



## Cisco Nexus 3600 スイッチ NX-OS セキュリティ構成ガイド、リリース 10.5(x)

最終更新：2025 年 8 月 4 日

### シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】シスコ製品をご使用になる前に、安全上の注意（[www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/)）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: <https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html>. Cisco product warranty information is available at <https://www.cisco.com/c/en/us/products/warranty-listing.html>. US Federal Communications Commission Notices are found here <https://www.cisco.com/c/en/us/products/us-fcc-notice.html>.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.



## 目次

---

### はじめに :

#### はじめに xv

対象読者 xv

表記法 xv

Cisco Nexus 3000 シリーズ スイッチの関連資料 xvi

マニュアルに関するフィードバック xvii

通信、サービス、およびその他の情報 xvii

---

### 第 1 章

#### 新機能および変更された機能に関する情報 1

新機能および変更された機能に関する情報 1

---

### 第 2 章

#### 概要 3

ライセンス要件 3

Authentication, Authorization, and Accounting（認証、許可、およびアカウンティング） 3

RADIUS および TACACS+ セキュリティ プロトコル 4

SSH および Telnet 5

IP ACL 5

---

### 第 3 章

#### AAA の設定 7

AAA の概要 7

AAA セキュリティ サービス 7

AAA を使用する利点 8

リモート AAA サービス 8

AAA サーバグループ 8

AAA サービス設定オプション 9

|                                                |    |
|------------------------------------------------|----|
| ユーザー ログインの認証および許可プロセス                          | 10 |
| リモート AAA の前提条件                                 | 11 |
| AAA の注意事項と制約事項                                 | 12 |
| AAA の設定                                        | 12 |
| コンソール ログイン認証方式の設定                              | 12 |
| デフォルトのログイン認証方式の設定                              | 14 |
| ログイン認証失敗メッセージの有効化                              | 15 |
| 成功したログイン試行と失敗したログイン試行                          | 16 |
| AAA コマンド許可の設定                                  | 17 |
| MSCHAP 認証のイネーブル化                               | 19 |
| LDAP サーバでの AAA 許可の設定                           | 20 |
| TACACS サーバでの AAA SSH 証明書認証の構成                  | 22 |
| デフォルトの AAA アカウンティング方式の設定                       | 23 |
| No Service Password-Recovery について              | 25 |
| No Service Password-Recovery のイネーブル化           | 25 |
| AAA サーバーの VSA の使用                              | 27 |
| VSA                                            | 27 |
| VSA の形式                                        | 27 |
| AAA サーバー上でのスイッチのユーザー ロールと SNMPv3 パラメータの指定      | 27 |
| セキュア ログインの機能拡張                                 | 28 |
| セキュア ログインの機能拡張                                 | 28 |
| ログイン パラメータの設定                                  | 28 |
| ログイン パラメータの設定例                                 | 30 |
| ユーザー 1 人あたりのセッション数の制限（ユーザー 1 人あたり、ログイン 1 回あたり） | 30 |
| ユーザー名のパスワード プロンプトの有効化                          | 31 |
| RADIUS/TACACS+ を使用するための共有キー値の設定                | 32 |
| ローカル AAA アカウンティング ログのモニタリングとクリア                | 33 |
| AAA 設定の確認                                      | 33 |
| AAA の設定例                                       | 34 |
| デフォルトの AAA 設定                                  | 35 |

## 第 4 章

**RADIUS の設定 37**

## RADIUS の概要 37

## RADIUS ネットワーク環境 37

## RADIUS の操作について 38

## RADIUS サーバのモニタリング 39

## ベンダー固有属性 39

## RADIUS の前提条件 40

## RADIUS の注意事項と制約事項 40

## RadSec の注意事項と制約事項 41

## RADIUS サーバの設定 41

## RADIUS サーバ ホストの設定 42

## RADIUS のグローバルな事前共有キーの設定 43

## RADIUS サーバーの事前共有キーの設定 44

## RadSec の設定 46

## DTLS を使用した RADIUS について 47

## DTLS を使用する RADIUS の構成 48

## RADIUS サーバ グループの設定 49

## RADIUS サーバ グループのためのグローバル発信元インターフェイスの設定 51

## ログイン時にユーザによる RADIUS サーバの指定を許可 52

## グローバルな RADIUS 送信リトライ回数とタイムアウト間隔の設定 53

## RADIUS サーバのアカウンティングおよび認証属性の設定 54

## RADIUS サーバーの定期的モニタリングの設定 56

## デッドタイム間隔の設定 57

## RADIUS サーバまたはサーバ グループの手動モニタリング 58

## RADIUS 設定の確認 59

## RADIUS サーバー統計情報の表示 59

## RADIUS サーバ統計情報のクリア 60

## RADIUS の設定例 60

## RADIUS のデフォルト設定 61

## RADIUS の機能の履歴 61

## 第 5 章

**TACACS+ の設定 63**

TACACS+ の設定に関する情報 63

TACACS+ の利点 64

TACACS+ を使用したユーザー ログイン 64

デフォルトの TACACS+ サーバー暗号化タイプと事前共有キー 65

TACACS+ サーバのモニタリング 65

TACACS+ の前提条件 66

TACACS+ の注意事項と制約事項 66

TACACS+ の設定 66

TACACS+ サーバの設定プロセス 66

TACACS+ のイネーブル化 67

TACACS+ サーバホストの設定 68

TACACS+ のグローバルな事前共有キーの設定 69

TACACS+ サーバグループの設定 71

TACACS+ サーバグループのためのグローバル発信元インターフェイスの設定 72

グローバルな TACACS+ タイムアウト間隔の設定 73

サーバーのタイムアウト間隔の設定 74

TCP ポートの設定 75

TACACS+ サーバーの定期的モニタリングの設定 75

デッドタイム間隔の設定 77

TACACS+ サーバーを使用した X.509 証明書ベースの SSH 認証の設定 78

TACACS+ サーバまたはサーバグループの手動モニタリング 79

TACACS+ のディセーブル化 79

TACACS+ 統計情報の表示 80

TACACS+ の設定の確認 81

TACACS+ の設定例 81

TACACS+ のデフォルト設定 82

## 第 6 章

**LDAP の設定 83**

LDAP について 83

|                         |     |
|-------------------------|-----|
| LDAP 認証および許可            | 84  |
| ユーザ ログインにおける LDAP の動作   | 84  |
| LDAP サーバのモニタリング         | 85  |
| LDAP のベンダー固有属性          | 86  |
| LDAP 用の Cisco VSA 形式    | 86  |
| LDAP のバーチャライゼーション サポート  | 86  |
| LDAP の前提条件              | 86  |
| LDAP の注意事項と制約事項         | 87  |
| LDAP のデフォルト設定           | 87  |
| LDAP の設定                | 88  |
| LDAP サーバの設定プロセス         | 88  |
| LDAP のイネーブル化/ディセーブル化    | 89  |
| LDAP サーバ ホストの設定         | 90  |
| LDAP サーバの rootDN の設定    | 91  |
| LDAP サーバ グループの設定        | 92  |
| グローバルな LDAP タイムアウト間隔の設定 | 94  |
| LDAP サーバのタイムアウト間隔の設定    | 95  |
| TCP ポートの設定              | 96  |
| LDAP 検索マップの設定           | 98  |
| LDAP サーバの定期的モニタリングの設定   | 99  |
| LDAP デッド タイム間隔の設定       | 100 |
| LDAP サーバでの AAA 許可の設定    | 101 |
| LDAP SSH 公開キー認証の設定      | 103 |
| LDAP SSH 証明書許可の設定       | 103 |
| LDAP サーバのモニタリング         | 104 |
| LDAP サーバ統計情報のクリア        | 105 |
| LDAP 設定の確認              | 106 |
| LDAP の設定例               | 106 |
| 次の作業                    | 107 |

|                                        |     |
|----------------------------------------|-----|
| SSH および Telnet の概要                     | 109 |
| SSH サーバー                               | 109 |
| SSH クライアント                             | 109 |
| SSH サーバ キー                             | 110 |
| デジタル証明書を使用した SSH 認証                    | 110 |
| Telnet サーバ                             | 111 |
| SSH の注意事項および制約事項                       | 111 |
| SSH の設定                                | 111 |
| SSH サーバ キーの生成                          | 111 |
| ユーザ アカウント用 SSH 公開キーの指定                 | 112 |
| Open SSH 形式による SSH 公開キーの指定             | 113 |
| IETF SECSH 形式による SSH 公開キーの指定           | 114 |
| PEM フォーマット化された公開キー証明書形式による SSH 公開キーの指定 | 115 |
| SSH 送信元インターフェイスの構成                     | 116 |
| リモート デバイスとの SSH セッションの開始               | 116 |
| SSH ホストのクリア                            | 117 |
| SSH サーバのディセーブル化                        | 117 |
| SSH サーバ キーの削除                          | 118 |
| SSH セッションのクリア                          | 119 |
| SSH の設定例                               | 119 |
| X.509v3 証明書ベースの SSH 認証の設定              | 121 |
| X.509v3 証明書ベースの SSH 認証の設定例             | 123 |
| Telnet の設定                             | 124 |
| Telnet サーバのイネーブル化                      | 124 |
| Telnet サーバーの再イネーブル化                    | 124 |
| Telnet 送信元インターフェイスの構成                  | 125 |
| リモート デバイスとの Telnet セッションの開始            | 126 |
| Telnet セッションのクリア                       | 126 |
| SSH および Telnet の設定の確認                  | 127 |
| SSH のデフォルト設定                           | 127 |



## 第 8 章

## PKI の設定 129

## PKI の概要 129

## CA とデジタル証明書 129

## 信頼モデル、トラストポイント、アイデンティティ CA 130

## CA 証明書の階層 130

## CA バンドルのインポート 131

## PKCS7 形式での CA 証明書バンドルのインポート 131

## RSA のキー ペアとアイデンティティ証明書 133

## 複数の信頼できる CA のサポート 134

## PKI の登録のサポート 134

## カットアンドペーストによる手動での登録 135

## 複数の RSA キー ペアとアイデンティティ CA のサポート 135

## ピア証明書の検証 135

## 証明書の取消確認 136

## CRL のサポート 136

## NDcPP : syslog の OCSP 136

## 証明書と対応するキー ペアのインポートとエクスポート 136

## PKI の注意事項と制約事項 137

## PKI のデフォルト設定 137

## CA の設定とデジタル証明書 138

## ホスト名と IP ドメイン名の設定 138

## RSA キー ペアの生成 139

## ECC キー ペアの生成 141

## トラストポイント CA のアソシエーションの作成 142

## 証明書マッピングのフィルタの設定 144

## CA の認証 146

## 証明書取消確認方法の設定 148

## 証明書要求の作成 149

## アイデンティティ証明書のインストール 151

## トラストポイントの設定がリブート後も維持されていることの確認 152

|                                                   |     |
|---------------------------------------------------|-----|
| PKCS 12 形式でのアイデンティティ情報のエクスポート                     | 153 |
| PKCS 12 または PKCS 7 フォーマットで ID 情報のインポート            | 154 |
| CRL の設定                                           | 156 |
| CA の設定からの証明書の削除                                   | 157 |
| Cisco NX-OS デバイスからの RSA キー ペアの削除                  | 158 |
| PKI の設定の確認                                        | 159 |
| PKI の設定例                                          | 160 |
| Cisco NX-OS デバイスでの証明書の設定                          | 160 |
| CA 証明書のダウンロード                                     | 163 |
| アイデンティティ証明書の要求                                    | 169 |
| 証明書の取り消し                                          | 183 |
| CRL の作成と公開                                        | 186 |
| CRL のダウンロード                                       | 188 |
| CRL のインポート                                        | 193 |
| Resource Public Key Infrastructure (RPKI)         | 196 |
| RPKI 構成                                           | 196 |
| RPKI キャッシュに接続するためのコマンド                            | 196 |
| 受信プレフィックスを RPKI 検証状態でマークするためのコマンド                 | 197 |
| BGP 最適パス計算で RPKI 検証状態を使用するためのコマンド                 | 197 |
| route-map を使用して特定の検証状態を持つプレフィックスを削除または操作するためのコマンド | 198 |
| RPKI Show コマンド                                    | 198 |
| RPKI Clear コマンド                                   | 199 |
| RPKI Debug および Event History コマンド                 | 200 |

---

第 9 章

|                |     |
|----------------|-----|
| IP ACL の設定     | 201 |
| ACL の概要        | 201 |
| IP ACL のタイプと適用 | 202 |
| 適用順序           | 202 |
| ルール            | 202 |
| 送信元と宛先         | 203 |

Cisco Nexus 3600 スイッチ NX-OS セキュリティ構成ガイド、リリース 10.5(x)

|                          |     |
|--------------------------|-----|
| ACL ロギング構成の確認            | 233 |
| ACL TCAM リージョン サイズの設定    | 234 |
| デフォルトの TCAM リージョン サイズに戻す | 236 |
| 仮想端末回線の ACL の設定          | 237 |
| VTY 回線の ACL の確認          | 238 |
| VTY 回線の ACL の設定例         | 239 |

---

## 第 10 章

|                       |     |
|-----------------------|-----|
| ユニキャスト RPF の設定        | 241 |
| ユニキャスト RPF の概要        | 241 |
| ユニキャスト RPF プロセス       | 242 |
| グローバル統計               | 243 |
| ユニキャスト RPF の注意事項と制約事項 | 243 |
| ユニキャスト RPF のデフォルト設定   | 245 |
| ユニキャスト RPF の設定        | 245 |
| ユニキャスト RPF の設定例       | 247 |
| ユニキャスト RPF の設定の確認     | 247 |
| ユニキャスト RPF に関する追加情報   | 248 |

---

## 第 11 章

|                           |     |
|---------------------------|-----|
| コントロールプレーン ポリシングの設定       | 249 |
| CoPP について                 | 249 |
| コントロールプレーン保護              | 251 |
| コントロールプレーンのパケット タイプ       | 251 |
| CoPP の分類                  | 252 |
| レート制御メカニズム                | 252 |
| ダイナミックおよびスタティック CoPP ACL  | 252 |
| デフォルトのポリシング ポリシー          | 253 |
| モジュラ QoS コマンドライン インターフェイス | 266 |
| CoPP と管理インターフェイス          | 267 |
| CoPP の注意事項と制約事項           | 267 |
| CoPP のデフォルト設定             | 270 |
| CoPP の設定                  | 270 |

|                                           |     |
|-------------------------------------------|-----|
| コントロールプレーン クラス マップの設定                     | 270 |
| コントロールプレーン ポリシー マップの設定                    | 272 |
| コントロールプレーン サービス ポリシーの設定                   | 275 |
| ラインカードごとの CoPP のスケール ファクタの設定              | 276 |
| デフォルトの CoPP ポリシーの変更または再適用                 | 278 |
| CoPP ベストプラクティス ポリシーのコピー                   | 278 |
| CoPP の設定の確認                               | 279 |
| CoPP 設定ステータスの表示                           | 282 |
| CoPP のモニタリング                              | 282 |
| CoPP 統計情報のクリア                             | 283 |
| CoPP の設定例                                 | 284 |
| CoPP の設定例                                 | 284 |
| セットアップ ユーティリティによるデフォルト CoPP ポリシーの変更または再適用 | 285 |
| CoPP に関する追加情報                             | 286 |

## 第 12 章

### MACsec の設定 287

|                              |     |
|------------------------------|-----|
| MACsec の設定                   | 287 |
| MACsec について                  | 287 |
| キー ライフタイムおよびヒットレス キー ロールオーバー | 287 |
| フォールバック キー                   | 288 |
| MACSec の注意事項と制約事項            | 288 |
| MACsec の有効化                  | 291 |
| MACsec の無効化                  | 291 |
| MACsec キーチェーンとキーの設定          | 292 |
| MACsec フォールバック キーの設定         | 294 |
| MACsec ポリシーの設定               | 295 |
| PSK のローテーション                 | 297 |
| MACsec 設定の確認                 | 297 |
| MACsec 統計の表示                 | 300 |
| MACsec の設定例                  | 303 |
| XML の例                       | 305 |

[MIB](#) 319

[関連資料](#) 319



## はじめに

この前書きは、次の項で構成されています。

- [対象読者](#) (xv ページ)
- [表記法](#) (xv ページ)
- [Cisco Nexus 3000 シリーズ スイッチの関連資料](#) (xvi ページ)
- [マニュアルに関するフィードバック](#) (xvii ページ)
- [通信、サービス、およびその他の情報](#) (xvii ページ)

## 対象読者

このマニュアルは、Cisco Nexus スイッチの設置、設定、および維持に携わるネットワーク管理者を対象としています。

## 表記法

コマンドの説明には、次のような表記法が使用されます。

| 表記法           | 説明                                                     |
|---------------|--------------------------------------------------------|
| <b>bold</b>   | 太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。                   |
| <i>italic</i> | イタリック体の文字は、ユーザが値を入力する引数です。                             |
| [x]           | 省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。                   |
| [x   y]       | いずれか1つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。      |
| {x   y}       | 必ずいずれか1つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。 |

| 表記法         | 説明                                                                                                    |
|-------------|-------------------------------------------------------------------------------------------------------|
| [x {y   z}] | 角かっこまたは波かっこが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角かっこ内の波かっこと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。 |
| variable    | ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。                                                        |
| string      | 引用符を付けない一組の文字。 <b>string</b> の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて <b>string</b> とみなされます。               |

例では、次の表記法を使用しています。

| 表記法                        | 説明                                                   |
|----------------------------|------------------------------------------------------|
| screen フォント                | スイッチが表示する端末セッションおよび情報は、スクリーンフォントで示しています。             |
| 太字の <b>screen</b> フォント     | ユーザが入力しなければならない情報は、太字のスクリーンフォントで示しています。              |
| イタリック体の <i>screen</i> フォント | ユーザが値を指定する引数は、イタリック体の <b>screen</b> フォントで示しています。     |
| <>                         | パスワードのように出力されない文字は、山カッコ (<>) で囲んで示しています。             |
| []                         | システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。              |
| !、#                        | コードの先頭に感嘆符 (!) またはポンド記号 (#) がある場合には、コメント行であることを示します。 |

## Cisco Nexus 3000 シリーズ スイッチの関連資料

Cisco Nexus 3000 シリーズ スイッチ全体のマニュアルセットは、次の URL にあります。

<https://www.cisco.com/c/en/us/support/switches/nexus-3000-series-switches/tsd-products-support-series-home.html>



## マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバック フォームよりご連絡ください。ご協力をよろしくお願いいたします。

## 通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、[Cisco Profile Manager](#) でサインアップしてください。
- 重要な技術によって求めるビジネス成果を得るには、[Cisco Services](#) [英語] にアクセスしてください。
- サービスリクエストを送信するには、[Cisco Support](#) [英語] にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、[Cisco DevNet](#) [英語] にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) [英語] にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#) にアクセスしてください。

### シスコバグ検索ツール

[シスコバグ検索ツール](#) (BST) は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。





# 第 1 章

## 新機能および変更された機能に関する情報

- [新機能および変更された機能に関する情報 \(1 ページ\)](#)

## 新機能および変更された機能に関する情報

表 1: 新機能および変更された機能

| 特長                       | 説明                                                                       | 変更が行われたリリース | 参照先                                                                               |
|--------------------------|--------------------------------------------------------------------------|-------------|-----------------------------------------------------------------------------------|
| RSA キー サイズを 4096 ビットに増やす | RSA キー サイズのサポートが、SSH の場合は 4096 ビット、暗号化証明書の場合は 3072 および 4096 ビットに拡張されました。 | 10.5 (2) F  | <a href="#">SSH サーバ キーの生成 (111 ページ)</a><br><a href="#">RSA キー ペアの生成 (139 ページ)</a> |
| N/A                      | このリリースの機能更新はありません。                                                       | 10.5(1)F    | N/A                                                                               |





## 第 2 章

### 概要

Cisco NX-OS ソフトウェアがサポートするセキュリティ機能を利用すると、ネットワークをパフォーマンスの劣化や障害から保護するだけでなく、故意に行われる攻撃や、善意のネットワークユーザの意図しない危険な間違いにより生ずるデータの紛失または毀損に対しても保護できます。

- [ライセンス要件 \(3 ページ\)](#)
- [Authentication, Authorization, and Accounting \(認証、許可、およびアカウントティング\)](#) , on page 3
- [RADIUS および TACACS+ セキュリティ プロトコル](#), on page 4
- [SSH および Telnet](#), on page 5
- [IP ACL](#), on page 5

### ライセンス要件

Cisco NX-OS ライセンス方式の推奨の詳細と、ライセンスの取得および適用の方法については、『[Cisco NX-OS ライセンス ガイド](#)』および『[Cisco NX-OS ライセンス オプション ガイド](#)』を参照してください。

## Authentication, Authorization, and Accounting (認証、許可、およびアカウントティング)

認証、許可、アカウントティング (AAA) は、3つの独立したセキュリティ機能をまとめて一貫性のあるモジュラ形式で設定するためのアーキテクチャ フレームワークです。

#### 認証

ログイン/パスワードダイアログ、チャレンジ/レスポンス、メッセージングサポート、および暗号化（選択したセキュリティプロトコルに基づく）などによるユーザの識別方法を提供します。認証は、ユーザに対してネットワークとネットワークサービスへのアクセスを許可する前に、ユーザの識別を行う方法です。AAA 認証を設定するには、まず認証方式の名前付きリストを定義し、そのリストを各種インターフェイスに適用します。

## 許可

ワンタイム許可またはサービスごとの許可、ユーザ単位のアカунトリストとプロフィール、ユーザグループサポート、および IP、IPX、ARA、Telnet のサポートなど、リモートアクセスの制御方法を提供します。

RADIUS や TACACS+ などのリモート セキュリティ サーバは、適切なユーザで該当する権利を定義した属性値 (AV) のペアをアソシエートすることによって、ユーザに特定の権限を付与します。AAA 許可は、ユーザが何を実行する権限を与えられるかを表す一連の属性を組み立てることで機能します。これらの属性とデータベースに格納されているユーザの情報とが比較され、その結果が AAA に返されてユーザの実際の権限と制限事項が決定されます。

## アカウンティング

ユーザ ID、開始時刻と終了時刻、実行コマンド (PPP など)、パケット数、バイト数といった、課金、監査、およびレポートに使用するセキュリティサーバ情報の収集と送信を行う手段を提供します。アカウンティングを使用することで、ユーザがアクセスしているサービスや、ユーザが消費しているネットワーク リソース量を追跡できます。



### Note

認証は AAA と別個に設定することができます。ただし RADIUS または TACACS+ を使用する場合や、バックアップの認証方式を設定する場合は、AAA を設定する必要があります。

# RADIUS および TACACS+ セキュリティ プロトコル

AAA は、セキュリティ機能の管理にセキュリティ プロトコルを使用します。ルータまたはアクセスサーバがネットワーク アクセスサーバとして動作している場合は、ネットワーク アクセスサーバと RADIUS または TACACS+ セキュリティサーバとの間の通信を確立する手段に、AAA が使用されます。

このマニュアルでは、次のセキュリティサーバ プロトコルを設定する手順を説明します。

## RADIUS

不正アクセスからネットワークを保護する分散型クライアント/サーバシステムです。RADIUS は AAA を使用して実装されます。シスコの実装では RADIUS クライアントは Cisco ルータ上で稼働します。認証要求は、すべてのユーザ認証情報とネットワーク サービス アクセス情報が格納されている中央の RADIUS サーバに送信されます。

## TACACS+

ルータまたはネットワーク アクセスサーバにアクセスしようとするユーザの検証を集中的に行うセキュリティ アプリケーションです。TACACS+ は AAA を使用して実装されます。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で動作する TACACS+ デーモンのデータベースで管理されます。TACACS+ では、独立したモジュラ型の認証、許可、アカウンティング機能が提供されます。

## SSH および Telnet

セキュアシェル (SSH) サーバーを使用すると、SSH クライアントは Cisco NX-OS デバイスとの間でセキュアな暗号化された接続を確立できます。SSH は強化暗号化を使用して認証を行います。Cisco NX-OS ソフトウェアの SSH サーバーは、市販の一般的な SSH クライアントと相互運用ができます。

Cisco NX-OS ソフトウェアの SSH クライアントは、市販の一般的な SSH クライアントと相互運用ができます。

Telnet プロトコルは、ホストとの TCP/IP 接続を確立します。Telnet を使用すると、あるサイトのユーザが別のサイトのログインサーバと TCP 接続を確立し、キーストロークをデバイス間でやり取りできます。Telnet は、リモート デバイス アドレスとして IP アドレスまたはドメイン名のいずれかを受け入れます。

## IP ACL

IP ACL は、トラフィックをパケットのレイヤ 3 ヘッダーの IPv4 情報に基づいてフィルタリングするために使用できるルールの順序セットです。各ルールには、パケットがルールに一致するために満たさなければならない条件のセットが規定されています。Cisco NX-OS ソフトウェアがパケットに IP ACL を適用することを判定するときは、すべてのルールの条件に照らしてパケットを調べます。最初の一致によってパケットを許可するか拒否するか判定します。一致するものがない場合は、Cisco NX-OS ソフトウェアは適切なデフォルトルールを適用します。Cisco NX-OS ソフトウェアは、許可されたパケットの処理を継続し、拒否されたパケットをドロップします。







## 第 3 章

# AAA の設定

この章では、Cisco NX-OS デバイスで認証、許可、アカウンティング（AAA）を設定する手順について説明します。

- [AAA の概要（7 ページ）](#)
- [リモート AAA の前提条件, on page 11](#)
- [AAA の注意事項と制約事項（12 ページ）](#)
- [AAA の設定（12 ページ）](#)
- [ローカル AAA アカウンティング ログのモニタリングとクリア , on page 33](#)
- [AAA 設定の確認, on page 33](#)
- [AAA の設定例, on page 34](#)
- [デフォルトの AAA 設定, on page 35](#)

## AAA の概要

### AAA セキュリティ サービス

認証、許可、アカウンティング（AAA）機能では、Cisco Nexus デバイスを管理するユーザーの ID 確認、アクセス権付与、およびアクション追跡を実行できます。Cisco Nexus デバイスは、Remote Access Dial-In User Service（RADIUS）プロトコルまたは Terminal Access Controller Access Control device Plus（TACACS+）プロトコルをサポートします。

ユーザーが入力したユーザー ID とパスワードに基づいて、スイッチは、ローカルデータベースを使用してローカル認証/ローカル許可を実行するか、1 つまたは複数の AAA サーバーを使用してリモート認証/リモート許可を実行します。スイッチと AAA サーバー間の通信は、事前共有秘密キーによって保護されます。すべての AAA サーバ用または特定の AAA サーバ専用

に共通秘密キーを設定できます。

AAA セキュリティは、次のサービスを実行します。

- **認証**：ユーザーを識別します。選択したセキュリティプロトコルに応じて、ログインとパスワードのダイアログ、チャレンジ/レスポンス、メッセージング サポート、暗号化などが行われます。

- 許可：アクセス コントロールを実行します。

Cisco Nexus デバイスにアクセスする許可は、AAA サーバーからダウンロードされる属性によって提供されます。RADIUS や TACACS+ などのリモートセキュリティサーバーは、適切なユーザーで該当する権利を定義した属性値 (AV) のペアをアソシエートすることによって、ユーザーに特定の権限を付与します。

- アカウンティング：課金、監査、レポートのための情報収集、ローカルでの情報のログイン、および AAA サーバーへの情報の送信の方式を提供します。

**Note**

Cisco NX-OS ソフトウェアは、認証、許可、アカウンティングをそれぞれ個別にサポートします。たとえば、アカウンティングは設定せずに、認証と許可を設定したりできます。

## AAA を使用する利点

AAA は、次のような利点を提供します。

- アクセス設定の柔軟性と制御性の向上
- 拡張性
- 標準化された認証方式 (RADIUS、TACACS+ など)
- 複数のバックアップ デバイス

## リモート AAA サービス

RADIUS プロトコルおよび TACACS+ プロトコルを介して提供されるリモート AAA サービスには、ローカル AAA サービスと比べて次のような利点があります。

- ファブリック内の各スイッチに関するユーザーパスワードリストを簡単に管理できます。
- AAA サーバーはすでに企業内に幅広く導入されており、簡単に AAA サービスに使用できます。
- ファブリック内のすべてのスイッチのアカウンティング ログを集中管理できます。
- スイッチ上のローカルデータベースを使用する方法に比べて、ファブリック内の各スイッチのユーザー属性は管理が簡単です。

## AAA サーバグループ

認証、許可、アカウンティングのためのリモート AAA サーバは、サーバグループを使用して指定できます。サーバグループとは、同じ AAA プロトコルを実装した一連のリモート AAA サーバーです。リモート AAA サーバーが応答しなかった場合、サーバグループは、フェールオーバー サーバーを提供します。グループ内の最初のリモート サーバーが応答しなかった

場合、いずれかのサーバーが応答を送信するまで、グループ内の次のリモートサーバーで試行が行われます。サーバー グループ内のすべての AAA サーバーが応答しなかった場合、そのサーバー グループ オプションには障害が発生しているものと見なされます。必要に応じて、複数のサーバー グループを指定できます。スイッチが最初のグループ内のサーバーからエラーを受信すると、次のサーバー グループのサーバーが試行されます。

## AAA サービス設定オプション

Cisco Nexus デバイスでは、次のサービスに個別の AAA 設定を使用できます。

- User Telnet または Secure Shell (SSH) ログイン認証
- コンソール ログイン認証
- ユーザー管理セッション アカウンティング

次の表に、AAA サービス設定オプションの CLI コマンドを示します。

**Table 2: AAA サービス コンフィギュレーション コマンド**

| AAA サービス コンフィギュレーション オプション | 関連コマンド                                  |
|----------------------------|-----------------------------------------|
| Telnet または SSH ログイン        | <b>aaa authentication login default</b> |
| コンソール ログイン                 | <b>aaa authentication login console</b> |
| ユーザー セッション アカウンティング        | <b>aaa accounting default</b>           |

AAA サービスには、次の認証方式を指定できます。

- RADIUS サーバー グループ : RADIUS サーバーのグローバルプールを認証に使用します。
- 特定のサーバー グループ : 指定した RADIUS または TACACS+ サーバー グループを認証に使用します。
- ローカル : ユーザー名またはパスワードのローカル データベースを認証に使用します。
- なし : ユーザー名だけを使用します。



### Note

方式がすべて RADIUS サーバーになっており、特定のサーバー グループが指定されていない場合、Cisco Nexus デバイスは、設定されている RADIUS サーバーのグローバル プールから、設定された順序で RADIUS サーバーを選択します。このグローバルプールからのサーバーは、Cisco Nexus デバイス上の RADIUS サーバー グループ内で選択的に設定できるサーバーです。

次の表に、AAA サービスに対して設定できる AAA 認証方式を示します。

Table 3: AAA サービスの AAA 認証方式

| AAA サービス             | AAA の方式         |
|----------------------|-----------------|
| コンソール ログイン認証         | サーバグループ、ローカル、なし |
| ユーザー ログイン認証          | サーバグループ、ローカル、なし |
| ユーザー管理セッション アカウンティング | サーバグループ、ローカル    |



**Note** コンソール ログイン認証、ユーザー ログイン認証、およびユーザー管理セッション アカウンティングでは、Cisco Nexus デバイスは、各オプションを指定された順序で試行します。その他の設定済みオプションが失敗した場合、ローカル オプションがデフォルト方式です。

## ユーザー ログインの認証および許可プロセス

ユーザー ログインの認証および許可プロセスは、次のように実行されます。

- 目的のCisco Nexus デバイスにログインする際、Telnet、SSH、Fabric Manager または Device Manager、コンソール ログインのいずれかのオプションを使用できます。
- サーバー グループ認証方式を使用して AAA サーバー グループが設定してある場合は、Cisco Nexus デバイスが、グループ内の最初の AAA サーバーに認証要求を送信し、次のように処理されます。

その AAA サーバーが応答しなかった場合、リモートのいずれかの AAA サーバーが認証要求に応答するまで、試行が継続されます。

サーバー グループのすべての AAA サーバーが応答しなかった場合、その次のサーバー グループのサーバーが試行されます。

設定されているすべての認証方式が失敗した場合、ローカルデータベースを使用して認証が実行されます。

- Cisco Nexus デバイスがリモート AAA サーバーで正常に認証できた場合は、次の条件が適用されます。

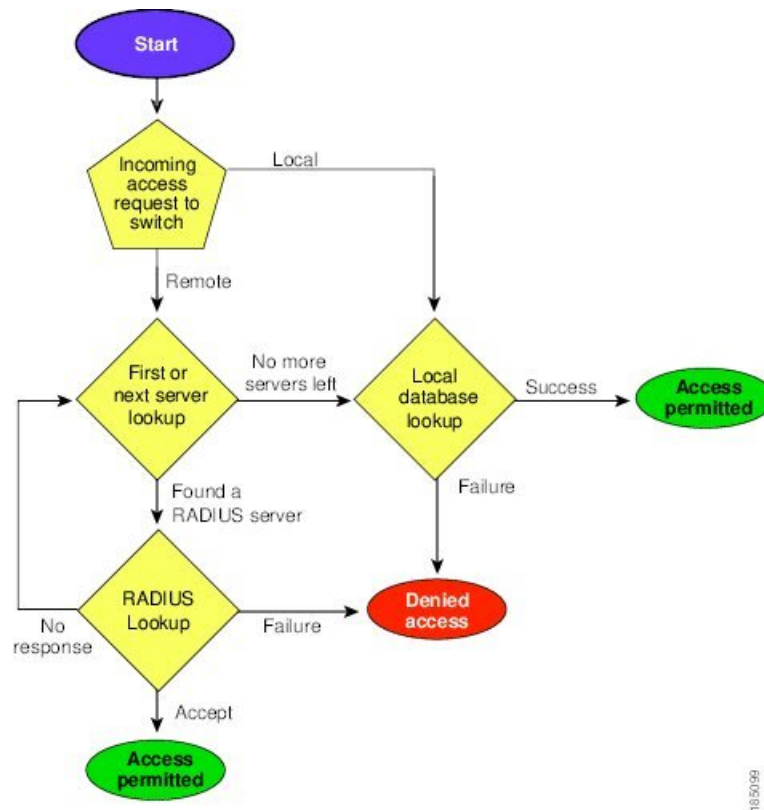
AAA サーバー プロトコルが RADIUS の場合、cisco-av-pair 属性で指定されているユーザー ロールが認証応答とともにダウンロードされます。

AAA サーバー プロトコルが TACACS+ の場合、シェルのカスタム属性として指定されているユーザー ロールを取得するために、もう 1 つの要求が同じサーバーに送信されます。

- ユーザー名とパスワードがローカルで正常に認証された場合は、Cisco Nexus デバイスにログインでき、ローカル データベース内で設定されているロールが割り当てられます。

次の図に、認証および許可プロセスのフロー チャートを示します。

Figure 1: ユーザー ログインの認証および許可のフロー



**Note** この図は、ユーザー名パスワード SSH 認証にのみ適用されます。公開キー SSH 認証には適用されません。すべてのユーザー名、パスワード、SSH 認証は AAA を通過します。

この図に示されている「残りのサーバーなし」とは、現在のサーバー グループ内のいずれのサーバーからも応答がないということです。

## リモート AAA の前提条件

リモート AAA サーバには、次の前提条件があります。

- 少なくとも 1 台の RADIUS サーバーまたは TACACS+ サーバーが、IP で到達可能であること。
- Cisco Nexus デバイスが AAA サーバーのクライアントとして設定されている。
- 事前に共有された秘密キーが Cisco Nexus デバイス上およびリモート AAA サーバー上で設定されている。
- リモート サーバーが Cisco Nexus デバイスからの AAA 要求に応答する。

## AAA の注意事項と制約事項

そのユーザー名が TACACS+ または RADIUS で作成されたのか、ローカルで作成されたのかに関係なく、Cisco Nexus デバイスでは、すべて数値のユーザー名はサポートされません。AAA サーバーに数字だけのユーザー名が存在し、ログイン時にその名前を入力した場合でも、ユーザーは Cisco Nexus デバイスにログインを許可されます。

AAA ログイン認証のデフォルト グループ TACACS-SERVER-GROUP を構成すると、コンソールのログインも上書きされます。このオーバーライドは、**aaa authentication login console local** がスイッチのデフォルト コマンドである場合でも発生します。これを防ぐには、**aaa authentication login console local** を構成する必要があります。



**注意** すべて数字のユーザー名でユーザー アカウントを作成しないでください。

## AAA の設定

### コンソール ログイン認証方式の設定

認証方式には、次のものがあります。

- RADIUS サーバのグローバル プール
- RADIUS サーバーまたは TACACS+ サーバーの名前付きサブセット
- Cisco Nexus デバイス上のローカル データベース
- ユーザー名だけ **none**

デフォルトの方式は、ローカルです。



**Note** 事前に設定されている一連の RADIUS サーバーに関しては、**aaa authentication** コマンドの **group radius** 形式および **group server-name** 形式を使用します。ホストサーバーを設定するには、**radius server-host** コマンドを使用します。サーバーの名前付きグループを作成するには、**aaa group server radius** コマンドを使用します。



**Note** AAA ログイン認証のデフォルト グループ TACACS-SERVER-GROUP を構成すると、コンソールのログインも上書きされます。このオーバーライドは、**aaa authentication login console local** がスイッチのデフォルト コマンドである場合でも発生します。これを防ぐには、**aaa authentication login console local** を構成する必要があります。

必要に応じて、コンソール ログイン認証方式を設定する前に RADIUS または TACACS+ サーバー グループを設定します。

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **aaa authentication login console { group group-list [none] | local | none}**
3. switch(config)# **exit**
4. (Optional) switch# **show aaa authentication**
5. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

### Procedure

|        | Command or Action                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|---------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                                                                 | グローバル コンフィギュレーション モードを開始します。                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| ステップ 2 | switch(config)# <b>aaa authentication login console { group group-list [none]   local   none}</b> | <p>コンソールのログイン認証方式を設定します。</p> <p><i>group-list</i> 引数には、グループ名をスペースで区切ったリストを指定します。グループ名は、次のように指定します。</p> <ul style="list-style-type: none"> <li>• <b>radius</b> RADIUS サーバーのグローバル プールを使用して認証を行います。</li> <li>• <b>named-group</b> を指定すると、TACACS+ サーバーまたは RADIUS サーバーの名前付きサブセットが認証に使用されます。</li> </ul> <p><b>local</b> 方式では、ローカル データベースが認証に使用されます。<b>none</b> 方式では、ユーザー名だけが使用されます。</p> <p>デフォルトのコンソール ログイン方式は、<b>local</b> です。これは認証方式が何も設定されていない場合、または設定された認証方式すべてについて応答が得られなかった場合に使用されます。</p> |
| ステップ 3 | switch(config)# <b>exit</b>                                                                       | グローバル コンフィギュレーション モードを終了します。                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| ステップ 4 | (Optional) switch# <b>show aaa authentication</b>                                                 | コンソール ログイン認証方式の設定を表示します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| ステップ 5 | (Optional) switch# <b>copy running-config startup-config</b>                                      | 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。                                                                                                                                                                                                                                                                                                                                                                                                                                                |

### Example

次に、コンソール ログインの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
switch(config)# exit
switch# show aaa authentication
switch# copy running-config startup-config
```

## デフォルトのログイン認証方式の設定

デフォルトの方式は、ローカルです。

必要に応じて、デフォルトのログイン認証方式を設定する前に RADIUS または TACACS+ サーバー グループを設定します。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **aaa authentication login default { group group-list [none] | local | none}**
3. switch(config)# **exit**
4. (Optional) switch# **show aaa authentication**
5. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

#### Procedure

|        | Command or Action                                                                                 | Purpose                                                                                                                                                                                                                                                                                      |
|--------|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                                                                 | グローバル コンフィギュレーション モードを開始します。                                                                                                                                                                                                                                                                 |
| ステップ 2 | switch(config)# <b>aaa authentication login default { group group-list [none]   local   none}</b> | <p>デフォルト認証方式を設定します。</p> <p><i>group-list</i> 引数には、グループ名をスペースで区切ったリストを指定します。グループ名は、次のように指定します。</p> <ul style="list-style-type: none"> <li>• <b>radius</b> RADIUS サーバーのグローバル プールを使用して認証を行います。</li> <li>• <b>named-group</b> を指定すると、TACACS+ サーバーまたは RADIUS サーバーの名前付きサブセットが認証に使用されます。</li> </ul> |



|        | Command or Action                                            | Purpose                                                                                                                                                                 |
|--------|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        |                                                              | <b>local</b> 方式では、ローカル データベースが認証に使用されます。 <b>none</b> 方式では、ユーザー名だけが使用されます。<br><br>デフォルトのログイン方式は <b>local</b> です。この方式は、方式が一切設定されていない場合、または設定済みのどの方式でも応答が得られなかった場合に使用されます。 |
| ステップ 3 | switch(config)# <b>exit</b>                                  | コンフィグレーション モードを終了します。                                                                                                                                                   |
| ステップ 4 | (Optional) switch# <b>show aaa authentication</b>            | デフォルトのログイン認証方式の設定を表示します。                                                                                                                                                |
| ステップ 5 | (Optional) switch# <b>copy running-config startup-config</b> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                                                                                               |

## ログイン認証失敗メッセージの有効化

ユーザーがログインして、リモート AAA サーバーが応答しなかった場合は、ローカル ユーザーデータベースによってログインが処理されます。ログイン失敗メッセージの表示をイネーブルにしていた場合は、次のような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.
```

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **aaa authentication login error-enable**
3. switch(config)# **exit**
4. (Optional) switch# **show aaa authentication**
5. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

#### Procedure

|        | Command or Action                                            | Purpose                                    |
|--------|--------------------------------------------------------------|--------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                            | グローバル コンフィギュレーション モードを開始します。               |
| ステップ 2 | switch(config)# <b>aaa authentication login error-enable</b> | ログイン認証失敗メッセージを有効にします。デフォルトではディセーブルになっています。 |
| ステップ 3 | switch(config)# <b>exit</b>                                  | コンフィグレーション モードを終了します。                      |

|        | Command or Action                                            | Purpose                                   |
|--------|--------------------------------------------------------------|-------------------------------------------|
| ステップ 4 | (Optional) switch# <b>show aaa authentication</b>            | ログイン失敗メッセージの設定を表示します。                     |
| ステップ 5 | (Optional) switch# <b>copy running-config startup-config</b> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。 |

## 成功したログイン試行と失敗したログイン試行

成功したログイン試行と失敗したログイン試行をすべて、設定されたsyslogサーバに記録するようにスイッチを設定できます。

### 手順の概要

1. **configure terminal**
2. **[no] login on-failure log**
3. **[no] login on-success log**
4. (任意) **show login on-failure log**
5. (任意) **show login on-successful log**
6. (任意) **copy running-config startup-config**

### 手順の詳細

#### 手順

|        | コマンドまたはアクション                                                                                  | 目的                                                                                                                                                                                                                                                                                                                       |
|--------|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例：<br>switch# <b>configure terminal</b>                      | グローバル設定モードを開始します。                                                                                                                                                                                                                                                                                                        |
| ステップ 2 | 必須: <b>[no] login on-failure log</b><br><br>例：<br>switch(config)# <b>login on-failure log</b> | 失敗した認証に関するすべてのメッセージを構成済みの syslog サーバーに記録します。この設定では、ログイン失敗後に次のsyslogメッセージが表示されます。<br><br>AUTHPRIV-3-SYSTEM_MSG : pam_aaa :<br>Authentication failed for user admin from 172.22.00.00<br><br>(注)<br>ログインレベル authpriv が 6 の場合、追加の Linux カーネル認証メッセージが以前のメッセージとともに表示されます。これらの追加のメッセージを無視する必要がある場合、authpriv 値を 3 に設定する必要があります。 |

|        | コマンドまたはアクション                                                                                                               | 目的                                                                                                                                                                                                                                                                             |
|--------|----------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 3 | 必須: <b>[no] login on-success log</b><br><br>例 :<br><pre>switch(config)# login on-success log</pre>                         | 成功した認証に関するすべてのメッセージを構成済みの syslog サーバーに記録します。この設定では、ログインに成功すると次の syslog メッセージが表示されます。<br><br><b>AUTHPRIV-6-SYSTEM_MSG : pam_aaa : Authentication success for user admin from 172.22.00.00</b><br><br>(注)<br>ログイン レベル authpriv が 6 の場合、追加の Linux カーネル認証メッセージが以前のメッセージとともに表示されます。 |
| ステップ 4 | (任意) <b>show login on-failure log</b><br><br>例 :<br><pre>switch(config)# show login on-failure log</pre>                   | 失敗した認証メッセージを syslog サーバに記録するようにスイッチが設定されているかどうかを表示します。                                                                                                                                                                                                                         |
| ステップ 5 | (任意) <b>show login on-successful log</b><br><br>例 :<br><pre>switch(config)# show login on-successful log</pre>             | 成功した認証メッセージを syslog サーバに記録するようにスイッチが設定されているかどうかを表示します。                                                                                                                                                                                                                         |
| ステップ 6 | (任意) <b>copy running-config startup-config</b><br><br>例 :<br><pre>switch(config)# copy running-config startup-config</pre> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                                                                                                                                                                                                      |

## AAA コマンド許可の設定

TACACS+ サーバーの許可方式が構成されている場合は、ユーザーが TACACS+ サーバーで実行するすべてのコマンド（すべての EXEC モード コマンドおよびすべての構成モード コマンドを含む）を許可できます。

許可方式には、次のものがあります。

- Group : TACACS+ サーバー グループ
- Local : ローカル ロールベース許可
- None : 許可は実行されません

デフォルトの方式は、Local です。



(注) コンソール セッションでは承認は行えません。

## 始める前に

AAA コマンドの許可を設定する前に、TACACS+ をイネーブルにする必要があります。

## 手順の概要

1. **configure terminal**
2. **aaa authorization {commands | config-commands} {default} {[ group group-name] | [ local]} | {[ group group-name] | [ none]}**

## 手順の詳細

## 手順

|        | コマンドまたはアクション                                                                                                                                                                                                                                                                                         | 目的                                                                                                                                                                                                       |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br><pre>switch# configure terminal switch(config)#</pre>                                                                                                                                                                                                            | グローバル コンフィギュレーション モードを開始します。                                                                                                                                                                             |
| ステップ 2 | <b>aaa authorization {commands   config-commands} {default} {[ group group-name]   [ local]}   {[ group group-name]   [ none]}</b><br>例 :<br><pre>switch(config)# aaa authorization config-commands default group tac1</pre> 例 :<br><pre>switch# aaa authorization commands default group tac1</pre> | 許可パラメータを設定します。<br>EXEC モード コマンドを許可するには、 <b>commands</b> キーワードを使用します。<br>構成モード コマンドを許可するには、 <b>config-commands</b> キーワードを使用します。<br>許可方式を指定するには、 <b>group</b> 、 <b>local</b> 、または <b>none</b> キーワードを使用します。 |

## 例

次に、TACACS+ サーバー グループ *tac1* で EXEC モード コマンドを許可する例を示します。

```
switch# aaa authorization commands default group tac1
```

次に、TACACS+ サーバー グループ *tac1* でコンフィギュレーション モード コマンドを許可する例を示します。

```
switch(config)# aaa authorization config-commands default group tac1
```

次に、TACACS+ サーバー グループ *tac1* でコンフィギュレーション モード コマンドを許可する例を示します。

- サーバーが到達可能である場合、コマンドはサーバー応答に基づいて許可され、または許可されません。
- サーバーに到達する際にエラーが生じた場合、コマンドはユーザーのローカルロールに基づいて許可されます。

```
switch(config)# aaa authorization config-commands default group tac1 local
```

次に、TACACS+ サーバー グループ *tac1* でコンフィギュレーション モード コマンドを許可する例を示します。

- サーバーが到達可能である場合、コマンドはサーバー応答に基づいて許可され、または許可されません。
- サーバーに到達する際にエラーが生じた場合は、ローカル ロールにかかわらずコマンドを許可します。

```
switch# aaa authorization commands default group tac1 none
```

次に、ローカル ロールにかかわらず EXEC モード コマンドを許可する例を示します。

```
switch# aaa authorization commands default none
```

次に、ローカル ロールを使用して EXEC モード コマンドを許可する例を示します。

```
switch# aaa authorization commands default local
```

## MSCHAP 認証のイネーブル化

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 (MSCHAP) は、マイクロソフト 版の CHAP です。リモート 認証サーバー (RADIUS または TACACS+) を通じて、Cisco Nexus デバイスへのユーザー ログインに MSCHAP を使用できます。

デフォルトでは、Cisco Nexus デバイスはスイッチとリモート サーバーの間でパスワード 認証 プロトコル (PAP) 認証を使用します。MSCHAP がイネーブルの場合は、MSCHAP VSA (Vendor-Specific Attribute; ベンダー固有属性) を認識するように RADIUS サーバーを設定する必要があります。

次の表に、MSCHAP に必要な RADIUS VSA を示します。

Table 4: MSCHAP RADIUS VSA

| ベンダー ID<br>番号 | ベンダー タ<br>イプ番号 | VSA              | 説明                                                                                                |
|---------------|----------------|------------------|---------------------------------------------------------------------------------------------------|
| 311           | 11             | MSCHAP-Challenge | AAA サーバーから MSCHAP ユーザーに送信されるチャレンジを保持します。これは、Access-Request パケットと Access-Challenge パケットの両方で使用できます。 |
| 211           | 11             | MSCHAP-Response  | チャレンジに対する応答として MSCHAP ユーザーが入力した値を保持します。Access-Request パケットでしか使用されません。                             |

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **aaa authentication login mschap enable**
3. switch(config)# **exit**
4. (Optional) switch# **show aaa authentication login mschap**
5. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

## Procedure

|        | Command or Action                                              | Purpose                                    |
|--------|----------------------------------------------------------------|--------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                              | グローバル コンフィギュレーション モードを開始します。               |
| ステップ 2 | switch(config)# <b>aaa authentication login mschap enable</b>  | MS-CHAP 認証をイネーブルにします。デフォルトではディセーブルになっています。 |
| ステップ 3 | switch(config)# <b>exit</b>                                    | コンフィギュレーション モードを終了します。                     |
| ステップ 4 | (Optional) switch# <b>show aaa authentication login mschap</b> | MS-CHAP 設定を表示します。                          |
| ステップ 5 | (Optional) switch# <b>copy running-config startup-config</b>   | 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。 |

## LDAP サーバでの AAA 許可の設定

LDAP サーバのデフォルトの AAA 許可方式を設定できます。

**Before you begin**

LDAP を有効にします。

**SUMMARY STEPS**

1. **configure terminal**
2. **aaa authorization ssh-certificate default { group group-list [none] | local | none}**
3. **exit**
4. (Optional) **show aaa authorization [all]**
5. (Optional) **copy running-config startup-config**

**DETAILED STEPS****Procedure**

|        | Command or Action                                                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                 |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>                                                                                                   | グローバル コンフィギュレーション モードを開始します                                                                                                                                                                                                                                                                                                                             |
| ステップ 2 | <b>aaa authorization ssh-certificate default { group group-list [none]   local   none}</b><br><b>Example:</b><br><pre>switch(config)# aaa authorization ssh-certificate default group ldap1 ldap2</pre> | <p>LDAP サーバのデフォルトの AAA 許可方式を設定します。</p> <p><b>ssh-certificate</b> キーワードは、証明書認証を使用した LDAP 許可またはローカル許可を設定します。デフォルトの許可は、ユーザに割り当てたロールに対して許可されたコマンドのリストであるローカル許可です。</p> <p><b>group-list</b> 引数には、LDAP サーバ グループ名をスペースで区切ったリストを指定します。このグループに属するサーバに対して、AAA 許可のためのアクセスが行われます。<b>local</b> 方式では、ローカル データベースを認証に使用します。<b>none</b> 方式では、AAA 認証が使用されないように指定します。</p> |
| ステップ 3 | <b>exit</b><br><b>Example:</b><br><pre>switch(config)# exit switch#</pre>                                                                                                                               | グローバル コンフィギュレーション モードを終了します。                                                                                                                                                                                                                                                                                                                            |
| ステップ 4 | (Optional) <b>show aaa authorization [all]</b><br><b>Example:</b><br><pre>switch# show aaa authorization</pre>                                                                                          | AAA 許可設定を表示します。 <b>all</b> キーワードを指定すると、デフォルト値が表示されます。                                                                                                                                                                                                                                                                                                   |

|        | Command or Action                                                                                                                    | Purpose                                   |
|--------|--------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| ステップ 5 | (Optional) <b>copy running-config startup-config</b><br><br><b>Example:</b><br><pre>switch# copy running-config startup-config</pre> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。 |

## TACACS サーバでの AAA SSH 証明書認証の構成

TACACS サーバに AAA SSH 証明書認証を設定するには、次の手順を実行します。

### 手順の概要

1. **configure terminal**
2. **aaa authorization ssh-certificate default { group group-list [none] | local | none}**
3. **exit**
4. (任意) **show aaa authorization [all]**
5. (任意) **copy running-config startup-config**

### 手順の詳細

#### 手順

|        | コマンドまたはアクション                                                                                                                                                                                    | 目的                                                                                                                                                                                                                                                                                                                                                                                        |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br><b>例 :</b><br><pre>switch# configure terminal switch(config)#</pre>                                                                                            | グローバル コンフィギュレーション モードを開始します                                                                                                                                                                                                                                                                                                                                                               |
| ステップ 2 | <b>aaa authorization ssh-certificate default { group group-list [none]   local   none}</b><br><br><b>例 :</b><br><pre>switch(config)# aaa authorization ssh-certificate default group tac1</pre> | <p>TACACS サーバ グループとして X509 証明書を持つ SSH 要求のデフォルトの AAA 認証方式を設定します。</p> <p><b>ssh-certificate</b> キーワードは、証明書認証を使用した TACACS 許可またはローカル許可を構成します。デフォルトの許可は、ユーザに割り当てたロールに対して許可されたコマンドのリストであるローカル許可です。</p> <p><b>group-list</b> 引数には、TACACS サーバ グループの名前をスペースで区切ったリストを指定します。このグループに属するサーバに対して、AAA 許可のためのアクセスが行われます。<b>local</b> 方式では、ローカルデータベースを認証に使用します。<b>none</b> 方式では、AAA 認証が使用されないように指定します。</p> |



|        | コマンドまたはアクション                                                                                                   | 目的                                                    |
|--------|----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| ステップ 3 | <b>exit</b><br>例 :<br><pre>switch(config)# exit switch#</pre>                                                  | グローバル コンフィギュレーション モードを終了します。                          |
| ステップ 4 | (任意) <b>show aaa authorization [all]</b><br>例 :<br><pre>switch# show aaa authorization</pre>                   | AAA 許可設定を表示します。 <b>all</b> キーワードを指定すると、デフォルト値が表示されます。 |
| ステップ 5 | (任意) <b>copy running-config startup-config</b><br>例 :<br><pre>switch# copy running-config startup-config</pre> | 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。            |

## デフォルトの AAA アカウンティング方式の設定

Cisco Nexus デバイスは、アカウンティングに TACACS+ 方式と RADIUS 方式をサポートします。スイッチは、ユーザー アクティビティをアカウンティング レコードの形で TACACS+ セキュリティ サーバーまたは RADIUS セキュリティ サーバーに報告します。各アカウンティング レコードに、アカウンティング属性値 (AV) のペアが入っており、それが AAA サーバーに格納されます。

AAA アカウンティングをアクティブにすると、Cisco Nexus デバイスは、これらの属性をアカウンティング レコードとして報告します。そのアカウンティング レコードは、セキュリティ サーバー上のアカウンティング ログに格納されます。

特定のアカウンティング方式を定義するデフォルト方式のリストを作成できます。それには次の方式があります。

- RADIUS サーバー グループ : RADIUS サーバーのグローバル プールをアカウンティングに使用します。
- 特定のサーバー グループ : 指定した RADIUS または TACACS+ サーバー グループをアカウンティングに使用します。
- ローカル : ユーザー名またはパスワードのローカルデータベースをアカウンティングに使用します。



### Note

サーバー グループが設定されていて、そのサーバー グループが応答しない場合、デフォルトではローカル データベースが認証に使用されます。

**Before you begin**

必要に応じて、AAA アカウンティングのデフォルト方式を設定する前に RADIUS または TACACS+ サーバー グループを設定します。

**SUMMARY STEPS**

1. switch# **configure terminal**
2. switch(config)# **aaa accounting default { group group-list | local}**
3. switch(config)# **exit**
4. (Optional) switch# **show aaa accounting**
5. (Optional) switch# **copy running-config startup-config**

**DETAILED STEPS****Procedure**

|        | Command or Action                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|---------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                                         | グローバル コンフィギュレーション モードを開始します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| ステップ 2 | switch(config)# <b>aaa accounting default { group group-list   local}</b> | <p>デフォルトのアカウント方式を設定します。スペースで区切ったリストで、1つまたは複数のサーバー グループ名を指定できます。</p> <p><i>group-list</i> 引数には、グループ名をスペースで区切ったリストを指定します。グループ名は、次のように指定します。</p> <ul style="list-style-type: none"> <li>• <b>radius</b> RADIUS サーバーのグローバルプールを使用してアカウントを行います。</li> <li>• <b>named-group</b> を指定すると、TACACS+ サーバーまたは RADIUS サーバーの名前付きサブセットがアカウントに使用されます。</li> </ul> <p><b>local</b> 方式はローカル データベースを使用してアカウントを行います。</p> <p>デフォルトの方式は <b>local</b> です。サーバー グループが設定されていないとき、または設定済みのすべてのサーバー グループから応答がないときに、このデフォルトの方式が使用されます。</p> |
| ステップ 3 | switch(config)# <b>exit</b>                                               | コンフィギュレーション モードを終了します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| ステップ 4 | (Optional) switch# <b>show aaa accounting</b>                             | デフォルトの AAA アカウンティング方式の設定を表示します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

|        | Command or Action                                            | Purpose                                   |
|--------|--------------------------------------------------------------|-------------------------------------------|
| ステップ 5 | (Optional) switch# <b>copy running-config startup-config</b> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。 |

## No Service Password-Recovery について

No Service Password-Recovery 機能により、コンソールへのアクセスを持つ誰もがルータおよびルータのネットワークにアクセスする機能を与えられることになります。

## No Service Password-Recovery のイネーブル化

No Service Password-Recovery 機能が有効になっている場合、ネットワーク権限を持つ管理者以外は管理者パスワードを変更できません。

始める前に

no service password-recovery コマンドを開始する場合、シスコでは、デバイスから離れた場所にシステム コンフィギュレーション ファイルのコピーを保存することを推奨しています。

### 手順の概要

1. **configure terminal**
2. **no service password-recovery**
3. (任意) **copy running-config startup-config**
4. **Reload**
5. **exit**
6. (任意) **show user-account**
7. (任意) **copy running-config startup-config**

### 手順の詳細

#### 手順

|        | コマンドまたはアクション                                                                                                                                                                                                | 目的                           |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例 :<br><pre>switch# configure terminal switch(config)#</pre>                                                                                                               | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | <b>no service password-recovery</b><br><br>例 :<br><pre>switch(config)# no service password-recovery WARNING: Executing this command will disable the password recovery mechanism. Do not execute this</pre> | パスワード回復メカニズムを無効にします。         |

|        | コマンドまたはアクション                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 目的                                        |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
|        | <pre>command without another plan for password recovery. Are you sure you want to continue? (y/n) : [y] y switch(config)# copy run start [#####] 100% Copy complete, now saving to disk (please wait)... Copy complete.</pre>                                                                                                                                                                                                                                                                                                                                                                          |                                           |
| ステップ 3 | <p>(任意) <b>copy running-config startup-config</b></p> <p>例 :</p> <pre>switch# copy running-config startup-config</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。 |
| ステップ 4 | <p><b>Reload</b></p> <p>例 :</p> <pre>switch(config)# Reload This command will reboot the system. (y/n)? [n] y 2018 Jun 26 16:23:19 BAR %\$ VDC-1 %\$ %PLATFORM-2-PFM_SYSTEM_RESET: Manual system restart from Command Line Interface  CISCO SWITCH Ver 8.34  CISCO SWITCH Ver 8.34 Manual system restart from Command Line Interface writing reset reason 9, .. ..  switch(boot)# config t Enter configuration commands, one per line. End with CNTL/Z. switch(boot)(config)# admin-password Abcd!123\$ ERROR: service password-recovery disabled. Cannot change password! switch(boot)(config)#</pre> |                                           |
| ステップ 5 | <p><b>exit</b></p> <p>例 :</p> <pre>switch(config)# exit switch#</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | グローバル コンフィギュレーション モードを終了します。              |
| ステップ 6 | <p>(任意) <b>show user-account</b></p> <p>例 :</p> <pre>switch# show user-account</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | ロール設定を表示します。                              |
| ステップ 7 | <p>(任意) <b>copy running-config startup-config</b></p> <p>例 :</p> <pre>switch# copy running-config startup-config</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。 |

## AAA サーバーの VSA の使用

### VSA

ベンダー固有属性（VSA）を使用して、AAA サーバー上での Cisco Nexus デバイスのユーザーロールおよび SNMPv3 パラメータを指定できます。

インターネット技術特別調査委員会（IETF）が、ネットワーク アクセス サーバと RADIUS サーバの間での VSA の通信のための方式を規定する標準を作成しています。IETF は属性 26 を使用します。ベンダーは VSA を使用して、一般的な用途には適さない独自の拡張属性をサポートできます。シスコの RADIUS 実装は、この仕様で推奨される形式を使用して、1 つのベンダー固有オプションをサポートしています。シスコのベンダー ID は 9、サポートされるオプションのベンダー タイプは 1（名前付き `cisco-av-pair`）です。値は次の形式のストリングです。

```
protocol : attribute seperator value *
```

プロトコルは、特定のタイプの許可用のシスコ属性です。必須属性の区切り文字は等号（=）で、アスタリスク（\*）は任意属性を示します。

Cisco Nexus デバイスでの認証に RADIUS サーバーを使用する場合は、認証結果とともに許可情報などのユーザー属性を返すよう、RADIUS プロトコルが RADIUS サーバーに指示します。この許可情報は、VSA で指定されます。

### VSA の形式

次の VSA プロトコル オプションが、Cisco Nexus デバイスでサポートされています。

- **Shell** : ユーザー プロファイル情報を提供する `access-accept` パケットで使用されます。
- **Accounting** : `accounting-request` パケットで使用されます。値にスペースが含まれている場合は、二重引用符で囲ってください。

次の属性が Cisco Nexus デバイスでサポートされています。

- **roles** : ユーザーに割り当てるすべてのロールをリストします。値フィールドは、グループ名を空白で区切ったリストの入ったストリングです。
- **accountinginfo** : 標準の RADIUS アカウンティングプロトコルで処理される属性に加えて、追加のアカウンティング情報が格納されます。この属性が送信されるのは、スイッチ上の RADIUS クライアントからの Account-Request フレームの VSA 部分内だけです。この属性は、アカウンティングプロトコル関連の PDU でしか使用できません。

## AAA サーバー上でのスイッチのユーザー ロールと SNMPv3 パラメータの指定

AAA サーバーで VSA `cisco-av-pair` を使用して、次の形式で、Cisco Nexus デバイスのユーザーロール マッピングを指定できます。

```
shell:roles="roleA roleB ..."
```

cisco-av-pair 属性にロール オプションを指定しなかった場合のデフォルトのユーザー ロールは、network-operator です。



**Note** Cisco Unified Wireless Network TACACS+ 設定と、ユーザー ロールの変更については、『[Cisco Unified Wireless Network TACACS+ Configuration](#)』を参照してください。

次のように SNMPv3 認証とプライバシー プロトコル属性を指定することもできます。

```
shell:roles="roleA roleB..." snmpv3:auth=SHA priv=AES-128
```

SNMPv3 認証プロトコルに指定できるオプションは、SHA と MD5 です。プライバシープロトコルに指定できるオプションは、AES-128 と DES です。cisco-av-pair 属性にこれらのオプションを指定しなかった場合のデフォルトの認証プロトコルは、MD5 と DES です。

追加情報については、Cisco Nexus デバイスの『System Management Configuration Guide』の「Configuring User Accounts and RBAC」の章を参照してください。

## セキュア ログインの機能拡張

### セキュア ログインの機能拡張

Cisco NX-OS では、次のセキュアなログイン拡張機能がサポートされています：

- ログイン パラメータの設定
- ログイン パラメータの設定例
- ユーザー 1 人あたりのセッション数の制限（ユーザー 1 人あたり、ログイン 1 回あたり）
- ユーザー名のパスワードプロンプトの有効化
- RADIUS/TACACS+ を使用するための共有キー値の設定

### ログイン パラメータの設定

Cisco NX-OS デバイスへの DoS 攻撃の疑いを検出し、辞書攻撃による影響の緩和に役立つログインパラメータを設定するには、ここに示す手順を実行します。

すべてのログインパラメータは、デフォルトではディセーブルです。他のログインコマンドを使用する前に、デフォルトのログイン機能を有効にする **login block-for** コマンドを入力する必要があります。**login block-for** コマンドを有効にすると、次のデフォルトが強制されます。

- Telnet または SSH を通じて行われるすべてのログイン試行は、待機時間中拒否されます。つまり、**login quiet-mode access-class** コマンドが入力されるまで、ACL はログイン時間から除外されません。

#### 手順の概要

##### 1. configure terminal

2. **[no] login block-for** *seconds* **attempts** *tries* **within** *seconds*
3. **[no] login quiet-mode access-class** {*acl-name* | *acl-number*}
4. **exit**
5. **show login failures**

## 手順の詳細

## 手順

|        | コマンドまたはアクション                                                                                                                                                                        | 目的                                                                                                                                       |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br><pre>Switch# configure terminal</pre>                                                                                                           | グローバル コンフィギュレーション モードを開始します。                                                                                                             |
| ステップ 2 | <b>[no] login block-for</b> <i>seconds</i> <b>attempts</b> <i>tries</i> <b>within</b> <i>seconds</i><br>例 :<br><pre>Switch(config)# login block-for 100 attempts 2 within 100</pre> | Cisco NX-OS デバイスで DoS 検出の提供に役立つログイン パラメータを構成します。<br>(注)<br>このコマンドは、その他のログイン コマンドを使用する前に発行する必要があります。                                      |
| ステップ 3 | <b>[no] login quiet-mode access-class</b> { <i>acl-name</i>   <i>acl-number</i> }<br>例 :<br><pre>Switch(config)# login quiet-mode access-class myacl</pre>                          | (任意) このコマンドはオプションですが、デバイスが静音モードに切り替わる時にデバイスに適用される ACL を指定するように設定することを推奨します。デバイスが待機モードになっている間は、すべてのログイン要求が拒否され、使用できる接続はコンソール経由の接続のみになります。 |
| ステップ 4 | <b>exit</b><br>例 :<br><pre>Switch(config)# exit</pre>                                                                                                                               | 特権 EXEC モードに戻ります。                                                                                                                        |
| ステップ 5 | <b>show login failures</b><br>例 :<br><pre>Switch# show login</pre>                                                                                                                  | ログイン パラメータを表示します。<br><ul style="list-style-type: none"> <li>• <b>failures</b> : 失敗したログイン試行に関連する情報のみを表示します。</li> </ul>                    |

## ログインパラメータの設定例

### ログインパラメータの設定例

次に、100 秒以内に 15 回ログイン要求が失敗した場合に 100 秒の待機モードに入るようにスイッチを設定する例を示します。待機時間中、ACL「myacl」からのホスト以外、すべてのログイン要求が拒否されます。

```
Switch(config)# login block-for 100 attempts 15 within 100
Switch(config)# login quiet-mode access-class myacl
```

### ログインパラメータの表示例

**show login** コマンドからの次のサンプル出力は、ログインパラメータが指定されていないことを確認します。

```
Switch# show login
```

```
No Quiet-Mode access list has been configured, default ACL will be applied.
```

```
Switch is enabled to watch for login Attacks.
If more than 2 login failures occur in 45 seconds or less, logins will be disabled for
70 seconds.
```

```
Switch presently in Normal-Mode.
Current Watch Window remaining time 10 seconds.
Present login failure count 0.
```

**show login failures** コマンドからの次のサンプル出力は、スイッチ上で失敗したすべてのログイン試行を表示します。

```
Switch# show login failures
```

```
Information about last 20 login failures with the device.
```

| Username | Line  | Source                | Appname |
|----------|-------|-----------------------|---------|
| admin    | pts/0 | bgl-ads-728.cisco.com | login   |
| admin    | pts/0 | bgl-ads-728.cisco.com | login   |

**show login failures** コマンドからの次のサンプル出力は、現在記録されている情報が無いことを確認します。

```
Switch# show login failures
*** No logged failed login attempts with the device.***
```

## ユーザー1人あたりのセッション数の制限（ユーザー1人あたり、ログイン1回あたり）

このタスクは、ユーザーごとの最大セッション数を制限するために使用します。



## 手順の概要

1. **configure terminal**
2. **[no] user max-logins max-logins**
3. **exit**

## 手順の詳細

## 手順

|        | コマンドまたはアクション                                                                                  | 目的                                                                                                      |
|--------|-----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br><pre>Switch# configure terminal</pre>                     | グローバル コンフィギュレーション モードを開始します。                                                                            |
| ステップ 2 | <b>[no] user max-logins max-logins</b><br>例 :<br><pre>Switch(config)# user max-logins 1</pre> | ユーザーごとの最大セッション数を制限します。指定できる範囲は 1 ～ 7 です。最大ログイン制限を 1 に設定すると、ユーザー 1 人あたりのセッション数 (telnet/SSH) が 1 に制限されます。 |
| ステップ 3 | <b>exit</b><br>例 :<br><pre>Switch(config)# exit</pre>                                         | 特権 EXEC モードに戻ります。                                                                                       |

## ユーザー名のパスワード プロンプトの有効化

## 手順の概要

1. **configure terminal**
2. **[no] password prompt username**
3. **exit**

## 手順の詳細

## 手順

|        | コマンドまたはアクション                                                              | 目的                           |
|--------|---------------------------------------------------------------------------|------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br><pre>Switch# configure terminal</pre> | グローバル コンフィギュレーション モードを開始します。 |

## RADIUS/TACACS+ を使用するための共有キー値の設定

|        | コマンドまたはアクション                                                                                       | 目的                                                                                                                                                                          |
|--------|----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 2 | <b>[no] password prompt username</b><br>例 :<br><pre>Switch(config)# password prompt username</pre> | ログインプロンプトを有効にします。このコマンドが有効になっている場合、ユーザーが <b>username</b> コマンドをパスワードオプションなしで入力すると、パスワードを入力するよう求められます。パスワードの入力には隠し文字を使用できます。ログインパスワード入力要求を無効にするには、このコマンドの <b>no</b> 形式を使用します。 |
| ステップ 3 | <b>exit</b><br>例 :<br><pre>Switch(config)# exit</pre>                                              | 特権 EXEC モードに戻ります。                                                                                                                                                           |

## RADIUS/TACACS+ を使用するための共有キー値の設定

リモート認証およびアカウントिंग用に設定する共有秘密は非表示にする必要があります。**radius-server key** および **tacacs-server key** コマンドでは、別のコマンドを使用して暗号化された共有秘密を使用できます。

## 手順の概要

1. **configure terminal**
2. **generate type7\_encrypted\_secret**
3. **exit**

## 手順の詳細

## 手順

|        | コマンドまたはアクション                                                                                                | 目的                                                                                                                                               |
|--------|-------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br><pre>Switch# configure terminal</pre>                                   | グローバル コンフィギュレーション モードを開始します。                                                                                                                     |
| ステップ 2 | <b>generate type7_encrypted_secret</b><br>例 :<br><pre>Switch(config)# generate type7_encrypted_secret</pre> | キー タイプ 7 で RADIUS および TACACS の共有秘密を構成します。暗号化された共有秘密を生成する間はユーザー入力为非表示になります。<br><br>(注)<br>プレーン テキストから暗号化された文字列を別個に生成して、暗号化された共有秘密を後から設定することもできます。 |

|        | コマンドまたはアクション                                       | 目的                |
|--------|----------------------------------------------------|-------------------|
| ステップ 3 | <b>exit</b><br><br>例 :<br><br>Switch(config)# exit | 特権 EXEC モードに戻ります。 |

## ローカル AAA アカウンティング ログのモニタリングとクリア

Cisco Nexus デバイスは、AAA アカウンティング アクティビティのローカル ログを保持しています。

### SUMMARY STEPS

1. switch# **show accounting log** [size] [ start-time year month day hh : mm : ss]
2. (Optional) switch# **clear accounting log**

### DETAILED STEPS

#### Procedure

|        | Command or Action                                                                   | Purpose                                                                                                                                         |
|--------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | switch# <b>show accounting log</b> [size] [ start-time year month day hh : mm : ss] | アカウンティング ログを表示します。このコマンド出力には、デフォルトで最大 250,000 バイトのアカウントング ログが表示されます。サイズ引数を指定すれば、コマンドの出力を制限できます。指定できる範囲は 0 ～ 250000 バイトです。ログ出力の開始時刻を指定することもできます。 |
| ステップ 2 | (Optional) switch# <b>clear accounting log</b>                                      | アカウンティング ログの内容をクリアします。                                                                                                                          |

## AAA 設定の確認

AAA の設定情報を表示するには、次のいずれかの作業を行います。

| コマンド                                                           | 目的                     |
|----------------------------------------------------------------|------------------------|
| <b>show aaa accounting</b>                                     | AAA アカウンティングの設定を表示します。 |
| <b>show aaa authentication</b> [login {error-enable   mschap}] | AAA 認証情報を表示します。        |

| コマンド                                                          | 目的                                                                                                                                                 |
|---------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>show aaa authorization</b>                                 | AAA 許可の情報を表示します。                                                                                                                                   |
| <b>show aaa groups</b>                                        | AAA サーバ グループの設定を表示します。                                                                                                                             |
| <b>show login [failures]</b>                                  | ログインパラメータを表示します。 <b>failures</b> オプションは、失敗したログイン試行に関連する情報のみを表示します。<br><br><b>Note</b><br><b>clear login failures</b> コマンドは、現在の監視期間内のログイン失敗をクリアします。 |
| <b>show login on-failure log</b>                              | syslog サーバに対して認証失敗メッセージをログ記録するようにスイッチが設定されているか表示します。                                                                                               |
| <b>show login on-successful log</b>                           | syslog サーバに対して認証成功メッセージをログ記録するようにスイッチが設定されているか表示します。                                                                                               |
| <b>show running-config aaa [all]</b>                          | 実行コンフィギュレーションの AAA 設定を表示します。                                                                                                                       |
| <b>show running-config aaa [all]</b>                          | 実行コンフィギュレーションの AAA 設定を表示します。                                                                                                                       |
| <b>show running-config all   i max-login</b>                  | ユーザ 1 人あたりの最大同時セッション数を表示します。                                                                                                                       |
| <b>show startup-config aaa</b>                                | スタートアップ コンフィギュレーションの AAA 設定を表示します。                                                                                                                 |
| <b>show userpassphrase {length   max-length   min-length}</b> | ユーザ パスワードの最小長と最大長を表示します。                                                                                                                           |

## AAA の設定例

次に、AAA を設定する例を示します。

```
switch(config)# aaa authentication login default group radius
switch(config)# aaa authentication login console group radius
switch(config)# aaa accounting default group radius
```

## デフォルトの AAA 設定

次の表に、AAA パラメータのデフォルト設定を示します。

**Table 5:** デフォルトの AAA パラメータ

| パラメータ             | デフォルト  |
|-------------------|--------|
| コンソール認証方式         | ローカル   |
| デフォルト認証方式         | ローカル   |
| ログイン認証失敗メッセージ     | ディセーブル |
| MSCHAP 認証         | ディセーブル |
| デフォルト アカウンティング方式  | ローカル   |
| アカウンティング ログの表示サイズ | 250 KB |





## 第 4 章

# RADIUS の設定

この章は、次の項で構成されています。

- [RADIUS の概要, on page 37](#)
- [RADIUS の前提条件, on page 40](#)
- [RADIUS の注意事項と制約事項 \(40 ページ\)](#)
- [RadSec の注意事項と制約事項 \(41 ページ\)](#)
- [RADIUS サーバの設定, on page 41](#)
- [RADIUS 設定の確認 \(59 ページ\)](#)
- [RADIUS サーバー統計情報の表示, on page 59](#)
- [RADIUS サーバ統計情報のクリア \(60 ページ\)](#)
- [RADIUS の設定例, on page 60](#)
- [RADIUS のデフォルト設定, on page 61](#)
- [RADIUS の機能の履歴 \(61 ページ\)](#)

## RADIUS の概要

Remote Access Dial-In User Service (RADIUS) 分散クライアント/サーバー システムを使用すると、不正アクセスからネットワークを保護できます。シスコの実装では、RADIUS クライアントは Cisco Nexus デバイスで稼働し、すべてのユーザー認証情報およびネットワーク サービス アクセス情報が格納された中央の RADIUS サーバに認証要求およびアカウントिंग要求を送信します。

## RADIUS ネットワーク環境

RADIUS は、高度なセキュリティを必要とし、同時にリモートユーザのネットワーク アクセスを維持する必要があるさまざまなネットワーク環境に実装できます。

RADIUS は、アクセス セキュリティを必要とする次のネットワーク環境で使用します。

- RADIUS をサポートしている複数ベンダーのネットワーク デバイスを使用したネットワーク。

たとえば、複数ベンダーのネットワーク デバイスで、単一の RADIUS サーバ ベースのセキュリティ データベースを使用できます。

- すでに RADIUS を使用中のネットワーク。

RADIUS 機能を持つ Cisco Nexus デバイスをネットワークに追加できます。この作業は、AAA サーバーに移行するときの最初の手順になります。

- リソース アカウンティングが必要なネットワーク。

RADIUS アカウンティングは、RADIUS 認証または RADIUS 認可とは個別に使用できます。RADIUS アカウンティング機能を使用すると、サービスの開始および終了時に、セッション中に使用したリソース（時間、パケット、バイトなど）の量を示すデータを送信できます。インターネット サービス プロバイダー（ISP）は、RADIUS アクセス コントロールおよび アカウンティング用ソフトウェアのフリーウェア版を使用して、特殊なセキュリティおよび課金ニーズに対応しています。

- 認証 プロファイルをサポートするネットワーク。

ネットワークで RADIUS サーバを使用すると、AAA 認証を設定し、ユーザごとのプロファイルを設定アップできます。ユーザごとのプロファイルにより、Cisco Nexus デバイスは、既存の RADIUS ソリューションを使用してポートを管理できると同時に、共有リソースを効率的に管理してさまざまなサービス レベル契約を提供できます。

## RADIUS の操作について

ユーザーが RADIUS を使用して Cisco Nexus デバイスへのログインおよび認証を試行すると、次のプロセスが実行されます。

1. ユーザが、ユーザ名とパスワードの入力を求められ、入力します。
2. ユーザ名および暗号化されたパスワードが、ネットワーク経由で RADIUS サーバに送信されます。
3. ユーザは、RADIUS サーバから次のいずれかの応答を受信します。
  - ACCEPT：ユーザーが認証されたことを表します。
  - REJECT：ユーザーは認証されず、ユーザー名とパスワードの再入力を求められるか、アクセスを拒否されます。
  - CHALLENGE：RADIUS サーバによってチャレンジが発行されます。チャレンジは、ユーザーから追加データを収集します。
  - CHANGE PASSWORD：RADIUS サーバからユーザーに対して新しいパスワードの選択を求める要求が発行されます。

ACCEPT 応答または REJECT 応答には、EXEC 許可またはネットワーク許可に使用される追加データが含まれています。RADIUS 認可を使用するには、まず RADIUS 認証を完了する必要があります。ACCEPT または REJECT パケットに含まれる追加データの内容は次のとおりです。



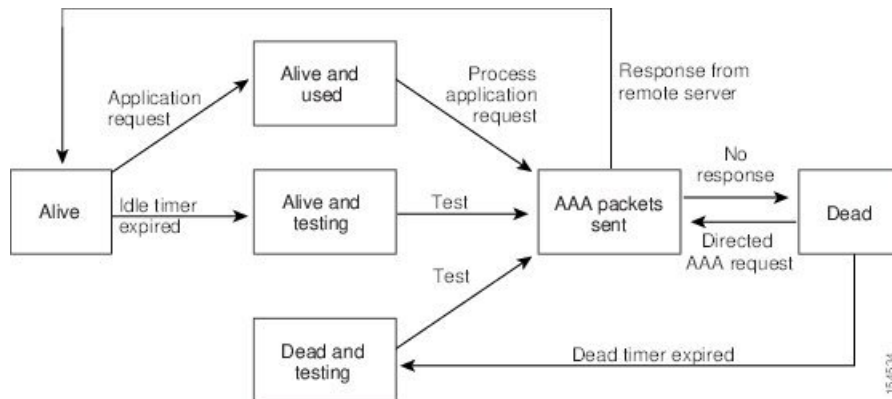
- ユーザがアクセス可能なサービス（Telnet、rlogin、またはローカルエリアトランスポート（LAT）接続、ポイントツーポイントプロトコル（PPP）、シリアルラインインターネットプロトコル（SLIP）、EXEC サービスなど）
- 接続パラメータ（ホストまたはクライアントの IPv4 アドレス、アクセスリスト、ユーザータイムアウト）

## RADIUS サーバのモニタリング

応答を返さない RADIUS サーバがあると、AAA 要求の処理に遅延が発生する可能性があります。AAA 要求の処理時間を節約するために、定期的に RADIUS サーバをモニタリングし、RADIUS サーバが応答を返す（アライブ状態である）かどうかを調べるよう、スイッチを設定できます。スイッチは、応答を返さない RADIUS サーバをデッド（dead）状態としてマークし、デッド RADIUS サーバには AAA 要求を送信しません。また、定期的にデッド RADIUS サーバをモニタリングし、それらが応答を返したらアライブ状態に戻します。このプロセスにより、RADIUS サーバが稼働状態であることを確認してから、実際の AAA 要求がサーバに送信されます。RADIUS サーバの状態がデッドまたはアライブに変わると、簡易ネットワーク管理プロトコル（SNMP）トラップが生成され、障害が発生したことを知らせるエラーメッセージがスイッチによって表示されます。

次の図に、さまざまな RADIUS サーバの状態を示します。

Figure 2: RADIUS サーバの状態



### Note

アライブサーバとデッドサーバのモニタリング間隔は異なります。これらはユーザが設定できます。RADIUS サーバモニタリングを実行するには、テスト認証要求を RADIUS サーバに送信します。

## ベンダー固有属性

インターネット技術特別調査委員会（IETF）が、ネットワークアクセスサーバと RADIUS サーバの間でのベンダー固有属性（VSA）の通信のための方式を規定する標準を作成してい

ます。IETF は属性 26 を使用します。ベンダーは VSA を使用して、一般的な用途には適さない独自の拡張属性をサポートできます。シスコの RADIUS 実装は、この仕様で推奨される形式を使用して、1 つのベンダー固有オプションをサポートしています。シスコのベンダー ID は 9、サポートされるオプションのベンダータイプは 1（名前付き `cisco-av-pair`）です。値は次の形式のストリングです。

```
protocol : attribute separator value *
```

プロトコルは、特定のタイプの許可用のシスコ属性です。必須属性の区切り文字は等号 (=) で、アスタリスク (\*) は任意属性を示します。

Cisco Nexus デバイスでの認証に RADIUS サーバーを使用する場合は、許可情報などのユーザー属性を認証結果とともに返すように、RADIUS サーバーに RADIUS プロトコルで指示します。この許可情報は、VSA で指定されます。

次の VSA プロトコル オプションが Cisco Nexus デバイスでサポートされています：

- **Shell**：ユーザー プロファイル情報を提供する `access-accept` パケットで使用されます。
- **Accounting**：`accounting-request` パケットで使用されます。値にスペースが含まれている場合は、二重引用符で囲む必要があります。

Cisco Nexus デバイスは次の属性をサポートしています：

- **roles**：ユーザーが属するすべてのロールの一覧です。値フィールドは、スペースで区切られた複数のロール名をリストするストリングです。
- **accountinginfo**：標準の RADIUS アカウンティングプロトコルで処理される属性に加えて、アカウンティング情報が格納されます。この属性は、スイッチ上の RADIUS クライアントからの `Account-Request` フレームの VSA 部分だけに送信されます。この属性と共に使用できるのは、アカウンティングのプロトコルデータユニット (PDU) だけです。

## RADIUS の前提条件

RADIUS には、次の前提条件があります。

- RADIUS サーバーの IPv4 アドレスまたはホスト名を取得すること。
- RADIUS サーバーから事前共有キーを取得すること。
- Cisco Nexus デバイスが、AAA サーバーの RADIUS クライアントとして設定されていること。

## RADIUS の注意事項と制約事項

RADIUS 設定時の注意事項と制限事項は次のとおりです。

- デバイスに構成できる RADIUS サーバの最大数は 64 です。

## RadSec の注意事項と制約事項

RadSec には、次の注意事項と制約事項 があります。

- Cisco NX-OS リリース 10.3(1)F 以降、トランスポート層での RADIUS/TCP ピア間の通信を保護するために、RADIUS Secure (RadSec) サポートが Cisco Nexus スイッチで提供されます。
- RadSec はスイッチ レベルで有効/無効にする必要があります。これは、異なるトランスポート プロトコル (つまり、UDP と TCP-with-TLS) を持つサーバーの組み合わせが不可能であるためです。
- **radius-serverdirected-request** コマンドは、RadSec 機能ではサポートされていません。
- **test aaa server radius** コマンドは RadSec サーバーではサポートされていません。RadSec でサポートされるのは **test aaa group** コマンドだけです。
- Dot1x は RadSec で公式にサポートされていません。
- RADIUS サーバーの監視は、RadSec サーバーではサポートされていません。
- RADIUS サーバーの再送信とタイムアウトは、UDP ベースの RADIUS モードに適用されますが、RadSec サーバーに対してはサポートされません。
- Cisco NX-OS リリース 10.4(3)F 以降、TLS バージョン 1.3 および 1.2 が、Cisco Nexus スイッチでサポートされています。TLS v1.1 は廃止されました。

## RADIUS サーバの設定

ここでは、RADIUS サーバーの設定方法について説明します。

### SUMMARY STEPS

1. Cisco Nexus デバイスと RADIUS サーバとの接続を確立します。
2. RADIUS サーバーの事前共有秘密キーを設定します。
3. 必要に応じて、AAA 認証方式用に、RADIUS サーバのサブセットを使用して RADIUS サーバ グループを設定します。
4. 必要に応じて、次のオプションのパラメータを設定します。
5. 必要に応じて、定期的に RADIUS サーバーをモニタリングするよう設定します。

### DETAILED STEPS

#### Procedure

---

**ステップ 1** Cisco Nexus デバイスと RADIUS サーバとの接続を確立します。

「[RADIUS サーバホストの設定, on page 42](#)」を参照してください。

**ステップ 2** RADIUS サーバーの事前共有秘密キーを設定します。

「[RADIUS のグローバルな事前共有キーの設定, on page 43](#)」を参照してください。

**ステップ 3** 必要に応じて、AAA 認証方式用に、RADIUS サーバのサブセットを使用して RADIUS サーバグループを設定します。

ログイン時にユーザによる RADIUS サーバの指定を許可, [on page 52](#) および RADIUS サーバのアカウントिंगおよび認証属性の設定, [on page 54](#) を参照してください。

**ステップ 4** 必要に応じて、次のオプションのパラメータを設定します。

- デッドタイム間隔「[デッドタイム間隔の設定, on page 57](#)」を参照してください。
- ログイン時に RADIUS サーバーの指定を許可「[ログイン時にユーザによる RADIUS サーバの指定を許可, on page 52](#)」を参照してください。
- 送信リトライ回数とタイムアウト間隔「[グローバルな RADIUS 送信リトライ回数とタイムアウト間隔の設定, on page 53](#)」を参照してください。
- アカウントिंगおよび認証属性「[RADIUS サーバのアカウントINGおよび認証属性の設定, on page 54](#)」を参照してください。

**ステップ 5** 必要に応じて、定期的に RADIUS サーバーをモニタリングするよう設定します。

「[RADIUS サーバーの定期的モニタリングの設定, on page 56](#)」を参照してください。

## RADIUS サーバホストの設定

認証に使用する各 RADIUS サーバーについて、IPv4 アドレスまたはホスト名を構成する必要があります。すべての RADIUS サーバーホストは、デフォルトの RADIUS サーバーグループに追加されます。最大 64 の RADIUS サーバーを設定できます。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **radius-server host {ipv4-address | host-name}**
3. switch(config)# **exit**
4. (Optional) switch# **show radius-server**
5. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

#### Procedure

|        | Command or Action                 | Purpose           |
|--------|-----------------------------------|-------------------|
| ステップ 1 | switch# <b>configure terminal</b> | グローバル構成モードを開始します。 |

|        | Command or Action                                                    | Purpose                                                            |
|--------|----------------------------------------------------------------------|--------------------------------------------------------------------|
| ステップ 2 | switch(config)# <b>radius-server host</b> {ipv4-address   host-name} | RADIUS サーバーの IPv4 アドレスまたはホスト名を指定します。                               |
| ステップ 3 | switch(config)# <b>exit</b>                                          | コンフィグレーション モードを終了します。                                              |
| ステップ 4 | (Optional) switch# <b>show radius-server</b>                         | RADIUS サーバーの設定を表示します。                                              |
| ステップ 5 | (Optional) switch# <b>copy running-config startup-config</b>         | リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。 |

### Example

次に、RADIUS サーバーとしてホスト 10.10.1.1 を設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1
switch(config)# exit
switch# copy running-config startup-config
```

## RADIUS のグローバルな事前共有キーの設定

Cisco Nexus デバイスで使用するすべてのサーバーについて、グローバルレベルで事前共有キーを構成できます。事前共有キーとは、スイッチと RADIUS サーバー ホスト間の共有秘密テキスト ストリングです。

### Before you begin

リモートの RADIUS サーバーの事前共有キー値を取得していること。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **radius-server key [0 | 7] key-value**
3. switch(config)# **exit**
4. (Optional) switch# **show radius-server**
5. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

#### Procedure

|        | Command or Action                 | Purpose           |
|--------|-----------------------------------|-------------------|
| ステップ 1 | switch# <b>configure terminal</b> | グローバル構成モードを開始します。 |

|        | Command or Action                                                 | Purpose                                                                                                                                                          |
|--------|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 2 | switch(config)# <b>radius-server key</b> [0   7] <i>key-value</i> | すべての RADIUS サーバーで使用する事前共有キーを指定します。クリアテキスト形式（ <b>0</b> ）または暗号化形式（ <b>7</b> ）事前共有キーを指定できます。デフォルトの形式はクリア テキストです。<br><br>最大で 63 文字です。<br><br>デフォルトでは、事前共有キーは設定されません。 |
| ステップ 3 | switch(config)# <b>exit</b>                                       | コンフィグレーション モードを終了します。                                                                                                                                            |
| ステップ 4 | (Optional) switch# <b>show radius-server</b>                      | RADIUS サーバーの設定を表示します。<br><br><b>Note</b><br>事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。暗号化された事前共有キーを表示するには、 <b>show running-config</b> コマンドを使用します。                      |
| ステップ 5 | (Optional) switch# <b>copy running-config startup-config</b>      | リブートおよびリスタート時に実行構成をスタートアップ構成にコピーして、変更を継続的に保存します。                                                                                                                 |

### Example

次に、デバイスで使用するすべてのサーバーについて、グローバル レベルで事前共有キーを設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server key 0 QsEfThUkO
switch(config)# exit
switch# copy running-config startup-config
```

## RADIUS サーバーの事前共有キーの設定

事前共有キーとは、Cisco Nexus デバイスと RADIUS サーバー ホスト間の共有秘密テキスト スtring です。

### Before you begin

リモートの RADIUS サーバーの事前共有キー値を取得していること。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **radius-server host** {*ipv4-address* | *host-name*} **key** [0 | 7] *key-value*

3. switch(config)# **exit**
4. (Optional) switch# **show radius-server**
5. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

### Procedure

|        | Command or Action                                                                                 | Purpose                                                                                                                                                                     |
|--------|---------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                                                                 | グローバル構成モードを開始します。                                                                                                                                                           |
| ステップ 2 | switch(config)# <b>radius-server host</b> {ipv4-address   host-name} <b>key</b> [0   7] key-value | <p>特定の RADIUS サーバーの事前共有キーを指定します。クリアテキスト形式 (<b>0</b>) または暗号化形式 (<b>7</b>) 事前共有キーを指定できます。デフォルトの形式はクリア テキストです。</p> <p>最大で 63 文字です。</p> <p>この事前共有キーがグローバル事前共有キーの代わりに使用されます。</p> |
| ステップ 3 | switch(config)# <b>exit</b>                                                                       | コンフィグレーション モードを終了します。                                                                                                                                                       |
| ステップ 4 | (Optional) switch# <b>show radius-server</b>                                                      | <p>RADIUS サーバーの設定を表示します。</p> <p><b>Note</b><br/>事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。暗号化された事前共有キーを表示するには、<b>show running-config</b> コマンドを使用します。</p>                          |
| ステップ 5 | (Optional) switch# <b>copy running-config startup-config</b>                                      | リブートおよびリスタート時に実行構成をスタートアップ構成にコピーして、変更を継続的に保存します。                                                                                                                            |

### Example

次に、RADIUS 事前共有キーを設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1 key 0 PlIjUhYg
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

## RadSec の設定

RadSec は、TLS 経由で RADIUS データグラムを転送するためのプロトコルです。

この手順では、スイッチで RadSec を有効または無効にする方法について説明します。

### 始める前に

- サーバーのクライアント ID 証明書と CA 証明書がスイッチにインストールされていることを確認します。
- サーバー証明書のサブジェクト名が、スイッチで構成されているサーバーのホスト名/IP アドレスと一致していることを確認してください。
- RadSec サーバーを使用するように AAA 認証とアカウンティングを設定する前に、**test aaa group** コマンドを使用して、RadSec 認証が成功することを確認します。
- スイッチからの頻繁な TLS セッションの再試行を避けるために、RadSec サーバーで TLS アイドル タイムアウトを最大値に設定します。

### 手順の概要

1. **configure terminal**
2. **radius-server secure tls**
3. **radius-server host t {ipv4-address | ipv6-address | hostname} key {key} auth-port 2083 acct-port 2083 authentication accounting**
4. **radius-server host {ipv4-address | ipv6-address | hostname} tls client-trustpoint trustpoint**
5. **radius-server host {ipv4-address | ipv6-address | hostname} tls idle-timeout value**

### 手順の詳細

#### 手順

|        | コマンドまたはアクション                                                                                                                           | 目的                                                                       |
|--------|----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br>switch# <b>configure terminal</b>                                                                  | コンフィギュレーション モードに入ります。                                                    |
| ステップ 2 | <b>radius-server secure tls</b><br>例 :<br>switch# <b>radius-server secure tls</b>                                                      | グローバル レベルで有効にします。<br><br>(注)<br>この CLI は、RadSec に使用されるポート番号を変更または影響しません。 |
| ステップ 3 | <b>radius-server host t {ipv4-address   ipv6-address   hostname} key {key} auth-port 2083 acct-port 2083 authentication accounting</b> | 認証およびアカウンティングポートとともに共有秘密キーを使用して RadSec サーバーを構成します。<br><br>(注)            |



|        | コマンドまたはアクション                                                                                                                                                                                          | 目的                                                                                                                                                                                            |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        | <p>例 :</p> <pre>switch# radius-server host 10.105.222.161 key radsec auth-port 2083 acct-port 2083 authentication accounting</pre>                                                                    | <p>サーバーの場合、認証とアカウンティングのデフォルトの RadSec ポートは「2083」で、キーは「radsec」です。スイッチの場合、RadSec ポートとキーのデフォルト設定はありません。サーバーで定義されているように、この設定を明示的に追加してください。</p>                                                     |
| ステップ 4 | <p><b>radius-server host {ipv4-address   ipv6-address   hostname} tls client-trustpoint trustpoint</b></p> <p>例 :</p> <pre>switch# radius-server host 10.105.222.161 tls client-trustpoint rad1</pre> | <p>クライアント ID 証明書がインストールされている TLS クライアントトラストポイントを設定します。</p>                                                                                                                                    |
| ステップ 5 | <p><b>radius-server host {ipv4-address   ipv6-address   hostname} tls idle-timeout value</b></p> <p>例 :</p> <pre>switch# radius-server host 10.105.222.161 tls idle-timeout 80</pre>                  | <p>TLS アイドルタイムアウトを設定します。デフォルト値は 600 秒です。</p> <p>(注)</p> <p>RadSec クライアントからのトランザクションがない場合、サーバーはタイムアウト値に基づいて接続を閉じることができます。クライアントの TLS アイドルタイムアウトは、このリリースではサポートされていません。クライアントは自分自身で接続を閉じません。</p> |



- (注) リモートユーザーがログインすると、約 20 秒間のログインの遅延が見られることがあります。つまり、スイッチと RadSec サーバーの間で TLS セッションの確立が初めて行われるときです。TLS セッションが起動すると、連続したリモート ログインで遅延は見られません。



- (注) RadSec クライアントで、証明書が存在しない、または無効な証明書がサーバーと交換されているなどの証明書関連の問題が発生している場合、show run コマンドで遅延が発生する可能性があります。

## DTLS を使用した RADIUS について

Cisco NX-OS リリース 10.4(1)F から、DTLS プロトコルを使用した RADIUS が導入されました。このプロトコルは、UDP を使用してセキュア チャネルを介して RADIUS データグラムを転送するためのものです。

RADIUS と DTLS は、トランスポート層での RADIUS ピア間のセキュアな通信を可能にします。このプロトコルは、さまざまな管理ドメインや疑わしい、安全でないネットワークを介してセキュアな RADIUS パケット転送を行いたい場合に役立ちます。

## DTLS を使用する RADIUS の構成

### 始める前に

- スイッチの IP アドレス/DNS ホスト名と同じサブジェクトと代替名を使用してクライアントアイデンティティ証明書を作成してください。トラストポイントを使用して、スイッチにクライアントアイデンティティ証明書をインストールします。
- DTLS/RADIUS に使用される ISE サーバのサーバ証明書がスイッチにインストールされていることを確認します。
- クライアントアイデンティティ証明書の署名に使用される CA 証明書が ISE サーバの信頼できる証明書ストアにインストールされていることを確認します。
- サーバ証明書のサブジェクト名が、スイッチで構成されているサーバのホスト名/IP アドレスと同じであることを確認します。
- RADIUS サーバを使用するように AAA 認証およびアカウンティンググループを構成する前に、`test aaa group` コマンドで RADIUS 認証が成功することを確認します。
- スイッチ レベルで RADIUS と DTLS プロトコルを有効にする必要があります。
- DTLS と TLS など、異なるトランスポートプロトコルを使用するように RADIUS サーバを組み合わせることはサポートされていません。一度に 1 つのプロトコルを構成できます。

### 手順

|        | コマンドまたはアクション                                                                                                                                        | 目的                                                        |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br><pre>switch# configure terminal switch(config)#</pre>                                                           | コンフィギュレーション モードに入ります。                                     |
| ステップ 2 | <b>radius-server secure dtls</b><br>例 :<br><pre>switch(config)# radius-server secure dtls</pre>                                                     | スイッチで RADIUS with DTLS プロトコルを有効にします。                      |
| ステップ 3 | <b>radius-server host {ipv4-address   ipv6-address   hostname} key {radius/dtls} auth-port 2083 acct-port 2083 authentication accounting</b><br>例 : | 共有秘密キー、および認証ポートとアカウンティングポートを使用して、RADIUS サーバを構成します。<br>(注) |

|        | コマンドまたはアクション                                                                                                                                                                                                    | 目的                                                                                                                                                                                                                                |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        | <pre>switch(config)# radius-server host 10.105.222.161 key radius/dtls auth-port 2083 acct-port 2083 authentication accounting</pre>                                                                            | <p>認証およびアカウンティングのデフォルトの接続先 DTLS ポートは <b>UDP/2083</b> です。RFC に従って、DTLS のデフォルトのサーバー キーはありません。サーバーで定義されているように、この構成を明示的に追加してください。ISE サーバーは、その時点で「radius/dtls」キーで事前設定されている必要があります。ISE サーバーで DTLS を構成するときに、Nexus スイッチでキーを確認して追加します。</p> |
| ステップ 4 | <p><b>radius-server host {ipv4-address   ipv6-address   hostname} dtls client-trustpoint trustpoint</b></p> <p>例 :</p> <pre>switch(config)# radius-server host 10.105.222.161 dtls client-trustpoint rad1</pre> | <p>スイッチ ID 証明書がインストールされているトラストポイントで、DTLS client-trustpoint パラメータを構成します。<i>rad1</i> は、クライアントアイデンティティ証明書が必要なスイッチ上のトラストポイントです。</p>                                                                                                   |
| ステップ 5 | <p><b>radius-server host {ipv4-address   ipv6-address   hostname} dtls idle-timeout value</b></p> <p>例 :</p> <pre>switch# radius-server host 10.105.222.161 dtls idle-timeout 80</pre>                          | <p>DTLS アイドル タイムアウトを設定します。デフォルト値は 600 秒です。</p> <p>(注)</p> <p>RADIUS クライアントからのトランザクションがない場合、サーバは定義されたタイムアウト値に従い接続を閉じます。クライアントの DTLS アイドルタイムアウトは、このリリースではサポートされていません。クライアントは自分自身で接続を閉じません。</p>                                      |



(注)

- リモートユーザーがログインすると、約 20 秒の遅延が発生することがあります。これは、スイッチと RADIUS サーバの間で TLS セッションが初めて確立されるときに発生します。いったん TLS セッションが確立されれば、後続のリモートログインで遅延は発生しません。
- RADIUS クライアントで、証明書が存在しない、または無効な証明書がサーバと交換されているなどの証明書関連の問題が発生している場合、show run コマンドで遅延が発生する可能性があります。

## RADIUS サーバグループの設定

サーバグループを使用して、1 台または複数台のリモート AAA サーバによる認証を指定できます。グループのメンバーはすべて、RADIUS プロトコルに属している必要があります。設定した順序に従ってサーバが試行されます。

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch (config)# **aaa group server radius group-name**
3. switch (config-radius)# **server** {ipv4-address |server-name}
4. (Optional) switch (config-radius)# **deadtime minutes**
5. (Optional) switch(config-radius)# **source-interface interface**
6. switch(config-radius)# **exit**
7. (Optional) switch(config)# **show radius-server group** [group-name]
8. (Optional) switch(config)# **copy running-config startup-config**

## DETAILED STEPS

## Procedure

|        | Command or Action                                                   | Purpose                                                                                                                                         |
|--------|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                                   | グローバル構成モードを開始します。                                                                                                                               |
| ステップ 2 | switch (config)# <b>aaa group server radius group-name</b>          | RADIUS サーバー グループを作成し、そのグループの RADIUS サーバー グループ コンフィギュレーション サブモードを開始します。<br><br><i>group-name</i> 引数は、最大 127 文字の英数字のストリングで、大文字小文字が区別されます。         |
| ステップ 3 | switch (config-radius)# <b>server</b> {ipv4-address  server-name}   | RADIUS サーバを、RADIUS サーバグループのメンバーとして設定します。<br><br>指定した RADIUS サーバが見つからない場合は、 <b>radius-server host</b> コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。         |
| ステップ 4 | (Optional) switch (config-radius)# <b>deadtime minutes</b>          | モニタリング デッド タイムを設定します。デフォルト値は 0 分です。指定できる範囲は 1 ～ 1440 です。<br><br><b>Note</b><br>RADIUS サーバグループのデッド タイム間隔が 0 より大きい場合は、この値がグローバルなデッド タイム値より優先されます。 |
| ステップ 5 | (Optional) switch(config-radius)# <b>source-interface interface</b> | 特定の RADIUS サーバー グループに発信元インターフェイスを割り当てます。<br><br>サポートされているインターフェイスのタイプは管理および VLAN です。<br><br><b>Note</b>                                         |

|        | Command or Action                                                       | Purpose                                                                                             |
|--------|-------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
|        |                                                                         | source-interface コマンドを使用して、ip radius source-interface コマンドによって割り当てられたグローバル ソース インターフェイスをオーバーライドします。 |
| ステップ 6 | switch(config-radius)# <b>exit</b>                                      | 設定モードを終了します。                                                                                        |
| ステップ 7 | (Optional) switch(config)# <b>show radius-server group</b> [group-name] | RADIUS サーバ グループの設定を表示します。                                                                           |
| ステップ 8 | (Optional) switch(config)# <b>copy running-config startup-config</b>    | リブートおよびリスタート時に実行構成をスタートアップ構成にコピーして、変更を継続的に保存します。                                                    |

### Example

次に、RADIUS サーバ グループを設定する例を示します。

```
switch# configure terminal
switch (config)# aaa group server radius RadServer
switch (config-radius)# server 10.10.1.1
switch (config-radius)# deadtime 30
switch (config-radius)# use-vrf management
switch (config-radius)# exit
switch (config)# show radius-server group
switch (config)# copy running-config startup-config
```

### What to do next

AAA サービスに RADIUS サーバ グループを適用します。

## RADIUS サーバ グループのためのグローバル発信元インターフェイスの設定

RADIUS サーバ グループにアクセスする際に使用する、RADIUS サーバ グループ用のグローバル発信元インターフェイスを設定できます。また、特定の RADIUS サーバ グループ用に異なる発信元インターフェイスを設定することもできます。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **ip radius source-interface interface**
3. switch(config)# **exit**
4. (Optional) switch# **show radius-server**
5. (Optional) switch# **copy running-config startup config**

## DETAILED STEPS

## Procedure

|        | Command or Action                                            | Purpose                                                                                                 |
|--------|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                            | グローバル コンフィギュレーション モードを開始します。                                                                            |
| ステップ 2 | switch(config)# <b>ip radius source-interface interface</b>  | このデバイスで設定されているすべての RADIUS サーバー グループ用のグローバル発信元インターフェイスを設定します。発信元インターフェイスは、管理または VLAN インターフェイスにすることができます。 |
| ステップ 3 | switch(config)# <b>exit</b>                                  | コンフィギュレーション モードを終了します。                                                                                  |
| ステップ 4 | (Optional) switch# <b>show radius-server</b>                 | RADIUS サーバーの設定情報を表示します。                                                                                 |
| ステップ 5 | (Optional) switch# <b>copy running-config startup-config</b> | 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。                                                              |

## Example

次に、RADIUS サーバー グループのグローバル発信元インターフェイスとして、mgmt 0 インターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# ip radius source-interface mgmt 0
switch(config)# exit
switch# copy running-config startup-config
```

## ログイン時にユーザによる RADIUS サーバの指定を許可

ログイン時に RADIUS サーバーを指定することをユーザーに許可できます。

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **radius-server directed-request**
3. switch(config)# **exit**
4. (Optional) switch# **show radius-server directed-request**
5. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

## Procedure

|        | Command or Action                                             | Purpose                                                          |
|--------|---------------------------------------------------------------|------------------------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                             | グローバル構成モードを開始します。                                                |
| ステップ 2 | switch(config)# <b>radius-server directed-request</b>         | ログイン時にユーザーが認証要求の送信先となる RADIUS サーバーを指定できるようにします。デフォルトでは無効になっています。 |
| ステップ 3 | switch(config)# <b>exit</b>                                   | コンフィギュレーション モードを終了します。                                           |
| ステップ 4 | (Optional) switch# <b>show radius-server directed-request</b> | directed request の設定を表示します。                                      |
| ステップ 5 | (Optional) switch# <b>copy running-config startup-config</b>  | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                        |

## Example

次に、ネットワークにログインしたときに、ユーザーが RADIUS サーバーを選択できるようにする例を示します。

```
switch# configure terminal
switch(config)# radius-server directed-request
switch# exit
switch# copy running-config startup-config
```

## グローバルな RADIUS 送信リトライ回数とタイムアウト間隔の設定

すべての RADIUS サーバーに対するグローバルな再送信リトライ回数とタイムアウト間隔を設定できます。デフォルトでは、スイッチはローカル認証に戻す前に、RADIUS サーバーへの送信を 1 回だけ再試行します。このリトライの回数は、サーバーごとに最大 5 回まで増やすことができます。タイムアウト間隔には、Cisco Nexus デバイスが RADIUS サーバからの応答を待つ時間を指定します。これを過ぎるとタイムアウト エラーになります。

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **radius-server retransmit count**
3. switch(config)# **radius-server timeout seconds**
4. switch(config)# **exit**
5. (Optional) switch# **show radius-server**
6. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

## Procedure

|        | Command or Action                                            | Purpose                                                          |
|--------|--------------------------------------------------------------|------------------------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                            | グローバル構成モードを開始します。                                                |
| ステップ 2 | switch(config)# <b>radius-server retransmit count</b>        | すべての RADIUS サーバの再送信回数を指定します。デフォルトの再送信回数は 1 で、範囲は 0 ～ 5 です。       |
| ステップ 3 | switch(config)# <b>radius-server timeout seconds</b>         | RADIUS サーバの送信タイムアウト間隔を指定します。デフォルトのタイムアウト間隔は 5 秒で、範囲は 1 ～ 60 秒です。 |
| ステップ 4 | switch(config)# <b>exit</b>                                  | グローバル コンフィギュレーション モードを終了します。                                     |
| ステップ 5 | (Optional) switch# <b>show radius-server</b>                 | RADIUS サーバーの設定を表示します。                                            |
| ステップ 6 | (Optional) switch# <b>copy running-config startup-config</b> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                        |

## Example

次に、RADIUS サーバーで、リトライ回数を 3、伝送タイムアウト間隔を 5 秒に設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server retransmit 3
switch(config)# radius-server timeout 5
switch(config)# exit
switch# copy running-config startup-config
```

## RADIUS サーバのアカウントिंगおよび認証属性の設定

RADIUS サーバをアカウントング専用、または認証専用に使用するかを指定できます。デフォルトでは、RADIUS サーバはアカウントングと認証の両方に使用されます。RADIUS のアカウントングおよび認証メッセージの宛先 UDP ポート番号も指定できます。

## SUMMARY STEPS

1. switch# **configure terminal**
2. (Optional) switch(config)# **radius-server host {ipv4-address || host-name} acct-port udp-port**
3. (Optional) switch(config)# **radius-server host {ipv4-address || host-name} accounting**
4. (Optional) switch(config)# **radius-server host {ipv4-address || host-name} auth-port udp-port**
5. (Optional) switch(config)# **radius-server host {ipv4-address || host-name} authentication**



6. switch(config)# **exit**
7. (Optional) switch(config)# **show radius-server**
8. switch(config)# **copy running-config startup-config**

## DETAILED STEPS

### Procedure

|        | Command or Action                                                                                          | Purpose                                                                                    |
|--------|------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                                                                          | グローバル構成モードを開始します。                                                                          |
| ステップ 2 | (Optional) switch(config)# <b>radius-server host</b> {ipv4-address    host-name} <b>acct-port udp-port</b> | RADIUS アカウンティングのメッセージに使用する UDP ポートを指定します。デフォルトの UDP ポートは 1812 です。<br><br>範囲は 0 ～ 65535 です。 |
| ステップ 3 | (Optional) switch(config)# <b>radius-server host</b> {ipv4-address    host-name} <b>accounting</b>         | 特定の RADIUS サーバーをアカウンティング用にのみ使用することを指定します。デフォルトでは、アカウンティングと認証の両方に使用されます。                    |
| ステップ 4 | (Optional) switch(config)# <b>radius-server host</b> {ipv4-address    host-name} <b>auth-port udp-port</b> | RADIUS 認証メッセージ用の UDP ポートを指定します。デフォルトの UDP ポートは 1812 です。<br><br>範囲は 0 ～ 65535 です。           |
| ステップ 5 | (Optional) switch(config)# <b>radius-server host</b> {ipv4-address    host-name} <b>authentication</b>     | 特定の RADIUS サーバーを認証用にのみ使用することを指定します。デフォルトでは、アカウンティングと認証の両方に使用されます。                          |
| ステップ 6 | switch(config)# <b>exit</b>                                                                                | コンフィグレーション モードを終了します。                                                                      |
| ステップ 7 | (Optional) switch(config)# <b>show radius-server</b>                                                       | RADIUS サーバーの設定を表示します。                                                                      |
| ステップ 8 | switch(config)# <b>copy running-config startup-config</b>                                                  | リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。                         |

### Example

次に、RADIUS サーバーのアカウントリング属性と認証属性を設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1 acct-port 2004
switch(config)# radius-server host 10.10.1.1 accounting
switch(config)# radius-server host 10.10.2.2 auth-port 2005
switch(config)# radius-server host 10.10.2.2 authentication
switch # exit
switch # copy running-config startup-config
switch #
```

## RADIUS サーバーの定期的モニタリングの設定

RADIUS サーバーの可用性をモニタリングできます。パラメータとして、サーバーに使用するユーザー名とパスワード、およびアイドル タイマーがあります。アイドル タイマーには、RADIUS サーバーがどのくらいの期間要求を受信しなかった場合にスイッチがテスト パケットを送信するかを指定します。このオプションを設定することで、サーバーを定期的にテストできます。



**Note** セキュリティ上の理由から、RADIUS データベース内の既存のユーザー名と同じテスト ユーザー名を設定しないことを推奨します。

テスト アイドル タイマーには、RADIUS サーバーがどのくらいの期間要求を受信しなかった場合にスイッチがテスト パケットを送信するかを指定します。

デフォルトのアイドル タイマー値は 0 分です。アイドル時間間隔が 0 分の場合、スイッチは RADIUS サーバーの定期的なモニタリングを実行しません。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **radius-server host** {ipv4-address | host-name} **test** {idle-time minutes | password password [idle-time minutes] | username name [password password [idle-time minutes]]}
3. switch(config)# **radius-server deadtime minutes**
4. switch(config)# **exit**
5. (Optional) switch# **show radius-server**
6. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

#### Procedure

|        | Command or Action                                                                                                                                                                                    | Purpose                                                                                                                                                                                                                 |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                                                                                                                                                                    | グローバル構成モードを開始します。                                                                                                                                                                                                       |
| ステップ 2 | switch(config)# <b>radius-server host</b> {ipv4-address   host-name} <b>test</b> {idle-time minutes   password password [idle-time minutes]   username name [password password [idle-time minutes]]} | <p>サーバー モニタリング用のパラメータを指定します。デフォルトのユーザー名は test、デフォルトのパスワードは test です。</p> <p>デフォルトのアイドル タイマー値は 0 分です。</p> <p>有効な範囲は、0 ～ 1440 分です。</p> <p><b>Note</b><br/>RADIUS サーバーの定期的なモニタリングを行うには、アイドル タイマーに 0 より大きな値を設定する必要があります。</p> |

|        | Command or Action                                            | Purpose                                                                                             |
|--------|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| ステップ 3 | switch(config)# <b>radius-server</b> <i>deadtime minutes</i> | スイッチが、前回応答しなかった RADIUS サーバーをチェックするまでの時間（分）を指定します。<br><br>デフォルト値は 0 分です。<br><br>有効な範囲は 1 ～ 1440 分です。 |
| ステップ 4 | switch(config)# <b>exit</b>                                  | コンフィグレーション モードを終了します。                                                                               |
| ステップ 5 | (Optional) switch# <b>show radius-server</b>                 | RADIUS サーバーの設定を表示します。                                                                               |
| ステップ 6 | (Optional) switch# <b>copy running-config startup-config</b> | リブートおよびリスタート時に実行構成をスタートアップ構成にコピーして、変更を継続的に保存します。                                                    |

### Example

次に、ユーザー名（user1）およびパスワード（Ur2Gd2BH）と、3 分のアイドル タイマーおよび 5 分のデッドタイムで、RADIUS サーバー ホスト 10.10.1.1 を設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1 test username user1 password Ur2Gd2BH
idle-time 3
switch(config)# radius-server deadtime 5
switch(config)# exit
switch# copy running-config startup-config
```

## デッドタイム間隔の設定

すべての RADIUS サーバのデッドタイム間隔を設定できます。デッドタイム間隔には、Cisco Nexus デバイスが、RADIUS サーバーをデッド状態であると宣言した後、そのサーバーがオンライン状態に戻ったかどうかを確認するためにテストパケットを送信するまでの間隔を指定します。デフォルト値は 0 分です。



#### Note

デッドタイム間隔が 0 分の場合、RADIUS サーバは、応答を返さない場合でも、デッドとしてマークされません。RADIUS サーバ グループに対するデッドタイム間隔を設定できます。  
「[RADIUS サーバ グループの設定, on page 49](#)」を参照してください。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **radius-server deadtime**
3. switch(config)# **exit**

4. (Optional) switch# **show radius-server**
5. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

### Procedure

|        | Command or Action                                            | Purpose                                           |
|--------|--------------------------------------------------------------|---------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                            | グローバル構成モードを開始します。                                 |
| ステップ 2 | switch(config)# <b>radius-server deadtime</b>                | デッドタイム間隔を設定します。デフォルト値は 0 分です。有効な範囲は 1 ～ 1440 分です。 |
| ステップ 3 | switch(config)# <b>exit</b>                                  | コンフィグレーション モードを終了します。                             |
| ステップ 4 | (Optional) switch# <b>show radius-server</b>                 | RADIUS サーバーの設定を表示します。                             |
| ステップ 5 | (Optional) switch# <b>copy running-config startup-config</b> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。         |

### Example

次に、RADIUS サーバーに 5 分間のデッドタイムを設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server deadtime 5
switch(config)# exit
switch# copy running-config startup-config
```

## RADIUS サーバまたはサーバ グループの手動モニタリング

### SUMMARY STEPS

1. switch# **test aaa server radius {ipv4-address | server-name} [ vrf vrf-name] username password**  
**test aaa server radius {ipv4-address | server-name} [ vrf vrf-name] username password**
2. switch# **test aaa group group-name username password**

## DETAILED STEPS

## Procedure

|        | Command or Action                                                                                                                                                                                               | Purpose                                  |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| ステップ 1 | switch# <b>test aaa server radius</b> {ipv4-address   server-name} [ <b>vrf</b> vrf-name] username password <b>test aaa server radius</b> {ipv4-address   server-name} [ <b>vrf</b> vrf-name] username password | RADIUS サーバーにテストメッセージを送信して可用性を確認します。      |
| ステップ 2 | switch# <b>test aaa group</b> group-name username password                                                                                                                                                      | RADIUS サーバー グループにテストメッセージを送信して可用性を確認します。 |

## Example

次に、可用性を確認するために、RADIUS サーバーとサーバー グループにテストメッセージを送信する例を示します。

```
switch# test aaa server radius 10.10.1.1 user 1 Ur2Gd2BH
switch# test aaa group RadGroup user2 As3He3CI
```

## RADIUS 設定の確認

AAA 情報を表示するには、次のいずれかの作業を行います：

| コマンド                                                                                                                    | 目的                                    |
|-------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| <b>show running-config radius</b> [all]                                                                                 | 実行構成中の RADIUS の構成を表示します。              |
| <b>show startup-config radius</b>                                                                                       | スタートアップ コンフィギュレーションの RADIUS 設定を表示します。 |
| <b>show radius-server</b> [server-name   ipv4-address   ipv6-address] [directed-request   groups   sorted   statistics] | 設定済みのすべての RADIUS サーバのパラメータを表示します。     |

## RADIUS サーバー統計情報の表示

## SUMMARY STEPS

1. switch# **show radius-server statistics** {hostname | ipv4-address}

## DETAILED STEPS

## Procedure

|        | Command or Action                                                      | Purpose            |
|--------|------------------------------------------------------------------------|--------------------|
| ステップ 1 | switch# <b>show radius-server statistics</b> {hostname   ipv4-address} | RADIUS 統計情報を表示します。 |

## RADIUS サーバ統計情報のクリア

Cisco NX-OS デバイスが保持している RADIUS サーバーのアクティビティに関する統計情報を表示します。

## 始める前に

Cisco NX-OS デバイスに RADIUS サーバーを設定します。

## 手順の概要

1. (任意) switch# **show radius-server statistics** {hostname | ipv4-address}
2. switch# **clear radius-server statistics** {hostname | ipv4-address}

## 手順の詳細

## 手順

|        | コマンドまたはアクション                                                                | 目的                                        |
|--------|-----------------------------------------------------------------------------|-------------------------------------------|
| ステップ 1 | (任意) switch# <b>show radius-server statistics</b> {hostname   ipv4-address} | Cisco NX-OS デバイスでの RADIUS サーバー統計情報を表示します。 |
| ステップ 2 | switch# <b>clear radius-server statistics</b> {hostname   ipv4-address}     | RADIUS サーバ統計情報をクリアします。                    |

## RADIUS の設定例

次に、RADIUS を設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server key 7 "ToIkLhPpG"
switch(config)# radius-server host 10.10.1.1 key 7 "ShMoMhTl" authentication accounting
switch(config)# aaa group server radius RadServer
switch(config-radius)# server 10.10.1.1
switch(config-radius)# exit
```

```
switch(config-radius)# use-vrf management
```

## RADIUS のデフォルト設定

次の表に、RADIUS パラメータのデフォルト設定を示します。

**Table 6:** デフォルトの **RADIUS** パラメータ

| パラメータ               | デフォルト       |
|---------------------|-------------|
| サーバーの役割             | 認証とアカウンティング |
| デッド タイマー間隔          | 0 分         |
| 再送信回数               | 1           |
| 再送信タイマー間隔           | 5 秒         |
| アイドル タイマー間隔         | 0 分         |
| サーバの定期的モニタリングのユーザ名  | test        |
| サーバの定期的モニタリングのパスワード | テスト         |

## RADIUS の機能の履歴

**表 7:** **RADIUS** の機能の履歴

| 機能名    | リリース        | 機能情報               |
|--------|-------------|--------------------|
| RADIUS | 5.0(3)U1(1) | この機能が導入されました。      |
| IPv6   | 5.0(3)U3(1) | IPv6 サポートが導入されました。 |







## 第 5 章

# TACACS+ の設定

この章は、次の項で構成されています。

- [TACACS+ の設定に関する情報, on page 63](#)
- [TACACS+ の前提条件, on page 66](#)
- [TACACS+ の注意事項と制約事項 \(66 ページ\)](#)
- [TACACS+ の設定 \(66 ページ\)](#)

## TACACS+ の設定に関する情報

Terminal Access Controller Access Control System Plus (TACACS+) セキュリティプロトコルは、Cisco Nexus デバイスにアクセスしようとするユーザーの検証を集中的に行います。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で稼働する TACACS+ デモンのデータベースで管理されます。Cisco Nexus デバイスに構成した TACACS+ 機能を使用できるようにするには、TACACS+ サーバーにアクセスして構成しておく必要があります。

TACACS+ では、認証、許可、アカウンティングの各ファシリティを個別に提供します。TACACS+ を使用すると、単一のアクセス コントロール サーバー (TACACS+ デモン) で、各サービス (認証、許可、アカウンティング) を個別に提供できます。各サービスは固有のデータベースにアソシエートされており、デモンの機能に応じて、そのサーバーまたはネットワーク上で使用可能な他のサービスを利用できます。

TACACS+ クライアント/サーバー プロトコルでは、トランスポート要件を満たすため TCP (TCP ポート 49) を使用します。Cisco Nexus デバイスは、TACACS+ プロトコルを使用して集中型の認証を行います。

Cisco NX-OS リリース 10.4(3)F 以降、TACACS+ サーバーを使用した X.509 証明書の SSH ベースの認証は、Cisco Nexus 3600 シリーズ プラットフォーム スイッチで **aaa authorization ssh-certificate default group** コマンドを使用して実行できます。し設定の詳細については、[TACACS サーバーを使用した X.509 証明書ベースの SSH 認証の設定, on page 78](#)を参照してください。

## TACACS+ の利点

TACACS+ には、RADIUS 認証にはない次の利点があります。

- 独立した AAA ファシリティを提供する。たとえば、Cisco Nexus デバイスは、認証を行わずにアクセスを許可できます。
- AAA クライアントとサーバ間のデータ送信に TCP トランスポート プロトコルを使用しているため、コネクション型プロトコルによる確実な転送を実行します。
- スイッチと AAA サーバ間でプロトコルペイロード全体を暗号化して、高度なデータ機密性を実現します。RADIUS プロトコルはパスワードだけを暗号化します。

## TACACS+ を使用したユーザー ログイン

ユーザが TACACS+ を使用して、パスワード認証プロトコル (PAP) によるログインを Cisco Nexus デバイスに対して試行すると、次のプロセスが実行されます：

1. Cisco Nexus デバイスが接続を確立すると、TACACS+ デーモンにアクセスして、ユーザー名とパスワードを取得します。



**Note** TACACS+ では、デーモンがユーザを認証するために十分な情報を得られるまで、デーモンとユーザとの自由な対話を許可します。この動作ではユーザー名とパスワードの入力が要求されますが、ユーザーの母親の旧姓など、その他の項目の入力が要求されることもあります。

2. Cisco Nexus デバイスが、TACACS+ デーモンから次のいずれかの応答を受信します。
  - **ACCEPT** : ユーザの認証に成功したので、サービスを開始します。Cisco Nexus デバイスがユーザー許可を必要とする場合は、許可処理が始まります。
  - **REJECT** : ユーザーの認証に失敗しました。TACACS+ デーモンは、ユーザーに対してそれ以上のアクセスを拒否するか、ログイン シーケンスを再試行するよう要求します。
  - **ERROR** : デーモンによる認証サービスの途中でエラーが発生したか、またはデーモンと Cisco Nexus デバイスの間のネットワーク接続でエラーが発生しました。Cisco Nexus デバイスが **ERROR** 応答を受信した場合、スイッチは代替りのユーザー認証方式の使用を試みます。

Cisco Nexus デバイスで許可がイネーブルになっている場合は、この後、許可フェーズの処理が実行されます。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。

3. TACACS+ 許可が必要な場合、Cisco Nexus デバイスは再度 TACACS+ デーモンにアクセスします。デーモンは **ACCEPT** または **REJECT** 許可応答を返します。**ACCEPT** 応答には、ユーザに対する **EXEC** または **NETWORK** セッションの送信に使用される属性が含まれます。また **ACCEPT** 応答により、ユーザがアクセス可能なサービスが決まります。

この場合のサービスは次のとおりです。

- Telnet、rlogin、ポイントツーポイントプロトコル（PPP）、シリアルラインインターネットプロトコル（SLIP）、EXEC サービス
- 接続パラメータ（ホストまたはクライアントの IP アドレス（IPv4）、アクセスリスト、ユーザタイムアウトなどを含まず）

## デフォルトの TACACS+ サーバー暗号化タイプと事前共有キー

TACACS+ サーバーに対してスイッチを認証するには、TACACS+ 事前共有キーを設定する必要があります。事前共有キーとは、Cisco Nexus デバイスと TACACS+ サーバー ホスト間の共有秘密テキスト文字列です。キーの長さは 63 文字で、出力可能な任意の ASCII 文字を含めることができます（スペースは使用できません）。使用する Cisco Nexus デバイス上のすべての TACACS+ サーバー設定で使用されるグローバルな事前共有秘密キーを設定できます。

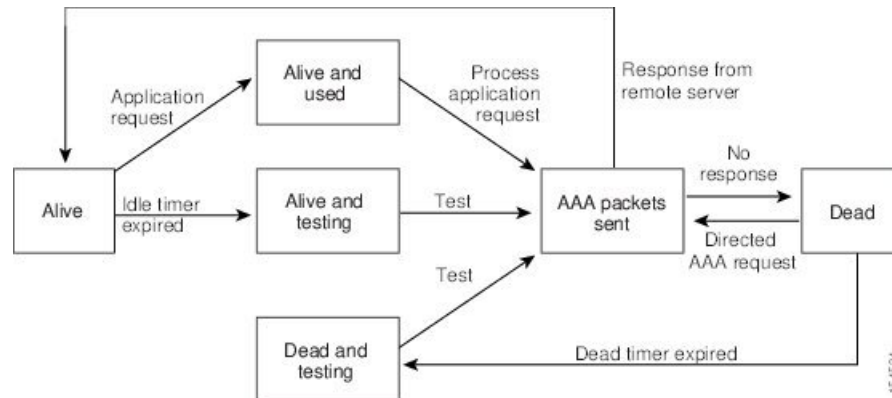
グローバルな事前共有キーの設定は、個々の TACACS+ サーバーの設定時に **key** オプションを使用することによって無効にできます。

## TACACS+ サーバのモニタリング

応答を返さない TACACS+ サーバーがあると、AAA 要求の処理に遅延が発生する可能性があります。AAA 要求の処理時間を節約するため、Cisco Nexus デバイスは定期的に TACACS+ サーバーをモニタリングし、TACACS+ サーバーが応答を返す（アライブ）かどうかを調べることができます。Cisco Nexus デバイスは、応答を返さない TACACS+ サーバーをデッド（dead）としてマークし、デッド TACACS+ サーバーには AAA 要求を送信しません。また、Cisco Nexus デバイスは、定期的にデッド TACACS+ サーバーをモニタリングし、それらが応答を返したら、アライブ状態に戻します。このプロセスでは、TACACS+ サーバーが稼働状態であることを確認してから、実際の AAA 要求がサーバーに送信されます。TACACS+ サーバの状態がデッドまたはアライブに変わると、簡易ネットワーク管理プロトコル（SNMP）トラップが生成され、Cisco Nexus デバイスによって、パフォーマンスに影響が出る前に、障害が発生していることを知らせるエラー メッセージが表示されます。

次の図に、さまざまな TACACS+ サーバーの状態を示します。

Figure 3: TACACS+ サーバーの状態

**Note**

アライブ サーバとデッドサーバのモニタリング間隔は異なります。これらはユーザが設定できます。TACACS+ サーバ モニタリングを実行するには、テスト認証要求を TACACS+ サーバに送信します。

## TACACS+ の前提条件

TACACS+ には、次の前提条件があります。

- TACACS+ サーバーの IPv4 または IPv6 アドレスまたはホスト名を取得すること。
- TACACS+ サーバーから事前共有キーを取得していること。
- Cisco Nexus デバイスが、AAA サーバーの TACACS+ クライアントとして構成されていること。

## TACACS+ の注意事項と制約事項

TACACS+ に関する注意事項と制約事項は次のとおりです。

- Cisco Nexus デバイスに設定できる TACACS+ サーバーの最大数は 64 です。

## TACACS+ の設定

### TACACS+ サーバの設定プロセス

ここでは、TACACS+ サーバーを設定する方法について説明します。

## SUMMARY STEPS

1. TACACS+ をイネーブルにします。
2. TACACS+ サーバーと Cisco Nexus デバイスとの接続を確立します。
3. TACACS+ サーバーの事前共有秘密キーを設定します。
4. 必要に応じて、AAA 認証方式用に、TACACS+ サーバーのサブセットを使用して TACACS+ サーバー グループを設定します。
5. 必要に応じて、定期的に TACACS+ サーバーをモニタリングするよう設定します。

## DETAILED STEPS

### Procedure

ステップ 1 TACACS+ をイネーブルにします。

「[TACACS+ のイネーブル化](#), on page 67」を参照してください。

ステップ 2 TACACS+ サーバーと Cisco Nexus デバイスとの接続を確立します。

[TACACS+ サーバ ホストの設定](#), on page 68

ステップ 3 TACACS+ サーバーの事前共有秘密キーを設定します。

[TACACS+ のグローバルな事前共有キーの設定](#), on page 69

ステップ 4 必要に応じて、AAA 認証方式用に、TACACS+ サーバーのサブセットを使用して TACACS+ サーバー グループを設定します。

[TACACS+ サーバ グループの設定](#), on page 71

ステップ 5 必要に応じて、定期的に TACACS+ サーバーをモニタリングするよう設定します。

[TACACS+ サーバーの定期的モニタリングの設定](#), on page 75

## TACACS+ のイネーブル化

デフォルトでは、Cisco Nexus デバイスで TACACS+ 機能は無効に設定されています。TACACS+ 機能をイネーブルに設定すると、認証に関するコンフィギュレーションコマンドと検証コマンドを使用できます。

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **feature tacacs+**
3. switch(config)# **exit**
4. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

## Procedure

|        | Command or Action                                            | Purpose                                    |
|--------|--------------------------------------------------------------|--------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                            | グローバル コンフィギュレーション モードを開始します。               |
| ステップ 2 | switch(config)# <b>feature tacacs+</b>                       | TACACS+ をイネーブルにします。                        |
| ステップ 3 | switch(config)# <b>exit</b>                                  | コンフィギュレーション モードを終了します。                     |
| ステップ 4 | (Optional) switch# <b>copy running-config startup-config</b> | 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。 |

## TACACS+ サーバホストの設定

リモートの TACACS+ サーバにアクセスするには、Cisco Nexus デバイス上でその TACACS+ サーバの IPv4 または IPv6 アドレスかホスト名を構成する必要があります。すべての TACACS+ サーバー ホストは、デフォルトの TACACS+ サーバー グループに追加されます。最大 64 の TACACS+ サーバーを設定できます。

設定済みの TACACS+ サーバーに事前共有キーが設定されておらず、グローバルキーも設定されていない場合は、警告メッセージが表示されます。TACACS+ サーバー キーが設定されていない場合は、グローバル キー（設定されている場合）が該当サーバーで使用されます。

（詳細については、「TACACS+ グローバル事前共有キーの構成」および「TACACS+ サーバー事前共有キーの構成」の項を参照してください）。

TACACS+ サーバー ホストを設定する前に、次の点を確認してください。

- TACACS+ をイネーブルにします。詳細については、「[TACACS+ のイネーブル化, on page 67](#)」を参照してください。
- リモート TACACS+ サーバの IP アドレス（IPv4 または IPv6）またはホスト名を取得していること。

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **tacacs-server host {ipv4-address | ipv6-address | host-name}**
3. switch(config)# **tacacs-server host {ipv4-address | host-name}**
4. switch(config)# **exit**
5. (Optional) switch# **show tacacs-server**
6. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

## Procedure

|        | Command or Action                                                                   | Purpose                                       |
|--------|-------------------------------------------------------------------------------------|-----------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                                                   | グローバル コンフィギュレーション モードを開始します。                  |
| ステップ 2 | switch(config)# <b>tacacs-server host</b> {ipv4-address   ipv6-address   host-name} | TACACS+ サーバの IPv4 または IPv6 アドレスまたはホスト名を指定します。 |
| ステップ 3 | switch(config)# <b>tacacs-server host</b> {ipv4-address   host-name}                | TACACS+ サーバの IPv4 アドレスまたはホスト名を指定します。          |
| ステップ 4 | switch(config)# <b>exit</b>                                                         | コンフィギュレーション モードを終了します。                        |
| ステップ 5 | (Optional) switch# <b>show tacacs-server</b>                                        | TACACS+ サーバの設定を表示します。                         |
| ステップ 6 | (Optional) switch# <b>copy running-config startup-config</b>                        | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。     |

## Example

サーバー グループから TACACS+ サーバ ホストを削除できます。

## TACACS+ のグローバルな事前共有キーの設定

Cisco Nexus デバイスで使用するすべてのサーバについて、グローバルレベルで事前共有キーを構成できます。事前共有キーとは、Cisco Nexus デバイスと TACACS+ サーバ ホスト間の共有秘密テキスト文字列です。

事前共有キーを設定する前に、次の点を確認してください。

- TACACS+ をイネーブルにします。
- リモートの TACACS+ サーバの事前共有キー値を取得していること。

## SUMMARY STEPS

1. switch# **configure terminal**
2. **tacacs-server key** [0 | 6 | 7] *key-value*
3. switch(config)# **exit**
4. (Optional) switch# **show tacacs-server**
5. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

## Procedure

|        | Command or Action                                                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                  |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                                                                                                                                                                  | グローバル コンフィギュレーション モードを開始します。                                                                                                                                                                                                                                                                                                                             |
| ステップ 2 | <b>tacacs-server key [0   6   7] key-value</b><br><b>Example:</b><br>switch(config)# <b>tacacs-server key 0 QsEfThUkO</b><br><b>Example:</b><br>switch(config)# <b>tacacs-server key 7 "fewhg"</b> | <p>すべての TACACS+ サーバ用の TACACS+ キーを指定します。key-value がクリアテキスト形式 (0) か、タイプ 6 暗号化形式 (6) か、タイプ 7 暗号化形式 (7) かを指定できます。Cisco NX-OS ソフトウェアでは、実行構成に保存する前にクリア テキストのキーを暗号化します。デフォルトの形式はクリア テキストです。最大で 63 文字です。</p> <p>デフォルトでは、秘密キーは設定されていません。</p> <p><b>Note</b><br/> <b>generate type7_encrypted_secret</b> を使用してすでに共有秘密を設定している場合 コマンドを使用して、二番目の例に示すように引用符に入力します。</p> |
| ステップ 3 | switch(config)# <b>exit</b>                                                                                                                                                                        | コンフィギュレーション モードを終了します。                                                                                                                                                                                                                                                                                                                                   |
| ステップ 4 | (Optional) switch# <b>show tacacs-server</b>                                                                                                                                                       | TACACS+ サーバーの設定を表示します。<br><b>Note</b><br>事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。暗号化された事前共有キーを表示するには、 <b>show running-config</b> コマンドを使用します。                                                                                                                                                                                                                 |
| ステップ 5 | (Optional) switch# <b>copy running-config startup-config</b>                                                                                                                                       | 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。                                                                                                                                                                                                                                                                                                               |

## Example

次に、グローバルな事前共有キーを設定する例を示します。

```
switch# configure terminal
switch(config)# tacacs-server key 0 QsEfThUkO
switch(config)# exit
switch# show tacacs-server
switch# copy running-config startup-config
```



## TACACS+ サーバグループの設定

サーバグループを使用して、1 台または複数台のリモート AAA サーバによるユーザ認証を指定することができます。グループのメンバーはすべて、TACACS+ プロトコルに属している必要があります。設定した順序に従ってサーバが試行されます。

これらのサーバグループはいつでも設定できますが、設定したグループを有効にするには、AAA サービスに適用する必要があります。

### Before you begin

TACACS+ を設定する前に、`feature tacacs+` コマンドを使用して、TACACS+ をイネーブルにする必要があります。

### SUMMARY STEPS

1. `switch# configure terminal`
2. `switch(config)# aaa group server tacacs+ group-name`
3. (Optional) `switch(config-tacacs+)# deadtime minutes`
4. (Optional) `switch(config-tacacs+)# source-interface interface`
5. `switch(config-tacacs+)# exit`
6. (Optional) `switch(config)# show tacacs-server groups`
7. (Optional) `switch(config)# copy running-config startup-config`

### DETAILED STEPS

#### Procedure

|        | Command or Action                                                          | Purpose                                                                                                                                            |
|--------|----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <code>switch# configure terminal</code>                                    | グローバル コンフィギュレーション モードを開始します。                                                                                                                       |
| ステップ 2 | <code>switch(config)# aaa group server tacacs+ group-name</code>           | TACACS+ サーバー グループを作成し、そのグループの TACACS+ サーバー グループ コンフィギュレーション モードを開始します。                                                                             |
| ステップ 3 | (Optional) <code>switch(config-tacacs+)# deadtime minutes</code>           | モニタリング デッド タイムを設定します。デフォルト値は 0 分です。指定できる範囲は 0 ～ 1440 です。<br><br><b>Note</b><br>TACACS+ サーバー グループのデッド タイム間隔が 0 より大きい場合は、その値がグローバルなデッド タイム値より優先されます。 |
| ステップ 4 | (Optional) <code>switch(config-tacacs+)# source-interface interface</code> | 特定の TACACS+ サーバー グループに発信元インターフェイスを割り当てます。                                                                                                          |

|        | Command or Action                                                    | Purpose                                                                                                                                                        |
|--------|----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        |                                                                      | サポートされているインターフェイスのタイプは管理および VLAN です。<br><br><b>Note</b><br>source-interface コマンドを使用して、ip tacacs source-interface コマンドによって割り当てられたグローバル ソース インターフェイスをオーバーライドします。 |
| ステップ 5 | switch(config-tacacs+)# <b>exit</b>                                  | コンフィグレーション モードを終了します。                                                                                                                                          |
| ステップ 6 | (Optional) switch(config)# <b>show tacacs-server groups</b>          | TACACS+ サーバグループの設定を表示します。                                                                                                                                      |
| ステップ 7 | (Optional) switch(config)# <b>copy running-config startup-config</b> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                                                                                      |

### Example

次に、TACACS+ サーバグループを設定する例を示します。

```
switch# configure terminal
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# server 10.10.2.2
switch(config-tacacs+)# deadtime 30
switch(config-tacacs+)# exit
switch(config)# show tacacs-server groups
switch(config)# copy running-config startup-config
```

## TACACS+ サーバグループのためのグローバル発信元インターフェイスの設定

TACACS+ サーバグループにアクセスする際に使用する、TACACS+ サーバグループ用のグローバル発信元インターフェイスを設定できます。また、特定のTACACS+サーバグループ用に異なる発信元インターフェイスを設定することもできます。

### SUMMARY STEPS

1. **configure terminal**
2. **ip tacacs source-interface interface**
3. **exit**
4. (Optional) **show tacacs-server**
5. (Optional) **copy running-config startup config**

## DETAILED STEPS

## Procedure

|        | Command or Action                                                                                                         | Purpose                                                                                                  |
|--------|---------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b>                                                                                                 | グローバル コンフィギュレーション モードを開始します                                                                              |
| ステップ 2 | <b>ip tacacs source-interface interface</b><br><br><b>Example:</b><br>switch(config)# ip tacacs source-interface mgmt 0   | このデバイスで設定されているすべての TACACS+ サーバー グループ用のグローバル発信元インターフェイスを設定します。発信元インターフェイスは、管理または VLAN インターフェイスにすることができます。 |
| ステップ 3 | <b>exit</b><br><br><b>Example:</b><br>switch(config)# exit<br>switch#                                                     | 設定モードを終了します。                                                                                             |
| ステップ 4 | (Optional) <b>show tacacs-server</b><br><br><b>Example:</b><br>switch# show tacacs-server                                 | TACACS+ サーバの設定情報を表示します。                                                                                  |
| ステップ 5 | (Optional) <b>copy running-config startup config</b><br><br><b>Example:</b><br>switch# copy running-config startup-config | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                                |

## グローバルな TACACS+ タイムアウト間隔の設定

Cisco Nexus デバイスのグローバルなタイムアウト間隔も設定できます。タイムアウトエラーを宣言する前に、すべての TACACS+ サーバーからの応答を待機する時間です。タイムアウト間隔には、スイッチが TACACS+ サーバーからの応答を待つ時間を指定します。これを過ぎるとタイムアウトエラーになります。

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **tacacs-server timeout seconds**
3. switch(config)# **exit**
4. (Optional) switch# **show tacacs-server**
5. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

## Procedure

|        | Command or Action                                            | Purpose                                                          |
|--------|--------------------------------------------------------------|------------------------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                            | グローバル コンフィギュレーション モードを開始します。                                     |
| ステップ 2 | switch(config)# <b>tacacs-server timeout seconds</b>         | TACACS+ サーバーのタイムアウト間隔を指定します。デフォルトのタイムアウト間隔は 5 秒で、範囲は 1 ～ 60 秒です。 |
| ステップ 3 | switch(config)# <b>exit</b>                                  | コンフィギュレーション モードを終了します。                                           |
| ステップ 4 | (Optional) switch# <b>show tacacs-server</b>                 | TACACS+ サーバーの設定を表示します。                                           |
| ステップ 5 | (Optional) switch# <b>copy running-config startup-config</b> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                        |

## サーバーのタイムアウト間隔の設定

Cisco Nexus デバイスが、タイムアウト エラーを宣言する前に、TACACS+ サーバからの応答を待機するタイムアウト間隔を設定できます。タイムアウト間隔は、スイッチがタイムアウトエラーを宣言する前に、TACACS+ サーバーからの応答を待機する時間を決定します。

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **exit**
3. (Optional) switch# **show tacacs-server**
4. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

## Procedure

|        | Command or Action                                            | Purpose                                   |
|--------|--------------------------------------------------------------|-------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                            | グローバル コンフィギュレーション モードを開始します。              |
| ステップ 2 | switch(config)# <b>exit</b>                                  | コンフィギュレーション モードを終了します。                    |
| ステップ 3 | (Optional) switch# <b>show tacacs-server</b>                 | TACACS+ サーバーの設定を表示します。                    |
| ステップ 4 | (Optional) switch# <b>copy running-config startup-config</b> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。 |

## TCP ポートの設定

別のアプリケーションとポート番号が競合している場合は、TACACS+ サーバ用に別の TCP ポートを設定できます。デフォルトでは、Cisco Nexus デバイスは、すべての TACACS+ 要求にポート 49 を使用します。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **exit**
3. (Optional) switch# **show tacacs-server**
4. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

#### Procedure

|        | Command or Action                                            | Purpose                                   |
|--------|--------------------------------------------------------------|-------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                            | グローバル コンフィギュレーション モードを開始します。              |
| ステップ 2 | switch(config)# <b>exit</b>                                  | コンフィギュレーション モードを終了します。                    |
| ステップ 3 | (Optional) switch# <b>show tacacs-server</b>                 | TACACS+ サーバーの設定を表示します。                    |
| ステップ 4 | (Optional) switch# <b>copy running-config startup-config</b> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。 |

#### Example

次に、TCP ポートを設定する例を示します。

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.1.1 port 2
switch(config)# exit
switch# show tacacs-server
switch# copy running-config startup-config
```

## TACACS+ サーバーの定期的モニタリングの設定

TACACS+ サーバーの可用性をモニタリングできます。パラメータとして、サーバーに使用するユーザー名とパスワード、およびアイドルタイマーがあります。アイドルタイマーには、TACACS+ サーバーがどのくらいの期間要求を受信しなかった場合に、Cisco Nexus デバイスがテストパケットを送信するかを指定します。このオプションを設定して、サーバーを定期的にテストしたり、1 回だけテストを実行したりすることができます。



**Note** ネットワークのセキュリティ保護のため、TACACS+ データベース内の既存のユーザ名と同じユーザ名を使用しないことを推奨します。

テストアイドルタイマーには、TACACS+サーバーがどのくらいの期間要求を受信しなかった場合に、Cisco Nexus デバイスがテスト パケットを送信するかを指定します。



**Note** デフォルトのアイドル タイマー値は 0 分です。アイドル タイム間隔が 0 分の場合、TACACS+ サーバの定期的なモニタリングは実行されません。

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **tacacs-server dead-time minutes**
3. switch(config)# **exit**
4. (Optional) switch# **show tacacs-server**
5. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

### Procedure

|        | Command or Action                                            | Purpose                                                                                         |
|--------|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                            | グローバル コンフィギュレーション モードを開始します。                                                                    |
| ステップ 2 | switch(config)# <b>tacacs-server dead-time minutes</b>       | Cisco Nexus デバイスが、前回応答しなかった TACACS+サーバーをチェックするまでの時間（分）を指定します。デフォルト値は 0 分、指定できる範囲は 0 ～ 1440 分です。 |
| ステップ 3 | switch(config)# <b>exit</b>                                  | コンフィギュレーション モードを終了します。                                                                          |
| ステップ 4 | (Optional) switch# <b>show tacacs-server</b>                 | TACACS+ サーバーの設定を表示します。                                                                          |
| ステップ 5 | (Optional) switch# <b>copy running-config startup-config</b> | 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。                                                      |

### Example

次に、TACACS+ サーバーの定期的モニタリングを設定する例を示します。

```
switch# configure terminal
```

```

switch(config)# tacacs-server host 10.10.1.1 test username user1 password Ur2Gd2BH
idle-time 3
switch(config)# tacacs-server dead-time 5
switch(config)# exit
switch# show tacacs-server
switch# copy running-config startup-config

```

## デッドタイム間隔の設定

すべての TACACS+ サーバーのデッドタイム間隔を設定できます。デッドタイム間隔には、Cisco Nexus デバイスが TACACS+ サーバをデッド状態であると宣言した後、そのサーバがアライブ状態に戻ったかどうかを判断するためにテストパケットを送信するまでの間隔を指定します。



**Note** デッドタイム間隔が 0 分の場合、TACACS+ サーバーは、応答を返さない場合でも、デッドとしてマークされません。デッドタイム間隔はグループ単位で設定できます。「[TACACS+ サーバグループの設定, on page 71](#)」を参照してください。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **tacacs-server deadtime** *minutes*
3. switch(config)# **exit**
4. (Optional) switch# **show tacacs-server**
5. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

#### Procedure

|        | Command or Action                                            | Purpose                                                 |
|--------|--------------------------------------------------------------|---------------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                            | グローバル コンフィギュレーション モードを開始します。                            |
| ステップ 2 | switch(config)# <b>tacacs-server deadtime</b> <i>minutes</i> | グローバルなデッドタイム間隔を設定します。デフォルト値は 0 分です。有効な範囲は 1 ～ 1440 分です。 |
| ステップ 3 | switch(config)# <b>exit</b>                                  | コンフィギュレーション モードを終了します。                                  |
| ステップ 4 | (Optional) switch# <b>show tacacs-server</b>                 | TACACS+ サーバーの設定を表示します。                                  |
| ステップ 5 | (Optional) switch# <b>copy running-config startup-config</b> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。               |

## TACACS サーバーを使用した X.509 証明書ベースの SSH 認証の設定

Cisco NX-OS リリース 10.4(3)F 以降では、Cisco Nexus スイッチの TACACS+ サーバーを使用して、x509v3 証明書の SSH ベースの認証を設定できます。

TACACS+ サーバーを使用して X.509 証明書ベースの SSH 認証を設定するには、次の手順に従います。

### 手順の概要

1. **configure terminal**
2. **aaa authorization ssh-certificate default group tacacs-group-name**
3. **exit**
4. (任意) **show aaa authorization [all]**
5. (任意) **copy running-config startup-config**

### 手順の詳細

#### 手順

|        | コマンドまたはアクション                                                                                                                                                      | 目的                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br><pre>switch# configure terminal switch(config)#</pre>                                                                         | グローバル コンフィギュレーション モードを開始します。                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| ステップ 2 | <b>aaa authorization ssh-certificate default group tacacs-group-name</b><br>例 :<br><pre>switch(config)# aaa authorization ssh-certificate default group tac</pre> | <p>TACACS+ サーバーのデフォルトの AAA 許可方式を設定します。</p> <p><b>ssh-certificate</b> キーワードは、証明書認証を使用した TACACS 許可またはローカル許可を構成します。デフォルトの許可は、ユーザに割り当てたロールに対して許可されたコマンドのリストであるローカル許可です。</p> <p>(注)</p> <ul style="list-style-type: none"> <li>• <b>aaa group server tacacs+ tacacs-group-name</b> コマンドを使用して、TACACS サーバー構成で <i>tacacs-group-name</i> が構成されていることを確認します。</li> <li>• SSH 証明書ベースの認証をサポートするには、暗号トラストポイントを設定し、ルート CA をインストールします。詳細については、<a href="#">PKI の設定 (129 ページ)</a> のセクションを参照してください。</li> </ul> |



|        | コマンドまたはアクション                                                                                                      | 目的                                                    |
|--------|-------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| ステップ 3 | <b>exit</b><br><br>例 :<br>switch(config)# <b>exit</b><br>switch#                                                  | グローバル コンフィギュレーション モードを終了します。                          |
| ステップ 4 | (任意) <b>show aaa authorization [all]</b><br><br>例 :<br>switch# show aaa authorization                             | AAA 許可設定を表示します。 <b>all</b> キーワードを指定すると、デフォルト値が表示されます。 |
| ステップ 5 | (任意) <b>copy running-config startup-config</b><br><br>例 :<br>switch# <b>copy running-config</b><br>startup-config | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。             |

## TACACS+ サーバまたはサーバグループの手動モニタリング

### SUMMARY STEPS

1. switch# **test aaa server tacacs+ {ipv4-address | host-name} [vrf vrf-name] username password**
2. switch# **test aaa group group-name username password**

### DETAILED STEPS

#### Procedure

|        | Command or Action                                                                                  | Purpose                                    |
|--------|----------------------------------------------------------------------------------------------------|--------------------------------------------|
| ステップ 1 | switch# <b>test aaa server tacacs+ {ipv4-address   host-name} [vrf vrf-name] username password</b> | TACACS+ サーバーにテスト メッセージを送信して可用性を確認します。      |
| ステップ 2 | switch# <b>test aaa group group-name username password</b>                                         | TACACS+ サーバー グループにテスト メッセージを送信して可用性を確認します。 |

#### Example

次に、手動でテスト メッセージを送信する例を示します。

```
switch# test aaa server tacacs+ 10.10.1.1 user1 Ur2Gd2BH
switch# test aaa group TacGroup user2 As3He3CI
```

## TACACS+ のディセーブル化

TACACS+ をディセーブルにできます。

**Caution**

TACACS+ をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。

**SUMMARY STEPS**

1. switch# **configure terminal**
2. switch(config)# **no feature tacacs+**
3. switch(config)# **exit**
4. (Optional) switch# **copy running-config startup-config**

**DETAILED STEPS****Procedure**

|        | Command or Action                                            | Purpose                                   |
|--------|--------------------------------------------------------------|-------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                            | グローバル コンフィギュレーション モードを開始します。              |
| ステップ 2 | switch(config)# <b>no feature tacacs+</b>                    | TACACS+ をディセーブルにします。                      |
| ステップ 3 | switch(config)# <b>exit</b>                                  | コンフィギュレーション モードを終了します。                    |
| ステップ 4 | (Optional) switch# <b>copy running-config startup-config</b> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。 |

**TACACS+ 統計情報の表示**

スイッチが TACACS+ のアクティビティについて保持している統計情報を表示するには、次の作業を行います。

**SUMMARY STEPS**

1. switch# **show tacacs-server statistics** [hostname | ipv4-address | ipv6-address]

**DETAILED STEPS****Procedure**

|        | Command or Action                                                                     | Purpose                                                                                 |
|--------|---------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| ステップ 1 | switch# <b>show tacacs-server statistics</b> [hostname   ipv4-address   ipv6-address] | TACACS+ 統計情報を表示します。<br><br><b>Note</b><br>ipv6-address パラメータは Nexus 3548 ではサポートされていません。 |

**Example**

このコマンドの出力フィールドの詳細については、Nexus スイッチの『*Command Reference*』を参照してください。

**TACACS+ の設定の確認**

TACACS+ の情報を表示するには、次のいずれかの作業を行います：

| コマンド                                                                                                                 | 目的                                                    |
|----------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| <b>show tacacs+ {status   pending   pending-diff}</b>                                                                | Cisco Fabric Services の TACACS+ 設定の配布状況と他の詳細事項を表示します。 |
| <b>show running-config tacacs [all]</b>                                                                              | 実行コンフィギュレーションの TACACS+ 設定を表示します。                      |
| <b>show startup-config tacacs</b>                                                                                    | スタートアップ コンフィギュレーションの TACACS+ 設定を表示します。                |
| <b>show tacacs-serve [host-name   ipv4-address   ipv6-address] [directed-request   groups   sorted   statistics]</b> | 設定済みのすべての TACACS+ サーバーのパラメータを表示します。                   |

**TACACS+ の設定例**

次に、TACACS+ を設定する例を示します。

```
switch# configure terminal
switch(config)# feature tacacs+
switch(config)# tacacs-server key 7 "ToIkLhPpG"
switch(config)# tacacs-server host 10.10.2.2 key 7 "ShMoMhTl"
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# server 10.10.2.2
switch(config-tacacs+)# use-vrf management
```

次に、TACACS+ をイネーブルにし、TACACS+ サーバーの事前共有キーを設定して、サーバーグループ TacServer1 を認証するためにリモート AAA サーバーを指定する例を示します。

```
switch# configure terminal
switch(config)# feature tacacs+
switch(config)# tacacs-server key 7 "ikvhw10"
switch(config)# tacacs-server host 1.1.1.1
switch(config)# tacacs-server host 1.1.1.2

switch(config)# aaa group server tacacs+ TacServer1
switch(config-tacacs+)# server 1.1.1.1
switch(config-tacacs+)# server 1.1.1.2
```

## TACACS+ のデフォルト設定

次の表に、TACACS+ パラメータのデフォルト設定を示します。

**Table 8: TACACS+ のデフォルト パラメータ**

| パラメータ               | デフォルト  |
|---------------------|--------|
| TACACS+             | ディセーブル |
| デッドタイム間隔            | 0 分    |
| タイムアウト間隔            | 5 秒    |
| アイドル タイマー間隔         | 0 分    |
| サーバの定期的モニタリングのユーザ名  | test   |
| サーバの定期的モニタリングのパスワード | テスト    |



## 第 6 章

# LDAP の設定

この章では、Cisco NX-OS デバイス上で Lightweight Directory Access Protocol (LDAP) を設定する方法について説明します。次の項が含まれています。

- [LDAP について \(83 ページ\)](#)
- [LDAP の前提条件 \(86 ページ\)](#)
- [LDAP の注意事項と制約事項 \(87 ページ\)](#)
- [LDAP のデフォルト設定 \(87 ページ\)](#)
- [LDAP の設定 \(88 ページ\)](#)
- [LDAP サーバのモニタリング \(104 ページ\)](#)
- [LDAP サーバ統計情報のクリア \(105 ページ\)](#)
- [LDAP 設定の確認 \(106 ページ\)](#)
- [LDAP の設定例 \(106 ページ\)](#)
- [次の作業 \(107 ページ\)](#)

## LDAP について

Lightweight Directory Access Protocol (LDAP) は、Cisco NX-OS デバイスにアクセスしようとするユーザの検証を集中的に行います。LDAP サービスは、通常 UNIX または Windows NT ワークステーション上で稼働する LDAP デーモンのデータベースで管理されます。Cisco NX-OS デバイスに設定した LDAP 機能を使用可能にするには、LDAP サーバにアクセスして設定しておく必要があります。

LDAP では、認証と認可のファシリティが別々に提供されます。LDAP では、1 台のアクセスコントロールサーバ (LDAP デーモン) で各サービス認証と認可を個別に提供できます。各サービスを固有のデータベースに結合し、デーモンの機能に応じてそのサーバまたはネットワークで利用できる他のサービスを使用できます。

LDAP クライアント/サーバプロトコルでは、トランスポート要件を満たすために、TCP (ポート 389) を使用します。Cisco NX-OS デバイスは、LDAP プロトコルを使用して集中型の認証を行います。

## LDAP 認証および許可

クライアントは、簡易バインド（ユーザ名とパスワード）を使用して LDAP サーバとの TCP 接続および認証セッションを確立します。許可プロセスの一環として、LDAP サーバはそのデータベースを検索し、ユーザ プロファイルやその他の情報を取得します。

バインドしてから検索する（認証を行ってから許可する）か、または検索してからバインドするように、バインド操作を設定できます。デフォルトでは、検索してからバインドする方式が使用されます。

検索してからバインドする方式の利点は、baseDN の前にユーザ名（cn 属性）を追加することで認定者名（DN）を形成するのではなく、検索結果で受け取った DN をバインディング時にユーザ DN として使用できることです。この方式は、ユーザ DN がユーザ名と baseDN の組み合わせとは異なる場合に特に役立ちます。ユーザ バインドのために、bindDN が baseDN + append-with-baseDN として構成されます。ここで、append-with-baseDN は cn=\$userid のデフォルト値です。



(注) バインド方式の代わりに、比較方式を使用して LDAP 認証を確立することもできます。比較方式では、サーバでユーザ入力の属性値を比較します。たとえば、ユーザパスワード属性を比較して認証を行うことができます。デフォルトのパスワード属性タイプは userPassword です。

## ユーザ ログインにおける LDAP の動作

LDAP を使用する Cisco NX-OS デバイスに対して、ユーザがパスワード認証プロトコル（PAP）ログインを試みると、次の処理が行われます。

1. Cisco NX-OS デバイスは接続が確立されると、ユーザ名とパスワードを取得するために LDAP デーモンに接続します。
2. Cisco NX-OS デバイスは、最終的に LDAP デーモンから次のいずれかの応答を得ます。
  - **ACCEPT** : ユーザの認証に成功したので、サービスを開始します。Cisco NX-OS デバイスがユーザ許可を必要とする場合は、許可処理が始まります。
  - **REJECT** : ユーザ認証は失敗します。LDAP デーモンは、ユーザに対してそれ以上のアクセスを拒否するか、ログイン操作を再試行するように要求します。
  - **ERROR** : デーモンによる認証サービスの途中でエラーが発生したか、またはデーモンと Cisco NX-OS デバイスの間のネットワーク接続でエラーが発生しました。Cisco NX-OS デバイスは ERROR 応答を受信した場合、別の方法でユーザの認証を試行します。

認証が終了し、Cisco NX-OS デバイスで許可がイネーブルになっていれば、続いてユーザの許可フェーズに入ります。LDAP 許可に進むには、まず LDAP 認証を正常に終了する必要があります。

3. LDAP 許可が必要な場合、Cisco NX-OS デバイスは再び LDAP デーモンに接続し、デーモンから ACCEPT または REJECT 応答が返されます。ACCEPT 応答には、ユーザに対する EXEC または NETWORK セッションの送信に使用される属性が含まれます。また ACCEPT

応答により、ユーザがアクセス可能なサービスが決まります。この場合のサービスは次のとおりです。

- Telnet、rlogin、ポイントツーポイントプロトコル（PPP）、シリアルラインインターネットプロトコル（SLIP）、EXEC サービス
- 接続パラメータ（ホストまたはクライアントの IP アドレス（IPv4 または IPv6）、アクセスリスト、ユーザタイムアウト）



(注) LDAP では、デーモンがユーザを認証するために十分な情報を得られるまで、デーモンとユーザとの自由な対話を許可します。通常、デーモンはユーザ名とパスワードの組み合わせを入力するよう求めますが、他の項目を求めることもできます。

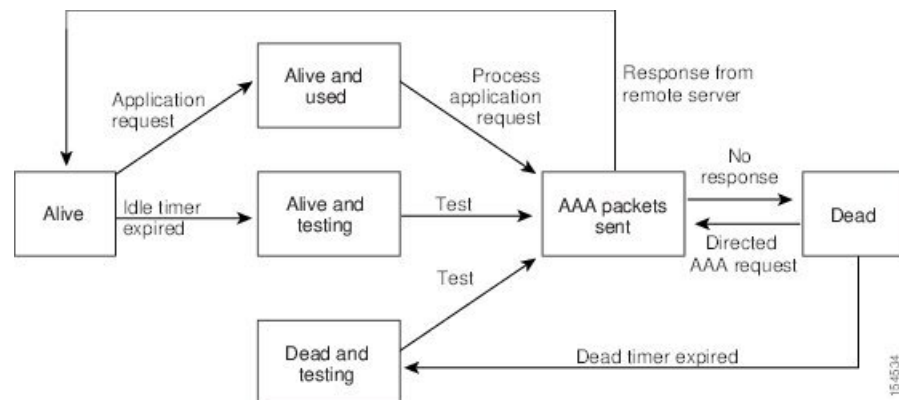


(注) LDAP では、認証の前に許可を行うことができます。

## LDAP サーバのモニタリング

応答を返さない LDAP サーバがあると、AAA 要求の処理に遅延が発生することがあります。AAA 要求の処理時間を短縮するために、LDAP サーバを定期的にモニタして LDAP サーバが応答している（アライブ）かどうかを調べることができます。Cisco NX-OS デバイスは、応答の遅い LDAP サーバをデッド（dead）としてマークし、デッド LDAP サーバには AAA 要求を送信しません。Cisco NX-OS デバイスはデッド LDAP サーバを定期的にモニタし、応答があればアライブ状態に戻します。このモニタリングプロセスでは、実際の AAA 要求が送信される前に、LDAP サーバが稼働状態であることを確認します。LDAP サーバがデッドまたはアライブの状態に変わると、簡易ネットワーク管理プロトコル（SNMP）トラップが生成され、Cisco NX-OS デバイスは、パフォーマンスに影響が出る前に、障害が発生していることをエラーメッセージで表示します。次の図に、LDAP サーバモニタリングのサーバの状態を示します。

図 4: LDAP サーバの状態





- (注) 稼働中のサーバと停止中のサーバのモニタリング間隔はそれぞれ別で、ユーザが設定できません。LDAP サーバ モニタリングを実行するには、テスト認証要求を LDAP サーバに送信します。

## LDAP のベンダー固有属性

Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) ドラフト標準には、ネットワーク アクセス サーバと LDAP サーバ間での Vendor-Specific Attribute (VSA; ベンダー固有属性) の通信方法が規定されています。IETF は属性 26 を使用します。ベンダーは VSA を使用して、一般的な用途には適さない独自の拡張属性をサポートできます。

### LDAP 用の Cisco VSA 形式

シスコの LDAP 実装では、IETF 仕様で推奨される形式を使用したベンダー固有オプションを 1 つサポートしています。シスコのベンダー ID は 9、サポートされるオプションのベンダータイプは 1 (名前付き `cisco-av-pair`) です。値は次の形式のストリングです。

```
protocol : attribute separator value *
```

`protocol` は、特定の許可タイプを表すシスコの属性です。`separator` は、必須属性の場合は `=` (等号)、オプションの属性の場合は `*` (アスタリスク) です。Cisco NX-OS デバイス上の認証に LDAP サーバを使用した場合、LDAP では LDAP サーバに対して、認証結果とともに権限付与情報などのユーザ属性を返すように指示します。この許可情報は、VSA で指定されます。Cisco NX-OS ソフトウェアでは、次の VSA プロトコル オプションをサポートしています。

- `shell` : ユーザ プロファイル情報を提供する `access-accept` パケットで使用するプロトコル。

Cisco NX-OS ソフトウェアは、次の属性をサポートしています。

- `roles` : ユーザが属するすべてのロールの一覧です。値フィールドは、スペースで区切られたロール名を一覧表示したストリングです。

## LDAP のバーチャライゼーション サポート

Cisco NX-OS デバイスは、仮想ルーティング/転送 (VRF) インスタンスを使用して LDAP サーバにアクセスします。VRF の詳細情報については、を参照してください。Cisco Nexus 3600 スイッチ NX-OS ユニキャスト ルーティング構成ガイド

## LDAP の前提条件

LDAP の前提条件は次のとおりです。

- LDAP サーバの IPv4 または IPv6 アドレスまたはホスト名を取得すること
- Cisco NX-OS デバイスが AAA サーバの LDAP クライアントとして設定されていること



## LDAP の注意事項と制約事項

LDAP に関する注意事項と制約事項は次のとおりです。

- Cisco NX-OS デバイス上には最大 64 の LDAP サーバを設定できます。
- Cisco NX-OS は LDAP バージョン 3 だけをサポートします。
- Cisco NX-OS は次の LDAP サーバだけをサポートします。
  - OpenLDAP
  - Microsoft Active Directory
- Secure Sockets Layer (SSL) 上の LDAP は、SSL バージョン 3 および Transport Layer Security (TLS) バージョン 1.2 のみをサポートします。
- Cisco NX-OS リリース 10.4(3)F 以降、Secure Sockets Layer (SSL) を介した LDAP は、Cisco Nexus スイッチで TLS バージョン 1.3 および 1.2 をサポートします。TLS v1.1 は廃止されました。
- LDAP over SSL の場合、LDAP クライアント設定では、LDAP サーバ証明書のサブジェクトとしてホスト名を含める必要があります。
- ローカルの Cisco NX-OS デバイス上に設定されているユーザ アカウントが、AAA サーバ上のリモート ユーザ アカウントと同じ名前の場合、Cisco NX-OS ソフトウェアは、AAA サーバ上に設定されているユーザ ロールではなく、ローカル ユーザ アカウントのユーザ ロールをリモート ユーザに適用します。
- Cisco NX-OS リリース 10.3(1)F 以降、LDAP は Cisco Nexus 9808 スイッチでサポートされます。
  - Cisco NX-OS リリース 10.4(1)F 以降、LDAP は、Cisco Nexus X98900CD-A および X9836DM-A ラインカードを搭載した Cisco Nexus 9808 スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、LDAP は Cisco Nexus 9804 スイッチ、Cisco Nexus X98900CD-A および X9836DM-A ラインカードでサポートされます。
- Cisco NX-OS リリース 10.4(2)F 以降、構成の置換機能は Cisco NX-OS デバイスの LDAP でサポートされます。

## LDAP のデフォルト設定

次の表に、LDAP パラメータのデフォルト設定を示します。

| パラメータ | デフォルト  |
|-------|--------|
| LDAP  | ディセーブル |

| パラメータ               | デフォルト      |
|---------------------|------------|
| LDAP 認証方式           | 検索してからバインド |
| LDAP 認証メカニズム        | プレーン       |
| デッドタイム間隔            | 0 分        |
| タイムアウト間隔            | 5 秒        |
| アイドル タイマー間隔         | 60 分       |
| サーバの定期的モニタリングのユーザ名  | test       |
| サーバの定期的モニタリングのパスワード | Cisco      |

## LDAP の設定

ここでは、Cisco NX-OS デバイスで LDAP を設定する手順を説明します。

## LDAP サーバの設定プロセス

次の設定プロセスに従って、LDAP サーバを設定できます。

1. LDAP をイネーブルにします。
2. LDAP サーバと Cisco NX-OS デバイスの接続を確立します。
3. 必要に応じて、AAA 認証方式用に、LDAP サーバのサブセットを使用して LDAP サーバグループを設定します。
4. (任意) TCP ポートを設定します。
5. (任意) LDAP サーバにデフォルト AAA 認証方式を設定します。
6. (任意) LDAP 検索マップを設定します。
7. (任意) 必要に応じて、LDAP サーバの定期モニタリングを設定します。

### 関連トピック

[LDAP のイネーブル化/ディセーブル化](#) (89 ページ)

[LDAP サーバホストの設定](#) (90 ページ)

[LDAP サーバの rootDN の設定](#) (91 ページ)

[LDAP サーバグループの設定](#) (92 ページ)

[TCP ポートの設定](#) (96 ページ)

[LDAP 検索マップの設定](#) (98 ページ)

[LDAP サーバの定期的モニタリングの設定](#) (99 ページ)

## LDAP のイネーブル化/ディセーブル化

デフォルトでは、Cisco NX-OS デバイスの LDAP 機能はディセーブルになっています。認証に関するコンフィギュレーションコマンドと検証コマンドを使用するには、LDAP 機能を明示的にイネーブルにする必要があります。

### 手順の概要

1. **configure terminal**
2. **[no] feature ldap**
3. (任意) **copy running-config startup-config**

### 手順の詳細

#### 手順

|        | コマンドまたはアクション                                                                                                               | 目的                                                                                                              |
|--------|----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例 :<br><pre>switch# configure terminal switch(config)#</pre>                              | グローバル設定モードを開始します。                                                                                               |
| ステップ 2 | 必須: <b>[no] feature ldap</b><br><br>例 :<br><pre>switch(config)# feature ldap</pre>                                         | LDAP をイネーブルにします。LDAP を無効にするには、このコマンドの <b>no</b> 形式を使用します。<br><br>(注)<br>LDAP をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。 |
| ステップ 3 | (任意) <b>copy running-config startup-config</b><br><br>例 :<br><pre>switch(config)# copy running-config startup-config</pre> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                                       |

### 関連トピック

- [LDAP サーバの設定プロセス \(88 ページ\)](#)
- [LDAP サーバ ホストの設定 \(90 ページ\)](#)
- [LDAP サーバの rootDN の設定 \(91 ページ\)](#)
- [LDAP サーバ グループの設定 \(92 ページ\)](#)
- [グローバルな LDAP タイムアウト間隔の設定 \(94 ページ\)](#)
- [LDAP サーバのタイムアウト間隔の設定 \(95 ページ\)](#)
- [TCP ポートの設定 \(96 ページ\)](#)
- [LDAP 検索マップの設定 \(98 ページ\)](#)
- [LDAP サーバの定期的モニタリングの設定 \(99 ページ\)](#)

[LDAP デッドタイム間隔の設定 \(100 ページ\)](#)

[LDAP サーバでの AAA 許可の設定 \(101 ページ\)](#)

## LDAP サーバホストの設定

リモートの LDAP サーバにアクセスするには、Cisco NX-OS デバイス上でその LDAP サーバの IP アドレスまたはホスト名を設定する必要があります。最大 64 の LDAP サーバを設定できます。



**Note** デフォルトでは、LDAP サーバの IP アドレスまたはホスト名を Cisco NX-OS デバイスで設定すると、LDAP サーバがデフォルトの LDAP サーバグループに追加されます。LDAP サーバを別の LDAP サーバグループに追加することもできます。

### Before you begin

LDAP を有効にします。

リモートの LDAP サーバの IPv4 または IPv6 アドレスまたはホスト名を取得します。

Secure Sockets Layer (SSL) プロトコルをイネーブルにする予定の場合は、Cisco NX-OS デバイスで LDAP サーバ証明書を手動で設定します。

### SUMMARY STEPS

1. **configure terminal**
2. **[no] ldap-server host {ipv4-address | ipv6-address | host-name} [enable-ssl] [referral-disable]**
3. (Optional) **show ldap-server**
4. (Optional) **copy running-config startup-config**

### DETAILED STEPS

#### Procedure

|        | Command or Action                                                                                                                                                                             | Purpose                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>                                                                                         | グローバル コンフィギュレーション モードを開始します                                                                                           |
| ステップ 2 | <b>[no] ldap-server host {ipv4-address   ipv6-address   host-name} [enable-ssl] [referral-disable]</b><br><b>Example:</b><br><pre>switch(config)# ldap-server host 10.10.2.2 enable-ssl</pre> | LDAP サーバの IPv4 または IPv6 アドレス、あるいはホスト名を指定します。<br><br><b>enable-ssl</b> キーワードは、LDAP クライアントに SSL セッションを確立させてからバインドまたは検索の |

|        | Command or Action                                                                                                                              | Purpose                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
|        |                                                                                                                                                | 要求を送信することにより、転送されたデータの整合性と機密保持を保証します。<br><br>キーワードは、不要な参照リンクをディセーブルにします。 <b>referral-disable</b> |
| ステップ 3 | (Optional) <b>show ldap-server</b><br><br><b>Example:</b><br><code>switch(config)# show ldap-server</code>                                     | LDAP サーバの設定を表示します。                                                                               |
| ステップ 4 | (Optional) <b>copy running-config startup-config</b><br><br><b>Example:</b><br><code>switch(config)# copy running-config startup-config</code> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                        |

### Related Topics

- [LDAP サーバの設定プロセス \(88 ページ\)](#)
- [LDAP のイネーブル化/ディセーブル化 \(89 ページ\)](#)
- [LDAP サーバ グループの設定 \(92 ページ\)](#)
- [LDAP サーバの rootDN の設定 \(91 ページ\)](#)
- [LDAP サーバ グループの設定 \(92 ページ\)](#)
- [LDAP サーバの定期的モニタリングの設定 \(99 ページ\)](#)
- [LDAP サーバのモニタリング \(104 ページ\)](#)
- [LDAP サーバ統計情報のクリア \(105 ページ\)](#)

## LDAP サーバの rootDN の設定

LDAP サーバデータベースのルート指定名 (DN) を設定できます。rootDN は、LDAP サーバにバインドしてそのサーバの状態を確認するために使用します。

### 始める前に

LDAP を有効にします。

リモートの LDAP サーバの IPv4 または IPv6 アドレスまたはホスト名を取得します。

### 手順の概要

1. **configure terminal**
2. **[no] ldap-server host {ipv4-address | ipv6-address | hostname} rootDN root-name [password password [port tcp-port [timeout seconds] | timeout seconds]]**
3. (任意) **show ldap-server**
4. (任意) **copy running-config startup-config**

## 手順の詳細

## 手順

|        | コマンドまたはアクション                                                                                                                                                                                                                                                                                 | 目的                                                                                                                                                                                                                                                        |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br><pre>switch# configure terminal switch(config)#</pre>                                                                                                                                                                                                    | グローバル コンフィギュレーション モードを開始します                                                                                                                                                                                                                               |
| ステップ 2 | <b>[no] ldap-server host {ipv4-address   ipv6-address   hostname} rootDN root-name [password password [port tcp-port [timeout seconds]   timeout seconds]]</b><br>例 :<br><pre>switch(config)# ldap-server host 10.10.1.1 rootDN cn=manager,dc=acme,dc=com password Ur2Gd2BH timeout 60</pre> | LDAP サーバデータベースの rootDN を指定し、ルートのパスワードをバインドします。<br><br>任意で、サーバに送る LDAP メッセージに使用する TCP ポートを指定します。有効な範囲は 1 ～ 65535 です。デフォルトの TCP ポートはグローバル値です（グローバル値が設定されていない場合は 389）。また、サーバのタイムアウト間隔も指定します。値の範囲は 1 ～ 60 秒です。デフォルトのタイムアウト値はグローバル値です（グローバル値が設定されていない場合は 5 秒）。 |
| ステップ 3 | （任意） <b>show ldap-server</b><br>例 :<br><pre>switch(config)# show ldap-server</pre>                                                                                                                                                                                                           | LDAP サーバの設定を表示します。                                                                                                                                                                                                                                        |
| ステップ 4 | （任意） <b>copy running-config startup-config</b><br>例 :<br><pre>switch(config)# copy running-config startup-config</pre>                                                                                                                                                                       | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                                                                                                                                                                                 |

## 関連トピック

[LDAP サーバの設定プロセス](#)（88 ページ）

[LDAP のイネーブル化/ディセーブル化](#)（89 ページ）

[LDAP サーバホストの設定](#)（90 ページ）

## LDAP サーバグループの設定

サーバグループを使用して、1 台または複数台のリモート AAA サーバによるユーザ認証を指定することができます。グループのメンバはすべて、LDAP を使用するよう設定する必要があります。設定した順序に従ってサーバが試行されます。

これらのサーバグループはいつでも設定できますが、設定したグループを有効にするには、AAA サービスに適用する必要があります。

**Before you begin**

LDAP を有効にします。

**SUMMARY STEPS**

1. **configure terminal**
2. **[no] aaa group server ldap group-name**
3. **[no] server {ipv4-address | ipv6-address | host-name}**
4. (Optional) **[no] authentication {bind-first [append-with-baseDN DNstring] | compare [password-attribute password]}**
5. (Optional) **[no] enable user-server-group**
6. (Optional) **[no] enable Cert-DN-match**
7. (Optional) **no [use-vrf vrf-name]**
8. **exit**
9. (Optional) **show ldap-server groups**
10. (Optional) **copy running-config startup-config**

**DETAILED STEPS****Procedure**

|        | Command or Action                                                                                                                                                                                                               | Purpose                                                                                                                           |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>                                                                                                                           | グローバル コンフィギュレーション モードを開始します                                                                                                       |
| ステップ 2 | <b>[no] aaa group server ldap group-name</b><br><b>Example:</b><br><pre>switch(config)# aaa group server ldap LDAPServer1 switch(config-ldap)#</pre>                                                                            | 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。                                                                      |
| ステップ 3 | <b>[no] server {ipv4-address   ipv6-address   host-name}</b><br><b>Example:</b><br><pre>switch(config-ldap)# server 10.10.2.2</pre>                                                                                             | LDAP サーバを、LDAP サーバグループのメンバーとして設定します。<br><br>指定した LDAP サーバが見つからなかった場合は、 <b>ldap-server host</b> コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。 |
| ステップ 4 | (Optional) <b>[no] authentication {bind-first [append-with-baseDN DNstring]   compare [password-attribute password]}</b><br><b>Example:</b><br><pre>switch(config-ldap)# authentication compare password-attribute TyuL8r</pre> | バインド方式または比較方式を使用して LDAP 認証を実行します。デフォルトの LDAP 認証方式は、検索してからバインドするバインド方式です。                                                          |

|         | Command or Action                                                                                                                 | Purpose                                                                                                        |
|---------|-----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| ステップ 5  | (Optional) <b>[no] enable user-server-group</b><br><br><b>Example:</b><br>switch(config-ldap)# enable user-server-group           | グループ検証を有効にします。LDAP サーバでグループ名を設定する必要があります。ユーザは、ユーザ名が LDAP サーバで設定されたこのグループのメンバとして示されている場合にだけ、公開キー認証を通じてログインできます。 |
| ステップ 6  | (Optional) <b>[no] enable Cert-DN-match</b><br><br><b>Example:</b><br>switch(config-ldap)# enable Cert-DN-match                   | ユーザ プロファイルでユーザ証明書のサブジェクト DN がログイン可能と示されている場合にだけユーザがログインできるようにします。                                              |
| ステップ 7  | (Optional) <b>no [use-vrf vrf-name]</b><br><br><b>Example:</b><br>switch(config-ldap)# use-vrf vrf1                               | サーバグループ内のサーバとの接続に使用する VRF を指定します。                                                                              |
| ステップ 8  | <b>exit</b><br><br><b>Example:</b><br>switch(config-ldap)# exit<br>switch(config)#                                                | LDAP サーバ グループ コンフィギュレーション モードを終了します。                                                                           |
| ステップ 9  | (Optional) <b>show ldap-server groups</b><br><br><b>Example:</b><br>switch(config)# show ldap-server groups                       | LDAP サーバ グループの設定を表示します。                                                                                        |
| ステップ 10 | (Optional) <b>copy running-config startup-config</b><br><br><b>Example:</b><br>switch(config)# copy running-config startup-config | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                                      |

#### Related Topics

[LDAP サーバの設定プロセス](#) (88 ページ)

[LDAP サーバホストの設定](#) (90 ページ)

[LDAP のイネーブル化/ディセーブル化](#) (89 ページ)

[LDAP サーバホストの設定](#) (90 ページ)

## グローバルな LDAP タイムアウト間隔の設定

Cisco NX-OS デバイスがすべての LDAP サーバからの応答を待つ時間を決定するグローバル タイムアウト間隔を設定できます。これを過ぎるとタイムアウト エラーになります。

始める前に

LDAP をイネーブルにします。



## 手順の概要

1. **configure terminal**
2. **[no] ldap-server timeout seconds**
3. (任意) **show ldap-server**
4. (任意) **copy running-config startup-config**

## 手順の詳細

## 手順

|        | コマンドまたはアクション                                                                                                           | 目的                                                               |
|--------|------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br><pre>switch# configure terminal switch(config)#</pre>                              | グローバル コンフィギュレーション モードを開始します                                      |
| ステップ 2 | <b>[no] ldap-server timeout seconds</b><br>例 :<br><pre>switch(config)# ldap-server timeout 10</pre>                    | LDAP サーバのタイムアウト間隔を指定します。デフォルトのタイムアウト間隔は 5 秒です。有効な範囲は 1 ～ 60 秒です。 |
| ステップ 3 | (任意) <b>show ldap-server</b><br>例 :<br><pre>switch(config)# show ldap-server</pre>                                     | LDAP サーバの設定を表示します。                                               |
| ステップ 4 | (任意) <b>copy running-config startup-config</b><br>例 :<br><pre>switch(config)# copy running-config startup-config</pre> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                        |

## 関連トピック

[LDAP のイネーブル化/ディセーブル化](#) (89 ページ)

[LDAP サーバのタイムアウト間隔の設定](#) (95 ページ)

[LDAP サーバのタイムアウト間隔の設定](#) (95 ページ)

## LDAP サーバのタイムアウト間隔の設定

Cisco NX-OS デバイスが LDAP サーバからの応答を待つ時間を決定するタイムアウト間隔を設定できます。これを過ぎるとタイムアウト エラーになります。

## 始める前に

LDAP をイネーブルにします。

## 手順の概要

1. **configure terminal**
2. **[no] ldap-server host {ipv4-address | ipv6-address | hostname} timeout seconds**
3. (任意) **show ldap-server**
4. (任意) **copy running-config startup-config**

## 手順の詳細

## 手順

|        | コマンドまたはアクション                                                                                                                                                       | 目的                                                                                                                      |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例 :<br><pre>switch# configure terminal switch(config)#</pre>                                                                      | グローバル コンフィギュレーション モードを開始します                                                                                             |
| ステップ 2 | <b>[no] ldap-server host {ipv4-address   ipv6-address   hostname} timeout seconds</b><br><br>例 :<br><pre>switch(config)# ldap-server host server1 timeout 10</pre> | 特定のサーバのタイムアウト間隔を指定します。デフォルトはグローバル値です。<br><br>(注)<br>特定の LDAP サーバに指定したタイムアウト間隔は、すべての LDAP サーバで使用するグローバルなタイムアウト間隔を上書きします。 |
| ステップ 3 | (任意) <b>show ldap-server</b><br><br>例 :<br><pre>switch(config)# show ldap-server</pre>                                                                             | LDAP サーバの設定を表示します。                                                                                                      |
| ステップ 4 | (任意) <b>copy running-config startup-config</b><br><br>例 :<br><pre>switch(config)# copy running-config startup-config</pre>                                         | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                                               |

## 関連トピック

[グローバルな LDAP タイムアウト間隔の設定](#) (94 ページ)

[LDAP のイネーブル化/ディセーブル化](#) (89 ページ)

[グローバルな LDAP タイムアウト間隔の設定](#) (94 ページ)

## TCP ポートの設定

別のアプリケーションとポート番号が競合している場合は、LDAPサーバ用に別のTCPポートを設定できます。デフォルトでは、Cisco NX-OS デバイスはすべての LDAP 要求に対しポート 389 を使用します。

始める前に

LDAP をイネーブルにします。

#### 手順の概要

1. **configure terminal**
2. **[no] ldap-server host {ipv4-address | ipv6-address | hostname} port tcp-port [timeout seconds]**
3. (任意) **show ldap-server**
4. (任意) **copy running-config startup-config**

#### 手順の詳細

##### 手順

|        | コマンドまたはアクション                                                                                                                                                                             | 目的                                                                                                                                                                                                                                                                        |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br><pre>switch# configure terminal switch(config)#</pre>                                                                                                | グローバル コンフィギュレーション モードを開始します                                                                                                                                                                                                                                               |
| ステップ 2 | <b>[no] ldap-server host {ipv4-address   ipv6-address   hostname} port tcp-port [timeout seconds]</b><br>例 :<br><pre>switch(config)# ldap-server host 10.10.1.1 port 200 timeout 5</pre> | <p>サーバに送る LDAP メッセージに使用する TCP ポートを指定します。デフォルトの TCP ポートは 389 です。有効な範囲は 1 ～ 65535 です。</p> <p>任意でサーバのタイムアウト間隔を指定します。値の範囲は 1 ～ 60 秒です。デフォルトのタイムアウト値はグローバル値です（グローバル値が設定されていない場合は 5 秒）。</p> <p>(注)<br/>特定の LDAP サーバに指定したタイムアウト間隔は、すべての LDAP サーバで使用されるグローバルなタイムアウト間隔を上書きします。</p> |
| ステップ 3 | (任意) <b>show ldap-server</b><br>例 :<br><pre>switch(config)# show ldap-server</pre>                                                                                                       | LDAP サーバの設定を表示します。                                                                                                                                                                                                                                                        |
| ステップ 4 | (任意) <b>copy running-config startup-config</b><br>例 :<br><pre>switch(config)# copy running-config startup-config</pre>                                                                   | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                                                                                                                                                                                                 |

#### 関連トピック

[LDAP サーバの設定プロセス](#) (88 ページ)

LDAP のイネーブル化/ディセーブル化 (89 ページ)

## LDAP 検索マップの設定

検索クエリーを LDAP サーバに送信するように LDAP 検索マップを設定できます。サーバはそのデータベースで、検索マップで指定された基準を満たすデータを検索します。

始める前に

LDAP をイネーブルにします。

### 手順の概要

1. **configure terminal**
2. **ldap search-map map-name**
3. (任意) **[userprofile | trustedCert | CRLLookup | user-certdn-match | user-pubkey-match | user-switch-bind] attribute-name attribute-name search-filter filter base-DN base-DN-name**
4. (任意) **exit**
5. (任意) **show ldap-search-map**
6. (任意) **copy running-config startup-config**

### 手順の詳細

#### 手順

|        | コマンドまたはアクション                                                                                                                                                                                                                                                                                                                                                         | 目的                                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br><pre>switch# configure terminal switch(config)#</pre>                                                                                                                                                                                                                                                                            | グローバル コンフィギュレーション モードを開始します。                                                                                                                                                                            |
| ステップ 2 | <b>ldap search-map map-name</b><br>例 :<br><pre>switch(config)# ldap search-map map1 switch(config-ldap-search-map)#</pre>                                                                                                                                                                                                                                            | LDAP 検索マップを設定します。                                                                                                                                                                                       |
| ステップ 3 | (任意) <b>[userprofile   trustedCert   CRLLookup   user-certdn-match   user-pubkey-match   user-switch-bind] attribute-name attribute-name search-filter filter base-DN base-DN-name</b><br>例 :<br><pre>switch(config-ldap-search-map)# userprofile attribute-name att-name search-filter (&amp;(objectClass=inetOrgPerson)(cn=\$userid)) base-DN dc=acme,dc=com</pre> | ユーザプロファイル、信頼できる証明書、CRL、証明書 DN 一致、公開キー一致、または user-switchgroup ルックアップ検索操作の属性名、検索フィルタ、およびベース DN を設定します。これらの値は、検索クエリーを LDAP サーバに送信するために使用されます。<br><b>Attribute-name</b> 引数は Nexus ロール定義を含む LDAP サーバ属性の名前です。 |

|        | コマンドまたはアクション                                                                                                               | 目的                                        |
|--------|----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| ステップ 4 | (任意) <b>exit</b><br><br>例 :<br><pre>switch(config-ldap-search-map)# exit switch(config)#</pre>                             | LDAP 検索マップ コンフィギュレーション モードを終了します。         |
| ステップ 5 | (任意) <b>show ldap-search-map</b><br><br>例 :<br><pre>switch(config)# show ldap-search-map</pre>                             | 設定された LDAP 検索マップを表示します。                   |
| ステップ 6 | (任意) <b>copy running-config startup-config</b><br><br>例 :<br><pre>switch(config)# copy running-config startup-config</pre> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。 |

#### 関連トピック

[LDAP サーバの設定プロセス](#) (88 ページ)

[LDAP のイネーブル化/ディセーブル化](#) (89 ページ)

## LDAP サーバの定期的モニタリングの設定

LDAP サーバの可用性をモニタリングできます。設定パラメータには、サーバに対して使用するユーザ名とパスワード、サーバにバインドして状態を確認するための rootDN、およびアイドル タイマーがあります。アイドル タイマーには、LDAP サーバで何の要求も受信されない状態の時間を指定します。これを過ぎると Cisco NX-OS デバイスはテスト パケットを送信します。このオプションを設定して定期的にサーバをテストしたり、1 回だけテストを実行したりできます。



(注) ネットワークのセキュリティを保護するために、LDAP データベースの既存のユーザ名と同じものを使用しないことを推奨します。

#### 始める前に

LDAP をイネーブルにします。

#### 手順の概要

1. **configure terminal**
2. **[no] ldap-server host {ipv4-address | ipv6-address | hostname} test rootDN root-name [idle-time minutes | password password [idle-time minutes] | username name [password password [idle-time minutes]]]**
3. **[no] ldap-server deadtime minutes**
4. (任意) **show ldap-server**

5. (任意) **copy running-config startup-config**

## 手順の詳細

## 手順

|        | コマンドまたはアクション                                                                                                                                                                                                                                                                                                                               | 目的                                                                                                                                                           |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例：<br>switch# configure terminal<br>switch(config)#                                                                                                                                                                                                                                                       | グローバル コンフィギュレーション モードを開始します                                                                                                                                  |
| ステップ 2 | 必須: <b>[no] ldap-server host {ipv4-address   ipv6-address   hostname} test rootDN root-name [idle-time minutes   password password [idle-time minutes]   username name [password password [idle-time minutes]]]</b><br><br>例：<br>switch(config)# ldap-server host 10.10.1.1 test rootDN root1 username user1 password Ur2Gd2BH idle-time 3 | サーバモニタリング用のパラメータを指定します。デフォルトのユーザ名はtest、デフォルトのパスワードはCiscoです。アイドル タイマーのデフォルト値は60分です。有効な範囲は1～1,440分です。<br><br>(注)<br>LDAP サーバ データベースの既存のユーザでないユーザを指定することを推奨します。 |
| ステップ 3 | <b>[no] ldap-server deadtime minutes</b><br><br>例：<br>switch(config)# ldap-server deadtime 5                                                                                                                                                                                                                                               | 以前に応答の遅かった LDAP サーバを Cisco NX-OS デバイスがチェックを始めるまでの分数を指定します。デフォルト値は0分です。そして、有効な範囲は0～60分です。                                                                     |
| ステップ 4 | (任意) <b>show ldap-server</b><br><br>例：<br>switch(config)# show ldap-server                                                                                                                                                                                                                                                                 | LDAP サーバの設定を表示します。                                                                                                                                           |
| ステップ 5 | (任意) <b>copy running-config startup-config</b><br><br>例：<br>switch(config)# copy running-config startup-config                                                                                                                                                                                                                             | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                                                                                    |

## 関連トピック

[LDAP サーバの設定プロセス](#) (88 ページ)[LDAP のイネーブル化/ディセーブル化](#) (89 ページ)[LDAP サーバ ホストの設定](#) (90 ページ)

## LDAP デッドタイム間隔の設定

すべての LDAP サーバのデッドタイム間隔を設定できます。デッドタイム間隔では、Cisco NX-OS デバイスが LDAP サーバをデッドであると宣言した後、そのサーバがアライブになったかどうかを確認するためにテスト パケットを送信するまでの時間を指定します。



(注) デッドタイム間隔に 0 分を設定すると、LDAP サーバは、応答を返さない場合でも、デッドとしてマークされません。デッドタイム間隔はグループ単位で設定できます。

#### 始める前に

LDAP をイネーブルにします。

#### 手順の概要

1. **configure terminal**
2. **[no] ldap-server deadtime minutes**
3. (任意) **show ldap-server**
4. (任意) **copy running-config startup-config**

#### 手順の詳細

##### 手順

|        | コマンドまたはアクション                                                                                                | 目的                                                 |
|--------|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br>switch# configure terminal<br>switch(config)#                           | グローバル コンフィギュレーション モードを開始します                        |
| ステップ 2 | <b>[no] ldap-server deadtime minutes</b><br>例 :<br>switch(config)# ldap-server deadtime 5                   | グローバルなデッドタイム間隔を設定します。デフォルト値は 0 分です。範囲は 0 ～ 60 分です。 |
| ステップ 3 | (任意) <b>show ldap-server</b><br>例 :<br>switch(config)# show ldap-server                                     | LDAP サーバの設定を表示します。                                 |
| ステップ 4 | (任意) <b>copy running-config startup-config</b><br>例 :<br>switch(config)# copy running-config startup-config | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。          |

#### 関連トピック

[LDAP のイネーブル化/ディセーブル化](#) (89 ページ)

## LDAP サーバでの AAA 許可の設定

LDAP サーバのデフォルトの AAA 許可方式を設定できます。

始める前に

LDAP を有効にします。

## 手順の概要

1. **configure terminal**
2. **aaa authorization {ssh-certificate | ssh-publickey} default {group group-list | local}**
3. (任意) **show aaa authorization [all]**
4. (任意) **copy running-config startup-config**

## 手順の詳細

### 手順

|        | コマンドまたはアクション                                                                                                                                                                                               | 目的                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br><pre>switch# configure terminal switch(config)#</pre>                                                                                                                  | グローバル コンフィギュレーション モードを開始します                                                                                                                                                                                                                                                                                                                                                          |
| ステップ 2 | <b>aaa authorization {ssh-certificate   ssh-publickey} default {group group-list   local}</b><br>例 :<br><pre>switch(config)# aaa authorization ssh-certificate default group LDAPServer1 LDAPServer2</pre> | <p>LDAP サーバのデフォルトの AAA 許可方式を設定します。</p> <p><b>ssh-certificate</b> キーワードは証明書認証を使用した LDAP 許可またはローカル許可を設定し、<br/> <b>ssh-publickey</b> キーワードは SSH 公開キーを使用した LDAP 許可またはローカル許可を設定します。デフォルトの許可は、ユーザに割り当てたロールに対して許可されたコマンドのリストであるローカル許可です。</p> <p><i>group-list</i> 引数には、LDAP サーバ グループ名をスペースで区切ったリストを指定します。このグループに属するサーバに対して、AAA 許可のためのアクセスが行われます。<b>local</b> 方式はローカルデータベースを使用して許可を行います。</p> |
| ステップ 3 | (任意) <b>show aaa authorization [all]</b><br>例 :<br><pre>switch(config)# show aaa authorization</pre>                                                                                                       | AAA 許可設定を表示します。 <b>all</b> キーワードを指定すると、デフォルト値が表示されます。                                                                                                                                                                                                                                                                                                                                |
| ステップ 4 | (任意) <b>copy running-config startup-config</b><br>例 :<br><pre>switch(config)# copy running-config startup-config</pre>                                                                                     | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                                                                                                                                                                                                                                                                                                            |



## 関連トピック

[LDAP のイネーブル化/ディセーブル化](#) (89 ページ)

# LDAP SSH 公開キー認証の設定

AAA 認証は、LDAP サーバーのユーザーエントリに保存されているユーザーの公開キーを使用して、LDAP サーバーを介して実行されます。

LDAP SSH 公開キー認証を設定する前に、次の点を考慮したことを確認してください。

- ユーザーの公開キーをユーザー属性として LDAP サーバーに保存します。
- SSH クライアントからの秘密キーを使用してサインインします。



(注) SSH サインイン時に提示した秘密キーは、LDAP サーバーに保存されている公開キーを使用して検証されます。

次の例は、サンプルの LDAP クライアントの設定を示しています。

次の例では、ユーザーの公開キーが、**user-publickey-match** 構成で指定された属性（以下の場合には **sshPublicKeys** 属性）で LDAP サーバーに保存されます。

```
ldap-server host fully qualified domain name.com rootDN
"CN=ucsadmin1,CN=Users,DC=PI-Sec-DT,DC=com" password 7 password1
ldap search-map Map1
  userprofile attribute-name "description" search-filter "(cn=$userid)" base-DN
  "DC=PI-Sec-DT,DC=com"
  user-publickey-match attribute-name "sshPublicKeys" search-filter "(cn=$userid)" base-DN
  "DC=PI-Sec-DT,DC=com"
aaa group server ldap ldap1
  server fully qualified domain name.com
  use-vrf management
  ldap-search-map Map1

aaa authorization ssh-publickey default group ldap1
```

次に、ユーザの SSH クライアント秘密キーを使用して、スイッチ管理 IP アドレスにサインインする例を示します。

```
ssh ldapuser@10.0.0.1 -i ldap_pub_key_test
```

# LDAP SSH 証明書許可の設定

AAA 許可は、LDAP サーバーのユーザー属性に保存されている証明書と証明書の DN を使用して、LDAP サーバーを介して実行されます。

LDAP SSH 証明書の許可中に、次のことが処理されます。

- スイッチにインストールされている CA 証明書を使用して、SSH クライアントを介して提示されたユーザー証明書の検証。

- **enable cert-dn-match** 設定はデフォルトで有効になっているため、証明書を検証するための、LDAP サーバーに保存されている DN との **cert-DN-match** は、自動的に処理されます。

次の例は、サンプルの LDAP クライアントの設定を示しています。

- 次の例は、**user-certdn-match** 構成で指定された特定の属性の下で LDAP サーバーに証明書 DN を保存する方法を示しています。

形式は「x509v3-sign-rsa DN /DC=com, DC=PI-Sec-DT, CN=Users, CN=username1」です。

```
ldap-server host fully qualified domain name.com rootDN
"CN=uksadmin1,CN=Users,DC=PI-Sec-DT,DC=com" password 7 password1
ldap search-map Map24
  userprofile attribute-name "description" search-filter "(cn=$userid)" base-DN
"DC=PI-Sec-DT,DC=com"
  user-certdn-match attribute-name <attribute> search-filter "(cn=$userid)" base-DN
"DC=PI-Sec-DT,DC=com"
aaa group server ldap ldap24
  server fully qualified domain name.com
  enable Cert-DN-match
  use-vrf management
  ldap-search-map Map24
```

```
aaa authorization ssh-certificate default group ldap24
```

- 次の **show** コマンドは、ボックスにインストールされている **rootCA** 証明書の詳細を表示します。

```
switch# show crypto ca certificates
Trustpoint: ldap
CA certificate 0:
subject=C = IN, ST = KAR, L = BGL, O = Cisco, OU = DCBG-Cert, CN = RootCA
issuer=C = IN, ST = KAR, L = BGL, O = Cisco, OU = DCBG-Cert, CN = RootCA
serial=82EE7603BF7E74A9
notBefore=May 29 07:12:30 2023 GMT
notAfter=May 26 07:12:30 2033 GMT
SHA1 Fingerprint=D5:AE:75:8E:A1:4F:79:1E:80:3E:5E:67:C5:42:44:10:13:C6:F7:1D
purposes: sslserver sslclient

n7700-DE#
```

- 次の例は、SSH クライアントからユーザー サインインを実行する方法を示しています。
  - SSH クライアントでは、入力証明書には秘密キーとユーザー証明書の両方が含まれており、結合されて「<user>.crt」という単一のファイルになっています。
  - **rootCA.crt** は **rootCA** 証明書ファイルです。
  - IP アドレスはスイッチの管理 IP アドレスです。

```
ssh username1@10.0.0.1 -i username1.crt -vvv -oCACertificateFile=rootCA.crt
```

## LDAP サーバのモニタリング

Cisco NX-OS デバイスが保持している LDAP サーバのアクティビティに関する統計情報をモニタリングできます。

## 始める前に

Cisco NX-OS デバイスに LDAP サーバを設定します。

## 手順の概要

1. **show ldap-server statistics** {hostname | ipv4-address | ipv6-address}

## 手順の詳細

## 手順

|        | コマンドまたはアクション                                                                                                                                | 目的                   |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| ステップ 1 | <b>show ldap-server statistics</b> {hostname   ipv4-address   ipv6-address}<br><br>例 :<br><br>switch# show ldap-server statistics 10.10.1.1 | LDAP サーバの統計情報を表示します。 |

## 関連トピック

[LDAP サーバ ホストの設定](#) (90 ページ)

[LDAP サーバ統計情報のクリア](#) (105 ページ)

[LDAP サーバ統計情報のクリア](#) (105 ページ)

## LDAP サーバ統計情報のクリア

Cisco NX-OS デバイスが保持している LDAP サーバのアクティビティに関する統計情報を表示します。

## 始める前に

Cisco NX-OS デバイスに LDAP サーバを設定します。

## 手順の概要

1. (任意) **show ldap-server statistics** {hostname | ipv4-address | ipv6-address}
2. **clear ldap-server statistics** {hostname | ipv4-address | ipv6-address}

## 手順の詳細

## 手順

|        | コマンドまたはアクション                                                                     | 目的                   |
|--------|----------------------------------------------------------------------------------|----------------------|
| ステップ 1 | (任意) <b>show ldap-server statistics</b> {hostname   ipv4-address   ipv6-address} | LDAP サーバの統計情報を表示します。 |

|        | コマンドまたはアクション                                                                                                                              | 目的                   |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
|        | 例 :<br>switch# show ldap-server statistics 10.10.1.1                                                                                      |                      |
| ステップ 2 | <b>clear ldap-server statistics {hostname   ipv4-address   ipv6-address}</b><br><br>例 :<br>switch# clear ldap-server statistics 10.10.1.1 | LDAP サーバ統計情報をクリアします。 |

#### 関連トピック

[LDAP サーバのモニタリング](#) (104 ページ)

[LDAP サーバ ホストの設定](#) (90 ページ)

[LDAP サーバのモニタリング](#) (104 ページ)

## LDAP 設定の確認

LDAP 設定情報を表示するには、次の作業のいずれかを行います。

| コマンド                                                                        | 目的                                 |
|-----------------------------------------------------------------------------|------------------------------------|
| <b>show running-config ldap [all]</b>                                       | 実行コンフィギュレーションの LDAP 設定を表示します。      |
| <b>show startup-config ldap</b>                                             | スタートアップコンフィギュレーションの LDAP 設定を表示します。 |
| <b>show ldap-server</b>                                                     | LDAP 設定情報を表示します。                   |
| <b>show ldap-server groups</b>                                              | LDAP サーバ グループの設定情報を表示します。          |
| <b>show ldap-server statistics {hostname   ipv4-address   ipv6-address}</b> | LDAP 統計情報を表示します。                   |
| <b>show ldap-search-map</b>                                                 | 設定されている LDAP 属性マップに関する情報を表示します。    |

## LDAP の設定例

次に、LDAP サーバ ホストおよびサーバ グループを設定する例を示します。

```
feature ldap
ldap-server host 10.10.2.2 enable-ssl
aaa group server ldap LdapServer
server 10.10.2.2
exit
show ldap-server
```

```
show ldap-server groups
```

次に、LDAP 検索マップを設定する例を示します。

```
ldap search-map s0
userprofile attribute-name att-name search-filter "
(&(objectClass=Person)(sAMAccountName=$userid))" base-DN dc=acme,dc=com
exit
show ldap-search-map
```

次に、LDAP サーバに対する証明書認証を使用して AAA 許可を設定する例を示します。

```
aaa authorization ssh-certificate default group LDAPServer1 LDAPServer2
exit
show aaa authorization
```

次の例は、認証を検証する方法を示しています。

```
failing
test aaa group LdapServer user <user-password>
user has failed authentication

! working
test aaa group LdapServer user <user-password>
user has been authenticated
```

## 次の作業

これで、サーバグループも含めて AAA 認証方式を設定できるようになります。





## 第 7 章

# SSH および Telnet の設定

この章は、次の項で構成されています。

- [SSH および Telnet の概要 \(109 ページ\)](#)
- [SSH の注意事項および制約事項 \(111 ページ\)](#)
- [SSH の設定 \(111 ページ\)](#)
- [SSH の設定例, on page 119](#)
- [X.509v3 証明書ベースの SSH 認証の設定 \(121 ページ\)](#)
- [X.509v3 証明書ベースの SSH 認証の設定例 \(123 ページ\)](#)
- [Telnet の設定 \(124 ページ\)](#)
- [SSH および Telnet の設定の確認 \(127 ページ\)](#)
- [SSH のデフォルト設定, on page 127](#)

## SSH および Telnet の概要

### SSH サーバー

セキュア シェル (SSH) プロトコル サーバー機能を使用すると、SSH クライアントは Cisco Nexus デバイスとの間で、セキュアな暗号化された接続を確立できます。SSH は強化暗号化を使用して認証を行います。Cisco Nexus デバイス スイッチの SSH サーバーは、無償あるいは商用の SSH クライアントと連係して動作します。

SSH がサポートするユーザー認証メカニズムには、RADIUS、TACACS+、およびローカルに格納されたユーザー名とパスワードを使用した認証があります。

### SSH クライアント

SSH クライアント機能は、SSH プロトコルを介して実行されるアプリケーションで、認証と暗号化を行います。SSH クライアントを使用すると、スイッチは、別の Cisco Nexus スイッチとの間、または SSH サーバーを稼働している他の任意のデバイスとの間でセキュアな暗号化された接続を確立できます。この接続は、暗号化されたアウトバウンド接続を実現します。認証

と暗号化により、SSH クライアントは、セキュリティ保護されていないネットワーク上でもセキュアな通信を実現できます。

Cisco Nexus デバイスの SSH クライアントは、公開されているあるいは商用の SSH サーバーと連係して動作します。

## SSH サーバキー

SSH では、Cisco Nexus デバイスと安全な通信を行うためにサーバキーが必要です。SSH キーは、次の SSH オプションに使用できます。

- Rivest, Shamir, and Adelman (RSA) 公開キー暗号化を使用した SSH バージョン 2
- Digital System Algorithm (DSA) を使用した SSH バージョン 2

SSH サービスをイネーブルにする前に、適切なバージョンの SSH サーバキーペアを取得してください。使用中の SSH クライアントバージョンに応じて、SSH サーバキーペアを生成します。SSH サービスでは、SSH バージョン 2 に対応する 2 とおりのキーペアを使用できます。

- dsa オプションを使用すると、SSH バージョン 2 プロトコルに対応する DSA キーペアが生成されます。
- rsa オプションを使用すると、SSH バージョン 2 プロトコルに対応する RSA キーペアが生成されます。

デフォルトでは、Cisco Nexus デバイスは 1024 ビットの RSA キーを生成します。

SSH は、次の公開キー形式をサポートします。

- OpenSSH
- IETF SSH (SECSH)



**Caution** SSH キーをすべて削除すると、SSH サービスを開始できません。

## デジタル証明書を使用した SSH 認証

Cisco NX-OS デバイスでの SSH 認証では、ホスト認証用に X.509 デジタル証明書をサポートしています。X.509 デジタル証明書は、メッセージの出所と整合性を保証するデータ項目です。これには安全な通信のための暗号化されたキーが含まれています。また、発信者のアイデンティティを証明するために信頼できる認証局 (CA) によって署名されています。X.509 デジタル証明書のサポートにより、認証に DSA と RSA のいずれかのアルゴリズムを使用します。

証明書のインフラストラクチャでは、Secure Socket Layer (SSL) に対応し、セキュリティインフラストラクチャによってクエリーまたは通知を通じて最初に返される証明書が使用されます。証明書が信頼できる CA のいずれかから発行されたものであれば、証明書の検証は成功です。



X.509 証明書を使用する SSH 認証用にデバイスを設定できます。認証に失敗した場合は、パスワードの入力が求められます。

X.509v3 証明書 (RFC 6187) を使用する SSH 認証を設定できます。X.509v3 証明書ベースの SSH 認証では、スマートカードと組み合わせた証明書を使用して、シスコ デバイスへのアクセスの 2 要素認証を有効にします。SSH クライアントは、シスコパートナーの Pragma Systems によって提供されます。

## Telnet サーバ

Telnet プロトコルは、ホストとの TCP/IP 接続を確立します。Telnet を使用すると、あるサイトのユーザーが別サイトのログイン サーバーとの TCP 接続を確立して、システム間でキーストロークをやり取りできます。Telnet は、リモートシステムのアドレスとして、IP アドレスまたはドメイン名を受け取ります。

デフォルトでは、Telnet サーバは Cisco Nexus デバイス上で無効になっています。

## SSH の注意事項および制約事項

SSH には、次の注意事項および制限事項があります。

- Cisco Nexus デバイスは、SSH バージョン 2 (SSHv2) だけをサポートしています。
- SSH パスワードレス ファイルコピーを目的として AAA プロトコル (RADIUS や TACACS+ など) を介してリモート認証されたユーザ アカウントにインポートされた SSH 公開キーと秘密キーは、同じ名前のローカル ユーザ アカウントでない限り、Nexus デバイスがリロードされると保持されません。リモート ユーザ アカウントは、SSH キーがインポートされる前にデバイスで設定されます。

## SSH の設定

### SSH サーバ キーの生成

セキュリティ要件に基づいて SSH サーバ キーを生成できます。デフォルトの SSH サーバ キーは、1024 ビットで生成される RSA キーです。

#### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **ssh key {dsa [force] | rsa [bits [force]]}**
3. switch(config)# **exit**
4. (Optional) switch# **show ssh key [dsa | rsa] [md5]**
5. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

## Procedure

|        | Command or Action                                                 | Purpose                                                                                                                                                                                                                           |
|--------|-------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                                 | グローバル構成モードを開始します。                                                                                                                                                                                                                 |
| ステップ 2 | switch(config)# <b>ssh key {dsa [force]   rsa [bits [force]]}</b> | SSH サーバー キーを生成します。<br><br><i>bits</i> 引数には、キーの生成に使用するビット数を指定します。有効な範囲は 768 ～ 4096 です。デフォルト値は 1024 です。<br><br>既存のキーを置き換える場合は、キーワード <b>force</b> を使用します。                                                                            |
| ステップ 3 | switch(config)# <b>exit</b>                                       | グローバル コンフィギュレーション モードを終了します。                                                                                                                                                                                                      |
| ステップ 4 | (Optional) switch# <b>show ssh key [dsa   rsa] [md5]</b>          | SSH サーバー キーを表示します。<br><br>Cisco NX-OS リリース 7.0(3)I4(6) および 7.0(3)I4(x) 以降のリリースでは、このコマンドはデフォルトで SHA256 形式でフィンガープリントを表示します。SHA256 は、以前のデフォルトの MD5 形式よりも安全です。ただし、フィンガープリントを MD5 形式で表示する必要がある場合の下位互換性のために、 <b>md5</b> オプションが追加されています。 |
| ステップ 5 | (Optional) switch# <b>copy running-config startup-config</b>      | 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。                                                                                                                                                                                        |

## Example

次に、SSH サーバー キーを生成する例を示します。

```
switch# configure terminal
switch(config)# ssh key rsa 2048
switch(config)# exit
switch# show ssh key
switch# copy running-config startup-config
```

## ユーザ アカウント用 SSH 公開キーの指定

SSH 公開キーを設定すると、パスワードを要求されることなく、SSH クライアントを使用してログインできます。SSH 公開キーは、次の 3 種類のいずれかの形式で指定できます。

- Open SSH 形式

- Internet Engineering Task Force (IETF) SECSH 形式
- Privacy Enhanced Mail (PEM) 形式の公開キー証明書

## Open SSH 形式による SSH 公開キーの指定

ユーザー アカウント用に SSH 形式で SSH 公開キーを指定できます。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **username username sshkey ssh-key**
3. switch(config)# **exit**
4. (Optional) switch# **show user-account**
5. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

#### Procedure

|        | Command or Action                                            | Purpose                                   |
|--------|--------------------------------------------------------------|-------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                            | グローバル構成モードを開始します。                         |
| ステップ 2 | switch(config)# <b>username username sshkey ssh-key</b>      | SSH 形式で SSH 公開キーを設定します。                   |
| ステップ 3 | switch(config)# <b>exit</b>                                  | グローバル コンフィギュレーション モードを終了します。              |
| ステップ 4 | (Optional) switch# <b>show user-account</b>                  | ユーザー アカウントの設定を表示します。                      |
| ステップ 5 | (Optional) switch# <b>copy running-config startup-config</b> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。 |

#### Example

次に、Open SSH 形式で SSH 公開キーを指定する例を示します。

```
switch# configure terminal
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAri3mQy4W1AV9Y2t2hrEWgbUEYz
CfTPO5B8LRkedn56BEy2N9ZcdpqE6aqJLZwFZcTFEzaAAZp9AS86dgBAjsKGs7UxmhGySr8ZELv+DQBsDQH6rZt0KR+2Da8hJD4Z
XIeccWk0gS1DQUNZ300xstQsYZUtqnx1bvm5Ninn0McNinn0Mc=
switch(config)# exit
switch# show user-account
switch# copy running-config startup-config
```



**Note** 上記の例の **username** コマンドは、読みやすくするために改行されていますが、単一行です。

## IETF SECSH 形式による SSH 公開キーの指定

ユーザー アカウント用に IETF SECSH 形式で SSH 公開キーを指定できます。

### SUMMARY STEPS

1. switch# **copy server-file bootflash: filename**
2. switch# **configure terminal**
3. switch(config)# **username username sshkey file filename**
4. switch(config)# **exit**
5. (Optional) switch# **show user-account**
6. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

#### Procedure

|        | Command or Action                                             | Purpose                                                                                                                                                                 |
|--------|---------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | switch# <b>copy server-file bootflash: filename</b>           | サーバーから IETF SECSH 形式の SSH キーを含むファイルをダウンロードします。File Transfer Protocol (FTP)、SCP、SSH File Transfer Protocol (SFTP)、または Trivial File Transfer Protocol (TFTP) サーバーを利用できます。 |
| ステップ 2 | switch# <b>configure terminal</b>                             | グローバル構成モードを開始します。                                                                                                                                                       |
| ステップ 3 | switch(config)# <b>username username sshkey file filename</b> | SSH 形式で SSH 公開キーを設定します。                                                                                                                                                 |
| ステップ 4 | switch(config)# <b>exit</b>                                   | グローバル コンフィギュレーション モードを終了します。                                                                                                                                            |
| ステップ 5 | (Optional) switch# <b>show user-account</b>                   | ユーザー アカウントの設定を表示します。                                                                                                                                                    |
| ステップ 6 | (Optional) switch# <b>copy running-config startup-config</b>  | 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。                                                                                                                              |

#### Example

次に、IETF SECSH 形式で SSH 公開キーを指定する例を示します。

```
switch#copy tftp://10.10.1.1/secsh_file.pub bootflash:secsh_file.pub
switch# configure terminal
switch(config)# username User1 sshkey file bootflash:secsh_file.pub
switch(config)# exit
switch# show user-account
switch# copy running-config startup-config
```

## PEM フォーマット化された公開キー証明書形式による SSH 公開キーの指定

ユーザー アカウント用に PEM フォーマット化された公開キー証明書形式で SSH 公開キーを指定できます。

### SUMMARY STEPS

1. switch# **copy server-file bootflash: filename**
2. switch# **configure terminal**
3. (Optional) switch# **show user-account**
4. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

#### Procedure

|        | Command or Action                                            | Purpose                                                                                    |
|--------|--------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| ステップ 1 | switch# <b>copy server-file bootflash: filename</b>          | サーバーから PEM フォーマット化された公開キー証明書形式の SSH キーを含むファイルをダウンロードします。FTP、SCP、SFTP、または TFTP サーバーを利用できます。 |
| ステップ 2 | switch# <b>configure terminal</b>                            | グローバル構成モードを開始します。                                                                          |
| ステップ 3 | (Optional) switch# <b>show user-account</b>                  | ユーザー アカウントの設定を表示します。                                                                       |
| ステップ 4 | (Optional) switch# <b>copy running-config startup-config</b> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                  |

#### Example

次に、PEM フォーマット化された公開キー証明書形式で SSH 公開キーを指定する例を示します。

```
switch# copy tftp://10.10.1.1/cert.pem bootflash:cert.pem
switch# configure terminal
switch# show user-account
switch# copy running-config startup-config
```

## SSH 送信元インターフェイスの構成

SSH は、特定のインターフェイスを使用するように構成できます。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **ip ssh source-interface type slot/port**
3. switch(config)# **show ip ssh source-interface**

### 手順の詳細

#### 手順

|        | コマンドまたはアクション                                                  | 目的                                                                                                                                                                                                              |
|--------|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                             | グローバル構成モードを開始します。                                                                                                                                                                                               |
| ステップ 2 | switch(config)# <b>ip ssh source-interface type slot/port</b> | すべての SSH パケットの送信元インターフェイスを構成します。次のリストに、 <i>interface</i> として有効な値を示します。 <ul style="list-style-type: none"> <li>• ethernet</li> <li>• loopback</li> <li>• mgmt</li> <li>• port-channel</li> <li>• vlan</li> </ul> |
| ステップ 3 | switch(config)# <b>show ip ssh source-interface</b>           | 構成済みの SSH 送信元インターフェイスを表示します。                                                                                                                                                                                    |

#### 例

次に、SSH 送信元インターフェイスを構成する例を示します。

```
switch(config)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip ssh source-interface ethernet 1/7
switch(config)# show ip ssh source-interface
VRF Name                               Interface
default                                Ethernet1/7
```

## リモート デバイスとの SSH セッションの開始

Cisco Nexus デバイスからリモート デバイスに接続する SSH セッションを開始できます。

## SUMMARY STEPS

1. switch# **ssh** {hostname | username@hostname} [ **vrf** vrf-name]

## DETAILED STEPS

## Procedure

|        | Command or Action                                                        | Purpose                                                                    |
|--------|--------------------------------------------------------------------------|----------------------------------------------------------------------------|
| ステップ 1 | switch# <b>ssh</b> {hostname   username@hostname} [ <b>vrf</b> vrf-name] | リモート デバイスとの SSH セッションを作成します。引数 <i>hostname</i> には、IPv4 アドレス、またはホスト名を指定します。 |

## SSH ホストのクリア

SCP または SFTP を使用してサーバーからファイルをダウンロードする場合は、サーバーと信頼性のある SSH 関係を確立します。

## SUMMARY STEPS

1. switch# **clear ssh hosts**

## DETAILED STEPS

## Procedure

|        | Command or Action              | Purpose               |
|--------|--------------------------------|-----------------------|
| ステップ 1 | switch# <b>clear ssh hosts</b> | SSH ホスト セッションをクリアします。 |

## SSH サーバのディセーブル化

Cisco Nexus デバイスでは、デフォルトで SSH サーバーが有効になっています。

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# [no] **feature ssh**
3. switch(config)# **exit**
4. (Optional) switch# **show ssh server**
5. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

## Procedure

|        | Command or Action                                            | Purpose                                     |
|--------|--------------------------------------------------------------|---------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                            | グローバル構成モードを開始します。                           |
| ステップ 2 | switch(config)# <b>[no] feature ssh</b>                      | SSH サーバーをイネーブル/ディセーブルにします。デフォルトでは有効になっています。 |
| ステップ 3 | switch(config)# <b>exit</b>                                  | グローバル コンフィギュレーション モードを終了します。                |
| ステップ 4 | (Optional) switch# <b>show ssh server</b>                    | SSH サーバーの設定を表示します。                          |
| ステップ 5 | (Optional) switch# <b>copy running-config startup-config</b> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。   |

## SSH サーバ キーの削除

SSH サーバーをディセーブルにした後、SSH サーバ キーを削除できます。



## Note

SSH を再度イネーブルにするには、まず、SSH サーバ キーを生成する必要があります。

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **no feature ssh**
3. switch(config)# **no ssh key [dsa | rsa]**
4. switch(config)# **exit**
5. (Optional) switch# **show ssh key**
6. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

## Procedure

|        | Command or Action                             | Purpose              |
|--------|-----------------------------------------------|----------------------|
| ステップ 1 | switch# <b>configure terminal</b>             | グローバル構成モードを開始します。    |
| ステップ 2 | switch(config)# <b>no feature ssh</b>         | SSH サーバーをディセーブルにします。 |
| ステップ 3 | switch(config)# <b>no ssh key [dsa   rsa]</b> | SSH サーバ キーを削除します。    |



|        | Command or Action                                            | Purpose                                   |
|--------|--------------------------------------------------------------|-------------------------------------------|
|        |                                                              | デフォルトでは、すべての SSH キーが削除されます。               |
| ステップ 4 | switch(config)# <b>exit</b>                                  | グローバル コンフィギュレーション モードを終了します。              |
| ステップ 5 | (Optional) switch# <b>show ssh key</b>                       | SSH サーバーの設定を表示します。                        |
| ステップ 6 | (Optional) switch# <b>copy running-config startup-config</b> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。 |

## SSH セッションのクリア

SSH セッションは Cisco Nexus デバイスからクリアできます。

### SUMMARY STEPS

1. switch# **show users**
2. switch# **clear line vty-line**

### DETAILED STEPS

#### Procedure

|        | Command or Action                  | Purpose               |
|--------|------------------------------------|-----------------------|
| ステップ 1 | switch# <b>show users</b>          | ユーザー セッション情報を表示します。   |
| ステップ 2 | switch# <b>clear line vty-line</b> | ユーザ SSH セッションをクリアします。 |

## SSH の設定例

次に、SSH を設定する例を示します。

### SUMMARY STEPS

1. SSH サーバ キーを生成します。
2. SSH サーバをイネーブルにします。
3. SSH サーバ キーを表示します。
4. Open SSH 形式による SSH 公開キーを指定します。
5. 設定を保存します。

## DETAILED STEPS

### Procedure

**ステップ 1** SSH サーバ キーを生成します。

```
switch(config)# ssh key rsa
generating rsa key(1024 bits).....
.
generated rsa key
```

**ステップ 2** SSH サーバをイネーブルにします。

```
switch# configure terminal
switch(config)# feature ssh
```

#### Note

SSH サーバーはデフォルトでイネーブルになっているため、この手順は必要ありません。

**ステップ 3** SSH サーバー キーを表示します。

```
switch(config)# show ssh key

rsa Keys generated:Fri May  8 22:09:47 2009

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAri3mQy4W1AV9Y2t2hrEWgbUEYzCfTPO5B8LRkedn56BEy2N9ZcdpqE6aqJLZwfZ/
cTFEzaAAZp9AS86dgBAjsKGs7UxnhGySr8ZELv+DQBsDQH6rZt0KR+2Da8hJD4ZXIeccWk0gS1DQUNZ300xstQsYZUtqnx1bvm5/
Ninn0Mc=

bitcount:1024
fingerprint:
4b:4d:f6:b9:42:e9:d9:71:3c:bd:09:94:4a:93:ac:ca
*****
could not retrieve dsa key information
*****
```

**ステップ 4** Open SSH 形式による SSH 公開キーを指定します。

```
switch(config)# username User1 sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAri3mQy4W1AV9Y2t2hrEWgbUEYz
CfTPO5B8LRkedn56BEy2N9ZcdpqE6aqJLZwfZcTFEzaAAZp9AS86dgBAjsKGs7UxnhGySr8ZELv+DQBsDQH6rZt0KR+2Da8hJD4Z
XIeccWk0gS1DQUNZ300xstQsYZUtqnx1bvm5Ninn0McNinn0Mc=
```

**ステップ 5** 設定を保存します。

```
switch(config)# copy running-config startup-config
```

## X.509v3 証明書ベースの SSH 認証の設定

X.509v3 証明書を使用する SSH 認証を設定できます。

始める前に

リモート デバイスの SSH サーバをイネーブルにします。

### 手順の概要

1. **configure terminal**
2. **username user-id [password [0 | 5] password]**
3. **username user-id ssh-cert-dn dn-name {dsa | rsa}**
4. **[no] crypto ca trustpoint trustpoint**
5. **[no] crypto ca authentication trustpoint**
6. **crypto ca crt request trustpoint bootflash:static-crl.crl**
7. (任意) **show crypto ca certificates**
8. (任意) **show crypto ca crt trustpoint**
9. (任意) **show user-account**
10. (任意) **show users**
11. (任意) **copy running-config startup-config**

### 手順の詳細

#### 手順

|        | コマンドまたはアクション                                                                                                        | 目的                                                                                                                                                                                                                                                 |
|--------|---------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例 :<br>switch# configure terminal<br>switch(config)#                               | グローバル コンフィギュレーション モードを開始します                                                                                                                                                                                                                        |
| ステップ 2 | <b>username user-id [password [0   5] password]</b><br><br>例 :<br>switch(config)# username jsmith password 4Ty18Rnt | ユーザ アカウントを設定します。 <i>user-id</i> 引数は、最大 28 文字の英数字で、大文字と小文字が区別されます。指定できる文字は、A ～ Z の英大文字、a ～ z の英小文字、0 ～ 9 の数字、ハイフン (-)、ピリオド (.)、アンダースコア (_)、プラス符号 (+)、および等号 (=) です。アットマーク (@) はリモート ユーザ名では使用できますが、ローカル ユーザ名では使用できません。<br><br>ユーザ名の先頭は英数字で始まる必要があります。 |

|        | コマンドまたはアクション                                                                                                                                                                                                                                            | 目的                                                                                                                                                                                                                                                                        |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        |                                                                                                                                                                                                                                                         | <p>デフォルト パスワードは定義されていません。オプションの <b>0</b> は、パスワードがクリア テキストであり、<b>5</b> はパスワードが暗号化されていることを意味します。デフォルトは <b>0</b> (クリア テキスト) です。</p> <p>(注)<br/>パスワードを指定しなかった場合、ユーザーは Cisco NX-OS デバイスにログインできません。</p> <p>(注)<br/>暗号化パスワードオプションを使用してユーザアカウントを作成する場合、対応する SNMP ユーザは作成されません。</p> |
| ステップ 3 | <b>username user-id ssh-cert-dn dn-name {dsa   rsa}</b><br><br>例 :<br><pre>switch(config)# username jsmith ssh-cert-dn "/O = ABCcompany, OU = ABC1, emailAddress = jsmith@ABCcompany.com, L = Metropolis, ST = New York, C = US, CN = jsmith" rsa</pre> | <p>既存のユーザアカウント認証に使用する SSH X.509 証明書の識別名と DSA アルゴリズムを指定します。識別名は最大 512 文字で、例に示す形式に従う必要があります。電子メールアドレスと状態がそれぞれ <b>emailAddress</b> と <b>ST</b> に設定されていることを確認します。</p>                                                                                                         |
| ステップ 4 | <b>[no] crypto ca trustpoint trustpoint</b><br><br>例 :<br><pre>switch(config)# crypto ca trustpoint winca</pre>                                                                                                                                         | <p>トラストポイントを設定します。</p>                                                                                                                                                                                                                                                    |
| ステップ 5 | <b>[no] crypto ca authentication trustpoint</b><br><br>例 :<br><pre>switch(config)# crypto ca authentication winca</pre>                                                                                                                                 | <p>トラストポイントの証明書チェーンを構成します。</p>                                                                                                                                                                                                                                            |
| ステップ 6 | <b>crypto ca crl request trustpoint bootflash:static-crl.crl</b><br><br>例 :<br><pre>switch(config)# crypto ca crl request winca bootflash:crllist.crl</pre>                                                                                             | <p>トラストポイントの証明書失効リスト (CRL) を設定します。CRL ファイルは、トラストポイントによって失効した証明書のリストのスナップショットです。このスタティック CRL リストは、認証局 (CA) からデバイスに手動でコピーされます。</p> <p>(注)<br/>スタティック CRL は、サポートされている唯一の失効チェック方式です。</p>                                                                                      |
| ステップ 7 | (任意) <b>show crypto ca certificates</b><br><br>例 :<br><pre>switch(config)# show crypto ca certificates</pre>                                                                                                                                            | <p>設定されている証明書またはチェーンと、関連付けられているトラストポイントを表示します。</p>                                                                                                                                                                                                                        |

|         | コマンドまたはアクション                                                                                                    | 目的                                        |
|---------|-----------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| ステップ 8  | (任意) <b>show crypto ca crt trustpoint</b><br><br>例 :<br>switch(config)# show crypto ca crt winca                | 指定したトラストポイントの CRL リストの内容を表示します。           |
| ステップ 9  | (任意) <b>show user-account</b><br><br>例 :<br>switch(config)# show user-account                                   | 設定されたユーザアカウントの詳細を表示します。                   |
| ステップ 10 | (任意) <b>show users</b><br><br>例 :<br>switch(config)# show users                                                 | デバイスにログオンしているユーザが表示されます。                  |
| ステップ 11 | (任意) <b>copy running-config startup-config</b><br><br>例 :<br>switch(config)# copy running-config startup-config | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。 |

## X.509v3 証明書ベースの SSH 認証の設定例

次の例は、X.509v3 証明書を使用する SSH 認証の設定方法を示しています。

```
configure terminal
username jsmith password 4Ty18Rnt
username jsmith ssh-cert-dn "/O = ABCcompany, OU = ABC1,
emailAddress = jsmith@ABCcompany.com, L = Metropolis, ST = New York, C = US, CN = jsmith"
  rsa
crypto ca trustpoint tp1
crypto ca authentication tp1
crypto ca crt request tp1 bootflash:crl1.crl

show crypto ca certificates
Trustpoint: tp1
CA certificate 0:
subject= /CN=SecDevCA
issuer= /CN=SecDevCA
serial=01AB02CD03EF04GH05IJ06KL07MN
notBefore=Jun 29 12:36:26 2016 GMT
notAfter=Jun 29 12:46:23 2021 GMT
SHA1 Fingerprint=47:29:E3:00:C1:C1:47:F2:56:8B:AC:B2:1C:64:48:FC:F4:8D:53:AF
purposes: sslserver sslclient

show crypto ca crt tp1
Trustpoint: tp1 CRL: Certificate Revocation List (CRL):
  Version 2 (0x1)
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: /CN=SecDevCA
  Last Update: Aug 8 20:03:15 2016 GMT
  Next Update: Aug 16 08:23:15 2016 GMT
  CRL extensions:
    X509v3 Authority Key Identifier:
      keyid:30:43:AA:80:10:FE:72:00:DE:2F:A2:17:E4:61:61:44:CE:78:FF:2A
```

```

show user-account
user:user1
    this user account has no expiry date
    roles:network-operator
    ssh cert DN : /C = US, ST = New York, L = Metropolis, O = cisco , OU = csg, CN
= user1; Algo: x509v3-sign-rsa

show users
NAME      LINE      TIME      IDLE      PID      COMMENT
user1     pts/1     Jul 27 18:43 00:03     18796    (10.10.10.1)  session=ssh

```

## Telnet の設定

### Telnet サーバのイネーブル化

デフォルトでは、Telnet サーバーはイネーブルに設定されています。Cisco Nexus デバイスの Telnet サーバーを無効にできます。

#### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **[no] feature telnet**

#### DETAILED STEPS

##### Procedure

|        | Command or Action                          | Purpose                                           |
|--------|--------------------------------------------|---------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>          | グローバル構成モードを開始します。                                 |
| ステップ 2 | switch(config)# <b>[no] feature telnet</b> | Telnet サーバーをイネーブル/ディセーブルにします。デフォルトではイネーブルになっています。 |

### Telnet サーバーの再イネーブル化

Cisco Nexus デバイスの Telnet サーバーが無効にされていた場合は、再度有効にすることができます。

#### SUMMARY STEPS

1. switch(config)# **[no] feature telnet**

## DETAILED STEPS

## Procedure

|        | Command or Action                          | Purpose                  |
|--------|--------------------------------------------|--------------------------|
| ステップ 1 | switch(config)# <b>[no] feature telnet</b> | Telnet サーバーを再度イネーブルにします。 |

## Telnet 送信元インターフェースの構成

Telnet は、特定のインターフェースを使用するように構成できます。

## 手順の概要

1. switch# **configure terminal**
2. switch(config)# **ip telnet source-interface type slot/port**

## 手順の詳細

## 手順

|        | コマンドまたはアクション                                                     | 目的                                                                                                                                                                                                                 |
|--------|------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                                | グローバル構成モードを開始します。                                                                                                                                                                                                  |
| ステップ 2 | switch(config)# <b>ip telnet source-interface type slot/port</b> | すべての Telnet パケットの送信元インターフェースを設定します。次のリストに、 <i>interface</i> として有効な値を示します。 <ul style="list-style-type: none"> <li>• ethernet</li> <li>• loopback</li> <li>• mgmt</li> <li>• port-channel</li> <li>• vlan</li> </ul> |

## 例

次に、Telnet 送信元インターフェースを構成する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip telnet source-interface ethernet 1/6
switch(config)# show ip telnet source-interface
VRF Name                               Interface
default                               Ethernet1/6
switch(config)#
```

## リモート デバイスとの Telnet セッションの開始

Telnet セッションを開始してリモート デバイスに接続する前に、次の作業を行う必要があります。

- リモート デバイスのホスト名を取得します。必要に応じて、リモート デバイスのユーザー名も取得します。
- Cisco Nexus デバイス上で Telnet サーバを有効にします。
- リモート デバイス上で Telnet サーバーをイネーブルにします。

### SUMMARY STEPS

1. switch# **telnet** *hostname*

### DETAILED STEPS

#### Procedure

|        | Command or Action                     | Purpose                                                                       |
|--------|---------------------------------------|-------------------------------------------------------------------------------|
| ステップ 1 | switch# <b>telnet</b> <i>hostname</i> | リモート デバイスとの Telnet セッションを作成します。引数 <i>hostname</i> には、IPv4 アドレス、またはホスト名を指定します。 |

#### Example

次に、Telnet セッションを開始してリモート デバイスに接続する例を示します。

```
switch# telnet 10.10.1.1
Trying 10.10.1.1...
Connected to 10.10.1.1.
Escape character is '^]'.
switch login:
```

## Telnet セッションのクリア

Telnet セッションは Cisco Nexus デバイスからクリアできます。

### SUMMARY STEPS

1. switch# **show users**
2. switch# **clear line** *vty-line*



## DETAILED STEPS

## Procedure

|        | Command or Action                  | Purpose                  |
|--------|------------------------------------|--------------------------|
| ステップ 1 | switch# <b>show users</b>          | ユーザー セッション情報を表示します。      |
| ステップ 2 | switch# <b>clear line vty-line</b> | ユーザ Telnet セッションをクリアします。 |

## SSH および Telnet の設定の確認

SSH の設定情報を表示するには、次のいずれかの作業を行います。

| コマンドまたはアクション                                      | 目的                                                                                      |
|---------------------------------------------------|-----------------------------------------------------------------------------------------|
| switch# <b>show ssh key [dsa   rsa][md5]</b>      | SSH サーバー キーを表示します。                                                                      |
| switch# <b>show running-config security [all]</b> | 実行コンフィギュレーション内の SSH とユーザ アカウントの設定を表示します。all キーワードを指定すると、SSH およびユーザ アカウントのデフォルト値が表示されます。 |
| switch# <b>show ssh server</b>                    | SSH サーバーの設定を表示します。                                                                      |
| switch# <b>show user-account</b>                  | ユーザ アカウント情報を表示します。                                                                      |
| switch# <b>show users</b>                         | デバイスにログオンしているユーザが表示されます。                                                                |
| switch# <b>show crypto ca certificates</b>        | X.509v3証明書ベースのSSH認証に設定された証明書チェーンおよび関連するトラストポイントを表示します。                                  |
| switch# <b>show crypto ca crl trustpoint</b>      | 指定したトラストポイントのCRLリストの内容を表示します。                                                           |

## SSH のデフォルト設定

次の表に、SSH パラメータのデフォルト設定を示します。

Table 9: デフォルトの SSH パラメータ

| パラメータ   | デフォルト |
|---------|-------|
| SSH サーバ | イネーブル |

| パラメータ        | デフォルト                 |
|--------------|-----------------------|
| SSH サーバ キー   | 1024 ビットで生成された RSA キー |
| RSA キー生成ビット数 | 1024                  |
| Telnet サーバ   | 有効 (Enabled)          |



## 第 8 章

# PKI の設定

この章では、Cisco NX-OS での公開キー インフラストラクチャ（PKI）のサポートについて説明します。PKI を使用すると、ネットワーク上で通信を安全に行うためのデジタル証明書をデバイスが入手して使用できるようになり、セキュアシェル（SSH）の管理性と拡張性も向上します。

この章は、次の項で構成されています。

- [PKI の概要, on page 129](#)
- [PKI の注意事項と制約事項（137 ページ）](#)
- [PKI のデフォルト設定, on page 137](#)
- [CA の設定とデジタル証明書, on page 138](#)
- [PKI の設定の確認, on page 159](#)
- [PKI の設定例, on page 160](#)
- [Resource Public Key Infrastructure（RPKI）（196 ページ）](#)
- [RPKI 構成（196 ページ）](#)
- [RPKI Show コマンド（198 ページ）](#)
- [RPKI Clear コマンド（199 ページ）](#)
- [RPKI Debug および Event History コマンド（200 ページ）](#)

## PKI の概要

ここでは、PKI について説明します。

## CA とデジタル証明書

証明機関（CA）は証明書要求を管理して、ホスト、ネットワーク デバイス、ユーザなどの参加エンティティに証明書を発行します。CA は参加エンティティに対して集中型のキー管理を行います。

デジタル署名は、公開キー暗号法に基づいて、デバイスや個々のユーザをデジタル的に認証します。RSA 暗号化システムなどの公開キー暗号法では、各デバイスやユーザはキー ペアを持ち、これには秘密キーと公開キーが含まれています。秘密キーは秘密裡に保管し、これを知つ

ているのは所有するデバイスまたはユーザだけです。一方、公開キーは誰もが知っているものです。これらのキーの一方で暗号化されたものは、他方のキーで復号化できます。署名は、送信者の秘密キーを使用してデータを暗号化したときに作成されます。受信側は、送信側の公開キーを使用してメッセージを復号化することで、シグニチャを検証します。このプロセスは、受信者が送信者の公開キーのコピーを持っていて、これが本当に送信者のものであり、送信者を騙る他人のものではないことを高い確実性を持って知っていることを基盤としています。

デジタル証明書は、デジタル署名と送信者を結び付けるものです。デジタル証明書には、名前、シリアル番号、企業、部署または IP アドレスなど、ユーザまたはデバイスを特定する情報を含んでいます。また、エンティティの公開キーのコピーも含んでいます。証明書に署名する CA は、受信者が明示的に信頼する第三者機関であり、アイデンティティの正当性を立証し、デジタル証明書を作成します。

CA のシグニチャを検証するには、受信者は、CA の公開キーを認識する必要があります。一般的にはこのプロセスはアウトオブバンドか、インストール時に行われる操作によって処理されます。たとえば、通常の Web ブラウザでは、デフォルトで、複数の CA の公開キーが設定されています。

## 信頼モデル、トラストポイント、アイデンティティ CA

PKI の信頼モデルは、設定変更が可能な複数の信頼できる CA によって階層化されています。信頼できる CA のリストを使用して各参加デバイスを設定して、セキュリティプロトコルの交換の際に入手したピアの証明書がローカルに信頼できる CA のいずれかで発行されていた場合には、これを認証できるようにすることができます。Cisco NX-OS ソフトウェアでは、信頼できる CA の自己署名ルート証明書（または下位 CA の証明書チェーン）をローカルに保存しています。信頼できる CA のルート証明書（または下位 CA の場合には全体のチェーン）を安全に入手するプロセスを、CA 認証と呼びます。

信頼できる CA について設定された情報をトラストポイントと呼び、CA 自体もトラストポイント CA と呼びます。この情報は、CA 証明書（下位 CA の場合は証明書チェーン）と証明書取消確認情報で構成されています。

Cisco NX-OS デバイスは、トラストポイントに登録して、アイデンティティ証明書を入手し、キーペアと関連付けることができます。このトラストポイントをアイデンティティ CA と呼びます。

## CA証明書の階層

セキュアサービスの場合、通常は複数の信頼できる CA があります。CA は通常、すべてのホストにバンドルとしてインストールされます。NX-OS PKI インフラストラクチャは、証明書チェーンのインポートをサポートします。ただし、現在の CLI では、一度に 1 つのチェーンをインストールできます。インストールする CA チェーンが複数ある場合、この手順は面倒です。これには、複数の中間 CA とルート CA を含む CA バンドルをダウンロードする機能が必要です。

## CA バンドルのインポート

`crypto CA trustpoint` コマンドは、CA 証明書、CRL、アイデンティティ証明書、およびキーペアを名前付きラベルにバインドします。これらの各エンティティに対応するすべてのファイルは、NX-OS `certstore` ディレクトリ（`/isan/etc/certstore`）に保存され、トラストポイントラベルでタグ付けされます。

CA 証明書にアクセスするには、SSL アプリケーションは標準の NX-OS 証明書ストアをポイントし、SSL 初期化中に CA パスとして指定するだけです。CA がインストールされているトラストポイントラベルを認識する必要はありません。

クライアントがアイデンティティ証明書にバインドする必要がある場合は、トラストポイントラベルをバインディングポイントとして使用する必要があります。

`import pkcs` コマンドは、トラストポイントラベルの下に CA 証明書をインストールするように拡張されています。CA バンドルをインストールするようにさらに拡張できます。`import` コマンド構造が変更され、pkcs7 形式の CA バンドルファイルを提供するために使用される `pkcs7` オプションが追加されました。

Cisco NX-OS リリース 10.1(1) 以降、CA バンドルを解凍し、独自のラベルの下に各 CA チェーンをインストールするために、`pkcs7` ファイル形式がサポートされています。ラベルは、メイントラストポイントラベルにインデックスを追加することによって形成されます。

一度インストールすると、バンドルへのすべての CA チェーンの論理バインディングはありません。

## PKCS7 形式での CA 証明書バンドルのインポート

複数の独立した証明書チェーンで構成される CA 証明書バンドルのインポートをサポートするために、`'pkcs7'` のオプションが `crypto import` コマンドに導入されました。

### 手順の概要

1. `configure terminal`
2. `crypto ca import <baselabel> pkcs7 <uri0> force`
3. `crypto ca bundle <bundle-name>`
4. `exit`
5. （任意）`show crypto ca certificates`
6. （任意）`copy running-config startup-config`

### 手順の詳細

#### 手順

|        | コマンドまたはアクション                                  | 目的                          |
|--------|-----------------------------------------------|-----------------------------|
| ステップ 1 | <b><code>configure terminal</code></b><br>例 : | グローバル コンフィギュレーション モードを開始します |

|        | コマンドまたはアクション                                                                             | 目的                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        | switch# configure terminal<br>switch(config)#                                            |                                                                                                                                                                                                                                                                                                                                                                                                        |
| ステップ 2 | <b>crypto ca import &lt;baselabel&gt; pkcs7 &lt;uri0&gt; force</b>                       | <p>コマンドには2つの入力引数があります。Ca バンドルファイルであるソースファイルは、&lt;uri0&gt;、入力ファイルは pkcs7 形式である必要があります。これは cabundle ファイルであることを示します。</p> <p>複数の証明書チェーンが cabundle から抽出されます。このコマンドは、CA証明書チェーンが接続された複数のトラストポイントを作成します。import コマンドは、グローバル CA バンドル構成と、生成された各トラストポイントごとの CA バンドル下位構成の、2 つの構成を作成します。</p> <p>force オプションを指定すると、CA バンドルおよび関連するトラストポイント構成が削除され、同じバンドル名を持つ新しいCAバンドルがインポートされ、その CA バンドルに関連する新しいトラストポイント構成が生成されます。</p> |
| ステップ 3 | <b>crypto ca cabundle &lt;bundle-name&gt;</b>                                            | <p>bundle-name は、インポートの場合の baselabel と同じです。このコマンドの <b>no</b> 形式を使用すると、CA バンドル、トラストポイント、および関連する証明書チェーンを削除できます。</p> <p>特定のベースラベル名で CA バンドルをインポートし、すべてのトラストポイントを作成した後、ユーザーが同じベースラベル名で import コマンドを再度実行しようとする、CA バンドルがすでに存在するというエラーがスローされます。ユーザーは force オプションを使用して、既存の CA バンドルを変更できます。</p> <p>サポートされる CA バンドルの最大数は 20 です。</p>                                                                              |
| ステップ 4 | <b>exit</b><br><br>例：<br>switch(config)# exit<br>switch#                                 | 設定モードを終了します。                                                                                                                                                                                                                                                                                                                                                                                           |
| ステップ 5 | (任意) <b>show crypto ca certificates</b><br><br>例：<br>switch# show crypto ca certificates | CA 証明書を表示します。                                                                                                                                                                                                                                                                                                                                                                                          |
| ステップ 6 | (任意) <b>copy running-config startup-config</b><br><br>例：                                 | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                                                                                                                                                                                                                                                                                                                              |

|  | コマンドまたはアクション                               | 目的 |
|--|--------------------------------------------|----|
|  | switch# copy running-config startup-config |    |

## RSA のキー ペアとアイデンティティ証明書

アイデンティティ証明書を入手するには、1 つまたは複数の RSA キー ペアを作成し、各 RSA キー ペアと Cisco NX-OS デバイスが登録しようとしているトラストポイント CA を関連付けます。Cisco NX-OS デバイスは、CA ごとにアイデンティティを 1 つだけ必要とします。これは CA ごとに 1 つのキー ペアと 1 つのアイデンティティ証明書で構成されています。

Cisco NX-OS ソフトウェアでは、設定変更が可能なキーのサイズ（またはモジュラス）で RSA キー ペアを作成できます。デフォルトのキーのサイズは 512 です。また、RSA キー ペアのラベルも設定できます。デフォルトのキーラベルは、デバイスの完全修飾ドメイン名（FQDN）です。

トラストポイント、RSA キー ペア、およびアイデンティティ証明書の関係を要約したものを次に示します。

- トラストポイントとは、Cisco NX-OS デバイスが、あらゆるアプリケーション（SSH など）のピア証明書用に信頼する特定の CA です。
- Cisco NX-OS デバイスでは、デバイス上に多くのトラストポイントを置くことができ、デバイス上のすべてのアプリケーションは、任意のトラストポイント CA によって発行されたピア証明書を信頼できます。
- トラストポイントは特定のアプリケーション用に限定されません。
- Cisco NX-OS デバイスは、トラストポイントに対応する CA に登録して、アイデンティティ証明書を入手します。デバイスは複数のトラストポイントに登録できます。これは、各トラストポイントから異なるアイデンティティ証明書を入手できることを意味します。アイデンティティ証明書は、発行する CA によって証明書に指定されている目的に応じてアプリケーションで使用します。証明書の目的は、証明書の拡張機能として証明書に保存されます。
- トラストポイントに登録するときには、証明を受ける RSA キー ペアを指定する必要があります。このキーペアは、登録要求を作成する前に作成されていて、トラストポイントに関連付けられている必要があります。トラストポイント、キーペア、およびアイデンティティ証明書との間のアソシエーション（関連付け）は、証明書、キーペア、またはトラストポイントが削除されて明示的になくなるまで有効です。
- アイデンティティ証明書のサブジェクト名は、Cisco NX-OS デバイスの完全修飾ドメイン名です。
- デバイス上には 1 つまたは複数の RSA キー ペアを作成でき、それぞれを 1 つまたは複数のトラストポイントに関連付けることができます。しかし、1 つのトラストポイントに関連付けられるキー ペアは 1 だけです。これは 1 つの CA からは 1 つのアイデンティティ証明書しか入手できないことを意味します。

- Cisco NX-OS デバイスが複数のアイデンティティ証明書を（それぞれ別の CA から）入手する場合は、アプリケーションがピアとのセキュリティプロトコルの交換で使用する証明書は、アプリケーション固有のものになります。
- 1 つのアプリケーションに 1 つまたは複数のトラストポイントを指定する必要はありません。証明書の目的がアプリケーションの要件を満たしていれば、どのアプリケーションもあらゆるトラストポイントで発行されたあらゆる証明書を使用できます。
- あるトラストポイントから複数のアイデンティティ証明書を入手したり、あるトラストポイントに複数のキー ペアを関連付ける必要はありません。ある CA はあるアイデンティティ（または名前）を 1 回だけ証明し、同じ名前で複数の証明書を発行することはありません。ある CA から複数のアイデンティティ証明書を入手する必要がある、またその CA が同じ名前で複数の証明書の発行を許可している場合は、同じ CA 用の別のトラストポイントを定義して、別のキー ペアを関連付け、証明を受ける必要があります。

## 複数の信頼できる CA のサポート

Cisco NX-OS デバイスは、複数のトラストポイントを設定して、それぞれを別の CA に関連付けることにより、複数の CA を信頼できるようになります。信頼できる CA が複数あると、ピアに証明書を発行した特定の CA にデバイスを登録する必要がなくなります。代わりに、ピアが信頼する複数の信頼できる CA をデバイスに設定できます。すると、Cisco NX-OS デバイスは設定されている信頼できる CA を使用して、ピアから受信した証明書で、ピア デバイスの ID で定義されている CA から発行されたものではないものを検証できるようになります。

## PKI の登録のサポート

登録とは、SSH などのアプリケーションに使用するデバイス用のアイデンティティ証明書を入手するプロセスです。これは、証明書を要求するデバイスと、認証局の間で生じます。

Cisco NX-OS デバイスでは、PKI 登録プロセスを実行する際に、次の手順を取ります。

- デバイスで RSA の秘密キーと公開キーのペアを作成します。
- 標準の形式で証明書要求を作成し、CA に送ります。



### Note

要求が CA で受信されたとき、CA サーバでは CA アドミニストレータが登録要求を手動で承認しなくてはならない場合があります。

- 発行された証明書を CA から受け取ります。これは CA の秘密キーで署名されています。
- デバイスの不揮発性のストレージ領域（ブートフラッシュ）に証明書を書き込みます。



## カットアンドペーストによる手動での登録

Cisco NX-OS ソフトウェアでは、手動でのカットアンドペーストによる証明書の取得と登録をサポートしています。カットアンドペーストによる登録とは、証明書要求をカットアンドペーストして、デバイスと CA 間で認証を行うことを意味します。

手動による登録プロセスでカットアンドペーストを使用するには、次の手順を実行する必要があります。

- 証明書登録要求を作成します。これは Cisco NX-OS デバイスで base64 でエンコードされたテキスト形式として表示されます。
- エンコードされた証明書要求のテキストを E メールまたは Web フォームにカットアンドペーストし、CA に送ります。
- 発行された証明書（base64 でエンコードされたテキスト形式）を CA から E メールまたは Web ブラウザによるダウンロードで受け取ります。
- 証明書のインポート機能を使用して、発行された証明書をデバイスにカットアンドペーストします。

## 複数の RSA キー ペアとアイデンティティ CA のサポート

複数のアイデンティティ CA を使用すると、デバイスが複数のトラストポイントに登録できるようになり、その結果、別々の CA から複数のアイデンティティ証明書が発行されます。この機能によって、Cisco NX-OS デバイスは複数のピアを持つ SSH およびアプリケーションに、これらのピアに対応する CA から発行された証明書を使用して参加できるようになります。

また複数の RSA キー ペアの機能を使用すると、登録している各 CA ごとの別々のキー ペアをデバイスで持てるようになります。これは、他の CA で指定されているキーの長さなどの要件と競合することなく、各 CA のポリシー要件に適合させることができます。デバイスでは複数の RSA キー ペアを作成して、各キー ペアを別々のトラストポイントに関連付けることができます。したがって、トラストポイントに登録するときには、関連付けられたキー ペアを証明書要求の作成に使用します。

## ピア証明書の検証

PKI では、Cisco NX-OS デバイスでのピア証明書の検証機能をサポートしています。Cisco NX-OS では、SSH などのアプリケーションのためのセキュリティ交換の際にピアから受け取った証明書を検証します。アプリケーションはピア証明書の正当性を検証します。Cisco NX-OS ソフトウェアでは、ピア証明書の検証の際に次の手順を実行します。

- ピア証明書がローカルの信頼できる CA のいずれかから発行されていることを確認します。
- ピア証明書が現在時刻において有効であること（期限切れでない）ことを確認します。
- ピア証明書が、発行した CA によって取り消されていないことを確認します。

取消確認については、Cisco NX-OS ソフトウェアでは証明書失効リスト（CRL）をサポートしています。トラストポイント CA ではこの方法を使用して、ピア証明書が取り消されていないことを確認できます。

## 証明書の取消確認

Cisco NX-OS ソフトウェアでは、CA 証明書の取消のステータスを確認できます。アプリケーションでは、指定した順序に従って取消確認メカニズムを使用できます。CRL、NDcPP:OCSP for Syslog、なし、またはこれらの方式の組み合わせを指定できます。

### CRL のサポート

CA では証明書失効リスト（CRL）を管理して、有効期限前に取り消された証明書についての情報を提供します。CA では CRL をリポジトリで公開して、発行したすべての証明書の中にダウンロード用の公開 URL 情報を記載しています。ピア証明書を検証するクライアントは、発行した CA から最新の CRL を入手して、これを使用して証明書が取り消されていないかどうかを確認できます。クライアントは、自身の信頼できる CA のすべてまたは一部の CRL をローカルにキャッシュして、その CRL が期限切れになるまで必要に応じて使用することができます。

Cisco NX-OS ソフトウェアでは、先にダウンロードしたトラストポイントについての CRL を手動で設定して、これをデバイスのブートフラッシュ（cert-store）にキャッシュすることができます。ピア証明書の検証の際、Cisco NX-OS ソフトウェアは、CRL がすでにローカルにキャッシュされていて、取消確認でこの CRL を使用するよう設定されている場合にだけ、発行した CA からの CRL をチェックします。それ以外の場合、Cisco NX-OS ソフトウェアでは CRL チェックを実行せず、他の取消確認方式が設定されている場合を除き、証明書は取り消されていないと見なします。

### NDcPP : syslog の OCSP

Online Certificate Status Protocol（OCSP）は、ピアがこの失効情報を取得し、それを検証して証明書失効ステータスを確認する必要がある場合に、証明書失効をチェックする方法です。この方式では、クラウドを介して OCSP レスポンダに到達するピアの機能、または証明書失効情報を取得する証明書送信者のパフォーマンスによって、証明書失効ステータスが制限されます。

リモート syslog サーバが OCSP レスポンダ URL を持つ証明書を共有すると、クライアントはサーバ証明書を外部 OCSP レスポンダ（CA）サーバに送信します。CA サーバはこの証明書を検証し、有効な証明書か失効した証明書かを確認します。この場合、クライアントは失効した証明書リストをローカルに保持する必要はありません。

## 証明書と対応するキー ペアのインポートとエクスポート

CA 認証と登録のプロセスの一環として、下位 CA 証明書（または証明書チェーン）とアイデンティティ証明書を標準の PEM（base64）形式でインポートできます。

トラストポイントでのアイデンティティ情報全体を、パスワードで保護される PKCS#12 標準形式でファイルにエクスポートできます。このファイルは、後で同じデバイス（システムク

ラッシュの後など）や交換したデバイスにインポートすることができます。PKCS#12 ファイル内の情報は、RSA キー ペア、アイデンティティ証明書、および CA 証明書（またはチェーン）で構成されています。

## PKI の注意事項と制約事項

PKI に関する注意事項と制約事項は次のとおりです。

- Cisco NX-OS デバイスに設定できるキー ペアの最大数は 16 です。
- Cisco NX-OS デバイスで宣言できるトラスト ポイントの最大数は 16 です。
- Cisco NX-OS デバイスに設定できるアイデンティティ証明書の最大数は 16 です。
- CA 証明書チェーン内の証明書の最大数は 10 です。
- ある CA に対して認証できるトラストポイントの最大数は 10 です。
- 設定のロールバックでは PKI の設定はサポートしていません。
- Cisco NX-OS リリース 9.3 (5) 以降では、Cisco NX-OS ソフトウェアは NDePP: OCSP for Syslog をサポートしています。
- Cisco NX-OS リリース 10.3(3)F 以降、Cisco Nexus スイッチで証明書を生成およびインポートするために、楕円曲線暗号（ECC）キー ペアのサポートが提供されます。



(注) Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

## PKI のデフォルト設定

次の表に、PKI パラメータのデフォルト設定を示します。

**Table 10: PKI パラメータのデフォルト値**

| パラメータ           | デフォルト      |
|-----------------|------------|
| トラスト ポイント       | なし         |
| RSA キー ペア       | なし         |
| RSA キー ペアのラベル   | デバイスの FQDN |
| RSA キー ペアのモジュール | 512        |

| パラメータ               | デフォルト |
|---------------------|-------|
| RSA キー ペアのエクスポートの可否 | イネーブル |
| 取消確認方式              | CRL   |

## CA の設定とデジタル証明書

ここでは、Cisco NX-OS デバイス上で CA とデジタル証明書が相互に連携して動作するようにするために、実行が必要な作業について説明します。

### ホスト名と IP ドメイン名の設定

デバイスのホスト名または IP ドメイン名をまだ設定していない場合は、設定する必要があります。これは、Cisco NX-OS ソフトウェアでは、アイデンティティ証明書のサブジェクトとして完全修飾ドメイン名（FQDN）を使用するためです。また、Cisco NX-OS ソフトウェアでは、キーの作成の際にラベルが指定されていないと、デバイスの FQDN をデフォルトのキー ラベルとして使用します。たとえば、DeviceA.example.com という名前の証明書は、DeviceA というデバイスのホスト名と example.com というデバイスの IP ドメイン名に基づいています。



**Caution** 証明書を作成した後にホスト名または IP ドメイン名を変更すると、証明書が無効になります。

#### SUMMARY STEPS

1. **configure terminal**
2. **hostname** *hostname*
3. **ip domain-name** *name* [**use-vrf** *vrf-name*]
4. **exit**
5. (Optional) **show hosts**
6. (Optional) **copy running-config startup-config**

#### DETAILED STEPS

##### Procedure

|        | Command or Action                                                                                         | Purpose                      |
|--------|-----------------------------------------------------------------------------------------------------------|------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre> | グローバル コンフィギュレーション モードを開始します。 |

|        | Command or Action                                                                                                                                   | Purpose                                                         |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| ステップ 2 | <b>hostname</b> <i>hostname</i><br><b>Example:</b><br><code>switch(config)# hostname DeviceA</code>                                                 | デバイスのホスト名を設定します。                                                |
| ステップ 3 | <b>ip domain-name</b> <i>name</i> [ <b>use-vrf</b> <i>vrf-name</i> ]<br><b>Example:</b><br><code>DeviceA(config)# ip domain-name example.com</code> | デバイスの IP ドメイン名を設定します。VRF 名が指定されていないと、このコマンドではデフォルトの VRF を使用します。 |
| ステップ 4 | <b>exit</b><br><b>Example:</b><br><code>switch(config)# exit</code><br><code>switch#</code>                                                         | コンフィギュレーション モードを終了します。                                          |
| ステップ 5 | (Optional) <b>show hosts</b><br><b>Example:</b><br><code>switch# show hosts</code>                                                                  | IP ドメイン名を表示します。                                                 |
| ステップ 6 | (Optional) <b>copy running-config startup-config</b><br><b>Example:</b><br><code>switch# copy running-config startup-config</code>                  | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                       |

## RSA キー ペアの生成

RSA キー ペアは、アプリケーション向けのセキュリティプロトコルの交換時に、セキュリティペイロードの署名、暗号化、および復号化のために作成します。デバイスのための証明書を取得する前に、RSA キー ペアを作成する必要があります。

Cisco NX-OS リリース 9.3(3) 以降では、Cisco NX-OS デバイスをトラスト ポイント CA に関連付ける前に、明示的に RSA キー ペアを生成する必要があります。Cisco NX-OS リリース 9.3(3) よりも前では、使用できない場合、RSA キー ペアは自動生成されます。

### SUMMARY STEPS

1. **configure terminal**
2. **crypto key generate rsa** [*label label-string*] [**exportable**] [*modulus size*]
3. **exit**
4. (Optional) **show crypto key mypubkey rsa**
5. (Optional) **copy running-config startup-config**

## DETAILED STEPS

## Procedure

|        | Command or Action                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>                                                               | グローバル コンフィギュレーション モードを開始します                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| ステップ 2 | <b>crypto key generate rsa [label label-string] [exportable] [modulus size]</b><br><br><b>Example:</b><br><pre>switch(config)# crypto key generate rsa exportable</pre> | <p>RSA キーペアを生成します。デバイスに設定できるキー ペアの最大数は 16 です。</p> <p>ラベル文字列には、大文字と小文字を区別して、最大 64 文字の英数字で値を指定します。デフォルトのラベル文字列は、ピリオド文字 (.) で区切ったホスト名と FQDN です。</p> <p>有効なモジュラスの値は 512、768、1024、1536、2048、3072 および 4096 です。デフォルトのモジュラスのサイズは 512 です。</p> <p><b>Note</b><br/>適切なキーのモジュラスを決定する際には、Cisco NX-OS デバイスと CA（登録を計画している対象）のセキュリティ ポリシーを考慮する必要があります。</p> <p>デフォルトでは、キーペアはエクスポートできません。エクスポート可能なキー ペアだけ、PKCS#12 形式でエクスポートできます。</p> <p><b>Caution</b><br/>キーペアのエクスポートの可否は変更できません。</p> |
| ステップ 3 | <b>exit</b><br><br><b>Example:</b><br><pre>switch(config)# exit switch#</pre>                                                                                           | コンフィギュレーション モードを終了します。                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| ステップ 4 | <b>(Optional) show crypto key mypubkey rsa</b><br><br><b>Example:</b><br><pre>switch# show crypto key mypubkey rsa</pre>                                                | 作成したキーを表示します。                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| ステップ 5 | <b>(Optional) copy running-config startup-config</b><br><br><b>Example:</b><br><pre>switch# copy running-config startup-config</pre>                                    | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                                                                                                                                                                                                                                                                                                                                                                                            |

## ECC キー ペアの生成

ECC キー ペアは、アプリケーション向けのセキュリティプロトコルの交換時に、セキュリティペイロードの署名、暗号化、および復号化のために作成します。デバイスのための証明書を取得する前に、ECC キー ペアを作成する必要があります。ECC キーは、同じ長さの場合、RSA キーと比較して強力です。

Cisco NX-OS リリース 10.3(3)F リリース以降、ECC キー ペアを生成して、Cisco NX-OS デバイスをトラストポイント CA に関連付けることができます。

### 手順の概要

1. **configure terminal**
2. **crypto key generate ecc [label ecc-key-label] [exportable] [modulus size]**
3. **no crypto key generate ecc [label ecc-key-label]**
4. **exit**
5. (任意) **show crypto key mypubkey ecc**
6. (任意) **copy running-config startup-config**

### 手順の詳細

#### 手順

|        | コマンドまたはアクション                                                                                                                                                         | 目的                                                                                                                                                                                                                                                                                                            |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br><pre>switch# configure terminal switch(config)#</pre>                                                                            | グローバル コンフィギュレーション モードを開始します。                                                                                                                                                                                                                                                                                  |
| ステップ 2 | <b>crypto key generate ecc [label ecc-key-label] [exportable] [modulus size]</b><br>例 :<br><pre>switch(config)# crypto key generate ecc exportable modulus 224</pre> | <p>ECC キーペアを生成します。デバイスに設定できるキー ペアの最大数は 16 です。</p> <p>ラベル文字列には最大 64 文字の英数字で値を指定します。大文字と小文字は区別されます。デフォルトのラベル文字列は、ピリオド文字 (.) で区切ったホスト名と FQDN です。</p> <p>有効なモジュラス値は、224、384、および 521 です。デフォルトのモジュラスのサイズは 224 です。</p> <p>(注)<br/>適切なキーのモジュラスを決定する際には、Cisco NX-OS デバイスと CA（登録を計画している対象）のセキュリティ ポリシーを考慮する必要があります。</p> |

|        | コマンドまたはアクション                                                                                                                                           | 目的                                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
|        |                                                                                                                                                        | デフォルトでは、キーペアはエクスポートできません。エクスポート可能なキー ペアだけ、PKCS#12 形式でエクスポートできます。<br><br><b>注意</b><br>キー ペアのエクスポートの可否は変更できません。 |
| ステップ 3 | <b>no crypto key generate ecc [label <i>ecc-key-label</i>]</b><br><br>例：<br><pre>switch(config)# no crypto key generate ecc label<br/>label-name</pre> | ECC キーを削除します。                                                                                                 |
| ステップ 4 | <b>exit</b><br><br>例：<br><pre>switch(config)# exit<br/>switch#</pre>                                                                                   | 設定モードを終了します。                                                                                                  |
| ステップ 5 | (任意) <b>show crypto key mypubkey ecc</b><br><br>例：<br><pre>switch# show crypto key mypubkey ecc</pre>                                                  | 作成した ECC キーを表示します。                                                                                            |
| ステップ 6 | (任意) <b>copy running-config startup-config</b><br><br>例：<br><pre>switch# copy running-config startup-config</pre>                                      | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                                     |

## トラストポイント CA のアソシエーションの作成

Cisco NX-OS デバイスとトラスト ポイント CA を関連付ける必要があります。

### Before you begin

RSA キー ペアを作成します。

### SUMMARY STEPS

1. **configure terminal**
2. **crypto ca trustpoint *name***
3. **ca bundle *baselabel***
4. **enrollment terminal**
5. **rsa keypair *label***
6. **exit**
7. (Optional) **show crypto ca trustpoints**
8. (Optional) **copy running-config startup-config**



## DETAILED STEPS

## Procedure

|        | Command or Action                                                                                                                          | Purpose                                                                                                                                     |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>                                      | グローバル構成モードを開始します。                                                                                                                           |
| ステップ 2 | <b>crypto ca trustpoint name</b><br><b>Example:</b><br><pre>switch(config)# crypto ca trustpoint admin-ca switch(config-trustpoint)#</pre> | デバイスが信頼するトラストポイント CA を宣言し、トラストポイント コンフィギュレーション モードを開始します。<br><br><b>Note</b><br>設定できるトラストポイントの最大数は 50 です。                                   |
| ステップ 3 | <b>cabundle baselabel</b><br><b>Example:</b><br><pre>switch(config-trustpoint)# cabundle test</pre>                                        | 特定の CA バンドル下でトラストポイントをグループ化します。このコマンドの <b>No</b> 形式を使用すると、CA バンドルからトラストポイントが切り離されます。このコマンドは、トラストポイントを既存の CA バンドルに関連付けます。新しい CA バンドルは設定しません。 |
| ステップ 4 | <b>enrollment terminal</b><br><b>Example:</b><br><pre>switch(config-trustpoint)# enrollment terminal</pre>                                 | 手動でのカットアンドペーストによる証明書の登録をイネーブルにします。デフォルトではイネーブルになっています。<br><br><b>Note</b><br>Cisco NX-OS ソフトウェアでは、手動でのカットアンドペースト方式による証明書の登録だけをサポートしています。    |
| ステップ 5 | <b>rsakeypair label</b><br><b>Example:</b><br><pre>switch(config-trustpoint)# rsakeypair SwitchA</pre>                                     | RSA キーペアのラベルを指定して、このトラストポイントを登録用に関連付けます。<br><br><b>Note</b><br>CA ごとに 1 つの RSA キー ペアだけを指定できます。                                              |
| ステップ 6 | <b>exit</b><br><b>Example:</b><br><pre>switch(config-trustpoint)# exit switch(config)#</pre>                                               | トラストポイント コンフィギュレーション モードを終了します。                                                                                                             |
| ステップ 7 | (Optional) <b>show crypto ca trustpoints</b><br><b>Example:</b>                                                                            | トラストポイントの情報を表示します。                                                                                                                          |

|        | Command or Action                                                                                                                          | Purpose                                   |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
|        | <code>switch(config)# show crypto ca trustpoints</code>                                                                                    |                                           |
| ステップ 8 | (Optional) <b>copy running-config startup-config</b><br><b>Example:</b><br><code>switch(config)# copy running-config startup-config</code> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。 |

### Related Topics

[RSA キー ペアの生成](#) (139 ページ)

## 証明書マッピングのフィルタの設定

認証に使用される CA 証明書を検証するためのマッピングのフィルタを設定できます。マッピングのフィルタは、CA 証明書をユーザ名と照合するために使用されます。

Cisco NX-OS は次の証明書マッピングのフィルタをサポートします。

- `%username%` : ユーザのログイン名が代入されます。
- `%hostname%` : ピアのホスト名が代入されます。

### 始める前に

証明書認証の `cert-store` を設定します。

### 手順の概要

1. **configure terminal**
2. **crypto certificatemap mapname map-name**
3. **filter** [**subject-name** *subject-name* | **altname-email** *e-mail-ID* | **altname-upn** *user-principal-name*]
4. **exit**
5. (任意) **crypto cert ssh-authorize** [**default** | *issuer-CAname*] [**map** *map-name1* [*map-name2*]]
6. (任意) **show crypto certificatemap**
7. (任意) **show crypto ssh-auth-map**
8. (任意) **copy running-config startup-config**

### 手順の詳細

#### 手順

|        | コマンドまたはアクション                                                                                                | 目的                           |
|--------|-------------------------------------------------------------------------------------------------------------|------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br><code>switch# configure terminal</code><br><code>switch(config)#</code> | グローバル コンフィギュレーション 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 | <b>crypto certificatemap mapname map-name</b><br><br>例 :<br><pre>switch(config)# crypto certificatemap mapname filtermap1</pre>                                                                       | 新しいフィルタ マップを作成します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| ステップ 3 | <b>filter [subject-name subject-name   altname-email e-mail-ID   altname-upn user-principal-name]</b><br><br>例 :<br><pre>switch(config-certmap-filter)# filter altname-upn %username%@cisco.com</pre> | <p>フィルタ マップ内で証明書マッピングのフィルタを 1 つまたは複数設定します。これらの証明書のフィールド属性は、フィルタでサポートされています。証明書は、マップで設定されたすべてのフィルタを通過した場合に検証にパスします。</p> <ul style="list-style-type: none"> <li>• <b>subject-name</b> : 必要なサブジェクト名です。LDAP の認定者名 (DN) 文字列の形式で指定します。次に例を示します。<br/> <pre>filter subject-name CN=%username%</pre>           または<br/> <pre>filter subject-name /C=IN/ST=KA/L=BLR/O=CISCO/OU=ABC/CN=%username%</pre> </li> <li>• <b>altname-email</b> : サブジェクト名の代わりに証明書に含まれている必要がある E メールアドレスです。次に例を示します。<br/> <pre>filter altname-email %username%@cisco.com</pre> </li> <li>• <b>altname-upn</b> : サブジェクト名の代わりに証明書に含まれている必要があるプリンシパル名です。次に例を示します。<br/> <pre>filter altname-upn %username%@%hostname%</pre> </li> </ul> <p>証明書は、マップで設定されたすべてのフィルタを通過した場合に検証にパスします。</p> |
| ステップ 4 | <b>exit</b><br><br>例 :<br><pre>switch(config-certmap-filter)# exit switch(config)#</pre>                                                                                                              | 証明書マッピングのフィルタ コンフィギュレーション モードを終了します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| ステップ 5 | (任意) <b>crypto cert ssh-authorize [default   issuer-CAname] [map map-name1 [map-name2]]</b><br><br>例 :<br><pre>switch(config)# crypto cert ssh-authorize default map filtermap1</pre>                 | <p>セキュアシェル (SSH) プロトコル用の証明書マッピングのフィルタを設定します。SSH 認証用のデフォルトのフィルタ マップを使用するか、CA 証明書の発行元を指定できます。デフォルトのマップを使用しない場合は、認証用のフィルタ マップを 1 つまたは 2 つ指定できます。</p> <p>CA 証明書の発行元を指定した場合、ユーザ アカウントにバインドされた証明書が検証され、設定され</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

|        | コマンドまたはアクション                                                                                                    | 目的                                        |
|--------|-----------------------------------------------------------------------------------------------------------------|-------------------------------------------|
|        |                                                                                                                 | たマップのいずれかを通過すると検証にパスします。                  |
| ステップ 6 | (任意) <b>show crypto certificatemap</b><br><br>例 :<br>switch(config)# show crypto certificatemap                 | 証明書マッピングのフィルタを表示します。                      |
| ステップ 7 | (任意) <b>show crypto ssh-auth-map</b><br><br>例 :<br>switch(config)# show crypto ssh-auth-map                     | SSH 認証用に設定されたマッピングのフィルタを表示します。            |
| ステップ 8 | (任意) <b>copy running-config startup-config</b><br><br>例 :<br>switch(config)# copy running-config startup-config | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。 |

## CA の認証

CA が Cisco NX-OS デバイスに対して認証されると、CA を信頼するプロセスの設定が完了します。まず、PEM 形式の CA の自己署名証明書入手し、Cisco NX-OS デバイスを CA に対して認証する必要があります。この証明書には、CA の公開キーが含まれています。この CA の証明書は自己署名（CA が自身の証明書を署名したもの）であるため、CA の公開キーは、CA アドミニストレータに連絡し、CA 証明書のフィンガープリントを比較して手動で認証する必要があります。



### Note

認証する CA が他の CA の下位 CA である場合、認証する CA は自己署名 CA ではありません。その上位の CA がさらに別の CA の下位である場合もあります。最終的には自己署名 CA に到達します。このタイプの CA 証明書を、認証する CA の CA 証明書チェーンと呼びます。この場合は、CA 認証の際に、証明書チェーン内のすべての CA の CA 証明書の完全なリストを入力する必要があります。CA 証明書チェーン内の証明書の最大数は 10 です。

### Before you begin

CA とのアソシエーションを作成します。

CA 証明書または CA 証明書チェーン入手します。

### SUMMARY STEPS

1. **configure terminal**
2. **crypto ca authenticate name pemfile uri0**
3. **exit**
4. (Optional) **show crypto ca trustpoints**

## 5. (Optional) copy running-config startup-config

## DETAILED STEPS

## Procedure

|        | Command or Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Purpose                                                                                                                                                                                                                                                                                                          |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | グローバル コンフィギュレーション モードを開始します                                                                                                                                                                                                                                                                                      |
| ステップ 2 | <b>crypto ca authenticate name pemfile uri0</b><br><b>Example:</b><br><pre>switch(config)# crypto ca authenticate admin-ca input (cut &amp; paste) CA certificate (chain) in PEM format; end the input with a line containing only END OF INPUT : -----BEGIN CERTIFICATE----- MIIC4jCCAcygAwIBAgIQBWD5Iay0GZRP5R1ljK0ZeJANBgkqhkiG9w0BAQUFADCB kDEgMB4GCSqGSIb3DQEJARYRYWlhamRrZUBjaXNjb3Y5bj20xCzAJBgNVBAYTAk1O MRITwEAYDQIQIEwLLYXJ1eXRha2ExEjAQBGNVBACTCUUhbmhnbG9yZTEOMAwGA1UE ChMEQ2l2Y28xZzARBGNVBAsTCm5ldHN0b3JhZ2UxEjAQBGNVBAMTCUFWYXJ1eSBD QTAeFw0wNTA1MDMyMjQzMzdaFw0wNTA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN AQkBFhhFhWfuzGt1QGnpC2NvImNvbTElMAkGA1UEBhMCSU4xEjAQBGNVBAGTCUth cm5hdGFyYTESMBAGA1UEBxMUQmFuZ2Fsb3JlMQ4wDAYDVOQKEwVdaXNjb2ETMBEG A1UECzMKmV0c3RvcnFhZTESMBAGA1UEAxMUCXBhcn5hIENBMFwwDQYJKoZIhvcN AQEEBQADSwAwSAJBAMW/7b3+DKJPANBSIHHzluNccNM87ypyzwuosNZXOMpeRXXi OzyBagiXT2ASFuUOWQliiMBro/41jf8RxxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E BAMCACYwDwYDVROTAQH/BAUwAwEB/zAdBgNVHQ4EFgQUUjyRcMbrCNMRU2OyRhQ GgsWbHEwawYDVROfBgQwYrjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs Ll0FwYXJ1eSUYjMENBmNybDAwOC6gLLYgZmlsZTovL1xccc3N1L1TA4XEN1cnREbnJv bGxcQXBhcn5hJTIwQ0Euy3JSMBAAGCSsGAQQBgjcVAQQDAgEAMAGCSqGSIb3DQEB BQUAA0EAHv6QU+8ne399Tww+KaGr0g0NIJaQNgLh0AFcT0rEyyut/WYGPzksF9Ea NBG7E0oN66zex0EOEFg1Vs6mXp1//w== -----END CERTIFICATE----- END OF INPUT Fingerprint(s): MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12 Do you accept this certificate? [yes/no]: yes</pre> | <p>CA の証明書をカットアンドペーストするようプロンプトが表示されます。CA を宣言したときに使用した名前と同じ名前を使用します。</p> <p>また、CA チェーンを検証し、指定されたトラストポイントに直接接続します。</p> <p>ある CA に対して認証できるトラストポイントの最大数は 10 です。</p> <p><b>Note</b><br/> 下位 CA の認証の場合、Cisco NX-OS ソフトウェアでは、自己署名 CA に到達する CA 証明書の完全なチェーンが必要になります。これは証明書の検証や PKCS#12 形式でのエクスポートに CA チェーンが必要になるためです。</p> |
| ステップ 3 | <b>exit</b><br><b>Example:</b><br><pre>switch(config)# exit switch#</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | コンフィギュレーション モードを終了します。                                                                                                                                                                                                                                                                                           |
| ステップ 4 | <b>(Optional) show crypto ca trustpoints</b><br><b>Example:</b><br><pre>switch# show crypto ca trustpoints</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | トラストポイント CA の情報を表示します。                                                                                                                                                                                                                                                                                           |
| ステップ 5 | <b>(Optional) copy running-config startup-config</b><br><b>Example:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                                                                                                                                                                                                                                        |

|  | Command or Action                          | Purpose |
|--|--------------------------------------------|---------|
|  | switch# copy running-config startup-config |         |

### Related Topics

[トラストポイント CA のアソシエーションの作成](#) (142 ページ)

## 証明書取消確認方法の設定

クライアント（SSH ユーザなど）とのセキュリティ交換の際に、Cisco NX-OS デバイスは、クライアントから送られたピア証明書の検証を実行します。検証プロセスには、証明書の取消状況の確認が含まれます。

CA からダウンロードした CRL を確認するよう、デバイスに設定できます。CRL のダウンロードとローカルでの確認では、ネットワーク上にトラフィックは発生しません。しかし、証明書がダウンロードとダウンロードの途中で取り消され、デバイス側ではその取り消しに気付かない場合も考えられます。

### Before you begin

CA を認証します。

CRL チェックを使用する場合は、CRL が設定済みであることを確認します。

### SUMMARY STEPS

1. **configure terminal**
2. **crypto ca trustpoint name**
3. **revocation-check {crl [none] | none}**
4. **exit**
5. (Optional) **show crypto ca trustpoints**
6. (Optional) **copy running-config startup-config**

### DETAILED STEPS

#### Procedure

|        | Command or Action                                                                                                                              | Purpose                                        |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>                                      | グローバル構成モードを開始します。                              |
| ステップ 2 | <b>crypto ca trustpoint name</b><br><br><b>Example:</b><br><pre>switch(config)# crypto ca trustpoint admin-ca switch(config-trustpoint)#</pre> | トラストポイント CA を指定し、トラストポイントコンフィギュレーションモードを開始します。 |

|        | Command or Action                                                                                                                        | Purpose                                                                                   |
|--------|------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| ステップ 3 | <b>revocation-check</b> {crl [none]   none}<br><b>Example:</b><br><pre>switch(config-trustpoint)# revocation-check none</pre>            | 証明書取消確認方法を設定します。デフォルトの方式は <b>crl</b> です。<br>Cisco NX-OS ソフトウェアでは、指定した順序に従って証明書取消方式を使用します。 |
| ステップ 4 | <b>exit</b><br><b>Example:</b><br><pre>switch(config-trustpoint)# exit switch(config)#</pre>                                             | トラストポイント コンフィギュレーション モードを終了します。                                                           |
| ステップ 5 | (Optional) <b>show crypto ca trustpoints</b><br><b>Example:</b><br><pre>switch(config)# show crypto ca trustpoints</pre>                 | トラストポイント CA の情報を表示します。                                                                    |
| ステップ 6 | (Optional) <b>copy running-config startup-config</b><br><b>Example:</b><br><pre>switch(config)# copy running-config startup-config</pre> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                 |

#### Related Topics

[CA の認証](#) (146 ページ)

[CRL の設定](#) (156 ページ)

## 証明書要求の作成

使用する各デバイスの RSA キー ペア用に、対応するトラストポイント CA からアイデンティティ証明書を入手するために、要求を作成する必要があります。その後、表示された要求を CA 宛の E メールまたは Web サイトのフォームにカットアンドペーストします。

#### Before you begin

CA とのアソシエーションを作成します。

CA 証明書または CA 証明書チェーンを入手します。

#### SUMMARY STEPS

1. **configure terminal**
2. **crypto ca enroll name**
3. **exit**
4. (Optional) **show crypto ca certificates**
5. (Optional) **copy running-config startup-config**

## DETAILED STEPS

## Procedure

|        | Command or Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Purpose                                                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | グローバル構成モードを開始します。                                                                                                                                                                                    |
| ステップ 2 | <b>crypto ca enroll name</b><br><br><b>Example:</b><br><pre>switch(config)# crypto ca enroll admin-ca Create the certificate request .. Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons your password will not be saved in the configuration. Please make a note of it. Password:nbv123 The subject name in the certificate will be: DeviceA.cisco.com Include the switch serial number in the subject name? [yes/no]: no Include an IP address in the subject name [yes/no]: yes ip address:172.22.31.162 The certificate request will be displayed... -----BEGIN CERTIFICATE REQUEST----- MIIBqQCARQCAQAwHDEaMBGGAUEFAxMRVnVnYXNjby5jb20wgZ8wDQYJ KoZlHvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUUI1DvaSMqNigJ2kt8r141Kx 0JC6anNy4qxk8VeMXZSiLJ4JgTzKwdbLDkITysnjuCXGvjbo+wj0hEhv/y51T9y E2NUJ8omqShrvfZgC7ysN/PymkKogzhbVpj+rargZvHtGJ91XTq4WoVksCzXv8S VqyH0vEvAgmBAAGgTzAVBgkqhkiG9w0BOQcxCHMGbmJ2MTIzMDYGCScqSIb3DQEJ DjBpMCcwJQYDR0RAQH/BBSwGYIRVnVnYXNjby5jb22HEKwMH6IwDQYJ KoZlHvcNAQEBBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99G1FWgt PftRnGwUE/pw6HayfQl2T3ecgNwe12d15133YBF2bktExiIT6U188ntOjglXMjja8 8a23bNDpNsM8rklwA6hWkrVL8NUZEFUxqbjfngPNTZacJCUS6ZqfKCMetbkYtUx0= -----END CERTIFICATE REQUEST-----</pre> | <p>認証した CA に対する証明書要求を作成します。</p> <p><b>Note</b><br/>           チャレンジパスワードを記憶しておいてください。<br/>           このパスワードは設定と一緒に保存されません。証<br/>           明書を取り消す必要がある場合には、このパスワ<br/>          ードを入力する必要があります。</p> |
| ステップ 3 | <b>exit</b><br><br><b>Example:</b><br><pre>switch(config-trustpoint)# exit switch(config)#</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | トラストポイント コンフィギュレーション モードを終了します。                                                                                                                                                                      |
| ステップ 4 | <b>(Optional) show crypto ca certificates</b><br><br><b>Example:</b><br><pre>switch(config)# show crypto ca certificates</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | CA 証明書を表示します。                                                                                                                                                                                        |
| ステップ 5 | <b>(Optional) copy running-config startup-config</b><br><br><b>Example:</b><br><pre>switch(config)# copy running-config startup-config</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 実行コンフィギュレーションを、スタートアップコ<br>ンフィギュレーションにコピーします。                                                                                                                                                        |



## Related Topics

トラストポイント CA のアソシエーションの作成 (142 ページ)

# アイデンティティ証明書のインストール

アイデンティティ証明書は、CA から E メールまたは Web ブラウザ経由で base64 でエンコードされたテキスト形式で受信できます。CA から入手したアイデンティティ証明書を、エンコードされたテキストをカットアンドペーストしてインストールする必要があります。

## Before you begin

CA とのアソシエーションを作成します。

CA 証明書または CA 証明書チェーンを入手します。

## SUMMARY STEPS

1. **configure terminal**
2. **crypto ca import** *name* **certificate**
3. **exit**
4. (Optional) **show crypto ca certificates**
5. (Optional) **copy running-config startup-config**

## DETAILED STEPS

## Procedure

|       | Command or Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Purpose                                                                                                         |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| ステップ1 | <b>configure terminal</b><br><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | グローバル構成モードを開始します。                                                                                               |
| ステップ2 | <b>crypto ca import name certificate</b><br><br><b>Example:</b><br><pre>switch(config)# crypto ca import admin-ca certificate input (cut &amp; paste) certificate in PEM format: -----BEGIN CERTIFICATE----- MIIEADCCA6ggAwIBAgIKCj00oQAAAAAADANBgkqhkiG9w0BAQUFADCBkDEgMBAG CSqGSIb3DQEJARYRZWlhmRrZUBjaXNjb55jb20xCzAJBgNVBAYTAklQMRlWEAYD VQQUeWlLYXJuYXRha2ExEjAQBGMBAwTCCUJhbmRhbG9yZTEQMAwGA1UEChMFQ2l2 Y28xEzARBGMBAwTCCm5ldHNBb3JhZ2UxEjAQBGMBAwTCCUFWYXJuYXN5SEBQTAeFw0w NTEyMTIwMzAyNDBaFw0wNjE5MTIwMzE5NDBaMBwxGjAYBgNVBAMTEVZlZ2FzLTUu Y2l2Y28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBggQCNVADChQ41C dQ1WkKjSICdpLfk5eJSmNQURjGozcuKsZPFxfJ2UoiyeCYE8yLncWYw5E08rJ47 glxr42/sI9IRIb/8udU/cj9jSSfKk56koa7xWYAurDfz8jMcnIM4WLaY/q2q4Gd x7RldfV06uFqFEgs17/Elash9LxLwIDAQAB04ICEzCCAqg8wJQYDVROAQH/BBSw GYIRVmtVnYXMTMS5jaXNjb55jb2ZHEKwWH6TwHQYDVROBBYEFKCLi+2sspWEfgrR bhWmLVyo9jngMIHMBGnVHSMEGcQwgcGAFCco8kaDG6wjTEVnjskYUBOLfmxoxYGV pTGIMIQQSMAHqYJKoZlthvcaQKBHfbbWFrZGtLQGNpc2NvImNvbTElMAkGA1UE</pre> | <p>admin-ca という名前の CA に対するアイデンティティ証明書をカットアンドペーストするよう、プロンプトが表示されます。</p> <p>デバイスに設定できるアイデンティティ証明書の最大数は 16 です。</p> |

■ トラストポイントの設定がリブート後も維持されていることの確認

|        | Command or Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Purpose                                    |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|
|        | <pre> BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFyYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w DAYDMQOKBwVDAhNjBzETIMBGA1UECzMKamV0c3RvcmFhZTESMBAGA1UEAxMJQXBh cm5hIENBghAFYNKJrLQZ1E9UEiWMrR16MGsGA1UdHwRkMGItwLgAsoCgKgGh0dHA6 Ly9zc2UtdGvQ2VydEVucm9sbC9BcGFybmElmJBDQS5jcmwwMKAuoCyGKmZpbGU6 Ly9cXHNzZS0wOFxDZXJ0RWF5b2xsXEEFWYXJlYSUyMENBLmNyYDDBiGyTKwYBBQUH AQEFfjB8MDsGCCsGAQUFBzAChi9odiHRwOi8vc3N1LTA4L0N1cnRfbnJvbGwvc3N1 LTA4X0FwYXJlYSUyMENBLmNyYDA9BggrBgEFBQcwAoYxcmIsZTovL1xoc3N1LTA4 XEN1cnRfbnJvbGwvc3N1LTA4X0FwYXJlYSUyMENBLmNyYDANBgkqhkiG9w0BAQUF AANBALBGBGsbE7GNLh9xeOTWENam24U69ZSuDDCcOZUUTgprnTqVpPyejtsyflw E36cIZu4WsExREqxbTk8ycx7V5o= -----END CERTIFICATE----- </pre> |                                            |
| ステップ 3 | <p><b>exit</b></p> <p><b>Example:</b></p> <pre> switch(config)# exit switch# </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 設定モードを終了します。                               |
| ステップ 4 | <p>(Optional) <b>show crypto ca certificates</b></p> <p><b>Example:</b></p> <pre> switch# show crypto ca certificates </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | CA 証明書を表示します。                              |
| ステップ 5 | <p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre> switch# copy running-config startup-config </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。 |

### Related Topics

[トラストポイント CA のアソシエーションの作成](#) (142 ページ)

## トラストポイントの設定がリブート後も維持されていることの確認

トラストポイントの設定が、Cisco NX-OS デバイスのリブート後も維持されていることを確認できます。

トラストポイントの設定は、通常の Cisco NX-OS デバイスの設定であり、スタートアップ コンフィギュレーションに確実にコピーした場合にだけ、システムのリブート後も維持されます。トラストポイント設定をスタートアップ コンフィギュレーションにコピーしておけば、トラストポイントに関連する証明書、キーペア、および CRL が自動的に保持されます。逆に、トラストポイントがスタートアップ コンフィギュレーションにコピーされていないと、証明書、キーペア、および関連 CRL は保持されません。リブート後に、対応するトラストポイント設定が必要になるからです。設定した証明書、キーペア、および CRL を確実に保持するために、必ず、実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーしてください。また、証明書またはキーペアを削除した後は実行コンフィギュレーションを保存して、削除が永続的に反映されるようにしてください。

トラストポイントに関連付けられた証明書と CRL は、そのトラストポイントがすでにスタートアップ コンフィギュレーションに保存されていれば、インポートした時点で（つまりスタートアップ コンフィギュレーションにコピーしなくても）維持されるようになります。

パスワードで保護したアイデンティティ証明書のバックアップを作成して、これを外部のサーバに保存することを推奨します。



**Note** コンフィギュレーションを外部サーバにコピーすると、証明書およびキー ペアも保存されます。

#### Related Topics

[PKCS 12 形式でのアイデンティティ情報のエクスポート](#) (153 ページ)

## PKCS 12 形式でのアイデンティティ情報のエクスポート

アイデンティティ証明書を、トラストポイントの RSA キー ペアや CA 証明書（または下位 CA の場合はチェーン全体）と一緒に PKCS#12 ファイルにバックアップ目的でエクスポートすることができます。デバイスのシステムクラッシュからの復元の際や、スーパーバイザモジュールの交換の際には、証明書や RSA キー ペアをインポートすることができます。



**Note** エクスポートの URL を指定するときに使用できるのは、`bootflash:filename` という形式だけです。

#### Before you begin

CA を認証します。

アイデンティティ証明書をインストールします。

### SUMMARY STEPS

1. **configure terminal**
2. **crypto ca export name pkcs12 bootflash:filename password**
3. **exit**
4. **copy bootflash:filename scheme://server/ [url /]filename**

### DETAILED STEPS

#### Procedure

|        | Command or Action                                                                                 | Purpose                     |
|--------|---------------------------------------------------------------------------------------------------|-----------------------------|
| ステップ 1 | <b>configure terminal</b><br><br><b>Example:</b><br>switch# configure terminal<br>switch(config)# | グローバル コンフィギュレーション モードを開始します |

|        | Command or Action                                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                     |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 2 | <b>crypto ca export name pkcs12 bootflash:filename password</b><br><br><b>Example:</b><br><pre>switch(config)# crypto ca export admin-ca pkcs12 bootflash:adminid.p12 nbv123</pre> | アイデンティティ証明書と、トラストポイント CA の対応するキーペアと CA 証明書をエクスポートします。パスワードには、大文字と小文字を区別して、最大 128 文字の英数字で値を指定します。                                                                                                                                                                                            |
| ステップ 3 | <b>exit</b><br><br><b>Example:</b><br><pre>switch(config)# exit switch#</pre>                                                                                                      | コンフィギュレーション モードを終了します。                                                                                                                                                                                                                                                                      |
| ステップ 4 | <b>copy bootflash:filename scheme://server/ [url /]filename</b><br><br><b>Example:</b><br><pre>switch# copy bootflash:adminid.p12 tftp:adminid.p12</pre>                           | <p>PKCS#12形式のファイルをリモートサーバにコピーします。</p> <p><i>scheme</i> 引数に対しては、<b>tftp:</b>、<b>ftp:</b>、<b>scp:</b>、または <b>sftp:</b> を入力できます。<i>server</i> 引数は、リモートサーバのアドレスまたは名前であり、<i>url</i> 引数はリモートサーバにあるソース ファイルへのパスです。</p> <p><i>server</i>、<i>url</i>、および <i>filename</i> の各引数は、大文字小文字を区別して入力します。</p> |

#### Related Topics

[RSA キー ペアの生成](#) (139 ページ)

[CA の認証](#) (146 ページ)

[アイデンティティ証明書のインストール](#) (151 ページ)

## PKCS 12または PKCS 7 フォーマットで ID 情報のインポート

デバイスのシステム クラッシュからの復元の際や、スーパーバイザ モジュールの交換の際には、証明書や RSA キー ペアをインポートすることができます。



**Note** インポートの URL を指定するときに使用できるのは、`bbootflash:filename` という形式だけです。

#### Before you begin

CA 認証によってトラストポイントに関連付けられている RSA キー ペアがないこと、およびトラストポイントに関連付けられている CA がいないことを確認して、トラストポイントが空であるようにします。

#### SUMMARY STEPS

1. **copy scheme:// server/[url /]filename bootflash:filename**

2. **configure terminal**
3. **crypto ca import name [pkcs12 | pkcs7] bootflash:filename**
4. **exit**
5. (Optional) **show crypto ca certificates**
6. (Optional) **copy running-config startup-config**

## DETAILED STEPS

### Procedure

|        | Command or Action                                                                                                                                                               | Purpose                                                                                                                                                                                                                                                                                            |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>copy scheme:// server/[url /]filename bootflash:filename</b><br><b>Example:</b><br><pre>switch# copy tftp:adminid.p12 bootflash:adminid.p12</pre>                            | PKCS#12 形式のファイルをリモート サーバからコピーします。<br><br><i>scheme</i> 引数に対しては、 <b>tftp:</b> 、 <b>ftp:</b> 、 <b>scp:</b> 、または <b>sftp:</b> を入力できます。 <i>server</i> 引数は、リモートサーバのアドレスまたは名前であり、 <i>url</i> 引数はリモートサーバにあるソース ファイルへのパスです。<br><br><i>server</i> 、 <i>url</i> 、および <i>filename</i> の各引数は、大文字小文字を区別して入力します。 |
| ステップ 2 | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>                                                                           | グローバル コンフィギュレーション モードを開始します                                                                                                                                                                                                                                                                        |
| ステップ 3 | <b>crypto ca import name [pkcs12   pkcs7] bootflash:filename</b><br><b>Example:</b><br><pre>switch(config)# crypto ca import admin-ca pkcs12 bootflash:adminid.p12 nbv123</pre> | アイデンティティ証明書と、トラストポイント CA の対応するキー ペアと CA 証明書をインポートします。                                                                                                                                                                                                                                              |
| ステップ 4 | <b>exit</b><br><b>Example:</b><br><pre>switch(config)# exit switch#</pre>                                                                                                       | 設定モードを終了します。                                                                                                                                                                                                                                                                                       |
| ステップ 5 | (Optional) <b>show crypto ca certificates</b><br><b>Example:</b><br><pre>switch# show crypto ca certificates</pre>                                                              | CA 証明書を表示します。                                                                                                                                                                                                                                                                                      |
| ステップ 6 | (Optional) <b>copy running-config startup-config</b><br><b>Example:</b><br><pre>switch# copy running-config startup-config</pre>                                                | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                                                                                                                                                                                                                          |

## CRL の設定

トラストポイントからダウンロードした CRL を手動で設定することができます。Cisco NX-OS ソフトウェアでは、CRL をデバイスのブートフラッシュ (cert-store) にキャッシュします。ピア証明書の検証の際、Cisco NX-OS ソフトウェアが発行した CA からの CRL をチェックするのは、CRL をデバイスにダウンロードしていて、この CRL を使用する証明書取消確認を設定している場合だけです。

### Before you begin

証明書取消確認がイネーブルになっていることを確認します。

### SUMMARY STEPS

1. **copy scheme:[//server/[url /]]filename bootflash:filename**
2. **configure terminal**
3. **crypto ca crl request name bootflash:filename**
4. **exit**
5. (Optional) **show crypto ca crl name**
6. (Optional) **copy running-config startup-config**

### DETAILED STEPS

#### Procedure

|        | Command or Action                                                                                                                                              | Purpose                                                                                                                                                                                                                                                                                     |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>copy scheme:[//server/[url /]]filename bootflash:filename</b><br><br><b>Example:</b><br><pre>switch# copy tftp:adminca.crl bootflash:adminca.crl</pre>      | リモート サーバから CRL をダウンロードします。<br><br><i>scheme</i> 引数に対しては、 <b>tftp:</b> 、 <b>ftp:</b> 、 <b>scp:</b> 、または <b>sftp:</b> を入力できます。 <i>server</i> 引数は、リモートサーバのアドレスまたは名前であり、 <i>url</i> 引数はリモートサーバにあるソース ファイルへのパスです。<br><br><i>server</i> 、 <i>url</i> 、および <i>filename</i> の各引数は、大文字小文字を区別して入力します。 |
| ステップ 2 | <b>configure terminal</b><br><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>                                                      | グローバル コンフィギュレーション モードを開始します                                                                                                                                                                                                                                                                 |
| ステップ 3 | <b>crypto ca crl request name bootflash:filename</b><br><br><b>Example:</b><br><pre>switch(config)# crypto ca crl request admin-ca bootflash:adminca.crl</pre> | ファイルで指定されている CRL を設定するか、現在の CRL と置き換えます。                                                                                                                                                                                                                                                    |
| ステップ 4 | <b>exit</b><br><br><b>Example:</b>                                                                                                                             | コンフィギュレーション モードを終了します。                                                                                                                                                                                                                                                                      |

|        | Command or Action                                                                                                         | Purpose                                   |
|--------|---------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
|        | switch(config)# exit<br>switch#                                                                                           |                                           |
| ステップ 5 | (Optional) <b>show crypto ca crt name</b><br><br><b>Example:</b><br>switch# show crypto ca crt admin-ca                   | CA の CRL 情報を表示します。                        |
| ステップ 6 | (Optional) <b>copy running-config startup-config</b><br><br><b>Example:</b><br>switch# copy running-config startup-config | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。 |

## CA の設定からの証明書の削除

トラストポイントに設定されているアイデンティティ証明書や CA 証明書を削除できます。最初にアイデンティティ証明書を削除し、その後で CA 証明書を削除します。アイデンティティ証明書を削除した後で、RSA キー ペアとトラストポイントの関連付けを解除できます。証明書の削除は、期限切れになった証明書や取り消された証明書、破損した（あるいは破損したと思われる）キー ペア、現在は信頼されていない CA を削除するために必要です。

### SUMMARY STEPS

1. **configure terminal**
2. **crypto ca trustpoint name**
3. **delete ca-certificate**
4. **delete certificate [force]**
5. **exit**
6. (Optional) **show crypto ca certificates [name]**
7. (Optional) **copy running-config startup-config**

### DETAILED STEPS

#### Procedure

|        | Command or Action                                                                                                                      | Purpose                                         |
|--------|----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br><b>Example:</b><br>switch# configure terminal<br>switch(config)#                                      | グローバル構成モードを開始します。                               |
| ステップ 2 | <b>crypto ca trustpoint name</b><br><br><b>Example:</b><br>switch(config)# crypto ca trustpoint admin-ca<br>switch(config-trustpoint)# | トラストポイント CA を指定し、トラストポイントコンフィギュレーション モードを開始します。 |

|        | Command or Action                                                                                                                   | Purpose                                                                                                                                                                                                                             |
|--------|-------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 3 | <b>delete ca-certificate</b><br><br><b>Example:</b><br>switch(config-trustpoint)# delete ca-certificate                             | CA 証明書または証明書チェーンを削除します。                                                                                                                                                                                                             |
| ステップ 4 | <b>delete certificate [force]</b><br><br><b>Example:</b><br>switch(config-trustpoint)# delete certificate                           | アイデンティティ証明書を削除します。<br><br>削除しようとしているアイデンティティ証明書が証明書チェーン内の最後の証明書である場合や、デバイス内の唯一のアイデンティティ証明書である場合は、 <b>force</b> オプションを使用する必要があります。この要件は、証明書チェーン内の最後の証明書や唯一のアイデンティティ証明書を誤って削除してしまい、アプリケーション（SSH など）で使用する証明書がなくなってしまうことを防ぐために設けられています。 |
| ステップ 5 | <b>exit</b><br><br><b>Example:</b><br>switch(config-trustpoint)# exit<br>switch(config)#                                            | トラストポイント コンフィギュレーション モードを終了します。                                                                                                                                                                                                     |
| ステップ 6 | (Optional) <b>show crypto ca certificates [name]</b><br><br><b>Example:</b><br>switch(config)# show crypto ca certificates admin-ca | CA の証明書情報を表示します。                                                                                                                                                                                                                    |
| ステップ 7 | (Optional) <b>copy running-config startup-config</b><br><br><b>Example:</b><br>switch(config)# copy running-config startup-config   | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                                                                                                                                                           |

## Cisco NX-OS デバイスからの RSA キー ペアの削除

RSA キーペアが何らかの理由で破損し、現在は使用されていないと見られるときには、その RSA キー ペアを Cisco NX-OS デバイスから削除することができます。



### Note

デバイスから RSA キー ペアを削除した後、CA アドミニストレータに、その CA にあるこのデバイスの証明書を取り消すよう依頼します。その証明書を最初に要求したときに作成したチャレンジパスワードを入力する必要があります。

## SUMMARY STEPS

1. **configure terminal**
2. **crypto key zeroize rsa label**



3. **exit**
4. (Optional) **show crypto key mypubkey rsa**
5. (Optional) **copy running-config startup-config**

## DETAILED STEPS

### Procedure

|        | Command or Action                                                                                                                | Purpose                                    |
|--------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>                            | グローバル コンフィギュレーション モードを開始します                |
| ステップ 2 | <b>crypto key zeroize rsa label</b><br><b>Example:</b><br><pre>switch(config)# crypto key zeroize rsa MyKey</pre>                | RSA キー ペアを削除します。                           |
| ステップ 3 | <b>exit</b><br><b>Example:</b><br><pre>switch(config)# exit switch#</pre>                                                        | コンフィギュレーション モードを終了します。                     |
| ステップ 4 | (Optional) <b>show crypto key mypubkey rsa</b><br><b>Example:</b><br><pre>switch# show crypto key mypubkey rsa</pre>             | RSA キー ペアの設定を表示します。                        |
| ステップ 5 | (Optional) <b>copy running-config startup-config</b><br><b>Example:</b><br><pre>switch# copy running-config startup-config</pre> | 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。 |

### Related Topics

[証明書要求の作成](#) (149 ページ)

## PKI の設定の確認

PKI 設定情報を表示するには、次のいずれかの作業を行います。

| コマンド                                | 目的                                        |
|-------------------------------------|-------------------------------------------|
| <b>show crypto key mypubkey rsa</b> | Cisco NX-OS デバイスで作成された RSA 公開キーの情報を表示します。 |

| コマンド                               | 目的                            |
|------------------------------------|-------------------------------|
| <b>show crypto ca certificates</b> | CA とアイデンティティ証明書についての情報を表示します。 |
| <b>show crypto ca crl</b>          | CA の CRL についての情報を表示します。       |
| <b>show crypto ca trustpoints</b>  | CA トラストポイントについての情報を表示します。     |

## PKI の設定例

ここでは、Microsoft Windows Certificate サーバを使用して Cisco NX-OS デバイスで証明書と CRL を設定する作業の例について説明します。



**Note** デジタル証明書の作成には、どのようなタイプのサーバでも使用できます。Microsoft Windows Certificate サーバに限られることはありません。

## Cisco NX-OS デバイスでの証明書の設定

Cisco NX-OS デバイスで証明書を設定するには、次の手順に従ってください。

### Procedure

**ステップ 1** デバイスの FQDN を設定します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# hostname Device-1
Device-1(config)#
```

**ステップ 2** デバイスの DNS ドメイン名を設定します。

```
Device-1(config)# ip domain-name cisco.com
```

**ステップ 3** トラストポイントを作成します。

```
Device-1(config)# crypto ca trustpoint myCA
Device-1(config-trustpoint)# exit
Device-1(config)# show crypto ca trustpoints
trustpoint: myCA; key:
revocation methods: crl
```

#### ステップ4 このデバイス用の RSA キー ペアを作成します。

```
Device-1(config)# crypto key generate rsa label myKey exportable modulus 1024
Device-1(config)# show crypto key mypubkey rsa
key label: myKey
key size: 1024
exportable: yes
```

## ステップ5 RSA キー ペアとトラストポイントを関連付けます。

```
Device-1(config)# crypto ca trustpoint myCA
Device-1(config-trustpoint)# rsakeypair myKey
Device-1(config-trustpoint)# exit
Device-1(config)# show crypto ca trustpoints
trustpoint: myCA; key: myKey
revocation methods: crl
```

## ステップ6 Microsoft Certificate Service の Web インターフェイスから CA をダウンロードします。

## ステップ1

```

Device-1(config)# crypto ca authenticating myCA
input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRIIjK0ZejaNBGkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYWlhbmrZUBjaXNjb3Y5b20xXzA2BgNVBAYTAk10
MRIwEAYDVQQIEw1LYXJuYXRha2EueXjAQBgNVBACTCUJhbmdbG9yZTEOMAwGA1UE
ChMFQ2l1Z28xXzARBGNVBAStcm5ldHN0b3JhZ2UueXjAQBgNVBAMTCUFwYXJuYzSD
QTAcFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgJKoZiIhvcN
AQkBfHfHbWfWZgTlQGNpc2NvLmNvbTElMAkGA1UEBhMCSU4xXzA2BgNVBAGTCUth
cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDAxNjBzETMBEG
A1UECgMKbWV0c3RvcnFnZTESMBAGA1UEAxMjQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSABJAMW/7b3+DXJPANBsIHHzlUcNcNM87ypyzwuoSNZXOMperXXI
OzyBqgiXT2ASFuUoWqlidM8ro/41jf8RxxYKvysCAWAdA0BvzCBvDALBgNVHQ8E
BAMCAcYwDwYDVR0TAAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyJyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0FBGQwYjAuOCyGKoYoAHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYzUyMENBLmNybDAwocG6gLIYqZmlsZTovL1xccc3N1LT44XEN1cnRfbnJv
bGxcQXBhcm5hJT1wQ2U0EuY3JsbMABGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQE
BQUAAOEAHv6UQ+8nE399Tww+KaGr0gONiJagNgLh0AFcT0rEyuyt/WYGpKsF9Ea
NBG7E0nN66zex0EOEFG1Vs6mXp1//w==
-----END CERTIFICATE-----
END OF INPUT
Fingerprint(s): MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
Do you accept this certificate? [yes/no]:y

```

**ステップ8**    トラストポイントに登録するために使用する証明書要求を作成します。

```

Device-1(config)# crypto ca enroll myCA
Create the certificate request ..
Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password: nbv123
The subject name in the certificate will be: Device-1.cisco.com
Include the switch serial number in the subject name? [yes/no]: no
Include an IP address in the subject name [yes/no]: yes
ip address: 10.10.1.1
The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIIBQzCCARQCAQAwHDEaMBGAlUEAxMRVmVnYXMTMS5jaXNjbY5jb20wgZ8wDQYJ
KoZIHvcNAQEIBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8r14lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjB+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVKSzcXv8S
VqyH0vEvAgMBAAGTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCsGSIb3DQEJ
DjEpMCCwJQYDVORAQH/BBswGYIRVmVnYXMTMS5jaXNjbY5jb22HBKwWH6IwDQYJ
KoZIHvcNAQEIBBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99G1FWgt
PftrNcWUE/pw6HayfQ12T3ecgNwel2d15133YBF2bktExiI6U188nTOjglXMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=
-----END CERTIFICATE REQUEST-----

```

**ステップ 9** Microsoft Certificate Service の Web インターフェイスからアイデンティティ証明書を要求します。

**ステップ 10** アイデンティティ証明書をインポートします。

```

Device-1(config)# crypto ca import myCA certificate
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIEADCCA6qgAwIBAgIKCj00oQAAAAAAdANBgkqhkiG9w0BAQUFADCBkDEgMB4G
CSQGSU1b3DQEJARYRYW1hbmRrZUBjaXNjbY5jb20xCzAJBgNVBAYTAk1OMRIwEAYD
VQQIEw1LYXJuYXRha2ExEjAQBGNVBACTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ2l2
Y28xEzARBGNVBASTCm5ldhN0b3JhZ2UxEjAQBGNVBAMTCUFwYXJuYSDQTAeFw0w
NTEwMTIwMzAyNDYwNjExMTIwMzEyNDYwMzEyNDYwMzEyNDYwMzEyNDYwMzEyNDYw
Y2l2Y28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C
dQ1WkjKjSICdpLfk5eJSnNCQujGpzcKsZPFxfF2UoiyeCYE8y1ncWyw5E08rJ47
glxr42/sI9IRib/8udu/cj9jSSfKK56koa7xWYA8rDfz8jMCnIM4W1aY/q2q4Gb
x7Rifdv06uFqFZEgS17/Elash9LxLwIDAQABO4ICEzCCAg8wJQYDVORAQH/BBsw
GYIRVmVnYXMTMS5jaXNjbY5jb22HBKwWH6IwHQYDVOR0OBByEFKCLi+2sspWEfgrR
bhWm1Vyo9jngMIHMBGNVHSMEGcQwgcGAFFCo8kaDG6wjTEVNjskYUBoLFmxxoYGW
pIGTMIGQMSAwHgYJKoZIHvcNAQkBFhFhbWVnZGt1QGNpc2NvLmNvbTElMAkGA1UE
BhMCSU4xEjAQBGNVBAGTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w
DAYDVQQKEWVdaXNjbzE0MDEGA1UECzMkY0MDEGA1UECzMkY0MDEGA1UECzMkY0MDE
cm5hIENBghAFYNKJrLQZLE9JEiWMrRl6MGsGA1UdHwRkMGiWlQAsOCqGKGh0dHA6
Ly9zc2UtdMDgV2VydEVucm9sbC9BcGFybmElMjBDBQ55jcmwMKAuoCyGKwZpbGU6
Ly9cXHNzZS0wOFx0ZDZlJ0Rw5yb2xsXEFwYXJuYSDYUyMENBLmNybDcBicYIKwYBBQUH
AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0NlcnRFbnJvbGwvc3Nl
LTA4X0FwYXJuYSDYUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xccc3NlLTA4
XENlcnRFbnJvbGwvc3NlLTA4X0FwYXJuYSDYUyMENBLmNydANBgkqhkiG9w0BAQUF
AANBAdBgBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyjtsyflw
E36cIZu4WsExREqxbTk8ycx7V5o=
-----END CERTIFICATE-----
Device-1(config)# exit
Device-1#

```

**ステップ 11** 証明書の設定を確認します。

**ステップ 12** 証明書の設定をスタートアップ コンフィギュレーションに保存します。

**Related Topics**[CA 証明書のダウンロード](#) (163 ページ)[アイデンティティ証明書の要求](#) (169 ページ)

## CA 証明書のダウンロード

Microsoft Certificate Service の Web インターフェイスから CA 証明書をダウンロードする手順は、次のとおりです。

## Procedure

**ステップ 1** Microsoft Certificate Services の Web インターフェイスから、[Retrieve the CA certificate or certificate revocation task] をクリックし、[Next] をクリックします。

**Microsoft** Certificate Services -- Apama CA

### Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. You will be able to securely identify yourself to other people over the web, sign your e-mail messages, and so on, depending upon the type of certificate you request.

#### Select a task:

- ☒ Retrieve the CA certificate or certificate revocation list
- ☐ Request a certificate
- ☐ Check on a pending certificate

**ステップ 2** 表示されたリストから、ダウンロードする CA 証明書ファイルを選択します。[Base 64 encoded] をクリックし、[Download CA certificate] をクリックします。

Microsoft Certificate Services -- Aparna CA

### Retrieve The CA Certificate Or Certificate Revocation List

[Install this CA certification path](#) to allow your computer to trust certificates issued from this certificate.

It is not necessary to manually install the CA certification path if you request and install a certificate. The CA certification path will be installed for you automatically.

#### Choose file to download:

CA Certificate: Current [Aparna CA]

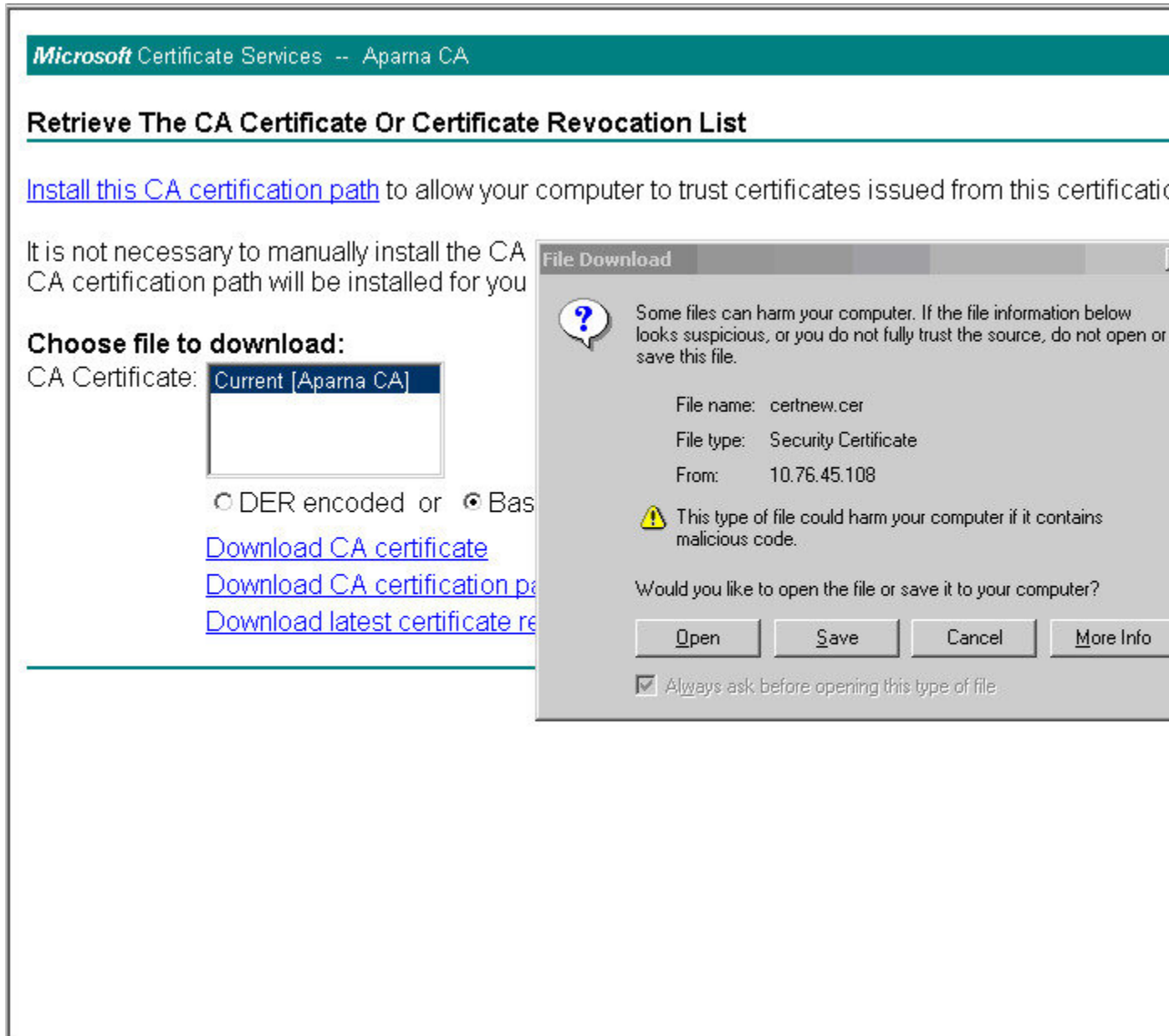
☐ DER encoded or ☒ Base 64 encoded

[Download CA certificate](#)

[Download CA certification path](#)

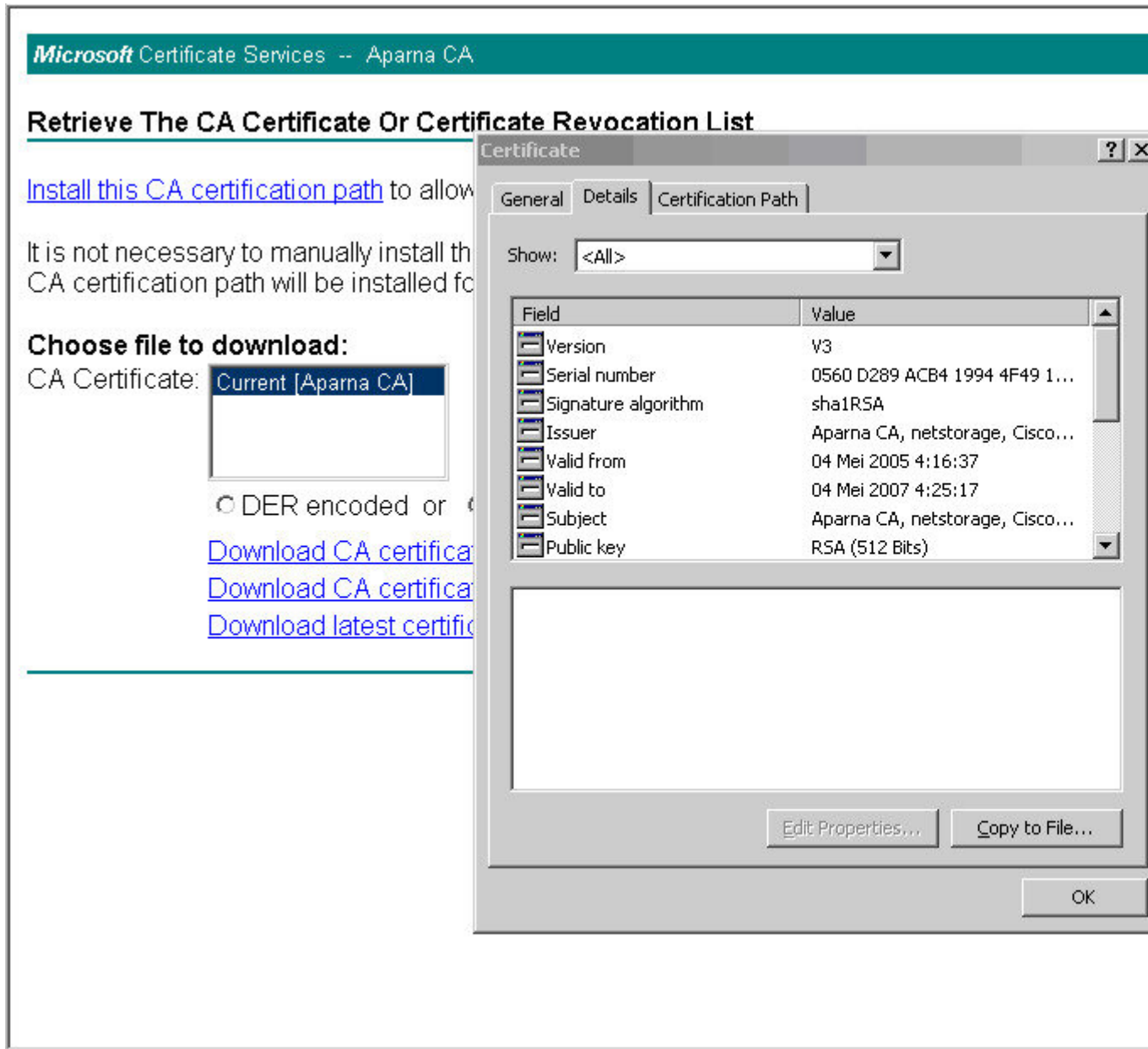
[Download latest certificate revocation list](#)

ステップ 3 [File Download] ダイアログボックスにある [Open] をクリックします。

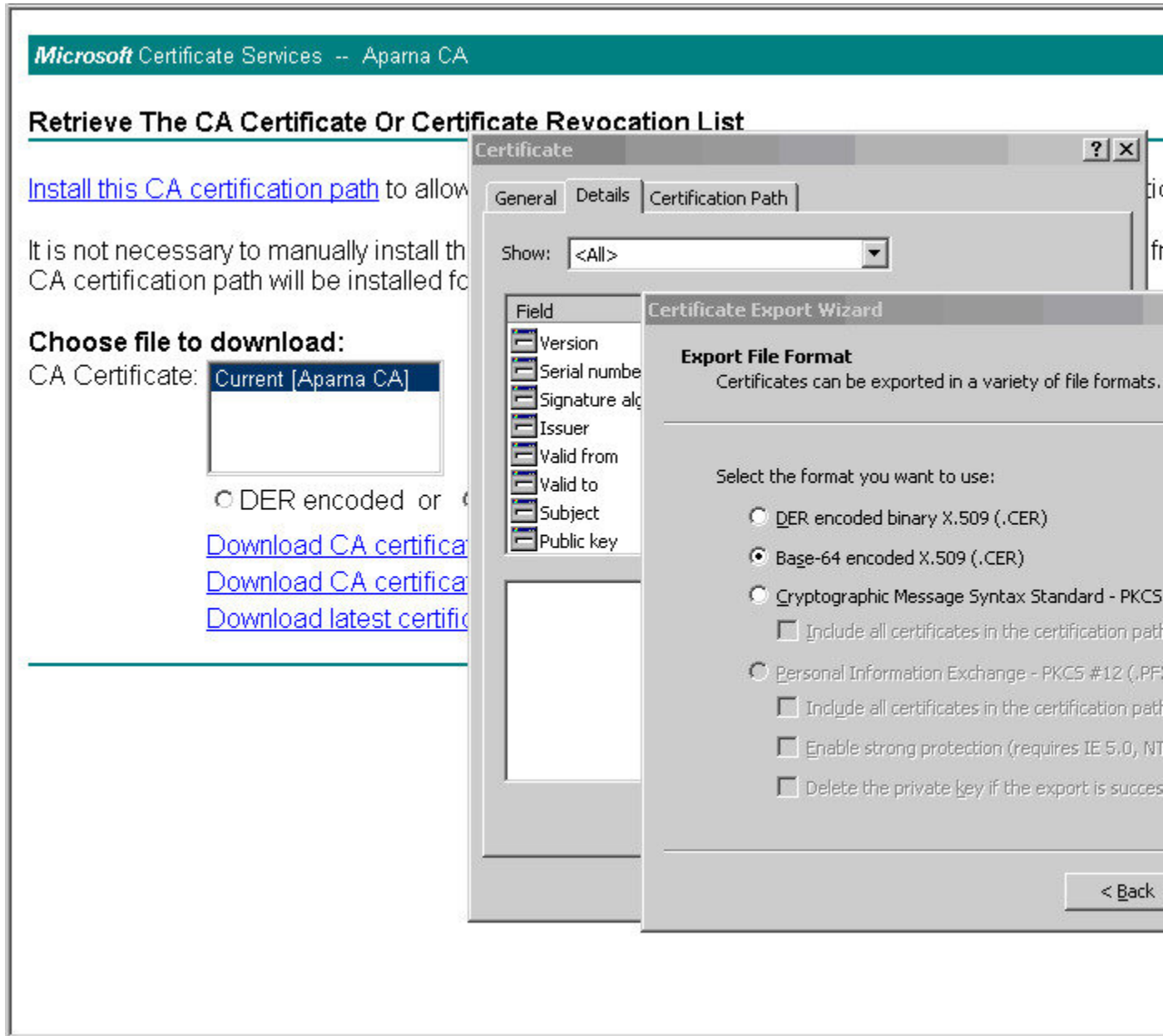




ステップ 4 [Certificate] ダイアログボックスにある [Copy to File] をクリックし、[OK] をクリックします。



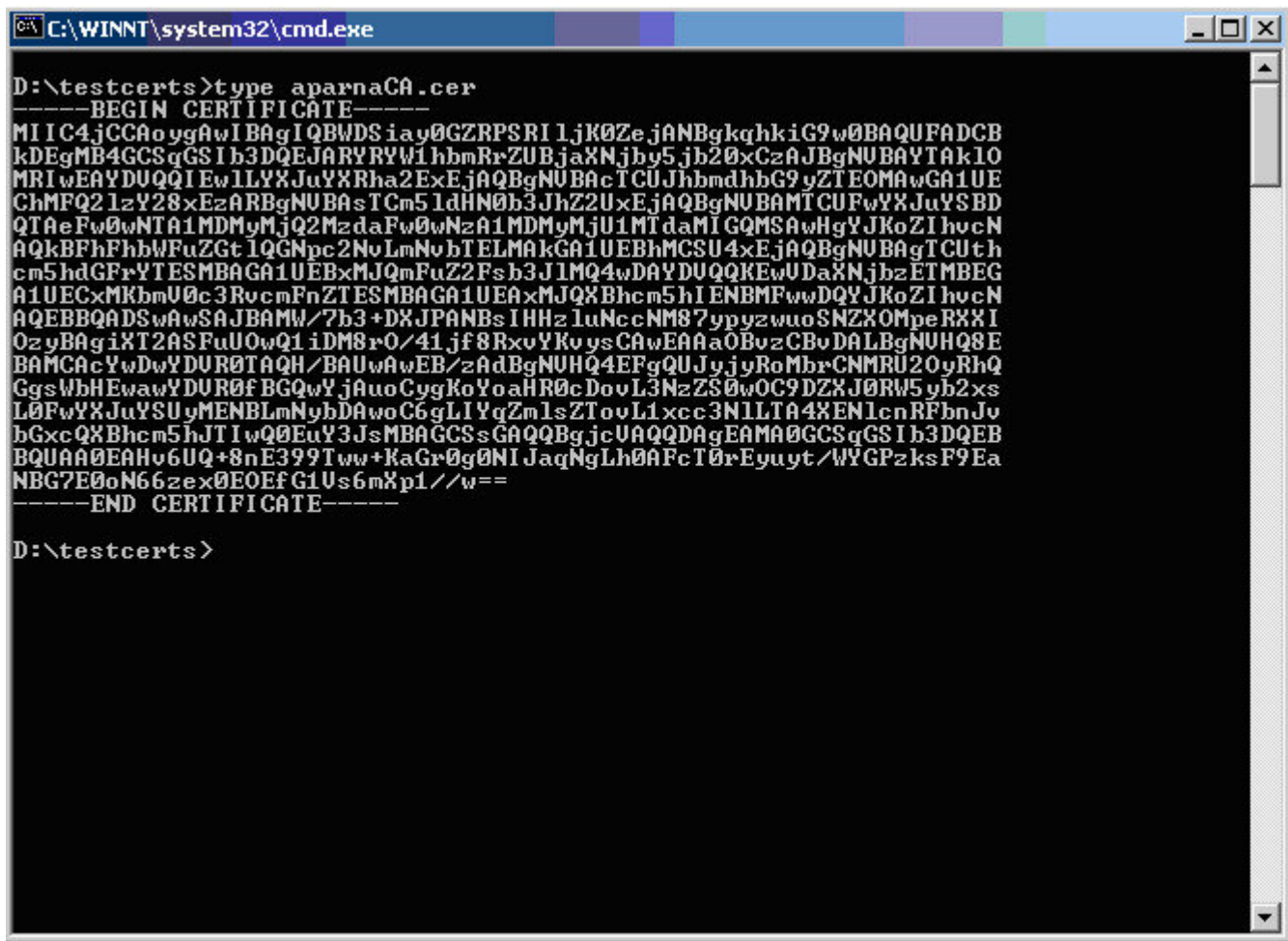
ステップ 5 [Certificate Export Wizard] ダイアログボックスから [Base-64 encoded X.509 (.CER)] を選択し、[Next] をクリックします。



ステップ 6 [Certificate Export Wizard] ダイアログボックスにある [File name:] テキスト ボックスに保存するファイル名を入力し、[Next] をクリックします。

ステップ 7 [Certificate Export Wizard] ダイアログボックスで、[Finish] をクリックします。

ステップ 8 Microsoft Windows の type コマンドを入力して、Base-64（PEM）形式で保存されている CA 証明書を表示します。



```

C:\WINNT\system32\cmd.exe

D:\testcerts>type aparnaCA.cer
-----BEGIN CERTIFICATE-----
MIIC4jCCAoygAwIBAgIQBWDSiaY0GZRPSRI1jK0Ze.jANBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjb3Y5LjB20xCzAJBgNVBAYTAk10
MRIwEAYDUQIIEwLLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmddhbG9yZTEOMAwGA1UE
ChMFQ21zY28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD
QTAEFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIQMSAwHgYJKoZIhvcN
AQkBFHhFhbWFuZGt1QGNpc2NvLmNvbnRTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth
cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDUQKewVDAxNjBzETMBEG
A1UECxMKbmU0c3RvcnFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHZluNccNM87yppzwuoSNZXOMpeRXXI
OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAaOBuzCBuDALBgNUHQSE
BAMCAcYwDwYDUR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyJyRoMbrCNMRU20yRhQ
GgsWbHEwawYDUR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYSUyMENBLmNybdAwOC6gLIYqZmlsZTovL1xccc3N1LTA4XENlcuRFbnJv
bGxcQXBhcm5hJT1wQ0EuY3JsMBAGCSsGAQQBgjcUAQQAgaEAMAGCSqGSIb3DQEB
BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJagNgLh0AFcT0rEyuyt/WYGPzksF9Ea
NBG7E0oN66zex0EOEfG1Us6mXp1//w==
-----END CERTIFICATE-----

D:\testcerts>
  
```

## アイデンティティ証明書の要求

PKCS#12 証明書署名要求（CSR）を使用して Microsoft Certificate サーバにアイデンティティ証明書を要求するには、次の手順に従ってください。

## Procedure

- ステップ 1** Microsoft Certificate Services の Web インターフェイスから、**[証明書の要求 (Request a certificate)]** をクリックし、**[次へ (Next)]** をクリックします。

Microsoft Certificate Services -- Aparna CA

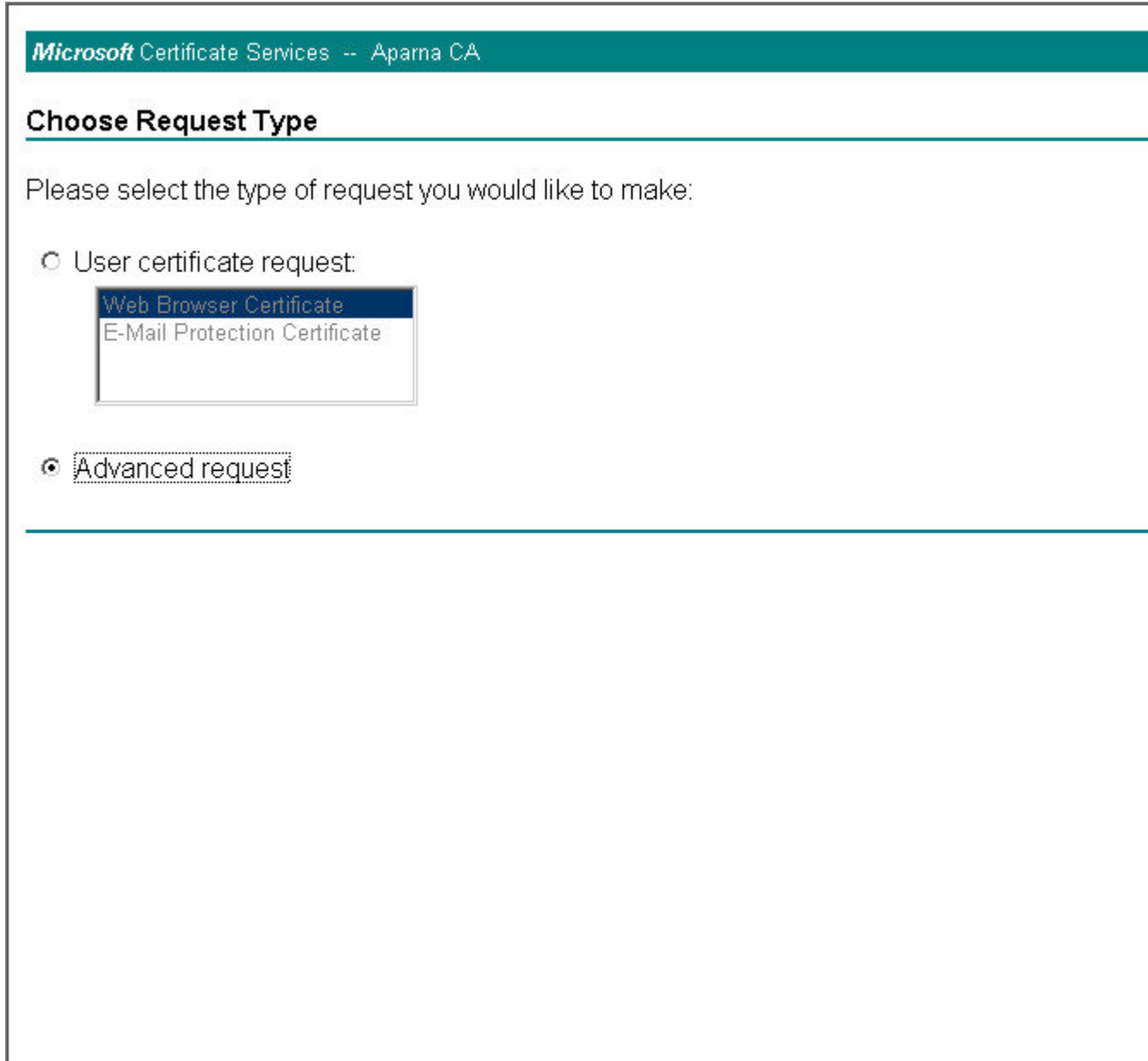
### Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure product. You will be able to securely identify yourself to other people over the web, sign your e-mail messages, and so on, depending upon the type of certificate you request.

#### Select a task:

- ☐ Retrieve the CA certificate or certificate revocation list
- ☒ Request a certificate
- ☐ Check on a pending certificate

ステップ 2 [詳細な要求 (Advanced request)] をクリックし、[次へ (Next)] をクリックします。



Microsoft Certificate Services -- Aparna CA

### Choose Request Type

Please select the type of request you would like to make:

☐ User certificate request:

- Web Browser Certificate
- E-Mail Protection Certificate

☒ Advanced request

ステップ 3 [Base64 エンコード済み PKCS#10 を使用する証明書要求または base64 エンコード済み PKCS#7 ファイルを使用する更新要求を送信する (Submit a certificate request using a base64 encoded PKCS#10 file or a

renewal request using a base64 encoded PKCS#7 file) ] をクリックし、[次へ (Next) ] をクリックします。

Microsoft Certificate Services -- Aparna CA

### Advanced Certificate Requests

You can request a certificate for yourself, another user, or a computer using one of the following methods. The certification authority (CA) will determine the certificates that you can obtain.

- ☐ Submit a certificate request to this CA using a form.
- ☒ Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.
- ☐ Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Wizard.  
*You must have an enrollment agent certificate to submit a request for another user.*

**ステップ 4** [保存済みの要求 (Saved Request) ] テキスト ボックスに、base64 の PKCS#10 証明書要求をペーストし、[次へ (Next) ] をクリックします。証明書要求が Cisco NX-OS デバイスのコンソールからコピーされま

す。

**Microsoft** Certificate Services -- Aparna CA

### Submit A Saved Request

Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generate server) into the request field to submit the request to the certification authority (CA).

#### Saved Request:

Base64 Encoded  
Certificate Request  
(PKCS #10 or #7):

```
VqyHOvEvAgMBAAAGTzAVBgkqhkiG9wOBCQcxCBMG  
DjEpMCcwJQYDVRORAQH/BBswGYIRVmVnYXMtMS5j  
KoZIhvcNAQEEBQADgYEAKT6OKER6Qo8nj0sDXZVH  
PftrNcWUE/pw6HayfQ12T3ecgNwel2d15133YBF2  
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPN  
-----END CERTIFICATE REQUEST-----
```

[Browse](#) for a file to insert.

#### Additional Attributes:

Attributes:

ステップ 5 CA アドミニストレータから証明書が発行されるまで、1 ～ 2 日間待ちます。

Microsoft Certificate Services -- Aparna CA

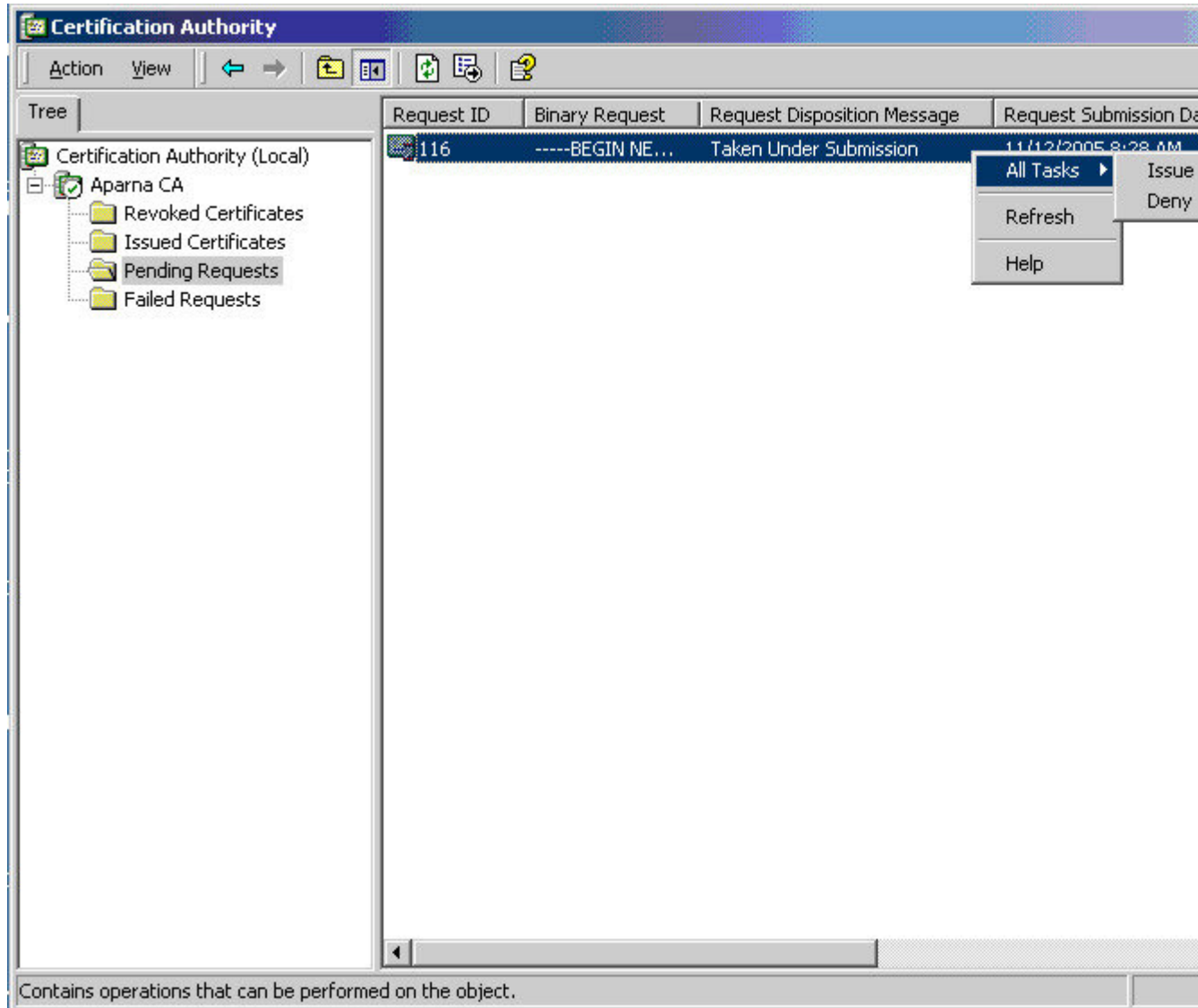
### Certificate Pending

Your certificate request has been received. However, you must wait for an administrator to issue the certificate.  
Please return to this web site in a day or two to retrieve your certificate.

**Note:** You must return with **this** web browser within 10 days to retrieve your certificate



**ステップ 6** CA アドミニストレータが証明書要求を承認するのを確認します。



**ステップ 7** Microsoft Certificate Services の Web インターフェイスから、[保留中の証明書をチェックする (Check on a pending certificate)] をクリックし、[次へ (Next)] をクリックします。

Microsoft Certificate Services -- Aparna CA

## Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure product. You will be able to securely identify yourself to other people over the web, sign your e-mail messages, and encrypt data, depending upon the type of certificate you request.

### Select a task:

- ☐ Retrieve the CA certificate or certificate revocation list
- ☐ Request a certificate
- ☒ Check on a pending certificate

**ステップ 8** チェックする証明書要求を選択して、[次へ (Next)] をクリックします。

Microsoft Certificate Services -- Aparna CA

### Check On A Pending Certificate Request

Please select the certificate request you want to check:

Saved-Request Certificate (12 November 2005 20:30:22)

ステップ 9 [Base 64 エンコード済み (Base 64 encoded)] をクリックして、[CA 証明書のダウンロード (Download CA certificate)] をクリックします。

Microsoft Certificate Services -- Aparna CA

### Certificate Issued

The certificate you requested was issued to you.

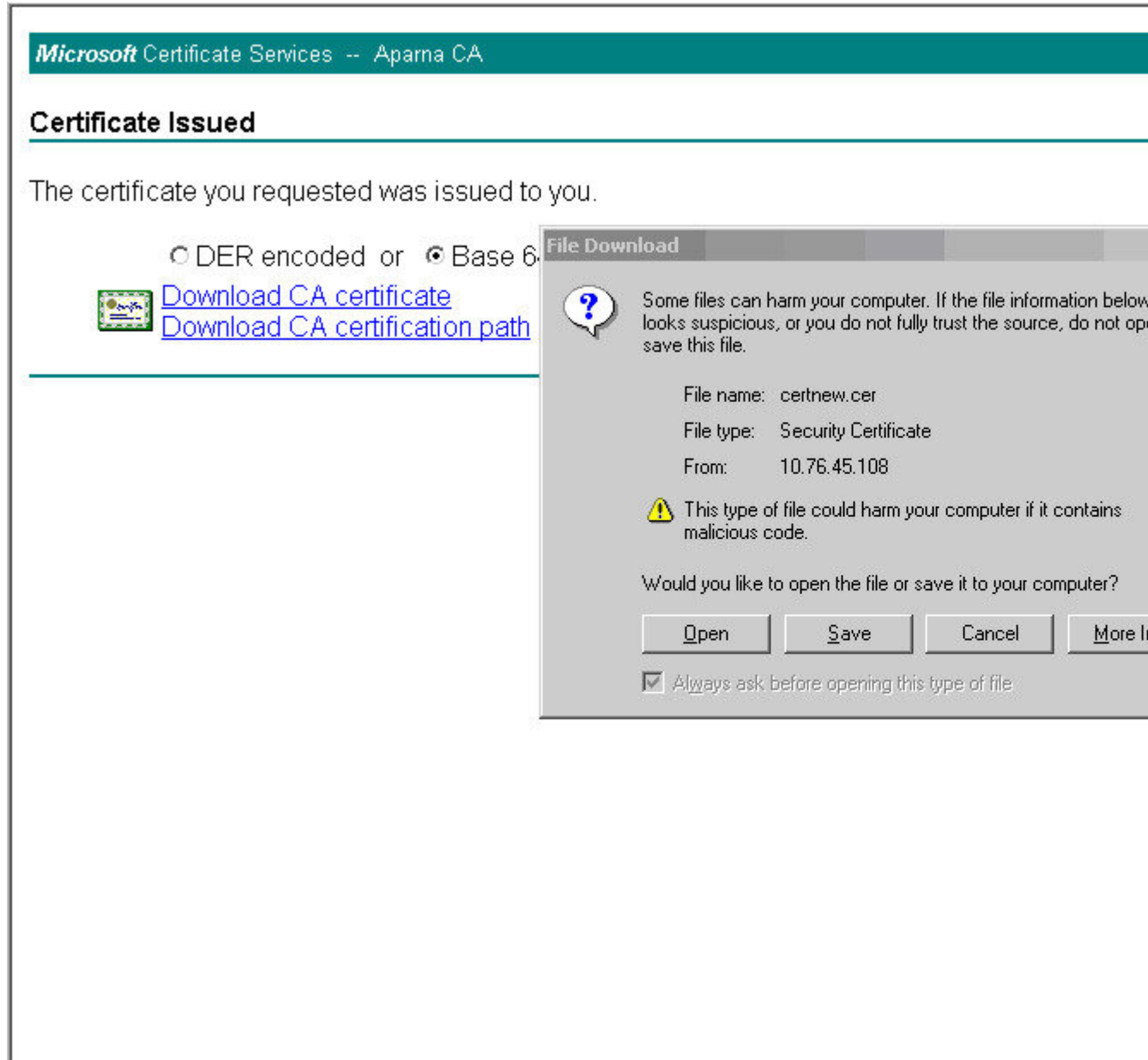
☐ DER encoded or ☒ Base 64 encoded



[Download CA certificate](#)

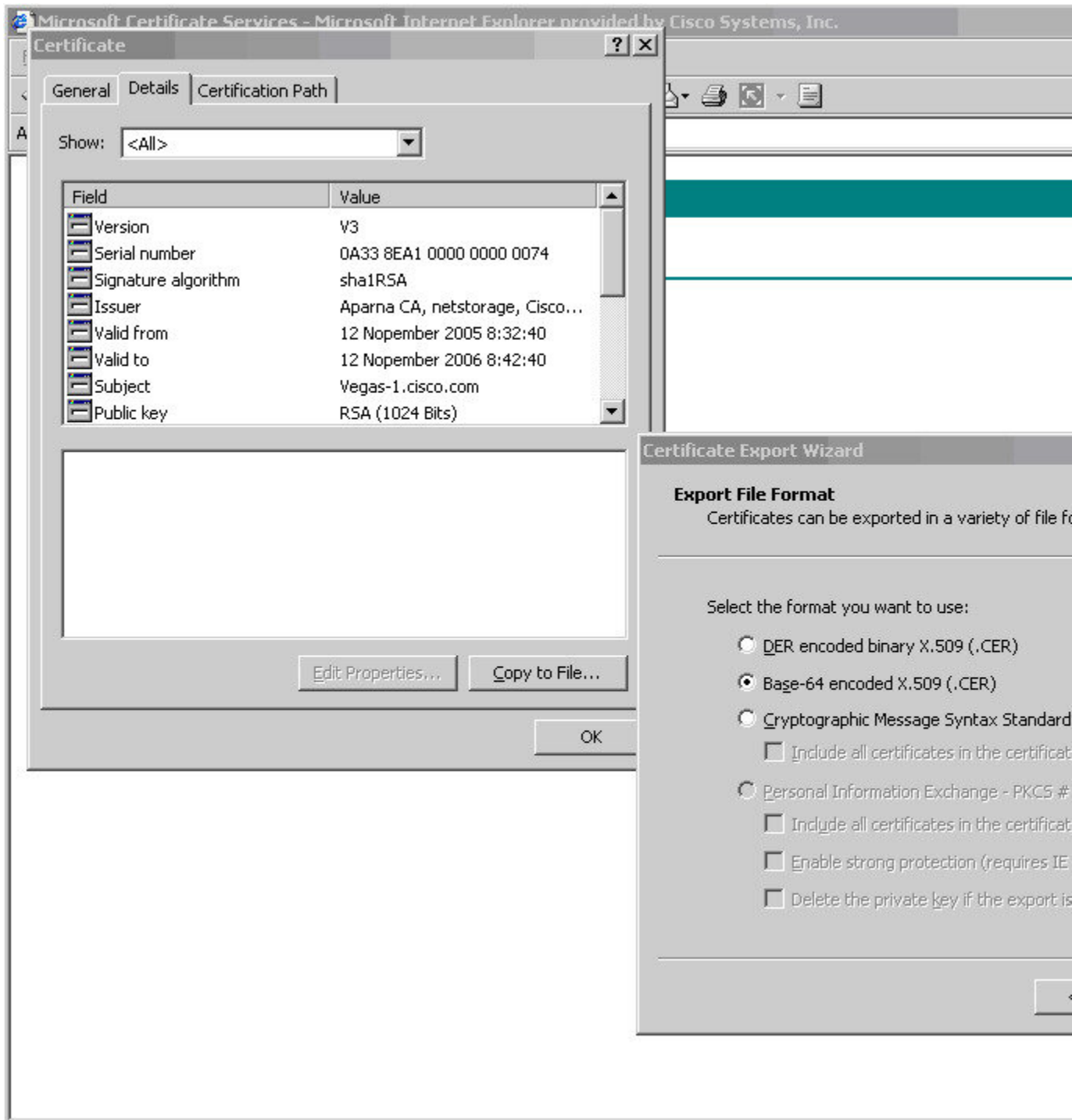
[Download CA certification path](#)

**ステップ 10** [ファイルのダウンロード (File Download) ] ダイアログ ボックスで、**[開く (Open) ]** をクリックします。

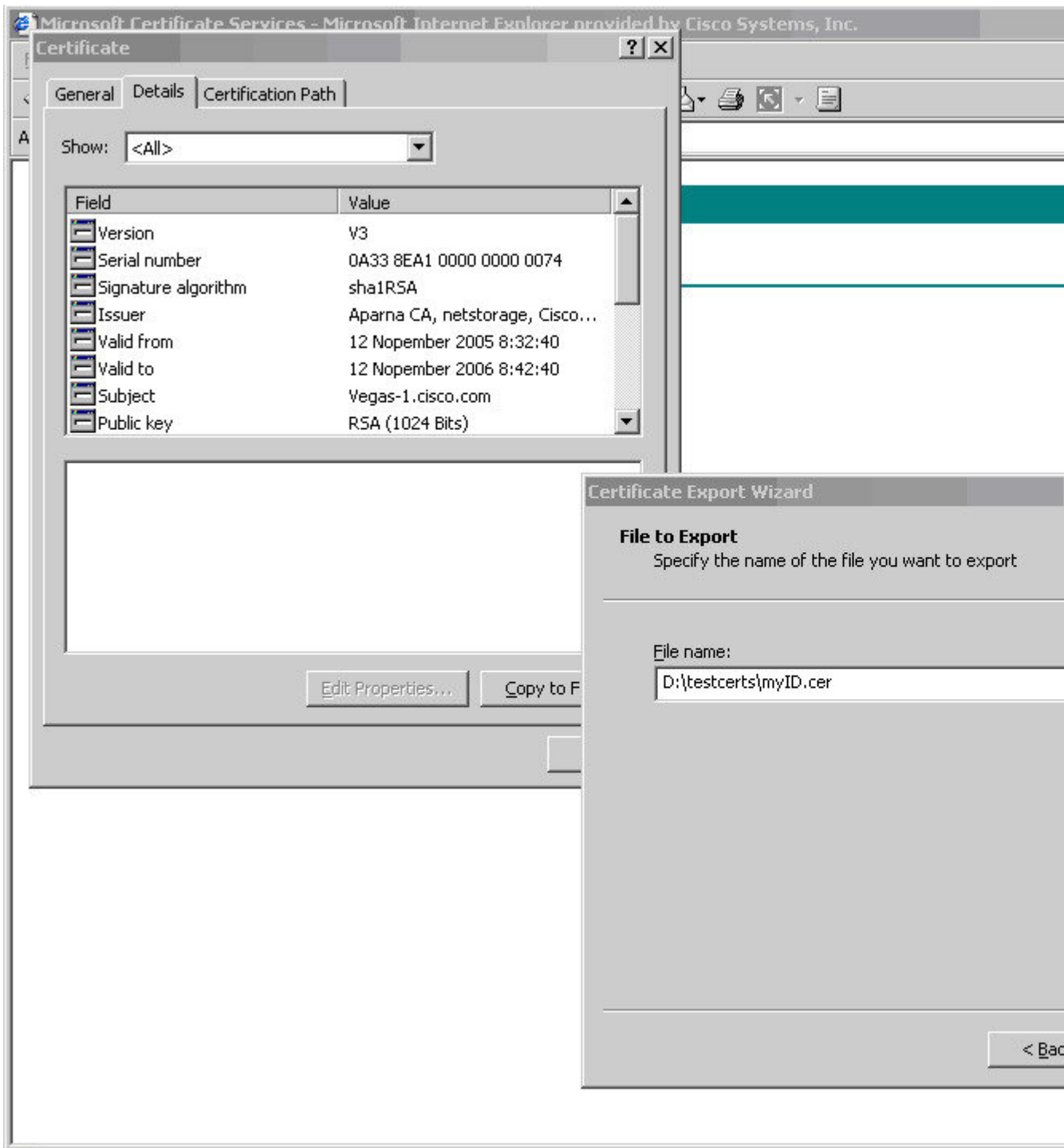


**ステップ 11** [Certificate] ボックスで、**[Details]** タブをクリックし、**[Copy to File...]** をクリックします。.[証明書のエクスポート ダイアログ (Certificate Export Dialog) ] ボックスで、**[Base-64 エンコード済み X.509 (.CER)]**

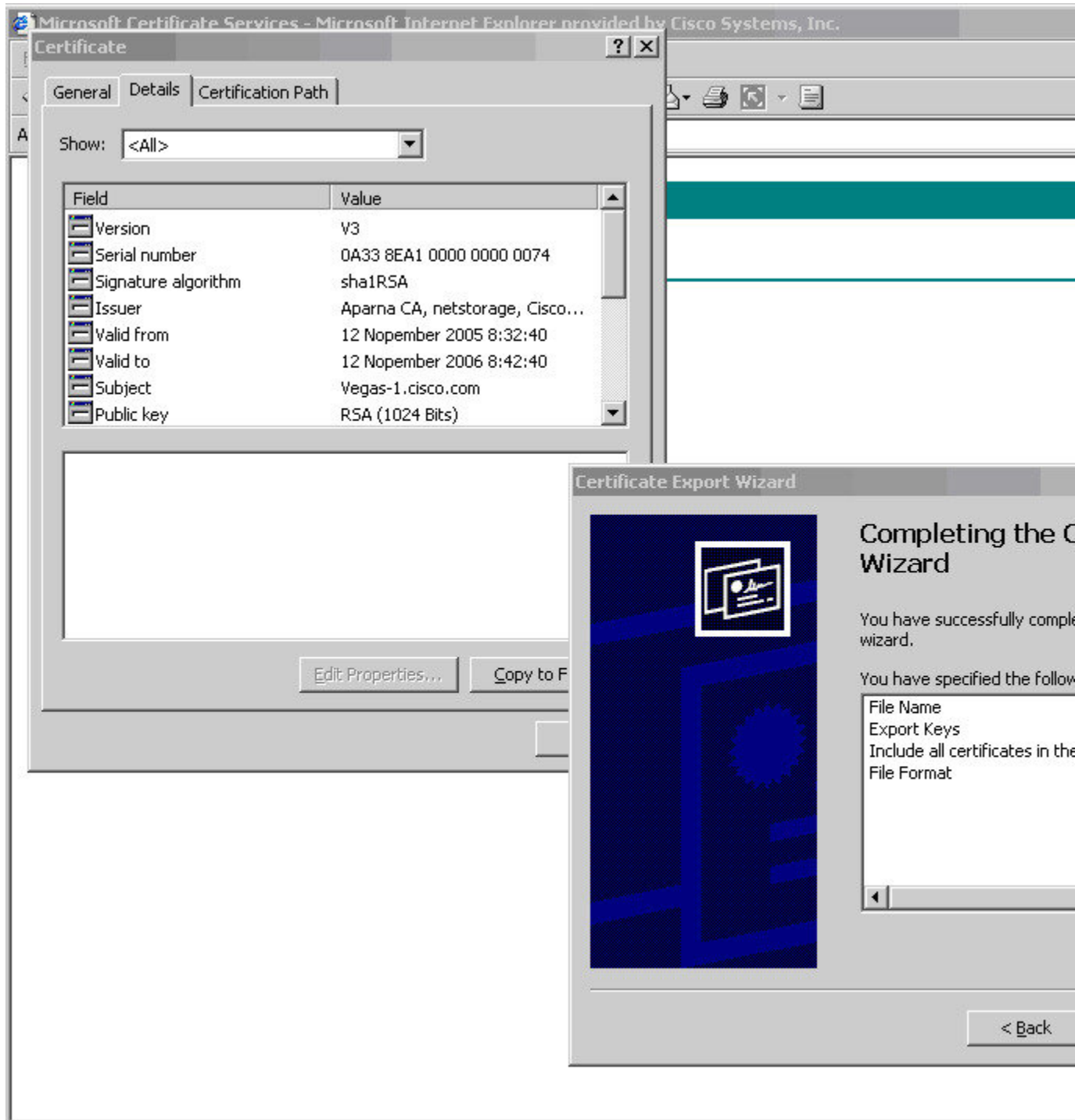
(**Base-64 encoded X.509 (.CER)**) ] をクリックし、[次へ (Next) ] をクリックします。



**ステップ 12** [証明書エクスポート ウィザード (Certificate Export Wizard)] ダイアログボックスにある [ファイル名 : (File name:)] テキストボックスに保存するファイル名を入力し、[次へ (Next)] をクリックします。



ステップ 13 [完了 (Finish)] をクリックします。





**ステップ 14** Microsoft Windows の **type** コマンドを入力して、アイデンティティ証明書を Base-64 でエンコードされた形式で表示します。

```

C:\WINNT\system32\cmd.exe

D:\testcerts>type myID.cer
-----BEGIN CERTIFICATE-----
MIIEADCCA6ggAwIBAgIKCj00oQAAAAAADANBgkqhkiG9w0BAQUFADCBIkDEgMB4G
CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjb3Y5b20xOzA5BjBNUBAVTak10MRIwEAyD
UQQIEwILYXJuYXRha2ExEjAQBGNUBAcICUJhbmdbG9yZTEOMAwGA1UEChMFQ21z
Y28xEzARBGNUBAsTCm5ldHN0b3JhZ2UxEjAQBGNUBAMTCUFWYXJuYXNBDQTAeFw0w
NTExMTIwMzA5NDBaFw0wNTExMTIwMzE5NDBaMBwxGjAYBgNUBAMTEUZZ1Z2FzLTEx
Y21zY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNUACdJQu41C
dQ1WkjkjSICdpLfK5eJSmNCQujGpzcukS ZPFxjF2Uo iyeCYE8y1ncWvw5E08rJ47
g1xr42/sI9IRIh/8udU/cj9jSSfKK56koa7x4WYAu8rDfz8jMCnIM4W1aY/q2g4Gb
x7RifdU06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDUR0RAQH/BBsw
GYIRUmUnYXMcMS5jaXNjb3Y5b22HBKwWH6IwHQYDUR0OBBYEFKCLi+2ssplWEfgrR
bhWm1Uyo9jngMIHMBGhNUHSMegcQwgcGAFCCo8kaDG6wjTEUNjskYUBoLFmxxoYGW
pIGTMIQMSAwHgYJKoZlIhvcNAQkBFhFhbWZGt1QGNpc2NoLmNoTELMAkGA1UE
BhMCSU4xEjAQBGNUBAcICUthcm5hdGFyYTESMBAGA1UEBxMJQmFuZ2FzY21zY28u
DAYDUQQKEwUDaXNjb3Y5b22HBKwWH6IwHQYDUR0OBBYEFKCLi+2ssplWEfgrR
cm5hIENBgghAFYNNKJrLQZ1E9JEiWMrR16MGsGA1UdHwRkMG1wLqAssoCqGKGh0dHA6
Ly9zc2U0tMDgvQ2UydeUucm9sbC9BcGFybmELMjBDQS5jcmwwMKAuoCyGKwZpbGU6
Ly9zc2U0tMDgvQ2UydeUucm9sbC9BcGFybmELMjBDQS5jcmwwMKAuoCyGKwZpbGU6
AQEEFjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3N1LTA4L0N1cnRFbnJvbGwvc3N1
LT A4X0FwYXJuYXNBMENBLmNydDA9BggrBgEFBQcwAoYxZm1sZTovL1xc3N1LT A4
XEN1cnRFbnJvbGwvc3N1LT A4X0FwYXJuYXNBMENBLmNydDANBgkqhkiG9w0BAQUF
AANBAdBGBGbsbe7GNLh9xe0TWBNbm24U69ZSuDDc0cUzUUTgrpnTqUpPyejtsyf1w
E36cIZu4WsExREqxbTk8ycx7U5o=
-----END CERTIFICATE-----

D:\testcerts>

```

### Related Topics

[証明書要求の作成](#) (149 ページ)

[Cisco NX-OS デバイスでの証明書の設定](#) (160 ページ)

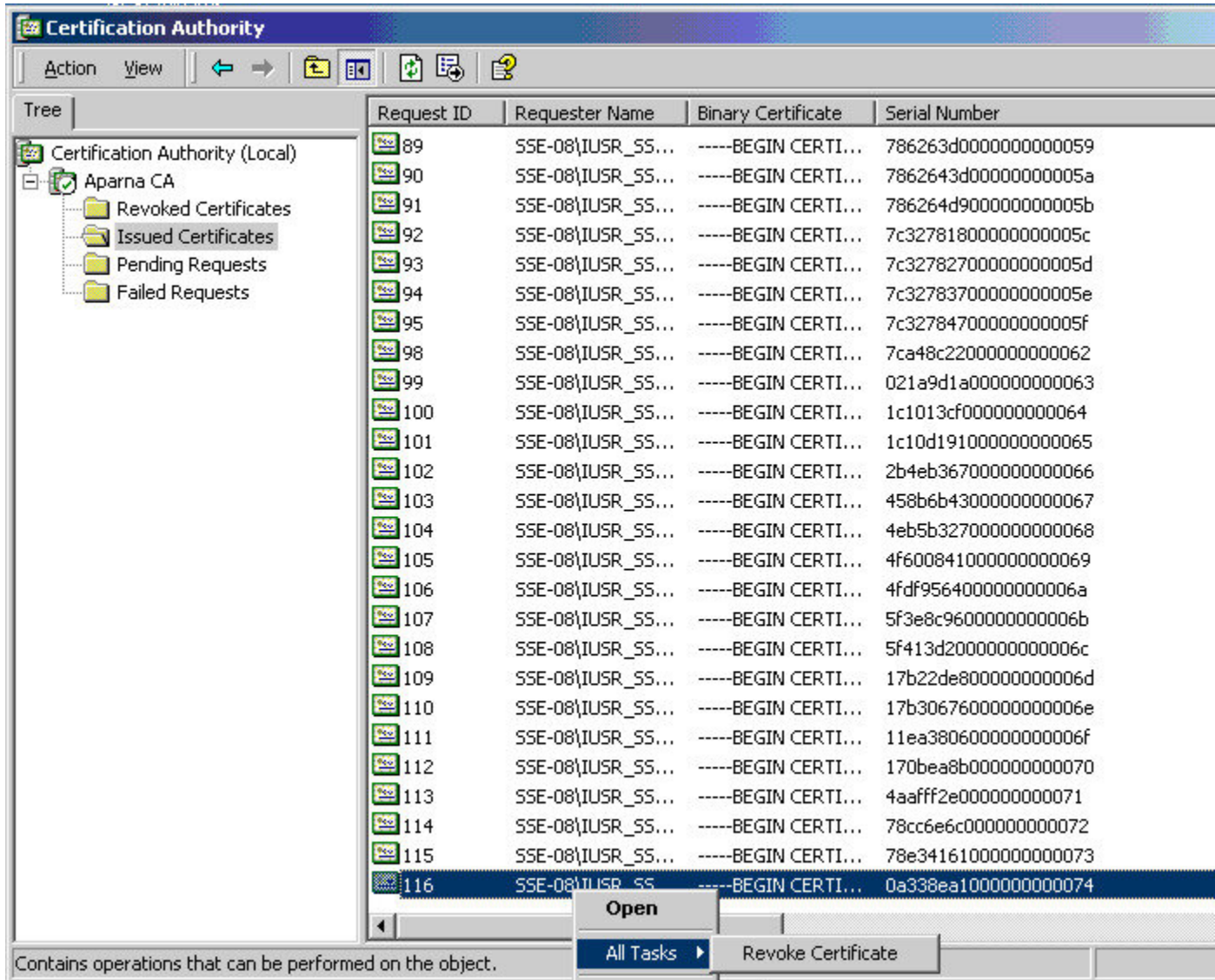
## 証明書の取り消し

Microsoft CA 管理者プログラムを使用して証明書を取り消す手順は、次のとおりです。

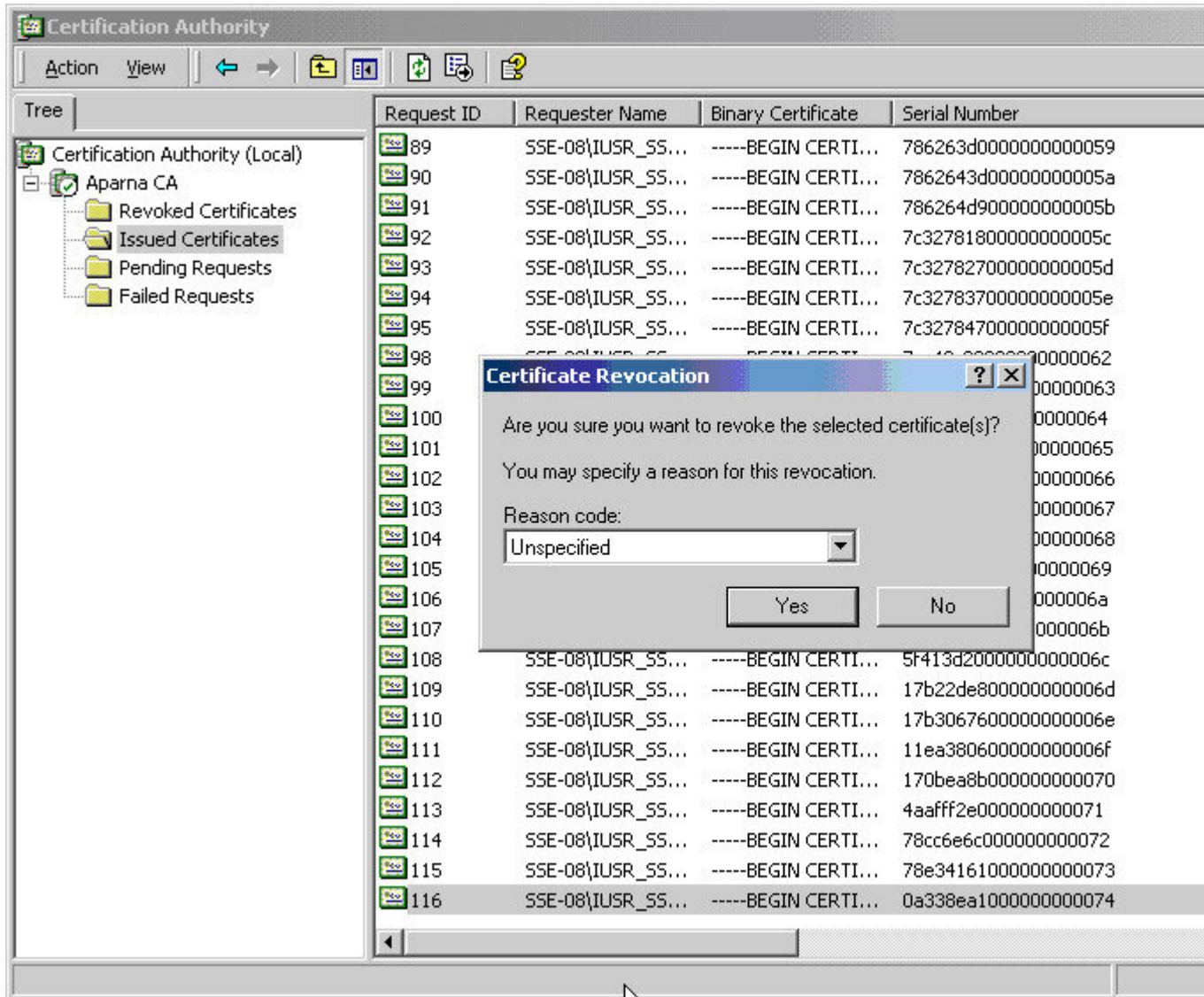
### Procedure

**ステップ 1** [Certification Authority] ツリーから、[Issued Certificates] フォルダをクリックします。リストから、取り消す証明書を右クリックします。

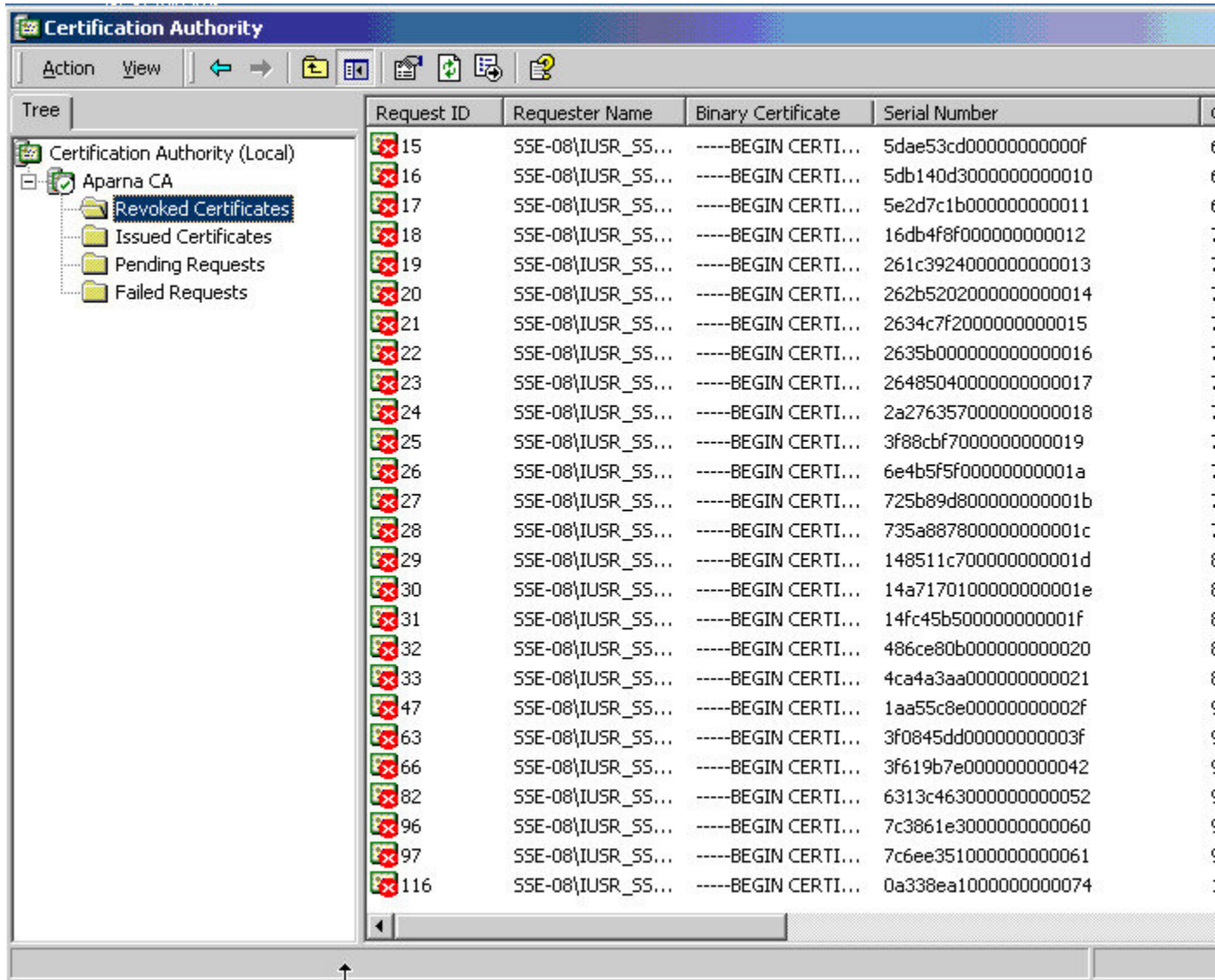
ステップ 2 [All Tasks] > [Revoke Certificate] の順に選択します。



ステップ3 [Reason code] ドロップダウン リストから取り消しの理由を選択し、[Yes] をクリックします。



ステップ 4 [Revoked Certificates] フォルダをクリックして、証明書の取り消しを表示および確認します。



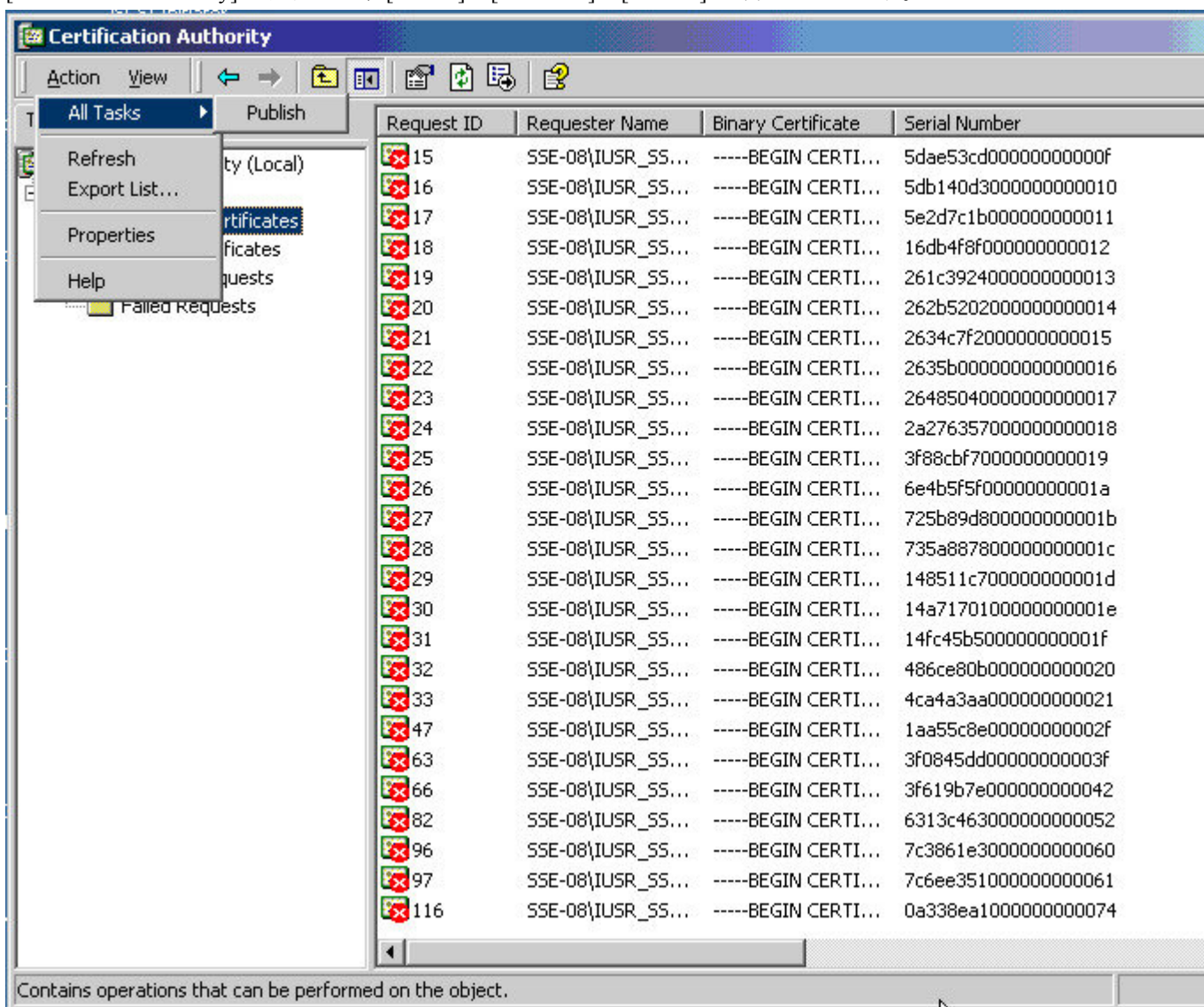
## CRL の作成と公開

Microsoft CA 管理者プログラムを使用して CRL を作成および公開する手順は、次のとおりです。

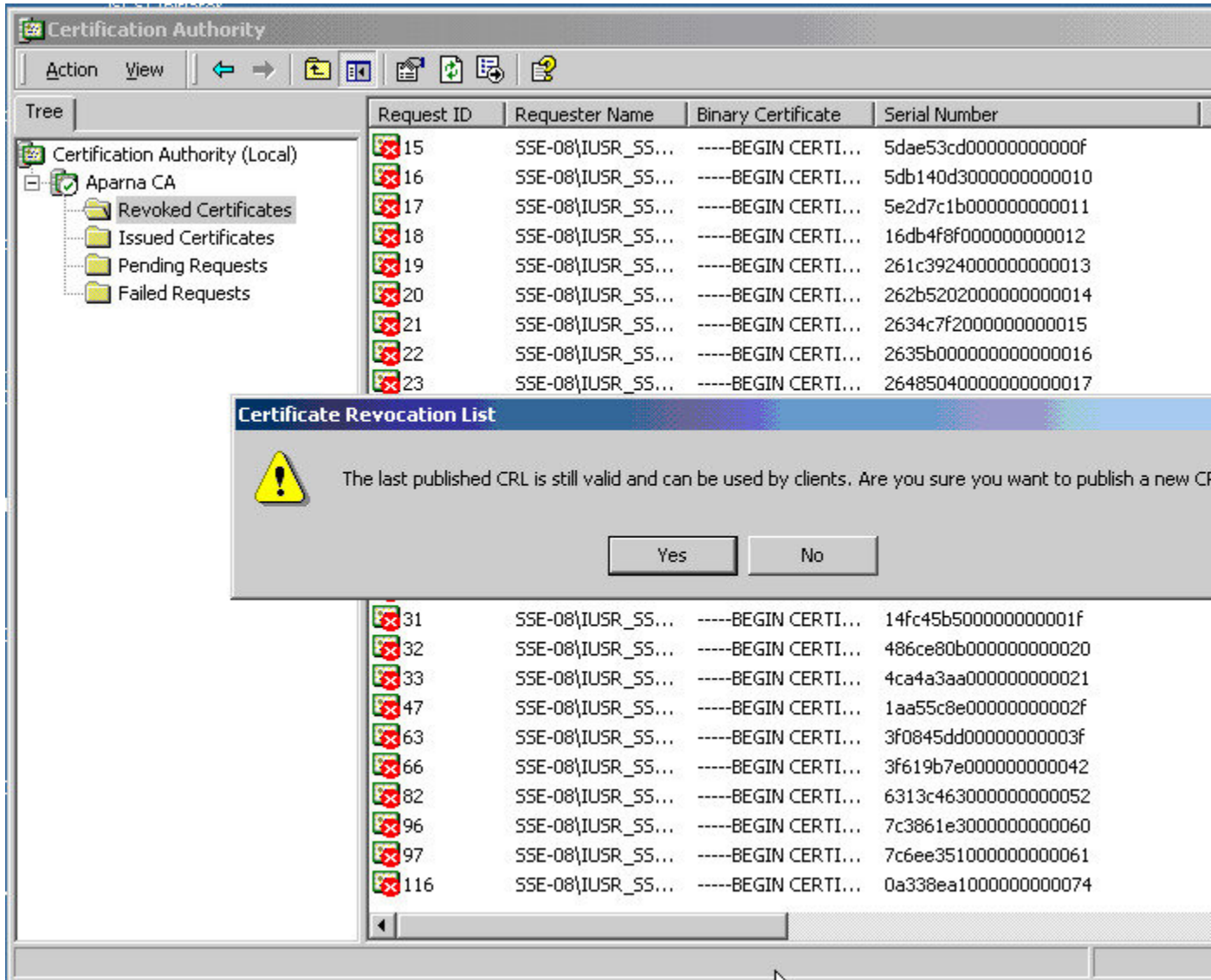


## Procedure

ステップ 1 [Certification Authority] の画面から、[Action] > [All Tasks] > [Publish] の順に選択します。



ステップ 2 [Certificate Revocation List] ダイアログボックスで、[Yes] をクリックして最新の CRL を公開します。



## CRL のダウンロード

Microsoft 社の CA の Web サイトから CRL をダウンロードする手順は、次のとおりです。

## Procedure

- ステップ 1** Microsoft Certificate Services の Web インターフェイスから、[Retrieve the CA certificate or certificate revocation list] をクリックし、[Next] をクリックします。

*Microsoft* Certificate Services -- Aparna CA

### Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure p... will be able to securely identify yourself to other people over the web, sign your e-mail messages, depending upon the type of certificate you request.

#### Select a task:

- ☒ Retrieve the CA certificate or certificate revocation list
- ☐ Request a certificate
- ☐ Check on a pending certificate

ステップ 2 [Download latest certificate revocation list] をクリックします。

Microsoft Certificate Services -- Apama CA

### Retrieve The CA Certificate Or Certificate Revocation List

[Install this CA certification path](#) to allow your computer to trust certificates issued from this certification

It is not necessary to manually install the CA certification path if you request and install a certificate from this CA. The CA certification path will be installed for you automatically.

#### Choose file to download:

CA Certificate: 

☐ DER encoded or ☒ Base 64 encoded

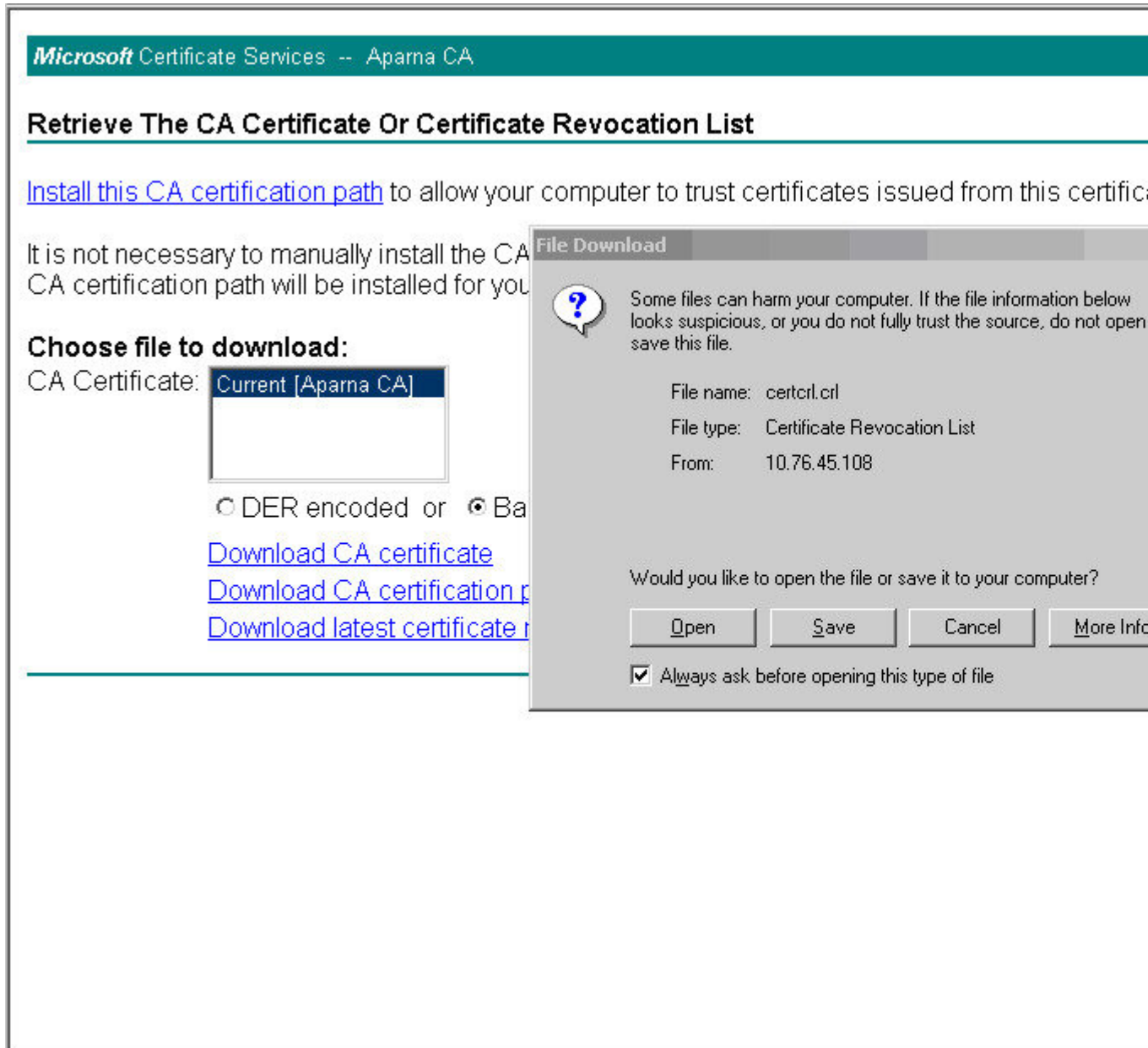
[Download CA certificate](#)

[Download CA certification path](#)

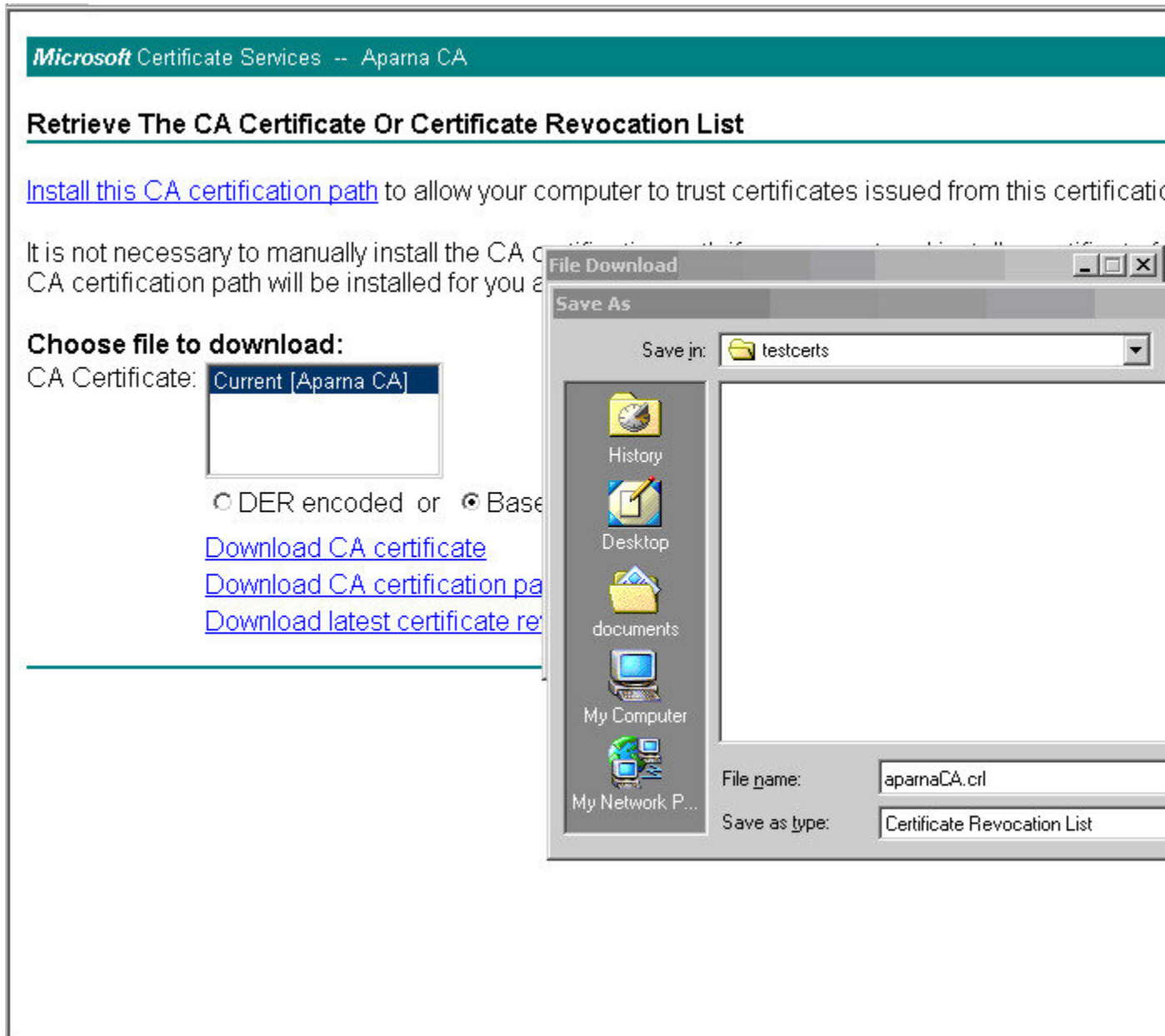
[Download latest certificate revocation list](#)



ステップ 3 [File Download] ダイアログボックスで、[Save] をクリックします。



ステップ 4 [Save As] ダイアログボックスで、保存するファイル名を入力して、[Save] をクリックします。



```
C:\WINNT\system32\cmd.exe

D:\testcerts>type aparnaCA.crl
-----BEGIN X509 CRL-----
MIIGBTCCBa8CAQEWdQYJKoZIHvcNAQEFBQAawgZAxiDAeBgkqhkiG9w0BCQEWEMFt
YW5ka2VAY2ZlY28uY29tMQswCQYDUQGEWJITjESMBAGA1UECBMJS2FybhmF0YUWt
hMRIWEAYDUQGEWJICWY5NlYwXucmUxdDjAMBGNuBA0TBUNpc2NoMRMwEQYDUQGLEWpu
ZXRzdG9yYWdlMlMRIWEAYDUQGEWlBcGFybHEgQ0EXDTA1MTExMjA0MzYwNFoXDTA1
MTExOTE2NTYwNFowggSxMBsCCmEbCaEAAAAAAAAAIXDTA1MDgxNjI1xNTI1xOUowGwIK
TN5GTgAAAAAAAAxcNMDUwODE2MjE1MjI5WjAbaGppM/CtCAAAAAAAAAEFw0wNTA4MTYy
MTUyNDFuMBsCCmXpnsIAAAAAAAAAUXDTA1MDgxNjI1xNTI1MlowGwIKbM993AAAAAAB
ghcNMDFAmJAB4MDAxMjA0WjAbaGppwzE//AAAAAAAAAHFw0wNTA4MTYyMTUzMTUaMBsC
Ck2bERYAAAAAAAAAGXDTA1MDgxNjI1xNTMxNUowKQIKUggCAAAAAAAAAACRcNMDUwNjI3
MjM0NzA2WjAMMAoGA1UdFQQDCgECMCkCC1NjUyYAAAAAAAAA0XDTA1MDYyNzIzNDcy
MlowDDAKBgNVHRIEYw0BAjAbaGppTvrC8AAAAAAAAALFw0wNTA3MDQxODAwMDFAmAw
CgYDUR0UBAMKAQEWGwIkwR56zgAAAAAAAAADBCNMDUwODE2MjE1MzE1WjAbaGppDP9Uu
AAAAAAAAANFw0wNTA2MjkyMjA3MjUaMAwwCgYDUR0UBAMKAQEWGwIKXat3EwAAAAAA
DhcNMDUwNzE0MDAzMzU2WjAbaGppdr1PNAAAAAAAAAPFw0wNTA4MTYyMTUzMTUaMBsC
Cl2xQNMAAAAAAAAAAXDTA1MDgxNjI1xNTMxNUowKQIKXi18GwAAAAAAERcNMDUwNzA2
MjExMjEwWjAMMAoGA1UdFQQDCgEFMBsCCHbBT48AAAAAAAAABIXDTA1MDgxNjI1xNTMx
NUowGwIKJhw5JAAAAAAAAAExcNMDUwODE2MjE1MzE1WjAbaGomK1ICAAAAAAAAUFw0w
NTA3MTQwMDMzMjBAMBsCCiY0x/IAAAAAABUXDTA1MDcxNDcxNDcxNDcxNDcxNDcxNDcx
AAAAAAAAAFhcNMDUwNzE0MDAzMTUxWjAbaGomSFBAAAAAAAAAXFw0wNTA3MTQwMDMy
MjUaMBsCCionY1cAAAAAABGxDTA1MDgxNjI1xNTMxNUowGwIKP4jL9wAAAAAAGRcN
MDUwODE2MjE1MzE1WjAbaGppuS19fAAAAAAAAAFw0wNTA4MTYyMTUzMTUaMBsCCnJb
idgAAAAAAAAABsXDTA1MDgxNjI1xNTMxNUowGwIKc1qIeAAAAAAAAAHBCNMDUwODE2MjE1
MzE1WjAbaGouUhrHHAUAAAAAADFw0wNTA4MTYyMTUzMTUaMBsCCHsnFwEAAAAAAB4X
DTA1MDgxNjI1xNTMxNUowGwIKFPxFTqAAAAAABHxcNMDUwODE3MTgzMDYwJABaGppI
b0gLAaaaaaaAgFw0wNTA4MTcxODMwNDNaMBsCCkyko6oAAAAAAGEXDTA1MDgxNzE4
MzA0M1owGwIKGgUcJgAAAAAALxcNMDUwOTA1MTcwNzA2WjAbaGo/CEXdaAAAAAAB/
Fw0wNTA5MDgyMDI0MzJAMBsCCj9hm34AAAAAAEIXDTA1MDkwODIxNDAB0FowGwIK
YxPEYwAAAAAAUHCNMDUwOTE5MTczNzE4WjAbaGpp8OGHjAAAAAABGfW0wNTA5MjA5
NzUyNTZAMBsCCnxu41EAAAAAAGEXDTA1MDkyMDE4NTIzMfowGwIKCj00oQAAAAAA
dBcNMDUxMTeyMDQzNDQyWqA1MDMwHwYDUR0jBBgwFoAUJyJyRoMbrCNMRU2OyRhQ
GgsWbhEwEAYJKwYBBAQGNxUBBAMCAQAwDQYJKoZIHvcNAQEFBQAADQALy91DCrhi
HoCUBm9NqWzYjJjEjgeU168CuaacFP3rkM8YyZYpu1c32R/UvU6aSxgrAC/SbsEa
nxpJt5xYJNdy
-----END X509 CRL-----

D:\testcerts>
```

[証明書取消確認方法の設定](#) (148 ページ)

CRL を CA に対応するトラストポイントにインポートする手順は、次のとおりです。

**ステップ1** CRL ファイルを Cisco NX-OS デバイスのブートフラッシュにコピーします。

```
Device-1# copy tftp:aparnaCA.crl bootflash:aparnaCA.crl
```

## ステップ 2 CRL を設定します。

```
Device-1# configure terminal
Device-1(config)# crypto ca crl request myCA bootflash:aparnaCA.crl
Device-1(config)#
```

## ステップ 3 CRL の内容を表示します。

```
Device-1(config)# show crypto ca crl myCA
Trustpoint: myCA
CRL:
Certificate Revocation List (CRL):
  Version 2 (0x1)
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: /emailAddress=admin@yourcompany.com/C=IN/ST=Karnatak
Yourcompany/OU=netstorage/CN=Aparna CA
  Last Update: Nov 12 04:36:04 2005 GMT
  Next Update: Nov 19 16:56:04 2005 GMT
  CRL extensions:
    X509v3 Authority Key Identifier:
      keyid:27:28:F2:46:83:1B:AC:23:4C:45:4D:8E:C9:18:50:1
      1.3.6.1.4.1.311.21.1:
        ...
Revoked Certificates:
  Serial Number: 611B09A100000000000002
    Revocation Date: Aug 16 21:52:19 2005 GMT
  Serial Number: 4CDE464E00000000000003
    Revocation Date: Aug 16 21:52:29 2005 GMT
  Serial Number: 4CFC2B4200000000000004
    Revocation Date: Aug 16 21:52:41 2005 GMT
  Serial Number: 6C699EC200000000000005
    Revocation Date: Aug 16 21:52:52 2005 GMT
  Serial Number: 6CCF7DDC00000000000006
    Revocation Date: Jun 8 00:12:04 2005 GMT
  Serial Number: 70CC4FFF00000000000007
    Revocation Date: Aug 16 21:53:15 2005 GMT
  Serial Number: 4D9B111600000000000008
    Revocation Date: Aug 16 21:53:15 2005 GMT
  Serial Number: 52A8023000000000000009
    Revocation Date: Jun 27 23:47:06 2005 GMT
  CRL entry extensions:
    X509v3 CRL Reason Code:
      CA Compromise
  Serial Number: 5349AD460000000000000A
    Revocation Date: Jun 27 23:47:22 2005 GMT
  CRL entry extensions:
    X509v3 CRL Reason Code:
      CA Compromise
  Serial Number: 53BD173C0000000000000B
    Revocation Date: Jul 4 18:04:01 2005 GMT
  CRL entry extensions:
    X509v3 CRL Reason Code:
      Certificate Hold
  Serial Number: 591E7ACE0000000000000C
    Revocation Date: Aug 16 21:53:15 2005 GMT
  Serial Number: 5D3FD52E0000000000000D
    Revocation Date: Jun 29 22:07:25 2005 GMT
  CRL entry extensions:
    X509v3 CRL Reason Code:
      Key Compromise
  Serial Number: 5DAB77130000000000000E
```

```

    Revocation Date: Jul 14 00:33:56 2005 GMT
Serial Number: 5DAE53CD00000000000F
    Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 5DB140D30000000000010
    Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 5E2D7C1B0000000000011
    Revocation Date: Jul  6 21:12:10 2005 GMT
CRL entry extensions:
    X509v3 CRL Reason Code:
        Cessation Of Operation
Serial Number: 16DB4F8F0000000000012
    Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 261C39240000000000013
    Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 262B52020000000000014
    Revocation Date: Jul 14 00:33:10 2005 GMT
Serial Number: 2634C7F20000000000015
    Revocation Date: Jul 14 00:32:45 2005 GMT
Serial Number: 2635B0000000000000016
    Revocation Date: Jul 14 00:31:51 2005 GMT
Serial Number: 264850400000000000017
    Revocation Date: Jul 14 00:32:25 2005 GMT
Serial Number: 2A2763570000000000018
Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 3F88CBF70000000000019
    Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 6E4B5F5F000000000001A
    Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 725B89D8000000000001B
    Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 735A8878000000000001C
    Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 148511C7000000000001D
    Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 14A71701000000000001E
    Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 14FC45B5000000000001F
    Revocation Date: Aug 17 18:30:42 2005 GMT
Serial Number: 486CE80B0000000000020
    Revocation Date: Aug 17 18:30:43 2005 GMT
Serial Number: 4CA4A3AA0000000000021
    Revocation Date: Aug 17 18:30:43 2005 GMT
Serial Number: 1AA55C8E000000000002F
    Revocation Date: Sep  5 17:07:06 2005 GMT
Serial Number: 3F0845DD000000000003F
    Revocation Date: Sep  8 20:24:32 2005 GMT
Serial Number: 3F619B7E0000000000042
    Revocation Date: Sep  8 21:40:48 2005 GMT
Serial Number: 6313C4630000000000052
    Revocation Date: Sep 19 17:37:18 2005 GMT
Serial Number: 7C3861E30000000000060
    Revocation Date: Sep 20 17:52:56 2005 GMT
Serial Number: 7C6EE3510000000000061
    Revocation Date: Sep 20 18:52:30 2005 GMT
Serial Number: 0A338EA10000000000074  <-- Revoked identity certificate
    Revocation Date: Nov 12 04:34:42 2005 GMT
Signature Algorithm: sha1WithRSAEncryption
0b:cb:dd:43:0a:b8:62:1e:80:95:06:6f:4d:ab:0c:d8:8e:32:
44:8e:a7:94:97:af:02:b9:a6:9c:14:fd:eb:90:cf:18:c9:96:
29:bb:57:37:d9:1f:d5:bd:4e:9a:4b:18:2b:00:2f:d2:6e:c1:
1a:9f:1a:49:b7:9c:58:24:d7:72

```

**Note**

取り消されたデバイスのアイデンティティ証明書（シリアル番号は 0A338EA10000000000074）が最後に表示されています。

## Resource Public Key Infrastructure (RPKI)

RPKI は、BGP（インターネット）プレフィックスを認証済みの送信元 AS 番号にマッピングする情報を含む、グローバルに配布されたデータベースです。BGP パスの送信元 AS を検証するために、BGP を実行しているルータは、RPKI に接続できます。

RPKI-Cache-to-Router 接続は多対多にすることができ、1 つの RPKI キャッシュは複数のルーターに origin-AS 検証データを提供でき、1 つのルーターは複数の RPKI キャッシュに接続できます。ルーターは RPKI キャッシュに接続して情報をダウンロードし、BGP がインターネットルーティングテーブルの発信元 AS 番号を検証するために使用できる特別な RPKI データベースを構築します。

RPKI データベースは、BGP が接続するさまざまな RPKI キャッシュから集約された Route-Origin-Attestation (ROA) オブジェクトのセットです。ROA オブジェクトは、BGP プレフィックスブロックと、そのブロックの発信を許可された AS 番号との間のマッピングを提供します。

## RPKI 構成

RPKI 構成は次のように分類されます。

- RPKI キャッシュに接続するためのコマンド。
- 受信プレフィックスに RPKI 検証状態をマークするためのコマンド。
- BGP ベストパス計算で RPKI 検証状態を使用するためのコマンド。
- route-map を使用して特定の検証状態を持つプレフィックスを削除または操作するためのコマンド。

## RPKI キャッシュに接続するためのコマンド

RPKI キャッシュ構成は、router-bgp サブモードの新しい rpki-cache サブモードで行います。これは、デフォルトの VRF での BGP ピアの構成に似ています。サブモードに入るには、「rpki cache <IP address>」コマンドを使用します。サブモードに入ると、RPKI キャッシュのさまざまなパラメータを構成できます。

```
router bgp 100
  rpki cache 147.28.0.11
    description      A description to identify the cache
    shutdown          Shutdown the cache
    transport tcp port Transport port on which cache is listening
```

|                  |                                                                |
|------------------|----------------------------------------------------------------|
| vrf              | Vrf in which RPKI cache is reachable                           |
| refresh-interval | Specify periodic wait time between cache poll attempts         |
| retry-interval   | Specify wait time before retrying failed serial or reset query |
| expiry-interval  | Specify how long to use current data while unable to perform   |
| successful query |                                                                |



(注) トランスポート TCP ポートが明示的に構成されていない限り、BGP は RPKI-RTR ポート 323 で RPKI キャッシュへ接続します。

明示的に設定されていない限り、すべての間隔は、データ PDU の末尾の RPKI キャッシュによって提案されたとおりに決定されます。

## 受信プレフィックスを RPKI 検証状態でマークするためのコマンド

RPKI プレフィックス検証処理の動作を制御するためのノブがあります。これらのノブは、アドレス ファミリ レベルで構成できます。

- **origin-as validate** : アドレス ファミリ レベルで構成すると、ROA データベースに対する eBGP パス検証が有効になります。デフォルトでは無効になっています。



(注) このコマンドは、iBGP パスには関係ありません。iBGP パスは、ROA データベースに対して検証されません。iBGP パスでパス検証状態をマークする唯一の方法は、BGP プレフィックス発信元検証状態拡張コミュニティを受信することであり、コマンドを構成せずにデフォルトで実行されます。

- **origin-as validate signal ibgp** : アドレス ファミリ レベルで構成すると、BGP プレフィックス発信元検証状態拡張コミュニティを介した検証状態の iBGP シグナリングが有効になります。

## BGP 最適パス計算で RPKI 検証状態を使用するためのコマンド

RPKI プレフィックス検証処理の動作を制御するためのコマンドがあります。これらのコマンドは、アドレス ファミリ レベルで構成できます。

- **bestpath origin-as use-validity** : アドレス ファミリ レベルで構成することで、BGP ベストパス処理でのパスのプリファレンスに影響する BGP パスの有効性状態を有効にします。デフォルトでは無効になっています。
- **bestpath origin-as allow invalid** : アドレス ファミリ レベルで構成することで、すべての「無効な」パスが BGP 最適パス計算のために考慮されるようにします (best-path origin-as 検証が設定されている場合、そのようなパスはどれも最適パス候補ではありません)。デフォルトでは無効になっています。

## route-map を使用して特定の検証状態を持つプレフィックスを削除または操作するためのコマンド

以下は、ルートマップを使用して特定の検証状態を持つプレフィックスを削除または操作するためのコマンドです。

```
route-map sample1 permit 10
  match rpki {not-found | invalid | valid}
```

match rpki コマンドのパラメータは次のとおりです。

- not-found : この origin-AS は RPKI データベースでは不明です。
- invalid : RPKI データベース内の無効な origin-AS です。
- valid : RPKI データベース内の有効な origin-AS です。

この match 句は、インバウンドルートマップにのみ関連します。

iBGP で学習されたパスの場合、更新の入力 BGP プレフィックス発信元検証状態拡張コミュニティが、このルートマップ句と比較されます。

eBGP 学習パスの場合、ROA データベースルックアップによって取得された検証状態が、このルートマップ句と比較されます。

検証状態が無効であるとマークされたプレフィックスは、BGP での最適パスの計算に考慮されないため、無効になります。管理者は、システムメモリを節約するために、そのようなプレフィックスを完全に削除するように決定する場合があります。この目的には、次のインバウンドルートマップが推奨されます。

```
route-map sample deny 10
match rpki invalid
route-map sample permit 20
```

## RPKI Show コマンド

RPKI 構成情報を表示するには、次のいずれかのタスクを行います。

| コマンド                         | 目的                                  |
|------------------------------|-------------------------------------|
| <b>show bgp rpki summary</b> | RPKI キャッシュの数を含む RPKI 統計情報の概要を表示します。 |



| コマンド                                                                                               | 目的                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>show bgp rpki table {ipv4   ipv6} {IP address/masklength}</b>                                   | <p>現在の RPKI ROA データベースに関する情報を表示します。オプションを指定しなかった場合、コマンドは IPv4 ROA データベースを表示します。IPv6 オプション (show bgp rpki table ipv6) を指定すると、このコマンドは IPv6 ROA データベースを表示します。(接続の問題などにより) 一時的にダウンしているキャッシュから受信した ROA は (*) で表示されます。キャッシュセッションがそのキャッシュのパージ時間内に確立されない場合、これらの ROA は RPKI データベースから削除されます。</p> <p>table show コマンドの後に ROA プレフィックスブロックが指定されている場合 (たとえば、show bgp rpki table 67.21.36.0/24 max 24)、その特定の ROA エントリが詳細に表示されます (ROA が存在する場合)。</p> <p>(注)<br/>1 つの ROA (IP アドレス/最小-最大) は、複数のオリジン AS を持つことができ、複数のキャッシュからソースを取得できます。</p> |
| <b>show bgp rpki cache {IP address}</b>                                                            | <p>構成されているすべてのキャッシュとそのパラメータ (show bgp summary など) の要約リストを表示します。</p> <p>前のコマンドでキャッシュ IP アドレスが指定されている場合、そのキャッシュの詳細情報が表示されます。</p>                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>show bgp {ipv4 unicast   ipv6 unicast} origin-as validity-state {valid   invalid   unknown}</b> | <p>BGP ピアに関する情報を表示します。このコマンドには、パス (validation_state) に基づいて BGP テーブル出力をフィルタリングする新しいオプションがあります。このコマンドで有効性状態 (有効、無効、または不明) を指定すると、BGP テーブルから関連情報がフィルタリングされ、その有効性状態に一致する BGP パスのみが表示されます。</p>                                                                                                                                                                                                                                                                                                                              |

## RPKI Clear コマンド

以下は RPKI Clear コマンドです。

- **clear bgp rpki cache \*** - このコマンドは、構成されているすべての RPKI キャッシュのトランスポートセッションをリセットし、すべてのキャッシュから受信したすべての IPv4 および IPv6 ROA の RPKI データベースを即座に消去します。

## RPKI Debug および Event History コマンド

以下は、RPKI Debug および Event History コマンドです。

- **debug bgp rpki** - このコマンドは、プレフィックス検証を除くすべての RPKI 関連操作のデバッグをオンにします。これには、RPKI キャッシュ接続、RPKI キャッシュのプロトコルステートマシン、ROA の挿入や削除などの RPKI データベース イベントなどのデバッグ イベントが含まれます。
- **sh bgp event-history rpki** - このコマンドは、RPKI に関する高レベルの情報をダンプします。



## 第 9 章

# IP ACL の設定

この章では、Cisco NX-OS デバイスの IP アクセス コントロール リスト（ACL）を設定する方法について説明します。

特に指定がなければ、IP ACL は IPv4 および IPv6 の ACL を意味します。

- [ACL の概要, on page 201](#)
- [ACL の前提条件 \(204 ページ\)](#)
- [ACL の注意事項と制約事項 \(205 ページ\)](#)
- [デフォルトの ACL 設定, on page 207](#)
- [IP ACL の設定 \(208 ページ\)](#)
- [システム ACL について \(224 ページ\)](#)
- [ACL ロギングの構成 \(229 ページ\)](#)
- [ACL TCAM リージョン サイズの設定 \(234 ページ\)](#)
- [仮想端末回線の ACL の設定 \(237 ページ\)](#)

## ACL の概要

アクセス コントロール リスト（ACL）とは、トラフィックのフィルタリングに使用する順序付きのルールセットのことです。各ルールには、パケットがルールに一致するために満たさなければならない条件のセットが規定されています。スイッチは、あるパケットに対してある ACL を適用するかどうかを判断するとき、そのパケットを ACL 内のすべてのルールの条件に対してテストします。一致する条件が最初に見つかった時点で、パケットを許可するか拒否するかが決まります。一致する条件が見つからないと、スイッチは適用可能なデフォルトのルールを適用します。許可されたパケットについては処理が続行され、拒否されたパケットはドロップされます。

ACL を使用すると、ネットワークおよび特定のホストを、不要なトラフィックや望ましくないトラフィックから保護できます。たとえば、ACL を使用して、厳重にセキュリティ保護されたネットワークからインターネットに HTTP トラフィックが流入するのを禁止できます。また、特定のサイトへの HTTP トラフィックだけを許可することもできます。その場合は、サイトの IP アドレスが、IP ACL に指定されているかどうかによって判定します。

## IP ACL のタイプと適用

Cisco Nexus デバイスは、セキュリティトラフィック フィルタリングのために IPv4、IPv6、および MAC ACL をサポートします。スイッチでは、次の表に示すように、ポート ACL、およびルータ ACL として、IP アクセス コントロール リスト (ACL) を使用できます。

**Table 11:** セキュリティ ACL の適用

| 適用      | サポートするインターフェイス                                                                                                                                                                                                                                      | サポートする ACL のタイプ                 |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| ポート ACL | ACL は、次のいずれかに適用した場合、ポート ACL と見なされます。 <ul style="list-style-type: none"> <li>イーサネット インターフェイス</li> <li>イーサネット ポート チャンネル インターフェイス</li> </ul>                                                                                                           | IPv4 ACL<br>IPv6 ACL<br>MAC ACL |
| ルータ ACL | <ul style="list-style-type: none"> <li>物理層 3 インターフェイス</li> <li>レイヤ 3 イーサネット サブインターフェイス</li> <li>レイヤ 3 イーサネット ポート チャンネル インターフェイス</li> <li>レイヤ 3 イーサネット ポート チャンネル サブインターフェイス</li> <li>管理インターフェイス</li> <li>Switched Virtual Interface (SVI)</li> </ul> | IPv4 ACL<br>IPv6 ACL            |
| VTY ACL | VTY                                                                                                                                                                                                                                                 | IPv4 ACL<br>IPv6 ACL            |

## 適用順序

デバイスは、パケットを処理する際に、そのパケットの転送パスを決定します。デバイスがトラフィックに適用する ACL はパスによって決まります。デバイスは、次の順序で ACL を適用します。

1. ポート ACL
2. 入力ルータ ACL

## ルール

アクセス リスト コンフィギュレーション モードでルールを作成するには、**permit** または **deny** コマンドを使用します。スイッチは、許可ルール内の基準と一致するトラフィックを許可し、

拒否ルール内の基準と一致するトラフィックをブロックします。ルールに一致するためにトラフィックが満たさなければならない基準を設定するためのオプションが多数用意されています。

## 送信元と宛先

各ルールには、ルールに一致するトラフィックの送信元と宛先を指定します。指定する送信元および宛先には、特定のホスト、ホストのネットワークまたはグループ、あるいは任意のホストを使用できます。

## プロトコル

IPv4およびMACのACLでは、トラフィックをプロトコルで識別できます。指定の際の手間を省くために、一部のプロトコルは名前で指定できます。たとえば、IPv4 ACL では、ICMP を名前で指定できます。

インターネット プロトコル番号を表す整数でプロトコルを指定できます。

## 暗黙のルール

IP ACL および MAC ACL には暗黙ルールがあります。暗黙ルールは、実行コンフィギュレーションには設定されていませんが、ACL 内の他のルールと一致しない場合にスイッチがトラフィックに適用するルールです。

すべての IPv4 ACL には、次の暗黙のルールがあります。

```
deny ip any any
```

この暗黙のルールによって、どの条件にも一致しない IP トラフィックは拒否されます。

すべての IPv6 ACL には、次の暗黙のルールがあります。

```
deny ipv6 any any
```

すべての MAC ACL には、次の暗黙のルールがあります。

```
deny any any protocol
```

この暗黙ルールによって、デバイスは、トラフィックのレイヤ2ヘッダーに指定されているプロトコルに関係なく、不一致トラフィックを確実に拒否します。

## その他のフィルタリング オプション

追加のオプションを使用してトラフィックを識別できます。IPv4 ACL には、次の追加フィルタリング オプションが用意されています。

- レイヤ 4 プロトコル
- TCP/UDP ポート
- IGMP タイプ
- 確立済み TCP 接続

## シーケンス番号

Cisco Nexus デバイスはルールของシーケンス番号をサポートしています。入力するすべてのルールにシーケンス番号が割り当てられます（ユーザによる割り当てまたはデバイスによる自動割り当て）。シーケンス番号によって、次の ACL 設定作業が容易になります。

- 既存のルールの中に新規のルールを追加する：シーケンス番号を指定することによって、ACL 内での新規ルールの挿入場所を指定します。たとえば、ルール番号 100 と 110 の間に新しいルールを挿入する必要がある場合は、シーケンス番号 105 を新しいルールに割り当てます。
- ルールを削除する：シーケンス番号を使用しない場合は、ルールを削除するのに、次のようにルール全体を入力する必要があります。

```
switch(config-acl)# no permit tcp 10.0.0.0/8 any
```

このルールに 101 番のシーケンス番号が付いていれば、次コマンドだけでルールを削除できます。

```
switch(config-acl)# no 101
```

- ルールを移動する：シーケンス番号を使用すれば、同じ ACL 内の異なる場所にルールを移動する必要がある場合に、そのルールのコピーをシーケンス番号で正しい位置に挿入してから、元のルールを削除できます。この方法により、トラフィックを中断せずにルールを移動できます。

シーケンス番号を使用せずにルールを入力すると、デバイスはそのルールを ACL の最後に追加し、そのルールの直前のルールのシーケンス番号よりも 10 大きい番号を割り当てます。たとえば、ACL 内の最後のルールのシーケンス番号が 225 で、シーケンス番号を指定せずにルールを追加した場合、デバイスはその新しいルールにシーケンス番号 235 を割り当てます。

また、デバイスでは、ACL 内ルールのシーケンス番号を再割り当てすることができます。シーケンス番号の再割り当ては、ACL 内に、100、101 のように連続するシーケンス番号のルールがある場合、それらのルールの間に 1 つ以上のルールを挿入する必要があるときに便利です。

## 論理演算子と論理演算ユニット

TCP および UDP トラフィックの IP ACL ルールでは、論理演算子を使用して、ポート番号に基づきトラフィックをフィルタリングできます。

Cisco Nexus デバイスは、演算子とオペランドの組み合わせを論理演算ユニット（LOU）というレジスタ内に格納し、IP ACL で指定された TCP および UDP ポート上で演算（より大きい、より小さい、等しくない、包含範囲）を行います。

## ACL の前提条件

IP ACL の前提条件は次のとおりです。

- IP ACL を設定するためには、IP アドレッシングおよびプロトコルに関する知識が必要です。

- ACL を設定するインターフェイス タイプについての知識が必要です。

## ACL の注意事項と制約事項

IP ACL の設定に関する注意事項と制約事項は次のとおりです。

- HTTP メソッド照合の拡張として、`tcp-option-length` オプションが ACE 構文に追加され、パケットの TCP オプション ヘッダーの長さを指定できます。ACE には最大 4 つの `tcp-option-length` を構成できます。これには、TCP オプション長が 0 のものも含まれます。`tcp-option-length` オプションを構成しない場合、長さは 0 と見なされます。これは、TCP オプション ヘッダーのないパケットだけがこの ACE と一致することを意味します。この機能により、可変長の TCP オプション ヘッダーを持つパケットでも HTTP メソッドを照合できるようになり、柔軟性が向上します。
- ACL の設定には **Session Manager** を使用することを推奨します。この機能によって、ACL の設定を確認し、設定を実行コンフィギュレーションにコミットする前に、その設定が必要とするリソースが利用可能かどうかを確認できます。この機能は、約 1,000 以上のルールが含まれている ACL に対して特に有効です。
- TCAM スペースが使用可能な限り、任意の数の ACL を構成できます。
- 出力 RACL は、リリース 7.x ではサポートされていません。ただし、構成がエラーや警告なしで許可される場合があります。
- 通常、IP パケットに対する ACL 処理は I/O モジュール上で実行されます。これには、ACL 処理を加速化するハードウェアを使用します。場合によっては、スーパーバイザモジュールで処理が実行されることもあります。この場合、特に多数のルールが設定されている ACL を処理する際には、処理速度が遅くなることがあります。管理インターフェイス トラフィックは、常にスーパーバイザモジュールで処理されます。次のカテゴリのいずれかに属する IP パケットがレイヤ 3 インターフェイスから出る場合、これらのパケットはスーパーバイザ モジュールに送られて処理されます。
  - レイヤ 3 最大伝送単位チェックに失敗し、そのためにフラグメント化を要求しているパケット
  - IP オプションがある IPv4 パケット（追加された IP パケット ヘッダーのフィールドは、宛先アドレス フィールドの後）
  - 拡張 IPv6 ヘッダー フィールドがある IPv6 パケット
- 時間範囲を使用する ACL を適用すると、デバイスは、その ACL エントリで参照される時間範囲の開始時または終了時に ACL エントリを更新します。時間範囲によって開始されるアップデートはベストエフォート型のプライオリティで実行されます。時間範囲によってアップデートが生じたときにデバイスの処理負荷が非常に高い場合、デバイスはアップデートを最大数秒間遅らせることがあります。時間範囲が有効で、アクティブな状態であることを確認します。

- すべての着信および発信トラフィックに **match-local-traffic** オプションを使用するには、最初に ソフトウェアで ACL を有効にする必要があります。
- 出力 RACL が構成された Cisco N3K-C36180YC-R スイッチの場合、7.x リリースから 9.x リリースにアップグレードする際、次の手順に従って RACL が維持され、アップグレードが問題なく完了していることを確認してください。
  1. **hardware access-list tcam region e-racl** コマンドを使用して、出力 RACL の TCAM エントリを追加します。
  2. 構成を保存してリロードします。
  3. 9.x リリースにアップグレードします。

構成の詳細については、[ACL TCAM リージョン \(225 ページ\)](#) および [ACL TCAM リージョン サイズの設定 \(234 ページ\)](#) を参照してください。

- Cisco NX-OS リリース 9.3(2) 以降、Cisco Nexus 36180YC-R および 3636C-R では、ユーザー定義の MAC アドレス制限を 16 ～ 256 の範囲で設定できます。
- Cisco NX-OS リリース 9.3(3) において、Cisco Nexus 3636C-R プラットフォーム スイッチは、出力 IPv6 RACL について次をサポートします：
  - レイヤ 4 プロトコル
  - TCP フラグ
  - フラグメント
  - ACL ログ
- Cisco NX-OS リリース 9.3(3) において、Cisco Nexus 3636C-R プラットフォーム スイッチは、次をサポートしません：
  - 出力のアトミック アップデート
  - 外部 TCAM の出力ルータ ACL
  - UDF を伴う出力 ルータ ACL
  - 出力と入力の両方のルータ ACL v6 カウンタ
  - l4 ops による出力および出力ルータ ACL IPv6
  - サブインターフェイスの出力ルータ ACL
  - IPv6 ICMP タイプおよびコードによる出力および入力ルータ ACL
  - tcp-flag を使用した IPv6 入力ルータ ACL
  - 追加オプション付きの IPv4 ルータ ACL
- Cisco NX-OS リリース 9.3(3) において、Cisco Nexus 3636C-R プラットフォーム スイッチは、出力 IPv4 RACL について次をサポートします：



- TCP フラグ
  - ICMP のタイプとコード
  - ACL ログ
- hardware profile acl-stats module xx コマンドを使用して ACL TCAM エントリのカウンタを有効にすると、show interface の input discard フィールドは常にゼロになります。この制限は、N3K-C3636C-R および N3K-C36180YC-R ラインカードを搭載した Cisco Nexus 3600 プラットフォーム スイッチにのみ適用されます。
  - Cisco NX-OS リリース 9.3(5) において、IPv6 出力 ACL は、Cisco Nexus 3636C-R および 36180YC-R スイッチで以下をサポートします：
    - レイヤ 4 プロトコル
    - TCP フラグ
    - フラグメント
    - ACL ログ
    - IPv6 ヘッダーのフィールド

## デフォルトの ACL 設定

次の表は、IP ACL パラメータのデフォルト設定をリスト表示しています。

**Table 12: IP ACL のデフォルトパラメータ**

| パラメータ   | デフォルト                    |
|---------|--------------------------|
| IP ACL  | デフォルトの IP ACL は存在しません。   |
| ACL ルール | すべての ACL に暗黙のルールが適用されます。 |

次の表は、MAC ACL パラメータのデフォルト設定をリスト表示しています。

**Table 13: MAC ACL のデフォルトパラメータ**

| パラメータ   | デフォルト                    |
|---------|--------------------------|
| MAC ACL | デフォルトでは MAC ACL は存在しません。 |
| ACL ルール | すべての ACL に暗黙のルールが適用されます。 |

# IP ACL の設定

## IP ACL の作成

デバイスに IPv4 または IPv6 ACL を作成し、これにルールを追加できます。

### Before you begin

ACL の設定には Session Manager を使用することを推奨します。この機能によって、ACL の設定を確認し、設定を実行コンフィギュレーションにコミットする前に、その設定が必要とするリソースが利用可能かどうかを確認できます。この機能は、約 1,000 以上のルールが含まれている ACL に対して特に有効です。

### SUMMARY STEPS

1. **configure terminal**
2. 次のいずれかのコマンドを入力します。
  - **ip access-list name**
  - **ipv6 access-list name**
3. **[sequence-number] {permit | deny} protocol {source-ip-prefix | source-ip-mask} {destination-ip-prefix | destination-ip-mask}**
4. **statistics per-entry**
5. **hardware profile acl-stats module xx**
6. **reload**
7. 次のいずれかのコマンドを入力します。
  - **show ip access-lists name**
  - **show ipv6 access-lists name**
8. **copy running-config startup-config**
9. (Optional) **switch# copy running-config startup-config**

### DETAILED STEPS

#### Procedure

|        | Command or Action                                                                                         | Purpose           |
|--------|-----------------------------------------------------------------------------------------------------------|-------------------|
| ステップ 1 | <b>configure terminal</b><br><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre> | グローバル構成モードを開始します。 |

|        | Command or Action                                                                                                                                                                                                                              | Purpose                                                                                                                                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 2 | <p>次のいずれかのコマンドを入力します。</p> <ul style="list-style-type: none"> <li>• <b>ip access-list name</b></li> <li>• <b>ipv6 access-list name</b></li> </ul> <p><b>Example:</b></p> <pre>switch(config)# ip access-list acl-01 switch(config-acl)#</pre>   | IP ACL を作成して、IP ACL コンフィギュレーション モードを開始します。name 引数は 64 文字以内で指定します。                                                                                                                                                                |
| ステップ 3 | <p>[sequence-number] {<b>permit</b>   <b>deny</b>} protocol {source-ip-prefix   source-ip-mask} {destination-ip-prefix   destination-ip-mask}</p> <p><b>Example:</b></p> <pre>switch(config-acl)# 10 permit ipv6 1::1 2::2 3::3 4::4</pre>     | <p>IP ACL 内にルールを作成します。多数のルールを作成できます。sequence-number 引数には、1 ～ 4294967295 の整数を指定します。</p> <p><b>permit</b> コマンドと <b>deny</b> コマンドには、トラフィックを識別するための多くの方法が用意されています。詳細については、特定の Cisco Nexus デバイスのコマンド リファレンスを参照してください。</p>             |
| ステップ 4 | <p><b>statistics per-entry</b></p> <p><b>Example:</b></p> <pre>switch(config-acl)# statistics per-entry</pre>                                                                                                                                  | その ACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。                                                                                                                                                                                  |
| ステップ 5 | <p><b>hardware profile acl-stats module xx</b></p> <p><b>Example:</b></p> <pre>switch(config-acl)# hardware profile acl-stats module 1</pre>                                                                                                   | <p>内部 TCAM と外部 TCAM の両方で ACL TCAM エントリのカウンタを有効にします。</p> <p><b>Note</b><br/>このコマンドは、-R および -RX ライン カードと Cisco Nexus 3636C-R および 36180YC-R スイッチを備えた Cisco Nexus 9500 プラットフォームスイッチにのみ適用されます。カウンタを有効にすると、VLAN と SVI の統計情報は失われます。</p> |
| ステップ 6 | <p><b>reload</b></p> <p><b>Example:</b></p> <pre>switch(config)# reload</pre>                                                                                                                                                                  | <p>スイッチをリロードします。</p> <p><b>Note</b><br/><b>reload</b> コマンドは、Cisco Nexus 3636C-R および 36180YC-R スイッチでは必須です。</p>                                                                                                                    |
| ステップ 7 | <p>次のいずれかのコマンドを入力します。</p> <ul style="list-style-type: none"> <li>• <b>show ip access-lists name</b></li> <li>• <b>show ipv6 access-lists name</b></li> </ul> <p><b>Example:</b></p> <pre>switch(config-acl)# show ip access-lists acl-01</pre> | IP ACL の設定を表示します。                                                                                                                                                                                                                |
| ステップ 8 | <p><b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch(config-acl)# copy running-config startup-config</pre>                                                                                                      | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                                                                                                                                                        |

|        | Command or Action                                            | Purpose                                   |
|--------|--------------------------------------------------------------|-------------------------------------------|
| ステップ 9 | (Optional) switch# <b>copy running-config startup-config</b> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。 |

### Example

次に、IPv4 ACL を作成する例を示します。

```
switch# configure terminal
switch(config)# ip access-list acl-01
switch(config-acl)# permit ip 192.168.2.0/24 any
```

次に、IPv6 ACL を作成する例を示します。

```
switch# configure terminal
switch(config)# ipv6 access-list acl-01-ipv6
switch(config-ipv6-acl)# permit tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
```

## IPv4 ACL ロギングの設定

IPv4 ACL ロギングプロセスを設定するには、最初にアクセス リストを作成してから、指定された ACL を使用してインターフェイス上の IPv4 トラフィックのフィルタリングをイネーブルにし、最後に ACL ロギングプロセス パラメータを設定します。

### 手順の概要

1. **configure terminal**
2. **ip access-list name**
3. **{permit | deny} ip source-address destination-address log**
4. **exit**
5. **interface ethernet slot/port**
6. **ip access-group name in**
7. **exit**
8. **logging ip access-list cache interval interval**
9. **logging ip access-list cache entries number-of-flows**
10. **logging ip access-list cache threshold threshold**
11. **logging ip access-list detailed**
12. **hardware rate-limiter access-list-log** パケット
13. **aclog match-log-level severity-level**
14. (任意) **show logging ip access-list cache [detail]**

## 手順の詳細

## 手順

|        | コマンドまたはアクション                                                                                                                              | 目的                                                                                                                                                                                                                                                                               |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br><pre>switch# configure terminal switch(config)#</pre>                                                 | グローバル構成モードを開始します。                                                                                                                                                                                                                                                                |
| ステップ 2 | <b>ip access-list name</b><br>例 :<br><pre>switch(config)# ip access-list logging-test switch(config-acl)#</pre>                           | IPv4 ACL を作成し、IP ACL コンフィギュレーション モードを開始します。 <i>name</i> 引数は 64 文字以内で指定します。                                                                                                                                                                                                       |
| ステップ 3 | <b>{permit   deny} ip source-address destination-address log</b><br>例 :<br><pre>switch(config-acl)# permit ip any 10.30.30.0/24 log</pre> | <p>条件に一致する IPv4 トラフィックを許可または拒否する、ACL のルールを作成します。システムがルールに一致する各パケットに関する情報ロギングメッセージを生成できるようにするには、log キーワードを含める必要があります。</p> <p><i>Source-address</i> および <i>destination-address</i> 引数には、IP アドレスとネットワーク ワイルドカード、IP アドレスと可変長サブネット マスク、ホスト アドレス、または任意のアドレスを指定する <b>any</b> があります。</p> |
| ステップ 4 | <b>exit</b><br>例 :<br><pre>switch(config-acl)# exit switch(config)#</pre>                                                                 | 設定を更新し、IP ACL コンフィギュレーション モードを終了します。                                                                                                                                                                                                                                             |
| ステップ 5 | <b>interface ethernet slot/port</b><br>例 :<br><pre>switch(config)# interface ethernet 1/1 switch(config-if)#</pre>                        | インターフェイス設定モードを開始します。                                                                                                                                                                                                                                                             |
| ステップ 6 | <b>ip access-group name in</b><br>例 :<br><pre>switch(config-if)# ip access-group logging-test in</pre>                                    | 指定された ACL を使用してインターフェイス上の IPv4 トラフィックのフィルタリングをイネーブルにします。着信トラフィックに ACL を適用できます。                                                                                                                                                                                                   |
| ステップ 7 | <b>exit</b><br>例 :<br><pre>switch(config-if)# exit switch(config)#</pre>                                                                  | 設定を更新し、インターフェイスコンフィギュレーション モードを終了します。                                                                                                                                                                                                                                            |

|         | コマンドまたはアクション                                                                                                                               | 目的                                                                                                                                                                                                               |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 8  | <b>logging ip access-list cache interval interval</b><br>例 :<br><pre>switch(config)# logging ip access-list cache interval 490</pre>       | ACL ロギング プロセスのログ更新間隔（秒単位）を設定します。デフォルト値は300秒です。範囲は5～86400秒です。                                                                                                                                                     |
| ステップ 9  | <b>logging ip access-list cache entries number-of-flows</b><br>例 :<br><pre>switch(config)# logging ip access-list cache entries 8001</pre> | ACL ロギング プロセスでモニタするフローの最大数を指定します。デフォルト値は8000です。サポートされる値の範囲は0～1048576です。                                                                                                                                          |
| ステップ 10 | <b>logging ip access-list cache threshold threshold</b><br>例 :<br><pre>switch(config)# logging ip access-list cache threshold 490</pre>    | アラート期限が切れる前に、指定されたパケット数がログ記録された段階で、Syslog メッセージが生成されます。                                                                                                                                                          |
| ステップ 11 | <b>logging ip access-list detailed</b><br>例 :<br><pre>switch(config)# logging ip access-list detailed</pre>                                | <b>show logging ip access-list cache</b> コマンドの出力で、ACL 名、ACE シーケンス番号、アクション、ACL の方向、ACL フィルタタイプ、およびACL 適用インターフェイスが表示されるようにします。                                                                                     |
| ステップ 12 | <b>hardware rate-limiter access-list-log</b> パケット<br>例 :<br><pre>switch(config)# hardware rate-limiter access-list-log 200</pre>           | ACL ロギングのためにスーパーバイザ モジュールにコピーされるパケットのレート制限をppsで設定します。範囲は0～30000です。<br><br>(注)<br>Cisco Nexus NX-OS 7.0(3)F3(1) は、 <b>hardware rate-limiter access-list-log</b> コマンドをサポートしていません。                                  |
| ステップ 13 | <b>aclog match-log-level severity-level</b><br>例 :<br><pre>switch(config)# aclog match-log-level 5</pre>                                   | ACL の一致を記録する最小シビラティ（重大度）レベルを指定します。デフォルトは6（情報）です。範囲は0（緊急）～7（デバッグ）です。                                                                                                                                              |
| ステップ 14 | (任意) <b>show logging ip access-list cache [detail]</b><br>例 :<br><pre>switch(config)# show logging ip access-list cache</pre>              | 送信元IPおよび宛先IPアドレス、送信元ポートおよび宛先ポート情報、送信元インターフェイスなど、アクティブなログフローに関する情報を表示します。 <b>logging ip access-list detailed</b> コマンドを入力すると、出力には、ACL の名前、ACE のシーケンス番号、アクション、ACL の方向、ACL のフィルタタイプ、そして ACL の適用インターフェイスも含まれるようになります。 |

## IP ACL の変更

既存の IPv4 または IPv6 ACL に対してルールの追加または削除を行うことができます。既存のルールは変更できません。ルールを変更するには、そのルールを削除してから、変更を加えたルールを再作成します。

既存のルールの中に新しいルールを挿入する必要がある場合で、現在のシーケンス番号の空き状況ではすべてを挿入できないときは、**resequence** コマンドを使用してシーケンス番号を再割り当てします。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **{ip | ipv6} ip access-list name**
3. switch(config)# **ip access-list name**
4. switch(config-acl)# **[sequence-number] {permit | deny} protocol source destination**
5. (Optional) switch(config-acl)# **no {sequence-number | {permit | deny} protocol source destination}**
6. (Optional) switch# **show ip access-lists name**
7. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

#### Procedure

|        | Command or Action                                                                                        | Purpose                                                                                                                                                                                                                                                                                    |
|--------|----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                                                                        | グローバル コンフィギュレーション モードを開始します。                                                                                                                                                                                                                                                               |
| ステップ 2 | switch(config)# <b>{ip   ipv6} ip access-list name</b>                                                   | 名前で指定した ACL の IP ACL コンフィギュレーション モードを開始します。                                                                                                                                                                                                                                                |
| ステップ 3 | switch(config)# <b>ip access-list name</b>                                                               | 名前で指定した ACL の IP ACL コンフィギュレーション モードを開始します。                                                                                                                                                                                                                                                |
| ステップ 4 | switch(config-acl)# <b>[sequence-number] {permit   deny} protocol source destination</b>                 | IP ACL 内にルールを作成します。シーケンス番号を指定すると、ACL 内のルール挿入位置を指定できます。シーケンス番号を指定しないと、ルールは ACL の末尾に追加されます。 <b>sequence-number</b> 引数には、1 ～ 4294967295 の整数を指定します。<br><br><b>permit</b> コマンドと <b>deny</b> コマンドには、トラフィックを識別するための多くの方法が用意されています。詳細については、Cisco Nexus デバイスの『 <i>Command Reference</i> 』を参照してください。 |
| ステップ 5 | (Optional) switch(config-acl)# <b>no {sequence-number   {permit   deny} protocol source destination}</b> | 指定したルールを IP ACL から削除します。                                                                                                                                                                                                                                                                   |

|        | Command or Action                                            | Purpose                                                                                                               |
|--------|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
|        |                                                              | permit コマンドと deny コマンドには、トラフィックを識別するための多くの方法が用意されています。詳細については、Cisco Nexus デバイスの『 <i>Command Reference</i> 』を参照してください。 |
| ステップ 6 | (Optional) switch# <b>show ip access-lists name</b>          | IP ACL の設定を表示します。                                                                                                     |
| ステップ 7 | (Optional) switch# <b>copy running-config startup-config</b> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                                             |

### Related Topics

[IP ACL 内のシーケンス番号の変更](#) (215 ページ)

## IP ACL の削除

スイッチから IP ACL を削除できます。

スイッチから IP ACL を削除する前に、ACL がインターフェイスに適用されているかどうかを確認してください。削除できるのは、現在適用されている ACL だけです。ACL を削除しても、その ACL が適用されていたインターフェイスの設定は影響を受けません。スイッチは、削除対象の ACL が空であると見なします。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **no ip access-list name**
3. switch(config)# **no ip access-list name**
4. (Optional) switch# **show running-config**
5. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

#### Procedure

|        | Command or Action                             | Purpose                               |
|--------|-----------------------------------------------|---------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>             | グローバル コンフィギュレーション モードを開始します。          |
| ステップ 2 | switch(config)# <b>no ip access-list name</b> | 名前で指定した IP ACL を実行コンフィギュレーションから削除します。 |
| ステップ 3 | switch(config)# <b>no ip access-list name</b> | 名前で指定した IP ACL を実行コンフィギュレーションから削除します。 |



|        | Command or Action                                            | Purpose                                   |
|--------|--------------------------------------------------------------|-------------------------------------------|
| ステップ 4 | (Optional) switch# <b>show running-config</b>                | ACL の設定を表示します。削除された IP ACL は表示されないはずです。   |
| ステップ 5 | (Optional) switch# <b>copy running-config startup-config</b> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。 |

## IP ACL 内のシーケンス番号の変更

IP ACL 内のルールに付けられたすべてのシーケンス番号を変更できます。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **resequence ip access-list name starting-sequence-number increment**
3. (Optional) switch# **show ip access-lists name**
4. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

#### Procedure

|        | Command or Action                                                                        | Purpose                                                                                                                                                                                                 |
|--------|------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                                                        | グローバル コンフィギュレーション モードを開始します。                                                                                                                                                                            |
| ステップ 2 | switch(config)# <b>resequence ip access-list name starting-sequence-number increment</b> | ACL 内に記述されているルールにシーケンス番号を付けます。指定した開始シーケンス番号が最初のルールに付けられます。後続の各ルールには、直前のルールよりも大きい番号が付けられます。番号の間隔は、指定した増分によって決まります。<br><i>starting-sequence-number</i> 引数と <i>increment</i> 引数は、1 ～ 4294967295 の整数で指定します。 |
| ステップ 3 | (Optional) switch# <b>show ip access-lists name</b>                                      | IP ACL の設定を表示します。                                                                                                                                                                                       |
| ステップ 4 | (Optional) switch# <b>copy running-config startup-config</b>                             | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                                                                                                                               |

## mgmt0 への IP-ACL の適用

管理インターフェイス (mgmt0) に適用できるのは、IPv4 と IPv6 の ACL です。

## 始める前に

適用する ACL が存在し、目的に応じたトラフィック フィルタリングが設定されていることを確認します。

## 手順の概要

1. **configure terminal**
2. **ip access-group access-list {in | out}**
3. (任意) **show running-config aclmgr**
4. (任意) **copy running-config startup-config**

## 手順の詳細

## 手順

|        | コマンドまたはアクション                                                                                                              | 目的                                                                                |
|--------|---------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br><pre>switch# configure terminal switch(config)#</pre>                                 | グローバル コンフィギュレーション モードを開始します。                                                      |
| ステップ 2 | <b>ip access-group access-list {in   out}</b><br>例 :<br><pre>switch(config-if)# ip access-group acl-120 out</pre>         | IPv4 ACL または IPv6 ACL を、指定方向のトラフィックのレイヤ 3 インターフェイスに適用します。各方向にルータ ACL を 1 つ適用できます。 |
| ステップ 3 | (任意) <b>show running-config aclmgr</b><br>例 :<br><pre>switch(config-if)# show running-config aclmgr</pre>                 | ACL の設定を表示します。                                                                    |
| ステップ 4 | (任意) <b>copy running-config startup-config</b><br>例 :<br><pre>switch(config-if)# copy running-config startup-config</pre> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                         |

## 関連項目

- IP ACL の作成

## ポート ACL としての IP ACL の適用

IPv4 ACL は、物理イーサネットインターフェイスまたは PortChannel に適用できます。これらのインターフェイス タイプに適用された ACL は、ポート ACL と見なされます。

**Note**

一部の設定パラメータは、ポート チャンネルに適用されていると、メンバー ポートの設定に反映されません。

**SUMMARY STEPS**

1. switch# **configure terminal**
2. switch(config)# **interface** {**ethernet** [chassis/]slot/port | **port-channel** channel-number}
3. switch(config-if)# **ip port access-group** access-list in
4. (Optional) switch# **show running-config**
5. (Optional) switch# **copy running-config startup-config**

**DETAILED STEPS****Procedure**

|        | Command or Action                                                                                            | Purpose                                                                                                        |
|--------|--------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                                                                            | グローバル コンフィギュレーション モードを開始します。                                                                                   |
| ステップ 2 | switch(config)# <b>interface</b> { <b>ethernet</b> [chassis/]slot/port   <b>port-channel</b> channel-number} | 指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。                                                                |
| ステップ 3 | switch(config-if)# <b>ip port access-group</b> access-list in                                                | IPv4 ACL を、インターフェイスまたはポート チャンネルに適用します。ポート ACL では、インバウンドフィルタリングだけがサポートされています。1 つのインターフェイスに 1 つのポート ACL を適用できます。 |
| ステップ 4 | (Optional) switch# <b>show running-config</b>                                                                | ACL の設定を表示します。                                                                                                 |
| ステップ 5 | (Optional) switch# <b>copy running-config startup-config</b>                                                 | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                                      |

**ルータ ACL としての IP ACL の適用**

IPv4 ACL または IPv6 ACL は、次のタイプのインターフェイスに適用できます：

- 物理層 3 インターフェイスおよびサブインターフェイス
- レイヤ 3 イーサネット ポート チャンネル インターフェイスおよびサブインターフェイス
- 管理インターフェイス

**Before you begin**

適用する ACL が存在し、目的に応じたトラフィック フィルタリングが設定されていることを確認します。

**SUMMARY STEPS**

1. switch# **configure terminal**
2. 次のいずれかのコマンドを入力します。
  - switch(config)# **interface ethernet** *slot/port* [ *. number* ]
  - switch(config)# **interface port-channel** *channel-number* [ *. number* ]
  - switch(config)# **interface mgmt** *port*
3. 次のいずれかのコマンドを入力します。
  - switch(config-if)# **ip access-group** *access-list* {*in*}
  - switch(config-if)# **ipv6 traffic-filter** *access-list* {*in*}
4. (Optional) switch(config-if)# **show running-config aclmgr**
5. (Optional) switch(config-if)# **copy running-config startup-config**

**DETAILED STEPS****Procedure**

|        | Command or Action                                                                                                                                                                                                                                                                                                     | Purpose                                                   |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                                                                                                                                                                                                                                                                                     | グローバル コンフィギュレーション モードを開始します。                              |
| ステップ 2 | 次のいずれかのコマンドを入力します。 <ul style="list-style-type: none"> <li>• switch(config)# <b>interface ethernet</b> <i>slot/port</i> [ <i>. number</i> ]</li> <li>• switch(config)# <b>interface port-channel</b> <i>channel-number</i> [ <i>. number</i> ]</li> <li>• switch(config)# <b>interface mgmt</b> <i>port</i></li> </ul> | 指定したインターフェイス タイプのコンフィギュレーション モードを開始します。                   |
| ステップ 3 | 次のいずれかのコマンドを入力します。 <ul style="list-style-type: none"> <li>• switch(config-if)# <b>ip access-group</b> <i>access-list</i> {<i>in</i>}</li> <li>• switch(config-if)# <b>ipv6 traffic-filter</b> <i>access-list</i> {<i>in</i>}</li> </ul>                                                                               | IPv4 ACL または IPv6 ACL を、入力方向のトラフィックのレイヤ 3 インターフェイスに適用します。 |
| ステップ 4 | (Optional) switch(config-if)# <b>show running-config aclmgr</b>                                                                                                                                                                                                                                                       | ACL の設定を表示します。                                            |
| ステップ 5 | (Optional) switch(config-if)# <b>copy running-config startup-config</b>                                                                                                                                                                                                                                               | 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。                |

## インターフェイス MAC アドレスの設定と制限

SVI、レイヤ 3 インターフェイス、ポート チャネル、レイヤ 3 サブインターフェイス、およびトンネル インターフェイスにスタティック MAC アドレスを設定できます。ポートおよびポート チャネルの範囲でスタティック MAC アドレスを設定することもできます。ただし、すべてのポートがレイヤ 3 にある必要があります。ポートの範囲内の 1 つのポートがレイヤ 2 にある場合でも、コマンドは拒否され、エラー メッセージが表示されます。

デフォルトでは、スイッチに設定できる MAC アドレスの最大数は 16 です。ただし、この制限を変更して、MAC アドレス数の範囲を 16 ～ 256 に設定することができます。

vPC 対応スイッチでの構成制限には、ローカルに構成されたユーザー定義の MAC アドレスと、vPC ピアから同期されたユーザー定義の MAC アドレスの両方が含まれます。

### 手順の概要

1. **configure terminal**
2. **interface ethernet slot/port**
3. **[no] mac-address static router MAC address**
4. (任意) **show interface ethernet slot/port**
5. **mac address-table limit 16-256 user-defined**
6. (任意) **show mac address-table limit user-defined**

### 手順の詳細

#### 手順

|        | コマンドまたはアクション                                                                                                         | 目的                                                                                                                                                                                                                   |
|--------|----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br><pre>switch# configure terminal switch(config)#</pre>                            | グローバル設定モードを開始します。                                                                                                                                                                                                    |
| ステップ 2 | <b>interface ethernet slot/port</b><br>例 :<br><pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>   | インターフェイス設定モードを開始します。                                                                                                                                                                                                 |
| ステップ 3 | <b>[no] mac-address static router MAC address</b><br>例 :<br><pre>switch(config-if)# mac-address 0019.D2D0.00AE</pre> | インターフェイスに MAC アドレスを設定します。設定を削除するには、このコマンドの no 形式を使用します。MAC アドレスは、サポートされている次の 4 つの形式のいずれかで入力できます。 <ul style="list-style-type: none"> <li>• E.E.E</li> <li>• EE-EE-EE-EE-EE-EE</li> <li>• EE:EE:EE:EE:EE:EE</li> </ul> |

|        | コマンドまたはアクション                                                                                                                                         | 目的                                                                                                                                                                                                                                                                               |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        |                                                                                                                                                      | <ul style="list-style-type: none"> <li>• EEEE.EEEE.EEEE</li> </ul> <p>(注)<br/>次の無効なMACアドレスは入力しないでください。</p> <ul style="list-style-type: none"> <li>• ノルMACアドレス : 0000.0000.0000</li> <li>• ブロードキャストMACアドレス : FFFF.FFFF.FFFF</li> <li>• マルチキャストMACアドレス : 0100.DAAA.ADDD</li> </ul> |
| ステップ 4 | (任意) <b>show interface ethernet slot/port</b><br><br>例 :<br><pre>switch(config-if)# show interface ethernet 2/1 switch(config)#</pre>                | インターフェイスのすべての情報を表示します。                                                                                                                                                                                                                                                           |
| ステップ 5 | <b>mac address-table limit 16-256 user-defined</b><br><br>例 :<br><pre>switch(config)# mac address-table limit 200 user-defined switch(config)#</pre> | スイッチに設定できる MAC アドレスの最大数を設定します。                                                                                                                                                                                                                                                   |
| ステップ 6 | (任意) <b>show mac address-table limit user-defined</b><br><br>例 :<br><pre>switch(config)# show mac address-table limit user-defined</pre>             | スイッチに設定できる MAC アドレスの最大数を表示します。                                                                                                                                                                                                                                                   |

## 例

インターフェイスの MAC アドレスを構成する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/3
switch(config-if)# mac-address aaaa.bbbb.dddd
switch(config-if)# show interface ethernet 3/3
switch(config-if)#
switch(config)# mac address-table limit 100 user-defined
Warning: Configure the same User-Defined Mac Limit on the peer.
Warning: New Fhrp max group limit is 390
switch# show mac address-table limit user-defined
User Defined Mac Limit: 100
FHRP Mac Limit: 390
=====
```

## UDF ベースの MAC ACL の設定

この機能により、デバイスはユーザ定義フィールド（UDF）で照合し、一致するパケットを MAC ACL に適用できます。

Cisco NX-OS リリース 9.3(2) 以降では、Cisco Nexus 36180YC-R および 3636C-R プラットフォーム スイッチの UDF ベースで MAC アクセス リスト（ACL）を構成できます。

### 手順の概要

1. **configure terminal**
2. **udf udf-name offset-base offset length**
3. **hardware access-list tcam region ing-ifacl qualify {udf udf-name }**
4. **copy running-config startup-config**
5. **reload**
6. **mac access-list udf-acl**
7. **permit mac source destination udf udf-name value mask**
8. **interface port-channel channel-number**
9. **mac port access-group udf-access-list**
10. （任意） **copy running-config startup-config**

### 手順の詳細

#### 手順

|        | コマンドまたはアクション                                                                                                       | 目的                                                                                                                                                                                                                                                                                                                                                                                |
|--------|--------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br><pre>switch# configure terminal switch(config)#</pre>                          | グローバル コンフィギュレーション モードを開始します                                                                                                                                                                                                                                                                                                                                                       |
| ステップ 2 | <b>udf udf-name offset-base offset length</b><br>例 :<br><pre>switch(config)# udf pkttoff10 packet-start 10 2</pre> | 次のように UDF を定義します。 <ul style="list-style-type: none"> <li>• <b>udf-name</b> : UDF の名前を指定します。名前には最大 16 文字の英数字を入力できます。</li> <li>• <b>offset-base</b> : UDF オフセット ベースを <b>{packet-start}</b> のように指定します。</li> <li>• <b>オフセット</b> : オフセット ベースからバイト オフセットの数を指定します。</li> <li>• <b>長さ</b> : オフセット からバイトの数を指定します。1 または 2 バイトのみがサポートされています。追加のバイトに一致させるためには、複数の UDF を定義する必要があります。</li> </ul> |

|        | コマンドまたはアクション                                                                                                                                                                        | 目的                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        |                                                                                                                                                                                     | 複数の UDF を定義できますが、シスコは必要な UDF のみ定義することを推奨します。                                                                                                                                                                                                                                                                                                                                                           |
| ステップ 3 | <b>hardware access-list tcam region ing-ifac1 qualify {udf udf-name }</b><br><br>例 :<br><pre>switch(config)# hardware access-list tcam region ing-ifac1 qualify udf pkttoff10</pre> | IPv4 または IPv6 ポート ACL に適用する ing-ifac1 TCAM リージョンに UDF をアタッチします。<br><br>最大 18 個の UDF がサポートされます。<br><br>(注)<br>UDF 修飾子が追加されると、TCAM リージョンはシングル幅から倍幅に拡大します。十分な空き領域があることを確認してください。そうでない場合、このコマンドは拒否されます。必要な場合、未使用のリージョンから TCAM スペースが減りますので、このコマンドを再入力します。詳細については、「 <a href="#">ACL TCAM リージョン サイズの設定 (234 ページ)</a> 」を参照してください。<br><br>(注)<br>このコマンドの <b>no</b> 形式は、UDF を TCAM リージョンから切り離し、リージョンをシングル幅に戻します。 |
| ステップ 4 | 必須: <b>copy running-config startup-config</b><br><br>例 :<br><pre>switch(config)# copy running-config startup-config</pre>                                                           | リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。                                                                                                                                                                                                                                                                                                                                     |
| ステップ 5 | 必須: <b>reload</b><br><br>例 :<br><pre>switch(config)# reload</pre>                                                                                                                   | デバイスがリロードされます。<br><br>(注)<br>UDF 設定は <b>copy running-config startup-config + reload</b> を入力した後のみ有効になります。                                                                                                                                                                                                                                                                                               |
| ステップ 6 | <b>mac access-list udf-acl</b><br><br>例 :<br><pre>switch(config)# mac access-list udfacl switch(config-acl)#</pre>                                                                  | MAC アクセス コントロール リスト (ACL) を作成して、MAC ACL コンフィギュレーション モードを開始します。                                                                                                                                                                                                                                                                                                                                         |
| ステップ 7 | <b>permit mac source destination udf udf-name value mask</b><br><br>例 :<br><pre>switch(config-acl)# permit mac any any udf pkttoff10 0x1234 0xffff</pre>                            | MAC ACL を設定して、外部パケット フィールドについて現在のアクセス コントロール エントリ (ACE) と併せて UDF で一致させるように設定します (例 2)。値とマスクの引数の範囲は 0x0～0xFFFF です。<br><br>シングル ACL は、UDF がある場合とない場合の両方とも、ACE を有することができます。各 ACE に                                                                                                                                                                                                                        |



|         | コマンドまたはアクション                                                                                                              | 目的                                                         |
|---------|---------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|
|         |                                                                                                                           | は一致する異なる UDF フィールドがあるか、すべての ACE を UDF の同じリストに一致させることができます。 |
| ステップ 8  | <b>interface port-channel channel-number</b><br><br>例 :<br>switch(config)# interface port-channel 5<br>switch(config-if)# | レイヤ 2 のポート チャネル インターフェイスのインターフェイス コンフィギュレーション モードを開始します。   |
| ステップ 9  | <b>mac port access-group udf-access-list</b><br><br>例 :<br>switch(config-if)# mac port access-group udf-acl-01            | UDF ベース MAC ACL をインターフェイスに適用します。                           |
| ステップ 10 | (任意) <b>copy running-config startup-config</b><br><br>例 :<br>switch(config)# copy running-config startup-config           | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                  |

## IPv6 拡張ヘッダーの ACL の設定

この手順は、次のデバイスにのみ適用されます。

- Cisco Nexus 9504 および 9508 モジュラ シャーシ (N9K-X9636C-R、N9K-X9636Q-R、N9K-X9636C-RX、および N9K-X96136YC-R)
- Cisco Nexus 3600 プラットフォーム スイッチ (N3K-C36180YC-R および N3K-C3636C-R)

Cisco NX-OS リリース 9.3(7) 以降では、ここにリストされているデバイスで IPv6 ACL を設定する場合、拡張ヘッダーを含む IPv6 パケットの処理に関する新しいルールを含める必要があります。IPv6 拡張ヘッダーの詳細については、*Cisco Nexus 3600 シリーズ NX-OS ユニキャストルーティング構成ガイド*のNX-OS リリース 9.3(x)以降の「簡素化したIPv6パケットヘッダー」を参照してください。



(注) この手順で選択した許可ルールまたは拒否ルールは、パケットの他のフィールドに一致する他の ACL ルールに関係なく、少なくとも 1 つの拡張ヘッダーを持つ IPv6 パケットに適用されます。

### 手順の概要

1. **configure terminal**
2. **ipv6 access-list name**
3. **extension-header {permit-all | deny-all}**

## 手順の詳細

## 手順

|        | コマンドまたはアクション                                                                                                                             | 目的                                                                                                                                                                                                             |
|--------|------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br><pre>switch# configure terminal switch(config)#</pre>                                                | グローバル構成モードを開始します。                                                                                                                                                                                              |
| ステップ 2 | <b>ipv6 access-list name</b><br>例 :<br><pre>switch(config)# ipv6 access-list acl-01 switch(config-acl)#</pre>                            | MAC ACL を作成して、ACL コンフィギュレーションモードを開始します。                                                                                                                                                                        |
| ステップ 3 | <b>extension-header {permit-all   deny-all}</b><br>例 :<br><pre>switch(config-acl)# extension-header permit-all switch(config-acl)#</pre> | 一致したパケットに必要なアクションを選択します。<br><ul style="list-style-type: none"> <li>• <b>permit-all</b> : 少なくとも 1 つの拡張ヘッダーを持つ IPv6 パケットが許可されます。</li> <li>• <b>deny-all</b> : 少なくとも 1 つの拡張ヘッダーを持つ IPv6 パケットがドロップされます。</li> </ul> |

## システム ACL について

36180YC-R および C3636C-R スイッチでシステム ACL を構成することができます。システム ACL を使用すると、スイッチ内の同じアクセスリストを持つすべてのポートにレイヤ 2 ポート ACL (PACL) を設定できます。システム ACL を設定すると、TCAM の使用率が低下し、ポリシーの適用または変更中に時間とメモリの使用率が低下します。

システム ACL の設定については、次の注意事項と制限事項を参照してください。

- システム PACL は、レイヤ 2 インターフェイスでのみサポートされます。
- ACE 統計情報は、システム ACL ではまだサポートされていません。
- IPv6 は、システム ACL ではまだサポートされていません。
- システム ACL は、ブレイクアウト ポートではサポートされません。
- Cisco Nexus 3600 プラットフォーム スイッチでのサービス品質、ACL、または TCAM カービング構成については、[Cisco Nexus 3600 NX-OS サービス品質構成ガイド](#)を参照してください。

## ACL TCAM リージョン

ハードウェアの ACL Ternary Content Addressable Memory (TCAM) リージョンのサイズを変更できます。

IPv4 TCAM はシングル幅です。

IPv6、ポート ACL、およびルータ ACL を作成でき、QoS の IPv6 アドレスとマッチングできます。Cisco NX-OS は、3 つすべての TCAM を同時にサポートします。これらの新しい IPv6 TCAM を有効にするには、既存の TCAM を削除するか、サイズを小さくする必要があります。

TCAM リージョン サイズには、次の注意事項と制約事項があります。

- デフォルトの ACL TCAM サイズに戻すには、**no hardware access list tcam region** コマンドを使用します。デフォルトのサイズに戻す場合は、モジュールをリロードする必要があります。
- プラットフォームによっては、各 TCAM リージョンの最小/最大/集約サイズ制限が異なる場合があります。
- TCAM の総数は 16 です。
  - 大型 TCAM は 12 あり、それぞれに 160 ビット キー サイズのエントリが 2048 あります。
  - 小型 TCAM は 4 つあり、それぞれに 160 ビット キー サイズのエントリが 256 あります。
- TCAM リージョン RACL v6、QoS、CoPP、およびマルチキャストを 0 に設定することはできません。
- Redirect\_v6、RACL v4 は TCAM を他の機能と共有できません。
- TCAM の切り分け後には、スイッチをリロードする必要があります。
- RACL v6、CoPP、およびマルチキャストにはデフォルトの TCAM サイズがあります。以下の Cisco 3600 ラインカードでは、リロード中にラインカード障害が発生しないように、これらの TCAM サイズをゼロ以外にする必要があります。
  - N3K-C3636C-R
  - N3K-C36180YC-R
- IPv6 RACL は IPv6 IFCAL で部分的に使用できます。これは、Cisco Nexus N3K-C36180YC-R および N3K-C3636C-R ラインカードに適用されます。

表 14: ACL リージョンによる TCAM サイズ

| TCAM ACL リージョン         | デフォルト サイズ |
|------------------------|-----------|
| PACL_IPv4 [ifacl]      | 1024      |
| PACL_IPV6 [ipv6-ifacl] | 1024      |

| TCAM ACL リージョン           | デフォルト サイズ |
|--------------------------|-----------|
| PACL_MAC [mac-ifacl]     | 2048      |
| IPv4 ポート QoS [qos]       | 640       |
| IPv6 ポート QoS [ipv6-qos]  | 256       |
| IPv4 RACL [racl]         | 1024      |
| IPv6 RACL [ipv6-racl]    | 1024      |
| IPv4 L3 QoS [l3qos]      | 640       |
| IPv6 L3 QoS [ipv6-l3qos] | 256       |
| SPAN [span]              | 96        |
| 入力 CoPP [copp]           | 128       |
| リダイレクト v4                | 1024      |
| リダイレクト v6                | 2048      |

## TCAM リージョンの分割

システム ACL を設定する前に、まず TCAM リージョンを分割します。1k 未満の ACL を設定する場合は、TCAM リージョンを分割する必要がないことに注意してください。詳細については、「[ACL TCAM リージョン サイズの設定 \(234 ページ\)](#)」を参照してください。



(注) PACL IPv4、RACL IPv4、および RACL IPv6 が 12k を超えていても構成できます。

## システム ACL の設定

IPv4 ACL を作成したら、システム ACL を設定します。

始める前に

デバイスで IPv4 ACL を作成します。詳細については、「[IP ACL の作成 \(208 ページ\)](#)」を参照してください。

### 手順の概要

1. `config t`
2. `system acl`
3. `ip port access-group <pacl name> in`

## 手順の詳細

## 手順

|        | コマンドまたはアクション                                    | 目的                                                                                                      |
|--------|-------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>config t</b>                                 | コンフィギュレーション モードを開始します。                                                                                  |
| ステップ 2 | <b>system acl</b>                               | システムACLを設定します。                                                                                          |
| ステップ 3 | <b>ip port access-group &lt;acl name&gt; in</b> | インターフェイスにレイヤ 2 PACL を適用します。<br>ポート ACL では、インバウンドフィルタリングだけがサポートされています。1 つのインターフェイスに 1 つのポート ACL を適用できます。 |

## システム ACL の設定および show コマンドの例

システム ACL の show コマンドについては、次の設定例を参照してください。

**1K スケールのシステム PACL の設定（デフォルト TCAM を使用）**

1K スケールのシステム PACL の設定については、次の例を参照してください（デフォルト TCAM を使用）。

ステップ 1 : PACL を作成します。

```
config t
ip access-list PACL-DNA
  10 permit ip 1.1.1.1/32 any
  20 permit tcp 3.0.0.0/8 255.0.0.0 eq 1500
  25 deny udp any any eq 500
  26 deny tcp any eq 490 any
  ....
  1000 deny any any
```

ステップ 2 : PACL をシステム レベルに適用します。

```
configuration terminal
system acl
  ip port access-group PACL-DNA in
```

スイッチに設定されているシステム ACL を検証するには、**sh run aclmgr | sec system** コマンドを使用します。

```
switch# sh run aclmgr | sec system
system acl
  ip port access-group test in
switch#
```

スイッチに設定されている PACL を検証するには、**sh ip access-lists <name> [summary]** コマンドを使用します。

```
switch# sh ip access-lists test

IP access list test
 10 deny udp any any eq 27
 20 permit ip 1.1.1.1/32 100.100.100.100/32
 30 permit ip 1.2.1.1/32 100.100.100.100/32
 40 permit ip 1.3.1.1/32 100.100.100.100/32
 50 permit ip 1.4.1.1/32 100.100.100.100/32
 60 permit ip 1.5.1.1/32 100.100.100.100/32
 70 permit ip 1.6.1.1/32 100.100.100.100/32
 80 permit ip 1.7.1.1/32 100.100.100.100/32
 90 permit ip 1.8.1.1/32 100.100.100.100/32

switch# sh ip access-lists test summary
IPV4 ACL test
Total ACEs Configured: 12279
Configured on interfaces:
Active on interfaces:
  - ingress
  - ingress

switch#
```

PACL IPv4 (ifacl) TCAMリージョンサイズを検証するには、**show hardware access-list tcam region** コマンドを使用します。

```
switch# show hardware access-list tcam region
*****WARNING*****
*****The output shows NFE tcam region info*****
***Please refer to 'show hardware access-list tcam template' for NFE2***
*****
          IPV4 PACL [ifacl] size = 12280
          IPV6 PACL [ipv6-ifacl] size = 0
          MAC PACL [mac-ifacl] size = 0
          IPV4 Port QoS [qos] size = 640
          IPV6 Port QoS [ipv6-qos] size = 256
          MAC Port QoS [mac-qos] size = 0
          FEX IPV4 PACL [fex-ifacl] size = 0
          FEX IPV6 PACL [fex-ipv6-ifacl] size = 0
          FEX MAC PACL [fex-mac-ifacl] size = 0
          FEX IPV4 Port QoS [fex-qos] size = 0
          FEX IPV6 Port QoS [fex-ipv6-qos] size = 0
          FEX MAC Port QoS [fex-mac-qos] size = 0
          IPV4 VACL [vacl] size = 0
          IPV6 VACL [ipv6-vacl] size = 0
          MAC VACL [mac-vacl] size = 0
          IPV4 VLAN QoS [vqos] size = 0
          IPV6 VLAN QoS [ipv6-vqos] size = 0
          MAC VLAN QoS [mac-vqos] size = 0
          IPV4 RACL [racl] size = 0
          IPV6 RACL [ipv6-racl] size = 128
          IPV4 Port QoS Lite [qos-lite] size = 0
          FEX IPV4 Port QoS Lite [fex-qos-lite] size = 0
          IPV4 VLAN QoS Lite [vqos-lite] size = 0
          IPV4 L3 QoS Lite [l3qos-lite] size = 0
          Egress IPV4 QoS [e-qos] size = 0
          Egress IPV6 QoS [e-ipv6-qos] size = 0
          Egress MAC QoS [e-mac-qos] size = 0
```

```

Egress IPV4 VACL [vACL] size = 0
Egress IPV6 VACL [ipv6-vACL] size = 0
Egress MAC VACL [mac-vACL] size = 0
Egress IPV4 RACL [e-rACL] size = 0
Egress IPV6 RACL [e-ipv6-rACL] size = 0
Egress IPV4 QoS Lite [e-qos-lite] size = 0
IPV4 L3 QoS [l3qos] size = 640
IPV6 L3 QoS [ipv6-l3qos] size = 256
MAC L3 QoS [mac-l3qos] size = 0
Ingress System size = 0
Egress System size = 0
SPAN [span] size = 96
Ingress COPP [copp] size = 128
Ingress Flow Counters [flow] size = 0
switch#

```

ACL 関連のテクニカル サポート情報を表示するには、**show tech-support aclmgr** および **show tech-support aclqos** コマンドを使用します。

```

show tech-support aclmgr
show tech-support aclqos

```

## ACL ロギングの構成

### ACL ロギング

Cisco Nexus デバイスは ACL ロギングをサポートしているため、特定のアクセス コントロール リスト (ACL) にヒットするフローをモニターできます。ACL エントリの機能を有効にするには、オプションの **log** キーワードを使用して特定の ACE を構成します。

### ACL ロギング キャッシュの設定

#### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **logging ip access-list cache entries num\_entries**
3. switch(config)# **logging ip access-list cache interval seconds**
4. switch(config)# **logging ip access-list cache threshold num\_packets**
5. (任意) switch(config)# **copy running-config startup-config**

## 手順の詳細

## 手順

|        | コマンドまたはアクション                                                              | 目的                                                                                                            |
|--------|---------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                                         | グローバル コンフィギュレーション モードを開始します。                                                                                  |
| ステップ 2 | switch(config)# <b>logging ip access-list cache entries num_entries</b>   | ソフトウェア内にキャッシュする最大ログエントリ数を設定します。範囲は 0 ～ 1000000 エントリです。デフォルト値は 8000 エントリです。                                    |
| ステップ 3 | switch(config)# <b>logging ip access-list cache interval seconds</b>      | ログの更新の間隔を秒数で設定します。エントリがこの期間非アクティブである場合、そのエントリはキャッシュから削除されます。指定できる範囲は 5 ～ 86400 秒です。デフォルト値は 300 秒です。           |
| ステップ 4 | switch(config)# <b>logging ip access-list cache threshold num_packets</b> | エントリがログに記録されるまでに一致するパケット数を設定します。範囲は 0 ～ 1000000 パケットです。デフォルト値は 0 パケットです。つまり、パケットの一致数によってロギングがトリガーされることはありません。 |
| ステップ 5 | (任意) switch(config)# <b>copy running-config startup-config</b>            | リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。                                            |

## 例

次に、ログ エントリの最大数を 5000、間隔を 120 秒、しきい値を 500000 に設定する例を示します。

```
switch# configure terminal
switch(config)# logging ip access-list cache entries 5000
switch(config)# logging ip access-list cache interval 120
switch(config)# logging ip access-list cache threshold 500000
switch(config)# copy running-config startup-config
```

## インターフェイスへの ACL ロギングの適用

イーサネット インターフェイスおよびポート チャネルに ACL ロギングを適用できます。

## 始める前に

- ACL を作成します。
- ロギング用に設定された少なくとも 1 つのアクセス コントロール エントリ (ACE) で IP アクセス リストを作成します。



- ACL ログイン キャッシュを設定します。
- ACL ログの一致レベルを設定します。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet slot/port**
3. switch(config-if)# **ip access-group name in**
4. (任意) switch(config-if)# **copy running-config startup-config**

### 手順の詳細

#### 手順

|        | コマンドまたはアクション                                                      | 目的                                                                            |
|--------|-------------------------------------------------------------------|-------------------------------------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                                 | グローバル コンフィギュレーション モードを開始します。                                                  |
| ステップ 2 | switch(config)# <b>interface ethernet slot/port</b>               | イーサネット インターフェイスを指定します。                                                        |
| ステップ 3 | switch(config-if)# <b>ip access-group name in</b>                 | 指定されたインターフェイスに ACL とログをアタッチします。ACL ログインは、ACL がハードウェア上のインターフェイスに適用されると有効になります。 |
| ステップ 4 | (任意) switch(config-if)# <b>copy running-config startup-config</b> | リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。            |

#### 例

次に、すべての入力トラフィックに対して acl1 で指定されたログインにイーサネット インターフェイスを適用する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# ip access-group acl1 in
switch(config-if)# copy running-config startup-config
```

## ACL ログの一致レベルの適用

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **acllog match-log-level number**

### 3. (任意) switch(config)# copy running-config startup-config

#### 手順の詳細

#### 手順

|        | コマンドまたはアクション                                                   | 目的                                                                                                                                                                                             |
|--------|----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                              | グローバル コンフィギュレーション モードを開始します。                                                                                                                                                                   |
| ステップ 2 | switch(config)# <b>aclog match-log-level number</b>            | ACL ログ (aclog) で記録されるエントリと一致するようにログ レベルを指定します。number は 0 ～ 7 までの値です。デフォルト値は 6 です。<br><br>(注)<br>ログ メッセージは、ACL ログ ファシリティ (aclog) のログ レベルとログ ファイルのロギング 重大度が、ACL ログの一致ログ レベル設定よりも大きい場合、ログに入力されます。 |
| ステップ 3 | (任意) switch(config)# <b>copy running-config startup-config</b> | リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。                                                                                                                             |

#### 例

次に、ACL ログに記録されるエントリのログ一致レベルを適用する例を示します。

```
switch# configure terminal
switch(config)# aclog match-log-level 3
switch(config)# copy running-config startup-config
```

## ログ ファイルのクリア

ログ ファイルおよび NVRAM のメッセージは表示したり消去したりできます。

#### 手順の概要

#### 1. switch# clear logging ip access-list cache

## 手順の詳細

## 手順

|        | コマンドまたはアクション                                      | 目的                          |
|--------|---------------------------------------------------|-----------------------------|
| ステップ 1 | switch# <b>clear logging ip access-list cache</b> | アクセス制御リスト（ACL）キャッシュをクリアします。 |

## ACL ロギング構成の確認

ACL ロギング構成情報を表示するには、次のいずれかの作業を実行します：

| コマンド                                                      | 目的                                                                                                                                                                   |
|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| switch# <b>show hardware access-list tcam region</b>      | デバイスで次のリロード時に適用される TCAM サイズを表示します。                                                                                                                                   |
| switch# <b>show ip access-lists</b>                       | IPv4 ACL の設定を表示します。                                                                                                                                                  |
| switch# <b>show ipv6 access-lists</b>                     | IPv6 ACL の設定を表示します。                                                                                                                                                  |
| switch# <b>show logging ip access-list cache [detail]</b> | 送信元IPおよび宛先IPアドレス、送信元ポートおよび宛先ポート情報、送信元インターフェイスなど、アクティブなログフローに関する情報を表示します。                                                                                             |
| switch# <b>show logging ip access-list status</b>         | 拒否フローの最大数、現在の有効なログ間隔と現在の有効なしきい値を表示します。                                                                                                                               |
| switch# <b>show startup-config acllog</b>                 | スタートアップ構成のアクセス制御リスト（ACL）ログ ファイルを表示します。                                                                                                                               |
| switch# <b>show startup-config aclmgr [all]</b>           | スタートアップ構成のアクセス制御リスト（ACL）ログ ファイルを表示します。<br><br>(注)<br>このコマンドは、スタートアップ コンフィギュレーションのユーザ設定 ACL を表示します。all オプションを使用すると、スタートアップ構成のデフォルト（CoPP 構成）とユーザ一定義による ACL の両方が表示されます。 |
| switch# <b>show running-config acllog</b>                 | 実行構成のアクセス制御リスト（ACL）ログ ファイルを表示します。                                                                                                                                    |

| コマンド                                            | 目的                                                                                                                                                                                                        |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| switch# <b>show running-config aclmgr [all]</b> | <p>実行構成のアクセス制御リスト（ACL）ログファイルを表示します。IP ACL の構成および IP ACL が適用されるインターフェイスを含みます。</p> <p>（注）<br/>このコマンドは、実行コンフィギュレーションのユーザ設定 ACL を表示します。all オプションを使用すると、スタートアップ構成のデフォルト（CoPP 構成）とユーザー定義による ACL の両方が表示されます。</p> |

## ACL TCAM リージョン サイズの設定

ハードウェアの ACL Ternary Content Addressable Memory（TCAM）リージョンのサイズを変更できます。



（注） 小規模 TCAM（TCAM 12 ～ 15）のサイズは変更できません。

### 手順の概要

1. switch# **configure terminal**
2. **hardware access-list tcam region { ifacl | {ipv6-qos | qos} | {ipv6-racl | racl} tcam\_size**
3. **copy running-config startup-config**
4. switch(config)# **show hardware access-list tcam region**
5. switch(config)# **reload**

### 手順の詳細

#### 手順

|        | コマンドまたはアクション                                                                                      | 目的                                                                                                                                                              |
|--------|---------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                                                                 | グローバル コンフィギュレーション モードを開始します。                                                                                                                                    |
| ステップ 2 | <b>hardware access-list tcam region { ifacl   {ipv6-qos   qos}   {ipv6-racl   racl} tcam_size</b> | <p>ACL TCAM リージョン サイズを変更します。</p> <ul style="list-style-type: none"> <li>• <b>ifacl</b> : インターフェイス ACL (ifacl) TCAM リージョンサイズを設定します。エントリの最大数は 1500 です。</li> </ul> |

|        | コマンドまたはアクション                                                                                                                             | 目的                                                                                                                                                                                                                                                           |
|--------|------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        |                                                                                                                                          | <ul style="list-style-type: none"> <li>• <b>qos</b> : Quality of Service (QoS) TCAM リージョン サイズを設定します。</li> <li>• <b>racl</b> : ルータの ACL (RACL) TCAM リージョン サイズを設定します。</li> <li>• <b>tcam_size</b> : TCAM サイズ。指定できる範囲は 0 ~ 256、512、(256 の倍数) エントリです。</li> </ul> |
| ステップ 3 | <b>copy running-config startup-config</b><br>例 :<br><pre>switch(config)# copy running-config startup-config</pre>                        | リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。                                                                                                                                                                                           |
| ステップ 4 | <pre>switch(config)# show hardware access-list tcam region</pre> 例 :<br><pre>switch(config)# show hardware access-list tcam region</pre> | スイッチの次回のリロード時に適用される TCAM サイズを表示します。                                                                                                                                                                                                                          |
| ステップ 5 | <pre>switch(config)# reload</pre> 例 :<br><pre>switch(config)# reload</pre>                                                               | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。<br><br>(注)<br><b>copy running-config to startup-config</b> を保存した後、次回のリロード時に新しいサイズ値が有効になります。                                                                                                                        |

## 例

次に、RACL TCAM リージョンのサイズを変更する例を示します。

```
switch(config)# hardware access-list tcam region racl 256
[SUCCESS] New tcam size will be applicable only at boot time.
You need to 'copy run start' and 'reload'
```

```
switch(config)# copy running-config startup-config
switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y
```

次に、変更を確認するために、TCAM リージョンのサイズを表示する例を示します。

```
switch(config)# show hardware accesslist tcam region | exclude "0"
```

```

      IPV4 PACL [ifacl] size = 1024
    IPV6 PACL [ipv6-ifacl] size = 1024
      MAC PACL [mac-ifacl] size = 2048
    IPV4 Port QoS [qos] size = 640
```

```

IPV6 Port QoS [ipv6-qos] size = 256
  IPV4 RACL [racl] size = 2048
  IPV6 RACL [ipv6-racl] size = 1024
  IPV4 L3 QoS [l3qos] size = 640
  IPV6 L3 QoS [ipv6-l3qos] size = 256
    SPAN [span] size = 96
  Ingress COPP [copp] size = 128
    Redirect v4 size = 1024
    Redirect v6 size = 2048

```

## デフォルトの TCAM リージョン サイズに戻す

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **no hardware profile tcam region {arpacl | e-racl} | ifacl | | nat | qos} | qoslbl | racl} | vacl } tcam\_size**
3. (任意) switch(config)# **copy running-config startup-config**
4. switch(config)# **reload**

### 手順の詳細

#### 手順

|        | コマンドまたはアクション                                                                                                                        | 目的                                               |
|--------|-------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                                                                                                   | グローバル コンフィギュレーション モードを開始します。                     |
| ステップ 2 | switch(config)# <b>no hardware profile tcam region {arpacl   e-racl}   ifacl     nat   qos}   qoslbl   racl}   vacl } tcam_size</b> | デフォルト ACL TCAM サイズに設定を戻します。                      |
| ステップ 3 | (任意) switch(config)# <b>copy running-config startup-config</b>                                                                      | リブートおよびリスタート時に実行構成をスタートアップ構成にコピーして、変更を継続的に保存します。 |
| ステップ 4 | switch(config)# <b>reload</b>                                                                                                       | スイッチをリロードします。                                    |

### 例

次に、デフォルトの RACL TCAM リージョンのサイズに戻す例を示します。

```

switch(config)# no hardware profile tcam region racl 256
[SUCCESS] New tcam size will be applicable only at boot time.
You need to 'copy run start' and 'reload'

```

```

switch(config)# copy running-config startup-config
switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y

```

## 仮想端末回線の ACL の設定

仮想端末（VTY）回線とアクセス リストのアドレス間の IPv4 の着信接続と発信接続を制限するには、ライン コンフィギュレーション モードで **access-class** コマンドを使用します。アクセス制限を解除するには、このコマンドの **no** 形式を使用します。

VTY 回線で ACL を設定する場合には、次のガイドラインに従ってください。

- すべての VTY 回線にユーザーが接続できるため、すべての VTY 回線に同じ制約を設定する必要があります。
- エントリ単位の統計情報は、VTY 回線の ACL ではサポートされません。

### 始める前に

適用する ACL が存在しており、この適用に対してトラフィックをフィルタリングするように設定されていることを確認してください。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **line vty**
3. switch(config-line)# **access-class access-list-number {in | out}**
4. （任意） switch(config-line)# **no access-class access-list-number {in | out}**
5. switch(config-line)# **exit**
6. （任意） switch# **show running-config aclmgr**
7. （任意） switch# **copy running-config startup-config**

### 手順の詳細

#### 手順

|        | コマンドまたはアクション                                                                                   | 目的                           |
|--------|------------------------------------------------------------------------------------------------|------------------------------|
| ステップ 1 | switch# <b>configure terminal</b>                                                              | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | switch(config)# <b>line vty</b><br><br>例 :<br>switch(config)# line vty<br>switch(config-line)# | ライン コンフィギュレーション モードを開始します。   |
| ステップ 3 | switch(config-line)# <b>access-class access-list-number {in   out}</b><br><br>例 :              | 着信または発信アクセス制限を指定します。         |

|        | コマンドまたはアクション                                                                                                                                                                                                       | 目的                                        |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
|        | <pre>switch(config-line)# access-class ozi2 in switch(config-line)#access-class ozi3 out switch(config)#</pre>                                                                                                     |                                           |
| ステップ 4 | (任意) switch(config-line)# <b>no access-class access-list-number {in   out}</b><br><br>例 :<br><pre>switch(config-line)# no access-class ozi2 in switch(config-line)# no access-class ozi3 out switch(config)#</pre> | 着信または発信アクセス制限を削除します。                      |
| ステップ 5 | <pre>switch(config-line)# exit</pre><br>例 :<br><pre>switch(config-line)# exit switch#</pre>                                                                                                                        | ライン コンフィギュレーション モードを終了します。                |
| ステップ 6 | (任意) switch# <b>show running-config aclmgr</b><br><br>例 :<br><pre>switch# show running-config aclmgr</pre>                                                                                                         | スイッチの ACL の実行コンフィギュレーションを表示します。           |
| ステップ 7 | (任意) switch# <b>copy running-config startup-config</b><br><br>例 :<br><pre>switch# copy running-config startup-config</pre>                                                                                         | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。 |

### 例

次に、VTY 回線の in 方向に access-class ozi2 のコマンドを適用する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# line vty
switch(config-line)# access-class ozi2 in
switch(config-line)# exit
switch#
```

## VTY 回線の ACL の確認

VTY 回線の ACL 設定を表示するには、次のいずれかの作業を行います。

| コマンド                                      | 目的                                   |
|-------------------------------------------|--------------------------------------|
| <b>show running-config aclmgr</b>         | スイッチで設定された ACL の実行コンフィギュレーションを表示します。 |
| <b>show users</b>                         | 接続されているユーザーを表示します。                   |
| <b>show access-lists access-list-name</b> | エントリ単位の統計情報を表示します。                   |



## VTY 回線の ACL の設定例

次に、コンソール回線（ttyS0）および VTY 回線（pts/0 および pts/1）の接続ユーザーの例を示します。

```
switch# show users
NAME      LINE      TIME          IDLE          PID COMMENT
admin     ttyS0     Aug 27 20:45   .             14425 *
admin     pts/0     Aug 27 20:06 00:46        14176 (172.18.217.82) session=ssh
admin     pts/1     Aug 27 20:52   .             14584 (10.55.144.118)
```

次に、172.18.217.82 を除き、すべての IPv4 ホストへの VTY 接続を許可する例と、10.55.144.118、172.18.217.79、172.18.217.82、172.18.217.92 を除き、すべての IPv4 ホストへの VTY 接続を拒否する例を示します。

```
switch# show running-config aclmgr
!Time: Fri Aug 27 22:01:09 2010
version 5.0(2)N1(1)
ip access-list ozi
  10 deny ip 172.18.217.82/32 any
  20 permit ip any any
ip access-list ozi2
  10 permit ip 10.55.144.118/32 any
  20 permit ip 172.18.217.79/32 any
  30 permit ip 172.18.217.82/32 any
  40 permit ip 172.18.217.92/32 any

line vty
  access-class ozi in
  access-class ozi2 out
```

次に、ACL のエントリ単位の統計情報をイネーブルにして、IP アクセス リストを設定する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
switch(config)# ip access-list ozi2
switch(config-acl)# statistics per-entry
switch(config-acl)# deny tcp 172.18.217.83/32 any
switch(config-acl)# exit

switch(config)# ip access-list ozi
switch(config-acl)# statistics per-entry
switch(config-acl)# permit ip 172.18.217.20/24 any
switch(config-acl)# exit
switch#
```

次に、in および out 方向で VTY の ACL を適用する例を示します。

```
switch(config)# line vty
switch(config-line)# ip access-class ozi in
switch(config-line)# access-class ozi2 out
switch(config-line)# exit
switch#
```

次に、VTY 回線でアクセス制限を削除する例を示します。

```
switch# configure terminal
```

```
Enter configuration commands, one per line. End
with CNTL/Z.
switch(config)# line vty
switch(config-line)# no access-class ozi2 in
switch(config-line)# no ip access-class ozi2 in
switch(config-line)# exit
switch#
```



## 第 10 章

# ユニキャスト RPF の設定

この章は、次の項で構成されています。

- [ユニキャスト RPF の概要, on page 241](#)
- [ユニキャスト RPF の注意事項と制約事項 \(243 ページ\)](#)
- [ユニキャスト RPF のデフォルト設定, on page 245](#)
- [ユニキャスト RPF の設定, on page 245](#)
- [ユニキャスト RPF の設定例, on page 247](#)
- [ユニキャスト RPF の設定の確認, on page 247](#)
- [ユニキャスト RPF に関する追加情報 \(248 ページ\)](#)

## ユニキャスト RPF の概要

ユニキャスト RPF 機能を使用すると、ネットワークに改変または偽造（スプーフィング）された IPv4 ソース アドレスが注入されて引き起こされる問題を、検証可能な IP ソース アドレスを持たない IPv4 パケットを廃棄することにより緩和します。たとえば、Smurf や Tribal Flood Network (TFN) など、いくつかの一般的なサービス拒絶 (DoS) 攻撃は、偽造の送信元 IPv4 または IPv6 アドレスやすぐに変更される送信元 IPv4 または IPv6 アドレスを利用して、攻撃を突き止めたりフィルタリングしたりする手段を妨ぐことができます。ユニキャスト RPF では、送信元アドレスが有効で IP ルーティング テーブルと一致するパケットだけを転送することにより、攻撃を回避します。

インターフェイス上でユニキャスト RPF を有効にすると、はそのインターフェイス上で受信されたすべての入力パケットを検証することにより、送信元アドレスと送信元インターフェイスがルーティング テーブル内に存在しており、さらにパケット受信場所のインターフェイスとマッチすることを確認します。この送信元アドレス検査は転送情報ベース (FIB) に依存しています。

ユニキャスト RPF は、FIB のリバース ルックアップを実行することにより、インターフェイスでの受信パケットがそのパケットの送信元への最良リターンパス（リターンルート）で着信していることを確認します。パケットが最適なリバース パス ルートのいずれかから受信された場合、パケットは通常どおりに転送されます。パケットを受信したインターフェイス上にリバース パス ルートがない場合、攻撃者によって送信元アドレスが変更される可能性があります。

ます。ユニキャスト RPF がそのパケットのリバース パスを見つけられない場合は、パケットはドロップされます。

**Note**

ユニキャスト RPF では、コストが等しいすべての「最良」リターン パスが有効と見なされます。つまり、複数のリターン パスが存在していても、各パスのルーティング コスト（ホップ カウントや重みなど）が他のパスと等しく、そのルートが FIB 内にある限り、ユニキャスト RPF は機能します。ユニキャスト RPF は、Enhanced Interior Gateway Routing Protocol (EIGRP) バリエーションが使用されていて、送信元 IP アドレスに戻る同等でない候補パスが存在する場合にも機能します。

## ユニキャスト RPF プロセス

ユニキャスト RPF には、キーの実装原則がいくつかあります。

- パケットは、パケットの送信元に対する最適なリターン パス（ルート）があるインターフェイスで受信される必要があります（このプロセスは対称ルーティングと呼ばれます）。FIB に受信インターフェイスへのルートと一致するルートが存在する必要があります。スタティック ルート、ネットワーク文、ダイナミック ルーティングによって FIB にルートが追加されます。
- 受信側インターフェイスでの IP 送信元アドレスは、そのインターフェイスのルーティング エントリと一致する必要があります。
- ユニキャスト RPF は入力機能であり、接続のアップストリーム エンドのデバイスの入力インターフェイスだけに適用されます。

ダウンストリームネットワークにインターネットへの他の接続があっても、ダウンストリームネットワークにユニキャスト RPF を使用できます。

**Caution**

攻撃者が送信元アドレスへの最良パスを変更する可能性があるため、加重やローカルプリファレンスなどのオプションの BGP 属性を使用する際には、十分に注意してください。変更によって、ユニキャスト RPF の操作に影響が出ます。

ユニキャスト RPF と ACL を設定したインターフェイスでパケットが受信されると、Cisco NX-OS ソフトウェアは次の動作を行います。

### Procedure

**ステップ 1** インバウンドインターフェイスで入力 ACL をチェックします。

**ステップ 2** ユニキャスト RPF を使用し、FIB テーブル内のリバース ルックアップを実行することにより、そのパケットが送信元への最良リターン パスで着信したことを確認します。

**ステップ3** パケットの転送を目的として FIB ルックアップを実行します。

**ステップ4** アウトバウンドインターフェイスで出力 ACL をチェックします。

**ステップ5** パケットを転送します。

## グローバル統計

Cisco NX-OS デバイスがユニキャスト RPF チェックの失敗によりインターフェイスでパケットをドロップするたびに、その情報が転送エンジン (FE) 単位でデバイスにおいてグローバルにカウントされます。ドロップされたパケットのグローバル統計からは、ネットワーク上での攻撃の可能性に関する情報を得ることができますが、攻撃の送信元となるインターフェイスは特定されません。ユニキャスト RPF チェックの失敗によりドロップされたパケットのインターフェイス単位の統計情報は利用できません。

## ユニキャスト RPF の注意事項と制約事項

ユニキャスト RPF (uRPF) に関する注意事項と制約事項は次のとおりです。

- uRPF は、ネットワーク内のより大きな部分からのダウンストリームのインターフェイスで適用する必要があります (ネットワークのエッジに適用するのが望ましい)。
- なるべくダウンストリームで uRPF を適用する方が、アドレス スプーフィングの軽減やスプーフされたアドレスの送信元の特定の精度が高くなります。たとえば、集約デバイスで uRPF を適用すると、多くのダウンストリーム ネットワークまたはクライアントからの攻撃を軽減できるとともに、管理が簡単になりますが、攻撃の送信元は特定できません。ネットワーク アクセス サーバに uRPF を適用すると、攻撃の範囲を絞り、攻撃元を追跡しやすくなります。ただし、多数のサイトにユニキャスト RPF を展開すると、ネットワーク運用の管理コストが増加します。
- インターネット、イントラネット、およびエクストラネットのリソース全体で uRPF を展開するエンティティが多いほど、インターネット コミュニティを通じた大規模なネットワークの中断が軽減される可能性が高くなり、攻撃の送信元をトレースできる可能性も高くなります。
- uRPF は、汎用ルーティング カプセル化 (GRE) トンネルのようなトンネルでカプセル化された IP パケットは検査しません。トンネリングとカプセル化のレイヤがパケットから除かれてから uRPF がネットワーク トラフィックを処理するように、uRPF はホーム ゲートウェイに設定する必要があります。
- uRPF は、ネットワークからのアクセス ポイントが 1 つだけ、またはアップストリーム接続が 1 つだけの「単一ホーム」環境で使用できます。アクセス ポイントが 1 つのネットワークは対称ルーティングを提供します。これはつまり、パケットがネットワークに入るインターフェイスはその IP パケットの送信元への最良のリターン パスでもあるということです。

- uRPF をネットワーク内部のインターフェイスに使用しないでください。内部インターフェイスは、ルーティングを非対称にする可能性が高く、パケットの送信元へのルートが複数存在する場合があります。uRPF を設定するのは、元々対称であるか、対称に設定されている場合だけにしてください。厳密な uRPF を構成しないでください。
- uRPF を使用すると、送信元が 0.0.0.0 で宛先が 255.255.255.255 のパケットを通過させて、ブートストラップ プロトコル (BOOTP) と Dynamic Host Configuration Protocol (DHCP) を正しく動作させることができます。
- uRPF が有効になっている場合、IPv4 と IPv6 の両方にルーズモードが適用されます。ただし、プロトコルごとに厳密モードを適用することはできません。
- 厳密な uRPF を機能させるには、入力インターフェイスと、送信元 IP アドレスを学習したインターフェイスの両方で有効にします。
- スイッチハードウェアは、設定されたルーティングインターフェイスごとに厳密な uRPF を実装しません。
- 厳密な uRPF は、厳密な uRPF 対応インターフェイスの学習ルートごとに実装されます。
- ルートが ECMP として解決されると、厳密な uRPF はルーズモードにフォールバックします。
- トラップ解決に関するハードウェアの制限により、uRPF はインバンド経由でスーパーバイザ宛パケットに適用されない場合があります。
- IP トラフィックの場合は、IPv4 と IPv6 の構成を同時に有効にするべきです。
- ハードウェアの制限により、Cisco Nexus 3600 シリーズ スイッチは次の組み合わせのみをサポートします：

| uRPF の設定 |        | 送信元 IP アドレスのトラフィックチェックの適用 |            |                     |
|----------|--------|---------------------------|------------|---------------------|
| IPv4     | IPv6   | IP Unipath                | IP ECMP    | MPLS Encap/VPN/ECMP |
| 無効       | 無効     | 許可                        | 許可         | 許可                  |
| Loose    | Loose  | uRPF loose                | uRPF loose | uRPF loose          |
| Strict   | Strict | uRPF strict               | uRPF loose | uRPF loose          |

## ユニキャスト RPF のデフォルト設定

次の表に、ユニキャスト RPF パラメータのデフォルト設定を示します。

**Table 15:** ユニキャスト RPF パラメータのデフォルト設定

| パラメータ      | デフォルト  |
|------------|--------|
| ユニキャスト RPF | ディセーブル |

## ユニキャスト RPF の設定

入力インターフェイスでは、厳密なユニキャスト RPF モードまたは緩やかなユニキャスト RPF モードを構成できます。厳密なユニキャスト モードでは、送信元 IP がアタッチされているインターフェイスに構成を適用します。これにより、特定の送信元の許可リストを構成できます。

### ストリクト ユニキャスト RPF モード

厳格モードでは、ユニキャスト RPF が FIB で一致するパケット送信元アドレスを見つけて、パケットを受信した入力インターフェイスが FIB 内のユニキャスト RPF インターフェイスのいずれかと一致した場合に、チェックに合格します。チェックに合格しないと、パケットは廃棄されます。このタイプのユニキャスト RPF チェックは、パケット フローが対称であると予想される場合に使用できます。

### ルーズ ユニキャスト RPF モード

緩和モードでは、FIB でのパケット送信元アドレスのルックアップで一致が戻り、FIB の結果からその送信元が少なくとも 1 つの実インターフェイスで到達可能であることが示された場合に、チェックに合格します。パケットを受信する入力インターフェイスが、FIB 内のインターフェイスのいずれかと一致する必要はありません。

### SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet slot/port**
3. **{ip | ipv6} verify unicast source reachable-via any**
4. **exit**
5. (Optional) **show ip interface ethernet slot/port**
6. (Optional) **show running-config interface ethernet slot/port**
7. (Optional) **copy running-config startup-config**

## DETAILED STEPS

## Procedure

|        | Command or Action                                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>                                                     | グローバル コンフィギュレーション モードを開始します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| ステップ 2 | <b>interface ethernet slot/port</b><br><b>Example:</b><br><pre>switch(config)# interface ethernet 2/3 switch(config-if)#</pre>                            | イーサネットインターフェイスを指定し、インターフェイス構成モードを開始します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| ステップ 3 | <b>{ip   ipv6} verify unicast source reachable-via any</b><br><b>Example:</b><br><pre>switch(config-if)# ip verify unicast source reachable-via any</pre> | <p>IPv4 と IPv6 の両方に対するインターフェイスでユニキャスト RPF を設定します。</p> <p><b>Note</b><br/>ユニキャスト RPF はデフォルトで無効になっているため、各インターフェイスで構成します。構成は、IPv4 と IPv6 の両方で共有されます。IPv4 と IPv6 のいずれかで有効または無効にすると、そのインターフェイス上のすべてのプロトコルに影響します。</p> <p><b>Note</b><br/>IPv4 または IPv6 の uRPF を有効にすると（<b>ip</b> または <b>ipv6</b> キーワードを使用）、ユニキャスト RPF は IPv4 と IPv6 の両方で有効になります。</p> <p><b>Note</b><br/>インターフェイスで利用できる IPv4 および IPv6 ユニキャスト RPF コマンドのバージョンは 1 つだけです。1 つのバージョンを設定する場合、すべてのモード変更をこのバージョンで行う必要があります。インターフェイスは、他のすべてのバージョンをブロックします。</p> |
| ステップ 4 | <b>exit</b><br><b>Example:</b><br><pre>switch(config-cmap)# exit switch(config)#</pre>                                                                    | クラスマップ コンフィギュレーション モードを終了します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| ステップ 5 | <b>(Optional) show ip interface ethernet slot/port</b><br><b>Example:</b><br><pre>switch(config)# show ip interface ethernet 2/3</pre>                    | インターフェイスの IP 情報を表示し、ユニキャスト RPF が有効かどうかを確認します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                |



|        | Command or Action                                                                                                                                                  | Purpose                                   |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| ステップ 6 | (Optional) <b>show running-config interface ethernet slot/port</b><br><br><b>Example:</b><br><pre>switch(config)# show running-config interface ethernet 2/3</pre> | 実行コンフィギュレーション内のインターフェイスの情報を表示します。         |
| ステップ 7 | (Optional) <b>copy running-config startup-config</b><br><br><b>Example:</b><br><pre>switch(config)# copy running-config startup-config</pre>                       | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。 |

## ユニキャスト RPF の設定例

次に、緩和モードの IPv4/IPv6 パケット用ユニキャスト RPF の構成例を示します。

- ```
interface Ethernet2/3
ip address 172.23.231.240/23
ip verify unicast source reachable-via any
```
- ```
interface Ethernet2/3
ipv6 address 2001:0DB8:c18:1::3/64
ipv6 verify unicast source reachable-via any
```

次に、厳密モードの IPv4/IPv6 パケット用ユニキャスト RPF の構成例を示します。

- ```
interface Ethernet2/2
ip address 172.23.231.240/23
ip verify unicast source reachable-via rx
```
- ```
interface Ethernet2/2
ipv6 address 2001:0DB8:c18:1::3/64
ipv6 verify unicast source reachable-via rx
```

## ユニキャスト RPF の設定の確認

ユニキャスト RPF の設定情報を表示するには、次のいずれかの作業を行います。

| コマンド                                                    | 目的                                |
|---------------------------------------------------------|-----------------------------------|
| <b>show running-config interface ethernet slot/port</b> | 実行コンフィギュレーション内のインターフェイスの設定を表示します。 |
| <b>show running-config ip [all]</b>                     | 実行コンフィギュレーション内の IPv4 設定を表示します。    |

| コマンド                                                    | 目的                                            |
|---------------------------------------------------------|-----------------------------------------------|
| <b>show running-config ip6 [all]</b>                    | 実行コンフィギュレーション内の IPv6 設定を表示します。                |
| <b>show startup-config interface ethernet slot/port</b> | スタートアップ コンフィギュレーション内のインターフェイスの設定を表示します。       |
| <b>show ip interface ethernet slot/port</b>             | インターフェイスの IP 情報を表示し、ユニキャスト RPF が有効か無効かを確認します。 |
| <b>show startup-config ip</b>                           | スタートアップ コンフィギュレーション内の IP 設定を表示します。            |

## ユニキャスト RPF に関する追加情報

ここでは、ユニキャスト RPF の実装に関する追加情報について説明します。

### 関連資料

| 関連項目        | マニュアル タイトル                                                    |
|-------------|---------------------------------------------------------------|
| MPLS<br>VPN | <a href="#">Cisco Nexus 3600 シリーズ NX-OS レイヤ 2 スイッチング構成ガイド</a> |



## 第 11 章

# コントロールプレーンポリシングの設定

この章は、次の項で構成されています。

- [CoPP について, on page 249](#)
- [CoPP の注意事項と制約事項 \(267 ページ\)](#)
- [CoPP のデフォルト設定, on page 270](#)
- [CoPP の設定, on page 270](#)
- [CoPP の設定の確認, on page 279](#)
- [CoPP 設定ステータスの表示, on page 282](#)
- [CoPP のモニタリング, on page 282](#)
- [CoPP 統計情報のクリア, on page 283](#)
- [CoPP の設定例, on page 284](#)
- [CoPP に関する追加情報, on page 286](#)

## CoPP について

コントロールプレーンポリシング (CoPP) はコントロールプレーンを保護し、それをデータプレーンから分離することによって、ネットワークの安定性、到達可能性、およびパケット配信を保証します。

この機能により、コントロールプレーンにポリシーマップを適用できるようになります。このポリシーマップは、通常の QoS ポリシーに似ており、非管理ポートからスイッチに入るすべてのトラフィックに適用されます。ネットワークデバイスへの一般的な攻撃ベクトルは、過剰なトラフィックがデバイスインターフェイスに転送されるサービス妨害 (DoS) 攻撃です。

Cisco NX-OS デバイスは、DoS 攻撃がパフォーマンスに影響しないようにするために CoPP を提供します。このような攻撃は誤って、または悪意を持って実行される場合があります。通常は、スーパーバイザ モジュールまたは CPU 自体に宛てられた大量のトラフィックが含まれます。

スーパーバイザ モジュールは、管理対象のトラフィックを次の 3 つの機能コンポーネント (プレーン) に分類します。

### データ プレーン

すべてのデータトラフィックを処理します。NX-OS デバイスの基本的な機能は、インターフェイス間でパケットを転送することです。スイッチ自身に向けられたものでないパケッ

トは、中継パケットと呼ばれます。データプレーンで処理されるのはこれらのパケットです。

### コントロールプレーン

ルーティングプロトコルのすべての制御トラフィックを処理します。ボーダーゲートウェイプロトコル（BGP）や Open Shortest Path First（OSPF）プロトコルなどのルーティングプロトコルは、デバイス間で制御パケットを送信します。これらのパケットはルータのアドレスを宛先とし、コントロールプレーンパケットと呼ばれます。

### 管理プレーン

コマンドラインインターフェイス（CLI）や簡易ネットワーク管理プロトコル（SNMP）など、NX-OS デバイスを管理する目的のコンポーネントを実行します。

スーパーバイザモジュールには、管理プレーンとコントロールプレーンの両方が搭載され、ネットワークの運用にクリティカルなモジュールです。スーパーバイザモジュールの動作が途絶したり、スーパーバイザモジュールが攻撃されたりすると、重大なネットワークの停止につながります。たとえばスーパーバイザに過剰なトラフィックが加わると、スーパーバイザモジュールが過負荷になり、NX-OS デバイス全体のパフォーマンスが低下する可能性があります。たとえば、スーパーバイザモジュールに対する DoS 攻撃は、コントロールプレーンに対して非常に高速に IP トラフィックストリームを生成することがあります。これにより、コントロールプレーンは、これらのパケットを処理するために大量の時間を費やしてしまい、本来のトラフィックを処理できなくなります。

DoS 攻撃の例は次のとおりです。

- インターネット制御メッセージプロトコル（ICMP）エコー要求
- IP フラグメント
- TCP SYN フラッディング

これらの攻撃によりデバイスのパフォーマンスが影響を受け、次のようなマイナスの結果をもたらします。

- サービス品質の低下（音声、ビデオ、または重要なアプリケーショントラフィックの低下など）
- ルートプロセッサまたはスイッチプロセッサの高い CPU 使用率
- ルーティングプロトコルのアップデートまたはキープアライブの消失によるルートフラップ
- 不安定なレイヤ 2 トポロジ
- CLI との低速な、または応答を返さない対話型セッション
- メモリやバッファなどのプロセッサリソースの枯渇
- 着信パケットの無差別のドロップ

**Caution**

コントロールプレーンの保護策を講じることで、スーパーバイザ モジュールを偶発的な攻撃や悪意ある攻撃から確実に保護することが重要です。

## コントロールプレーン保護

コントロールプレーンを保護するために、Cisco NX-OS デバイスはコントロールプレーンに向かうさまざまなパケットを異なるクラスに分離します。クラスの識別が終わると、Cisco NX-OS デバイスはパケットをポリシングします。これにより、スーパーバイザ モジュールに過剰な負担がかからないようになります。

### コントロールプレーンのパケット タイプ

コントロールプレーンには、次のような異なるタイプのパケットが到達します。

#### 受信パケット

ルータの宛先アドレスを持つパケット。宛先アドレスには、レイヤ 2 アドレス（ルータ MAC アドレスなど）やレイヤ 3 アドレス（ルータ インターフェイスの IP アドレスなど）があります。これらのパケットには、ルータ アップデートとキープアライブ メッセージも含まれます。ルータが使用するマルチキャストアドレス宛てに送信されるマルチキャストパケットも、このカテゴリに入ります。

#### 例外パケット

スーパーバイザモジュールによる特殊な処理を必要とするパケット。たとえば、宛先アドレスが Forwarding Information Base（FIB; 転送情報ベース）に存在せず、結果としてミスとなった場合は、スーパーバイザモジュールが送信側に到達不能パケットを返します。他には、IP オプションがセットされたパケットもあります。

次の例外は、ラインカードからのみ発生する可能性があります。

- match exception ip option
- match exception ipv6 option
- match exception ttl-failure

次の例外は、ファブリック モジュールからのみ発生する可能性があります。

- match exception ipv6 icmp unreachable
- match exception ip icmp unreachable

次の例外は、ラインカードとファブリック モジュールから発生する可能性があります。

- match exception mtu-failure

#### リダイレクトパケット

スーパーバイザ モジュールにリダイレクトされるパケット。

#### 収集パケット

宛先 IP アドレスのレイヤ 2 MAC アドレスが FIB に存在していない場合は、スーパーバイザ モジュールがパケットを受信し、ARP 要求をそのホストに送信します。

これらのさまざまなパケットはすべて、コントロールプレーンへの悪意ある攻撃に利用され、Cisco NX-OS デバイスに過剰な負荷をかける可能性があります。CoPP は、これらのパケットを異なるクラスに分類し、これらのパケットをスーパーバイザが受信する速度を個別に制御するメカニズムを提供します。

## CoPP の分類

効果的に保護するために、Cisco NX-OS デバイスはスーパーバイザ モジュールに到達するパケットを分類して、パケットタイプに基づいた異なるレート制御ポリシーを適用できるようにします。たとえば、Hello メッセージなどのプロトコルパケットには厳格さを緩め、IP オプションがセットされているためにスーパーバイザモジュールに送信されるパケットには厳格さを強めることが考えられます。クラスマップとポリシー マップを使用して、パケットの分類およびレート制御ポリシーを設定します。

## レート制御メカニズム

パケットの分類が終わると、Cisco NX-OS デバイスにはスーパーバイザモジュールに到達するパケットのレートを制御するメカニズムがあります。スーパーバイザモジュールへのトラフィックのレート制御には 2 つのメカニズムを使用します。1 つはポリシング、もう 1 つはレート制限と呼ばれるものです。

ハードウェアポリサーを使用すると、トラフィックが所定の条件に一致する場合、または違反する場合について異なるアクションを定義できます。このアクションには、パケットの送信、パケットのマーク付け、およびパケットのドロップがあります。

ポリシングには、次のパラメータを設定できます。

### 認定情報レート (CIR)

望ましい帯域幅を、ビット レート、またはリンク レートの割合として指定します。

### 認定バースト (BC)

指定した時間枠内に CIR を超過する可能性があるが、スケジューリングには影響を与えないトラフィック バーストのサイズ。

さらに、一致トラフィックおよび違反トラフィックに対して、送信またはドロップなどの異なるアクションを設定できます。

ポリシング パラメータの詳細については、『Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide』を参照してください。

## ダイナミックおよびスタティック CoPP ACL

CoPP アクセスコントロールリスト (ACL) は、ダイナミックまたはスタティックに分類されます。Cisco Nexus 9300 および 9500 シリーズ、3164Q、31128PQ、3232C、および 3264Q スイッチは、ダイナミック CoPP ACL のみを使用します。Cisco Nexus 9200 シリーズ スイッチは、ダイナミック CoPP ACL とスタティック CoPP ACL の両方を使用します。

ダイナミック CoPP ACL は、転送情報ベース (FIB) ベースのスーパーバイザリダイレクトパケットに対してのみ機能し、スタティック CoPP ACL は ACL ベースのスーパーバイザリダイレクトパケットに対してのみ機能します。ダイナミック CoPP ACL は myIP およびリンク ロー

カル マルチキャスト トラフィックでサポートされ、スタティック CoPP ACL は他のすべてのタイプのトラフィックでサポートされます。

スタティック CoPP ACL は、サブストリングによって識別されます。これらのサブストリングのいずれかを持つ ACL は、スタティック CoPP ACL として分類されます。

- MAC ベースのスタティック CoPP ACL サブストリング：
  - acl-mac-cdp-udld-vtp
  - acl-mac-cfsoe
  - acl-mac-dot1x
  - acl-mac-l2-tunnel
  - acl-mac-l3-isis
  - acl-mac-lacp
  - acl-mac-lldp
  - acl-mac-sdp-srp
  - acl-mac-stp
  - acl-mac-undesirable
- プロトコルベースのスタティック CoPP ACL サブストリング：
  - acl-dhcp
  - acl-dhcp-relay-response
  - acl-dhcp6
  - acl-dhcp6-relay-response
  - acl-ptp
- マルチキャストベースのスタティック CoPP ACL サブストリング：
  - acl-igmp

スタティック CoPP ACL の詳細については、[CoPP の注意事項と制約事項（267 ページ）](#) を参照してください。

## デフォルトのポリシングポリシー

Cisco NX-OS デバイスの初回起動時には、DoS 攻撃からスーパーバイザ モジュールを保護するためのデフォルトの `copp-system-p-policy-strict` ポリシーが Cisco NX-OS ソフトウェアによってインストールされます。最初のセットアップ ユーティリティで、次のいずれかの CoPP ポリシー オプションを選択することにより、保護レベルを設定できます。

- Strict：このポリシーは 1 レート、2 カラーです。

- **Moderate** : このポリシーは1レート、2カラーです。重要クラスのバーストサイズは **strict** ポリシーより大きく、**lenient** ポリシーより小さくなります。
- **Lenient** : このポリシーは1レート、2カラーです。重要クラスのバーストサイズは **moderate** ポリシーより大きく、**dense** ポリシーより小さくなります。
- **Dense** : このポリシーは1レート、2カラーです。ポリサーの CIR 値は、**strict** ポリシーよりも低くなります。
- **Skip** : コントロールプレーン ポリシーは適用されません。（ネットワークのコントロールプレーンに影響するため、**Skip** オプションの使用は推奨されません）。

オプションを選択しなかった場合や、セットアップユーティリティを実行しなかった場合には、**strict** ポリシングが適用されます。**strict** ポリシーから開始し、必要に応じて、**CoPP** ポリシーを変更することを推奨します。



**Note** POAPを使用する場合、デフォルトでは厳格なポリシングは適用されないため、**CoPP** ポリシーを設定する必要があります。

**copp-system-p-policy** ポリシーには、基本的なデバイス操作に最も適した値が設定されています。使用する **DoS** に対する保護要件に適合するよう、特定のクラスやアクセス コントロール リスト (ACL) を追加する必要があります。デフォルト **CoPP** ポリシーは、ソフトウェアをアップグレードしても変更されません。



**Caution** **skip** オプションを選択し、その後に **CoPP** 保護を設定していない場合、Cisco NX-OS デバイスは **DoS** 攻撃に対して脆弱な状態になります。

CLI プロンプトから **setup** コマンドを実行して再度セットアップユーティリティを起動するか、または **copp profile** コマンドを使用して、**CoPP** のデフォルト ポリシーを再割り当てできます。

## Default Class Maps

**copp-system-class-critical** クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-critical
  match access-group name copp-system-p-acl-bgp
  match access-group name copp-system-p-acl-rip
  match access-group name copp-system-p-acl-vpc
  match access-group name copp-system-p-acl-bgp6
  match access-group name copp-system-p-acl-ospf
  match access-group name copp-system-p-acl-rip6
  match access-group name copp-system-p-acl-eigrp
  match access-group name copp-system-p-acl-ospf6
  match access-group name copp-system-p-acl-eigrp6
  match access-group name copp-system-p-acl-auto-rp
  match access-group name copp-system-p-acl-mac-l3-isis
```

**copp-system-class-exception** クラスの設定は次のとおりです。



```
class-map type control-plane match-any copp-system-p-class-exception
  match exception ip option
  match exception ip icmp unreachable
  match exception ipv6 option
  match exception ipv6 icmp unreachable
```

**copp-system-class-exception-diag** クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-exception-diag
  match exception ttl-failure
  match exception mtu-failure
```

**copp-system-class-important** クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-important
  match access-group name copp-system-p-acl-hsrp
  match access-group name copp-system-p-acl-vrrp
  match access-group name copp-system-p-acl-hsrp6
  match access-group name copp-system-p-acl-vrrp6
  match access-group name copp-system-p-acl-mac-lldp
```

**copp-system-class-l2-default** クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-l2-default
  match access-group name copp-system-p-acl-mac-undesirable
```

**copp-system-class-l2-unpoliced** クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-l2-unpoliced
  match access-group name copp-system-p-acl-mac-stp
  match access-group name copp-system-p-acl-mac-lacp
  match access-group name copp-system-p-acl-mac-cfsoe
  match access-group name copp-system-p-acl-mac-sdp-srp
  match access-group name copp-system-p-acl-mac-l2-tunnel
  match access-group name copp-system-p-acl-mac-cdp-udld-vtp
```

**copp-system-class-l3mc-data** クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-l3mc-data
  match exception multicast rpf-failure
  match exception multicast dest-miss
```

**copp-system-class-l3uc-data** クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-l3uc-data
  match exception glean
```

**copp-system-class-management** クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-management
  match access-group name copp-system-p-acl-ftp
  match access-group name copp-system-p-acl-ntp
  match access-group name copp-system-p-acl-ssh
  match access-group name copp-system-p-acl-http
  match access-group name copp-system-p-acl-ntp6
  match access-group name copp-system-p-acl-sftp
  match access-group name copp-system-p-acl-snmp
  match access-group name copp-system-p-acl-ssh6
  match access-group name copp-system-p-acl-tftp
  match access-group name copp-system-p-acl-https
```

```

match access-group name copp-system-p-acl-snmp6
match access-group name copp-system-p-acl-tftp6
match access-group name copp-system-p-acl-radius
match access-group name copp-system-p-acl-tacacs
match access-group name copp-system-p-acl-telnet
match access-group name copp-system-p-acl-radius6
match access-group name copp-system-p-acl-tacacs6
match access-group name copp-system-p-acl-telnet6

```

copp-system-class-monitoring クラスの設定は次のとおりです。

```

class-map type control-plane match-any copp-system-p-class-monitoring
  match access-group name copp-system-p-acl-icmp
  match access-group name copp-system-p-acl-icmp6
  match access-group name copp-system-p-acl-traceroute

```

copp-system-class-multicast-host クラスの設定は次のとおりです。

```

class-map type control-plane match-any copp-system-p-class-multicast-host
  match access-group name copp-system-p-acl-mld

```

copp-system-class-multicast-router クラスの設定は次のとおりです。

```

class-map type control-plane match-any copp-system-p-class-multicast-router
  match access-group name copp-system-p-acl-pim
  match access-group name copp-system-p-acl-msdp
  match access-group name copp-system-p-acl-pim6
  match access-group name copp-system-p-acl-pim-reg
  match access-group name copp-system-p-acl-pim6-reg
  match access-group name copp-system-p-acl-pim-mdt-join

```

copp-system-class-nat-flow クラスの設定は次のとおりです。

```

class-map type control-plane match-any copp-system-p-class-nat-flow
  match exception nat-flow

```

copp-system-class-ndp クラスの設定は次のとおりです。

```

class-map type control-plane match-any copp-system-p-class-ndp
  match access-group name copp-system-p-acl-ndp

```

copp-system-class-normal クラスの設定は次のとおりです。

```

class-map type control-plane match-any copp-system-p-class-normal
  match access-group name copp-system-p-acl-mac-dot1x
  match protocol arp

```

copp-system-class-normal-dhcp クラスの設定は次のとおりです。

```

class-map type control-plane match-any copp-system-p-class-normal-dhcp
  match access-group name copp-system-p-acl-dhcp
  match access-group name copp-system-p-acl-dhcp6

```

copp-system-class-normal-dhcp-relay-response クラスの設定は次のとおりです。

```

class-map type control-plane match-any copp-system-p-class-normal-dhcp-relay-response
  match access-group name copp-system-p-acl-dhcp-relay-response
  match access-group name copp-system-p-acl-dhcp6-relay-response

```

copp-system-class-normal-igmp クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-normal-igmp
  match access-group name copp-system-p-acl-igmp
```

copp-system-class-redirect クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-redirect
  match access-group name copp-system-p-acl-ptp
```

copp-system-class-undesirable クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-undesirable
  match access-group name copp-system-p-acl-undesirable
  match exception multicast sg-rpf-failure
```

copp-system-class-fcoe クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-fcoe
  match access-group name copp-system-p-acl-mac-fcoe
```



(注) copp-system-class-fcoe クラスは Cisco Nexus 9200 シリーズ スイッチではサポートされていません。

## 厳密なデフォルト CoPP ポリシー

Cisco Nexus 9200 シリーズ スイッチの場合、strict CoPP ポリシーの設定は次のとおりです。

```
policy-map type control-plane copp-system-p-policy-strict
  class copp-system-p-class-l3uc-data
    set cos 1
    police cir 800 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-critical
    set cos 7
    police cir 36000 kbps bc 1280000 bytes conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 2500 kbps bc 1280000 bytes conform transmit violate drop
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 2600 kbps bc 128000 bytes conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 10000 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-multicast-host
    set cos 1
    police cir 1000 kbps bc 128000 bytes conform transmit violate drop
  class copp-system-p-class-l3mc-data
    set cos 1
    police cir 2400 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-normal
    set cos 1
    police cir 1400 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-ndp
    set cos 6
    police cir 1400 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-normal-dhcp
```

```

set cos 1
  police cir 1300 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-normal-dhcp-relay-response
  set cos 1
  police cir 1500 kbps bc 64000 bytes conform transmit violate drop
class copp-system-p-class-normal-igmp
  set cos 3
  police cir 3000 kbps bc 64000 bytes conform transmit violate drop
class copp-system-p-class-redirect
  set cos 1
  police cir 280 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-exception
  set cos 1
  police cir 150 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-exception-diag
  set cos 1
  police cir 150 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-monitoring
  set cos 1
  police cir 150 kbps bc 128000 bytes conform transmit violate drop
class copp-system-p-class-l2-unpoliced
  set cos 7
  police cir 50 mbps bc 8192000 bytes conform transmit violate drop
class copp-system-p-class-undesirable
  set cos 0
  police cir 200 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-nat-flow
  set cos 7
  police cir 800 kbps bc 64000 bytes conform transmit violate drop
class copp-system-p-class-l2-default
  set cos 0
  police cir 400 kbps bc 32000 bytes conform transmit violate drop
class class-default
  set cos 0
  police cir 400 kbps bc 32000 bytes conform transmit violate drop

```

Cisco Nexus 9300 と 9500 シリーズおよび、3164Q、31128PQ、3232C、および 3264Q スイッチの場合、strict CoPP ポリシーの設定は次のとおりです。

```

policy-map type control-plane copp-system-p-policy-strict
  class copp-system-p-class-l3uc-data
    set cos 1
    police cir 250 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-critical
    set cos 7
    police cir 19000 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 3000 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 3000 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 3000 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-multicast-host
    set cos 1
    police cir 2000 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-l3mc-data
    set cos 1
    police cir 3000 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-normal
    set cos 1

```

```
    police cir 1500 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-ndp
    set cos 6
    police cir 1500 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 300 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 400 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-normal-igmp
    set cos 3
    police cir 6000 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-redirect
    set cos 1
    police cir 1500 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-exception
    set cos 1
    police cir 50 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-exception-diag
    set cos 1
    police cir 50 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-monitoring
    set cos 1
    police cir 300 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-l2-unpoliced
    set cos 7
    police cir 20000 pps bc 8192 packets conform transmit violate drop
class copp-system-p-class-undesirable
    set cos 0
    police cir 15 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-fcoe
    set cos 6
    police cir 1500 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-nat-flow
    set cos 7
    police cir 100 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-l2-default
    set cos 0
    police cir 50 pps bc 32 packets conform transmit violate drop
class class-default
    set cos 0
    police cir 50 pps bc 32 packets conform transmit violate drop
```

## モデレート デフォルト CoPP ポリシー

Cisco Nexus 9200 シリーズ スイッチの場合、moderate CoPP ポリシーの設定は次のとおりです。

```
policy-map type control-plane copp-system-p-policy-moderate
class copp-system-p-class-l3uc-data
    set cos 1
    police cir 800 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-critical
    set cos 7
    police cir 36000 kbps bc 1920000 bytes conform transmit violate drop
class copp-system-p-class-important
    set cos 6
    police cir 2500 kbps bc 1920000 bytes conform transmit violate drop
class copp-system-p-class-multicast-router
    set cos 6
    police cir 2600 kbps bc 192000 bytes conform transmit violate drop
class copp-system-p-class-management
    set cos 2
```

```

    police cir 10000 kbps bc 48000 bytes conform transmit violate drop
class copp-system-p-class-multicast-host
    set cos 1
    police cir 1000 kbps bc 192000 bytes conform transmit violate drop
class copp-system-p-class-l3mc-data
    set cos 1
    police cir 2400 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-normal
    set cos 1
    police cir 1400 kbps bc 48000 bytes conform transmit violate drop
class copp-system-p-class-ndp
    set cos 6
    police cir 1400 kbps bc 48000 bytes conform transmit violate drop
class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 1300 kbps bc 48000 bytes conform transmit violate drop
class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 1500 kbps bc 96000 bytes conform transmit violate drop
class copp-system-p-class-normal-igmp
    set cos 3
    police cir 3000 kbps bc 64000 bytes conform transmit violate drop
class copp-system-p-class-redirect
    set cos 1
    police cir 280 kbps bc 48000 bytes conform transmit violate drop
class copp-system-p-class-exception
    set cos 1
    police cir 150 kbps bc 48000 bytes conform transmit violate drop
class copp-system-p-class-exception-diag
    set cos 1
    police cir 150 kbps bc 48000 bytes conform transmit violate drop
class copp-system-p-class-monitoring
    set cos 1
    police cir 150 kbps bc 192000 bytes conform transmit violate drop
class copp-system-p-class-l2-unpoliced
    set cos 7
    police cir 50 mbps bc 8192000 bytes conform transmit violate drop
class copp-system-p-class-undesirable
    set cos 0
    police cir 200 kbps bc 48000 bytes conform transmit violate drop
class copp-system-p-class-nat-flow
    set cos 7
    police cir 800 kbps bc 64000 bytes conform transmit violate drop
class copp-system-p-class-l2-default
    set cos 0
    police cir 400 kbps bc 48000 bytes conform transmit violate drop
class class-default
    set cos 0
    police cir 400 kbps bc 48000 bytes conform transmit violate drop

```

Cisco Nexus 9300 と 9500 シリーズおよび、3164Q、31128PQ、3232C、および 3264Q スイッチの場合、moderate CoPP ポリシーの設定は次のとおりです。

```

policy-map type control-plane copp-system-p-policy-moderate
  class copp-system-p-class-l3uc-data
    set cos 1
    police cir 250 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-critical
    set cos 7
    police cir 19000 pps bc 192 packets conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 3000 pps bc 192 packets conform transmit violate drop

```

```

class copp-system-p-class-multicast-router
  set cos 6
  police cir 3000 pps bc 192 packets conform transmit violate drop
class copp-system-p-class-management
  set cos 2
  police cir 3000 pps bc 48 packets conform transmit violate drop
class copp-system-p-class-multicast-host
  set cos 1
  police cir 2000 pps bc 192 packets conform transmit violate drop
class copp-system-p-class-l3mc-data
  set cos 1
  police cir 3000 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-normal
  set cos 1
  police cir 1500 pps bc 48 packets conform transmit violate drop
class copp-system-p-class-ndp
  set cos 6
  police cir 1500 pps bc 48 packets conform transmit violate drop
class copp-system-p-class-normal-dhcp
  set cos 1
  police cir 300 pps bc 48 packets conform transmit violate drop
class copp-system-p-class-normal-dhcp-relay-response
  set cos 1
  police cir 400 pps bc 96 packets conform transmit violate drop
class copp-system-p-class-normal-igmp
  set cos 3
  police cir 6000 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-redirect
  set cos 1
  police cir 1500 pps bc 48 packets conform transmit violate drop
class copp-system-p-class-exception
  set cos 1
  police cir 50 pps bc 48 packets conform transmit violate drop
class copp-system-p-class-exception-diag
  set cos 1
  police cir 50 pps bc 48 packets conform transmit violate drop
class copp-system-p-class-monitoring
  set cos 1
  police cir 300 pps bc 192 packets conform transmit violate drop
class copp-system-p-class-l2-unpoliced
  set cos 7
  police cir 20000 pps bc 8192 packets conform transmit violate drop
class copp-system-p-class-undesirable
  set cos 0
  police cir 15 pps bc 48 packets conform transmit violate drop
class copp-system-p-class-fcoe
  set cos 6
  police cir 1500 pps bc 192 packets conform transmit violate drop
class copp-system-p-class-nat-flow
  set cos 7
  police cir 100 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-l2-default
  set cos 0
  police cir 50 pps bc 48 packets conform transmit violate drop
class class-default
  set cos 0
  police cir 50 pps bc 48 packets conform transmit violate drop

```

Lenient デフォルト CoPP ポリシー :

Cisco Nexus 9200 シリーズ スイッチの場合、lenient CoPP ポリシーの設定は次のとおりです。

## Lenient デフォルト CoPP ポリシー :

```

policy-map type control-plane copp-system-p-policy-lenient
  class copp-system-p-class-l3uc-data
    set cos 1
    police cir 800 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-critical
    set cos 7
    police cir 36000 kbps bc 2560000 bytes conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 2500 kbps bc 2560000 bytes conform transmit violate drop
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 2600 kbps bc 256000 bytes conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 10000 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-multicast-host
    set cos 1
    police cir 1000 kbps bc 256000 bytes conform transmit violate drop
  class copp-system-p-class-l3mc-data
    set cos 1
    police cir 2400 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-normal
    set cos 1
    police cir 1400 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-ndp
    set cos 6
    police cir 1400 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 1300 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 1500 kbps bc 128000 bytes conform transmit violate drop
  class copp-system-p-class-normal-igmp
    set cos 3
    police cir 3000 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-redirect
    set cos 1
    police cir 280 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-exception
    set cos 1
    police cir 150 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-exception-diag
    set cos 1
    police cir 150 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-monitoring
    set cos 1
    police cir 150 kbps bc 256000 bytes conform transmit violate drop
  class copp-system-p-class-l2-unpoliced
    set cos 7
    police cir 50 mbps bc 8192000 bytes conform transmit violate drop
  class copp-system-p-class-undesirable
    set cos 0
    police cir 200 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-nat-flow
    set cos 7
    police cir 800 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-l2-default
    set cos 0
    police cir 400 kbps bc 64000 bytes conform transmit violate drop
  class class-default
    set cos 0

```



```
police cir 400 kbps bc 64000 bytes conform transmit violate drop
```

Cisco Nexus 9300 と 9500 シリーズおよび、3164Q、31128PQ、3232C、および 3264Q スイッチの場合、lenient CoPP ポリシーの設定は次のとおりです。

```
policy-map type control-plane copp-system-p-policy-lenient
class copp-system-p-class-l3uc-data
  set cos 1
  police cir 250 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-critical
  set cos 7
  police cir 19000 pps bc 256 packets conform transmit violate drop
class copp-system-p-class-important
  set cos 6
  police cir 3000 pps bc 256 packets conform transmit violate drop
class copp-system-p-class-multicast-router
  set cos 6
  police cir 3000 pps bc 256 packets conform transmit violate drop
class copp-system-p-class-management
  set cos 2
  police cir 3000 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-multicast-host
  set cos 1
  police cir 2000 pps bc 256 packets conform transmit violate drop
class copp-system-p-class-l3mc-data
  set cos 1
  police cir 3000 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-normal
  set cos 1
  police cir 1500 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-ndp
  set cos 6
  police cir 1500 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-normal-dhcp
  set cos 1
  police cir 300 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-normal-dhcp-relay-response
  set cos 1
  police cir 400 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-normal-igmp
  set cos 3
  police cir 6000 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-redirect
  set cos 1
  police cir 1500 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-exception
  set cos 1
  police cir 50 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-exception-diag
  set cos 1
  police cir 50 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-monitoring
  set cos 1
  police cir 300 pps bc 256 packets conform transmit violate drop
class copp-system-p-class-l2-unpoliced
  set cos 7
  police cir 20000 pps bc 8192 packets conform transmit violate drop
class copp-system-p-class-undesirable
  set cos 0
  police cir 15 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-fcoe
  set cos 6
  police cir 1500 pps bc 256 packets conform transmit violate drop
```

```

class copp-system-p-class-nat-flow
  set cos 7
  police cir 100 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-l2-default
  set cos 0
  police cir 50 pps bc 64 packets conform transmit violate drop
class class-default
  set cos 0
  police cir 50 pps bc 64 packets conform transmit violate drop

```

## 高密度デフォルト CoPP ポリシー

Cisco Nexus 9200 シリーズ スイッチの場合、dense CoPP ポリシーの設定は次のとおりです。

```

policy-map type control-plane copp-system-p-policy-dense
  class copp-system-p-class-l3uc-data
    set cos 1
    police cir 800 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-critical
    set cos 7
    police cir 4500 kbps bc 1280000 bytes conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 2500 kbps bc 1280000 bytes conform transmit violate drop
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 370 kbps bc 128000 bytes conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 2500 kbps bc 128000 bytes conform transmit violate drop
  class copp-system-p-class-multicast-host
    set cos 2
    police cir 300 kbps bc 128000 bytes conform transmit violate drop
  class copp-system-p-class-l3mc-data
    set cos 1
    police cir 600 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-normal
    set cos 1
    police cir 1400 kbps bc 128000 bytes conform transmit violate drop
  class copp-system-p-class-ndp
    set cos 1
    police cir 350 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 750 kbps bc 128000 bytes conform transmit violate drop
  class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 750 kbps bc 128000 bytes conform transmit violate drop
  class copp-system-p-class-normal-igmp
    set cos 3
    police cir 1400 kbps bc 128000 bytes conform transmit violate drop
  class copp-system-p-class-redirect
    set cos 1
    police cir 200 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-exception
    set cos 1
    police cir 200 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-exception-diag
    set cos 1
    police cir 200 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-monitoring
    set cos 1
    police cir 150 kbps bc 128000 bytes conform transmit violate drop

```

```
class copp-system-p-class-l2-unpoliced
  set cos 7
  police cir 50 mbps bc 8192000 bytes conform transmit violate drop
class copp-system-p-class-undesirable
  set cos 0
  police cir 100 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-l2-default
  set cos 0
  police cir 200 kbps bc 32000 bytes conform transmit violate drop
class class-default
  set cos 0
  police cir 200 kbps bc 32000 bytes conform transmit violate drop
```

Cisco Nexus 9300 と 9500 シリーズおよび、3164Q、31128PQ、3232C、および 3264Q スイッチの場合、dense CoPP ポリシーの設定は次のとおりです。

```
policy-map type control-plane copp-system-p-policy-dense
  class copp-system-p-class-l3uc-data
    set cos 1
    police cir 250 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-critical
    set cos 7
    police cir 2500 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 1200 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 1200 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 1200 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-multicast-host
    set cos 2
    police cir 1000 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-l3mc-data
    set cos 1
    police cir 1200 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-normal
    set cos 1
    police cir 750 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-ndp
    set cos 1
    police cir 750 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 150 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 200 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-normal-igmp
    set cos 3
    police cir 2500 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-redirect
    set cos 1
    police cir 1500 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-exception
    set cos 1
    police cir 50 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-exception-diag
    set cos 1
    police cir 50 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-monitoring
```

```

set cos 1
  police cir 50 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-l2-unpoliced
set cos 7
  police cir 20000 pps bc 8192 packets conform transmit violate drop
class copp-system-p-class-undesirable
set cos 0
  police cir 15 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-fcoe
set cos 6
  police cir 750 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-l2-default
set cos 0
  police cir 25 pps bc 32 packets conform transmit violate drop
class class-default
set cos 0
  police cir 25 pps bc 32 packets conform transmit violate drop

```

### 1 秒間あたりのパケットのクレジット制限

特定のポリシーの 1 秒間あたりのパケット（PPS）の合計（ポリシーの各クラス部分の PPS の合計）の上限は、PPS のクレジット制限（PCL）の上限になります。特定のクラスの PPS が増加して PCL 超過すると、設定が拒否されます。目的の PPS を増やすには、PCL を超える PPS の分を他のクラスから減少させる必要があります。

## モジュラ QoS コマンドライン インターフェイス

CoPP は、モジュラ QoS コマンドライン インターフェイス（MQC）を使用します。MQC は CLI の構造を持っています。MQC を使用すると、トラフィック クラスの定義、トラフィック ポリシー（ポリシー マップ）の作成、およびインターフェイスへのトラフィック ポリシーの適用が可能になります。トラフィック ポリシーには、トラフィック クラスに適用する CoPP 機能を含めます。

### SUMMARY STEPS

1. **class-map** コマンドを使用して、トラフィック クラスを定義します。トラフィック クラスは、トラフィックの分類に使用します。
2. **policy-map** コマンドを使用して、トラフィック ポリシーを定義します。トラフィック ポリシー（ポリシー マップ）には、トラフィック クラスと、トラフィック クラスに適用する 1 つまたは複数の CoPP 機能を含めます。トラフィック ポリシー内の CoPP の機能で、分類されたトラフィックの処理方法が決まります。
3. **control-plane** コマンドおよび **service-policy** コマンドを使用して、トラフィック ポリシー（ポリシー マップ）をコントロールプレーンに適用します。

## DETAILED STEPS

### Procedure

**ステップ 1** **class-map** コマンドを使用して、トラフィック クラスを定義します。トラフィック クラスは、トラフィックの分類に使用します。

次に、**copp-sample-class** と呼ばれる新しいマップを作成する例を示します。

```
class-map type control-plane copp-sample-class
```

**ステップ 2** **policy-map** コマンドを使用して、トラフィック ポリシーを定義します。トラフィック ポリシー（ポリシー マップ）には、トラフィック クラスと、トラフィック クラスに適用する 1 つまたは複数の CoPP 機能を含めます。トラフィック ポリシー内の CoPP の機能で、分類されたトラフィックの処理方法が決まります。

**ステップ 3** **control-plane** コマンドおよび **service-policy** コマンドを使用して、トラフィック ポリシー（ポリシー マップ）をコントロールプレーンに適用します。

次に、コントロールプレーンにポリシー マップを適用する例を示します。

```
control-plane  
service-policy input copp-system-policy
```

#### Note

**copp-system-policy** は常に設定され、適用されます。このコマンドを明示的に使用する必要はありません。

## CoPP と管理インターフェイス

Cisco NX-OS デバイスは、管理インターフェイス（**mgmt0**）をサポートしない、ハードウェアベースの CoPP だけをサポートします。アウトオブバンド **mgmt0** インターフェイスは CPU に直接接続するため、CoPP が実装されているインバンドトラフィック ハードウェアは通過しません。

**mgmt0** インターフェイスで、ACL を設定して、特定タイプのトラフィックへのアクセスを許可または拒否することができます。

## CoPP の注意事項と制約事項

CoPP に関する注意事項と制約事項は次のとおりです。

- リリース 9.3(7) にアップグレードする前に、**scale-factor 1 module multiple-module-range** コマンドを使用してスケール係数を 1 に設定します。
- 最初に **strict** デフォルト CoPP ポリシーを使用し、後で、データセンターおよびアプリケーションの要件に基づいて CoPP ポリシーを変更することを推奨します。

- CoPPのカスタマイズは継続的なプロセスです。CoPPを設定するときには、特定の環境で使用するプロトコルや機能に加えて、サーバ環境に必要なスーパーバイザ機能を考慮する必要があります。これらのプロトコルや機能が変更されたら、CoPPを変更する必要があります。
- CoPPを継続的にモニタすることを推奨します。ドロップが発生した場合は、CoPPがトラフィックを誤ってドロップしたのか、または誤動作や攻撃に応答してドロップしたのかを判定してください。いずれの場合も、状況を分析し、CoPPポリシーを変更する必要を評価します。
- 他のクラス マップで指定しないトラフィックはすべて、最後のクラス（デフォルト クラス）に配置されます。このクラス内のドロップをモニタし、これらのドロップが必要のないトラフィックに基づいているのか、または設定されていないために追加が必要な機能の結果であるかどうかを調査します。
- アクセス コントロール リスト（ACL）を通してルータ プロセッサにリダイレクトする必要のあるパケット（たとえば、ARPおよびDHCP）を判定するために、すべてのブロードキャストトラフィックがCoPPロジックを通して送信されます。リダイレクトする必要のないブロードキャストトラフィックはCoPPロジックに対して照合され、準拠したパケットと違反したパケットの両方がハードウェア内でカウントされますが、CPUには送信されません。CPUに送信する必要のあるブロードキャストトラフィックと、CPUに送信する必要のないブロードキャストトラフィックを異なるクラスに分離する必要があります。
- CoPPを設定した後、古いクラスマップや未使用のルーティングプロトコルなど、使用されていないものはすべて削除してください。
- CoPPポリシーによって、ルーティングプロトコルなどのクリティカルなトラフィック、またはデバイスへのインタラクティブなアクセスがフィルタリングされないように注意してください。このトラフィックをフィルタリングすると、Cisco NX-OS デバイスへのリモートアクセスが禁止され、コンソール接続が必要になる場合があります。
- Cisco NX-OS ソフトウェアは、出力 CoPP とサイレントモードをサポートしません。CoPP は、入力でのみサポートされます（コントロールプレーン インターフェイスに対して **service-policy output copp** コマンドは使用できません）。
- ハードウェアのアクセス コントロール エントリ（ACE）ヒットカウンタは、ACL 論理だけで使用できます。CPU のトラフィックを評価するには、ソフトウェアの ACE ヒットカウンタと **show access-lists** および **show policy-map type control-plane** コマンドを使用します。
- Cisco NX-OS デバイスのハードウェアは、フォワーディング エンジン単位で CoPP を実行します。CoPP は分散ポリシーをサポートしていません。したがって、レートを選択する場合は、集約トラフィックでスーパーバイザモジュールに過剰な負荷をかけることのない値にしてください。
- 複数のフローが同じクラスにマッピングされる場合、個々のフローの統計情報は使用できません。
- CoPP 機能をサポートする Cisco NX-OS リリースから、新しいプロトコルのその他のクラスを含む CoPP 機能をサポートする Cisco NX-OS リリースにアップグレードする場合は、

CoPPの新しいクラスを使用可能にするためにセットアップユーティリティを **setup** コマンドで実行するか **copp profile** コマンドを実行する必要があります。

- コントロールプレーンポリシング (CoPP) 機能をサポートしている Cisco NX-OS リリースから CoPP 機能をサポートしていない以前の Cisco NX-OS リリースへのダウングレードを実行する前に、**show incompatibility nxos bootflash:filename** コマンドを使用して互換性を確認しておく必要があります。非互換な部分が存在する場合は、ソフトウェアをダウングレードする前に、ダウングレードイメージと互換性がない機能をすべて無効化してください。
- CoPP は無効にできません。これを無効にしようとすると、パケットは 50 パケット/秒 (Cisco NX-OS リリース 7.0 (3) I2 (1) より前のリリース) でレート制限されるか、エラーメッセージが表示されます (Cisco NX-OS リリース 7.0(3)I2(1) 以降)。
- Cisco Nexus 9200 シリーズスイッチは、10 kbps の倍数でのみ CoPP ポリサーレートをサポートします。10 kbps の倍数でないレートが設定されている場合、そのレートは切り捨てられます。たとえば、55 Kbps のレートを設定しても、スイッチは 50 kbps を使用します。  
(**show policy-map type control-plane** コマンドで表示されるのはユーザ設定のレートです。詳細については、「[CoPP の設定の確認 \(279 ページ\)](#)」を参照してください)。
- Cisco Nexus 9200 シリーズスイッチでは、ip icmp redirect、ipv6 icmp redirect、ip icmp unreachable、ipv6 icmp unreachable、および mtu-failure は同じ TCAM エントリを使用し、これらがすべて分類されるクラスマップではポリシー中に最初の例外が存在します。CoPP 厳密プロファイルでは、クラス例外クラスマップに分類されます。別の CoPP ポリシーでは、最初の例外が異なるクラスマップ (たとえば、class-exception-diag) にある場合、残りの例外は同じクラスマップに分類されます。
- copp-system-class-fcoe クラスは Cisco Nexus 9200 シリーズスイッチではサポートされていません。
- スタティック CoPP ACL には、次のガイドラインと制限事項が適用されます。
  - Cisco Nexus 9200 シリーズスイッチのみがスタティック CoPP ACL を使用します。
  - スタティック CoPP ACL は、別の CoPP クラスに再マッピングできます。
  - スタティック CoPP ACL のアクセスコントロールエントリ (ACE) は変更または削除できません。
  - CoPP ACL にスタティック ACL のサブストリングがある場合、このタイプのトラフィックに対してマッピングされます。たとえば、ACL に acl-mac-stp サブストリングが含まれている場合、STP トラフィックはこの ACL のクラスマップに分類されます。
  - スタティック CoPP ACL は、CoPP ポリシー内での位置、設定される順序、および **show policy-map type control-plane** コマンドの出力での表示に関係なく、ダイナミック CoPP ACL よりも優先されます。
  - CoPP ポリシーにスタティック CoPP ACL が必要です。これを行わないと、CoPP ポリシーは拒否されます。

- Cisco NX-OS リリース 10.3(2)F 以降、CoPP の送信元 IP ベース フィルタリングが、Cisco Nexus 3600 プラットフォーム スイッチ（N3K-C36180YC-R および N3K-C3636C-R）でサポートされています。



(注) IPv6 の場合、ソース IP ベースのフィルタリングは、24b MSB まですサポートされます。



(注) Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合がありますので注意してください。

## CoPP のデフォルト設定

次の表に、CoPP パラメータのデフォルト設定を示します。

Table 16: CoPP パラメータのデフォルト設定

| パラメータ      | デフォルト                                                                  |
|------------|------------------------------------------------------------------------|
| デフォルト ポリシー | strict                                                                 |
| デフォルト ポリシー | 9 ポリシー エントリ<br><br><b>Note</b><br>関連するクラス マップでサポートされるポリシーの最大数は 128 です。 |
| スケールファクタ値  | 1.00                                                                   |

## CoPP の設定

ここでは、CoPP の設定方法について説明します。

### コントロールプレーン クラス マップの設定

コントロールプレーンポリシーのコントロールプレーンクラスマップを設定する必要があります。

トラフィックを分類するには、既存の ACL に基づいてパケットを照合します。ACL キーワードの permit および deny は、照合時には無視されます。



IP バージョン 4 (IPv4) および IP バージョン 6 (IPv6) のパケットに対してポリシーを設定できます。

### Before you begin

クラスマップ内で ACE ヒット カウンタを使用する場合は、IP ACL が設定してあることを確認します。

## SUMMARY STEPS

1. **configure terminal**
2. **class-map type control-plane [match-all | match-any] class-map-name**
3. (Optional) **match access-group name access-list-name**
4. (Optional) **match exception {ip | ipv6} icmp redirect**
5. (Optional) **match exception {ip | ipv6} icmp unreachable**
6. (Optional) **match exception {ip | ipv6} option**
7. **match protocol arp**
8. **exit**
9. (Optional) **show class-map type control-plane [class-map-name]**
10. (Optional) **copy running-config startup-config**

## DETAILED STEPS

### Procedure

|        | Command or Action                                                                                                                                                                           | Purpose                                                                                                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>                                                                                   | グローバル コンフィギュレーション モードを開始します                                                                                                                                                                           |
| ステップ 2 | <b>class-map type control-plane [match-all   match-any] class-map-name</b><br><br><b>Example:</b><br><pre>switch(config)# class-map type control-plane ClassMapA switch(config-cmap)#</pre> | <p>コントロールプレーンクラスマップを指定し、クラスマップ コンフィギュレーション モードを開始します。デフォルトのクラス一致は <b>match-any</b> です。名前は最大 64 文字で、大文字と小文字は区別されます。</p> <p><b>Note</b><br/>class-default、match-all、または match-any をクラスマップ名に使用できません。</p> |
| ステップ 3 | (Optional) <b>match access-group name access-list-name</b><br><br><b>Example:</b><br><pre>switch(config-cmap)# match access-group name MyAccessList</pre>                                   | <p>IP ACL のマッチングを指定します。</p> <p><b>Note</b><br/>ACL キーワード <b>permit</b> および <b>deny</b> は、CoPP マッチング時には無視されます。</p>                                                                                     |

|         | Command or Action                                                                                                                                        | Purpose                                                       |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| ステップ 4  | (Optional) <b>match exception {ip   ipv6} icmp redirect</b><br><b>Example:</b><br><pre>switch(config-cmap)# match exception ip icmp redirect</pre>       | IPv4 または IPv6 ICMP リダイレクト例外パケットのマッチングを指定します。                  |
| ステップ 5  | (Optional) <b>match exception {ip   ipv6} icmp unreachable</b><br><b>Example:</b><br><pre>switch(config-cmap)# match exception ip icmp unreachable</pre> | IPv4 または IPv6 ICMP 到達不能例外パケットのマッチングを指定します。                    |
| ステップ 6  | (Optional) <b>match exception {ip   ipv6} option</b><br><b>Example:</b><br><pre>switch(config-cmap)# match exception ip option</pre>                     | IPv4 または IPv6 ICMP オプション例外パケットのマッチングを指定します。                   |
| ステップ 7  | <b>match protocol arp</b><br><b>Example:</b><br><pre>switch(config-cmap)# match protocol arp</pre>                                                       | IP アドレス解決プロトコル (ARP) および逆アドレス解決プロトコル (RARP) パケットのマッチングを指定します。 |
| ステップ 8  | <b>exit</b><br><b>Example:</b><br><pre>switch(config-cmap)# exit<br/>switch(config)#</pre>                                                               | クラスマップ コンフィギュレーション モードを終了します。                                 |
| ステップ 9  | (Optional) <b>show class-map type control-plane [class-map-name]</b><br><b>Example:</b><br><pre>switch(config)# show class-map type control-plane</pre>  | コントロールプレーン クラスマップの設定を表示します。                                   |
| ステップ 10 | (Optional) <b>copy running-config startup-config</b><br><b>Example:</b><br><pre>switch(config)# copy running-config startup-config</pre>                 | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                     |

## コントロールプレーン ポリシー マップの設定

CoPP のポリシーマップを設定する必要があります。ポリシーマップにはポリシングパラメータを含めます。クラスのポリサーを設定しなかった場合、次のデフォルトが設定されます。

- 50 パケット/秒 (pps) 、 32 パケットのバースト (Cisco Nexus 9300 および 9500 シリーズ、3164Q、31128PQ、3232C、および 3264Q スイッチの場合)
- 150 キロビット/秒 (kbps) 、 32,000 バイトのバースト (Cisco Nexus 9200 シリーズ スイッチの場合)

## Before you begin

コントロールプレーン クラス マップが設定してあることを確認します。

## SUMMARY STEPS

1. **configure terminal**
2. **policy-map type control-plane *policy-map-name***
3. **class {*class-map-name* [*insert-before class-map-name2*] | class-default}**
4. 次のいずれかのコマンドを入力します。
  - **police [cir] {*cir-rate* [*rate-type*]}**
  - **police [cir] {*cir-rate* [*rate-type*] [*bc*] *burst-size* [*burst-size-type*]}**
  - **police [cir] {*cir-rate* [*rate-type*]}** **conform transmit [*violate drop*]**
5. (Optional) **logging drop threshold [*drop-count* [*level syslog-level*]]**
6. (Optional) **set cos *cos-value***
7. **exit**
8. **exit**
9. (Optional) **show policy-map type control-plane [*expand*] [*name class-map-name*]**
10. (Optional) **copy running-config startup-config**

## DETAILED STEPS

### Procedure

|        | Command or Action                                                                                                                                                                                                                                          | Purpose                                                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>                                                                                                                                                      | グローバル コンフィギュレーション モードを開始します。                                                                                                                     |
| ステップ 2 | <b>policy-map type control-plane <i>policy-map-name</i></b><br><b>Example:</b><br><pre>switch(config)# policy-map type control-plane ClassMapA switch(config-pmap)#</pre>                                                                                  | コントロールプレーン ポリシー マップを指定し、ポリシー マップ コンフィギュレーション モードを開始します。ポリシー マップ 名は最大 64 文字で、大文字と小文字は区別されます。                                                      |
| ステップ 3 | <b>class {<i>class-map-name</i> [<i>insert-before class-map-name2</i>]   class-default}</b><br><b>Example:</b><br><pre>switch(config-pmap)# class ClassMapA switch(config-pmap-c)#</pre>                                                                   | コントロールプレーン クラス マップ 名またはクラス デフォルトを指定し、コントロールプレーン クラス コンフィギュレーション モードを開始します。<br><br><b>class-default</b> クラス マップは、必ずポリシー マップのクラス マップ リストの末尾に位置します。 |
| ステップ 4 | 次のいずれかのコマンドを入力します。 <ul style="list-style-type: none"> <li>• <b>police [cir] {<i>cir-rate</i> [<i>rate-type</i>]}</b></li> <li>• <b>police [cir] {<i>cir-rate</i> [<i>rate-type</i>] [<i>bc</i>] <i>burst-size</i> [<i>burst-size-type</i>]}</b></li> </ul> | 認定情報レート (CIR) を指定します。レート範囲を次に示します。                                                                                                               |

|        | Command or Action                                                                                                                                                                                                                                                                | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        | <p>• <b>police</b> [cir] {cir-rate [rate-type]} <b>conform transmit</b> [violate drop]</p> <p><b>Example:</b></p> <pre>switch(config-pmap-c)# police cir 52000 bc 1000 packets</pre> <p><b>Example:</b></p> <pre>switch(config-pmap-c)# police cir 3400 kbps bc 200 kbytes</pre> | <ul style="list-style-type: none"> <li>• 01 ～ 268435456 pps (Cisco Nexus 9300 および 9500 シリーズ、3164Q、31128PQ、3232C、および 3264Q スイッチの場合)</li> <li>• 0 ～ 80000000000 bps / gbps / kbps / mbps (Cisco Nexus 9200 シリーズ スイッチの場合)</li> </ul> <p><b>Note</b><br/>CIR レートの範囲は 0 から始まります。以前のリリースでは、CIR レートの範囲は 1 から始まります。0 の値ではパケットがドロップします。</p> <p>committed burst (BC) 範囲は次のようになります。</p> <ul style="list-style-type: none"> <li>• 1 ～ 1073741 パケット (Cisco Nexus 9300 および 9500 シリーズ、3164Q、31128PQ、3232C、および 3264Q スイッチの場合)</li> <li>• 1 ～ 512000000 バイト / kbytes / mbytes (Cisco Nexus 9200 シリーズ スイッチの場合)</li> </ul> <p>適合送信アクションは、パケットを送信します。</p> <p><b>Note</b><br/>同じ CIR に BC と一致 (conform) アクションを指定できます。</p> |
| ステップ 5 | <p>(Optional) <b>logging drop threshold</b> [drop-count [level syslog-level]]</p> <p><b>Example:</b></p> <pre>switch(config-pmap-c)# logging drop threshold 100</pre>                                                                                                            | <p>ドロップされたパケットのしきい値を指定し、ドロップ数が設定したしきい値を超えた場合、Syslog を生成します。<i>drop-count</i> 引数の範囲は 1 ～ 8000000000 バイトです。<i>syslog-level</i> 引数の範囲は 1 ～ 7 であり、デフォルト レベルは 4 です。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| ステップ 6 | <p>(Optional) <b>set cos</b> cos-value</p> <p><b>Example:</b></p> <pre>switch(config-pmap-c)# set cos 1</pre>                                                                                                                                                                    | <p>802.1Q CoS 値を指定します。範囲は 0 ～ 7 です。デフォルト値は 0 です。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| ステップ 7 | <p><b>exit</b></p> <p><b>Example:</b></p> <pre>switch(config-pmap-c)# exit<br/>switch(config-pmap)#</pre>                                                                                                                                                                        | <p>ポリシー マップ クラス コンフィギュレーション モードを終了します。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| ステップ 8 | <p><b>exit</b></p> <p><b>Example:</b></p> <pre>switch(config-pmap)# exit<br/>switch(config)#</pre>                                                                                                                                                                               | <p>ポリシー マップ コンフィギュレーション モードを終了します。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

|         | Command or Action                                                                                                                                                                     | Purpose                                   |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| ステップ 9  | (Optional) <b>show policy-map type control-plane</b><br><b>[expand] [name class-map-name]</b><br><br><b>Example:</b><br><pre>switch(config)# show policy-map type control-plane</pre> | コントロールプレーン ポリシー マップの設定を表示します。             |
| ステップ 10 | (Optional) <b>copy running-config startup-config</b><br><br><b>Example:</b><br><pre>switch(config)# copy running-config startup-config</pre>                                          | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。 |

## コントロールプレーン サービス ポリシーの設定

CoPP サービス ポリシーに対して 1 つまたは複数のポリシー マップを設定できます。



### Note

CoPP ポリシーを変更し CoPP のカスタム ポリシーを適用しようとした場合、ハードウェア内では非アトミックとして設定され、次のメッセージが表示されます。

```
This operation can cause disruption of control traffic. Proceed (y/n)? [no] y
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT24-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT23-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT21-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT25-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT26-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT22-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT4-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
```

### Before you begin

コントロールプレーン ポリシー マップが設定してあることを確認します。

### SUMMARY STEPS

1. **configure terminal**
2. **control-plane**
3. **[no] service-policy input policy-map-name**
4. **exit**
5. (Optional) **show running-config copp [all]**
6. (Optional) **copy running-config startup-config**

## DETAILED STEPS

## Procedure

|        | Command or Action                                                                                                                 | Purpose                                                                                                                                   |
|--------|-----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br><b>Example:</b><br>switch# configure terminal<br>switch(config)#                                 | グローバル コンフィギュレーション モードを開始します                                                                                                               |
| ステップ 2 | <b>control-plane</b><br><br><b>Example:</b><br>switch(config)# control-plane<br>switch(config-cp)#                                | コントロールプレーンコンフィギュレーションモードを開始します。                                                                                                           |
| ステップ 3 | <b>[no] service-policy input policy-map-name</b><br><br><b>Example:</b><br>switch(config-cp)# service-policy input PolicyMapA     | 入トラフィックのポリシーマップを指定します。ポリシーマップが複数ある場合は、このステップを繰り返します。<br><br>CoPPはディセーブルにできません。このコマンドに <b>no</b> フォームを入力する場合、パケットは1秒あたり 50 パケットにレート制限されます。 |
| ステップ 4 | <b>exit</b><br><br><b>Example:</b><br>switch(config-cp)# exit<br>switch(config)#                                                  | コントロールプレーンコンフィギュレーションモードを終了します。                                                                                                           |
| ステップ 5 | (Optional) <b>show running-config copp [all]</b><br><br><b>Example:</b><br>switch(config)# show running-config copp               | CoPP 設定を表示します。                                                                                                                            |
| ステップ 6 | (Optional) <b>copy running-config startup-config</b><br><br><b>Example:</b><br>switch(config)# copy running-config startup-config | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                                                                 |

## ラインカードごとの CoPP のスケール ファクタの設定

ラインカードごとの CoPP のスケール ファクタを設定できます。

スケール ファクタの設定は、特定のラインカードに適用された CoPP のポリシーのポリサー レートのスケールリングに使用されます。受け入れ値は 0.10 ～ 2.00 です。特定のラインカードに対して現在の CoPP ポリシーを変更せずに、ポリサー レートを増加または削減できます。変更はすぐに有効となるため、CoPP ポリシーを再適用する必要はありません。

## SUMMARY STEPS

1. **configure terminal**
2. **control-plane**
3. **scale-factor value module multiple-module-range**
4. (Optional) **show policy-map interface control-plane**
5. (Optional) **copy running-config startup-config**

## DETAILED STEPS

### Procedure

|        | Command or Action                                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>                                                 | グローバル コンフィギュレーション モードを開始します                                                                                                                                                                                                                                                                                                           |
| ステップ 2 | <b>control-plane</b><br><br><b>Example:</b><br><pre>switch(config)# control-plane switch(config-cp)#</pre>                                                | コントロールプレーン コンフィギュレーション モードを開始します。                                                                                                                                                                                                                                                                                                     |
| ステップ 3 | <b>scale-factor value module multiple-module-range</b><br><br><b>Example:</b><br><pre>switch(config-cp)# scale-factor 1.10 module 1-2</pre>               | ラインカードごとにポリサー レートを設定します。許可されたスケールファクタ値は0.10～2.00です。スケールファクタ値が設定されている場合、ポリシング値にはモジュールの対応するスケールファクタ値が乗算され、特定のモジュールにプログラミングされます。<br><br>デフォルトのスケールファクタ値1.00に戻すには、 <b>no scale-factor value module multiple-module-range</b> コマンドを使用するか、 <b>scale-factor 1 module multiple-module-range</b> コマンドを使用して明示的にデフォルトのスケール ファクタである値 1.00 に設定します。 |
| ステップ 4 | (Optional) <b>show policy-map interface control-plane</b><br><br><b>Example:</b><br><pre>switch(config-cp)# show policy-map interface control-plane</pre> | CoPP ポリシーが適用される場合に適用されるスケール ファクタ値を表示します。                                                                                                                                                                                                                                                                                              |
| ステップ 5 | (Optional) <b>copy running-config startup-config</b><br><br><b>Example:</b><br><pre>switch(config)# copy running-config startup-config</pre>              | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                                                                                                                                                                                                                                                             |

## デフォルトの CoPP ポリシーの変更または再適用

別のデフォルト CoPP ポリシーに変更したり、同じデフォルト CoPP ポリシーを再適用したりすることができます。

### SUMMARY STEPS

1. `no copp profile strict moderate lenient dense`
2. (Optional) `show copp status`
3. (Optional) `show running-config copp`

### DETAILED STEPS

#### Procedure

|        | Command or Action                                                                                                                   | Purpose                                                                                                      |
|--------|-------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <code>no copp profile strict moderate lenient dense</code><br><b>Example:</b><br><code>switch(config)# copp profile moderate</code> | CoPP ベスト プラクティス ポリシーを適用します。<br><br>CoPP はディセーブルにできません。このコマンドの <b>no</b> 形式を入力すると、パケットのレート制限が 50 パケット/秒になります。 |
| ステップ 2 | (Optional) <code>show copp status</code><br><b>Example:</b><br><code>switch(config)# show copp status</code>                        | 最後の設定動作およびそのステータスなど、CoPP のステータスを表示します。このコマンドを実行すると、CoPP ベスト プラクティス ポリシーがコントロールプレーンにアタッチされていることを確認することもできます。  |
| ステップ 3 | (Optional) <code>show running-config copp</code><br><b>Example:</b><br><code>switch(config)# show running-config copp</code>        | 実行コンフィギュレーション内の CoPP 設定を表示します。                                                                               |

## CoPP ベスト プラクティス ポリシーのコピー

CoPP ベスト プラクティス ポリシーは読み取り専用です。その設定を変更する場合は、それをコピーする必要があります。

### SUMMARY STEPS

1. `copp copy profile {strict | moderate | lenient | dense} {prefix | suffix} string`
2. (Optional) `show copp status`
3. (Optional) `show running-config copp`



## DETAILED STEPS

### Procedure

|        | Command or Action                                                                                                                                             | Purpose                                                                                             |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>copp copy profile</b> {strict   moderate   lenient   dense} {prefix   suffix} string<br><br><b>Example:</b><br>switch# copp copy profile strict prefix abc | CoPP ベスト プラクティス ポリシーのコピーを作成します。<br><br>CoPP は、指定したプレフィックスまたはサフィックスのすべてのクラス マップおよびポリシー マップの名前を変更します。 |
| ステップ 2 | (Optional) <b>show copp status</b><br><br><b>Example:</b><br>switch# show copp status                                                                         | 最後の設定動作およびそのステータスなど、CoPP のステータスを表示します。このコマンドを実行すると、コピーされたポリシーがコントロールプレーンにアタッチされていないことを確認することもできます。  |
| ステップ 3 | (Optional) <b>show running-config copp</b><br><br><b>Example:</b><br>switch# show running-config copp                                                         | コピーされたポリシー設定を含む、実行コンフィギュレーション内の CoPP 設定を表示します。                                                      |

## CoPP の設定の確認

CoPP の設定情報を表示するには、次のいずれかの作業を行います。

| コマンド                                                                       | 目的                                                     |
|----------------------------------------------------------------------------|--------------------------------------------------------|
| <b>show policy-map type control-plane</b> [expand] [ name policy-map-name] | コントロールプレーン ポリシー マップと関連するクラス マップ、および CIR と BC の値を表示します。 |

| コマンド                                                             | 目的                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>show policy-map interface control-plane</b>                   | <p>ポリシーの値と関連するクラス マップ、およびポリシーごとまたはクラス マップごとのドロップが表示されます。また、CoPP ポリシーが適用されている場合は、スケールファクタ値も表示されます。スケールファクタ値がデフォルト（1.00）の場合は表示されません。</p> <p><b>Note</b><br/>スケールファクタは、CIR と BC の値を各モジュールで内部的に変更しますが、ディスプレイに表示されるのは、設定された CIR と BC の値のみです。モジュールに実際に適用される値は、スケールファクタに設定値を掛けた値です。</p> |
| <b>show class-map type control-plane</b> <i>[class-map-name]</i> | <p>このクラス マップにバインドされている ACL を含め、コントロールプレーンクラスマップの設定を表示します。</p>                                                                                                                                                                                                                    |

| コマンド                                                                                                                                                 | 目的                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>show copp diff profile {strict   moderate   lenient   dense} [prior-ver] profile {strict   moderate   lenient   dense} show copp diff profile</b> | <p>2つのCoPP ベストプラクティス ポリシーの違いを表示します。</p> <p>prior-ver オプションを指定しない場合、このコマンドは、現在適用されている2つのデフォルトのCoPPのベストプラクティス ポリシー（現在適用されている厳密なポリシーと現在適用されている中程度のポリシーなど）の差異を表示します。</p> <p>prior-ver オプションを指定した場合、このコマンドは、現在適用されているデフォルトのCoPP ベストプラクティス ポリシーと以前に適用したデフォルトのCoPP ベストプラクティス ポリシーの違いを表示します（現在適用されている厳密なポリシーと以前適用した緩いポリシーなど）。</p> |
| <b>show copp profile {strict   moderate   lenient   dense}</b>                                                                                       | <p>クラスおよびポリサー値とともに、CoPP ベストプラクティス ポリシーの詳細を表示します。</p>                                                                                                                                                                                                                                                                      |
| <b>show running-config aclmgr [all]</b>                                                                                                              | <p>実行コンフィギュレーションのユーザ設定によるアクセスコントロール リスト (ACL) を表示します。all オプションを使用すると、実行コンフィギュレーションのデフォルト (CoPP 設定) とユーザ定義によるACLの両方が表示されます。</p>                                                                                                                                                                                            |
| <b>show running-config copp [all]</b>                                                                                                                | <p>実行コンフィギュレーション内のCoPP設定を表示します。</p>                                                                                                                                                                                                                                                                                       |

| コマンド                                          | 目的                                                                                                                                           |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <code>show startup-config aclmgr [all]</code> | スタートアップ コンフィギュレーションのユーザ設定によるアクセスコントロールリスト (ACL) を表示します。 <b>all</b> オプションを使用すると、スタートアップ コンフィギュレーションのデフォルト (CoPP 設定) とユーザ定義による ACL の両方が表示されます。 |

## CoPP 設定ステータスの表示

### SUMMARY STEPS

1. `switch# show copp status`

### DETAILED STEPS

#### Procedure

|        | Command or Action                     | Purpose                |
|--------|---------------------------------------|------------------------|
| ステップ 1 | <code>switch# show copp status</code> | CoPP 機能の設定ステータスを表示します。 |

#### Example

次に、CoPP 設定ステータスを表示する例を示します。

```
switch# show copp status
```

## CoPP のモニタリング

### SUMMARY STEPS

1. `switch# show policy-map interface control-plane`

## DETAILED STEPS

### Procedure

|        | Command or Action                                      | Purpose                                                                                                                                            |
|--------|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | switch# <b>show policy-map interface control-plane</b> | 適用された CoPP ポリシーの一部であるすべてのクラスに関して、パケットレベルの統計情報を表示します。<br><br>統計情報は、OutPackets（コントロールプレーンに対して許可されたパケット）と DropPackets（レート制限によってドロップされたパケット）に関して指定します。 |

### Example

次に、CoPP をモニタする例を示します。

```
switch# show policy-map interface control-plane
Control Plane

Service-policy input: copp-system-p-policy-strict

class-map copp-system-p-class-critical (match-any)
  set cos 7
  police cir 19000 pps , bc 128 packets
  module 4 :
    transmitted 373977 packets;
    dropped 0 packets;
```

# CoPP 統計情報のクリア

## SUMMARY STEPS

1. (Optional) switch# **show policy-map interface control-plane**
2. switch# **clear copp statistics**

## DETAILED STEPS

### Procedure

|        | Command or Action                                                 | Purpose                                 |
|--------|-------------------------------------------------------------------|-----------------------------------------|
| ステップ 1 | (Optional) switch# <b>show policy-map interface control-plane</b> | 現在適用されている CoPP ポリシーおよびクラスごとの統計情報を表示します。 |
| ステップ 2 | switch# <b>clear copp statistics</b>                              | CoPP 統計情報をクリアします。                       |

**Example**

次に、インターフェイス環境で、CoPP 統計情報をクリアする例を示します。

```
switch# show policy-map interface control-plane
switch# clear copp statistics
```

## CoPP の設定例

ここでは、CoPP の設定例を示します。

## CoPP の設定例

次に、IP ACL と MAC ACL を使用する CoPP を設定する例を示します。

```
configure terminal
ip access-list copp-system-p-acl-igmp
permit igmp any 10.0.0.0/24

ip access-list copp-system-p-acl-msdp
permit tcp any any eq 639

mac access-list copp-system-p-acl-arp
permit any any 0x0806

ip access-list copp-system-p-acl-tacas
permit udp any any eq 49

ip access-list copp-system-p-acl-ntp
permit udp any 10.0.1.1/23 eq 123

ip access-list copp-system-p-acl-icmp
permit icmp any any

class-map type control-plane match-any copp-system-p-class-critical
match access-group name copp-system-p-acl-igmp
match access-group name copp-system-p-acl-msdp

class-map type control-plane match-any copp-system-p-class-normal
match access-group name copp-system-p-acl-icmp
match exception ip icmp redirect
match exception ip icmp unreachable
match exception ip option

policy-map type control-plane copp-system-p-policy

class copp-system-p-class-critical
police cir 19000 pps bc 128 packets conform transmit violate drop

class copp-system-p-class-important
police cir 500 pps bc 128 packets conform transmit violate drop

class copp-system-p-class-normal
police cir 300 pps bc 32 packets conform transmit violate drop

class class-default
```

```
police cir 50 pps bc 32 packets conform transmit violate drop

control-plane
service-policy input copp-system-p-policy
```

CoPP クラスを作成し、ACL を関連付けるには、次のようにします。

```
class-map type control-plane copp-arp-class
match access-group name copp-arp-acl
```

CoPP ポリシーにクラスを追加するには、次のようにします。

```
policy-map type control-plane copp-system-policy
class copp-arp-class
police pps 500
```

## セットアップユーティリティによるデフォルト CoPP ポリシーの変更または再適用

セットアップユーティリティを使用して CoPP のデフォルト ポリシーを再適用する例を次に示します。

```
switch# setup

---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes

Do you want to enforce secure password standard (yes/no) [y]: <CR>

Create another login account (yes/no) [n]: n

Configure read-only SNMP community string (yes/no) [n]: n

Configure read-write SNMP community string (yes/no) [n]: n

Enter the switch name : <CR>

Enable license grace period? (yes/no) [n]: n

Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: n

Configure the default gateway? (yes/no) [y]: n

Configure advanced IP options? (yes/no) [n]: <CR>
```

```

Enable the telnet service? (yes/no) [n]: y

Enable the ssh service? (yes/no) [y]: <CR>

Type of ssh key you would like to generate (dsa/rsa) : <CR>

Configure the ntp server? (yes/no) [n]: n

Configure default interface layer (L3/L2) [L3]: <CR>

Configure default switchport interface state (shut/noshut) [shut]: <CR>

Configure best practices CoPP profile (strict/moderate/lenient/dense/skip) [strict]:
strict

The following configuration will be applied:
password strength-check
no license grace-period
no telnet server enable
no system default switchport
system default switchport shutdown
policy-map type control-plane copp-system-p-policy

Would you like to edit the configuration? (yes/no) [n]: <CR>

Use this configuration and save it? (yes/no) [y]: y

switch#

```

## CoPPに関する追加情報

ここでは、CoPPの実装に関する追加情報について説明します。

### 関連資料

| 関連項目  | マニュアルタイトル                     |
|-------|-------------------------------|
| ライセンス | 『Cisco NX-OS Licensing Guide』 |

### 標準

| 標準       | タイトル                            |
|----------|---------------------------------|
| RFC 2698 | 『A Two Rate Three Color Marker』 |





## 第 12 章

# MACsec の設定

この章では、Cisco NX-OS デバイスに MACsec を設定する手順について説明します。

- [MACsec の設定 \(287 ページ\)](#)

## MACsec の設定

この章では、Cisco NX-OS デバイスに MACsec を設定する手順について説明します。

## MACsec について

Media Access Control Security (MACsec) である IEEE 802.1AE と MACsec Key Agreement (MKA) プロトコルは、イーサネットリンク上でセキュアな通信を提供します。次の機能があります。

- ライン レート暗号化機能を提供します。
- レイヤ 2 で強力な暗号化を提供することで、データの機密性を確保します。
- 整合性チェックを行い、転送中にデータを変更できないことを保証します。
- 中央集中型ポリシーを使用して選択的に有効にでき、MACsec 非対応コンポーネントがネットワークにアクセスできるようにしながら、必要に応じて適用することができます。
- レイヤ 2 ではホップバイホップ ベースでパケットを暗号化します。これにより、ネットワークは、既存のポリシーに従って、トラフィックを検査、モニター、マーク、転送できます。その点で、パケットの内容をネットワーク デバイスから隠すエンドツーエンド レイヤ 3 暗号化技術とは異なります。

## キー ライフタイムおよびヒットレス キー ロールオーバー

MACsec キー チェーンには、キー ID とオプションのライフタイムが設定された複数の事前共有キー (PSK) を含めることができます。キーのライフタイムでは、キーがいつ有効になり、いつ期限切れになるかが指定されます。ライフタイム設定が存在しない場合は、無期限のデフォルトライフタイムが使用されます。ライフタイムが構成されている場合に、ライフタイムの期限が切れると、MKA はキー チェーン内で次に構成された事前共有キーにロールオーバー

します。キーのタイムゾーンは、ローカルまたは UTC を指定できます。デフォルトの時間帯は UTC です。

MACsec キーチェーンを設定するには、[MACsec キーチェーンとキーの設定 \(292 ページ\)](#) を参照してください。

どのキーも、同じキーチェーンの中の 2 番目のキーにロールオーバーできます。それには 2 番目のキーを構成し、最初のキーではライフタイムを構成します。最初のキーのライフタイムが期限切れになると、リスト内の次のキーに自動的にロールオーバーします。同一のキーがリンクの両側で同時に構成されていた場合、キーのロールオーバーはノーヒットになります。つまり、キーはトラフィックを中断せずにロールオーバーされます。

## フォールバック キー

MACsec セッションは、キー/キー名 (CKN) のミスマッチで、またはスイッチとピア間のキーの期限が切れて、失敗する可能性があります。MACsec セッションが失敗した場合、フォールバック キーが設定されていれば、フォールバック セッションが引き継ぐことができます。フォールバック セッションは、プライマリ セッションの障害によるダウンタイムを防止し、ユーザが障害の原因となっている主要な問題を修正できるようにします。フォールバック キーは、プライマリ セッションの開始に失敗した場合のバックアップ セッションも提供します。この機能はオプションです。

MACsec フォールバック キーを設定するには、[MACsec フォールバック キーの設定 \(294 ページ\)](#) を参照してください。

## MACSec の注意事項と制約事項

MACsec に関する注意事項と制約事項は次のとおりです。

- MACsec は、次のインターフェイス タイプでサポートされます。
  - レイヤ 2 スイッチポート (アクセスとトランク) access and trunk)
  - レイヤ 3 ルーテッド インターフェイス (サブインターフェイスなし)



(注) レイヤ 3 ルーテッド インターフェイスで MACsec を有効にすると、そのインターフェイスで定義されているすべてのサブインターフェイスでも暗号化が有効になります。ただし、同じレイヤ 3 ルーテッド インターフェイスのサブインターフェイスのサブセットで MACsec を選択的に有効にすることはサポートされていません。

- 個々のレイヤ 2 およびレイヤ 3 ポート チャネル メンバー (サブインターフェイスなし)
- Secure Channel Identified (SCI) エンコーディングは、Cisco Nexus 3600 シリーズ スイッチでは無効にできません。

- リリース 10.x からダウングレードする場合、MACsec のサポートは Cisco Nexus ToR スイッチでは使用できません。
- MKA は、MACsec でサポートされている唯一のキー交換プロトコルです。Security Association Protocol (SAP) はサポートされていません。
- リンクレベルフロー制御 (LLFC) およびプライオリティフロー制御 (PFC) は、MACsec ではサポートされません。
- 同じインターフェイスに対する複数の MACsec ピア (異なる SCI 値) はサポートされません。
- **macsec shutdown** コマンドを使用して MACsec を無効にすると、MACsec 設定を保持できません。
- MACsec セッションは、最新の Rx および最新の Tx フラグが Tx SA のインストール後に最初に廃止されたキーサーバからのパケットを受け入れるのに寛容です。MACsec セッションは、セキュアな状態に収束します。
- Cisco NX-OS リリース 10.1(1) 以降では、ポリシーがインターフェイスによって参照されている間に MACsec ポリシーを変更できます。
- Cisco Nexus リリース 10.1(1) 以降では、MACsec は Cisco Nexus N3KC3636C-R プラットフォーム スイッチでサポートされます。
- N3K-C3636C-R : MACsec は、緑色でマークされた N3K-C3636C-R の次の 8 つのポートでサポートされます [ポート 29 ~ 36]。



(注) Cisco Nexus N3K-C3636C-R プラットフォーム スイッチでは、MACsec がポートで構成済みまたは未構成の場合のどちらでも、MACsec セキュリティポリシー タイプに関係なく、ポートフラッシュが発生します。

- Cisco Nexus 3600 シリーズ スイッチは、QSA が使用されている場合、MACsec 対応ポートで MACsec をサポートしません。
- MACsec はブレイクアウト ポートではサポートされません。また、MACsec が構成されている場合、N3K-C3636C-R のポート 29 からポート 36 までの 8 つのポートではブレイクアウトがサポートされません。
- MACsec ポリシーの **conf-offset** パラメータが動的に変更された場合、パケットは短期間ドロップされます。ポリシーがポートでアクティブでない場合は、静的構成でのみ **conf-offset** パラメータを変更してください。
- Cisco Nexus リリース 10.3(3)F 以降、MACsec は Cisco N3K-C36180YC-R スイッチでサポートされますが、次の制限があります：
  - MACsec は、Eth1/49、Eth1/51、Eth1/52、Eth1/53、および Eth1/54 ポートでのみサポートされます。

- Eth1/50 ポートでは MACsec がリンクをダウンさせるため、構成しないでください。

#### キーチェーンの制限：

- MACsec キーのオクテット文字列は上書きできません。代わりに、新しいキーまたは新しいキーチェーンを作成する必要があります。
- end または exit を入力すると、キーチェーンの新しいキーが設定されます。エディタ モードのデフォルトのタイムアウト値は 6 秒です。キーがキー オクテット文字列または 6 秒間の送信ライフタイムで設定されていない場合、MACsec セッションを起動するために不完全な情報が使用され、セッションが承認保留状態のままになる可能性があります。設定の完了後に MACsec セッションがコンバージされない場合は、ポートをシャットダウン/非シャットダウンすることをお勧めします。
- 指定したキーチェーンでは、キーの有効期間を重複させて、有効なキーの不在期間を避ける必要があります。キーがアクティブ化されない期間が発生すると、セッション ネゴシエーションが失敗し、トラフィックがドロップされる可能性があります。MACsec キー ロールオーバーでは、現在アクティブなキーの中で最も遅い開始時刻のキーが優先されます。

#### フォールバックの制限：

- MACsec セッションが古いプライマリキーで保護されている場合、最新のアクティブなプライマリ キーが一致しない場合、フォールバックセッションには進みません。そのため、セッションは古いプライマリ キーで保護されたままになり、ステータスが古い CA のキー再生成として表示されます。プライマリ PSK の新しいキーの MACsec セッションは init 状態になります。
- フォールバック キーチェーンでは、無期限のキーを 1 つだけ使用します。複数のキーはサポートされていません。
- フォールバック キー チェーンで使用されるキー ID (CKN) は、プライマリ キー チェーンで使用されるキー ID (CKN) のいずれとも一致しないようにしてください。
- 一度設定すると、インターフェイスのすべての MACsec 設定が削除されない限り、インターフェイスのフォールバック設定は削除できません。

#### MACsec ポリシーの制限：

- MACsec セッションがセキュアになる前に、BPDU パケットを送信できます。

#### レイヤ 2 トンネリング プロトコル (L2TP) の制限：

- MACsec は、dot1q トンネリングまたは L2TP 用に設定されたポートではサポートされません。

- 非ネイティブ VLAN のトランク ポートで STP が有効になっている場合、L2TP は機能しません。

#### 統計の制限：

- MACsec モードと非 MACsec モード（通常のポート シャットダウン/非シャットダウン）の間の移行中に発生する CRC エラーはほとんどありません。
- IEEE8021-SECY-MIB OID secyRxSASStatsOKPkts、secyTxSASStatsProtectedPkts、および secyTxSASStatsEncryptedPkts は最大 32 ビットのカウンタ値しか伝送できませんが、トラフィックは 32 ビットを超える可能性があります。

## MACsec の有効化

MACsec および MKA コマンドにアクセスする前に、MACsec 機能を有効に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 | <b>configure terminal</b><br><br>例：<br>switch# <b>configure terminal</b><br>switch(config)#                           | グローバル コンフィギュレーション モードを開始します               |
| ステップ 2 | <b>feature macsec</b><br><br>例：<br>switch(config)# <b>feature macsec</b>                                              | デバイスで MACsec および MKA を有効にします。             |
| ステップ 3 | (任意) <b>copy running-config startup-config</b><br><br>例：<br>switch(config)# <b>copy running-config startup-config</b> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。 |

## MACsec の無効化

Cisco NX-OS リリース 10.1(1) 以降では、MACsec 機能を無効にしても、この機能が非アクティブ化されるだけで、関連する MACsec 設定は削除されません。

MACsec の無効化には、次の条件があります。

- MACsec shutdown はグローバルコマンドであり、インターフェイス レベルでは使用できません。

- `macsec shutdown`、`show macsec mka session/summary`、`show macsec mka session detail`、および `show macsec mka/secy statistics` コマンドは、「Macsec is shutdown」メッセージを表示します。ただし、`show macsec policy` および `show key chain` コマンドは出力を表示します。
- 連続する MACsec ステータスが `macsec shutdown` から `no macsec shutdown` に変更された場合、またはその逆の場合は、ステータス変更の間に 30 秒の間隔が必要です。

## 手順

|        | コマンドまたはアクション                                                                                                                 | 目的                                                                                                                                                                   |
|--------|------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br><pre>switch# configure terminal switch(config)#</pre>                                    | グローバル コンフィギュレーション モードを開始します                                                                                                                                          |
| ステップ 2 | <b>macsec shutdown</b><br>例 :<br><pre>switch(config)# macsec shutdown</pre>                                                  | デバイスの MACsec 設定を無効にします。 <b>no</b> オプションは、MACsec 機能を復元します。                                                                                                            |
| ステップ 3 | (任意) <code>copy running-config startup-config</code><br>例 :<br><pre>switch(config)# copy running-config startup-config</pre> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。この手順は、スイッチのリロード後に MACsec をシャットダウン状態に維持する場合にのみ必要です。<br><br>(注)<br><b>no feature macsec</b> コマンドを使用して MACsec 機能を無効にすることもできます。 |

## MACsec キーチェーンとキーの設定

デバイスに MACsec キーチェーンとキーを作成できます。



(注) MACsec キーチェーンのみが MKA セッションをコンバージします。

始める前に

MACsec が有効であることを確認します。

## 手順

|        | コマンドまたはアクション                                                                                                                                                                                                                                                                        | 目的                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例 :<br><pre>switch# configure terminal switch(config)#</pre>                                                                                                                                                                                       | グローバル設定モードを開始します。                                                                                                                                                                                                                                                                                                                                                                                                   |
| ステップ 2 | (任意) <b>[no] key-chain macsec-psk no-show</b><br><br>例 :<br><pre>switch(config)# key-chain macsec-psk no-show</pre>                                                                                                                                                                 | <b>show running-config</b> および <b>show startup-config</b> コマンドの出力で、暗号化されたキー オクテット文字列をワイルドカード文字に置き換えて非表示にします。デフォルトでは、PSK キーは暗号化形式で表示され、簡単に復号化できます。このコマンドは、MACsec キーチェーンにのみ適用されます。<br><br>(注)<br>オクテット文字列は、設定をファイルに保存するときにも非表示になります。                                                                                                                                                                                  |
| ステップ 3 | <b>key chain namemacsec</b><br><br>例 :<br><pre>switch(config)# key chain 1 macsec switch(config-macseckeychain)#</pre>                                                                                                                                                              | MACSec キーチェーンを作成して MACSec キーのセットを保持し、MACSec キーチェーン設定モードを開始します。                                                                                                                                                                                                                                                                                                                                                      |
| ステップ 4 | <b>key key-id</b><br><br>例 :<br><pre>switch(config-macseckeychain)# key 1000 switch(config-macseckeychain-macseckey)#</pre>                                                                                                                                                         | MAC secキーを作成し、MACsec キー設定モードを開始します。範囲は 1〜32 オクテットで、最大サイズは 64 です。<br><br>(注)<br>キーの文字数は偶数でなければなりません。                                                                                                                                                                                                                                                                                                                 |
| ステップ 5 | <b>key-octet-string octet-string cryptographic-algorithm {AES_128_CMAC   AES_256_CMAC}</b><br><br>例 :<br><pre>switch(config-macseckeychain-macseckey)# key-octet-string ab0def0123456789ab0def0123456789ab0def0123456789ab0def0123456789 cryptographic-algorithm AES_256_CMAC</pre> | そのキーの octet スtringを設定します。octet-string 引数には、最大 64 文字の 16 進数文字を含めることができます。octet キーは内部でエンコードされるため、クリア テキストのキーは <b>show running-config macsec</b> コマンドの出力に表示されません。<br><br>キーオクテット文字列には、次のものが含まれます。 <ul style="list-style-type: none"> <li>• 0 暗号化タイプ - 暗号化なし (デフォルト)</li> <li>• 6 暗号化タイプ - 独自仕様 (タイプ 6 暗号化)。詳細については、MACsec キーでタイプ 6 暗号化を有効にするを参照してください。</li> <li>• 7 暗号化タイプ - 最大 64 文字の、独自仕様 WORD キー オクテット文列</li> </ul> |

|        | コマンドまたはアクション                                                                                                                                                            | 目的                                                                                                                                                                                                |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        |                                                                                                                                                                         | <p>(注)</p> <p>AES_128_CMAC 暗号化アルゴリズムを使用するためには、MACsec ピアは同じ Cisco NX-OS リリースを実行する必要があります。以前のリリースと、Cisco NX-OS リリース 7.0(3)I7(2) 以降のリリース間で相互運用できるようにするには、キーを AES_256_CMAC 暗号化アルゴリズムで使用する必要があります。</p> |
| ステップ 6 | <b>send-lifetime start-time duration duration</b><br><br>例 :<br><pre>switch(config-macseckeychain-macseckey) # send-lifetime 00:00:00 Oct 04 2016 duration 100000</pre> | <p>キーの送信ライフタイムを設定します。デフォルトでは、デバイスは開始時間を UTC として扱います。</p> <p><i>start-time</i> 引数は、キーがアクティブになる日時です。<i>duration</i> 引数はライフタイムの長さ (秒) です。最大値は 2147483646 秒 (約 68 年) です。</p>                          |
| ステップ 7 | (任意) <b>show key chain name</b><br><br>例 :<br><pre>switch(config-macseckeychain-macseckey) # show key chain 1</pre>                                                     | キーチェーンの設定を表示します。                                                                                                                                                                                  |
| ステップ 8 | (任意) <b>copy running-config startup-config</b><br><br>例 :<br><pre>switch(config-macseckeychain-macseckey) # copy running-config startup-config</pre>                    | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                                                                                                                         |

## MACsec フォールバック キーの設定

Cisco NX-OS リリース 10.1(1) 以降では、プライマリ セッションがスイッチとピア間のキー/キー名 (CKN) のミスマッチまたはキーの有効期限の結果として失敗した場合にバックアップセッションを開始するよう、デバイスのフォールバック キーを設定できます。

### 始める前に

MACsec が有効になっており、プライマリおよびフォールバック キーチェーンとキー ID が設定されていることを確認します。「[MACsec キーチェーンとキーの設定 \(292 ページ\)](#)」を参照してください。

### 手順

|        | コマンドまたはアクション                         | 目的                |
|--------|--------------------------------------|-------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例 : | グローバル構成モードを開始します。 |



|        | コマンドまたはアクション                                                                                                                                                                                                                      | 目的                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        | <pre>switch# configure terminal switch(config)#</pre>                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                      |
| ステップ 2 | <b>interface</b> <i>name</i><br><br>例 :<br><pre>switch(config)# interface ethernet 1/29 switch(config-if)#</pre>                                                                                                                  | 設定するインターフェイスを指定します。インターフェイス タイプと ID を指定できます。イーサネット ポートの場合は、「ethernet slot / port」を使用します。                                                                                                                                                                                                                                                                                                             |
| ステップ 3 | <b>macsec keychain</b> <i>keychain-name</i> <b>policy</b> <i>policy-name</i><br><b>fallback-keychain</b> <i>keychain-name</i><br><br>例 :<br><pre>switch(config-if)# macsec keychain kc2 policy abc fallback-keychain fb_kc2</pre> | <p>キー/キー ID のミスマッチまたはキーの期限切れによる MACsec セッションの失敗後に使用するフォールバック キーチェーンを指定します。フォールバック キー ID は、プライマリ キーチェーンのキー ID と一致してはなりません。</p> <p>フォールバック キーチェーン名を変更して同じコマンドを再発行することで、MACsec 設定を削除せずに、各インターフェイスのフォールバック キーチェーン設定を対応するインターフェイスで変更できます。</p> <p>(注)<br/>コマンドは、フォールバック キーチェーン名を除き、インターフェイスの既存のコンフィギュレーション コマンドとまったく同じように入力する必要があります。</p> <p>「<a href="#">MACsec キーチェーンとキーの設定 (292 ページ)</a>」を参照してください。</p> |
| ステップ 4 | (任意) <b>copy running-config startup-config</b><br><br>例 :<br><pre>switch(config-if)# copy running-config startup-config</pre>                                                                                                     | 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。                                                                                                                                                                                                                                                                                                                                                           |

## MACsec ポリシーの設定

異なるパラメータを使用して複数の MACsec ポリシーを作成できます。しかし、1 つのインターフェイスでアクティブにできるポリシーは 1 つのみです。

### 始める前に

MACsec が有効であることを確認します。

## 手順

|        | コマンドまたはアクション                                                                                                   | 目的                                                                                                                                                                                                                               |
|--------|----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br><pre>switch# configure terminal switch(config)#</pre>                      | グローバル構成モードを開始します。                                                                                                                                                                                                                |
| ステップ 2 | <b>macsec policy name</b><br>例 :<br><pre>switch(config)# macsec policy abc switch(config-macsec-policy)#</pre> | MACsec ポリシーを作成します。                                                                                                                                                                                                               |
| ステップ 3 | <b>cipher-suite name</b><br>例 :<br><pre>switch(config-macsec-policy)# cipher-suite GCM-AES-256</pre>           | 次のいずれかの暗号方式を構成します。<br><br>GCM-AES-128、GCM-AES-256、<br>GCM-AES-XPB-128、または GCM-AES-XPB-256。                                                                                                                                       |
| ステップ 4 | <b>key-server-priority number</b><br>例 :<br><pre>switch(config-macsec-policy)# key-server-priority 0</pre>     | キー交換中はピア間の接続が解除されるように、キー サーバのプライオリティを設定します。範囲は0（最高）～255（最低）で、デフォルト値は16です。                                                                                                                                                        |
| ステップ 5 | <b>security-policy name</b><br>例 :<br><pre>switch(config-macsec-policy)# security-policy should-secure</pre>   | 次のいずれかのセキュリティポリシーを設定して、データおよび制御パケットの処理を定義します。 <ul style="list-style-type: none"> <li>• <b>must-secure</b> : MACsec ヘッダーを持たないパケットはドロップされます。</li> <li>• <b>should-secure</b> : MACsec ヘッダーを持たないパケットも許可されます。これはデフォルト値です。</li> </ul> |
| ステップ 6 | <b>window-size number</b><br>例 :<br><pre>switch(config-macsec-policy)# window-size 512</pre>                   | インターフェイスが、設定されたウィンドウ サイズ未満のパケットを受け入れないように、再生保護ウィンドウを設定します。範囲は0～596000000です。                                                                                                                                                      |
| ステップ 7 | <b>sak-expiry-time time</b><br>例 :<br><pre>switch(config-macsec-policy)# sak-expiry-time 100</pre>             | SAK キー再生成を強制する時間を秒単位で設定します。このコマンドを使用して、セッション キーを予測可能な時間間隔に変更できます。デフォルトは0です。                                                                                                                                                      |
| ステップ 8 | <b>conf-offset name</b><br>例 :                                                                                 | 暗号化を開始するレイヤ 2 フレームの機密性オフセットの1つとして、CONF-OFFSET-0、                                                                                                                                                                                 |

|         | コマンドまたはアクション                                                                                                                                     | 目的                                                                                                                       |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
|         | <code>switch(config-macsec-policy)# <b>conf-offset</b> <b>CONF-OFFSET-0</b></code>                                                               | CONF-OFFSET-30、またはCONF-OFFSET-50 のいずれかを設定します。<br><br>このコマンドは、中間スイッチがパケットヘッダー {dmac、smac、etype} を MPLS タグのように使用するために必要です。 |
| ステップ 9  | (任意) <b>show macsec policy</b><br><br>例：<br><code>switch(config-macsec-policy)# <b>show macsec policy</b></code>                                 | MACSec ポリシー設定を表示します。                                                                                                     |
| ステップ 10 | (任意) <b>copy running-config startup-config</b><br><br>例：<br><code>switch(config-macsec-policy)# <b>copy running-config startup-config</b></code> | 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。                                                                                |

## PSK のローテーション

SAK の有効期限が MACsec ポリシーで 60 秒に設定されている場合は、次の手順に従って PSK を切り替えます。

### 手順

**ステップ 1** **no sak-expiry-time** コマンドを使用して、MACsec ポリシーから SAK 期限切れタイマーを削除します。

設定内のポリシーの数だけ、SAK の有効期限タイマーを削除する必要があります。インターフェイスごとに削除する必要はありません。ポリシーを 1 つだけ定義してすべてのインターフェイスに適用した場合は、このポリシーからのみ SAK の有効期限タイマーを削除する必要があります。

**ステップ 2** 2 分間待機します。

**ステップ 3** **key key-id** コマンドを使用して、キーチェーンの下に新しいキーをプログラムします。

**ステップ 4** 新しいキーとのセッションがセキュア化されたら、**no key key-id** コマンドを使用して古いキーを削除します。

**ステップ 5** 2 分間待機します。

**ステップ 6** **sak-expiry-timer 60** コマンドを使用して、SAK キー再生成タイマーを MACsec ポリシーに追加します。

## MACsec 設定の確認

MACsec 設定情報を表示するには、次のいずれかの作業を実行します。

| コマンド                                                               | 目的                                                        |
|--------------------------------------------------------------------|-----------------------------------------------------------|
| <b>show key chain name</b>                                         | キーチェーンの設定を表示します。                                          |
| <b>show macsec mka session [interface type slot/port] [detail]</b> | 特定のインターフェイスまたはすべてのインターフェイスの MACsec MKA セッションに関する情報を表示します。 |
| <b>show macsec mka session details</b>                             | MAC アドレスに関する情報を表示します。                                     |
| <b>show macsec mka summary</b>                                     | MACsec MKA 設定を表示します。                                      |
| <b>show macsec policy [policy-name]</b>                            | 特定の MACsec ポリシーまたはすべての MACsec ポリシーの設定を表示します。              |
| <b>show running-config macsec</b>                                  | MACsec の実行コンフィギュレーション情報を表示します。                            |

次に、すべてのインターフェイスの MACsec MKA セッションに関する情報を表示する例を示します。

```
switch(config)# show macsec mka session
Interface          Local-TxSCI          # Peers      Status
  Key-Server      Auth Mode
-----
Ethernet1/29      6c8b.d3db.e968/0001      1      Secured
  No              PRIMARY-PSK
Ethernet1/30      6c8b.d3db.e96c/0001      1      Secured
  No              PRIMARY-PSK
Ethernet1/31      6c8b.d3db.e970/0001      1      Secured
  Yes             PRIMARY-PSK
Ethernet1/32      6c8b.d3db.e974/0001      1      Secured
  Yes             PRIMARY-PSK
Ethernet1/33      6c8b.d3db.e978/0001      1      Secured
  Yes             PRIMARY-PSK
Ethernet1/34      6c8b.d3db.e97c/0001      1      Secured
  Yes             PRIMARY-PSK
Ethernet1/35      6c8b.d3db.e980/0001      1      Secured
  Yes             PRIMARY-PSK
Ethernet1/36      6c8b.d3db.e984/0001      1      Secured
  No              PRIMARY-PSK
-----
Total Number of Sessions : 8
  Secured Sessions : 8
  Pending Sessions : 0
switch(config)#
```

次に、特定のインターフェイスの MACsec MKA セッションに関する情報を表示する例を示します。前の例で説明したテーブルの一般的な要素に加えて、現在の MACsec セッションタイプを定義する認証モードも示します。

```
switch(config)# show macsec mka session interface e1/35
Interface          Local-TxSCI          # Peers      Status
  Key-Server      Auth Mode
-----
-----
```

```

Ethernet1/35      6c8b.d3db.e980/0001      1      Secured
Yes              PRIMARY-PSK
switch(config)#

```

次に、特定のイーサネット インターフェイスの MACsec MKA セッションに関する詳細情報を表示する例を示します。

```

switch(config)# show macsec mka session interface e1/35 details
Detailed Status for MKA Session
-----
Interface Name      : Ethernet1/35
Session Status      : SECURED - Secured MKA Session with MACsec
Local Tx-SCI        : 6c8b.d3db.e980/0001
Local Tx-SSCI       : 2
MKA Port Identifier : 2
CAK Name (CKN)      : 2006
CA Authentication Mode : PRIMARY-PSK
Member Identifier (MI) : 50BE8367F1C6D0AB1C442229
Message Number (MN) : 1048
MKA Policy Name      : mpsr1
Key Server Priority  : 1
Key Server           : Yes
Include ICV          : Yes
SAK Cipher Suite     : GCM-AES-128
SAK Cipher Suite (Operational) : GCM-AES-128
Replay Window Size   : 148809600
Confidentiality Offset : CONF-OFFSET-30
Confidentiality Offset (Operational) : CONF-OFFSET-30
Latest SAK Status    : Rx & TX
Latest SAK AN        : 0
Latest SAK KI        : 50BE8367F1C6D0AB1C44222900000021
Latest SAK KN        : 33
Last SAK key time     : 11:23:53 pst Tue Dec 15 2020
CA Peer Count        : 1
Eapol dest mac       : 0180.c200.0003
Ether-type           : 0x888e
Peer Status:
Peer MI              : 37AFE73EC8617FD32F70E21A
RxSCI                : 6c8b.d3db.e984/0001
Peer CAK             : Match
Latest Rx MKPDU      : 11:24:52 pst Tue Dec 15 2020
Fallback Data:
Fallback CKN         : FB2004
Fallback MI          : 849D72D5F6A900F5B0718C78
Fallback MN          : 0x3d6
Fallback Peer:
Peer MI              : 8DCE8CBE67B474D2C2955F58
RxSCI                : 6c8b.d3db.e984/0001
Peer CAK             : Match
Latest Rx MKPDU      : 11:24:52 pst Tue Dec 15 2020
switch(config)#

```

次に、MACsec MKA 設定を表示する例を示します。

```

switch# show macsec mka summary
Interface      MACSEC-policy      Keychain
-----
Ethernet2/13   1                   1/100000000000000000
Ethernet2/14   1                   1/100000000000000000
switch#

```

次に、すべての MACsec ポリシーの設定を表示する例を示します。

```

switch# show macsec policy
MACSec Policy Cipher Pri Window Offset Security SAK Rekey time ICV Indicator

```

```

-----
system-default-macsec-policy GCM-AES-XPB-256 16 148809600 0 should-secure
pn-rollover FALSE
tests1 GCM-AES-XPB-256 16 148809600 0 should-secure
pn-rollover FALSE
tests2 GCM-AES-XPB-256 16 148809600 0 should-secure
pn-rollover FALSE
tests3 GCM-AES-256 16 148809600 0 should-secure
pn-rollover FALSE

```

次の例では、**key-chain macsec-psk no-show** コマンドが構成されていない場合に **show running-config** および **show startup-config** コマンドの出力のキー オクテット文字列を表示します：

```

key chain KC256-1 macsec
  key 2000
    key-octet-string 7
075e701e1c5a4a5143475e5a527d7c7c706a6c724306170103555a5c57510b051e47080
a05000101005e0e50510f005c4b5f5d0b5b070e234e4d0a1d0112175b5e cryptographic-algorithm
AES_256_CM4C

```

次の例では、**key-chain macsec-psk no-show** コマンドが構成されている場合に **show running-config** および **show startup-config** コマンドの出力のキー オクテット文字列を表示します：

```

key chain KC256-1 macsec
  key 2000
    key-octet-string 7 ***** cryptographic-algorithm AES_256_CM4C

```

## MACsec 統計の表示

次のコマンドを使用して、MACsec 統計情報を表示できます。

| コマンド                                                          | 目的                       |
|---------------------------------------------------------------|--------------------------|
| <b>show macsec mka statistics</b> [interface type slot/port]  | MACsec MKA 統計情報を表示します。   |
| <b>show macsec secy statistics</b> [interface type slot/port] | MACsec セキュリティ統計情報を表示します。 |

次に、特定のイーサネット インターフェイスの MACsec MKA 統計情報の例を示します。

```

switch# show macsec mka statistics interface ethernet 1/29
MKA Statistics for Session on interface (Ethernet1/29)
=====
CA Statistics
  Pairwise CAK Rekeys..... 0

SA Statistics
  SAKs Generated..... 0
  SAKs Rekeyed..... 0
  SAKs Received..... 0
  SAK Responses Received.. 0

MKPDU Statistics
  MKPDUs Transmitted..... 41
  "Distributed SAK".. 0
  MKPDUs Validated & Rx... 41
  "Distributed SAK".. 0

```

```

MKA IDB Statistics
MKPDUs Tx Success..... 82
MKPDUs Tx Fail..... 0
MKPDUS Tx Pkt build fail... 0
MKPDUS No Tx on intf down.. 0
MKPDUS No Rx on intf down.. 0
MKPDUs Rx CA Not found..... 0
MKPDUs Rx Error..... 0
MKPDUs Rx Success..... 82

MKPDU Failures
MKPDU Rx Validation ..... 0
MKPDU Rx Bad Peer MN..... 0
MKPDU Rx Non-recent Peerlist MN..... 0
MKPDU Rx Drop SAKUSE, KN mismatch..... 0
MKPDU Rx Drop SAKUSE, Rx Not Set..... 0
MKPDU Rx Drop SAKUSE, Key MI mismatch.... 0
MKPDU Rx Drop SAKUSE, AN Not in Use..... 0
MKPDU Rx Drop SAKUSE, KS Rx/Tx Not Set... 0
MKPDU Rx Drop Packet, Ethertype Mismatch. 0
MKPDU Rx Drop Packet, DestMAC Mismatch... 0

SAK Failures
SAK Generation..... 0
Hash Key Generation..... 0
SAK Encryption/Wrap..... 0
SAK Decryption/Unwrap..... 0

CA Failures
ICK Derivation..... 0
KEK Derivation..... 0
Invalid Peer MACsec Capability... 0

MACsec Failures
Rx SA Installation..... 0
Tx SA Installation..... 0

switch(config)#

```

次に、特定のイーサネット インターフェイスの MACsec セキュリティ統計情報を表示する例を示します。



(注) Rx および Tx 統計情報の非制御パケットと制御パケットには、次の違いがあります。

- Rx 統計
  - 非制御=暗号化および非暗号化
  - 制御 = 非暗号化
- TX 統計情報 :
  - 非制御 = 非暗号化
  - 制御 = 暗号化
  - 共通 = 暗号化および非暗号化

```

switch(config)# show macsec secy statistics interface e1/29
Interface Ethernet1/29 MACSEC SecY Statistics:
-----
Interface Rx Statistics:
  Unicast Uncontrolled Pkts: 8067779
  Multicast Uncontrolled Pkts: 14
  Broadcast Uncontrolled Pkts: 0
  Uncontrolled Pkts - Rx Drop: 0
  Uncontrolled Pkts - Rx Error: 0
  Unicast Controlled Pkts: N/A (N3K-C3636C-R not supported)
  Multicast Controlled Pkts: N/A (N3K-C3636C-R not supported)
  Broadcast Controlled Pkts: N/A (N3K-C3636C-R not supported)
  Controlled Pkts: 8056748
  Controlled Pkts - Rx Drop: N/A (N3K-C3636C-R not supported)
  Controlled Pkts - Rx Error: N/A (N3K-C3636C-R not supported)
  In-Octets Uncontrolled: 37641828280 bytes
  In-Octets Controlled: 37324295914 bytes
  Input rate for Uncontrolled Pkts: N/A (N3K-C3636C-R not supported)
  Input rate for Uncontrolled Pkts: N/A (N3K-C3636C-R not supported)
  Input rate for Controlled Pkts: N/A (N3K-C3636C-R not supported)
  Input rate for Controlled Pkts: N/A (N3K-C3636C-R not supported)

Interface Tx Statistics:
  Unicast Uncontrolled Pkts: N/A (N3K-C3636C-R not supported)
  Multicast Uncontrolled Pkts: N/A (N3K-C3636C-R not supported)
  Broadcast Uncontrolled Pkts: N/A (N3K-C3636C-R not supported)
  Uncontrolled Pkts - Rx Drop: N/A (N3K-C3636C-R not supported)
  Uncontrolled Pkts - Rx Error: N/A (N3K-C3636C-R not supported)
  Unicast Controlled Pkts: N/A (N3K-C3636C-R not supported)
  Multicast Controlled Pkts: N/A (N3K-C3636C-R not supported)
  Broadcast Controlled Pkts: N/A (N3K-C3636C-R not supported)
  Controlled Pkts: 8049279
  Controlled Pkts - Rx Drop: N/A (N3K-C3636C-R not supported)
  Controlled Pkts - Rx Error: N/A (N3K-C3636C-R not supported)
  Out-Octets Uncontrolled: N/A (N3K-C3636C-R not supported)
  Out-Octets Controlled: 37262189352 bytes
  Out-Octets Common: 37699748491 bytes
  Output rate for Uncontrolled Pkts: N/A (N3K-C3636C-R not supported)
  Output rate for Uncontrolled Pkts: N/A (N3K-C3636C-R not supported)
  Output rate for Controlled Pkts: N/A (N3K-C3636C-R not supported)
  Output rate for Controlled Pkts: N/A (N3K-C3636C-R not supported)

SECY Rx Statistics:
  Transform Error Pkts: N/A (N3K-C3636C-R not supported)
  Control Pkts: 0
  Untagged Pkts: N/A (N3K-C3636C-R not supported)
  No Tag Pkts: 0
  Bad Tag Pkts: 0
  No SCI Pkts: 0
  Unknown SCI Pkts: 0
  Tagged Control Pkts: N/A (N3K-C3636C-R not supported)

SECY Tx Statistics:
  Transform Error Pkts: N/A (N3K-C3636C-R not supported)
  Control Pkts: 0
  Untagged Pkts: N/A (N3K-C3636C-R not supported)

SAK Rx Statistics for AN [0]:
  Unchecked Pkts: 0
  Delayed Pkts: 0
  Late Pkts: 0
  OK Pkts: 8056748
  Invalid Pkts: 0
  Not Valid Pkts: 0

```



```

Not-Using-SA Pkts: 0
Unused-SA Pkts: 0
Decrypted In-Octets: 36952542946 bytes
Validated In-Octets: 0 bytes

SAK Tx Statistics for AN [0]:
  Encrypted Protected Pkts: 8049279
  Too Long Pkts: N/A (N3K-C3636C-R not supported)
  SA-not-in-use Pkts: N/A (N3K-C3636C-R not supported)
  Encrypted Protected Out-Octets: 36909704659 bytes

switch(config)#

```

## MACsec の設定例

次に、ユーザ定義のMACsecポリシーを設定し、そのポリシーをインターフェイスに適用する例を示します。

```

switch(config)# macsec policy mpsr1
switch(config-macsec-policy)# cipher-suite GCM-AES-128
switch(config-macsec-policy)# key-server-priority 1
switch(config-macsec-policy)# window-size 1000
switch(config-macsec-policy)# conf-offset CONF-OFFSET-30
switch(config-macsec-policy)# security-policy must-secure
switch(config-macsec-policy)# sak-expiry-time 60
switch(config-macsec-policy)# include-icv-indicator

switch(config-macsec-policy)# interface e1/35-36
switch(config-if-range)# macsec keychain ksr policy mpsr1
switch(config-if-range)# show macsec mka session

```

| Interface    | Local-TxSCI         | # Peers | Status  |
|--------------|---------------------|---------|---------|
| Key-Server   | Auth Mode           |         |         |
| Ethernet1/35 | 6c8b.d3db.e980/0001 | 1       | Secured |
| Yes          | PRIMARY-PSK         |         |         |
| Ethernet1/36 | 6c8b.d3db.e984/0001 | 1       | Secured |
| No           | PRIMARY-PSK         |         |         |

```

switch(config-if-range)# show macsec mka summary
Interface      Status  Cipher (Operational)  Key-Server  MACSEC-policy
Keychain      Fallback-keychain
-----
Ethernet1/35   Secured  GCM-AES-128          Yes          mpsr1
ksr            no keychain
Ethernet1/36   Secured  GCM-AES-128          No           mpsr1
ksr            no keychain

switch(config-if-range)# show running-config macsec
!Command: show running-config macsec
!Running configuration last done at: Tue Dec 15 11:41:53 2020
!Time: Tue Dec 15 11:45:06 2020

version 10.1(1) Bios:version 01.14
feature macsec

macsec policy mpsr1
  cipher-suite GCM-AES-128
  key-server-priority 1

```

```

window-size 1000
conf-offset CONF-OFFSET-30
sak-expiry-time 60
include-icv-indicator

interface Ethernet1/35
  macsec keychain ksr policy mpsrl

interface Ethernet1/36
  macsec keychain ksr policy mpsrl

```

次に、MACsec キーチェーンを設定し、インターフェイスにシステムデフォルトの MACsec ポリシーを追加する例を示します。

```

switch(config)# key chain ksr macsec
switch(config-macsec-keychain)# key 2006
switch(config-macsec-keychain-macsec-key)# key-octet-string
1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef cryptographic-algorithm
AES_256_CMAC
switch(config-macsec-keychain-macsec-key)# interface e1/35-36
switch(config-if-range)# macsec keychain ksr

switch(config-if-range)# show running-config macsec
!Command: show running-config macsec
!Running configuration last done at: Tue Dec 15 11:53:10 2020
!Time: Tue Dec 15 11:54:40 2020

version 10.1(1) Bios:version 01.14
feature macsec

interface Ethernet1/35
  macsec keychain ksr policy system-default-macsec-policy

interface Ethernet1/36
  macsec keychain ksr policy system-default-macsec-policy

switch(config-if-range)# show macsec mka summary
Interface      Status    Cipher (Operational)  Key-Server  MACSEC-policy
      Keychain                               Fallback-keychain
-----
Ethernet1/35    Secured   GCM-AES-XPB-256      Yes
system-default-macsec-policy    ksr                                no keychain

Ethernet1/36    Secured   GCM-AES-XPB-256      No
system-default-macsec-policy    ksr                                no keychain

switch(config-if-range)# show macsec mka session
Interface      Local-TxSCI      # Peers      Status
      Key-Server      Auth Mode
-----
Ethernet1/35    6c8b.d3db.e980/0001    1    Secured
      Yes      PRIMARY-PSK
Ethernet1/36    6c8b.d3db.e984/0001    1    Secured
      No      PRIMARY-PSK

Total Number of Sessions : 2
  Secured Sessions : 2
  Pending Sessions : 0

```

```
switch(config-if-range)#
```

## XML の例

MACsec は、`|xml` を使用したスクリプト用に次の **show** コマンドの XML 出力をサポートします。

- **show key chain name |xml**
- **show macsec mka session interface interface slot/port details |xml**
- **show macsec mka statistics interface interface slot/port |xml**
- **show macsec mka summary |xml**
- **show macsec policy name |xml**
- **show macsec secy statistics interface interface slot/port |xml**
- **show running-config macsec |xml**

次に、上記の各 **show** コマンドの出力例を示します。

### 例 1：キーチェーンの構成を表示します

```
switch(config)# show key chain "ksr" | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns="http://www.cisco.com/nxos:1.0:rpm"
  xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0">
  <nf:data>
    <show>
      <key>
        <chain>
          <__XML__OPT_Cmd_rpm_show_keychain_cmd_keychain>
            <keychain>ksr</keychain>
            <__XML__OPT_Cmd_rpm_show_keychain_cmd__readonly__>
              <__readonly__>
                <TABLE_keychain>
                  <ROW_keychain>
                    <chain_name>ksr</chain_name>
                    <TABLE_key>
                      <ROW_key>
                        <key_id>2006</key_id>
                        <key_string>075e731fa5c4524f45b0d0629f212e6267147524054590f096951570a06e470101030604020c520b0705b530115576085653697614175918071416e0a</key_string>
                        <crypto_algo>AES_256_CM&O=AC</crypto_algo>
                        <send_valid>true</send_valid>
                      </ROW_key>
                    </TABLE_key>
                  </ROW_keychain>
                </TABLE_keychain>
              </__readonly__>
            </__XML__OPT_Cmd_rpm_show_keychain_cmd__readonly__>
          </__XML__OPT_Cmd_rpm_show_keychain_cmd_keychain>
        </chain>
      </key>
    </show>
  </nf:data>
</nf:rpc-reply>
```

```
]]>]]>
switch(config)#
```

## 例 2 : 特定のインターフェイスの MACsec MKA セッションに関する情報を表示します

```
switch(config)# show macsec mka session interface e1/35 details | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns="http://www.cisco.com/nxos:1.0:cts"
xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0">
<nf:data>
  <show>
    <macsec>
      <mka>
        <session>
          <__XML__OPT_Cmd_show_macsec_mka_session_interface>
            <interface>
              <__XML__INTF_ifname>
                <__XML__PARAM_value>
                  <__XML__INTF_output>Ethernet1/35</__XML__INTF_output>
                </__XML__PARAM_value>
              </__XML__INTF_ifname>
            </interface>
          <__XML__OPT_Cmd_show_macsec_mka_session_details>
            <details/>
          <__XML__OPT_Cmd_show_macsec_mka_session__readonly__>
            <__readonly__>
              <TABLE_mka_session_details>
                <ROW_mka_session_details>
                  <ifname>Ethernet1/35</ifname>
                  <status>SECURED - Secured MKA Session with MACsec</status>
                  <sci>6c8b.d3db.e980/0001</sci>
                  <ssci>2</ssci>
                  <port_id>2</port_id>
                  <ckn>2006</ckn>
                  <ca_auth_mode>PRIMARY-PSK</ca_auth_mode>
                  <mi>5AABE0AB9CC867AB0FF40F7D</mi>
                  <mn>3550</mn>
                  <policy>system-default-macsec-policy</policy>
                  <ks_prio>16</ks_prio>
                  <keyserver>Yes</keyserver>
                  <include_icv_indicator>No</include_icv_indicator>
                  <cipher>GCM-AES-XPB-256</cipher>
                  <cipher_operational>GCM-AES-XPB-256</cipher_operational>
                  <window>148809600</window>
                  <conf_offset>CONF-OFFSET-0</conf_offset>
                  <conf_offset_operational>CONF-OFFSET-0</conf_offset_operational>
                  <sak_status>Rx & TX</sak_status>
                  <sak_an>0</sak_an>
                  <sak_ki>5AABE0AB9CC867AB0FF40F7D00000001</sak_ki>
                  <sak_kn>1</sak_kn>
                  <last_sak_rekey_time>11:53:25 pst Tue Dec 15 2020</last_sak_rekey_time>
                  <peer_count>1</peer_count>
                  <mac_addr>0180.c200.0003</mac_addr>
                  <ether_type>0x888e</ether_type>
                  <TABLE_mka_peer_status>
                    <ROW_mka_peer_status>
                      <peer_mi>27FC36C2BFAFBDBC65419A40</peer_mi>
                      <rxsci>6c8b.d3db.e984/0001</rxsci>
                      <icv_status>Match</icv_status>
                      <last_rx_time>13:51:39 pst Tue Dec 15 2020</last_rx_time>
                    </ROW_mka_peer_status>
                  </TABLE_mka_peer_status>
                </ROW_mka_session_details>
              </TABLE_mka_session_details>
            </readonly__>
          </__XML__OPT_Cmd_show_macsec_mka_session__readonly__>
        </session>
      </mka>
    </macsec>
  </show>
</nf:data>
</nf:rpc-reply>
```

```

        </__readonly__>
        </__XML__OPT_Cmd_show_macsec_mka_session__readonly__>
        </__XML__OPT_Cmd_show_macsec_mka_session_details>
        </__XML__OPT_Cmd_show_macsec_mka_session_interface>
    </session>
</mka>
</macsec>
</show>
</nf:data>
</nf:rpc-reply>
]]>]]>
switch(config)#

```

### 例 3 : MACsec MKA 統計を表示します

```

switch(config)# show macsec mka statistics interface e1/29 | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns="http://www.cisco.com/nxos:1.0:cts"
xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0">
<nf:data>
  <show>
    <macsec>
      <mka>
        <statistics>
          <__XML__OPT_Cmd_some_macsec_mka_statistics_interface>
            <interface>
              <__XML__INTF_ifname>
                <__XML__PARAM_value>
                  <__XML__INTF_output>Ethernet1/29</__XML__INTF_output>
                </__XML__PARAM_value>
              </__XML__INTF_ifname>
            </interface>
          <__XML__OPT_Cmd_some_macsec_mka_statistics__readonly__>
            <__readonly__>
              <TABLE_mka_intf_stats>
                <ROW_mka_intf_stats>
                  <ifname2>Ethernet1/29</ifname2>
                  <TABLE_ca_stats>
                    <ROW_ca_stats>
                      <ca_stat_ckn>2002</ca_stat_ckn>
                      <ca_stat_pairwise_cak_rekey>0</ca_stat_pairwise_cak_rekey>
                      <sa_stat_sak_generated>0</sa_stat_sak_generated>
                      <sa_stat_sak_rekey>0</sa_stat_sak_rekey>
                      <sa_stat_sak_received>2</sa_stat_sak_received>
                      <sa_stat_sak_response_rx>0</sa_stat_sak_response_rx>
                      <mkpdu_stat_mkpdu_tx>4335</mkpdu_stat_mkpdu_tx>
                      <mkpdu_stat_mkpdu_tx_distsak>0</mkpdu_stat_mkpdu_tx_distsak>
                      <mkpdu_stat_mkpdu_rx>4335</mkpdu_stat_mkpdu_rx>
                      <mkpdu_stat_mkpdu_rx_distsak>2</mkpdu_stat_mkpdu_rx_distsak>
                    </ROW_ca_stats>
                  </TABLE_ca_stats>
                  <TABLE_idb_stats>
                    <ROW_idb_stats>
                      <ca_stat_pairwise_cak_rekey>0</ca_stat_pairwise_cak_rekey>
                      <sa_stat_sak_generated>0</sa_stat_sak_generated>
                      <sa_stat_sak_rekey>0</sa_stat_sak_rekey>
                      <sa_stat_sak_received>2</sa_stat_sak_received>
                      <sa_stat_sak_response_rx>0</sa_stat_sak_response_rx>
                      <mkpdu_stat_mkpdu_tx>4335</mkpdu_stat_mkpdu_tx>
                      <mkpdu_stat_mkpdu_tx_distsak>0</mkpdu_stat_mkpdu_tx_distsak>
                      <mkpdu_stat_mkpdu_rx>4335</mkpdu_stat_mkpdu_rx>
                      <mkpdu_stat_mkpdu_rx_distsak>2</mkpdu_stat_mkpdu_rx_distsak>
                      <idb_stat_mkpdu_tx_success>8666</idb_stat_mkpdu_tx_success>
                      <idb_stat_mkpdu_tx_fail>0</idb_stat_mkpdu_tx_fail>

```

```

        <idb_stat_mkpdu_tx_pkt_build_fail>0</idb_stat_mkpdu_tx_pkt_build_fail>
        <idb_stat_mkpdu_no_tx_on_intf_down>0</idb_stat_mkpdu_no_tx_on_intf_down>
        <idb_stat_mkpdu_no_rx_on_intf_down>0</idb_stat_mkpdu_no_rx_on_intf_down>
        <idb_stat_mkpdu_rx_ca_notfound>0</idb_stat_mkpdu_rx_ca_notfound>
        <idb_stat_mkpdu_rx_error>0</idb_stat_mkpdu_rx_error>
        <idb_stat_mkpdu_rx_success>8666</idb_stat_mkpdu_rx_success>

        <idb_stat_mkpdu_failure_rx_integrity_check_error>0</idb_stat_mkpdu_failure_rx_integrity_check_error>

        <idb_stat_mkpdu_failure_invalid_peer_mn_error>0</idb_stat_mkpdu_failure_invalid_peer_mn_error>

        <idb_stat_mkpdu_failure_nonrecent_peerlist_mn_error>0</idb_stat_mkpdu_failure_nonrecent_peerlist_mn_error>

        <idb_stat_mkpdu_failure_sakuse_kn_mismatch_error>0</idb_stat_mkpdu_failure_sakuse_kn_mismatch_error>

        <idb_stat_mkpdu_failure_sakuse_rx_not_set_error>0</idb_stat_mkpdu_failure_sakuse_rx_not_set_error>

        <idb_stat_mkpdu_failure_sakuse_key_mi_mismatch_error>0</idb_stat_mkpdu_failure_sakuse_key_mi_mismatch_error>

        <idb_stat_mkpdu_failure_sakuse_an_not_in_use_error>0</idb_stat_mkpdu_failure_sakuse_an_not_in_use_error>

        <idb_stat_mkpdu_failure_sakuse_ks_rx_tx_not_set_error>0</idb_stat_mkpdu_failure_sakuse_ks_rx_tx_not_set_error>

        <idb_stat_mkpdu_failure_sakuse_eapol_ether_type_mismatch_error>0</idb_stat_mkpdu_failure_sakuse_eapol_ether_type_mismatch_error>

        <idb_stat_mkpdu_failure_sakuse_eapol_destmac_mismatch_error>0</idb_stat_mkpdu_failure_sakuse_eapol_destmac_mismatch_error>

        <idb_stat_sak_failure_sak_generate_error>0</idb_stat_sak_failure_sak_generate_error>
        <idb_stat_sak_failure_hash_generate_error>0</idb_stat_sak_failure_hash_generate_error>
        <idb_stat_sak_failure_sak_encryption_error>0</idb_stat_sak_failure_sak_encryption_error>
        <idb_stat_sak_failure_sak_decryption_error>0</idb_stat_sak_failure_sak_decryption_error>
        <idb_stat_sak_failure_ick_derivation_error>0</idb_stat_sak_failure_ick_derivation_error>
        <idb_stat_sak_failure_kek_derivation_error>0</idb_stat_sak_failure_kek_derivation_error>
        <idb_stat_sak_failure_invalid_macsec_capability_error>0</idb_stat_sak_failure_invalid_macsec_capability_error>

        <idb_stat_macsec_failure_rx_sa_create_error>0</idb_stat_macsec_failure_rx_sa_create_error>

        <idb_stat_macsec_failure_tx_sa_create_error>0</idb_stat_macsec_failure_tx_sa_create_error>

        </ROW_idb_stats>
    </TABLE_idb_stats>
</ROW_mka_intf_stats>

```

```

        </TABLE_mka_intf_stats>
      </__readonly__>
    </__XML__OPT_Cmd_some_macsec_mka_statistics__readonly__>
  </__XML__OPT_Cmd_some_macsec_mka_statistics_interface>
</statistics>
</mka>
</macsec>
</show>
</nf:data>
</nf:rpc-reply>
]]>]]>
switch(config)#

```

#### 例 4 : MACsec MKA 構成を表示します

```

switch(config)# show macsec mka summary | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns="http://www.cisco.com/nxos:1.0:cts"
xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0">
<nf:data>
  <show>
    <macsec>
      <mka>
        <__XML__OPT_Cmd_some_macsec_summary>
          <__XML__OPT_Cmd_some_macsec__readonly__>
            <__readonly__>
              <TABLE_mka_summary>
                <ROW_mka_summary>
                  <ifname>Ethernet1/29</ifname>
                  <status>Secured</status>
                  <cipher>GCM-AES-128</cipher>
                  <keyserver>No</keyserver>
                  <policy>mpd1</policy>
                  <keychain>kd</keychain>
                  <fallback_keychain>fbkd</fallback_keychain>
                </ROW_mka_summary>
                <ROW_mka_summary>
                  <ifname>Ethernet1/30</ifname>
                  <status>Secured</status>
                  <cipher>GCM-AES-128</cipher>
                  <keyserver>No</keyserver>
                  <policy>mpd2</policy>
                  <keychain>kd</keychain>
                  <fallback_keychain>fbkd</fallback_keychain>
                </ROW_mka_summary>
                <ROW_mka_summary>
                  <ifname>Ethernet1/31</ifname>
                  <status>Secured</status>
                  <cipher>GCM-AES-128</cipher>
                  <keyserver>Yes</keyserver>
                  <policy>mps1</policy>
                  <keychain>ks</keychain>
                  <fallback_keychain>fbks</fallback_keychain>
                </ROW_mka_summary>
                <ROW_mka_summary>
                  <ifname>Ethernet1/32</ifname>
                  <status>Secured</status>
                  <cipher>GCM-AES-128</cipher>
                  <keyserver>Yes</keyserver>
                  <policy>mps2</policy>
                  <keychain>ks</keychain>
                  <fallback_keychain>fbks</fallback_keychain>
                </ROW_mka_summary>
              <ROW_mka_summary>

```

```

        <ifname>Ethernet1/33</ifname>
        <status>Secured</status>
        <cipher>GCM-AES-128</cipher>
        <keyserver>Yes</keyserver>
        <policy>mpsr1</policy>
        <keychain>ksr</keychain>
        <fallback_keychain>fbksr</fallback_keychain>
    </ROW_mka_summary>
    <ROW_mka_summary>
        <ifname>Ethernet1/34</ifname>
        <status>Secured</status>
        <cipher>GCM-AES-128</cipher>
        <keyserver>Yes</keyserver>
        <policy>mpsr2</policy>
        <keychain>ksr</keychain>
        <fallback_keychain>fbksr</fallback_keychain>
    </ROW_mka_summary>
    <ROW_mka_summary>
        <ifname>Ethernet1/35</ifname>
        <status>Secured</status>
        <cipher>GCM-AES-XPB-256</cipher>
        <keyserver>Yes</keyserver>
        <policy>system-default-macsec-policy</policy>
        <keychain>ksr</keychain>
        <fallback_keychain>no keychain</fallback_keychain>
    </ROW_mka_summary>
    <ROW_mka_summary>
        <ifname>Ethernet1/36</ifname>
        <status>Secured</status>
        <cipher>GCM-AES-XPB-256</cipher>
        <keyserver>No</keyserver>
        <policy>system-default-macsec-policy</policy>
        <keychain>ksr</keychain>
        <fallback_keychain>no keychain</fallback_keychain>
    </ROW_mka_summary>
    </TABLE_mka_summary>
    </__readonly__>
    </__XML__OPT_Cmd_some_macsec__readonly__>
    </__XML__OPT_Cmd_some_macsec_summary>
</mka>
</macsec>
</show>
</nf:data>
</nf:rpc-reply>
]]>]]>
switch(config)#

```

### 例 5 : 特定の MACsec ポリシーの構成を表示します

```

switch(config)# show macsec policy mpsr1 | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns="http://www.cisco.com/nxos:1.0:cts"
xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0">
<nf:data>
  <show>
    <macsec>
      <policy>
        <__XML__OPT_Cmd_show_macsec_policy_policy_name>
          <policy_name>mpsr1</policy_name>
        <__XML__OPT_Cmd_show_macsec_policy__readonly__>
          <__readonly__>
            <TABLE_macsec_policy>
              <ROW_macsec_policy>
                <name>mpsr1</name>

```



```

        <cipher_suite>GCM-AES-128</cipher_suite>
        <keyserver_priority>1</keyserver_priority>
        <window_size>1000</window_size>
        <conf_offset>30</conf_offset>
        <security_policy>should-secure</security_policy>
        <sak-expiry-time>60</sak-expiry-time>
        <include_icv_indicator>TRUE</include_icv_indicator>
      </ROW_macsec_policy>
    </TABLE_macsec_policy>
  </__readonly__>
</__XML__OPT_Cmd_show_macsec_policy__readonly__>
</__XML__OPT_Cmd_show_macsec_policy_policy_name>
</policy>
</macsec>
</show>
</nf:data>
</nf:rpc-reply>
]]>]]>
switch(config)#

```

## 例 6 : MACsec セキュリティ統計を表示します

```

switch(config)# show macsec secy statistics interface e1/29 | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns="http://www.cisco.com/nxos:1.0:cts"
  xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0">
  <nf:data>
    <show>
      <macsec>
        <secy>
          <statistics>
            <__XML__OPT_Cmd_some_macsec_secy_statistics_interface>
              <interface>
                <__XML__INTF_ifname>
                  <__XML__PARAM_value>
                    <__XML__INTF_output>Ethernet1/29</__XML__INTF_output>
                  </__XML__PARAM_value>
                </__XML__INTF_ifname>
              </interface>
            <__XML__OPT_Cmd_some_macsec_secy_statistics__readonly__>
              <__readonly__>
                <TABLE_statistics>
                  <ROW_statistics>
                    <ifname2>Ethernet1/29</ifname2>
                    <in_pkts_unicast_uncontrolled>6536205587</in_pkts_unicast_uncontrolled>
                    <in_pkts_multicast_uncontrolled>10775</in_pkts_multicast_uncontrolled>
                    <in_pkts_broadcast_uncontrolled>0</in_pkts_broadcast_uncontrolled>
                    <in_rx_drop_pkts_uncontrolled>0</in_rx_drop_pkts_uncontrolled>
                    <in_rx_err_pkts_uncontrolled>0</in_rx_err_pkts_uncontrolled>
                    <in_pkts_unicast_controlled>N/A (N3K-C3636C-R not
supported)</in_pkts_unicast_controlled>
                    <in_pkts_multicast_controlled>N/A (N3K-C3636C-R not
supported)</in_pkts_multicast_controlled>
                    <in_pkts_broadcast_controlled>N/A (N3K-C3636C-R not
supported)</in_pkts_broadcast_controlled>
                    <in_pkts_controlled>5173107800</in_pkts_controlled>
                    <in_rx_drop_pkts_controlled>N/A (N3K-C3636C-R not
supported)</in_rx_drop_pkts_controlled>
                    <in_rx_err_pkts_controlled>N/A (N3K-C3636C-R not
supported)</in_rx_err_pkts_controlled>
                    <in_octets_uncontrolled>30491280431357</in_octets_uncontrolled>
                    <in_octets_controlled>23935220809548</in_octets_controlled>
                    <input_rate_uncontrolled_pps>N/A (N3K-C3636C-R not
supported)</input_rate_uncontrolled_pps>

```

```

        <input_rate_uncontrolled_bps>N/A (N3K-C3636C-R not
supported) </input_rate_uncontrolled_bps>
        <input_rate_controlled_pps>N/A (N3K-C3636C-R not
supported) </input_rate_controlled_pps>
        <input_rate_controlled_bps>N/A (N3K-C3636C-R not
supported) </input_rate_controlled_bps>
        <out_pkts_unicast_uncontrolled>N/A (N3K-C3636C-R not
supported) </out_pkts_unicast_uncontrolled>
        <out_pkts_multicast_uncontrolled>N/A (N3K-C3636C-R not
supported) </out_pkts_multicast_uncontrolled>
        <out_pkts_broadcast_uncontrolled>N/A (N3K-C3636C-R not
supported) </out_pkts_broadcast_uncontrolled>
        <out_rx_drop_pkts_uncontrolled>N/A (N3K-C3636C-R not
supported) </out_rx_drop_pkts_uncontrolled>
        <out_rx_err_pkts_uncontrolled>N/A (N3K-C3636C-R not
supported) </out_rx_err_pkts_uncontrolled>
        <out_pkts_unicast_controlled>N/A (N3K-C3636C-R not
supported) </out_pkts_unicast_controlled>
        <out_pkts_multicast_controlled>N/A (N3K-C3636C-R not
supported) </out_pkts_multicast_controlled>
        <out_pkts_broadcast_controlled>N/A (N3K-C3636C-R not
supported) </out_pkts_broadcast_controlled>
        <out_pkts_controlled>5173113173</out_pkts_controlled>
        <out_rx_drop_pkts_controlled>N/A (N3K-C3636C-R not
supported) </out_rx_drop_pkts_controlled>
        <out_rx_err_pkts_controlled>N/A (N3K-C3636C-R not
supported) </out_rx_err_pkts_controlled>
        <out_octets_uncontrolled>N/A (N3K-C3636C-R not
supported) </out_octets_uncontrolled>
        <out_octets_controlled>23946219872208</out_octets_controlled>
        <out_octets_common>30664229104600</out_octets_common>
        <output_rate_uncontrolled_pps>N/A (N3K-C3636C-R not
supported) </output_rate_uncontrolled_pps>
        <output_rate_uncontrolled_bps>N/A (N3K-C3636C-R not
supported) </output_rate_uncontrolled_bps>
        <output_rate_controlled_pps>N/A (N3K-C3636C-R not
supported) </output_rate_controlled_pps>
        <output_rate_controlled_bps>N/A (N3K-C3636C-R not
supported) </output_rate_controlled_bps>
        <in_pkts_transform_error>N/A (N3K-C3636C-R not
supported) </in_pkts_transform_error>
        <in_pkts_control>0</in_pkts_control>
        <in_pkts_untagged>N/A (N3K-C3636C-R not supported) </in_pkts_untagged>
        <in_pkts_no_tag>0</in_pkts_no_tag>
        <in_pkts_badtag>0</in_pkts_badtag>
        <in_pkts_no_sci>0</in_pkts_no_sci>
        <in_pkts_unknown_sci>0</in_pkts_unknown_sci>
        <in_pkts_tagged_ctrl>N/A (N3K-C3636C-R not supported) </in_pkts_tagged_ctrl>
        <out_pkts_transform_error>N/A (N3K-C3636C-R not
supported) </out_pkts_transform_error>
        <out_pkts_control>0</out_pkts_control>
        <out_pkts_untagged>N/A (N3K-C3636C-R not supported) </out_pkts_untagged>
        <TABLE_rx_sa_an>
        <ROW_rx_sa_an>
        <rx_sa_an>2</rx_sa_an>
        <in_pkts_unchecked>0</in_pkts_unchecked>
        <in_pkts_delayed>0</in_pkts_delayed>
        <in_pkts_late>0</in_pkts_late>
        <in_pkts_ok>1951781408</in_pkts_ok>
        <in_pkts_invalid>0</in_pkts_invalid>
        <in_pkts_not_valid>0</in_pkts_not_valid>
        <in_pkts_not_using_sa>0</in_pkts_not_using_sa>
        <in_pkts_unused_sa>0</in_pkts_unused_sa>
        <in_octets_decrypted>8952613134278</in_octets_decrypted>

```

```

        <in_octets_validated>0</in_octets_validated>
      </ROW_rx_sa_an>
    </TABLE_rx_sa_an>
    <TABLE_tx_sa_an>
      <ROW_tx_sa_an>
        <tx_sa_an>2</tx_sa_an>
        <out_pkts_encrypted_protected>1951773387</out_pkts_encrypted_protected>
        <out_pkts_too_long>N/A (N3K-C3636C-R not supported)</out_pkts_too_long>
        <out_pkts_sa_not_inuse>N/A (N3K-C3636C-R not
supported)</out_pkts_sa_not_inuse>
        <out_octets_encrypted_protected>8952606203313</out_octets_encrypted_protected>
      </ROW_tx_sa_an>
    </TABLE_tx_sa_an>
  </ROW_statistics>
</TABLE_statistics>
</__readonly__>
</__XML__OPT_Cmd_some_macsec_secy_statistics__readonly__>
</__XML__OPT_Cmd_some_macsec_secy_statistics_interface>
</statistics>
</secy>
</macsec>
</show>
</nf:data>
</nf:rpc-reply>
]]>]]>
switch(config)#

```

### 例 7 : MACsec の実行構成情報を表示します

```
switch(config)# show running-config macsec | xml
```

```

!Command: show running-config macsec
!Running configuration last done at: Tue Dec 15 11:53:10 2020
!Time: Tue Dec 15 13:58:58 2020

```

```

version 10.1(1) Bios:version 01.14
*****
This may take time. Please be patient.
*****
<?xml version="1.0"?>
<nf:rpc xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="http://www.cisco.com/nxos:10.1.1.:configure_"
xmlns:m="http://www.cisco.com/nxos:10.1.1.:_exec"
xmlns:m1="http://www.cisco.com/nxos:10.1.1.:configure__macsec-policy"
xmlns:m2="http://www.cisco.com/nxos:10.1.1.:configure__if-ethernet-all" message-id="1">
  <nf:get-config>
    <nf:source>
      <nf:running/>
    </nf:source>
    <nf:filter>
      <m:configure>
        <m:terminal>
          <feature>
            <macsec/>
          </feature>
        <macsec>
          <policy>
            <__XML__PARAM_policy_name>
              <__XML__value>mpdl</__XML__value>
            <m1:cipher-suite>
              <m1:__XML__PARAM_suite>
                <m1:__XML__value>GCM-AES-128</m1:__XML__value>
              </m1:__XML__PARAM_suite>
            </m1:__XML__PARAM_suite>
          </policy>
        </macsec>
      </m:configure>
    </nf:filter>
  </nf:get-config>
</nf:rpc>

```

```

        </ml:cipher-suite>
        <ml:conf-offset>
          <ml:XML_PARAM_offset>
            <ml:XML_value>CONF-OFFSET-30</ml:XML_value>
          </ml:XML_PARAM_offset>
        </ml:conf-offset>
      </XML_PARAM_policy_name>
    </policy>
  </macsec>
<macsec>
  <policy>
    <XML_PARAM_policy_name>
      <XML_value>mpd2</XML_value>
      <ml:cipher-suite>
        <ml:XML_PARAM_suite>
          <ml:XML_value>GCM-AES-128</ml:XML_value>
        </ml:XML_PARAM_suite>
      </ml:cipher-suite>
      <ml:conf-offset>
        <ml:XML_PARAM_offset>
          <ml:XML_value>CONF-OFFSET-30</ml:XML_value>
        </ml:XML_PARAM_offset>
      </ml:conf-offset>
      <ml:security-policy>
        <ml:XML_PARAM_policy>
          <ml:XML_value>must-secure</ml:XML_value>
        </ml:XML_PARAM_policy>
      </ml:security-policy>
    </XML_PARAM_policy_name>
  </policy>
</macsec>
<macsec>
  <policy>
    <XML_PARAM_policy_name>
      <XML_value>mps1</XML_value>
      <ml:cipher-suite>
        <ml:XML_PARAM_suite>
          <ml:XML_value>GCM-AES-128</ml:XML_value>
        </ml:XML_PARAM_suite>
      </ml:cipher-suite>
      <ml:key-server-priority>
        <ml:XML_PARAM_pri>
          <ml:XML_value>1</ml:XML_value>
        </ml:XML_PARAM_pri>
      </ml:key-server-priority>
      <ml:conf-offset>
        <ml:XML_PARAM_offset>
          <ml:XML_value>CONF-OFFSET-30</ml:XML_value>
        </ml:XML_PARAM_offset>
      </ml:conf-offset>
      <ml:sak-expiry-time>
        <ml:XML_PARAM_ts>
          <ml:XML_value>60</ml:XML_value>
        </ml:XML_PARAM_ts>
      </ml:sak-expiry-time>
      <ml:include-icv-indicator/>
    </XML_PARAM_policy_name>
  </policy>
</macsec>
<macsec>
  <policy>
    <XML_PARAM_policy_name>
      <XML_value>mps2</XML_value>
      <ml:cipher-suite>

```

```

        <m1: __XML__PARAM__suite>
          <m1: __XML__value>GCM-AES-128</m1: __XML__value>
        </m1: __XML__PARAM__suite>
      </m1:cipher-suite>
    <m1:key-server-priority>
      <m1: __XML__PARAM__pri>
        <m1: __XML__value>1</m1: __XML__value>
      </m1: __XML__PARAM__pri>
    </m1:key-server-priority>
    <m1>window-size>
      <m1: __XML__PARAM__size>
        <m1: __XML__value>1000</m1: __XML__value>
      </m1: __XML__PARAM__size>
    </m1>window-size>
    <m1:conf-offset>
      <m1: __XML__PARAM__offset>
        <m1: __XML__value>CONF-OFFSET-30</m1: __XML__value>
      </m1: __XML__PARAM__offset>
    </m1:conf-offset>
    <m1:security-policy>
      <m1: __XML__PARAM__policy>
        <m1: __XML__value>must-secure</m1: __XML__value>
      </m1: __XML__PARAM__policy>
    </m1:security-policy>
    <m1:sak-expiry-time>
      <m1: __XML__PARAM__ts>
        <m1: __XML__value>60</m1: __XML__value>
      </m1: __XML__PARAM__ts>
    </m1:sak-expiry-time>
    <m1:include-icv-indicator/>
  </__XML__PARAM__policy_name>
</policy>
</macsec>
<macsec>
  <policy>
    <__XML__PARAM__policy_name>
      <__XML__value>mpsrl</__XML__value>
    <m1:cipher-suite>
      <m1: __XML__PARAM__suite>
        <m1: __XML__value>GCM-AES-128</m1: __XML__value>
      </m1: __XML__PARAM__suite>
    </m1:cipher-suite>
    <m1:key-server-priority>
      <m1: __XML__PARAM__pri>
        <m1: __XML__value>1</m1: __XML__value>
      </m1: __XML__PARAM__pri>
    </m1:key-server-priority>
    <m1>window-size>
      <m1: __XML__PARAM__size>
        <m1: __XML__value>1000</m1: __XML__value>
      </m1: __XML__PARAM__size>
    </m1>window-size>
    <m1:conf-offset>
      <m1: __XML__PARAM__offset>
        <m1: __XML__value>CONF-OFFSET-30</m1: __XML__value>
      </m1: __XML__PARAM__offset>
    </m1:conf-offset>
    <m1:sak-expiry-time>
      <m1: __XML__PARAM__ts>
        <m1: __XML__value>60</m1: __XML__value>
      </m1: __XML__PARAM__ts>
    </m1:sak-expiry-time>
    <m1:include-icv-indicator/>
  </__XML__PARAM__policy_name>

```

```

    </policy>
  </macsec>
<macsec>
  <policy>
    <__XML__PARAM__policy_name>
      <__XML__value>mpsr2</__XML__value>
      <m1:cipher-suite>
        <m1:__XML__PARAM__suite>
          <m1:__XML__value>GCM-AES-128</m1:__XML__value>
        </m1:__XML__PARAM__suite>
      </m1:cipher-suite>
      <m1:key-server-priority>
        <m1:__XML__PARAM__pri>
          <m1:__XML__value>1</m1:__XML__value>
        </m1:__XML__PARAM__pri>
      </m1:key-server-priority>
      <m1>window-size>
        <m1:__XML__PARAM__size>
          <m1:__XML__value>1000</m1:__XML__value>
        </m1:__XML__PARAM__size>
      </m1>window-size>
      <m1:conf-offset>
        <m1:__XML__PARAM__offset>
          <m1:__XML__value>CONF-OFFSET-30</m1:__XML__value>
        </m1:__XML__PARAM__offset>
      </m1:conf-offset>
      <m1:security-policy>
        <m1:__XML__PARAM__policy>
          <m1:__XML__value>must-secure</m1:__XML__value>
        </m1:__XML__PARAM__policy>
      </m1:security-policy>
      <m1:sak-expiry-time>
        <m1:__XML__PARAM__ts>
          <m1:__XML__value>60</m1:__XML__value>
        </m1:__XML__PARAM__ts>
      </m1:sak-expiry-time>
      <m1:include-icv-indicator/>
    </__XML__PARAM__policy_name>
  </policy>
</macsec>
<interface>
  <__XML__PARAM__interface>
    <__XML__value>Ethernet1/29</__XML__value>
    <m2:macsec>
      <m2:keychain>
        <m2:__XML__PARAM__keychain_name>
          <m2:__XML__value>kd</m2:__XML__value>
          <m2:policy>
            <m2:__XML__PARAM__policy_name>
              <m2:__XML__value>mpd1</m2:__XML__value>
              <m2:fallback-keychain>
                <m2:__XML__PARAM__fallback_kc_name>
                  <m2:__XML__value>fbkd</m2:__XML__value>
                </m2:__XML__PARAM__fallback_kc_name>
              </m2:fallback-keychain>
            </m2:__XML__PARAM__policy_name>
          </m2:policy>
        </m2:__XML__PARAM__keychain_name>
      </m2:keychain>
    </m2:macsec>
  </__XML__PARAM__interface>
</interface>
<interface>
  <__XML__PARAM__interface>

```

```

<__XML__value>Ethernet1/30</__XML__value>
<m2:macsec>
  <m2:keychain>
    <m2:__XML__PARAM__keychain_name>
      <m2:__XML__value>kd</m2:__XML__value>
    <m2:policy>
      <m2:__XML__PARAM__policy_name>
        <m2:__XML__value>mpd2</m2:__XML__value>
      <m2:fallback-keychain>
        <m2:__XML__PARAM__fallback_kc_name>
          <m2:__XML__value>fbkd</m2:__XML__value>
        </m2:__XML__PARAM__fallback_kc_name>
      </m2:fallback-keychain>
    </m2:__XML__PARAM__policy_name>
  </m2:policy>
</m2:__XML__PARAM__keychain_name>
</m2:keychain>
</m2:macsec>
</__XML__PARAM__interface>
</interface>
<interface>
  <__XML__PARAM__interface>
    <__XML__value>Ethernet1/31</__XML__value>
    <m2:macsec>
      <m2:keychain>
        <m2:__XML__PARAM__keychain_name>
          <m2:__XML__value>ks</m2:__XML__value>
        <m2:policy>
          <m2:__XML__PARAM__policy_name>
            <m2:__XML__value>mps1</m2:__XML__value>
          <m2:fallback-keychain>
            <m2:__XML__PARAM__fallback_kc_name>
              <m2:__XML__value>fbks</m2:__XML__value>
            </m2:__XML__PARAM__fallback_kc_name>
          </m2:fallback-keychain>
        </m2:__XML__PARAM__policy_name>
      </m2:policy>
    </m2:__XML__PARAM__keychain_name>
  </m2:keychain>
</m2:macsec>
</__XML__PARAM__interface>
</interface>
<interface>
  <__XML__PARAM__interface>
    <__XML__value>Ethernet1/32</__XML__value>
    <m2:macsec>
      <m2:keychain>
        <m2:__XML__PARAM__keychain_name>
          <m2:__XML__value>ks</m2:__XML__value>
        <m2:policy>
          <m2:__XML__PARAM__policy_name>
            <m2:__XML__value>mps2</m2:__XML__value>
          <m2:fallback-keychain>
            <m2:__XML__PARAM__fallback_kc_name>
              <m2:__XML__value>fbks</m2:__XML__value>
            </m2:__XML__PARAM__fallback_kc_name>
          </m2:fallback-keychain>
        </m2:__XML__PARAM__policy_name>
      </m2:policy>
    </m2:__XML__PARAM__keychain_name>
  </m2:keychain>
</m2:macsec>
</__XML__PARAM__interface>
</interface>

```

```

<interface>
  <__XML__PARAM__interface>
    <__XML__value>Ethernet1/33</__XML__value>
    <m2:macsec>
      <m2:keychain>
        <m2:__XML__PARAM__keychain_name>
          <m2:__XML__value>ksr</m2:__XML__value>
          <m2:policy>
            <m2:__XML__PARAM__policy_name>
              <m2:__XML__value>mpsrl</m2:__XML__value>
              <m2:fallback-keychain>
                <m2:__XML__PARAM__fallback_kc_name>
                  <m2:__XML__value>fbksr</m2:__XML__value>
                  </m2:__XML__PARAM__fallback_kc_name>
                </m2:fallback-keychain>
              </m2:__XML__PARAM__policy_name>
            </m2:policy>
          </m2:__XML__PARAM__keychain_name>
        </m2:keychain>
      </m2:macsec>
    </__XML__PARAM__interface>
  </interface>
  <interface>
    <__XML__PARAM__interface>
      <__XML__value>Ethernet1/34</__XML__value>
      <m2:macsec>
        <m2:keychain>
          <m2:__XML__PARAM__keychain_name>
            <m2:__XML__value>ksr</m2:__XML__value>
            <m2:policy>
              <m2:__XML__PARAM__policy_name>
                <m2:__XML__value>mpsrl2</m2:__XML__value>
                <m2:fallback-keychain>
                  <m2:__XML__PARAM__fallback_kc_name>
                    <m2:__XML__value>fbksr</m2:__XML__value>
                    </m2:__XML__PARAM__fallback_kc_name>
                  </m2:fallback-keychain>
                </m2:__XML__PARAM__policy_name>
              </m2:policy>
            </m2:__XML__PARAM__keychain_name>
          </m2:keychain>
        </m2:macsec>
      </__XML__PARAM__interface>
    </interface>
    <interface>
      <__XML__PARAM__interface>
        <__XML__value>Ethernet1/35</__XML__value>
        <m2:macsec>
          <m2:keychain>
            <m2:__XML__PARAM__keychain_name>
              <m2:__XML__value>ksr</m2:__XML__value>
              <m2:policy>
                <m2:__XML__PARAM__policy_name>
                  <m2:__XML__value>system-default-macsec-policy</m2:__XML__value>
                </m2:__XML__PARAM__policy_name>
              </m2:policy>
            </m2:__XML__PARAM__keychain_name>
          </m2:keychain>
        </m2:macsec>
      </__XML__PARAM__interface>
    </interface>
    <interface>
      <__XML__PARAM__interface>
        <__XML__value>Ethernet1/36</__XML__value>

```



```

<m2:macsec>
  <m2:keychain>
    <m2:__XML__PARAM__keychain_name>
      <m2:__XML__value>ksr</m2:__XML__value>
    <m2:policy>
      <m2:__XML__PARAM__policy_name>
        <m2:__XML__value>system-default-macsec-policy</m2:__XML__value>
      </m2:__XML__PARAM__policy_name>
    </m2:policy>
  </m2:__XML__PARAM__keychain_name>
</m2:keychain>
</m2:macsec>
</__XML__PARAM__interface>
</interface>
</m:terminal>
</m:configure>
</nf:filter>
</nf:get-config>
</nf:rpc>
]]>]]>

switch(config)#

```

## MIB

MACsec は次の MIB をサポートします。

- IEEE8021-SECY-MIB
- CISCO-SECY-EXT-MIB

## 関連資料

| 関連項目       | マニュアル タイトル                                                   |
|------------|--------------------------------------------------------------|
| キーチェーン管理   | 『Cisco Nexus 3600 Series NX-OS Security Configuration Guide』 |
| システム メッセージ | Cisco Nexus 3600 シリーズ NX-OS システム メッセージ リファレンス                |





## 索引

### A

- AAA [3, 7–8, 10–12, 19, 33, 35](#)
  - MSCHAP 認証の有効化 [19](#)
  - アカウントティング [7](#)
  - ガイドライン [12](#)
  - コンソール ログインの設定 [12](#)
  - 制限事項 [12](#)
  - 構成の確認 [33](#)
  - 設定例 [33](#)
  - 説明 [3](#)
  - 前提条件 [11](#)
  - デフォルト設定 [35](#)
  - 認証 [7](#)
  - ユーザ ログイン プロセス [10](#)
  - 利点 [8](#)
- aaa authorization {group | local} [102](#)
- aaa authorization {ssh-certificate | ssh-publickey} [102](#)
- aaa authorization default [102](#)
- aaa group server ldap [93](#)
- aaa authorization ssh-certificate default [21–22](#)
- AAA アカウントティング [23](#)
  - デフォルト方式の設定 [23](#)
- AAA アカウントティング ログ [33](#)
  - クリア [33](#)
  - 表示 [33](#)
- AAA サーバ [23, 27](#)
  - SNMPv3 パラメータの指定 [23, 27](#)
  - VSA でのユーザ ロールの指定 [23](#)
  - ユーザ ロールの指定 [27](#)
- AAA サーバ グループ [8](#)
  - 説明 [8](#)
- AAA サービス [8–9](#)
  - 設定オプション [9](#)
  - remote [8](#)
- AAA プロトコル [7](#)
  - RADIUS [7](#)
  - TACACS+ [7](#)
- AAA ログイン [15](#)
  - 認証失敗メッセージのイネーブル化 [15](#)
- ACL [202–204](#)
  - 処理順序 [202](#)

### ACL (続き)

- 前提条件 [204](#)
  - プロトコルによるトラフィックの識別 [203](#)
- ACL ロギング構成、確認 [233](#)
- ACL ロギング構成の確認 [233](#)
- aclog match-log-level [210, 212](#)
- ACL の暗黙のルール [203](#)
- ACL のロギング [229](#)
- authentication (bind-first | compare) [93](#)

### B

- BGP [242](#)
  - ユニキャスト RPF との使用 [242](#)

### C

- CA [129–130, 134–135, 138, 146, 149, 151, 157, 159–160, 163](#)
  - identity [130](#)
  - アイデンティティ証明書のインストール [151](#)
  - アイデンティティ証明書要求の作成 [149](#)
  - カット アンド ペーストによる登録 [135](#)
  - 構成 [138](#)
  - 証明書の削除 [157](#)
  - 証明書のダウンロードの例 [163](#)
  - 構成の表示 [159](#)
  - 設定例 [160](#)
  - 説明 [129](#)
  - 認証 [146](#)
  - ピア証明書 [135](#)
  - multiple [135](#)
  - 複数のトラスト ポイント [134](#)
  - 目的 [129](#)
- CA トラスト ポイント [142](#)
  - PKI のアソシエーションの作成 [142](#)
- cisco-av-pair [23, 27](#)
  - AAA ユーザ パラメータの指定 [23, 27](#)
- class class-default [273](#)
- class insert-before [273](#)
- class-map [266–267](#)
- class-map type control-plane {match-all | match-any} [271](#)
- clear ldap-server statistics [105–106](#)

clear copp statistics 283  
 control-plane 266–267, 275–277  
 copp copy profile {strict | Moderate | lenient} 高密度 278–279  
 copp copy profile prefix {サフィックス} 278–279  
 copp profile lenient 278  
 copp profile strict 278  
 copp profile 278  
 copp profile dense 278  
 copp profile Moderate 278  
 CRL 136, 156, 186, 188, 193  
   インポートの例 193  
   構成 156  
   生成 186  
   説明 136  
   ダウンロード 188  
   パブリッシュ 186  
 crypto ca crt request 121–122  
 crypto ca trustpoint 121–122

## D

deny 208–209  
 DoS 攻撃 243  
   ユニキャスト RPF、配置 243

## E

enable Cert-DN-match 93–94  
 enable user-server-group 93–94

## F

feature ldap 89

## G

generate type7\_encrypted\_secret 70

## H

hardware access-list tcam region ing-ifacl qualify udf 222  
 hardware rate-limiter access-list-log 210, 212

## I

ID 27  
   シスコのベンダー ID 27  
 ID 証明書 149, 151, 157  
   PKI の削除 157  
   インストール 151  
   要求の作成 149  
 ip access-list 208–209

IP ACL 5, 201, 215  
   シーケンス番号の変更 215  
   説明 5, 201  
 ip verify unicast source reachable-via any 245–246  
 ip access-group 210–211  
 IP ACL の暗黙のルール 203  
 ipv6 access-list 208–209  
 ipv6 verify unicast source reachable-via any 245–246  
 IP ドメイン名 138  
   PKI での設定 138

## L

ldap search-map 98  
 ldap-server deadtime 99–101  
 ldap-server host 90, 96–97, 99–100  
 ldap-server host idle-time 99–100  
 ldap-server host password 91–92, 99–100  
 ldap-server host port 91–92, 97  
 ldap-server host rootDN 91–92  
 ldap-server host test rootDN 99–100  
 ldap-server host timeout 91–92, 97  
 ldap-server host username 99–100  
 ldap-server timeout 95  
 logging drop threshold 273–274  
 logging ip access-list cache entries 210, 212  
 logging ip access-list cache interval 210, 212  
 logging ip access-list cache threshold 210, 212  
 logging ip access-list detailed 210, 212  
 login on-success log 16–17  
 login on-failure log 16

## M

mac access-list 222  
 mac port access-group 221, 223  
 MAC ACL の暗黙のルール 203  
 match access-group name 271  
 match exception {ip | ipv6} icmp redirect 271–272  
 match exception {ip | ipv6} icmp unreachable 271–272  
 match exception {ip | ipv6} option 271–272  
 match protocol arp 271–272  
 MSCHAP 19  
   認証の有効化 19

## P

permit 208–209  
 permit mac 222  
 PKI 129, 134, 136–139, 159–160  
   IP ドメイン名の設定 138  
   RSA キー ペアの生成 139  
   ガイドライン 137  
   証明書失効確認 136

## PKI (続き)

- 制限事項 137
- 構成の表示 159
- 設定例 160
- 説明 129
- デフォルト設定 137
- 登録のサポート 134
- ホスト名の設定 138

- police cir 273
- policy-map 266–267
- policy-map type control-plane 273

## R

- RADIUS 4
  - 説明 4
- RADIUS サーバ グループ 51
  - グローバル発信元インターフェイス 51
- RADIUS 統計情報 60
  - クリア 60
- reload 222
- RSA キー ペア 133, 135–136, 139, 153–154, 158–159
  - Cisco NX-OS デバイスからの削除 158
  - PKI に生成 139
  - インポート 136, 154
  - エクスポート 136, 153
  - 構成の表示 159
  - 説明 133
  - multiple 135

## S

- service-policy 266–267
- service-policy input 275–276
- set cos 273–274
- show aaa authorization 21, 102
- show class-map type control-plane 271–272, 280
- show copp profile 281
- show crypto ca certificates 121–122
- show crypto ca crt 121, 123
- show ldap-search-map 98–99, 106
- show ldap-server 90–92, 95–97, 99–101, 106
- show ldap-server groups 93–94, 106
- show ldap-server statistics 105–106
- show logging ip access-list cache 210, 212
- show login on-failure log 16–17
- show login on-successful log 16–17
- show policy-map interface control-plane 277, 280, 282–283
- show policy-map type control-plane 273, 275, 279
- show policy-map type control-plane expand 273, 275
- show policy-map type control-plane name 273, 275
- show running-config aclmgr 281
- show running-config copp 275–276, 278–279, 281

- show running-config copp all 275–276
- show running-config ldap 106
- show startup-config aclmgr 282
- show startup-config ldap 106
- show user-account 25–26, 121, 123
- show users 121, 123
- show aaa authorization all 21
- show copp status 278–279, 282
- show incompatibility nxos bootflash: 269
- show ip access-lists 208–209
- show ipv6 access-lists 208–209
- SNMPv3 23, 27
  - AAA サーバのパラメータの指定 27
  - AAA パラメータの指定 23
- SSH 5
  - 説明 5
- statistics per-entry 208–209

## T

- TACACS+ 4, 81–82
  - 設定例 81
  - 説明 4
    - フィールドの説明 82
- TACACS+ サーバ 79, 82
  - 手動モニタリング 79
  - フィールドの説明 82
- TACACS+ サーバ グループ 72
  - グローバル発信元インターフェイス 72
- Telnet 5
  - 説明 5

## U

- udf 221
- use-vrf 93–94
- username password 121

## V

- VSA 27
  - 形式 27
  - サポートの説明 27
  - プロトコル オプション 27

## あ

- アカウンティング 7
  - 説明 7
- 暗号化 ca 認証 121–122

## か

確認 [81](#)  
TACACS+構成 [81](#)

## き

許可 [10](#)  
ユーザー ログイン [10](#)

## く

class [273](#)

## さ

サーバ (Server) [93](#)  
サーバ グループ [8](#)  
サービス拒絶攻撃 [243](#)  
IP アドレス スプーフィング、軽減 [243](#)

## し

シスコ [27](#)  
ベンダー ID [27](#)  
証明機関。参照先：CA  
証明書 [183](#)  
取り消しの例 [183](#)  
証明書失効確認 [148](#)  
方法の設定 [148](#)  
証明書失効リスト。参照先：CRL

## す

スケール ファクタ [277](#)

## て

デジタル証明書 [129, 135–136, 138](#)  
インポート [136](#)  
エクスポート [136](#)  
構成 [138](#)  
説明 [129, 136](#)  
peers [135](#)  
目的 [129](#)  
デフォルト設定 [35, 137](#)  
AAA [35](#)  
PKI [137](#)

## と

トラスト ポイント [130, 134, 152](#)  
説明 [130](#)  
multiple [134](#)  
リブート後の設定の保存 [152](#)

## に

認証 [7, 9–10](#)  
説明 [7](#)  
方法 [9](#)  
ユーザー ログイン [10](#)  
remote [7](#)  
ローカル (local) [7](#)

## は

発信元インターフェイス [51, 72](#)  
RADIUS サーバグループ [51](#)  
TACACS+ サーバグループ [72](#)

## へ

ベンダー固有属性 [27](#)

## ほ

ホスト名 [138](#)  
PKI での設定 [138](#)  
police [273](#)

## ゆ

ユーザ ロール [23, 27](#)  
AAA サーバでの指定 [23, 27](#)  
ユーザー ログイン [10](#)  
許可プロセス [10](#)  
認証プロセス [10](#)  
ユニキャスト RPF [241–243, 245, 247](#)  
BGP 属性 [242](#)  
BOOTP [243](#)  
DHCP [243](#)  
FIB [241](#)  
ガイドライン [243](#)  
実装 [242](#)  
ストリクト モード [245](#)  
制限事項 [243](#)  
設定の確認 [247](#)  
設定例 [247](#)  
説明 [241](#)

ユニキャスト RPF (続き)  
デフォルト設定 [245](#)  
展開 [243](#)  
統計情報 [243](#)  
トンネリング [243](#)  
ルーズ モード [245](#)

## る

ルール [203](#)  
暗黙的 [203](#)

## れ

例 [34](#)  
AAA の設定 [34](#)

## ろ

ログ ファイルの表示とクリア [232](#)





## 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。