ユーザ アカウントの管理

この章は、次の項で構成されています。

- ローカル ユーザの設定 （1 ページ）
- 非 IPMI ユーザー モード （4 ページ）
- 強力なパスワードの無効化 （6 ページ）
- パスワードの有効期限切れ （7 ページ）
- ユーザ パスワードのリセット （8 ページ）
- ユーザに対するパスワード期限切れの設定 （9 ページ）
- LDAP サーバ （10 ページ）
- LDAP サーバの設定 （11 ページ）
- Cisco IMC での LDAP の設定 （12 ページ）
- Cisco IMC での LDAP グループの設定 （14 ページ）
- LDAP グループでのネストされたグループの検索深度の設定 （16 ページ）
- LDAP 証明書の概要 （17 ページ）
- ユーザ検索の優先順位の設定 （23 ページ）
- ユーザ セッションの表示 （24 ページ）
- ユーザ セッションの終了 （25 ページ）

ローカル ユーザの設定

始める前に

ローカルユーザアカウントを設定または変更するには、admin権限を持つユーザとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope user** *usernumber*	ユーザ番号 *usernumber* に対するユーザ コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	Server /user # **set enabled** {**yes** |**no**\\	Cisco IMC でユーザアカウントをイネーブルまたはディセーブルにします。
ステップ 3	Server /user # **set name** *username*	ユーザのユーザ名を指定します。
ステップ 4	Server /user # **set password**	パスワードを2回入力するように求められます。 （注） 強力なパスワードを有効にすると、ガイドラインに従ってパスワードを設定する必要があります。 • パスワードは 8 ～ 14 文字とすること。 • パスワードにユーザ名を含めないこと。 • パスワードには次の 4 つのカテゴリの中から 3 つに該当する文字を含めること。 • 大文字の英字（A ～ Z） • 小文字の英字（a ～ z） • 10 進数の数字（0 ～ 9） • アルファベット以外の文字（!、@、#、$、%、^、&、*、 強力なパスワードを無効にすると、1 ～ 20 文字の範囲で任意の文字（英数字、特殊文字または整数）を使用してパスワードを設定できます。

	コマンドまたはアクション	目的
ステップ 5	Server /user # **set role** {**readonly** |**user** |**admin**\\\	ユーザに割り当てるロールを指定します。ロールには、次のものがあります。 • readonly：このユーザは情報を表示できますが、変更することはできません。 • user：このユーザは、次の操作を実行できます。 • すべての情報を表示する • 電源のオン、電源再投入、電源のオフなどの電力制御オプションを管理する • KVM コンソールと仮想メディアを起動する • すべてのログをクリアする • ロケータ LED を切り替える • タイム ゾーンを設定する • IP アドレスを ping する • admin：このユーザは、GUI、CLI、IPMI で可能なすべての処理を実行できます。
ステップ 6	Server /user # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、ユーザ 5 を admin として設定する例を示します。

```
Server# scope user 5
Server /user # set enabled yes
Server /user *# set name john
Server /user *# set password
Warning:
Strong Password Policy is enabled!

For CIMC protection your password must meet the following requirements:
        The password must have a minimum of 8 and a maximum of 14 characters.
        The password must not contain the User's Name.
       The password must contain characters from three of the following four categories.

            English uppercase characters (A through Z)
```

```
            English lowercase characters (a through z)
            Base 10 digits (0 through 9)
Please enter password:
Please confirm password:
Server /user *# set role readonly
Server /user *# commit
Server /user #  show
User   Name             Role     Enabled
------ ---------------- -------- --------
5      john             readonly yes
```

非 IPMI ユーザー モード

リリース4.1 では、IPMI と非 IPMI の両方のユーザー モードを切り替えることができる**ユーザー モード**と呼ばれる新しいユーザー設定オプションが導入されています。非 IPMI ユーザー モードの導入では、ユーザー向けに強化されたパスワードセキュリティと、IPMI 2.0 標準による制約により以前のリリースで制限された BMC データベースに対してセキュリティ強化を提供します。非 IPMI ユーザー モードでは、127 文字を使用してユーザー パスワードを設定できますが、IPMI モードのユーザーはパスワードの長さが 20 文字に制限されます。非 IPMI ユーザー モードでは、このモードで設定されたユーザーに対してより強力なパスワードを設定できます。

次の場合に、ユーザー モードの切り替え中に発生する次の設定変更を考慮する必要があります。

- 非 IPMI モードに切り替えると、IPMI 経由の IPMI はサポートされません。
- 非 IPMI から IPMI モードに切り替えて、すべてのローカル ユーザーを削除し、ユーザー クレデンシャルをデフォルトのユーザー名とパスワードに戻します。続いてログインすると、デフォルトのパスワードを変更するように求められます。

  IPMI から非 IPMI モードに切り替えた場合、ユーザー データは影響を受けません。
- ファームウェアを 4.1 よりも低いバージョンにダウングレードします。ユーザー モードが非 IPMI の場合、はすべてのローカル ユーザーを削除し、ユーザー クレデンシャルをデフォルトのユーザー名とパスワードに戻します。続いてログインすると、デフォルトのパスワードを変更するように求められます。

（注） 工場出荷時の初期状態にリセットすると、ユーザー モードは IPMI モードに戻ります。

IPMI から非 IPMI へのユーザー モードの切り替え

始める前に

このアクションを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope user-policy**	ユーザ ポリシー コマンド モードを開始します。
ステップ 2	Server /user-policy # **scope user-mode**	ユーザー ポリシー コマンド モードを開始します。
ステップ 3	Server /user-policy/user-mode # **set user-mode non-ipmi**	IPMI 以外のユーザー モードに切り替えるには、確認プロンプトで y を入力します。
ステップ 4	Server /user-policy/user-mode * # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 5	Server /user-policy/user-mode # **show detail**	ユーザー モードを表示します。

例

次に、強力なパスワードを無効にする例を示します。

```
Server# scope user-policy
Server /user-policy # scope user-mode
Server /user-policy/user-mode # set user-mode non-ipmi
Server /user-policy/user-mode *# commit
Warning: This will enable NON-IPMI based user mode.
         Converting to Non-IPMI User Mode disables IPMI Services and removes IPMI user
support.
         SSH, KVM, Webserver, XMAPI and Redfish sessions will be disconnected.
Do you wish to continue? [y/N] y
Connection to 10.10.10.10 closed by remote host.
Connection to 10.10.10.10 closed.
Server /user-policy/user-mode # show detail
User Mode:
    User mode for IPMI accessibility: non-ipmi
Server /user-policy/user-mode #
```

非 IPMI から IPMI へのユーザー モードの切り替え

始める前に

このアクションを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope user-policy**	ユーザ ポリシー コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	Server /user-policy # **scope user-mode**	ユーザー ポリシー コマンド モードを開始します。
ステップ 3	Server /user-policy/user-mode # **set user-mode ipmi**	IPMI ユーザー モードに切り替えるには、確認プロンプトでyを入力します。 （注） IPMIユーザーモードに切り替えると、すべてのUCSユーザーが削除され、デフォルトのユーザー名とパスワードに戻ります。
ステップ 4	Server /user-policy/user-mode * # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 5	Server /user-policy/user-mode # **show detail**	ユーザー モードを表示します。

例

次に、強力なパスワードを無効にする例を示します。

```
Server# scope user-policy
Server /user-policy # scope user-mode
Server /user-policy/user-mode # set user-mode ipmi
Server /user-policy/user-mode *# commit
Warning: This will enable IPMI based user mode.
         Converting to IPMI User Mode deletes all UCS users and reverts to default
userid/password.
         SSH, KVM, Webserver, XMAPI and Redfish sessions will be disconnected.
Do you wish to continue? [y/N] y
Connection to 10.10.10.10 closed by remote host.
Connection to 10.10.10.10 closed.
Server /user-policy/user-mode # show detail
User Mode:
    User mode for IPMI accessibility: ipmi
Server /user-policy/user-mode #
```

強力なパスワードの無効化

Cisco IMC では、強力なパスワード ポリシーが実装されるようになったため、サーバに最初にログインした際に、ガイドラインに従って強力なパスワードを設定するよう要求されます。Cisco IMC の CLI では、強力なパスワード ポリシーを無効にし、ガイドラインを無視して希望するパスワードを設定することができます。強力なパスワードを無効にすると、[Enable Strong Password] ボタンが表示されます。デフォルトでは、強力なパスワード ポリシーが有効になっています。

始める前に

このアクションを実行するには、admin権限を持つユーザとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope user-policy**	ユーザ ポリシー コマンド モードを開始します。
ステップ 2	Server /user-policy # **set password-policy** {**enabled** | **disabled**}	確認プロンプトで、**y** を入力してアクションを完了するか、または **n** を入力してアクションをキャンセルします。強力なパスワードを有効または無効にします。
ステップ 3	Server /user-policy # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、強力なパスワードを無効にする例を示します。

```
Server# scope user-policy
Server /user-policy # set password-policy disabled
Warning: Strong password policy is being disabled.
Do you wish to continue? [y/N] y
Server /user-policy *# commit
Server /user-policy #
```

パスワードの有効期限切れ

パスワードの有効期限を設定することができ、その期限を過ぎるとパスワードは期限切れになります。管理者として、この時間を日数で設定できます。この設定は、すべてのユーザに共通です。パスワードの期限が切れると、ユーザはログイン時に通知され、パスワードをリセットしない限りログインできなくなります。

（注） 古いデータベースにダウングレードした場合、既存のユーザが削除されます。データベースはデフォルト設定に戻ります。以前に設定されたユーザは消去され、データベースは空になります。つまり、データベースのユーザ名はデフォルトの「admin」、パスワードは「password」となります。サーバにはデフォルトのユーザデータベースが残っているため、デフォルトのクレデンシャルの変更機能が有効になっています。これは、ダウングレード後に「admin」ユーザがデータベースに初めてログインする際に、そのユーザはデフォルトのクレデンシャルを強制的に変更する必要があることを意味します。

パスワード設定時刻

「パスワード設定時刻」は、すべての既存ユーザに対し、移行またはアップグレードが発生した時刻に設定されています。新規ユーザ（アップグレード後に作成されたユーザ）の場合、パスワード設定時刻は、ユーザが作成され、パスワードが設定された時刻に設定されます。一般ユーザ（新規および既存）の場合、パスワード設定時刻は、パスワードが変更されるたびに更新されます。

ユーザ パスワードのリセット

[パスワードの変更（Change Password）] オプションを使用してパスワードを変更できます。

（注）
- このオプションは、admin としてログインしているときには使用できません。読み取り専用の権限をもつ設定済みのユーザのパスワードだけが変更できます。
- パスワードを変更すると、Cisco IMC からログアウトされます。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope user** *user ID*	選択したユーザ コマンド モードを開始します。
ステップ 2	Server /chassis/user # **set password**	パスワードの要件の指示を読み、現在のパスワード、新しいパスワード、パスワードの確認をそれぞれのプロンプトで入力します。
ステップ 3	Server /chassis/user * # **commit**	トランザクションをシステムの設定にコミットします。

例

この例では、設定されているユーザのパスワードを変更する方法を示します。

```
Server # scope user 2
Server /chassis/user # set password
Warning:
Strong Password Policy is enabled!
For CIMC protection your password must meet the following requirements:
      The password must have a minimum of 8 and a maximum of 20 characters.
       The password must not contain the User's Name.
       The password must contain characters from three of the following four categories.

            English uppercase characters (A through Z)
            English lowercase characters (a through z)
```

```
            Base 10 digits (0 through 9)
            Non-alphabetic characters (!, @, #, $, %, ^, &, *, -, _, +, =)
Please enter current password:Testabcd1
Please enter password: Testabcd2
Please confirm password: Testabcd2
Server /chassis/user * # commit
Server /chassis/user #
```

ユーザに対するパスワード期限切れの設定

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope user-policy**	ユーザ ポリシー コマンド モードを開始します。
ステップ 2	Server /user-policy # **scope password-expiration**	パスワードの有効期限コマンド モードを開始します。
ステップ 3	Server /user-policy/password-expiration # **set password-expiry-duration** *0 ～ 3650* の整数	既存のパスワードに設定できる有効期間（その時間以後、新しいパスワードを設定するか、または既存のパスワードを変更します。）範囲は 0 ～ 3650 日です。0 を入力すると、このオプションが無効になります。
ステップ 4	Server /user-policy/password-expiration * # **set notification-period** *0 ～ 15* の整数	パスワードの期限が切れる時間を通知します。0～15 日の間の値を入力します。0 を入力すると、このオプションが無効になります。
ステップ 5	Server /user-policy/password-expiration * # **set grace-period** *0 ～ 5* の整数	既存のパスワードをまだ使用できる期間。この期間の後、パスワードは期限切れになります。0 ～ 5 日の間の値を入力します。0 を入力すると、このオプションが無効になります。
ステップ 6	Server /user-policy/password-expiration * # **set password-history** *0 ～ 5* の整数	パスワードが入力された回数。これを有効にすると、パスワードを繰り返すことができません。0 ～ 5 の間の値を入力します。0 を入力すると、このオプションが無効になります。
ステップ 7	Server /user-policy/password-expiration *# **commit**	トランザクションをコミットします。

	コマンドまたはアクション	目的
ステップ 8	（任意） Server /user-policy/password-expiration # **show detail**	パスワードの有効期限の詳細を表示します。
ステップ 9	（任意） Server /user-policy/password-expiration # **restore**	確認のプロンプトで、**yes** と入力してパスワード有効期限の設定をデフォルト値に復元します。

例

この例では、パスワードの有効期限を設定し、設定をデフォルト値に戻します。

```
Server # scope user-policy
Server /user-policy # scope password-expiration
Server /user-policy/password-expiration # set password-expiry-duration 5
Server /user-policy/password-expiration * # set notification-period 2
Server /user-policy/password-expiration *# set grace-period 1
Server /user-policy/password-expiration *# set password-history 4
Server /user-policy/password-expiration *# commit
Server /user-policy/password-expiration # show detail
Password expiration parameters:
 Valid password duration: 5
 Number of stored old passwords: 4
 Notification period: 2
 Grace period: 1
Server /user-policy/password-expiration #
Restoring the password expiry parameters to default values:
Server /user-policy/password-expiration # restoreAre you sure you want to restore
User password expiration parameters to defaults?
Please enter 'yes' to confirm:yes
Server /user-policy/password-expiration #
```

LDAP サーバ

Cisco IMC は、ディレクトリ内の情報を整理し、この情報へのアクセスを管理するディレクトリ サービスをサポートしています。Cisco IMC は、Lightweight Directory Access Protocol（LDAP）をサポートしています。これは、ネットワークでのディレクトリ情報を保存し維持するものです。さらに、Cisco IMC は Microsoft Active Directory（AD）もサポートします。Active Directory はさまざまなネットワーク サービスを提供するテクノロジーであり、LDAP と同様のディレクトリ サービス、Kerberos ベースの認証、DNS ベースの名前付けなどが含まれます。Cisco IMC は LDAP での Kerberos ベースの認証サービスを利用します。

Cisco IMC で LDAP が有効になっている場合、ローカル ユーザ データベース内に見つからないユーザ アカウントに関するユーザ認証とロール許可は、LDAP サーバによって実行されます。LDAP ユーザ認証の形式は username@domain.com です。

サーバの Active Directory 設定で暗号化をイネーブルにすることで、LDAP サーバへの送信データを暗号化するようサーバに要求できます。

LDAP サーバの設定

ユーザ認証および権限付与のためにLDAPを使用するよう、CiscoIMCを設定できます。LDAPを使用するには、Cisco IMC に関するユーザ ロール情報とロケール情報を保持する属性を使ってユーザを設定します。Cisco IMC のユーザ ロールとロケールにマップされた既存の LDAP 属性を使用できます。または、LDAP スキーマを変更して、属性 ID 1.3.6.1.4.1.9.287247.1 を持つ CiscoAVPair 属性などの新しいカスタム属性を追加できます。

重要 スキーマの変更の詳細については、http://technet.microsoft.com/en-us/library/bb727064.aspx の記事を参照してください。

（注） この例では CiscoAVPair という名前のカスタム属性を作成しますが、Cisco IMC のユーザ ロールとロケールにマップされた既存の LDAP 属性を使用することもできます。

Cisco IMC の LDAP 設定でグループ認証を使用している場合、手順 1 ~ 4 をスキップし、*Cisco IMC で LDAP 設定とグループ認証の構成*のセクションに記載されている手順を実行します。

LDAP サーバに対して次の手順を実行する必要があります。

手順

ステップ 1 LDAP スキーマ スナップインがインストールされていることを確認します。

ステップ 2 スキーマ スナップインを使用して、次のプロパティを持つ新しい属性を追加します。

プロパティ	値
Common Name	**CiscoAVPair**
LDAP Display Name	**CiscoAVPair**
Unique X500 Object ID	**1.3.6.1.4.1.9.287247.1**
Description	**CiscoAVPair**
Syntax	**Case Sensitive String**

ステップ 3 スナップインを使用して、ユーザ クラスに CiscoAVPair 属性を追加します。

a) 左ペインで [Classes] ノードを展開し、**u** を入力してユーザ クラスを選択します。

b) [Attributes] タブをクリックして、[Add] をクリックします。

c) **c** を入力して CiscoAVPair 属性を選択します。

d) [OK] をクリックします。

ステップ 4 Cisco IMC にアクセスできるようにするユーザに対し、次のユーザ ロール値を CiscoAVPair 属性に追加します。

ロール	CiscoAVPair 属性値
admin	`shell:roles="admin"`
user	`shell:roles="user"`
read-only	`shell:roles="read-only"`

（注） 属性に値を追加する方法の詳細については、http://technet.microsoft.com/en-us/library/bb727064.aspx の記事を参照してください。

次のタスク

Cisco IMC を使用して LDAP サーバを設定します。

Cisco IMC での LDAP の設定

ローカル ユーザの認証と許可に LDAP サーバを使用するには、Cisco IMC で LDAP を設定します。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ldap**	LDAP コマンド モードを開始します。
ステップ 2	Server /ldap # **set enabled** {**yes** |**no**\\	LDAP セキュリティをイネーブルまたはディセーブルにします。LDAPセキュリティがイネーブルの場合、ローカル ユーザ データベースにないユーザ アカウントに対し、ユーザ認証とロール許可が LDAP によって実行されます。
ステップ 3	Server /ldap # **set domain***LDAP* ドメイン名	LDAP ドメイン名を指定します。
ステップ 4	Server /ldap # **set timeout** *seconds*	LDAP 検索操作がタイムアウトするまで Cisco IMC が待機する秒数を指定し

	コマンドまたはアクション	目的
		ます。0 ～ 1800 秒の間隔を指定する必要があります。
ステップ 5	Server /ldap # **set encrypted** {**yes** |**no**\\	暗号化がイネーブルである場合、サーバは AD に送信されるすべての情報を暗号化します。
ステップ 6	Server /ldap # **set base-dn** *domain-name*	LDAP サーバで検索するベース DN を指定します。
ステップ 7	Server /ldap # **set attribute** 名	ユーザのロールとロケール情報を保持する LDAP 属性を指定します。このプロパティは、常に、名前と値のペアで指定されます。システムは、ユーザ レコードで、この属性名と一致する値を検索します。 Cisco IMC ユーザのロールおよびロケールにマップされた既存の LDAP 属性を使用するか、CiscoAVPair 属性など、次の属性 ID を持つカスタム属性を作成できます。 `1.3.6.1.4.1.9.287247.1` （注） このプロパティを指定しない場合、ユーザアクセスが拒否されます。
ステップ 8	Server /ldap # **set filter-attribute**	アカウント名属性を指定します。Active Directory を使用している場合は、このフィールドに **sAMAccountName** を指定します。
ステップ 9	Server /ldap # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 10	Server /ldap # **show** [**detail**]	（任意）LDAP の設定を表示します。

例

次に、CiscoAVPair 属性を使用して LDAP を設定する例を示します。

```
Server# scope ldap
Server /ldap # set enabled yes
Server /ldap *# set domain sample-domain
Server /ldap *# set timeout 60
```

```
Server /ldap *# set encrypted yes
Server /ldap *# set base-dn example.com
Server /ldap *# set attribute CiscoAVPair
Server /ldap *# set filter-attribute sAMAccountName
Server /ldap *# commit
Server /ldap # show detail
LDAP Settings:
    Enabled: yes
    Encrypted: yes
    Domain: sample-domain
    BaseDN: example.com
    Timeout: 60
    Filter-Attribute: sAMAccountName
    Attribute: CiscoAvPair
Server /ldap #
```

次のタスク

グループ許可用にLDAPグループを使用する場合は、「*Cisco IMC* での *LDAP* グループの設定」を参照してください。

Cisco IMC での LDAP グループの設定

（注） Active Directory（AD）グループ許可をイネーブルにして設定すると、ローカル ユーザ データベースにないユーザや、Active Directory で Cisco IMC の使用を許可されていないユーザに対するグループ レベルでのユーザ認証も行われます。

始める前に

- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。
- Active Directory（または LDAP）をイネーブルにして、設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ldap**	LDAP コマンド モードを開始して、AD を設定します。
ステップ 2	Server /ldap# **scope ldap-group-rule**	LDAP グループ ルール コマンド モードを開始して、AD を設定します。
ステップ 3	Server /ldap/ldap-group-rule # **set group-auth** {**yes** |**no**}	LDAP グループ許可をイネーブルまたはディセーブルにします。

	コマンドまたはアクション	目的
ステップ 4	Server /ldap # **scope role-group** *index*	設定に使用可能なグループ プロファイルのいずれかを選択します。ここで、*index* は 1 から 28 までの数字です。
ステップ 5	Server /ldap/role-group # **set name** *group-name*	サーバへのアクセスが許可されているグループの名前を AD データベースに指定します。
ステップ 6	Server /ldap/role-group # **set domain** *domain-name*	グループが存在する必要がある AD ドメインを指定します。

ステップ 7	Server /ldap/role-group # **set role** {**admin** | **user** | **readonly**}	この AD グループのすべてのユーザに割り当てられる権限レベル（ロール）を指定します。次のいずれかになります。
		• **admin**：ユーザは使用可能なすべてのアクションを実行できます。
		• **user**：ユーザは、次のタスクを実行できます。
		  • すべての情報を表示する
		  • 電源のオン、電源再投入、電源のオフなどの電力制御オプションを管理する
		  • KVM コンソールと仮想メディアを起動する
		  • すべてのログをクリアする
		  • ロケータ LED を切り替える
		• **readonly**：ユーザは情報を表示できますが、変更することはできません。

ステップ 8	Server /ldap/role-group # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、LDAP グループの許可を設定する例を示します。

```
Server# scope ldap
Server /ldap # scope ldap-group-rule
Server /ldap/ldap-group-rule # set group-auth yes
```

```
Server /ldap *# scope role-group 5
Server /ldap/role-group # set name Training
Server /ldap/role-group* # set domain example.com
Server /ldap/role-group* # set role readonly
Server /ldap/role-group* # commit
ucs-c250-M2 /ldap # show role-group
Group  Group Name       Domain Name      Assigned Role
------ -----------     --------------   --------------
1      (n/a)            (n/a)            admin
2      (n/a)            (n/a)            user
3      (n/a)            (n/a)            readonly
4      (n/a)            (n/a)            (n/a)
5      Training         example.com      readonly

Server /ldap/role-group #
```

LDAPグループでのネストされたグループの検索深度の設定

LDAP グループ マップで別の定義済みグループ内にネストされた LDAP グループを検索することができます。

- このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。
- Active Directory（または LDAP）をイネーブルにして、設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ldap**	LDAP コマンド モードを開始して、AD を設定します。
ステップ 2	Server /ldap# **scope ldap-group-rule**	LDAP グループ ルール コマンド モードを開始して、AD を設定します。
ステップ 3	Server /ldap/ldap-group-rule # **set group-search-depth** *value*	ネストされた LDAP グループの検索を有効にします。
ステップ 4	Server /ldap/role-group-rule # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、別の定義済みのグループ内にネストされた LDAP グループの検索を実行するために検索する例を示します。

```
Server# scope ldap
Server /ldap # scope ldap-group-rule
```

```
Server /ldap/ldap-group-rule # set group-search-depth 10
Server /ldap/role-group-rule* # commit
Server /ldap/role-group-rule # show detail
Group rules for LDAP:
    Group search attribute: memberOf
    Enable Group Authorization: yes
    Nested group search depth: 10
Server/ldap/ldap-group-rule #
```

LDAP 証明書の概要

Cisco C シリーズ サーバでは、LDAP バインディング ステップ時に、LDAP クライアントがインストール済み CA 証明書またはチェーン CA 証明書に対してディレクトリ サーバ証明書を検証できるようになっています。リモートユーザ認証のために信頼されたポイントまたはチェーン証明書を Cisco IMC に入力できないことにより、誰でもユーザ認証用のディレクトリ サーバを複製してセキュリティ違反が発生する恐れがある場合は、この機能を導入します。

暗号化された TLS/SSL 通信中にディレクトリ サーバ証明書を検証するには、LDAP クライアントに新しい設定オプションが必要です。

LDAP CA 証明書のエクスポート

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ldap**	LDAP コマンド モードを開始します。
ステップ 2	Server# /ldap **scope binding-certificate**	LDAP CA 証明書バインド コマンド モードを開始します。
ステップ 3	Server /ldap/binding-certificate # **export-ca-certificate** *remote-protocol IP アドレス LDAP CA 証明書ファイル*	リモート サーバに接続するためのプロトコルを指定します。次のいずれかのタイプを指定できます。 • TFTP • FTP • SFTP • SCP • HTTP

	コマンドまたはアクション	目的
		（注） Cisco UCS C シリーズ サーバでは、リモート サーバからファームウェアを更新したときの、サーバのフィンガープリントの確認をサポートするようになりました。このオプションは、リモート サーバ タイプとして SCP または SFTP を選択した場合にのみ使用できます。 このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?」というメッセージが表示されます。サーバ フィンガープリントの信頼性に応じて、[y] または [n] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。 証明書のエクスポートを開始します。

例

この例では、LDAP 証明書をエクスポートします。

```
Server # scope ldap
Server /ldap # scope binding-certificate
Server /ldap/binding-certificate #  export-ca-certificate tftp 172.22.141.66 test.csv
 Initiating Export
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1262    0     0  100  1262      0   1244  0:00:01  0:00:01 --:--:--  1653
100  1262    0     0  100  1262      0   1237  0:00:01  0:00:01 --:--:--  1237
LDAP CA Certificate is exported successfully
Server /ldap/binding-certificate #
```

コンテンツのコピーによる LDAP CA 証明書の内容のダウンロード

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ldap**	LDAP コマンド モードを開始します。
ステップ 2	Server# /ldap **scope binding-certificate**	LDAP CA 証明書バインド コマンド モードを開始します。
ステップ 3	Server# /ldap/binding-certificate **set enabled** {**yes** | **no**}	LDAP CA 証明書のバインドを有効または無効にします。
ステップ 4	Server /ldap/binding-certificate* # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 5	Server /ldap/binding-certificate # **paste-ca-certificate**	証明書の内容を貼り付け るよう求められます。
ステップ 6	証明書の内容を貼り付けて **CTRL+D** キーを押します。	確認のプロンプトが表示されます。
ステップ 7	確認プロンプトで、**y** と入力します。	これにより LDAP CA 証明書のダウンロードが開始されます。

例

この例では、LDAP 証明書をダウンロードします。

```
Server # scope ldap
Server /ldap # scope binding-certificate
Server /ldap/binding-certificate # set enabled yes
Server /ldap/binding-certificate *# commit
Server /ldap/binding-certificate # show detail
LDAP binding with Certificate:
    Enabled: yes
Server /ldap/binding-certificate # paste-ca-certificate
 Please paste your certificate here, when finished, press CTRL+D.
-----BEGIN CERTIFICATE-----
MIIDdzCCAl+gAwIBAgIQV06yJcJPAYNO8Cp+FYQttjANBgkqhkiG9w0BAQsFADBO
MRIwEAYKCZImiZPyLGQBGRYCaW4xGzAZBgoJkiaJk/IsZAEZFgs0T0JKUkEySkhC
UTEbMBkGA1UEAxMSV0lOLTRPQkpSQTJKSEJRLUNBMB4XDTE2MDIyNTE3MDczNloX
DTIxMDIyNTE3MTczM1owTjESMBAGCgmSJomT8ixkARkWAmluMRswGQYKCZImiZPy
LGQBGRYLNE9CSlJBMkpIQlExGzAZBgNVBAMTEldJTi00T0JKUkEySkhCUS1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMM2cdgmrPTkZe4K2zI+EbeZ
mfQnjfiUz8OIY97w8lC/2S4qK46T+fnX13rXe8vvVHAO5wgPDVQTGS4nlF46A6Ba
FK+krKcIgFrQB1gnF74qs/ln1YtKHNBjrvg5KyeWFrA7So6Mi2XEw8w/zMPL0d8T
b+LM1YnhnuXA9G8gVCJ/iUhXfMpB20L8sv30Mek7bw8x2cxJYTuJAviVIrjSwU5j
```

```
fO3WKttRuyFpeOIi00weklpF0+8D3Z9mBinoTbL2pl0U32am6wTI+8WmtJ+8W68v
jH4Y8YBY/kzMHdpwjpdZkC5pE9BcM0rL9xKoIu6X0kSNEssoGnepFyNaH3t8vnMC
AwEAAaNRME8wCwYDVR0PBAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYE
FBAUulHTAWBT1OBz8IgAEzXsfcCsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3
DQEBCwUAA4IBAQAzUMZr+0r1dWkVfFNBd7lu8tQbAEJf/A7PIKnJGNoUq8moAGs4
pMndoxdpNGZhYCWDWX3GWdeF1HqZHhb38gGQ9ylu0pIK7tgQufZmeCBH6T7Tzq/w
Dq+TMFGIjXF84xW3N665y4ePgUcUI7e/6aBGcGkGeUYodBPtExe28tQyeuYwD4Zj
nLuZKkT+I4PAYygVCqxDGsvfRHDpGneb3R+GeonOf4ED/0tn5PLSL9khb9qkHu/V
dO3/HmKVzUhloTDBuAMq/wES2WZAWhGr3hBc4nWQNjZWEMOKDpYZVK/GhBmNF+xi
eRcFqgh64oEmH9qAp0caGS1e7UyYaN+LtPRe
-----END CERTIFICATE-----
CTRL+D
  You are going to overwrite the LDAP CA Certificate.
  Are you sure you want to proceed and overwrite the LDAP CA Certificate? [y|N]
y
Server /ldap/binding-certificate #
```

リモート サーバからの LDAP CA 証明書のダウンロード

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ldap**	LDAP コマンド モードを開始します。
ステップ 2	Server# /ldap **scope binding-certificate**	LDAP CA 証明書バインド コマンド モードを開始します。
ステップ 3	Server# /ldap/binding-certificate **set enabled** {**yes** | **no**}	LDAP CA 証明書のバインドを有効または無効にします。
ステップ 4	Server /ldap/binding-certificate* # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 5	Server /ldap/binding-certificate # **download-ca-certificate** *remote-protocol IP アドレス LDAP CA 証明書ファイル*	リモート サーバに接続するためのプロトコルを指定します。次のいずれかのタイプを指定できます。 • TFTP • FTP • SFTP • SCP • HTTP

	コマンドまたはアクション	目的
		（注） Cisco UCS C シリーズ サーバでは、リモート サーバからファームウェアを更新したときの、サーバのフィンガープリントの確認をサポートするようになりました。このオプションは、リモートサーバタイプとして SCP または SFTP を選択した場合にのみ使用できます。 このアクションを実行しながら、リモートサーバタイプとして SCP または SFTP を選択した場合、「Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?」というメッセージが表示されます。サーバ フィンガープリントの信頼性に応じて、[y] または [n] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。
ステップ 6	確認プロンプトで、**y** と入力します。	これにより LDAP CA 証明書のダウンロードが開始されます。

例

この例では、LDAP 証明書をダウンロードします。

```
Server # scope ldap
Server /ldap # scope binding-certificate
Server /ldap/binding-certificate # set enabled yes
Server /ldap/binding-certificate *# commit
Server /ldap/binding-certificate # show detail
LDAP binding with Certificate:
    Enabled: yes
Server /ldap/binding-certificate #  download-ca-certificate tftp 172.22.141.66
new_com_chain.cer
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1282  100  1282    0     0   1247      0  0:00:01  0:00:01 --:--:--  1635
100  1282  100  1282    0     0   1239      0  0:00:01  0:00:01 --:--:--  1239
  You are going to overwrite the LDAP CA Certificate.
  Are you sure you want to proceed and overwrite the LDAP CA Certificate? [y|N]y
```

```
LDAP CA Certificate is downloaded successfully
Server /ldap/binding-certificate #
```

LDAP バインディングのテスト

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

（注） [Enable Encryption] チェックボックスと [Enable Binding CA Certificate] チェックボックスをオンにする場合は、[LDAP Server] フィールドに LDAP サーバの完全修飾ドメイン名（FQDN）を入力します。LDAP サーバの FQDN を解決するには、Cisco IMC ネットワークの優先 DNS を設定して適切な DNS IP アドレスを指定します。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ldap**	LDAP コマンド モードを開始します。
ステップ 2	Server# /ldap **scope binding-certificate**	LDAP CA 証明書バインド コマンド モードを開始します。
ステップ 3	Server /ldap/binding-certificate # **test-ldap-binding** ユーザ名	パスワードのプロンプトが表示されます。
ステップ 4	対応するパスワードを入力します。	ユーザを認証します。

例

次に、LDAP ユーザ バインドをテストする例を示します。

```
Server # scope ldap
Server /ldap # scope binding-certificate
Server /ldap/binding-certificate # test-ldap-binding user
Password:
diagldapbinding: Authenticated by LDAP
User user authenticated successfully.
Server /ldap/binding-certificate #
```

LDAP CA 証明書の削除

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ldap**	LDAP コマンド モードを開始します。
ステップ 2	Server# /ldap **scope binding-certificate**	LDAP CA 証明書バインド コマンド モードを開始します。
ステップ 3	Server /ldap/binding-certificate # **delete-ca-certificate**	確認のプロンプトが表示されます。
ステップ 4	確認プロンプトで、**y** と入力します。	これで LDAP CA 証明書が削除されます。

例

この例は、LDAP 証明書を削除します。

```
Server # scope ldap
Server /ldap # scope binding-certificate
Server /ldap/binding-certificate # delete-ca-certificate
You are going to delete the LDAP CA Certificate.
 Are you sure you want to proceed and delete the LDAP CA Certificate? [y|N]y
LDAP CA Certificate is deleted successfully
Server /ldap/binding-certificate #
```

ユーザ検索の優先順位の設定

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ldap**	BIOS コマンド モードを開始します。
ステップ 2	Server# /ldap **set userSearchPrecedence** {*localUserDB* | *ldapUserDB*}	選択したオプションに応じて、ローカル ユーザ データベースまたは LDAP データベースにユーザ検索の優先順位を設定します。
ステップ 3	Server# /ldap * **commit**	トランザクションをコミットします。
ステップ 4	（任意） Server# /ldap **show detail**	LDAP の詳細を表示します。

例

この例では、ユーザ検索の優先順位を設定します。

```
Server # scope ldap
Server /ldap # set userSearchPrecedence localUserDB
Server /ldap * # commit
Server /ldap # show detail
LDAP Settings:
Enabled: yes
Encrypted: no
Local User Search Precedence: localUserDB
Domain: new.com
Base DN: DC=new,DC=com
Timeout: 60
Filter Attribute: sAMAccountName
Attribute: CiscoAvPair
Server /ldap #
```

ユーザ セッションの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **show user-session**	現在のユーザ セッションの情報を表示します。

コマンドの出力には、現在のユーザ セッションに関する次の情報が表示されます。

名前	説明
[Terminate Session] ボタン	ユーザ アカウントに [admin] ユーザ ロールが割り当てられている場合、このオプションを使用して、関連付けられているユーザ セッションを強制的に終了できます。 （注） このタブから現在のセッションを終了することはできません。
[Session ID] カラム	セッションの固有識別情報。
[User name] カラム	ユーザのユーザ名。
[IP Address] カラム	ユーザがサーバにアクセスした IP アドレス。シリアル接続の場合は、[N/A] と表示されます。

名前	説明
[Type] カラム	ユーザがサーバにアクセスするために選択したセッション タイプ。次のいずれかになります。 • [webgui]：ユーザが Web UI を使用してサーバに接続されていることを示します。 • [CLI]：ユーザが CLI を使用してサーバに接続されていることを示します。 • [serial]：ユーザがシリアル ポートを使用してサーバに接続されていることを示します。

例

次に、現在のユーザ セッションに関する情報を表示する例を示します。

```
Server# show user-session
ID     Name             IP Address        Type         Killable
------ ---------------- ----------------- ------------ --------
15     admin            10.20.30.138      CLI          yes

Server /user #
```

ユーザ セッションの終了

始める前に

ユーザセッションを終了するには、admin権限を持つユーザとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **show user-session**	現在のユーザ セッションの情報を表示します。終了するユーザセッションは、終了可能（killable）であり、独自のセッションではないことが必要です。
ステップ 2	Server /user-session # **scope user-session** セッション番号	終了する番号付きのユーザ セッションに対してユーザ セッション コマンド モードを開始します。
ステップ 3	Server /user-session # **terminate**	ユーザ セッションを終了します。

例

次に、ユーザ セッション 10 の admin がユーザ セッション 15 を終了する例を示します。

```
Server# show user-session
ID     Name             IP Address        Type         Killable
------ ---------------- ----------------- ------------ --------
10     admin            10.20.41.234      CLI          yes
15     admin            10.20.30.138      CLI          yes
Server# scope user-session 15
Server /user-session # terminate
User session 15 terminated.

Server /user-session #
```