ユーザ アカウントの管理

この章の内容は、次のとおりです。

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# **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。
ステップ 2	Server /user # **set enabled** {**yes** | **no**}	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 # **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。

	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 • 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。

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 の設定

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。

Active Directory が CIMC でイネーブルになっている場合、ローカル ユーザ データベースに登録されていないユーザ アカウントに対して Active Directory がユーザ認証とロール許可を実行します。

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 の記事を参照してください。

Active Directory サーバで次の手順が実行します。

（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
Common Name	CiscoAVPair
LDAP Display Name	CiscoAVPair
Unique X500 Object ID	1.3.6.1.4.1.9.287247.1
Description	CiscoAVPair

プロパティ	値
Syntax	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。

Role	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 AD 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# **scope ldap**	AD を設定する LDAP 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 /ldap # **set enabled** {**yes** | **no**}	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見つからないユーザ アカウントについて、AD によってユーザ認証とロール許可が実行されます。
ステップ 3	Server /ldap # **set dc***n* *dc-host*	Active Directory ドメイン コントローラ（DC）のホスト名または IP アドレスを指定します。 1 ～ 3 のインデックス *n* 値を使用して最大 3 の DC を指定できます。
ステップ 4	Server /ldap # **set gc***n* *gc-host*	Active Directory グローバル カタログ（GC）サーバのホスト名または IP アドレスを指定します。 1 ～ 3 のインデックス *n* 値を使用して最大 3 の GC を指定できます。
ステップ 5	Server /ldap # **set timeout** *seconds*	LDAP 検索操作がタイムアウトするまで CIMC が待機する秒数を指定します。
ステップ 6	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 に送信するすべての情報を暗号化します。
ステップ 7	Server /ldap # **set base-dn** *domain-name*	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 8	Server /ldap # **set attribute** *name*	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 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）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 dc1 192.0.20.123
Server /ldap *# set gc1 192.0.20.11
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 #
```

次の作業

グループの認可に Active Directory グループを使用する場合は、『*Configuring Active Directory Groups in CIMC*』を参照してください。

CIMC での Active Directory 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 データベースに見つからないユーザや Active Directory で CIMC の使用を個別に許可されていないユーザの認証も、ユーザ グループ レベルで実行されます。

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。
- Active Directory（または LDAP）がイネーブル化され、設定されている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ldap**	AD を設定する LDAP コマンド モードを開始します。
ステップ 2	Server /ldap # **set group-auth** {**yes** | **no**}	AD 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。
ステップ 3	Server /ldap # **scope role-group** *index*	設定に使用可能な 5 種類のグループ プロファイルのいずれかを選択します。*index* は 1 ～ 5 の数字です。
ステップ 4	Server /ldap/role-group # **set name** *group-name*	サーバへのアクセスが許可された AD データベース内のグループの名前を指定します。

	コマンドまたはアクション	目的
ステップ 5	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 6	Server /ldap/role-group # **set role** {**admin** | **user** | **readonly**}	この AD グループで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、変更はできません。
ステップ 7	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。

次に、AD グループ許可を設定する例を示します。

```
Server# scope ldap
Server /ldap # 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  Name              Domain           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 #
```

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
[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。
[Action] カラム	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、関連付けられたユーザ セッションを強制的に終了できるときはこのカラムに [Terminate] と表示されます。 それ以外の場合は、N/A 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# **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** *session-number*	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。

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 #
```