ユーザ アカウントの管理

ローカル ユーザーの設定

始める前に

ローカルユーザーアカウントを設定または変更するには、admin 権限を持つユーザー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*	ユーザー番号のユーザーコマンドモードを入力します。
ステップ 2	Server /user # **set enabled** {**yes** |**no**\\	CIMC でユーザー 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*	ユーザーのユーザー名を指定します。
ステップ 4	Server /user # **set password**	ユーザーのパスワードを指定します。パスワードを 2 回入力するように求められます。
ステップ 5	Server /user # **set role** {**readonly** |**user** |**admin**\\	ユーザーに割り当てるロールを指定します。ロールは次のいずれかです。

	コマンドまたはアクション	目的
		• readonly：このユーザーは情報を表示できますが、変更することはできません。 • user：このユーザーは、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：このユーザーは、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、ユーザー 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   SSH Key Count
------ ---------------- --------  ---------  --------------
5      user             readonly  yes       (n/a)
```

LDAP サーバ（Active Directory）

CIMC では、情報をディレクトリ内で編成してこの情報へのアクセスを管理するディレクトリ サービスがサポートされます。CIMC は、ネットワークでディレクトリ情報を保管および保持する Lightweight Directory Access Protocol（LDAP）をサポートします。さらに、CIMC 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。CIMC は LDAP での Kerberos ベースの認証サービスを利用します。

CIMC で LDAP がイネーブルになっている場合、ローカル ユーザー データベース内に見つからないユーザー アカウントに関するユーザー認証とロール許可は、LDAP サーバーによって実行されます。LDAP ユーザー認証の形式は username@domain.com です。

[LDAP Settings] 領域で [Enable Encryption] チェックボックスをオンにすることで、LDAP サーバーへの送信データを暗号化するようサーバーに要求できます。

LDAP サーバの設定

CIMC を設定して、LDAP をユーザーの認証と許可に使用できます。LDAP を使用するには、CIMC のユーザー ロールとロケールを保持する属性を使用してユーザーを設定します。CIMC のユーザー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 Cisco AVPair 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 Cisco AVPair という名前のカスタム属性を作成しますが、CIMC のユーザー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。

LDAP サーバーに対して次の手順を実行する必要があります。

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
説明	CiscoAVPair
構文	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。

1. 左ペインで [クラス（Classes）] ノードを展開し、u を入力してユーザークラスを選択します。
2. [Attributes] タブをクリックして、[Add] をクリックします。
3. c を入力して CiscoAVPair 属性を選択します。
4. [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ーに対し、次のユーザー ロール値を CiscoAVPair 属性に追加します。

ロール	Cisco-AV-Pair 属性の値
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

CIMC を使用して LDAP サーバーを設定します。

CIMC での LDAP の設定

ローカル ユーザーの認証と許可に LDAP サーバーを使用するには、CIMC 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 権限を持つユーザー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 コマンドモードを入力します。
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 ユーザー データベースにないユーザー アカウントに対し、ユーザー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 domain name*	LDAP ドメイン名を指定します。

	コマンドまたはアクション	目的
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 CIMC が待機する秒数を指定します。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、サーバーは 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 サーバーで検索するベース DN を指定します。
ステップ 7	Server /ldap # **set attribute** 名	ユーザー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、ユーザー レコードで、この属性名と一致する値を検索します。 CIMC ユーザー 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、ユーザー 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 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
```

```
    Domain: sample-domain
    BaseDN: example.com
    Timeout (for each server): 60
    Filter-Attribute: sAMAccountName
    Attribute: CiscoAvPair
Server /ldap #
```

次のタスク

グループ承認用に LDAP グループを使用する場合は、CIMC での LDAP グループの設定 を参照してください。

CIMC 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 ユーザー データベースにないユーザーや、Active Directory で CIMC の使用を許可されていないユーザーに対するグループ レベルでのユーザー認証も行われます。

始める前に

- このタスクを実行するには、admin 権限を持つユーザー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。
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*	サーバー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。

	コマンドまたはアクション	目的

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ー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**：ユーザーは使用可能なすべてのアクションを実行できます。
		• **user**：ユーザーは、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**：ユーザー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 #
```

TACACS+ サーバー

TACACS+は、ユーザーによるルータまたはネットワーク アクセス サーバーへのアクセス試行の集中的な確認を可能にするセキュリティプロトコルです。TACACS+サービスは、TACACS+サーバー上のデータベースで維持されます。ネットワーク アクセス サーバーで TACACS+ 機能を設定し、使用可能にするには、TACACS+ サーバーを設定しておく必要があります。

TACACS+ サーバーで、Cisco Integrated Management Controller（CIMC）サービスの Cisco 属性値（AV）ペア権限レベル（priv-lvl）が管理者とオペレータの最小権限レベルに設定されていることを確認します。

CIMC の TACACS+ サポートの制約事項

- CIMC は、最大 6 台の TACACS+ サーバーへの接続をサポートします。
- ユーザは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。
- TACACS+ および LDAP の設定は排他的であり、一度に 1 つの設定のみが有効になります。
- デフォルトの時間は 5 秒です。
- デフォルトの TCP ポート接続は 49 です。
- デフォルトのログインは PAP ログインであり、ユーザーが入力した詳細データの代わりに、ユーザー名とパスワードが PAP プロトコルパケットでネットワーク アクセス サーバーに到着します。
- IPv4 だけがサポートされます。
- 事前共有キー（PSK）のサイズは 32 文字です。
- 共有秘密キーでサポートされる特殊文字は次の通りです：**! @% ^ * - _ .**

TACACS+ の動作

始める前に

ユーザーが TACACS+ を使用して CIMC に認証して単純な ASCII ログインを試行すると、次のオプションが提供されます。

CIMC は最終的に、TACACS+ サーバーから次のいずれかの応答を受信します。

- ACCEPT：ユーザは認証され、サービスを開始できます。CIMC が許可を要求するように設定されている場合は、この時点で許可のプロセスが開始されます。

- REJECT：ユーザは認証に失敗しました。ユーザは、今後のアクセスを拒否されるか、または、TACACS+ サーバによっては、ログイン シーケンスを再試行するプロンプトが表示されます。
- CONTINUE：ユーザーは、さらに認証情報の入力を求められます。

次のタスク

認証後、CIMC は承認要求を TACACS+ サーバーに送信します。承認結果に基づいて、CIMC はユーザーのロールを割り当てます。

TACACS+ サーバーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope tacacs+**	TACACS+ コンフィギュレーション モードを入力します。
ステップ 2	Server /tacacs+ # **set enabled** [**yes** | **no**]	TACACS+ ベースの認証を有効または無効にします。
ステップ 3	Server /tacacs+ # **fallback-only-on-no-connectivity** [**yes** | **no**]	他の認証優先順位へのフォールバックをイネーブルまたはディセーブルにします。
ステップ 4	Server /tacacs+/tacacs-server # **scope tacacs-server 1**	Enters tacacs-server 1 configuration mode.
ステップ 5	Server /tacacs+/tacacs-server # **set tacacs-server** *ip-address*	TACACS サーバーの IP アドレスを設定します。
ステップ 6	Server / tacacs+/tacacs-server # **set tacacs-port** *port*	TACACS ポートを設定します。
ステップ 7	Server /tacacs+/tacacs-server # **set tacacs-key** *key-string*	サーバーとの認証を開始するための事前共有キーを設定します。キーの最大長は 32 文字です。
ステップ 8	Server /tacacs+/tacacs-server # **scope tacacs-server 1**	Enters tacacs-server 1 configuration mode.
ステップ 9	Server /tacacs+/tacacs-server # **set tacacs-server** *ip-address*	TACACS サーバーの IP アドレスを設定します。
ステップ 10	Server / tacacs+/tacacs-server # port **set tacacs-port**	TACACS ポートを設定します。
ステップ 11	Server /tacacs+/tacacs-server # **set tacacs-key***key-string*	サーバーとの認証を開始するための事前共有キーを設定します。キーの最大長は 32 文字です。
ステップ 12	Server /tacacs # **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。

	コマンドまたはアクション	目的
ステップ 13	Server /tacacs # **show** [**detail**]	（任意）TACACS+ サーバーの設定を表示します。

例

次に、TACACS サーバーを設定する例を示します。

```
Server /# scope tacacs+
Server /tacacs+ #set enabled yes
Server /tacacs+ *#set fallback-only-on-no-connectivity no
Server /tacacs+ *#commit
Server /tacacs+ #scope tacacs-server 1
Server /tacacs+/tacacs-server #set tacacs-server 10.126.254.174
Server /tacacs+/tacacs-server *#set tacacs-port 49
Server /tacacs+/tacacs-server *#set tacacs-key
Please enter tacacs-key: _Abcded_abcde_123_abcd12_zxy123_
Please confirm tacacs-key: _Abcded_abcde_123_abcd12_zxy123_
Server /tacacs+/tacacs-server #commit
```

次に、TACACS+ サーバー設定を確認する例を示します。

```
Server /tacacs+/tacacs-server #show  detail
Server Id 1:
Server IP address/Hostname: 10.126.254.174
Server Key: ******
Server Port: 49
```

ユーザー 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**	現在のユーザー セッションの情報を表示します。

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

名前	説明
[セッション ID（Session ID）] カラム	セッションの固有識別情報。
[Username] カラム	ユーザーのユーザー名。
[IP Address] カラム	ユーザーがサーバーにアクセスした IP アドレス。
[Type] カラム	ユーザーがサーバーにアクセスした方法。たとえば、CLI、vKVM などです。

名前	説明
[Action] カラム	ユーザー アカウントに**admin** ユーザー 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ー 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。

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 #
```

ユーザー セッションの終了

始める前に

ユーザーセッションを終了するには、admin 権限を持つユーザー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**	現在のユーザーセッションの情報を表示します。終了するユーザーセッションは、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ー セッションに対してユーザーセッション コマンドモードを開始します。
ステップ 3	Server /user-session # **terminate**	ユーザー セッションを終了します。

例

次に、ユーザー セッション 10 の admin がユーザー 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 #
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。