

Konfigurieren von sicherem LDAP auf Servern der UCS C-Serie

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfiguration auf der Seite der UCS Server der C-Serie](#)

[Verifizierung](#)

Einleitung

In diesem Dokument wird die Konfiguration von SecureLDAP auf Servern der C-Serie beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundlegende Informationen zum Cisco UCS und CIMC.

Verwendete Komponenten

- Cisco UCS Server der C-Serie im Standalone-Modus

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Das Beispiel in diesem Leitfaden veranschaulicht die sichere LDAP-Konfiguration auf UCS-Servern der C-Serie:

- Richten Sie einen DNS-Server ein, und verwenden Sie Domännennamen für den LDAP-Server anstelle einer IP-Adresse auf dem UCS-Server. Stellen Sie sicher, dass die

entsprechenden A-Datensätze so konfiguriert wurden, dass sie auf den LDAP-Server und die IP-Adressen der UCS Server der C-Serie verweisen.

- Konfigurieren Sie Windows-Zertifikatdienste auf dem LDAP-Server, und aktivieren Sie die Zertifikatgenerierung für die sichere LDAP-Kommunikation. Die generierten Zertifikate (Root und Intermediate) werden auf den Server der UCS C-Serie hochgeladen.

Konfiguration auf der Seite der UCS Server der C-Serie

Um den UCS Server der C-Serie für die Interaktion mit einem vorkonfigurierten DNS-Server zu konfigurieren, rufen Sie die CIMC-Schnittstelle des UCS-Servers auf, und klicken Sie dann auf das Navigationssymbol oben links.



Server Properties

Product Name:

Serial Number:

PID:

UUID:

BIOS Version:

Description:

Asset Tag:

Unknown

Navigieren Sie zu Admin, und wählen Sie Networking aus.

Chassis



Compute

Networking



Storage



Admin



User Management

Networking

Communication Services

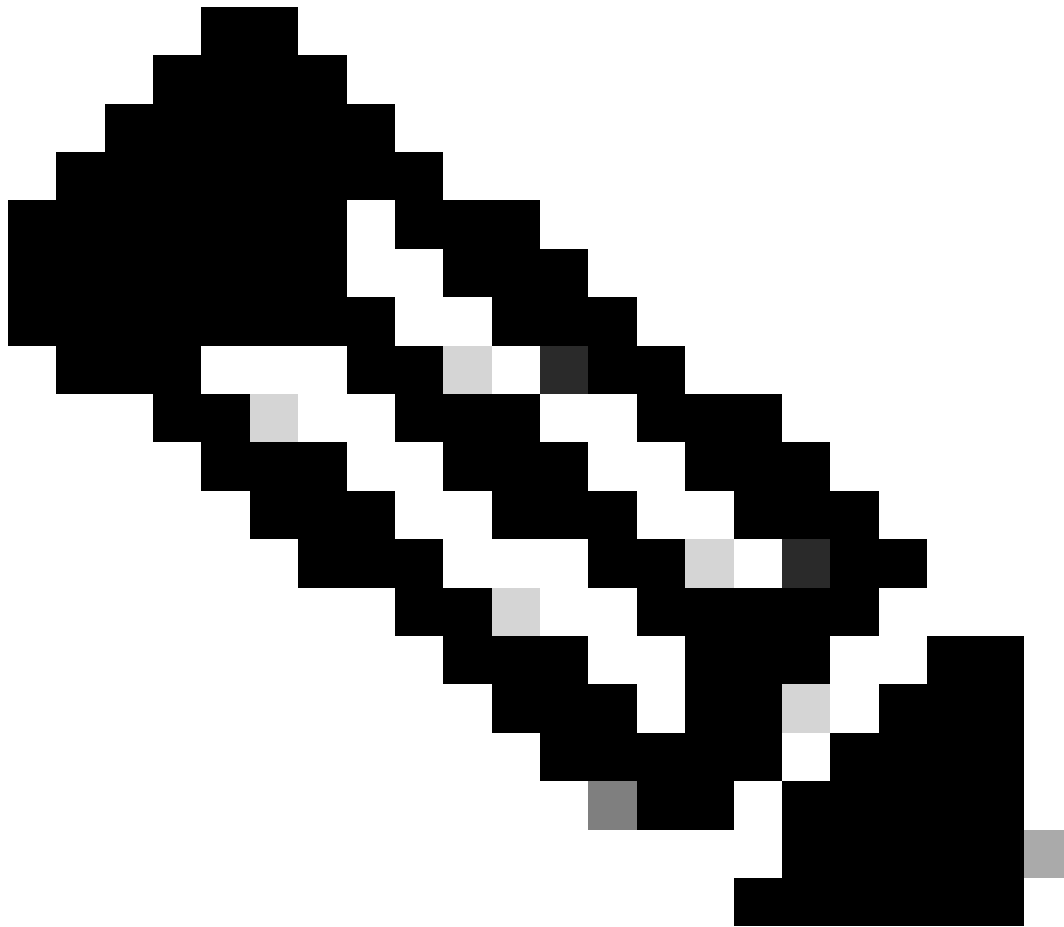
die Parameter BaseDN, Domain, Timeout und Bind in Übereinstimmung mit den standardmäßigen LDAP-Konfigurationsverfahren.

Aktivieren Sie dann das Kontrollkästchen Sicheres LDAP aktivieren.

The screenshot displays the 'LDAP' configuration tab within a management console. At the top, there are four tabs: 'Local User Management', 'LDAP' (selected), 'TACACS+', and 'Session Management'. The 'Enable LDAP' checkbox is checked. Below it, the 'Base DN' is set to 'dc=videotest,dc=local' and the 'Domain' is 'videotest.local'. The 'Enable Secure LDAP' checkbox is checked and highlighted with a red square. The 'Timeout (for each server)' is set to '60' seconds. To the right, the 'Binding Parameters' section is expanded, showing 'Method' as 'Configured Credentials', 'Binding DN' as 'CN=Administrator,CN=Users,DC=videotest,DC=local', and 'Password' as a masked field.

Wählen Sie im Popup-Fenster die Option Zertifikatsinhalt einfügen.

Für diese Demonstration wird ein selbstsigniertes Zertifikat verwendet, das von der Windows Server-Instanz mit Active Directory generiert und in einer Textdatei gespeichert wird. Dieses selbstsignierte Zertifikat wurde außerdem mit dem Stammzertifikat desselben Servers verknüpft, um eine Zertifikatskette zu bilden.



Anmerkung: Beachten Sie, dass der gesamte Inhalt der Base64-codierten X.509 (CER)-Datei, beginnend mit dem -----BEGIN CERTIFICATE----- bis zum -----END CERTIFICATE-----, kopiert werden muss, dann sofort in der nächsten Zeile, das nächste Zertifikat sein muss, beginnend mit dem -----BEGIN CERTIFICATE----- bis zum -----END CERTIFICATE-----, wenn mehrere -Zertifikate verwendet werden.

Fügen Sie den kopierten Inhalt in das Feld Zertifikatsinhalt einfügen ein, und klicken Sie auf Zertifikat hochladen.

Upload LDAP CA Certificate

To enable Secure LDAP, Certificate of Signing Authority of the LDAP server has to be uploaded to IMC. Please upload the CA Certificate.

☐ Upload from remote location
☐ Upload through browser Client
☒ Paste certificate content

Paste certificate content:

```

caBihvcc9bn0DTHo8
siQr88arNZ6Oj0E17zYkHilky0oHgtdrjn1wSX86CxKU7wP
5cig7mdal8PUzE
VGpHhHowpsRAnpzZnyMMe9o17tzwBW9AEFkhGyC9ua
GNzpjS
-----END CERTIFICATE-----

```

Upload Certificate

Close

Alle anderen Einstellungen in Secure LDAP bleiben mit der LDAP-Standardkonfiguration für Server der C-Serie identisch. Klicken Sie daher auf der allgemeinen LDAP-Konfigurationsseite auf Save Changes (Änderungen speichern).

User Management / LDAP

Refresh

Help

Launch WSM

Prog

CMC Refresh

Locate USB

Local User Management

LDAP

TACACS+

Session Management

LDAP Settings

Enable LDAP

Base DN

Domain

Enable Secure LDAP

Timeout (for each server)

Binding Parameters

Method

Binding DN

Password

Search Parameters

LDAP CA Certificate Status

Upload Status

Export Status

Configure LDAP Servers

Pre-Configure LDAP Servers

LDAP Servers

Use DNS to Configure LDAP Servers

Source

Group Authorization

LDAP Group Authorization

Configure

Delete

Index	Group Name	Group Domain	Role
☐ 1	IT	selected.local	read-only
☐ 2			
☐ 3			
☐ 4			
☐ 5			

Save Changes

Reset Values

Sicheres LDAP wurde jetzt erfolgreich auf dem UCS Server der C-Serie konfiguriert.

Verifizierung

Versuchen Sie, sich mit einem der konfigurierten Benutzerkonten in Active Directory beim UCS-Server der C-Serie anzumelden. Wählen Sie Ihre Domäne aus, und fahren Sie mit der Anmeldung fort.

Cisco Integrated Management Controller

testuser1

Language | English

Log In

Anmeldung von Testbenutzer1 über sicheres LDAP erfolgreich



testuser1 (LDAP)@



[Refresh](#)



Cisco Integrated Management Controller (Cisco IMC) Information

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.