TACACS+ サーバ経由で認証をセットアップ

TACACS+ サーバ経由で SSH 認証をセットアップ

リリース 11.5(1) 以降、DCNM には、TACACS+ サーバ経由で ssh アクセスの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 への SSH アクセスの場合、アクセスが許可されているかどうかを判断するために、資格情報が以前に設定された TACACS+ サーバに送信されます。成功した場合、DCNM への SSH 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。

DCNM は、sysadmin、poap、root の 3 人のユーザに SSH アクセスを許可します。**sysadmin** ユーザーには、DCNM への一般的な SSH アクセスがあります。**root** ユーザーは、デフォルトでは無効になっています。ただし、DCNM のプライマリ サーバとセカンダリ サーバは、ネイティブ HA のセットアップとメンテナンスのために、パスワードなしのアクセス権を持つ root ユーザを使用して、SSH を介して相互に通信します。**poap** ユーザーは、DCNM と NX-OS スイッチ間の情報の SSH/SCP アクセスに使用されます。これは通常、POAP やイメージ管理などの機能に使用されます。DCNM で SSH アクセスの TACACS+ 認証を有効にする場合は、リモート AAA サーバーで 3 人のユーザー (sysadmin、poap、root) を作成し、TACACS+ を有効にする必要があります。その後、DCNM への SSH アクセスが認証され、TACACS+ サーバーの監査ログで DCNM へのすべての SSH アクセスが追跡されます。

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。DCNM コンソールからのログインでは、ユーザー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。

（注） クラスタ モードの DCNM セットアップでは、すべてのノード、つまり、プライマリ、セカンダリ、およびすべてのコンピューティング ノードでリモート認証を有効にして構成する必要があります。

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、古い設定を常に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** <*address*> <*secret*> }

それぞれの説明は次のとおりです。

- **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。
- *address* はサーバーのアドレスです。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 形式である必要があります。IPv6 アドレスは [ ] で囲む必要があります。そうしないと、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。スペースを含む秘密は許可されません/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 テキストに表示されません。

例

1. 172.28.11.77 をリモート認証サーバとして設定し有効にして、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
```

3. 異なる共有秘密を持つ 3 つのサーバーを設定します。

```
dcnm# appmgr remote□auth set tacacs server tac1.cisco.com:2049 cisco123 server
                  tac2.cisco.com Cisco_123 server tac3.cisco.com C1sco_123
dcnm# appmgr remote□auth enable
```

4. 認証設定を無効にするか、削除します。

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

5. 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
```

6. 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

リモート認証が有効な場合、**poap** ユーザーのローカル パスワードは TACACS サーバー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 Cisco DCNM Native HA セットアップでは、このコマンドはプライマリ 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

スタンドアロン DCNM をネイティブ HA セットアップに変換する必要があるシナリオでは、リモート認証が有効になっている場合は、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無効にする必要があります。

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。