



## ユーザアカウントの管理

この章は、次の内容で構成されています。

- [ローカルユーザの設定, 1 ページ](#)
- [Active Directory, 2 ページ](#)
- [ユーザセッションの表示, 6 ページ](#)
- [ユーザセッションの終了, 6 ページ](#)

## ローカルユーザの設定

### はじめる前に

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# <b>scope user</b> <i>usernumber</i>	ユーザ番号 <i>usernumber</i> に対するユーザ コマンドモードを開始します。
ステップ 2	Server /user # <b>set enabled</b> { <b>yes</b>   <b>no</b> }	CIMC 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 # <b>set name</b> <i>username</i>	ユーザのユーザ名を指定します。
ステップ 4	Server /user # <b>set password</b>	パスワードを 2 回入力するように求められます。

	コマンドまたはアクション	目的
ステップ 5	Server /user # <b>set role</b> { <b>readonly</b>   <b>user</b>   <b>admin</b> }	<p>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。</p> <ul style="list-style-type: none"> <li>• <b>readonly</b> : 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。</li> <li>• <b>user</b> : このユーザは、次の操作を実行できます。 <ul style="list-style-type: none"> <li>• すべての情報を表示する</li> <li>• 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</li> <li>• KVM コンソールと仮想メディアを起動する</li> <li>• すべてのログをクリアする</li> <li>• ロケータ LED を切り替える</li> </ul> </li> <li>• <b>admin</b> : 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。</li> </ul>
ステップ 6	Server /user # <b>commit</b>	トランザクションをシステムの設定にコミットします。

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
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
    
```

## Active Directory

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。CIMC は、Active Directory の Kerberos ベースの認証サービスを利用します。

CIMC で Active Directory をイネーブルにすると、ローカルユーザデータベースで見つからなかったユーザアカウントのユーザ認証とロール許可が、Active Directory により行われます。

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

## Active Directory サーバの設定

CIMC を設定して、Active Directory をユーザの認証と認可に使用できます。Active Directory を使用するには、CIMC のユーザ ロールとロケールを保持する属性を使用してユーザを設定します。CIMC 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、Active Directory 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 属性のような新規のカスタム属性を追加できます。Active Directory スキーマの変更の詳細については、<http://technet.microsoft.com/en-us/library/bb727064.aspx> を参照してください。

Active Directory サーバでカスタム属性を作成するには、次の手順を実行します。



(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、CIMC 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。

### 手順

- ステップ 1 Active Directory 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 Active Directory 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
一般名	CiscoAVPair
LDAP 表示名	CiscoAVPair
一意の X500 オブジェクト ID	1.3.6.1.4.1.9.287247.1
説明	CiscoAVPair
構文	Case Sensitive String

- ステップ 3 Active Directory 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 CIMC 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> を参照してください。

### 次の作業

CIMC を使用して Active Directory を設定します。

## CIMC での Active Directory の設定

ローカルユーザの認証と許可に Active Directory (AD) サーバを使用するには、CIMC で Active Directory を設定します。

### はじめる前に

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# <b>scope ldap</b>	AD コンフィギュレーションに対して LDAP コマンドモードを開始します。
ステップ 2	Server /ldap # <b>set enabled {yes   no}</b>	AD をイネーブルまたはディセーブルにします。AD 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て、ユーザ認証とロール許可が AD によって実行されます。
ステップ 3	Server /ldap # <b>set timeout seconds</b>	LDAP 検索操作がタイムアウトになるまで CIMC が待機する秒数を指定します。
ステップ 4	Server /ldap # <b>set encrypted {yes   no}</b>	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。

	コマンドまたはアクション	目的
ステップ 5	Server /ldap # <b>set base-dn domain-name</b>	すべてのユーザが属する必要のあるドメインを指定します。
ステップ 6	Server /ldap # <b>set attribute name</b>	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。  CIMC ユーザ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、ユーザアクセスは read-only に制限されます。
ステップ 7	Server /ldap # <b>commit</b>	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 8	Server /ldap # <b>show [detail]</b>	(任意) AD の設定を表示します。

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

```
Server# scope ldap
Server /ldap # set enabled yes

Server /ldap ## set timeout 60
Server /ldap ## set encrypted yes
Server /ldap ## set base-dn example.com
Server /ldap ## set attribute CiscoAVPair
Server /ldap ## commit
Server /ldap # show detail
LDAP Settings:
  Domain Controller 1: 192.0.20.123
  Domain Controller 2: 0.0.0.0
  Domain Controller 3: 0.0.0.0
  BaseDN: example.com
  Encrypted: yes
  Timeout: 60
  Enabled: yes
  Attribute: CiscoAvPair
  Group Authorization: no
  Global Catalog 1: 192.0.20.11
  Global Catalog 2: 0.0.0.0
  Global Catalog 3: 0.0.0.0

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# <b>show user-session</b>	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
[Session ID] カラム	セッションの固有識別情報。
[Username] 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。
[Type] カラム	ユーザがサーバにアクセスした方法。たとえば、CLI、vKVM など。
[Action] カラム	ユーザアカウントに <b>admin</b> ユーザ ロールが割り当てられていて、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る場合は、このカラムに <b>[Terminate]</b> と表示されます。それ以外の場合は、 <b>N/A</b> と表示されます。  (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。

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

### はじめる前に

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# <b>show user-session</b>	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必要があります。
ステップ 2	Server /user-session # <b>scope user-session session-number</b>	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 # <b>terminate</b>	ユーザセッションを終了します。

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 #
```

