A コマンド

この章では、A で始まる Cisco NX-OS Security コマンドについて説明します。

aaa accounting default

アカウンティングの Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）方式を設定するには、**aaa accounting default** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

aaa accounting default {**group** *group-list* | **local**}

no aaa accounting default {**group** *group-list* | **local**}

構文の説明

group	アカウンティングにサーバ グループを使用するように指定します。
group-list	サーバ グループをスペースで区切って指定します。リストには、次のようなサーバ グループを含めることができます。 • **radius**：設定済みのすべての RADIUS サーバ • 設定済みの任意の RADIUS サーバまたは TACACS+ サーバのサーバ グループ名 リストには、最大 8 つのグループ名を格納できます。
local	アカウンティングにローカル データベースを使用するように指定します。

デフォルト

local

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

group *group-list* 方式は、以前に定義された一連のサーバを指します。ホスト サーバを設定するには、**radius-server host** コマンドおよび **tacacs-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。

デバイス上の RADIUS サーバ グループを表示するには、**show aaa groups** コマンドを使用します。

group 方式、**local** 方式、または両方を指定した場合にそれらの方式が失敗すると、アカウンティング認証は失敗します。

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに Cisco NX-OS ソフトウェアが各グループをチェックします。

このコマンドには、ライセンスは必要ありません。

例

次に、AAA アカウンティングに任意の RADIUS サーバを設定する例を示します。

```
switch# configure terminal
switch(config)# aaa accounting default group radius
```

関連コマンド

コマンド	説明
aaa group server	AAA RADIUS サーバ グループを設定します。
radius-server host	RADIUS サーバを設定します。
show aaa accounting	AAA アカウンティング ステータス情報を表示します。
show aaa groups	AAA サーバ グループ情報を表示します。
tacacs-server host	TACACS+ サーバを設定します。

aaa accounting dot1x

802.1X 認証の AAA アカウンティング方式を設定するには、**aaa accounting dot1x** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

aaa accounting dot1x {**group** *group-list* | **local**}

no aaa accounting dot1x {**group** *group-list* | **local**}

構文の説明

group	アカウンティングにサーバ グループを使用するように指定します。
group-list	RADIUS サーバ グループをスペースで区切って指定します。リストには、次のようなサーバ グループを含めることができます。 • **radius**：設定済みのすべての RADIUS サーバ • 設定済みの任意の RADIUS サーバ グループ名 リストには、最大 8 つのグループ名を格納できます。
local	アカウンティングにローカル データベースを使用するように指定します。

デフォルト

local

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

group *group-list* 方式は、以前に定義された一連の RADIUS サーバを指します。ホスト サーバを設定するには、**radius-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。

デバイス上の RADIUS サーバ グループを表示するには、**show aaa groups** コマンドを使用します。

group 方式、**local** 方式、または両方を指定した場合にそれらの方式が失敗すると、アカウンティング認証は失敗します。

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに Cisco NX-OS ソフトウェアが各グループをチェックします。

このコマンドには、ライセンスは必要ありません。

例

次に、802.1X 認証の Authentication, Authorization, and Accounting（AAA）アカウンティング方式を設定する例を示します。

```
switch# configure terminal
switch(config)# aaa accounting dot1x default group group-list
```

関連コマンド

コマンド	説明
aaa group server radius	AAA RADIUS サーバ グループを設定します。
radius-server host	RADIUS サーバを設定します。
show aaa accounting	AAA アカウンティング ステータス情報を表示します。
show aaa groups	AAA サーバ グループ情報を表示します。

aaa authentication cts default group

Cisco TrustSec 認証のデフォルト AAA RADIUS サーバ グループを設定するには、**aaa authentication cts default group** コマンドを使用します。デフォルト AAA 認証サーバ グループ リストからサーバ グループを削除するには、このコマンドの **no** 形式を使用します。

aaa authentication cts default group *group-list*

no aaa authentication cts default group *group-list*

構文の説明

group-list	RADIUS サーバ グループをスペースで区切って指定します。リストには、次のようなサーバ グループを含めることができます。 • **radius**：設定済みのすべての RADIUS サーバ • 設定済みの任意の RADIUS サーバ グループ名 リストには、最大 8 つのグループ名を格納できます。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

group-list は、以前に定義された一連の RADIUS サーバを指します。ホスト サーバを設定するには、**radius-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。

デバイス上の RADIUS サーバ グループを表示するには、**show aaa groups** コマンドを使用します。

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに Cisco NX-OS ソフトウェアが各グループをチェックします。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、Cisco TrustSec のデフォルト AAA 認証 RADIUS サーバ グループを設定する例を示します。

```
switch# configure terminal
swtich(config)# aaa authentication cts default group RadGroup
```

関連コマンド

コマンド	説明
aaa group server	AAA サーバ グループを設定します。
feature cts	Cisco TrustSec 機能をイネーブルにします。
radius-server host	RADIUS サーバを設定します。
show aaa authentication	AAA 認証の設定を表示します。
show aaa groups	AAA サーバ グループを表示します。

aaa authentication dot1x default group

802.1X の AAA 認証方式を設定するには、**aaa authentication dot1x default group** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authentication dot1x default group *group-list*

no aaa authentication dot1x default group *group-list*

構文の説明

group-list	RADIUS サーバ グループをスペースで区切って指定します。リストには、次のようなサーバ グループを含めることができます。 • **radius**：設定済みのすべての RADIUS サーバ • 設定済みの任意の RADIUS サーバ グループ名 リストには、最大 8 つのグループ名を格納できます。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

802.1X を設定する前に、**feature dot1x** コマンドを使用する必要があります。

group-list は、以前に定義された一連の RADIUS サーバを指します。ホスト サーバを設定するには、**radius-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。

デバイス上の RADIUS サーバ グループを表示するには、**show aaa groups** コマンドを使用します。

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに Cisco NX-OS ソフトウェアが各グループをチェックします。

このコマンドには、ライセンスは必要ありません。

例

次に、802.1X 認証方式を設定する例を示します。

```
switch# configure terminal
switch(config)# aaa authentication do1x default group Dot1xGroup
```

次に、デフォルトの 802.1X 認証方式に戻す例を示します。

```
switch# configure terminal
switch(config)# no aaa authentication do1x default group Dot1xGroup
```

関連コマンド

コマンド	説明
feature dot1x	802.1X をイネーブルにします。
radius-server host	RADIUS サーバを設定します。
show aaa authentication	AAA 認証の設定を表示します。
show aaa groups	AAA サーバ グループを表示します。

aaa authentication eou default group

EAP over UDP（EoU）の AAA 認証方式を設定するには、**aaa authentication eou default group** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authentication eou default group *group-list*

no aaa authentication eou default group *group-list*

構文の説明

group-list	RADIUS サーバ グループをスペースで区切って指定します。リストには、次のようなサーバ グループを含めることができます。 • **radius**：設定済みのすべての RADIUS サーバ • 設定済みの任意の RADIUS サーバ グループ名 リストには、最大 8 つのグループ名を格納できます。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルト EAPoUDP 認証方式を設定する前に、**feature eou** コマンドを使用して EAPoUDP をイネーブルにする必要があります。

group-list は、以前に定義された一連の RADIUS サーバを指します。ホスト サーバを設定するには、**radius-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。

デバイス上の RADIUS サーバ グループを表示するには、**show aaa groups** コマンドを使用します。

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに Cisco NX-OS ソフトウェアが各グループをチェックします。

このコマンドには、ライセンスは必要ありません。

例

次に、EAPoUDP 認証方式を設定する例を示します。

```
switch# configure terminal
switch(config)# aaa authentication eou default group EoUGroup
```

次に、デフォルトの EAPoUDP 認証方式に戻す例を示します。

```
switch# configure terminal
switch(config)# no aaa authentication eou default group EoUGroup
```

関連コマンド

コマンド	説明
feature eou	EAPoUDP をイネーブルにします。
radius-server host	RADIUS サーバを設定します。
show aaa authentication	AAA 認証の設定を表示します。
show aaa groups	AAA サーバ グループを表示します。

aaa authentication login ascii-authentication

TACACS+ サーバでパスワードの ASCII 認証をイネーブルにするには、**aaa authentication login ascii-authentication** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authentication login ascii-authentication

no aaa authentication login ascii-authentication

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
4.1(2)	このコマンドが追加されました。

使用上のガイドライン

この機能をサポートするのは、TACACS+ プロトコルだけです。

このコマンドには、ライセンスは必要ありません。

例

次の例では、TACACS+ サーバでパスワードの ASCII 認証をイネーブルにする方法を示します。

```
switch# configure terminal
switch(config)# aaa authentication login ascii-authentication
```

次の例では、TACACS+ サーバでパスワードの ASCII 認証をディセーブルにする方法を示します。

```
switch# configure terminal
switch(config)# no aaa authentication login ascii-authentication
```

関連コマンド

コマンド	説明
show aaa authentication login ascii-authentication	パスワードの ASCII 認証のステータスを表示します。

aaa authentication login chap enable

ログイン時の Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェーク認証プロトコル）認証をイネーブルにするには、**aaa authentication login chap enable** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authentication login chap enable

no aaa authentication login chap enable

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

Cisco NX-OS デバイスで CHAP と MSCHAP（または MSCHAP V2）の両方をイネーブルにすることはできません。

このコマンドには、ライセンスは必要ありません。

例

次に、CHAP 認証をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# aaa authentication login chap enable
```

次に、CHAP 認証をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no aaa authentication login chap enable
```

関連コマンド

コマンド	説明
show aaa authentication login chap	CHAP 認証のステータスを表示します。

aaa authentication login console

コンソール ログインの AAA 認証方式を設定するには、**aaa authentication login console** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authentication login console {**fallback error local** | **group** *group-list* [**none**] | **local** | **none**}

no aaa authentication login console {**fallback error local** | **group** *group-list* [**none**] | **local** | **none**}

構文の説明

fallback error local	リモート認証が設定されており、すべての AAA サーバが到達不能である場合、コンソール ログインのローカル認証へのフォールバックをイネーブルにします。ローカル認証へのフォールバックはデフォルトでイネーブルです。 **（注）** ローカル認証へのフォールバックをディセーブルにすると、Cisco NX-OS デバイスがロックされ、パスワード回復を実行しないとアクセスできなくなることがあります。デバイスがロックされないようにするには、デフォルトのログインとコンソール ログインの両方ではなく、いずれかに対してのみローカル認証へのフォールバックをディセーブルにすることを推奨します。
group	認証にサーバ グループを使用するように指定します。
group-list	サーバ グループのスペースで区切られたリスト。リストには、次のようなサーバ グループを含めることができます。 • **radius**：設定済みのすべての RADIUS サーバ • **tacacs+**：設定済みのすべての TACACS+ サーバ • **ldap**：設定済みのすべての LDAP サーバ • 設定済みの任意の RADIUS サーバ、TACACS+ サーバ、または LDAP サーバ グループ名
none	（任意）認証を使用しないことを指定します。
local	認証にローカル データベースを使用するように指定します。

デフォルト

local

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	LDAP サーバ グループのサポートが追加されました。

5.0(2)	**fallback error local** キーワードが追加されました。
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

group radius、**group tacacs+**、**group ldap**、および **group** *group-list* の各方式は、以前に定義された一連の RADIUS サーバ、TACACS+ サーバ、または LDAP サーバを指します。ホスト サーバを設定するには、**radius-server host**、**tacacs-server host**、または **ldap-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。

デバイス上のサーバ グループを表示するには、**show aaa group** コマンドを使用します。

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに Cisco NX-OS ソフトウェアが各グループをチェックします。

group 方式または **local** 方式を指定した場合にそれらの方式が失敗すると、認証は失敗する可能性があります。**none** 方式を単独または **group** 方式の後ろに指定した場合、認証は常に成功します。

このコマンドは、デフォルト VDC（VDC 1）でだけ機能します。

このコマンドには、ライセンスは必要ありません。

例

次に、コンソール ログインの AAA 認証方式を設定する例を示します。

```
switch# configure terminal
switch(config)# aaa authentication login console group radius
```

次に、デフォルトのコンソール ログインの AAA 認証方式に戻す例を示します。

```
switch# configure terminal
switch(config)# no aaa authentication login console group radius
```

関連コマンド

コマンド	説明
aaa group server	AAA サーバ グループを設定します。
ldap-server host	LDAP サーバを設定します。
radius-server host	RADIUS サーバを設定します。
show aaa authentication	AAA 認証情報を表示します。
show aaa groups	AAA サーバ グループを表示します。
tacacs-server host	TACACS+ サーバを設定します。

aaa authentication login default

デフォルト AAA 認証方式を設定するには、**aaa authentication login default** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authentication login default {**fallback error local** | **group** *group-list* [**none**] | **local** | **none**}

no aaa authentication login default {**fallback error local** | **group** *group-list* [**none**] | **local** | **none**}

構文の説明

fallback error local	リモート認証が設定されており、すべての AAA サーバが到達不能である場合、デフォルト ログインのローカル認証へのフォールバックをイネーブルにします。ローカル認証へのフォールバックはデフォルトでイネーブルです。 **（注）** ローカル認証へのフォールバックをディセーブルにすると、Cisco NX-OS デバイスがロックされ、パスワード回復を実行しないとアクセスできなくなることがあります。デバイスがロックされないようにするには、デフォルトのログインとコンソール ログインの両方ではなく、いずれかに対してのみローカル認証へのフォールバックをディセーブルにすることを推奨します。
group	認証に使用するサーバ グループ リストを指定します。
group-list	サーバ グループをスペースで区切って指定します。リストには、次のようなサーバ グループを含めることができます。 • **radius**：設定済みのすべての RADIUS サーバ • **tacacs+**：設定済みのすべての TACACS+ サーバ • **ldap**：設定済みのすべての LDAP サーバ • 設定済みの任意の RADIUS サーバ、TACACS+ サーバ、または LDAP サーバ グループ名
none	（任意）認証を使用しないことを指定します。
local	認証にローカル データベースを使用するように指定します。

デフォルト

local

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	LDAP サーバ グループのサポートが追加されました。

5.0(2)	**fallback error local** キーワードが追加されました。
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

group radius、**group tacacs+**、**group ldap**、および **group** *group-list* の各方式は、以前に定義された一連の RADIUS サーバ、TACACS+ サーバ、または LDAP サーバを指します。ホスト サーバを設定するには、**radius-server host**、**tacacs-server host**、または **ldap-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。

デバイス上のサーバ グループを表示するには、**show aaa group** コマンドを使用します。

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに Cisco NX-OS ソフトウェアが各グループをチェックします。

group 方式または **local** 方式を指定した場合にそれらの方式が失敗すると、認証は失敗します。**none** 方式を単独または **group** 方式の後ろに指定した場合、認証は常に成功します。

このコマンドには、ライセンスは必要ありません。

例

次に、デフォルト ログインの AAA 認証方式を設定する例を示します。

```
switch# configure terminal
switch(config)# aaa authentication login default group radius
```

次に、デフォルト ログインのデフォルトの AAA 認証方式に戻す例を示します。

```
switch# configure terminal
switch(config)# no aaa authentication login default group radius
```

関連コマンド

コマンド	説明
aaa group server	AAA サーバ グループを設定します。
ldap-server host	LDAP サーバを設定します。
radius-server host	RADIUS サーバを設定します。
show aaa authentication	AAA 認証情報を表示します。
show aaa groups	AAA サーバ グループを表示します。
tacacs-server host	TACACS+ サーバを設定します。

aaa authentication login error-enable

コンソールに AAA 認証失敗メッセージが表示されるように設定するには、**aaa authentication login error-enable** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authentication login error-enable

no aaa authentication login error-enable

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

ログイン時にリモート AAA サーバからの応答がない場合には、ローカル ユーザ データベースへのロールオーバーによってログインが処理されます。そのような場合に、ログイン失敗メッセージの表示がイネーブルになっていると、ユーザ端末に次のメッセージが表示されます。

```
Remote AAA servers unreachable; local authentication done.
Remote AAA servers unreachable; local authentication failed.
```

このコマンドには、ライセンスは必要ありません。

例

次に、AAA 認証失敗メッセージのコンソールへの表示をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# aaa authentication login error-enable
```

次に、AAA 認証失敗メッセージのコンソールへの表示をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no aaa authentication login error-enable
```

関連コマンド

コマンド	説明
show aaa authentication login error-enable	AAA 認証失敗メッセージ表示のステータスを表示します。

aaa authentication login mschap enable

ログイン時の Microsoft Challenge Handshake Authentication Protocol（MS-CHAP; マイクロソフト チャレンジ ハンドシェーク認証プロトコル）認証をイネーブルにするには、**aaa authentication login mschap enable** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authentication login mschap enable

no aaa authentication login mschap enable

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

Cisco NX-OS デバイスで MSCHAP と CHAP または MSCHAP V2 の両方をイネーブルにすることはできません。

このコマンドには、ライセンスは必要ありません。

例

次に、MSCHAP 認証をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# aaa authentication login mschap enable
```

次に、MSCHAP 認証をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no aaa authentication login mschap enable
```

関連コマンド

コマンド	説明
show aaa authentication login mschap	MSCHAP 認証のステータスを表示します。

aaa authentication login mschapv2 enable

ログイン時の Microsoft Challenge Handshake Authentication Protocol Version 2（MSCHAP V2）認証をイネーブルにするには、**aaa authentication login mschapv2 enable** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authentication login mschapv2 enable

no aaa authentication login mschapv2 enable

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.1(2)	このコマンドが追加されました。

使用上のガイドライン

Cisco NX-OS デバイスで MSCHAP V2 と CHAP または MSCHAP の両方をイネーブルにすることはできません。

このコマンドには、ライセンスは必要ありません。

例

次に、MSCHAP V2 認証をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# aaa authentication login mschapv2 enable
```

次に、MSCHAP V2 認証をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no aaa authentication login mschapv2 enable
```

関連コマンド

コマンド	説明
show aaa authentication login mschapv2	MSCHAP V2 認証のステータスを表示します。

aaa authorization commands default

すべての EXEC コマンドでデフォルト AAA 認可方式を設定するには、**aaa authorization commands default** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authorization commands default [**group** *group-list* [**local**] | **local**]

no aaa authorization commands default [**group** *group-list* [**local**] | **local**]

構文の説明

group	（任意）認可にサーバ グループを使用するように指定します。
group-list	サーバ グループのスペースで区切られたリスト。リストには、次のようなサーバ グループを含めることができます。 • **tacacs+**：設定済みのすべての TACACS+ サーバ • 設定済みの任意の TACACS+ サーバ グループ名
local	（任意）認証にローカル ロールベース データベースを使用するように指定します。

デフォルト

local

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	**none** キーワードが廃止されました。
4.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature tacacs+** コマンドを使用して TACACS+ 機能をイネーブルにする必要があります。

group tacacs+ 方式および **group** *group-list* 方式は、以前に定義された一連の TACACS+ サーバを指します。ホスト サーバを設定するには、**tacacs-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。デバイス上のサーバ グループを表示するには、**show aaa group** コマンドを使用します。

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに Cisco NX-OS ソフトウェアが各グループをチェックします。設定済みのすべてのサーバ グループで応答に失敗し、フォールバック方式として **local** を設定済みの場合、**local** 方式だけが使用されます。

group 方式または **local** 方式を指定した場合にその方式が失敗すると、認可は失敗する可能性があります。TACACS+ サーバ グループの方式のあとにフォールバック方式を設定していないと、すべてのサーバ グループから応答が得られなかった場合は許可に失敗します。

注意 コマンド認可では、デフォルトのロールを含む、ユーザ ロールに基づいた認可制御（RBAC）がディセーブルにされます。

（注） コマンド認可は、コンソールを使用しないセッションでのみ使用できます。コンソールを使用してサーバにログインすると、コマンド認可はディセーブルになります。

（注） デフォルトでは、状況依存ヘルプおよびコマンドのタブ補完に表示されるのは、割り当てられたロールでユーザに対するサポートが定義されているコマンドだけです。コマンド許可をイネーブルにすると、Cisco NX-OS ソフトウェアでは、ユーザに割り当てられているロールに関係なく、状況依存ヘルプおよびタブ補完にすべてのコマンドが表示されるようになります。

このコマンドには、ライセンスは必要ありません。

例

次に、EXEC コマンドでデフォルト AAA 認可方式を設定する例を示します。

```
switch# configure terminal
switch(config)# aaa authorization commands default group TacGroup local
Per command authorization will disable RBAC for all users. Proceed (y/n)?
```

（注） 確認プロンプトで Enter キーを押すと、デフォルトの応答は **n** になります。

次に、EXEC コマンドでデフォルト AAA 認可方式に戻す例を示します。

```
switch# configure terminal
switch(config)# no aaa authorization commands default group TacGroup local
```

関連コマンド

コマンド	説明
aaa authorization config-commands default	コンフィギュレーション コマンドでデフォルト AAA 認可方式を設定します。
feature tacacs+	TACACS+ 機能をイネーブルにします。
show aaa authorization	AAA 認可設定を表示します。
terminal verify-only	コマンド認可の確認をイネーブルにします。
test aaa authorization command-type	AAA コマンド認可方式を使用して、コマンド認可をテストします。

aaa authorization config-commands default

すべてのコンフィギュレーション コマンドでデフォルト AAA 認可方式を設定するには、**aaa authorization config-commands default** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authorization config-commands default [**group** *group-list* [**local**] | **local**]

no aaa authorization config-commands default [**group** *group-list* [**local**] | **local**]

構文の説明

group	（任意）認可にサーバ グループを使用するように指定します。
group-list	サーバ グループのスペースで区切られたリスト。リストには、次のようなサーバ グループを含めることができます。 • **tacacs+**：設定済みのすべての TACACS+ サーバ • 設定済みの任意の TACACS+ サーバ グループ名
local	（任意）認証にローカル ロールベース データベースを使用するように指定します。

デフォルト

local

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	**none** キーワードが廃止されました。
4.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature tacacs+** コマンドを使用して TACACS+ 機能をイネーブルにする必要があります。

group tacacs+ 方式および **group** *group-list* 方式は、以前に定義された一連の TACACS+ サーバを指します。ホスト サーバを設定するには、**tacacs-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。デバイス上のサーバ グループを表示するには、**show aaa group** コマンドを使用します。

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに Cisco NX-OS ソフトウェアが各グループをチェックします。設定済みのすべてのサーバ グループで応答に失敗し、フォールバック方式として **local** を設定済みの場合、**local** 方式だけが使用されます。

group 方式または **local** 方式を指定した場合にその方式が失敗すると、認可は失敗する可能性があります。TACACS+ サーバ グループの方式のあとにフォールバック方式を設定していないと、すべてのサーバ グループから応答が得られなかった場合は許可に失敗します。

注意 コマンド認可では、デフォルトのロールを含む、ユーザ ロールに基づいた認可制御（RBAC）がディセーブルにされます。

（注） コマンド認可は、コンソールを使用しないセッションでのみ使用できます。コンソールを使用してサーバにログインすると、コマンド認可はディセーブルになります。

（注） デフォルトでは、状況依存ヘルプおよびコマンドのタブ補完に表示されるのは、割り当てられたロールでユーザに対するサポートが定義されているコマンドだけです。コマンド許可をイネーブルにすると、Cisco NX-OS ソフトウェアでは、ユーザに割り当てられているロールに関係なく、状況依存ヘルプおよびタブ補完にすべてのコマンドが表示されるようになります。

このコマンドには、ライセンスは必要ありません。

例

次に、コンフィギュレーション コマンドでデフォルト AAA 認可方式を設定する例を示します。

```
switch# configure terminal
switch(config)# aaa authorization config-commands default group TacGroup local
```

次に、コンフィギュレーション コマンドでデフォルト AAA 認可方式に戻す例を示します。

```
switch# configure terminal
switch(config)# no aaa authorization config-commands default group TacGroup local
```

関連コマンド

コマンド	説明
aaa authorization commands default	EXEC コマンドでデフォルト AAA 認可方式を設定します。
feature tacacs+	TACACS+ 機能をイネーブルにします。
show aaa authorization	AAA 認可設定を表示します。
terminal verify-only	コマンド認可の確認をイネーブルにします。
test aaa authorization command-type	AAA コマンド認可方式を使用して、コマンド認可をテストします。

aaa authorization cts default group

Cisco TrustSec 認可のデフォルト AAA RADIUS サーバ グループを設定するには、**aaa authorization cts default group** コマンドを使用します。デフォルト AAA 認可サーバ グループ リストからサーバ グループを削除するには、このコマンドの **no** 形式を使用します。

aaa authorization cts default group *group-list*

no aaa authorization cts default group *group-list*

構文の説明

group-list	RADIUS サーバ グループをスペースで区切って指定します。リストには、次のようなサーバ グループを含めることができます。 • **radius**：設定済みのすべての RADIUS サーバ • 設定済みの任意の RADIUS サーバ グループ名 リストには、最大 8 つのグループ名を格納できます。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

aaa authorization cts default group コマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

group-list は、以前に定義された一連の RADIUS サーバを指します。ホスト サーバを設定するには、**radius-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。

デバイス上の RADIUS サーバ グループを表示するには、**show aaa groups** コマンドを使用します。

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに Cisco NX-OS ソフトウェアが各グループをチェックします。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、Cisco TrustSec のデフォルト AAA 認可 RADIUS サーバ グループを設定する例を示します。

```
switch# configure terminal
swtich(config)# aaa authorization cts default group RadGroup
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show aaa authorization	AAA 認可設定を表示します。
show aaa groups	AAA サーバ グループを表示します。

aaa authorization ssh-certificate

TACACS+ サーバまたは Lightweight Directory Access Protocol（LDAP）サーバのデフォルト AAA 認可方式を設定するには、**aaa authorization ssh-certificate** コマンドを使用します。この設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authorization ssh-certificate default {**group** *group-list* | **local**}

no aaa authorization ssh-certificate default {**group** *group-list* | **local**}

構文の説明

group	認可にサーバ グループを使用するように指定します。
group-list	サーバ グループのスペースで区切られたリスト。リストには、次のようなサーバ グループを含めることができます。 • **tacacs+**：設定済みのすべての TACACS+ サーバ • **ldap**：設定済みのすべての LDAP サーバ • 設定済みの任意の TACACS+ サーバまたは LDAP サーバ グループ名
local	認証にローカル データベースを使用するように指定します。

デフォルト

local

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature tacacs+** コマンドを使用して TACACS+ 機能をイネーブルにするか、または **feature ldap** コマンドを使用して LDAP 機能をイネーブルにする必要があります。

group tacacs+、**group ldap**、**group**、および *group-list* 方式は、以前に定義された一連の TACACS+ サーバおよび LDAP サーバを指します。ホスト サーバを設定するには、**tacacs-server host** コマンドまたは **ldap-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。デバイス上のサーバ グループを表示するには、**show aaa group** コマンドを使用します。

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに Cisco NX-OS ソフトウェアが各グループをチェックします。設定済みのすべてのサーバ グループで応答に失敗し、フォールバック方式として **local** を設定済みの場合、**local** 方式だけが使用されます。

group 方式または **local** 方式を指定した場合にそれらの方式が失敗すると、認可は失敗する可能性があります。TACACS+ または LDAP サーバ グループ方式の後に、フォールバック方式を設定していない場合、すべてのサーバ グループが応答に失敗すると、認可が失敗します。

このコマンドには、ライセンスは必要ありません。

例

次に、LDAP サーバのデフォルト AAA 認可方式として、証明書認証を使用した LDAP 認可を設定する例を示します。

```
switch# configure terminal
switch(config)# aaa authorization ssh-certificate default group LDAPServer1 LDAPServer2
```

関連コマンド

コマンド	説明
aaa authorization ssh-publickey	次に、LDAP サーバのデフォルト AAA 認可方式として、SSH 公開キーを使用した LDAP 認可またはローカル認可を設定する例を示します。
feature ldap	LDAP 機能をイネーブルにします。
feature tacacs+	TACACS+ 機能をイネーブルにします。
show aaa authorization	AAA 認可設定を表示します。

aaa authorization ssh-publickey

Lightweight Directory Access Protocol（LDAP）サーバのデフォルト AAA 認可方式として、セキュアシェル（SSH）公開キーを使用した LDAP 認可またはローカル認可を設定するには、**aaa authorization ssh-publickey** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authorization ssh-publickey default {**group** *group-list* | **local**}

no aaa authorization ssh-publickey default {**group** *group-list* | **local**}

構文の説明

group	認可にサーバ グループを使用するように指定します。
group-list	サーバ グループのスペースで区切られたリスト。リストには、次のようなサーバ グループを含めることができます。 • **ldap**：設定済みのすべての LDAP サーバ • 設定済みの任意の LDAP サーバ グループ名
local	認証にローカル データベースを使用するように指定します。

デフォルト

local

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature ldap** コマンドを使用して LDAP 機能をイネーブルにする必要があります。

group ldap 方式および **group** *group-list* 方式は、以前に定義された LDAP サーバを指します。ホストサーバを設定するには、**ldap-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。デバイス上のサーバ グループを表示するには、**show aaa group** コマンドを使用します。

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに Cisco NX-OS ソフトウェアが各グループをチェックします。設定済みのすべてのサーバ グループで応答に失敗し、フォールバック方式として **local** を設定済みの場合、**local** 方式だけが使用されます。

group 方式または **local** 方式を指定した場合にそれらの方式が失敗すると、認可は失敗する可能性があります。LDAP サーバ グループ方式の後に、フォールバック方式を設定していない場合、すべてのサーバ グループが応答に失敗すると、認可が失敗します。

このコマンドには、ライセンスは必要ありません。

例

次に、LDAP サーバのデフォルト AAA 認可方式として、SSH 公開キーを使用した LDAP 認可を設定する例を示します。

```
switch# configure terminal
switch(config)# aaa authorization ssh-publickey default group LDAPServer1 LDAPServer2
```

関連コマンド

コマンド	説明
aaa authorization ssh-certificate	LDAP サーバのデフォルト AAA 認可方式として、証明書認証を使用した LDAP 認可またはローカル認可を設定します。
feature ldap	LDAP 機能をイネーブルにします。
show aaa authorization	AAA 認可設定を表示します。

aaa group server ldap

Lightweight Directory Access Protocol（LDAP）サーバ グループを作成して、LDAP サーバ グループ コンフィギュレーション モードを開始するには、**aaa group server ldap** コマンドを使用します。LDAP サーバ グループを削除するには、このコマンドの **no** 形式を使用します。

aaa group server ldap *group-name*

no aaa group server ldap *group-name*

構文の説明

group-name	LDAP サーバ グループ名。名前には英数字を使用します。大文字と小文字が区別され、最大で 64 文字の長さまで指定可能です。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

LDAP を設定する前に、**feature ldap** コマンドを使用する必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、LDAP サーバ グループを作成し、LDAP サーバ コンフィギュレーション モードを開始する例を示します。

```
switch# configure terminal
switch(config)# aaa group server ldap LdapServer
switch(config-ldap)#
```

次に、LDAP サーバ グループを削除する例を示します。

```
switch# configure terminal
switch(config)# no aaa group server ldap LdapServer
```

関連コマンド

コマンド	説明
feature ldap	LDAP をイネーブルにします。
show aaa groups	サーバ グループ情報を表示します。

aaa group server radius

RADIUS サーバ グループを作成して、RADIUS サーバ グループ コンフィギュレーション モードを開始するには、**aaa group server radius** コマンドを使用します。RADIUS サーバ グループを削除するには、このコマンドの **no** 形式を使用します。

aaa group server radius *group-name*

no aaa group server radius *group-name*

構文の説明

group-name	RADIUS サーバ グループ名。名前には英数字を使用します。大文字と小文字が区別され、最大で 64 文字の長さまで指定可能です。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、RADIUS サーバ グループを作成し、RADIUS サーバ コンフィギュレーション モードを開始する例を示します。

```
switch# configure terminal
switch(config)# aaa group server radius RadServer
switch(config-radius)#
```

次に、RADIUS サーバ グループを削除する例を示します。

```
switch# configure terminal
switch(config)# no aaa group server radius RadServer
```

関連コマンド

コマンド	説明
show aaa groups	サーバ グループ情報を表示します。

aaa group server tacacs+

TACACS+ サーバ グループを作成して、TACACS+ サーバ グループ コンフィギュレーション モードを開始するには、**aaa group server tacacs+** コマンドを使用します。TACACS+ サーバ グループを削除するには、このコマンドの **no** 形式を使用します。

aaa group server tacacs+ *group-name*

no aaa group server tacacs+ *group-name*

構文の説明

group-name	TACACS+ サーバ グループ名。名前には英数字を使用します。大文字と小文字が区別され、最大で 64 文字の長さまで指定可能です。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、TACACS+ サーバ グループを作成し、TACACS+ サーバ コンフィギュレーション モードを開始する例を示します。

```
switch# configure terminal
switch(config)# aaa group server tacacs+ TacServer
switch(config-radius)#
```

次に、TACACS+ サーバ グループを削除する例を示します。

```
switch# configure terminal
switch(config)# no aaa group server tacacs+ TacServer
```

関連コマンド

コマンド	説明
feature tacacs+	TACACS+ をイネーブルにします。
show aaa groups	サーバ グループ情報を表示します。

aaa user default-role

ユーザ ロールを持たないリモート ユーザが、RADIUS または TACACS+ 経由でデフォルト ユーザ ロールを使用してデバイスにログインできるようにするには、**aaa user default-role** コマンドを使用します。リモート ユーザのデフォルト ユーザ ロールをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa user default-role

no aaa user default-role

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

イネーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(3)	このコマンドが追加されました。

使用上のガイドライン

Virtual Device Context（VDC; 仮想デバイス コンテキスト）のこの機能は、必要に応じてイネーブルまたはディセーブルにできます。デフォルトの VDC では、デフォルトのユーザ ロールは network-operator です。デフォルト以外の VDC では、デフォルトの VDC は vdc-operator です。AAA のデフォルトのユーザ ロール機能をディセーブルにすると、ユーザ ロールを持たないリモート ユーザはデバイスにログインできなくなります。

このコマンドには、ライセンスは必要ありません。

例

次に、リモート ユーザの AAA 認証のデフォルト ユーザ ロールをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# aaa user default-role
```

次に、リモート ユーザの AAA 認証のデフォルト ユーザ ロールをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no aaa user default-role
```

関連コマンド

コマンド	説明
show aaa user default-role	AAA デフォルト ユーザ ロール機能のステータスを表示します。

absolute

特定の開始日時、特定の終了日時、またはその両方が指定された時間範囲を指定するには、**absolute** コマンドを使用します。絶対時間範囲を削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **absolute** [**start** *time date*] [**end** *time date*]

no {*sequence-number* | **absolute** [**start** *time date*] [**end** *time date*]}

構文の説明

sequence-number	（任意）ルールのシーケンス番号。時間範囲内の該当番号の位置にコマンドが挿入されます。シーケンス番号により、時間範囲内のルールの順序が保持されます。 シーケンス番号には、1 ～ 4294967295 の間の整数を指定できます。 デフォルトでは、時間範囲内の最初のルールにシーケンス番号 10 が割り当てられます。 シーケンス番号を指定しないと、時間範囲の最後にルールが追加され、1 つ前のルールのシーケンス番号に 10 を加算した値が、シーケンス番号として割り当てられます。 ルールのシーケンス番号を再割り当てするには、**resequence** コマンドを使用します。
start *time date*	（任意）デバイスが、時間範囲に関連付けられた **permit**（許可）ルールおよび **deny**（拒否）ルールの実行を開始する正確な日時を指定します。開始日時を指定しない場合、デバイスは **permit**（許可）ルールまたは **deny**（拒否）ルールを即座に実行します。 *time* 引数と *date* 引数の値についての詳細は、「使用上のガイドライン」の項を参照してください。
end *time date*	（任意）デバイスが、時間範囲に関連付けられた **permit**（許可）コマンドおよび **deny**（拒否）コマンドの実行を停止する正確な日時を指定します。終了日時を指定しない場合、デバイスは毎回、開始日時が過ぎた時点で **permit**（許可）ルールまたは **deny**（拒否）ルールを実行します。 *time* 引数と *date* 引数の値についての詳細は、「使用上のガイドライン」の項を参照してください。

デフォルト

なし

コマンド モード

時間範囲コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

デバイスは、すべての時間範囲ルールを現地時間で解釈します。

start キーワードおよび **end** キーワードの両方を省略すると、デバイスは絶対時間範囲が常にアクティブであると見なします。

time 引数は、*hours*:*minutes* または *hours*:*minutes*:*seconds* の形式で 24 時間表記で指定します。たとえば、24 時間表記では、午前 8:00 は 8:00、午後 8:00 は 20:00 です。

date 引数は、*day month year* の形式で指定します。最小有効開始日時は 00:00:00 1 January 1970、最大有効開始日時は 23:59:59 31 December 2037 です。

このコマンドには、ライセンスは必要ありません。

例

次に、2007 年 9 月 17 日の午前 7 時に開始され、2007 年 9 月 19 日の午後 11 時 59 分 59 秒に終了する絶対時間ルールを作成する例を示します。

```
switch# configure terminal
switch(config)# time-range conference-remote-access
switch(config-time-range)# absolute start 07:00 17 September 2007 end 23:59:59 19
September 2007
```

関連コマンド

コマンド	説明
periodic	定期的な時間範囲ルールを設定します。
time-range	IPv4 ACL または IPv6 ACL で使用される時間範囲を設定します。

accept-lifetime

別のデバイスとのキー交換時にデバイスがそのキーを受け入れる期間を指定するには、**accept-lifetime** コマンドを使用します。時間間隔を削除するには、このコマンドの **no** 形式を使用します。

accept-lifetime [**local**] *start-time* [**duration** *duration-value* | **infinite** | *end-time*]

no accept-lifetime [**local**] *start-time* [**duration** *duration-value* | **infinite** | *end-time*]

構文の説明

local	（任意）デバイスが、設定された時間をローカル時間として扱うように指定します。デフォルトでは、デバイスは *start-time* 引数および *end-time* 引数を UTC として扱います。
start-time	デバイスがキーの受け入れを開始する時刻と日付。 *start-time* 引数の値の詳細については、「使用上のガイドライン」を参照してください。
duration *duration-value*	（任意）ライフタイムの長さを秒単位で指定します。最大値は 2147483646 秒（約 68 年）です。
infinite	（任意）キーが期限切れにならないように指定します。
end-time	（任意）デバイスがキーの受け入れを停止する時刻と日付。 *time of day* 引数と *date* 引数の値についての詳細は、「使用上のガイドライン」の項を参照してください。

デフォルト

infinite

コマンド モード

キー コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、デバイスはすべての時間範囲のルールを UTC として扱います。

デフォルトでは、別のデバイスとのキー交換時にデバイスがキーを受け入れる期間（受け入れライフタイム）は infinite です。つまり、キーは常に有効です。

start-time 引数および *end-time* 引数の両方には、次の形式の時間と日付のコンポーネントが必要です。

hour[:*minute*[:*second*]] *month day year*

24 時間表記で指定します。たとえば、24 時間表記では、午前 8:00 は 8:00、午後 8:00 は 20:00 です。最小の有効な *start-time* 値は 00:00:00 Jan 1 1970 で、最大の有効な *start-time* 値は 23:59:59 Dec 31 2037 です。

このコマンドには、ライセンスは必要ありません。

例

次に、2008 年 6 月 13 日の午前零時に開始され、2008 年 8 月 12 日の午後 11 時 59 分 59 秒に終了する受け入れライフタイムを作成する例を示します。

```
switch# configure terminal
switch(config)# key chain glbp-keys
switch(config-keychain)# key 13
switch(config-keychain-key)# accept-lifetime 00:00:00 Jun 13 2008 23:59:59 Sep 12 2008
switch(config-keychain-key)#
```

関連コマンド

コマンド	説明
key	キーを設定します。
keychain	キーチェーンを設定します。
key-string	キーのストリングを設定します。
send-lifetime	キーの送信ライフタイムを設定します。
show key chain	キーチェーンの設定を表示します。

action

パケットが VLAN Access Control List（VACL; VLAN アクセス コントロール リスト）の **permit** コマンドと一致した場合にデバイスが実行する処理を指定するには、**action** コマンドを使用します。**action** コマンドを削除するには、このコマンドの **no** 形式を使用します。

action drop [**log**]

no action drop [**log**]

action forward

no action forward

action redirect {**ethernet** *slot*/*port* | **port-channel** *channel-number*.*subinterface-number*}

no action redirect {**ethernet** *slot*/*port* | **port-channel** *channel-number*.*subinterface-number*}

構文の説明

drop	デバイスがパケットをドロップするように指定します。
log	（任意）デバイスが、**drop** キーワードに基づいてドロップしたパケットを記録するように指定します。
forward	デバイスがパケットをその宛先ポートに転送するように指定します。
redirect	デバイスがパケットをインターフェイスにリダイレクトするように指定します。
ethernet *slot*/*port*	デバイスがパケットをリダイレクトするイーサネット インターフェイスを指定します。
port-channel *channel-number*.*subinterface-number*	デバイスがパケットをリダイレクトするポート チャネル インターフェイスを指定します。 **（注）** *channel-number* 引数と *subinterface-number* 引数との間には、ドット区切り文字が必要です。

デフォルト

なし

コマンド モード

VLAN アクセスマップ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

action コマンドでは、パケットが、**action** コマンドと同じアクセス マップ エントリ内の **match** コマンドによって指定された ACL 内の条件に一致した場合に、デバイスが実行する処理を指定します。

このコマンドには、ライセンスは必要ありません。

例

次の例では、vlan-map-01 という名前の VLAN アクセス マップを作成し、それぞれに 2 つの **match** コマンドと 1 つの **action** コマンドがある 2 つのエントリを追加する方法を示します。

```
switch(config-access-map)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# action forward
switch(config-access-map)# match mac address mac-acl-00f
switch(config-access-map)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-320
switch(config-access-map)# match mac address mac-acl-00e
switch(config-access-map)# action drop
switch(config-access-map)# show vlan access-map

Vlan access-map vlan-map-01 10
        match ip: ip-acl-01
        match mac: mac-acl-00f
        action: forward
Vlan access-map vlan-map-01 20
        match ip: ip-acl-320
        match mac: mac-acl-00e
        action: drop
```

関連コマンド

コマンド	説明
match	VLAN アクセス マップにトラフィック フィルタリングの ACL を指定します。
show vlan access-map	すべての VLAN アクセス マップまたは 1 つの VLAN アクセス マップを表示します。
show vlan filter	VLAN アクセス マップが適用されている方法に関する情報を表示します。
statistics	Access Control List（ACL; アクセス コントロール リスト）または VLAN アクセス マップの統計情報をイネーブルにします。
vlan access-map	VLAN アクセス マップを設定します。
vlan filter	1 つ以上の VLAN に VLAN アクセス マップを適用します。

arp access-list

アドレス解決プロトコル（ARP）ACL を作成するか、特定の ARP ACL の ARP アクセス リスト コンフィギュレーション モードを開始するには、**arp access-list** コマンドを使用します。ARP ACL を削除するには、このコマンドの **no** 形式を使用します。

arp access-list *access-list-name*

no arp access-list *access-list-name*

構文の説明

access-list-name	ARP ACL の名前。名前では最大 64 文字までの英数字を使用でき、大文字と小文字が区別されます。名前にはスペースまたは引用符を含めることはできません。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

DHCP スヌーピングを使用できない場合は、ARP ACL を使用して ARP トラフィックをフィルタリングします。

デフォルトでは、ARP ACL は定義されていません。

arp access-list コマンドを使用すると、デバイスによって ARP アクセス リスト コンフィギュレーション モードが開始されます。このモードでは、ARP **deny** コマンドおよび **permit** コマンドを使用して、ACL のルールを設定できます。指定した ACL が存在しない場合は、このコマンドの入力時に新しい ACL が作成されます。

ARP ACL を VLAN に適用するには、**ip arp inspection filter** コマンドを使用します。

このコマンドには、ライセンスは必要ありません。

例

次に、arp-acl-01 という名前の ARP ACL の ARP アクセス リスト コンフィギュレーション モードを開始する例を示します。

```
switch# conf t
switch(config)# arp access-list arp-acl-01
switch(config-arp-acl)#
```

関連コマンド

コマンド	説明
deny（ARP）	ARP ACL に拒否（deny）ルールを設定します。
ip arp inspection filter	VLAN に ARP ACL を適用します。
permit（ARP）	ARP ACL の許可ルールを設定します。
show arp access-lists	すべての ARP ACL または特定の ARP ACL を表示します。

authentication（LDAP）

Lightweight Directory Access Protocol（LDAP）認証でバインド（bind）方式または比較（compare）方式を使用するように設定するには、**authentication** コマンドを使用します。この設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

authentication {**bind-first** [**append-with-baseDN** *DNstring*] | **compare** [**password-attribute** *password*]}

no authentication {**bind-first** [**append-with-baseDN** *DNstring*] | **compare** [**password-attribute** *password*]}

構文の説明

bind-first	LDAP 認証方式を、最初にバインドに設定します。
append-with-baseDN *DNstring*	（任意）指定名（DN）文字列を指定します。最大 63 文字の英数字を入力できます。
compare	LDAP 認証方式を、比較に設定します。
password-attribute *password*	（任意）ユーザ パスワードを指定します。最大 63 文字の英数字を入力できます。

デフォルト

最初に検索してからバインドするバインド方式

コマンド モード

LDAP サーバ グループ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、比較方式を使用するように LDAP 認証を設定する例を示します。

```
switch# conf t
switch(config)# aaa group server ldap LDAPServer1
switch(config-ldap)# server 10.10.2.2
switch(config-ldap)# authentication compare password-attribute TyuL8r
switch(config-ldap)#
```

関連コマンド

コマンド	説明
aaa group server ldap	LDAP サーバ グループを作成し、そのグループの LDAP サーバ グループ コンフィギュレーション モードを開始します。
server	LDAP サーバを、LDAP サーバ グループのメンバとして設定します。
show ldap-server groups	LDAP サーバ グループの設定を表示します。