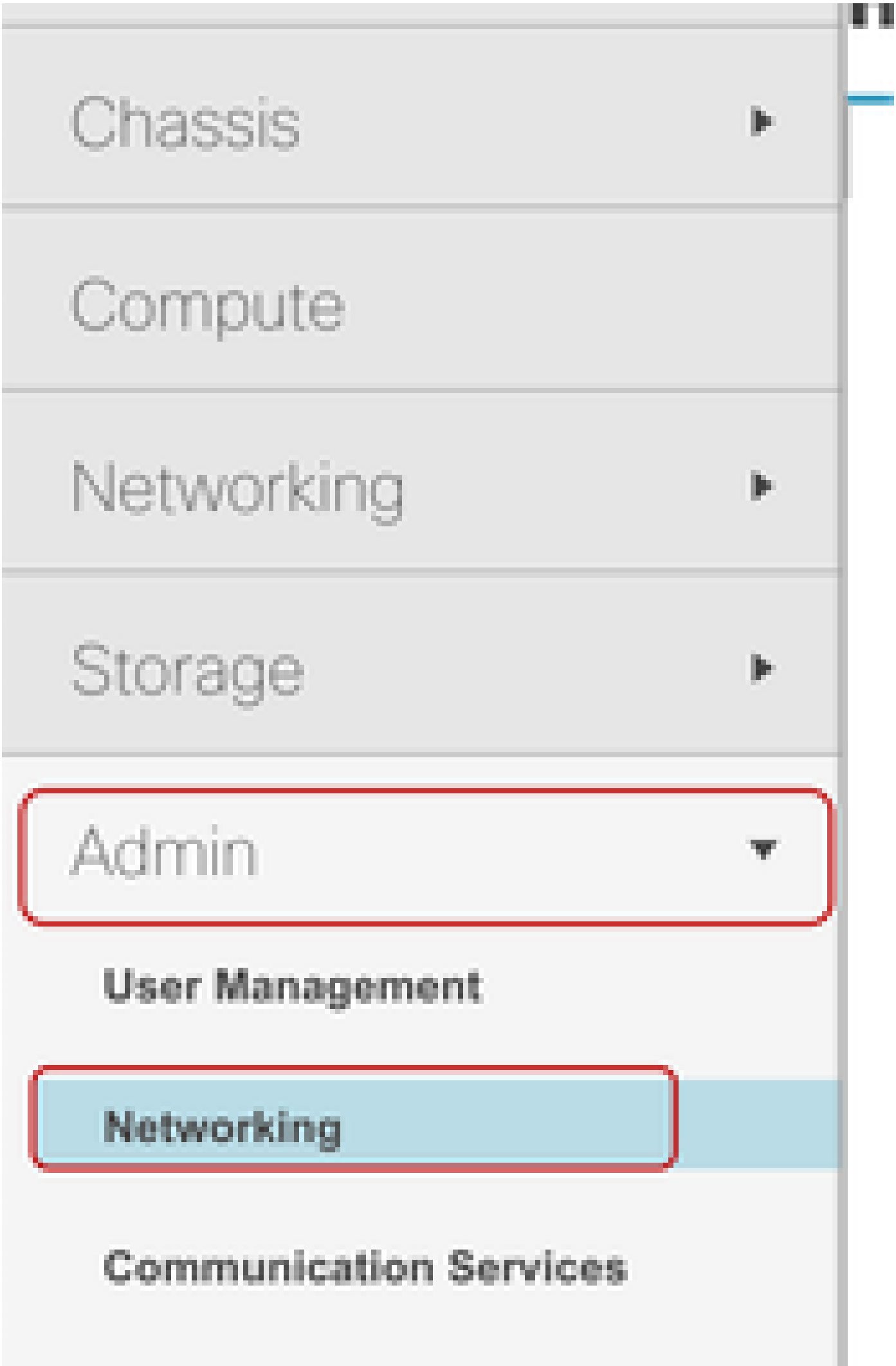
LDAP y del servidor de la serie C de UCS.
- Configure los Servicios de Certificate Server de Windows en el servidor LDAP, habilitando la Generación de certificados para la comunicación LDAP segura. Los certificados generados (raíz e intermedio) se cargan en el servidor de la serie C de UCS.

Configuración en el lado del servidor de la serie C de UCS

Para configurar el servidor de la serie C de UCS para que interactúe con un servidor DNS preconfigurado, acceda a la interfaz CIMC del servidor UCS y, a continuación, haga clic en el icono de navegación situado en la esquina superior izquierda.

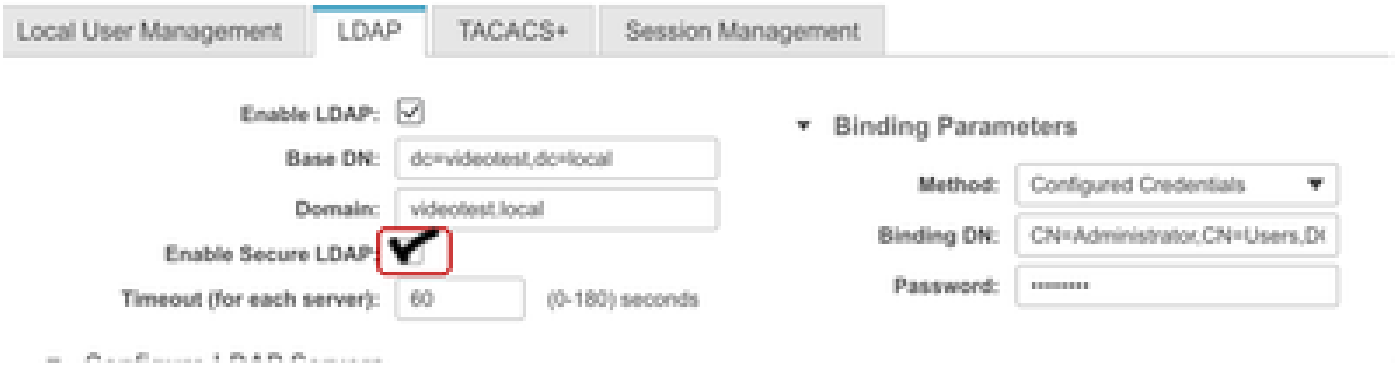


Navegue hasta Admin y elija Networking.


Chassis
Compute
Networking
Storage
Admin
User Management
Networking
Communication Services

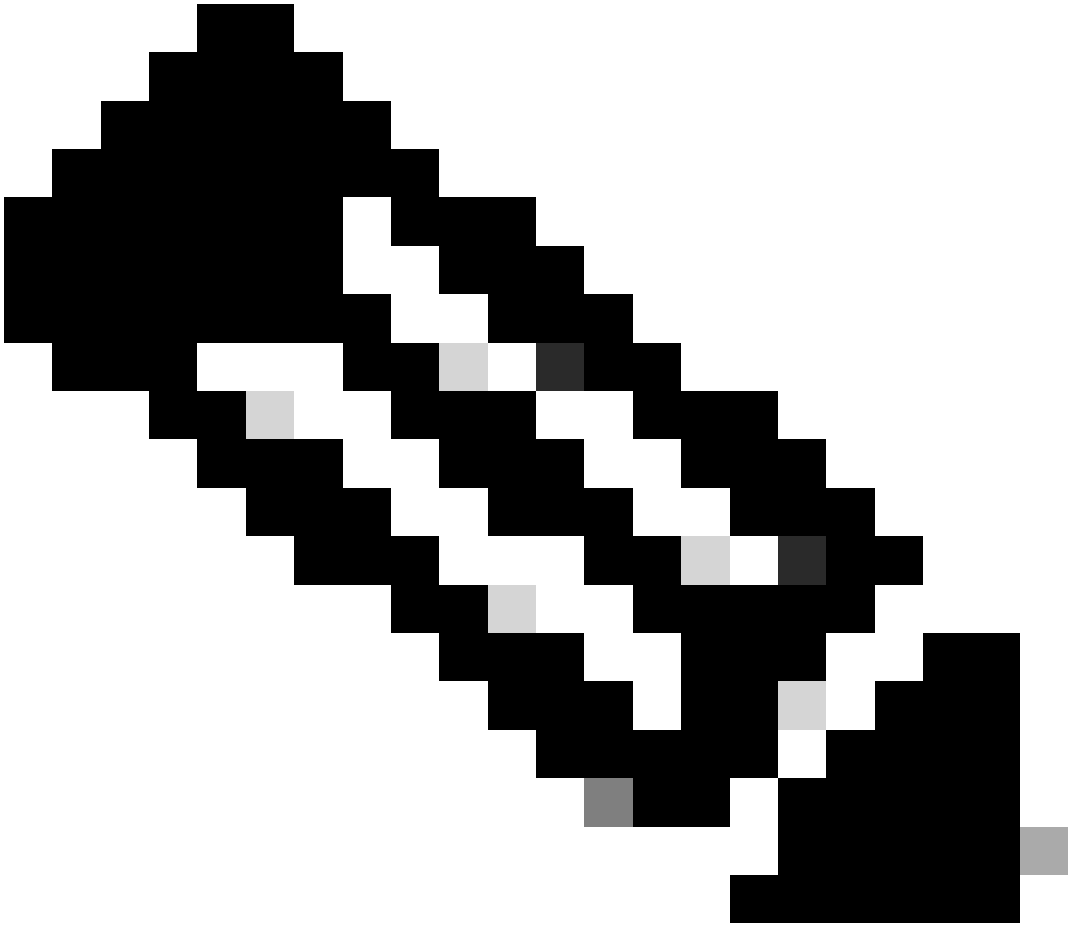
, configure los parámetros BaseDN, Domain, Timeout y Bind en alineación con las prácticas de configuración LDAP estándar.

A continuación, marque la casilla de verificación Enable Secure LDAP.



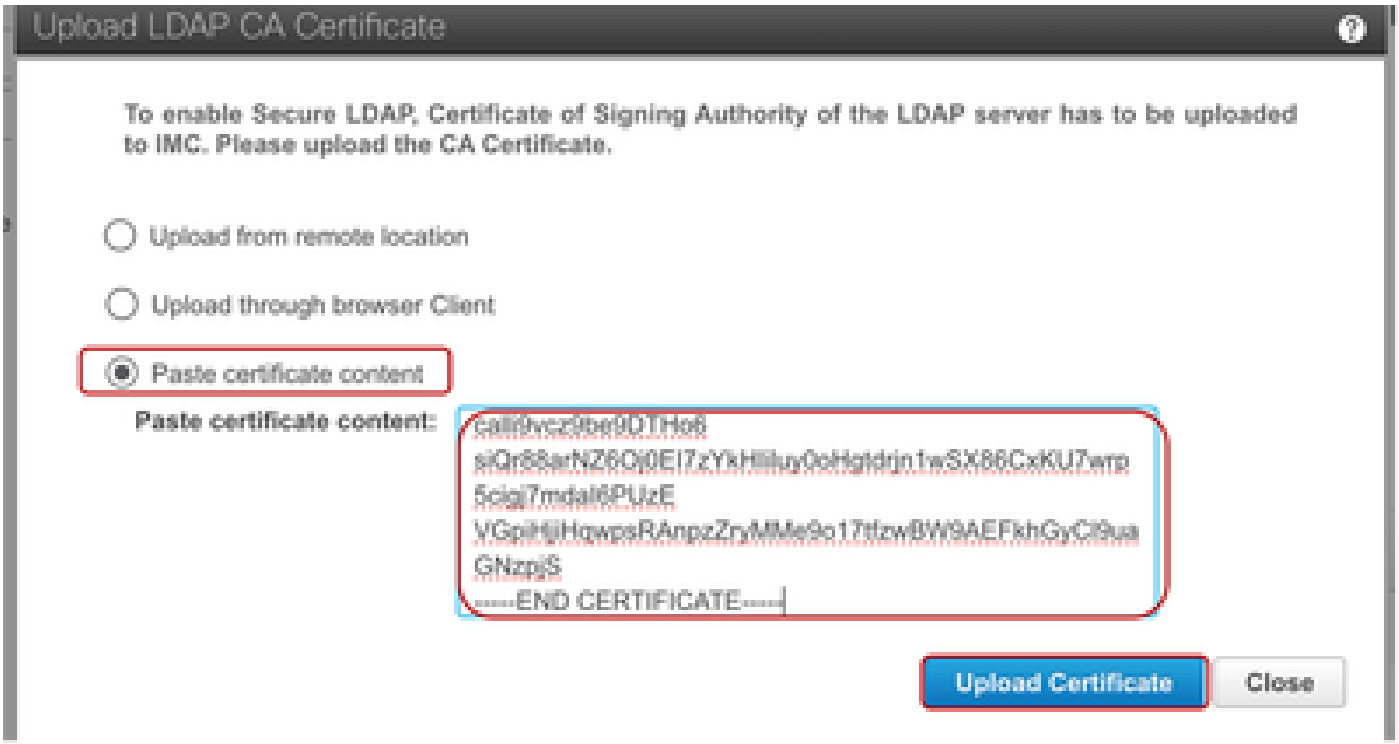
En la ventana emergente, seleccione la opción Pegar contenido del certificado.

Para esta demostración, se utiliza un certificado autofirmado, generado a partir de la instancia de Windows Server que ejecuta Active Directory y guardado en un archivo de texto. Este certificado autofirmado también se ha concatenado con el certificado raíz del mismo servidor para formar una cadena de certificados.

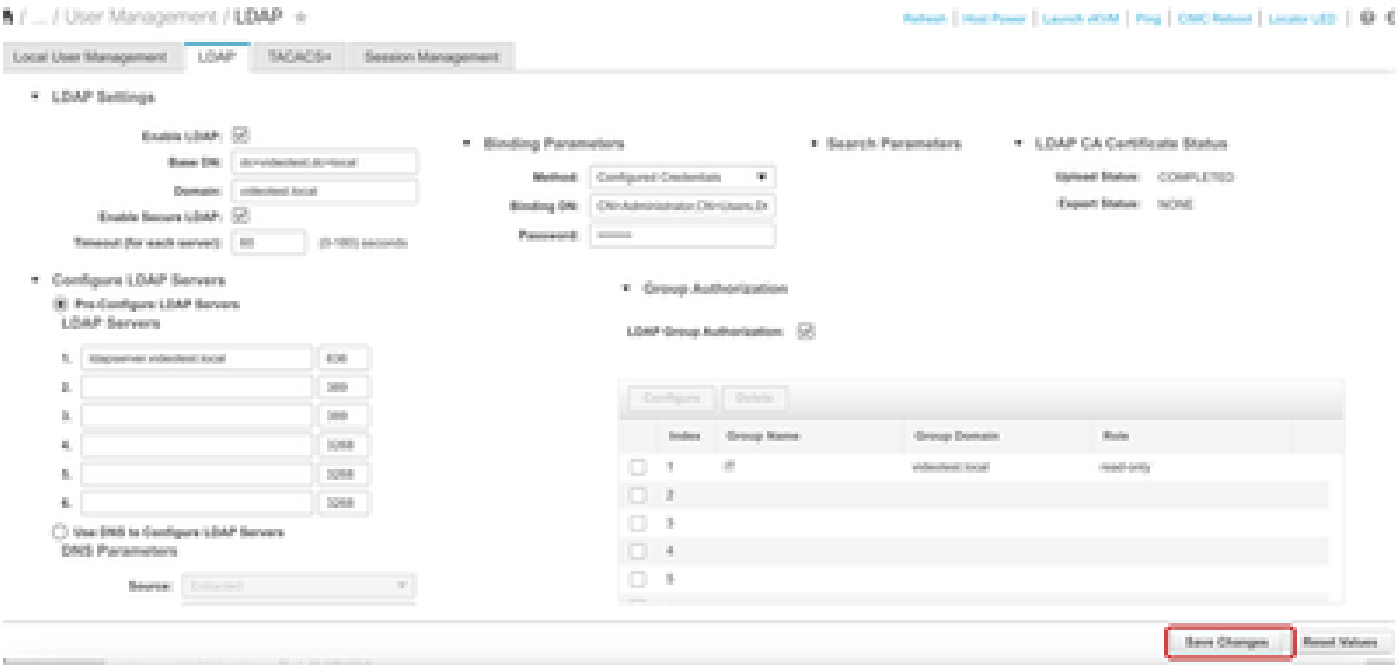


Nota: Tenga en cuenta que todo el contenido del archivo X.509 (CER) codificado en Base64 a partir del -----BEGIN CERTIFICATE----- hasta el -----END CERTIFICATE----- debe copiarse; a continuación, inmediatamente en la línea siguiente, debe ser el siguiente certificado a partir del -----BEGIN CERTIFICATE----- hasta el -----END CERTIFICATE----- en los casos en que se utilicen varios certificados.

Pegue el contenido copiado en el campo Paste Certificate Content y haga clic en Upload Certificate.



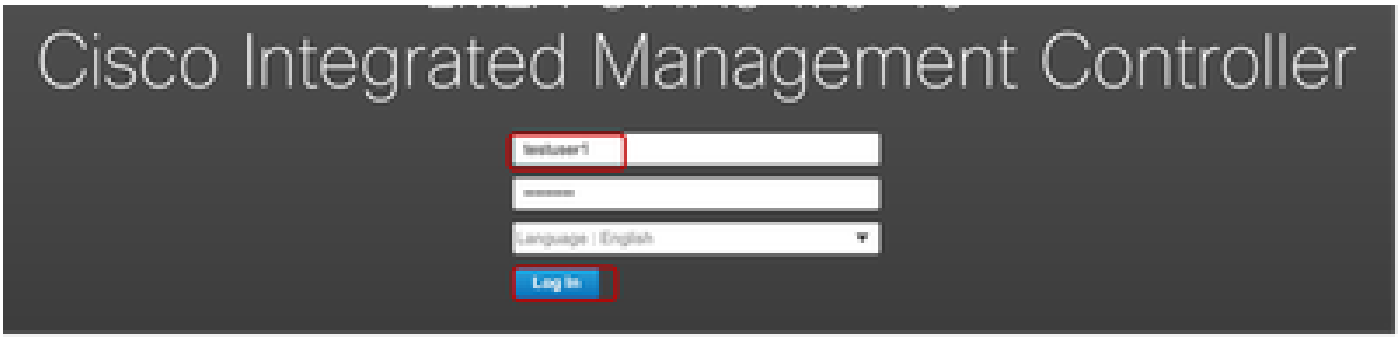
El resto de las configuraciones en LDAP seguro permanecen igual que la configuración LDAP estándar para servidores de la serie C; por lo tanto, haga clic en Guardar cambios en la página de configuración LDAP general.



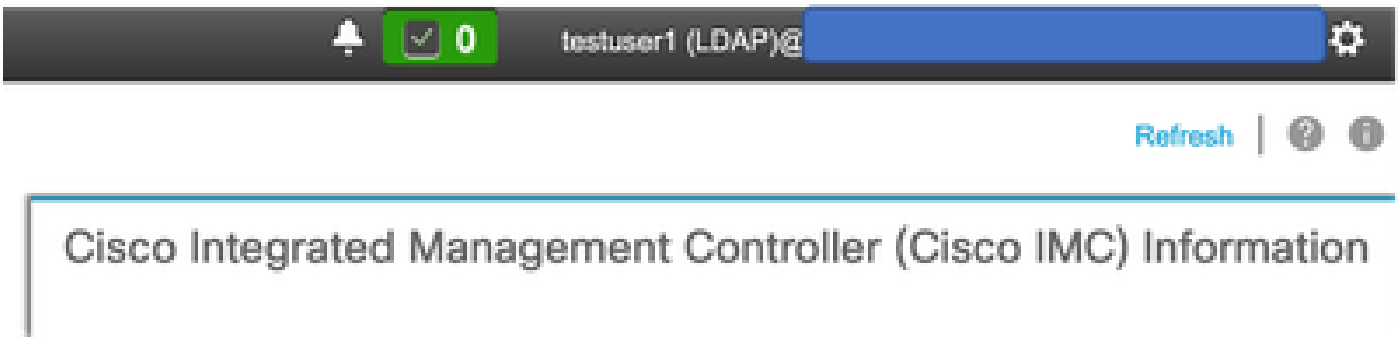
Ahora LDAP seguro se ha configurado correctamente en el servidor de la serie C de UCS.

Verificación

Para comprobarlo, intente iniciar sesión en el servidor de la serie C de UCS mediante una de las cuentas de usuario configuradas en Active Directory. Seleccione su dominio y continúe para iniciar sesión.



El inicio de sesión del usuario de prueba 1 se ha realizado correctamente en LDAP seguro



Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).