



TACACS+ サーバ経由で認証をセットアップ

• [TACACS+ Server 経由のリモート認証 \(1 ページ\)](#)

TACACS+ Server 経由のリモート認証

リリース 11.5(1) 以降、Cisco DCNM には、TACACS+ サーバ経由で認証を設定するための **appmgr** コマンドが用意されています。DCNM は TACACS+ サーバに接続して、アクセスが許可されているかどうかを判断します。成功すると、アクセスが許可されます。TACACS+ サーバに到達できない場合、システムはローカル認証に戻ります。

この機能によって認証されるユーザは、**root** ユーザ、**sysadmin** ユーザ、および **poap** ユーザです。すべてのユーザをリモートサーバで設定する必要があります。

リモート認証は、SSH セッションでのみサポートされます。**su** コマンドは常にローカル認証を使用します。アプライアンス コンソールからのログインでは、ユーザがシステムからロックアウトされないように、常にローカル認証が使用されます。

リモート認証の削除

リモート認証を削除するには、次のコマンドを使用します。

```
appmgr remote-auth set none
```



(注) **appmgr remote-auth set** コマンドは、常に古い設定を新しい設定に置き換えます。

TACACS+ を使用したリモート認証の設定

TACACS+ を使用してリモート認証を設定するには、次のコマンドを使用します。

```
appmgr remote-auth set tacacs [ auth {pap | chap | ascii } ] {server <addr> <secret> }
```

値は次のとおりです。

- **auth** は、認証タイプを定義します。指定しない場合、デフォルトは PAP です。ASCII および MSCHAP もサポートされます。

- **addr** はサーバのアドレスです。サーバアドレスは、ホスト名、IPv4 アドレス、または IPv6 アドレス形式にすることができます。ポート番号を指定することもできます。例：
my.tac.server.com:2049

IPv6 アドレスは、RFC2732 に準拠した完全修飾 IPv6 形式でなければなりません。IPv6 アドレスは [] で囲む必要があります。そうしないと、機能が正しく機能しません。

次に例を示します。

- [2001:420:1201:2::a] – 正解
- 2001:420:1201:2::a – 不正解

- **secret** は、DCNM と TACACS+ サーバ間で共有される秘密です。スペースを含むシークレットは許可されません/サポートされません。

リモート認証の有効化または無効化

リモート認証を有効または無効にするには、次のコマンドを使用します。

```
appmgr remote-auth { enable | disable }
```

リモート認証パスワードの表示

リモート認証パスワードを表示するには、次のコマンドを使用します。

```
appmgr remote-auth show
```

サンプル出力:

```
dcnm# appmgr remote-auth show
Remote Authentication is DISABLED

dcnm# appmgr remote-auth show
Remote Authentication is ENABLED
Protocol: tacacs+
Server: 172.28.11.77, secret: *****
Authentication type: ascii
```

dcnm#

デフォルトでは、[-S or --show-secret] キーワードを使用しない限り、共有秘密はクリアテキストで表示されません。

例

1. 172.28.11.77 をリモート認証サーバとして設定し、cisco123 を共有秘密として使用します。

```
dcnm# appmgr remote-auth set tacacs server 172.28.11.77 cisco123
dcnm# appmgr remote-auth enable
```

2. 認証タイプとして MSCHAP を使用し、172.28.11.77 をリモート認証サーバとして設定し、Cisco 123 を共有秘密として設定します。

```
dcnm# appmgr remote-auth set tacacs auth mschap 172.28.11.77 cisco123
dcnm# appmgr remote-auth enable
```

- 異なる共有秘密を持つ3つのサーバを設定します。

```
dcnm# appmgr remote-auth set tacacs server tac1.cisco.com:2049 cisco123 server
tac2.cisco.com Cisco_123 server tac3.cisco.com Cisco_123
dcnm# appmgr remote-auth enable
```

- 認証設定を無効にするか、削除します。

```
dcnm# appmgr remote-auth set tacacs none
```

- 設定を削除せずにリモート認証を無効にします。

```
dcnm# appmgr remote-auth disable
```

- 現在のリモート認証設定を有効にします。

```
dcnm# appmgr remote-auth enable
```

リモート認証と POAP

リモート認証がイネーブルの場合、POAP ユーザのローカルパスワードは TACACS サーバのパスワードと同じである必要があります。それ以外の場合、POAP は失敗します。

ローカルの POAP パスワードを同期するには、TACACS サーバでパスワードを設定または変更した後、次のコマンドを使用します。

appmgr change_pwd ssh poap

Cisco DCNM ネイティブ HA セットアップでは、このコマンドはアクティブ ノードでのみ実行します。

DCNM ネイティブ HA セットアップでのリモート認証

既存のスタンドアロンセットアップにセカンダリ HA ノードを追加する前、および **appmgr update ssh-peer-trust** コマンドを実行する前に、リモート認証を無効にする必要があります。

