



Cisco MDS 9000 シリーズ リリース 9.x セキュリティ構成ガイド

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/>



目次

はじめに :

はじめに	xix
対象読者	xix
表記法	xix
関連資料	xx
通信、サービス、およびその他の情報	xxi

第 1 章

新規および変更情報	1
-----------	---

第 2 章

セキュリティの概要	3
FIPS	3
ユーザー ロールおよび共通ロール	4
RADIUS および TACACS+	4
IP ACL	5
PKI	5
SSH サービスに関する情報	5
IPsec	6
FC-SP および DHCHAP	6
ポート セキュリティ	6
Fibre Channel Common Transport 管理サーバー クエリー	7
ファブリック バインディング	7
TrustSec ファイバチャネル リンク暗号化	7

第 3 章

Configuring FIPS	9
設定のガイドライン	9
FIPS モードのイネーブル化	10

FIPS ステータスの表示 10

FIPS のセルフテスト 10

第 4 章

ユーザアカウントおよび RBAC の設定 13

ユーザアカウントおよび RBAC の概要 13

ユーザアカウント 13

強力なパスワードの特性 15

パスワード強度の確認 15

ユーザーの設定 16

ユーザーのログアウト 17

ユーザーアカウント情報の表示 17

ロールベースの認証 18

ユーザロール 18

ロールの設定 19

カスタムロールによるロール変更の構成 20

ユーザロールとルール 21

SAN-OS リリース 3.3(1c) および NX-OS リリース 4.2(1a) 間のルール変更によるロールの動作への影響 22

プロファイルの変更 23

VSAN ポリシーの設定 24

VSAN ポリシーの変更 25

ロールの配信 26

ロールデータベースの概要 26

ファブリックのロック 26

ロールベース設定変更のコミット 27

ロールベース設定変更の廃棄 27

ロールベース設定の配布のイネーブル化 27

セッションのクリア 28

データベース マージの注意事項 28

ロールベース情報の表示 28

配信がイネーブルの場合のロールの表示 30

共通ロールの設定	32
CLI オペレーションから SNMP へのマッピング	33
デフォルト設定	34

第 5 章

外部 AAA サーバーでのセキュリティ機能の設定	37
スイッチ管理のセキュリティ	38
CLI セキュリティ オプション	38
SNMP セキュリティ オプション	38
スイッチの AAA 機能	39
認証	39
認証	39
アカウントिंग	40
リモート AAA サービス	40
リモート認証に関する注意事項	40
サーバー グループ	40
AAA サービス設定オプション	41
エラー対応ステータス	42
AAA サーバーのモニタリング	42
認証と許可のプロセス	43
AAA 認証のデフォルト ユーザ ロールのイネーブル化	45
TACACS+ サーバーでのロールベース認証の設定	45
認証のフォールバック メカニズムの設定	47
認可プロファイルの確認	48
認証のテスト	49
ログインパラメータの設定	49
AAA サーバーのモニタリング パラメータをグローバルに設定	51
LDAP の設定	52
LDAP 認証および許可	53
LDAP の注意事項と制約事項	53
LDAP の前提条件	54
LDAP のイネーブル化	54

リモート LDAP サーバ プロファイルを構成	55
LDAP サーバの rootDN の設定	56
LDAP サーバ グループの設定	57
グローバルな LDAP タイムアウト間隔の設定	58
LDAP サーバの接続タイムアウトの構成	59
グローバル LDAP サーバ ポートの設定	60
LDAP サーバの宛て先ポートを構成	61
LDAP サーバの SSL トランスポートの構成	61
LDAP 検索マップの設定	62
LDAP デッド タイム間隔の設定	63
LDAP サーバでの AAA 許可の設定	64
LDAP のディセーブル化	66
LDAP の設定例	67
デフォルト設定	68
RADIUS サーバ モニタリング パラメータの設定	68
RADIUS サーバのデフォルト設定	68
RADIUS サーバの IPv4 アドレスの設定	69
RADIUS サーバの IPv6 アドレスの設定	70
RADIUS サーバの DNS 名の設定	70
RADIUS サーバにおける暗号の種類と事前共有キーのデフォルト値の概要	71
RADIUS サーバにおける暗号の種類と事前共有キーのデフォルト値の設定	72
RADIUS サーバのタイムアウト間隔の設定	72
RADIUS サーバのタイムアウト間隔および再送信のデフォルト値の設定	73
RADIUS サーバ モニタリング パラメータの設定	73
テストアイドルタイマーの設定	73
テストユーザー名の設定	74
デッドタイマーの設定	75
RADIUS サーバの概要	76
テストアイドルタイマーの設定	76
テストユーザー名の設定	76
RADIUS サーバの検証の概要	76

モニタリング用 RADIUS テスト メッセージの送信	77
ログイン時にユーザによる RADIUS サーバの指定を許可	77
ベンダー固有属性の概要	78
VSA の形式	78
AAA サーバーでの SNMPv3 の指定	79
RADIUS サーバーの詳細の表示	80
RADIUS サーバー統計情報の表示	80
ワンタイム パスワード サポート	81
管理者パスワードの回復	81
network-admin 権限での CLI の使用	82
スイッチの電源の再投入	82
TACACS+ サーバー モニタリング パラメータの設定	84
TACACS+ について	84
TACACS+ サーバーのデフォルト設定	84
TACACS+ サーバーにおける暗号の種類と事前共有キーのデフォルト値の概要	85
TACACS+ のイネーブル化	85
TACACS+ サーバーの IPv4 アドレスの設定	85
TACACS+ サーバーの IPv6 アドレスの設定	86
TACACS+ サーバーの DNS 名の設定	87
グローバル秘密キーの設定	88
TACACS+ サーバーのタイムアウト間隔および再送信のデフォルト値の設定	89
タイムアウト値の設定	89
TACACS+ サーバーの概要	89
TACACS+ サーバー モニタリング パラメータの設定	90
TACACS+ テストアイドルタイマーの設定	90
テスト ユーザー名の設定	91
デッドタイマーの設定	91
モニタリング用 TACACS+ テスト メッセージの送信	92
TACACS+ サーバーからのパスワード エージング通知	92
TACACS+ サーバーの検証の概要	93
TACACS+ サーバーの定期的な検証	94

ユーザーによるログイン時の TACACS+ サーバー指定の概要	94
ユーザによるログイン時の TACACS+ サーバ指定の許可	94
Cisco Secure ACS 5.x GUI でのロールの定義	95
ロールのカスタム属性の定義	95
サポートされている TACACS+ サーバー パラメータ	95
TACACS+ サーバーの詳細の表示	96
TACACS+ サーバ統計情報のクリア	97
サーバー グループの設定	97
RADIUS サーバー グループの設定概要	98
TACACS+ サーバー グループの設定概要	99
無応答サーバーのバイパス（回避）の概要	101
AAA サーバーへの配信	101
AAA RADIUS サーバーへの配信のイネーブル化	101
AAA TACACS+ サーバーへの配信のイネーブル化	102
スイッチでの配信セッションの開始	102
セッションステータスの表示	103
配信する保留中の設定の表示	103
RADIUS 情報の配布のコミット	104
TACACS+ 情報の配信のコミット	104
RADIUS の配布セッションの廃棄	104
TACACS+ の配布セッションの廃棄	105
セッションのクリア	105
RADIUS および TACACS+ 設定のマージに関する注意事項	105
CHAP 認証	107
CHAP 認証の有効化	107
MSCHAP による認証	107
MSCHAP のイネーブル化の概要	108
MSCHAP 認証のイネーブル化	108
MSCHAPv2 認証のイネーブル化	108
ローカル AAA サービス	109
AAA 認証のディセーブル化	110

AAA 認証の表示	110
アカウントिंग サービスの設定	111
アカウントング設定の表示	111
アカウントング ログのクリア	113
Cisco Access Control Servers の設定	113
デフォルト設定	116

第 6 章

IPv4 および IPv6 のアクセス コントロール リストの設定	119
IPv4 および IPv6 のアクセス コントロール リストの概要	120
IPv4-ACL および IPv6-ACL 設定に関する考慮事項	121
フィルタの内容について	121
プロトコル情報	122
アドレス情報	122
ポート情報	123
ICMP 情報	124
ToS 情報	125
IPv4-ACL または IPv6-ACL の作成	125
IPv4-ACL の作成	125
IPv6-ACL の作成	126
IPv4-ACL の定義	127
IPv6-ACL の定義	127
IPv4-ACL のオペランドとポートのオプション	128
IPv6-ACL のオペランドとポートのオプション	128
既存の IPv4-ACL への IP フィルタの追加	129
既存の IPv6-ACL への IP フィルタの追加	129
既存の IPv4-ACL からの IP フィルタの削除	130
既存の IPv6-ACL からの IP フィルタの削除	130
IPv4-ACL または IPv6-ACL の設定の確認	131
IP-ACL ログ ダンプの読み取り	132
インターフェイスへの IP-ACL の適用	133
インターフェイスへの IPv6-ACL の適用	135

mgmt0 への IP-ACL の適用	135
インターフェイスの IP-ACL 設定の確認	136
Open IP Ports on Cisco MDS 9000 Series Platforms	137
IP-ACL カウンタのクリーンアップ	138

第 7 章

認証局およびデジタル証明書の設定 139

認証局およびデジタル証明書について	139
認証局およびデジタル証明書の目的	139
信頼モデル、トラストポイント、アイデンティティ 証明機関	140
RSA キー ペアおよびアイデンティティ 証明書	140
複数の信頼された証明機関	142
複数のアイデンティティ 証明機関	142
PKI 登録	142
カットアンドペーストによる手動登録	143
ピア証明書の検証	143
CRL のダウンロード、キャッシュ、およびチェックのサポート	144
証明書および関連キーペアのインポートとエクスポート	144
認証局およびデジタル証明書の設定	144
ホスト名および IP ドメイン名の設定	144
RSA キーペアの生成	145
トラスト ポイント認証局関連付けを作成	146
トラスト ポイントの認証局	147
証明書取消確認方法の設定	148
証明書署名要求の生成	149
アイデンティティ証明書のインストール	150
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	151
認証局および証明書の構成のモニタリングとメンテナンス	151
違うデバイスにキーペアと証明書署名要求を生成	152
PKCS12 フォーマットのアイデンティティ情報をエクスポート	152
PKCS12 形式でのアイデンティティ情報のインポート	153
CRL の設定	154

認証局構成から認定を削除	154
スイッチからの RSA キーペアの削除	155
キーペアと証明機関情報の表示	156
設定例	156
MDS スイッチでの証明書の設定	156
認証局の CA 証明書をダウンロード	160
アイデンティティ証明書の要求	168
証明書の取り消し	182
CRL の作成と公開	185
CRL のダウンロード	187
CRL のインポート	192
上限	195
デフォルト設定	195

第 8 章

SSH サービスおよび Telnet の構成	197
SSH サービスに関する情報	197
SSH サーバー	198
SSH クライアント	198
SSH サーバ キー	198
デジタル証明書を使用した SSH 認証	199
Telnet サーバ	199
SSH の設定	199
SSH 名の構成	199
SSH 接続の構成	200
SSH サーバー キー ペアの生成	201
SSH キーの指定	202
OpenSSH による SSH キーの指定	202
IETF SECSH による SSH キーの指定	202
PEM の公開キー証明書による SSH キーの指定	203
ログイン グレイス タイムの SSH コネクションの構成	204
生成したキー ペアの上書き	205

SSH ログイン試行の最大回数の設定	205
SSH ホストのクリア	207
SSH または Telnet サービスのイネーブル化	207
SSH プロトコル ステータスの表示	208
パスワードのないファイル コピーおよび SSH	209
SSH のデフォルト設定	211

第 9 章

IPS セキュリティ構成の指定	213
IPsecについての情報	214
IKE の概要	216
IPSec の互換性	216
IPSec および IKE に関する用語	217
サポート対象の IPSec トランスフォームおよびアルゴリズム	219
サポート対象の IKE トランスフォームおよびアルゴリズム	219
IPSec デジタル証明書のサポート	220
CA およびデジタル証明書を使用しない IPSec の実装	220
CA およびデジタル証明書を使用した IPSec の実装	221
IPSec デバイスによる CA 証明書の使用方法	222
IPsec および IKE の手動設定	223
IKE Prerequisites	224
IPsec Prerequisites	224
IKE のイネーブル化	224
IKE ドメインの設定	225
IKE トンネルの概要	225
IKE ポリシー ネゴシエーションの概要	225
IKE ポリシーの設定	227
オプションの IKE パラメータの設定	229
ポリシーのライフタイム アソシエーションの設定	230
ピアのキープアライブ タイムの設定	231
発信側バージョンの設定	231
IKE トンネルまたはドメインのクリア	232

SA のリフレッシュ	232
クリプト IPv4-ACL	233
クリプト IPv4-ACL の概要	233
クリプト IPv4-ACL の注意事項	233
ミラー イメージ クリプト IPv4-ACL	236
クリプト IPv4-ACL の any キーワード	237
クリプト IPv4-ACL の作成	237
IPSec のトランスフォーム セットの概要	238
トランスフォーム セットの設定	239
クリプト マップ エントリの概要	240
ピア間の SA の確立	241
クリプト マップ設定の注意事項	241
クリプト マップ エントリの作成	242
SA ライフタイム ネゴシエーションの概要	243
SA ライフタイムの設定	243
AutoPeer オプションの概要	244
AutoPeer オプションの設定	245
PFS の概要	246
PFS の設定	246
クリプト マップ セット インターフェイスの適用の概要	246
クリプト マップ セットの適用	247
IPSec のメンテナンス	247
グローバル ライフタイム値	248
IKE 設定の表示	249
IPSec 設定の表示	250
FCIP の設定例	254
iSCSI の設定例	259
デフォルト設定	260
第 10 章	FC-SP および DHCHAP の設定 263
	ファブリック認証の概要 263

DHCHAP	264
既存の Cisco MDS 機能との DHCHAP の互換性	265
DHCHAP イネーブル化の概要	266
DHCHAP のイネーブル化	266
DHCHAP 認証モードの概要	266
DHCHAP モードの設定	267
DHCHAP ハッシュ アルゴリズムの概要	268
DHCHAP ハッシュ アルゴリズムの設定	268
DHCHAP グループ設定の概要	269
DHCHAP グループの設定	269
DHCHAP パスワードの概要	270
ローカル スイッチの DHCHAP パスワードの設定	270
リモート デバイスのパスワード設定の概要	271
リモート デバイスの DHCHAP パスワードの設定	272
DHCHAP タイムアウト値の概要	272
DHCHAP タイムアウト値の設定	272
DHCHAP AAA 認証の設定	273
プロトコル セキュリティ情報の表示	273
設定例	275
デフォルト設定	276
第 11 章	ポート セキュリティの設定 279
ポート セキュリティの概要	279
ポート セキュリティの実行	280
自動学習の概要	280
ポート セキュリティのアクティブ化	281
ポート セキュリティの設定	282
自動学習と CFS 配信を使用するポート セキュリティの設定	282
自動学習を使用し、CFS 配信を使用しないポート セキュリティの設定	283
手動データベース設定によるポート セキュリティの設定	283
ポート セキュリティのイネーブル化	284

ポートセキュリティのアクティブ化	284
ポートセキュリティのアクティブ化	284
データベースのアクティブ化の拒否	285
ポートセキュリティの強制的なアクティブ化	285
データベースの再アクティブ化	286
自動学習	287
自動学習のイネーブル化の概要	287
自動学習のイネーブル化	287
自動学習のディセーブル化	288
自動学習デバイスの許可	288
許可の例	289
ポートセキュリティの手動設定	291
WWN の識別の概要	291
許可済みのポート ペアの追加	292
ポートセキュリティ設定の配信	293
配信のイネーブル化	293
ファブリックのロック	294
変更のコミット	295
変更の廃棄	295
アクティブ化および自動学習の設定の配信	296
データベース マージの注意事項	297
データベースの相互作用	298
データベースのシナリオ	298
ポートセキュリティ データベースのコピー	299
ポートセキュリティ データベースの削除	300
ポートセキュリティ データベースのクリア	300
ポートセキュリティ設定の表示	301
デフォルト設定	304
第 12 章	Fibre Channel Common Transport 管理セキュリティの設定
	305
	Fibre Channel Common Transport の概要
	305

設定のガイドライン	306
Fibre Channel Common Transport クエリーの設定	306
Fibre Channel Common Transport 管理セキュリティの確認	307
デフォルト設定	307

第 13 章

ファブリック バインディングの設定	309
ファブリック バインディングの概要	309
ライセンス要件	309
ポート セキュリティとファブリック バインディングの比較	309
ファブリック バインディングの実行	311
ファブリック バインディングの設定	311
ファブリック バインディングのイネーブル化	311
FICON VSAN のスイッチ WWN リストの設定	312
ファイバチャネル VSAN のスイッチ WWN リストの設定	313
ファブリック バインディングのアクティブ化	314
ファブリック バインディングの強制的なアクティベーション	315
ファブリック バインディング設定の保存	316
ファブリック バインディング統計情報のクリア	316
ファブリック バインディング データベースの削除	317
ファブリック バインディング設定の確認	317
デフォルト設定	320

第 14 章

Cisco TrustSec ファイバチャネル リンク暗号化の設定	321
Cisco TrustSec FC リンク暗号化に関する用語	321
AES 暗号化のサポート	322
Cisco TrustSec FC リンク暗号化の概要	322
Supported Modules	322
Cisco TrustSec FC リンク暗号化のイネーブル化	322
セキュリティ アソシエーションの設定	323
セキュリティ アソシエーションパラメータの設定	324
ESP の設定	324

入力および出力ポートでの ESP の設定	325
ESP モードの設定	326
Cisco TrustSec FC リンク暗号化情報の表示	328
FC-SP のインターフェイス情報の表示	328
実行中のシステム情報の表示	329
FC-SP インターフェイス統計情報の表示	329
Cisco TrustSec FC リンク暗号化のベストプラクティス	329
一般的なベストプラクティス	330
キーの変更に関するベストプラクティス	330

第 15 章

セキュアブートの構成	333
Cisco Secure Boot に関する情報	333
偽造防止対策について	334



はじめに

ここでは、『Cisco MDS 9000 Series Configuration Guide』を使用している対象読者、構成、および表記法について説明します。また、関連資料の入手方法の情報を説明し、次の章にも続きます。

- [対象読者 \(xix ページ\)](#)
- [表記法 \(xix ページ\)](#)
- [関連資料 \(xx ページ\)](#)
- [通信、サービス、およびその他の情報 \(xxi ページ\)](#)

対象読者

このインストラクションガイドは、電子回路および配線手順に関する知識を持つ電子または電気機器の技術者を対象にしています。

表記法

このマニュアルでは、次の表記法を使用しています。



(注) 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。



注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

警告は、次のように表しています。



警告 「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。ステートメント 1071。

関連資料

Cisco MDS 9000 シリーズ スイッチのドキュメンテーションには、次のマニュアルが含まれます。

Release Notes

<http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-release-notes-list.html>

『Regulatory Compliance and Safety Information』

<http://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/hw/regulatory/compliance/RCSI.html>

互換性に関する情報

<http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-device-support-tables-list.html>

インストールおよびアップグレード

<http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-installation-guides-list.html>

Configuration

<http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-installation-and-configuration-guides-list.html>

CLI

<http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-command-reference-list.html>

トラブルシューティングおよび参考資料

<http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/tsd-products-support-troubleshoot-and-alerts.html>

オンラインでドキュメントを検索するには、次の Web サイトにある Cisco MDS NX-OS Documentation Locator を使用してください。

http://www.cisco.com/c/en/us/td/docs/storage/san_switches/mds9000/roadmaps/doclocator.html

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。
- 重要な技術によりビジネスに必要な影響を与えるには、[シスコサービス](#)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、[シスコ サポート](#)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 Marketplace](#) 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](#) 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。

Cisco Bug Search Tool

[Cisco 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 Cisco 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

新規および変更情報

機能名	説明	リリース	参照先
show ssl info	SSLバージョンを表示するためのサポートが追加されました。	8.4(2)	デジタル証明書を使用した SSH 認証 (199 ページ)
カスタム ロール	カスタムロールを作成するためのサポートが追加されました。The attribute-admin keyword was added for the rule command.	8.3(1)	カスタムロールによるロール変更の構成 (20 ページ)
LDAP 拡張機能	ポート 636 の LDAP 接続は、SSL または TLS で自動的にセキュリティ保護されます。	8.2(1)	リモート LDAP サーバ プロファイルを構成 (55 ページ)



CHAPTER 2

セキュリティの概要

Cisco MDS 9000 NX-OS ソフトウェアは、ストレージエリア ネットワーク (SAN) 内にセキュリティを提供する高度なセキュリティ機能をサポートしています。これらの機能は、故意か故意でないかにかかわらず、内部や外部の脅威からネットワークを保護します。

この章は、次の項で構成されています。

- [FIPS, on page 3](#)
- [ユーザー ロールおよび共通ロール, on page 4](#)
- [RADIUS および TACACS+, on page 4](#)
- [IP ACL, on page 5](#)
- [PKI, on page 5](#)
- [SSH サービスに関する情報, on page 5](#)
- [IPsec, on page 6](#)
- [FC-SP および DHCHAP, on page 6](#)
- [ポート セキュリティ, on page 6](#)
- [Fibre Channel Common Transport 管理サーバー クエリー, on page 7](#)
- [ファブリック バインディング, on page 7](#)
- [TrustSec ファイバチャネル リンク暗号化, on page 7](#)

FIPS

連邦情報処理標準 (FIPS) 発行 140-2、暗号化モジュールのセキュリティ要件では、暗号化モジュールの米国政府要件が詳述されています。FIPS 140-2 では、暗号モジュールがハードウェア、ソフトウェア、ファームウェア、または何らかの組み合わせのセットで、暗号機能またはプロセスを実装し、暗号アルゴリズムおよび任意のキー生成機能を含み、明確に定義された暗号境界の内部に位置しなければならないと定義しています。FIPS は特定の暗号アルゴリズムがセキュアであることを条件とするほか、ある暗号モジュールが FIPS 準拠であると称する場合は、どのアルゴリズムを使用すべきかも指定しています。

FIPS の設定については、「[Configuring FIPS](#)」を参照してください。

ユーザー ロールおよび共通ロール

ロールベースの許可は、ユーザーにロールを割り当てることによってスイッチへのアクセスを制限します。Cisco MDS 9000 ファミリ内のすべての管理アクセスは、ロールに基づきます。ユーザーは、ユーザーが属するロールによって明示的に許可されている管理操作の実行に制限されます。

ユーザー ロールおよび共通ロールの設定については、「[ロールベースの認証](#)」を参照してください。

RADIUS および TACACS+

認証、許可、アカウントिंग (AAA) 機能は、スイッチ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します。リモート AAA サーバーを利用するソリューションを提供するため、すべての Cisco MDS 9000 ファミリスイッチで Remote Authentication Dial-In User Service (RADIUS) プロトコルおよび Terminal Access Controller Access Control System Plus (TACACS+) プロトコルが使用されています。このセキュリティ機能は、AAA サーバーでの中央集中型のユーザー アカウント管理機能を実現します。

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ーをネットワークアクセスサーバーとして使用している場合、ネットワークアクセスサーバーと RADIUS または TACACS+ セキュリティサーバーは AAA を介して通信します。

このマニュアルの各章では、次の機能について説明します。

- **スイッチ管理**：コマンドライン インターフェイス (CLI) や Simple Network Management Protocol (SNMP) などのすべての管理アクセス手段にセキュリティを提供する管理セキュリティ システム。
- **スイッチの AAA 機能**：Cisco MDS 9000 ファミリの任意のスイッチで、コマンドライン インターフェイス (CLI) または簡易ネットワーク管理プロトコル (SNMP) を使用して AAA スイッチ機能を設定する機能。
- **RADIUS**：不正なアクセスからネットワークを保護する、AAA を介して実装された分散型クライアント/サーバー システム。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、すべてのユーザー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 サーバーに送信されます。
- **TACACS+**：AAA を介して実装されるセキュリティアプリケーション。ルータまたはネットワーク アクセスサーバーへのアクセスを取得しようとするユーザーの中央集中型検証を実現します。TACACS+ サービスは、一般に UNIX または Windows NT ワークステーションで稼働する TACACS+ デモン上のデータベースに保持されます。TACACS+ では、独立したモジュラ型の認証、許可、アカウントング機能が提供されます。

RADIUS および TACACS+ の設定については、「[スイッチ管理のセキュリティ](#)」を参照してください。

IP ACL

IP アクセス コントロール リスト (ACL) は、帯域外管理イーサネット インターフェイスおよび帯域内 IP 管理インターフェイスでの基本的なネットワーク セキュリティを実現します。Cisco MDS 9000 ファミリー スイッチでは、IP ACL を使用して不明や送信元や信頼できない送信元からのトラフィックを制限し、ユーザー ID またはデバイス タイプに基づいてネットワークの使用を制限します。

IP ACL の設定については、「[IPv4 および IPv6 のアクセス コントロール リストの概要](#)」を参照してください。

PKI

公開キー インフラストラクチャ (PKI) は、MDS 9000 スイッチがネットワーク内のセキュアな通信を実現するためにデジタル証明書を取得し、使用することを可能にします。PKI のサポートにより、デジタル証明書をサポートする IP セキュリティ プロトコル (IPSec)、インターネットキー交換 (IKE)、およびセキュアシェル (SSH) などのアプリケーションの管理機能およびスケーラビリティが実現します。

PKI の設定については、「[認証局およびデジタル証明書について](#)」を参照してください。

SSH サービスに関する情報

セキュアシェル (SSH) は、Cisco NX-OS CLI に対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。SSH キーは、次の SSH オプションに使用できます。

- Rivest, Shamir, Adelman (RSA) を使用する SSH2
- DSA を使用する SSH2

Cisco MDS NX-OS リリース 8.2(1) 以降、SHA2 フィンガー プリント ハッシュはすべての Cisco MDS デバイスでデフォルトでサポートされています。

RSA キーによるセキュア SSH 接続は、Cisco MDS 9000 シリーズのすべてのスイッチでデフォルトで使用できます。DSA キーによるセキュア SSH 接続が必要な場合は、デフォルトの SSH 接続をディセーブルにし、DSA キーを生成して、SSH 接続をイネーブルにする必要があります (SSH サーバー キー ペアの生成, [on page 201](#)を参照)。

サーバー キーを生成するには、`ssh key` コマンドを使用します。



Caution SSH でスイッチにログインし、**aaa authentication login default none** コマンドを発行した場合、ログインするために1つ以上のキーストロークを入力する必要があります。少なくとも1つのキーストロークを入力せずに **Enter** キーを押すと、ログインは拒否されます。

SSH サービスの設定の詳細については、次を参照してください。 [SSH サービスおよび Telnet の構成, on page 197](#)

IPsec

IP Security (IPSec) プロトコルは、加入ピア間にデータ機密保持、データの整合性、およびデータ認証を提供する、Internet Engineering Task Force (IETF) によるオープン規格のフレームワークです。IPSec は、ホスト ペア間、セキュリティ ゲートウェイ ペア間、またはセキュリティ ゲートウェイとホスト間の1つまたは複数のデータフローの保護など、IP レイヤにセキュリティ サービスを提供します。

IPsec の設定については、「[IPsec についての情報](#)」を参照してください。

FC-SP および DHCHAP

Fibre Channel Security Protocol (FC-SP) 機能は、スイッチ間およびホストとスイッチ間で認証を実行して、企業全体のファブリックに関するセキュリティ問題を解決します。Diffie-Hellman (DH) Challenge Handshake Authentication Protocol (DHCHAP) は、Cisco MDS 9000 ファミリスイッチとその他のデバイス間で認証を行う FC-SP プロトコルです。DHCHAP は、CHAP プロトコルと Diffie-Hellman 交換を組み合わせて構成されています。

FC-SP の使用により、スイッチ、ストレージデバイス、およびホストは信頼性の高い管理可能な認証メカニズムを使ってそれぞれのアイデンティティを証明できます。FC-SP の使用により、ファイバチャネルトラフィックをフレーム単位で保護することで、信頼できないリンクであってもスヌーピングやハイジャックを防止できます。ポリシーと管理アクションの一貫した組み合わせがファブリックを介して伝播されて、ファブリック全体での均一なレベルのセキュリティが実現します。

FC-SP および DHCHAP の詳細については、「[ファブリック認証の概要](#)」を参照してください。

ポートセキュリティ

ポートセキュリティ機能は、1つ以上の所定のスイッチポートへのアクセス権を持つ特定の World-Wide Name (WWN) をバインドすることによって、スイッチポートへの不正なアクセスを防止します。

スイッチ ポートでポートセキュリティをイネーブルにしている場合は、そのポートに接続するすべてのデバイスがポートセキュリティ データベースになければならず、所定のポートにバインドされているものとしてデータベースに記されている必要があります。これらの両方の基準を満たしていないと、ポートは動作上アクティブな状態にならず、ポートに接続しているデバイスは SAN へのアクセスを拒否されます。

ポートセキュリティの設定については、[ポートセキュリティの概要, on page 279](#)を参照してください。

Fibre Channel Common Transport 管理サーバー クエリー

FC-CT クエリー管理機能により、管理者はストレージ管理者またはネットワーク管理者だけが、スイッチに対してクエリーを送信し、情報にアクセスできるようにネットワークを設定できます。このような情報には、ファブリック内のログインデバイス、ファブリック内のスイッチなどのデバイス、デバイスの接続方法、各スイッチのポートの数、各ポートの接続先、設定済みゾーンの情報、ゾーンまたはゾーンセットの追加と削除の権限、ファブリックに接続するすべてのホストのホスト バス アダプタ (HBA) の詳細などがあります。

ファブリック バインディングの設定については、[Fibre Channel Common Transport の概要, on page 305](#)を参照してください。

ファブリック バインディング

ファブリック バインディング機能では、ファブリック バインディング設定で指定したスイッチ間だけでスイッチ間リンク (ISL) をイネーブルにできます。この機能を使用すると、不正なスイッチがファブリックに参加したり、現在のファブリック処理が中断されたりすることがなくなります。この機能では、Exchange Fabric Membership Data (EEMD) プロトコルを使用することによって、許可されたスイッチのリストがファブリック内の全スイッチで同一になります。

ファブリック バインディングの設定については、[ファブリック バインディングの概要, on page 309](#)を参照してください。

TrustSec ファイバチャネル リンク暗号化

Cisco TrustSec ファイバチャネル リンク暗号化は、Fibre Channel-Security Protocol (FC-SP) の拡張機能であり、既存のFC-SPアーキテクチャを使用してトランザクションの整合性と機密保持を実現します。暗号化をピア認証に追加することにより、セキュリティを確保し、望ましくないトラフィック傍受を防止します。ピア認証は、Diffie-Hellman (DH) Challenge Handshake Authentication Protocol (DHCHAP) プロトコルを使用した FC-SP 標準に従って実装されます。

TrustSec ファイバチャネル リンク暗号化については、[Fibre Channel Common Transport の概要, on page 305](#)を参照してください。



CHAPTER 3

Configuring FIPS

The Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules, details the U.S. government requirements for cryptographic modules. FIPS 140-2 specifies that a cryptographic module should be a set of hardware, software, firmware, or some combination that implements cryptographic functions or processes, including cryptographic algorithms and, optionally, key generation, and is contained within a defined cryptographic boundary.

FIPS specifies certain crypto algorithms as secure, and it also identifies which algorithms should be used if a cryptographic module is to be called FIPS compliant.



Note From Cisco MDS NX-OS Release 8.3(1) and later, FIPS is compliant on Cisco MDS devices. On Cisco MDS NX-OS Release 7.x and earlier, FIPS feature is supported, but it is not FIPS compliant (certification process is with the U.S. government). For current FIPS compliance, refer to the Table 1 Current FIPS Compliance Reviews section in the [Cisco FIPS 140](#) document.

This chapter includes the following sections:

- [設定のガイドライン, on page 9](#)
- [FIPS モードのイネーブル化, on page 10](#)
- [FIPS ステータスの表示, on page 10](#)
- [FIPS のセルフテスト, on page 10](#)

設定のガイドライン

FIPS モードをイネーブルにする前に次の注意事項を守ってください。

- パスワードは最小限 8 文字の長さで作成してください。
- Telnet をディセーブルにします。ユーザーのログインは SSH だけで行ってください。
- RADIUS/TACACS+ によるリモート認証をディセーブルにしてください。スイッチに対してローカルのユーザーだけが認証可能です。
- SNMP v1 および v2 をディセーブルにしてください。SNMP v3 に対して設定された、スイッチ上の既存ユーザー アカウントのいずれについても、認証およびプライバシー用 AES/3DES は SHA で設定されていなければなりません。

- VRRP をディセーブルにしてください。
- スイッチ上で FIPS と IPsec を同時に構成しないでください。FIPS が有効になっている場合、IKE を構成すると、FCIP リンクは起動しません。
- SSH サーバーの RSA1 キーペアすべてを削除してください。
- FIPS が有効になっていて、Cisco MDS NX-OS リリース 6.x、7.x、または 8.1 (x) から Cisco MDS NX-OS リリース 8.2 (1) 以降のリリースにアップグレードする場合、8.2 (x) リリースにアップグレードされたリリースで FIPS を無効化することはできません。

FIPS モードのイネーブル化

FIPS モードを有効にするには、次の手順に従ってください。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal	コンフィギュレーションモードに入ります。
ステップ 2	fips mode enable Example: switch(config)# fips mode enable	FIPS モードをイネーブルにします。
ステップ 3	no fips mode enable Example: switch(config)# no fips mode enable	(オプション) FIPS モードをディセーブルにします。

FIPS ステータスの表示

FIPS のステータスを表示するには **show fips status** コマンドを入力します。

FIPS のセルフテスト

暗号モジュールは、適正に動作していることを確認するために、電源投入時のセルフテストと条件付きセルフテストを実行しなければなりません。



Note FIPS の電源投入時セルフテストは、`fips mode enable` コマンドを入力して FIPS モードがイネーブルにされていると自動的に実行されます。スイッチが FIPS モードに入るのは、すべてのセルフテストが正しく完了したときだけです。セルフテストのいずれかが失敗すると、スイッチは再起動します。

電源投入時セルフテストは、FIPS モードのイネーブル後、即時に実行されます。既知の解を使用する暗号アルゴリズムテストは、Cisco MDS 9000 ファミリ製品に実装されている FIPS 140-2 認定暗号アルゴリズムのそれぞれに対して、すべての暗号機能で実行されなければなりません。

既知解テスト (KAT) を利用すると、暗号アルゴリズムは正しい出力があらかじめわかっているデータに対して実行され、その計算出力は前回生成された出力と比較されます。計算出力が既知解と等しくない場合は、既知解テストに失敗したことになります。

何かに対応してセキュリティ機能または操作が始動された場合は、条件付きセルフテストが実行されなければなりません。電源投入時セルフテストとは異なって、条件付きセルフテストはそれぞれに関連する機能がアクセスされるたびに実行されます。

条件付きセルフテストでは次を含むテストが行われます。

- ペア整合性テスト：このテストは公開キー/秘密キー ペアが生成されたときに実行されません。
- 乱数連続生成テスト：このテストは乱数が生成されたときに実行されます。

以上の両方はスイッチが FIPS モードに入っていると自動的に実行されます。



第 4 章

ユーザアカウントおよび RBAC の設定

この章では、Cisco MDS デバイス上でユーザアカウントおよびロールベースアクセスコントロール（RBAC）を設定する手順について説明します。

この章は、次の項で構成されています。

- [ユーザアカウントおよび RBAC の概要, on page 13](#)
- [ロールベースの認証, on page 18](#)
- [ロールの配信, on page 26](#)
- [共通ロールの設定, on page 32](#)
- [デフォルト設定, on page 34](#)

ユーザアカウントおよび RBAC の概要

ユーザアカウントの作成および管理を行い、Cisco MDS デバイス上で実行できる操作を制限するロールを割り当てることができます。ロールベースアクセスコントロール（RBAC）を使用すると、割り当てたロールにルールを定義して、ユーザが行える管理操作の権限を制限できます。

Cisco MDS 9000 ファミリースイッチでは、すべてのユーザのアカウント情報がシステムに保管されます。ユーザーの認証情報、ユーザー名、ユーザーパスワード、パスワードの有効期限、およびロールメンバーシップが、そのユーザーのユーザープロファイルに保存されます。

ここで説明するタスクを利用すると、ユーザーの作成および既存ユーザーのプロファイルの修正を実行できます。これらのタスクは管理者によって定義されている特権ユーザーに制限されます。

ユーザアカウント

最大256のユーザアカウントを作成できます。デフォルトでは、明示的に期限を指定しないかぎり、ユーザアカウントは無期限に有効です。expire オプションを使用すると、ユーザアカウントをディセーブルにする日付を設定できます。

ユーザーを作成する際、次の点に注意してください。

- 次の単語は予約済みのため、ユーザー設定には使用できません：bin、daemon、adm、lp、sync、shutdown、halt、mail、news、uucp、operator、games、gopher、ftp、nobody、nscd、mailnull、rpc、rpcuser、xfs、gdm、mtuser、ftuser、man、およびsys。
- ユーザーパスワードはスイッチコンフィギュレーションファイルに表示されません。
- パスワードの長さは、ファブリックの検出用にCisco DCNMで8文字以上を指定する必要があります。この制限は、Cisco DCNM リリース 5.2(1) から適用されます。
- **snmp-server user** コマンドで指定したパスワードと、パスワード仕様**username** コマンドが同期します。
- デフォルトでは、明示的に期限を指定しないかぎり、ユーザーアカウントは無期限に有効です。**expire** オプションを使用すると、ユーザーアカウントをディセーブルにする日付を設定できます。日付はYYYY-MM-DD形式で指定します。
- パスワードが簡潔である場合（短く、解読しやすい場合）、パスワード設定は拒否されます。サンプル設定のように、強力なパスワードを設定してください。パスワードでは大文字と小文字が区別されます。「admin」はCisco MDS 9000ファミリスイッチのデフォルトパスワードではなくなりました。強力なパスワードを明確に設定する必要があります。
- Cisco MDS NX-OS リリース 8.2(1) 以降、デフォルトのユーザーアカウントでは、SHA-2で暗号化されたパスワードを使用します。作成された対応するSNMPユーザーは引き続きMD5で暗号化されます。MD5で暗号化された既存のユーザーアカウントは、パスワードを変更しない限りそのままです。この機能は、Cisco MDS 9132T、MDS 9148S、MDS 9148T、MDS 9396S、MDS 9396T、MDS 9220i、MDS 9250i、およびMDS 9700シリーズのスイッチでサポートされています。

snmp-server user user-name role-name auth sha privacy-encryption コマンドをHMAC-SHA-96認証レベルおよびプライバシー暗号化パラメータとともに使用して、ユーザーとそのロールの設定を変更します。

```
switch(config)# snmp-server user Bill network-admin auth sha abcd1234 priv abcdefgh
```

- トラブルシューティングのために**internal** キーワードを指定してコマンドを発行するには、**network-admin** グループのメンバーであるアカウントが必要です。



Caution

Cisco MDS NX-OS では、ユーザ名が英数字で始まる限り、リモートで作成するか（TACACS+またはRADIUSを使用）ローカルで作成するかに関係なく、英数字または特定の特殊文字（+（プラス）、=（等号）、_（下線）、-（ハイフン）、\（バックスラッシュ）、および.（ピリオド））を使って作成したユーザ名がサポートされます。特殊文字（指定された特殊文字を除く）を使用してローカルユーザ名を作成することはできません。サポートされていない特殊文字によるユーザ名がAAAサーバーに存在し、ログイン時に入力されると、そのユーザーはアクセスを拒否されます。

強力なパスワードの特性

強力なパスワードは、次の特性を持ちます。

- 長さが 8 文字以上である
- 複数の連続する文字 ("abcd" など) を含んでいない
- 複数の同じ文字の繰り返し ("aaabbb" など) を含んでいない
- 辞書に載っている単語を含んでいない
- 正しい名前を含んでいない
- 大文字および小文字の両方が含まれている
- 数字が含まれている

強力なパスワードの例を次に示します。

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

パスワードの強度確認をイネーブルにすると、パスワードが単純である場合（短く、簡単に解読されるパスワードなど）に、Cisco MDS NX-OS ソフトウェアによってパスワード設定が拒否されます。サンプル設定のように、強力なパスワードを設定してください。パスワードは大文字と小文字が区別されます。

パスワード強度の確認

ユーザアカウントに対して弱いパスワードを設定しないように、パスワードの強度確認機能をイネーブルにすることができます。



Note パスワード確認をイネーブル化にしても、既存パスワードの強度確認は行われません。

パスワードの強度の確認をイネーブルにするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **password strength-check**

パスワードの強度確認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。

パスワードの強度確認をディセーブルにするには、このコマンドの **no** 形式を使用します。

ステップ 3 switch(config)# **exit**

(任意) 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 switch(config)# **show password strength-check**

(任意) パスワードの強度確認の設定を表示します。

ステップ 5 switch(config)# **copy running-config startup-config**

(任意) 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。

ユーザーの設定

新規ユーザーの設定または既存ユーザーのプロファイル修正を行うには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **username usam password abcd123AAA expire 2003-05-31**

ユーザーアカウント (usam) を作成または更新し、パスワード (abcd123AAA) および有効期限 2003-05-31 を設定します。

ステップ 3 switch(config)# **username msam password 0 abcd12AAA role network-operator**

ユーザーアカウント (msam) を作成または更新し、クリアテキスト (0 で示される) のパスワード (abcd12AAA) を指定します。パスワードの長さは 64 文字に制限されています。

ステップ 4 switch(config)# **username user1 password 5 \$1\$UgOR6Xqb\$z.HZlMk.ZGr9VH67a**

ユーザーアカウント (user1) に暗号化 (5 で指定される) パスワード (!@*asdfsdfjh!@df) を指定します。

Note ユーザーが暗号化パスワードオプションを指定して作成された場合、対応する SNMP ユーザーは作成されません。

ステップ 5 switch(config)# **username usam role network-admin**

network-admin ロールに指定のユーザー (usam) を追加します。

ステップ 6 switch(config)# **no username usam role vsan-admin**

(オプション) vsan-admin ロールから指定のユーザー (usam) を削除します。

- ステップ 7** switch(config)# **username admin sshkey ssh-rsa**
既存のユーザー アカウント (admin) の SSH キーを指定します。
- ステップ 8** switch(config)# **no username admin sshkey ssh-rsa**
(オプション) ユーザー アカウント (admin) の SSH キーを削除します。
- ステップ 9** switch(config)# **username usam ssh-cert-dn usam-dn dsa**
既存のユーザー アカウント (usam) の認証に使用する SSH X.509 証明書の識別名と DSA アルゴリズムを指定します。
- ステップ 10** switch(config)# **username user1 ssh-cert-dn user1-dn rsa**
既存のユーザー アカウント (user1) の認証に使用する SSH X.509 証明書の識別名と RSA アルゴリズムを指定します。
- ステップ 11** switch(config)# **no username admin ssh-cert-dn admin-dn dsa**
ユーザー アカウント (admin) の SSH X.509 証明書の識別名を削除します。

ユーザーのログアウト

スイッチの他のユーザーをログアウトするには、**clear user** コマンドを使用します。

次の例では、vsam という名前のユーザーが、スイッチからログアウトされます。

```
switch# clear user vsam
```

ログインしているすべてのユーザーの表示

ログインしているユーザーのリストを表示するには、**show users** コマンドを使用します (次の例を参照)。

```
switch# show users

admin    pts/7      Jan 12 20:56 (10.77.202.149)
admin    pts/9      Jan 12 23:29 (user.example.com)
admin    pts/10     Jan 13 03:05 (dhcp-10-10-1-1.example.com)
admin    pts/11     Jan 13 01:53 (dhcp-10-10-2-2.example.com)
```

ユーザー アカウント情報の表示

指定したユーザーに関する情報の表示

ユーザー アカウントに関して設定されている情報を表示するには、**show user-account** コマンドを使用します。次の例を参照してください。

```
switch# show user-account user1

user:user1
    this user account has no expiry date
    roles:network-operator
no password set. Local login not allowed
Remote login through RADIUS is possible
```

すべてのユーザーに関する情報の表示

```
switch# show user-account
show user-account
user:admin
    this user account has no expiry date
    roles:network-admin
user:usam
    expires on Sat May 31 00:00:00 2003
    roles:network-admin network-operator
user:msam
    this user account has no expiry date
    roles:network-operator
user:user1
    this user account has no expiry date
    roles:network-operator
no password set. local login not allowed
Remote login through RADIUS is possible
```

ロールベースの認証

ユーザアカウントの作成および管理を行い、Cisco MDS デバイス上で実行できる操作を制限するロールを割り当てることができます。ロールベースアクセスコントロール (RBAC) を使用すると、割り当てたロールにルールを定義して、ユーザが行える管理操作の権限を制限できます。

ユーザーがコマンドの実行、コマンドの完了、またはコンテキストヘルプの取得を行った場合、ユーザーにそのコマンドへのアクセス権がある場合のみ、スイッチソフトウェアによって処理の続行が許可されます。

ユーザロール

ユーザーロールには、そのロールを割り当てられたユーザーが実行できる操作を定義するルールが含まれています。各ユーザーロールに複数のルールを含めることができ、各ユーザーが複数のロールを持つことができます。たとえば、ロール1ユーザーには構成コマンドへのアクセスだけが、ロール2ユーザーにはデバッグコマンドへのアクセスだけが許可されているとします。この場合、ロール1とロール2の両方に所属しているユーザーは、構成コマンドとデバッグコマンドにアクセスできます。



Note ユーザーが複数のロールに所属している場合、各ロールで許可されているすべてのコマンドを実行できます。コマンドへのアクセス権は、コマンドへのアクセス拒否よりも優先されます。たとえば、TechDocs グループに属しているユーザーが、コンフィギュレーション コマンドへのアクセスを拒否されているとします。ただし、このユーザーはエンジニアリング グループにも属しており、コンフィギュレーション コマンドへのアクセス権を持っています。この場合、このユーザーはコンフィギュレーション コマンドにアクセスできます。

Cisco NX-OS ソフトウェアには、デフォルトで次のユーザー ロールが用意されています。

- **network-admin** : 他のユーザのプロファイルを変更するコマンドを除く、Cisco NX-OS デバイス全体への完全な読み取りおよび書き込みアクセス。
- **network-operator** : Cisco NX-OS デバイス全体への完全な読み取りアクセス権
- **server-admin** : Cisco NX-OS デバイス全体およびアップグレード機能への完全な読み取りアクセス。



Tip ロールを作成した時点で、必要なコマンドへのアクセスが即時に許可されるわけではありません。管理者が各ロールに適切なルールを設定して、必要なコマンドへのアクセスを許可する必要があります。

ロールの設定

追加ロールの作成または既存ロールのプロファイル修正を行うには、次の手順を実行します。



Note network-admin ロールに属するユーザーだけがロールを作成できます。

Procedure

ステップ 1 switch# **config terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **role name techdocs**

```
switch(config-role)#
```

指定したロール サブ モードを開始します。

ステップ 3 switch(config)# **no role name techdocs**

(オプション) ロール techdocs を削除します。

ステップ4 switch(config-role)# **description Entire Tech Docs group**

新しいロールに記述を割り当てます。記述は1行に制限され、スペースを含めることができません。

ステップ5 switch(config-role)# **no description**

(オプション) Tech Docs グループの記述をリセットします。

カスタムロールによるロール変更の構成

Cisco MDS NX-OS リリース 8.3 (1) から、ユーザーが他のユーザーのアカウント（ロールまたはパスワード）を変更できる「管理者」ユーザーに相当するカスタムロールを作成できます。ロールを「admin」ユーザーと同等になるように変更するには、ロールで **attribute-admin**[ルール (rule)] を構成します。

**Note**

- **attribute-admin**[ルール (rule)] は、既存のルールと相互に排他的です。既存のルールを削除して、新しい **attribute-admin** ルールを構成します。
- サポートされていないソフトウェアイメージがファブリックに存在する場合、**attribute-admin** コマンドの設定中にロール配布機能が機能不全になることはありません。代わりに、それは受け入れられ、サポートされていないルールの無効なルールとして表示されます。
- サポートされていないソフトウェアイメージがファブリックに存在する場合、相互に排他的な構成のロール配布機能は機能不全にしません。
- **attribute-admin** 特権を持つユーザーは、Dplug のロードが機能しません。
- **attribute-admin** 特権を持つユーザーの場合、の下の **show system internal kernel memory global detail** コマンド出力は **show tech-support details** 機能不全にします。

カスタムロールを作成または、既存ロールのプロファイルを変更するには、次の手順を実行します。

Procedure**ステップ1** switch# **config terminal**

コンフィギュレーションモードに入ります。

ステップ2 switch(config)# **role name techdocs**

switch(config-role)#

指定したロールサブモードを開始します。

ステップ 3 switch(config)# **no role name techdocs**

(オプション) ロール techdocs を削除します。

ステップ 4 switch(config-role)# **rule rule-number attribute-admin**

新しいロールに権限を割り当てます。

ステップ 5 switch(config-role)# **no rule 1 attribute-admin**

(オプション) ロールに割り当てられている管理者権限を削除します。

ステップ 6 switch# **showuser-account user-name**

(任意) ユーザアカウントの構成した情報を表示します。

ユーザ ロールとルール

ロールごとに最大 16 のルールを設定できます。ユーザ ロールを複数のユーザアカウントに割り当てることができます。

ルールが適用される順序は、ユーザー指定のルール番号で決まります。たとえば、ルール1のあとにルール2が適用され、ルール3以降が順に適用されます。network-admin ロールに属さないユーザーは、ロールに関連したコマンドを実行できません。



Note ユーザー ロールに設定された **read-write** ルールに関係なく、一部のコマンドは、あらかじめ定義された **network-admin** ロールでのみ実行できます。

たとえば、ユーザー A にすべての **show** コマンドの実行を許可されていても、ユーザー A が **network-admin** ロールに所属していないかぎり、ユーザー A は **show role** コマンドの出力を表示できません。

rule コマンドでは特定のロールで実行できる動作を指定します。ルールを構成する要素は、ルール番号、ルールタイプ（許可または拒否）、コマンドタイプ（**config**、**clear**、**show**、**exec**、**debug** など）、および任意の機能名（FSPF、ゾーン、VSAN、fcping、インターフェイスなど）です。



Note この場合、**exec CLI** コマンドでは、**show**、**debug**、および **clear** の各 CLI コマンドのカテゴリに含まれない、EXEC モード内のすべてのコマンドが対象になります。

デフォルトのロールがすべてのユーザーに適用でき、設定済みロールが特定のユーザーに適用できる場合、次のシナリオについて検討します。

- 同じルールタイプ（許可または拒否）：デフォルトロールと特定のユーザーに設定されているロールで同じルールタイプを使用する場合、特定のユーザーはデフォルトと設定済みの両方のロールのすべてのルールにアクセスできます。



Note 全て拒否するステートメントはルール0と見なされるため、明示的に許可されない限り、ユーザーロールに対するアクションは実行できません。

デフォルトロール A の場合、次のルールがあります。

```
rule 5 permit show feature environment
rule 4 permit show feature hardware
rule 3 permit config feature ssh
rule 2 permit config feature ntp
rule 1 permit config feature tacacs+
```

特定のユーザーにはロール B が割り当てられ、ルールは 1 つあります。

```
rule 1 permit config feature dpvm
```

特定のユーザーは、A と B の両方のルールにアクセスできます。

- 異なるルールタイプ：デフォルトロールと特定のユーザーに設定されているロールで特定のルールのルールタイプが異なる場合、デフォルトロールによって設定済みロールの競合するルールステートメントが上書きされます。

デフォルトロール A の場合、次のルールがあります。

```
rule 5 permit show feature environment
rule 4 permit show feature hardware
rule 3 permit config feature ssh
rule 2 permit config feature ntp
rule 1 permit config feature tacacs+
```

特定のユーザーにはロール B が割り当てられ、ルールは 2 つあります。

```
rule 6 permit config feature dpvm
rule 2 deny config feature ntp
```

A と B のルール 2 が競合します。この場合、A は B の競合するルールを上書きし、ユーザーには、上書きルールを含む、A と B の残りのルールが割り当てられます。

```
rule 6 permit config feature dpvm
rule 5 permit show feature environment
rule 4 permit show feature hardware
rule 3 permit config feature ssh
rule 2 permit config feature ntp -----> Overridden rule
rule 1 permit config feature tacacs+
```

SAN-OS リリース 3.3(1c) および NX-OS リリース 4.2(1a) 間のルール変更によるロールの動作への影響

ロールに設定可能なルールは、SAN-OS リリース 3.3(1c) と NX-OS リリース 4.2(1a) 間で修正されています。その結果、SAN-OS リリース 3.3(1c) から NX-OS リリース 4.2(1a) にアップグレー

ド後は、ロールが期待どおりに動作しません。必要な動作を復元するには手動での設定変更が必要です。

ルール4およびルール3：アップグレード後、exec と feature が削除されます。次のようにルール4およびルール3を変更します。

SAN-OS リリース 3.3(1c) のルール	NX-OS リリース 4.2(1a) では、ルールを次のように設定します。
rule 4 permit exec feature debug	rule 4 permit debug
rule 3 permit exec feature clear	rule 3 permit clear

ルール2：アップグレード後、exec feature license は廃止されます。

SAN-OS リリース 3.3(1c) のルール	NX-OS リリース 4.2(1a) のルール
rule 2 permit exec feature debug	リリース 4.2(1) では使用できません。

ルール9、ルール8およびルール7：アップグレード後、設定するには、機能を有効にする必要があります。SAN-OS リリース 3.3(1c) では、有効にしなくてもこの機能を設定できます。

SAN-OS リリース 3.3(1c) のルール	NX-OS リリース 4.2(1a) では、ルールを維持するには次のようにします。
rule 9 deny config feature telnet	リリース 4.2(1) では使用できません。
rule 8 deny config feature tacacs-server	アップグレード中に、機能を有効化してルールを維持します。そうしないと、ルールが消失します。
rule 7 deny config feature tacacs+	アップグレード中に、機能を有効化してルールを維持します。そうしないと、ルールが消失します。

プロファイルの変更

既存ロールのプロファイルを変更するには、次の手順を実行します。

Procedure

ステップ1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ2 switch(config)# **role name sangroup**

switch(config-role)#

既存のロール sangroup のロール コンフィギュレーション サブモードを開始します。

ステップ3 switch(config-role)# **rule 1 permit config**

```
switch(config-role)# rule 2 deny config feature fspf
switch(config-role)# rule 3 permit debug feature zone
switch(config-role)# rule 4 permit exec feature fcping
```

sangroup ロールに属するユーザーが、**spf config** コマンドを除くすべてのコンフィギュレーション コマンドを実行できるようにします。これらのユーザーは、**zone debug** コマンドおよび **fcping EXEC** モード コマンドも実行できます。

ステップ 4 switch(config-role)# no rule 4

ルール 4 を削除し、sangroup が **fcping** コマンドを実行できないようにします。

Example

ステップ 3 で、ルール 1 が最初に適用され、sangroup ユーザーがすべての **config** コマンドにアクセスすることが許可されます。次にルール 2 が適用され、sangroup ユーザーには FSPF 設定が拒否されます。結果として、sangroup ユーザーは **fspf** コンフィギュレーション コマンドを除く、他のすべての **config** コマンドを実行できます。

VSAN ポリシーの設定

VSAN ポリシーの設定には、ENTERPRISE_PKG ライセンスが必要です（詳細については、『Cisco MDS 9000 Family NX-OS Licensing Guide』を参照してください）。

選択した VSAN セットだけにタスクの実行が許可されるように、ルールを設定できます。デフォルトでは、どのロールの VSAN ポリシーも許可に設定されているため、すべての VSAN に対してタスクが実行されます。選択した VSAN セットだけにタスクの実行が許可されるルールを設定できます。1 つのロールに対して選択的に VSAN を許可するには、VSAN ポリシーを拒否に設定し、あとでその設定を許可に設定するか、または適切な VSAN を設定します。



Note VSAN ポリシーが拒否に設定されているルールに設定されているユーザーは、E ポートの設定を変更できません。これらのユーザーが変更できるのは、（ルールの内容に応じて）F ポートまたは FL ポートの設定だけです。これにより、これらのユーザーは、ファブリックのコア トポロジに影響する可能性のある設定を変更できなくなります。



Tip ロールを使用して、VSAN 管理者を作成できます。設定したルールに応じて、これらの VSAN 管理者は他の VSAN に影響を与えることなく、VSAN に MDS 機能（ゾーン、fcdomain、VSAN プロパティなど）を設定できます。また、ルールが複数の VSAN での処理を許可している場合、VSAN 管理者はこれらの VSAN 間で F ポートまたは FL ポートのメンバーシップを変更できます。

VSAN ポリシーが拒否に設定されているロールに属すユーザーのことを、VSAN 制限付きユーザーと呼びます。

VSAN ポリシーの変更

既存ロールの VSAN ポリシーを変更するには、次の手順を実行します。



Note

- NX-OS リリース 4.x 以降では、VSAN の適用は、非 show コマンドに対してのみ実行されます。show コマンドは除外されます。
- SAN-OS リリース 3.x 以前では、VSAN の適用は非 show コマンドに対して実行されますが、すべての show コマンドが適用されるわけではありません。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **role name sangroup**

switch(config-role)#

sangroup ロールのロール コンフィギュレーション サブモードを開始します。

ステップ 3 switch(config)# **vsan policy deny**

switch(config-role-vsan)#

このロールの VSAN ポリシーを **deny** に変更し、VSAN を選択的に許可できるサブモードを開始します。

ステップ 4 switch(config-role)# **no vsan policy deny**

(オプション) 設定されている VSAN ロール ポリシーを削除し、工場出荷時のデフォルト (**permit**) に戻します。

ステップ 5 switch(config-role-vsan)# **permit vsan 10-30**

このロールが、VSAN 10 ~ 30 に許可されたコマンドを実行できるようにします。

ステップ 6 switch(config-role-vsan)# **no permit vsan 15-20**

(オプション) このロールの権限を、VSAN 15 ~ 20 のコマンドの実行について除外します。したがって、このロールは、VSAN 10 ~ 14、および 21 ~ 30 でコマンドを実行できるようになります。

ロールの配信

ロールベース設定は、Cisco Fabric Services (CFS) インフラストラクチャを利用して効率的なデータベース管理を可能にし、ファブリック全体に対するシングルポイントでの設定を提供します。

次の設定が配信されます。

- ロール名と説明
- ロールに対するルールのリスト
- VSAN ポリシーと許可されている VSAN のリスト

このセクションは、次のトピックで構成されています。

ロール データベースの概要

ロールベース設定は 2 つのデータベースを利用して設定内容の受け取りと実装を行います。

- コンフィギュレーションデータベース：ファブリックで現在実行されているデータベースです。
- 保留中のデータベース：以降の設定変更は保留中のデータベースに保存されます。設定を修正した場合は、保留中のデータベースの変更内容をコンフィギュレーションデータベースにコミットするかまたは廃棄する必要があります。その間、ファブリックはロックされた状態になります。保留中のデータベースへの変更は、その変更をコミットするまでコンフィギュレーションデータベースに反映されません。



Note お客様に「syslog"%VSHD-4-VSHD_ROLE_DATABASE_OUT_OF_SYNC"」が発生するとすぐに、ロール コンフィギュレーション データベースがマージ時にスイッチ間で異なることが検出されます。ファブリック内のすべてのスイッチで、ロール コンフィギュレーション データベースを一致させることを推奨します。いずれかのスイッチで設定を編集し、目的のロール コンフィギュレーション データベースを取得してからコミットします。

ファブリックのロック

データベースを修正する最初のアクションで保留中のデータベースが作成され、ファブリック全体の機能がロックされます。ファブリックがロックされると、次のような状況になります。

- 他のユーザーがこの機能の設定に変更を加えることができなくなります。
- コンフィギュレーションデータベースの複製が、最初の変更とともに保留中のデータベースになります。

ロールベース設定変更のコミット

保留中のデータベースに行われた変更をコミットすると、その設定はそのファブリック内のすべてのスイッチにコミットされます。コミットが正常に行われると、設定の変更がファブリック全体に適用され、ロックが解除されます。コンフィギュレーションデータベースはこれ以降、コミットされた変更を保持し、保留中のデータベースは消去されます。

ロールベースの設定変更をコミットするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **role commit**

ロールベースの設定変更をコミットします。

ロールベース設定変更の廃棄

保留中のデータベースに加えられた変更を廃棄（終了）する場合、構成データベースは影響を受けず、ロックがリリースされます。

ロールベースの設定変更を廃棄するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **role abort**

ロールベースの設定変更を廃棄し、保留中のコンフィギュレーションデータベースをクリアします。

ロールベース設定の配布のイネーブル化

ロールベース設定の配布をイネーブルにするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **role distribute**

ロールベース設定の配信をイネーブルにします。

ステップ 3 switch(config)# **no role distribute**

(オプション) ロールベース設定の配信をディセーブル (デフォルト) にします。

セッションのクリア

ファブリック内の既存のロールセッションを強制的にクリアするには、開始されたセッションに参加中のスイッチから **clear role session** コマンドを発行します。



Caution このコマンドを発行すると、保留中のデータベース内のすべての変更が失われます。

```
switch# clear role session
```

データベース マージの注意事項

ファブリックのマージではスイッチ上のロールデータベースは変更されません。2つのファブリックをマージし、それらのファブリックが異なるロールデータベースを持つ場合は、ソフトウェアがアラートメッセージを發します。

- ファブリック全体のすべてのスイッチでロールデータベースが同一であることを確認してください。
- 必ず目的のデータベースになるように任意のスイッチのロールデータベースを編集してから、コミットしてください。これによりファブリック内のすべてのスイッチ上のロールデータベースの同期が保たれます。

ロールベース情報の表示

スイッチに設定されたルールを表示するには、**show role** コマンドを使用します。ルールはルール番号別、およびそれぞれのルールに基づいて表示されます。ロール名を指定しなかった場合はすべてのルールが表示されます。次の例を参照してください。

すべてのルールに関する情報の表示

```

switch# show role

Role: network-admin
Description: Predefined Network Admin group. This role cannot be modified.
Vsan policy: permit (default)
-----
Rule      Type      Command-type      Feature
-----
1         permit   clear             *
2         permit   config            *
3         permit   debug             *
4         permit   exec              *
5         permit   show              *
Role: network-operator
Description: Predefined Network Operator group. This role cannot be modified.
Vsan policy: permit (default)
-----
Rule      Type      Command-type      Feature
-----
1         permit   show              *(excluding show running-config, show startup-config)
2         permit   exec              copy licenses
3         permit   exec              dir
4         permit   exec              ssh
5         permit   exec              terminal
6         permit   config            username
Role: server-admin
Description: Predefined system role for server administrators. This role
cannot be modified.
Vsan policy: permit (default)
-----
Rule      Type      Command-type      Feature
-----
1         permit   show              *
2         permit   exec              install
Role: priv-15
Description: This is a system defined privilege role.
Vsan policy: permit (default)
-----
Rule      Type      Command-type      Feature
-----
1         permit   show              *
2         permit   config            *
3         permit   clear             *
4         permit   debug             *
5         permit   exec              *
Role: priv-14
Description: This is a system defined privilege role.
Vsan policy: permit (default)
Role: priv-13
Description: This is a system defined privilege role.
Vsan policy: permit (default)
Role: priv-12
Description: This is a system defined privilege role.
Vsan policy: permit (default)
Role: priv-11
Description: This is a system defined privilege role.
Vsan policy: permit (default)
Role: priv-10
Description: This is a system defined privilege role.
Vsan policy: permit (default)
Role: priv-9
Description: This is a system defined privilege role.
Vsan policy: permit (default)
Role: priv-8

```

配信がイネーブルの場合のロールの表示

```

Description: This is a system defined privilege role.
Vsan policy: permit (default)
Role: priv-7
Description: This is a system defined privilege role.
Vsan policy: permit (default)
Role: priv-6
Description: This is a system defined privilege role.
Vsan policy: permit (default)
Role: priv-5
Description: This is a system defined privilege role.
Vsan policy: permit (default)
Role: priv-4
Description: This is a system defined privilege role.
Vsan policy: permit (default)
Role: priv-3
Description: This is a system defined privilege role.
Vsan policy: permit (default)
Role: priv-2
Description: This is a system defined privilege role.
Vsan policy: permit (default)
Role: priv-1
Description: This is a system defined privilege role.
Vsan policy: permit (default)
Role: priv-0
Description: This is a system defined privilege role.
Vsan policy: permit (default)
-----
Rule      Type      Command-type  Feature
-----
1         permit   show          *
2         permit   exec          enable
3         permit   exec          ssh
4         permit   exec          ping
5         permit   exec          telnet
6         permit   exec          traceroute
Role: default-role
Description: This is a system defined role and applies to all users.
Vsan policy: permit (default)
-----
Rule      Type      Command-type  Feature
-----
1         permit   show          system
2         permit   show          snmp
3         permit   show          module
4         permit   show          hardware
5         permit   show          environment

```

配信がイネーブルの場合のロールの表示

コンフィギュレーションデータベースを表示するには、**show role** コマンドを使用します。

配信がロール設定に対してイネーブルかどうか、現在のファブリックステータス（ロックまたはロック解除）、および最後に実行された動作を表示するには、**show role status** コマンドを使用します。次の例を参照してください。

ロールステータス情報の表示

```

switch# show role status
Distribution: Enabled
Session State: Locked

```

```
Last operation (initiated from this switch): Distribution enable
Last operation status: Success
```

保留中のロール データベースを表示するには、**show role pending** コマンドを使用します。
 下記の例は、次の手順に従って **show role pending** コマンドを実行した出力を示しています。

1. **role name myrole** コマンドを使用して **myrole** というロールを作成します。
2. **rule 1 permit config feature fspf** コマンドを入力します。
3. **show role pending** コマンドを入力して出力を確認します。

保留中のロール データベース情報の表示

```
switch# show role pending

Role: network-admin
Description: Predefined Network Admin group. This role cannot be modified
Access to all the switch commands
Role: network-operator
Description: Predefined Network Operator group. This role cannot be modified
Access to Show commands and selected Exec commands
Role: svc-admin
Description: Predefined SVC Admin group. This role cannot be modified
Access to all SAN Volume Controller commands
Role: svc-operator
Description: Predefined SVC Operator group. This role cannot be modified
Access to selected SAN Volume Controller commands
Role: TechDocs
  vsan policy: permit (default)
Role: sangroup
Description: SAN management group
  vsan policy: deny
  Permitted vsans: 10-30
-----
Rule      Type      Command-type      Feature
-----
  1.  permit  config            *
  2.  deny    config            fspf
  3.  permit  debug             zone
  4.  permit  exec              fcping
Role: myrole
  vsan policy: permit (default)
-----
Rule      Type      Command-type      Feature
-----
  1.  permit  config            fspf
```

保留中のロール データベースとコンフィギュレーションのロール データベースの相違を表示するには、**show role pending-diff** コマンドを使用します。次の例を参照してください。

2つのデータベースの相違の表示

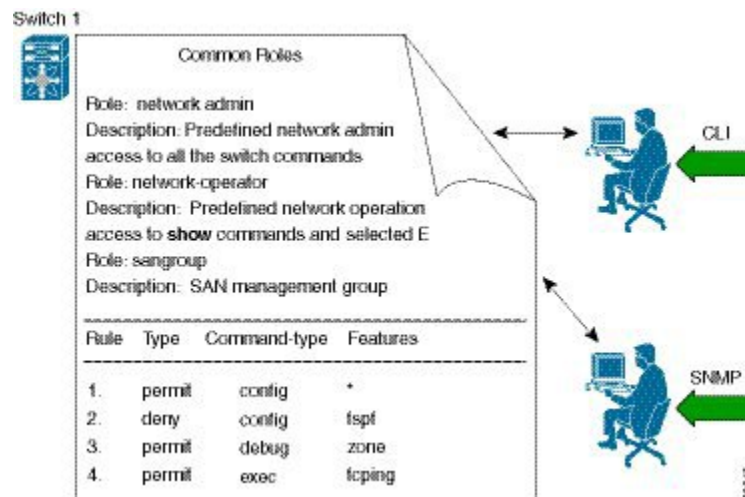
```
switch# show role pending-diff
+Role: myrole
+ vsan policy: permit (default)
+ -----
+ Rule      Type      Command-type      Feature
+ -----
+ 1.  permit  config            fspf
```

共通ロールの設定

CLIとSNMPは、Cisco MDS 9000シリーズのすべてのスイッチで共通のロールを使用します。SNMPを使用して作成したロールはCLIを使用して変更でき、その逆も可能です。

CLIユーザーとSNMPユーザーのユーザー、パスワード、ロールは、すべて同じです。CLIを通じて設定されたユーザーはSNMP（たとえば、Fabric ManagerやDevice Manager）を使用してスイッチにアクセスでき、その逆も可能です。

Figure 1: 共通ロール



ネットワーク管理者権限を持つカスタムロールユーザーは、他のユーザーのアカウントの変更が制限されています。ただし、管理者だけはすべてのユーザーアカウントを変更できます。

ユーザー権限を変更するには、次のタスクを実行します。

1. コンソール認証を使用してロールを変更します。

コンソール認証を 'local' に設定している場合は、ローカル管理者ユーザーでログオンし、ユーザーを変更します。

2. リモート認証を使用してロールを変更します。

リモート認証をオフにします。ローカル管理者権限でログオンし、ユーザーを変更します。リモート認証をオンにします。

3. LDAP/AAA を使用してロールを変更します。

LDAP/AAA でグループを作成し、このグループの名前をネットワーク管理者に変更します。必要なユーザーをこのグループに追加します。このグループのユーザーに完全なネットワーク管理者権限が付与されました。

SNMPの各ロールは、CLIを通じて作成または変更されたロールと同じです（[ロールベースの認証](#), on page 18 を参照）。

各ロールは、必要に応じて1つ以上のVSANに制限できます。

SNMPまたはCLIを使用して、新しいロールの作成、または既存のロールの変更を実行できます。

- SNMP : CISCO-COMMON-ROLES-MIB を使用してロールを設定または変更します。詳細については、『Cisco MDS 9000 Family MIB Quick Reference』を参照してください。
- CLI : **role name** コマンドを使用します。

CLIオペレーションからSNMPへのマッピング

SNMPでは、GET、SET、およびNOTIFYの3つの操作だけを行うことができます。CLIでは、DEBUG、SHOW、CONFIG、CLEAR、およびEXECの5つの操作を行うことができます。



Note NOTIFYには、CLIのsyslogメッセージのような制限はありません。

次の表は、CLIオペレーションがSNMPオペレーションにどのようにマッピングされるかを示します。

Table 1: CLIオペレーションからSNMPオペレーションへのマッピング

CLIオペレーション	SNMPオペレーション
DEBUG	Ignored
SHOW	GET
CONFIG	SET
CLEAR	SET
EXEC	SET

次に、my_role という名前のロールのCLIオペレーションをSNMPオペレーションへマッピングする特権およびルールの例を示します。

CLI操作からSNMP操作へのマッピングの表示

```
switch# show role name my_role
Role:my_role
vsan policy:permit (default)
-----
Rule      Type      Command-type      Feature
-----
1.    permit    clear              *
2.    deny      clear              ntp
3.    permit    config             *
4.    deny      config             ntp
5.    permit    debug              *
6.    deny      debug              ntp
7.    permit    show               *
```

```

8. deny show ntp
9. permit exec *
```



Note ルール4では、CONFIGはNTPでは拒否されますが、ルール9によって、NTP MIB オブジェクトに対するSETは許可されます。これは、EXECもSNMP SET操作にマッピングされているためです。

デフォルト設定

次の表に、任意のスイッチにおけるすべてのスイッチセキュリティ機能のデフォルト設定を示します。

Table 2: スイッチセキュリティのデフォルト設定

パラメータ	デフォルト
Cisco MDS スイッチでのロール	ネットワーク オペレータ (network-operator)
AAA 設定サービス	ローカル
認証ポート	1821
アカウントिंग ポート	1813
事前共有キーの送受信	クリア テキスト
RADIUS サーバー タイムアウト	1 秒
RADIUS サーバー再試行	1 回
TACACS+	ディセーブル
TACACS+ サーバー	未設定
TACACS+ サーバーのタイムアウト	5 秒
AAA サーバーへの配信	ディセーブル
ロールに対する VSAN ポリシー	Permit
ユーザー アカウント	有効期限なし (設定されていない場合)
パスワード	なし
パスワード強度	イネーブル
アカウントिंग ログ サイズ	250 KB

パラメータ	デフォルト
SSH サービス	イネーブル
Telnet サービス	ディセーブル



第 5 章

外部 AAA サーバーでのセキュリティ機能の設定

認証、許可、アカウントिंग（AAA）機能は、スイッチ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します。Cisco MDS 9000 ファミリのすべてのスイッチで、Remote Access Dial-In User Service（RADIUS）プロトコルまたは Terminal Access Controller Access Control device Plus（TACACS+）プロトコルを使用することで、リモート AAA サーバーを使用するソリューションが実現されます。

指定されたユーザー ID およびパスワードの組み合わせに基づいて、スイッチはローカル認証やローカルデータベースによる認可、またはリモート認証や AAA サーバーによる認可を実行します。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。この秘密キーはすべての AAA サーバー、または特定の AAA サーバーに設定できます。このセキュリティ機能により、AAA サーバーを中央で管理できます。

この章は、次の項で構成されています。

- [スイッチ管理のセキュリティ, on page 38](#)
- [スイッチの AAA 機能, on page 39](#)
- [ログインパラメータの設定, on page 49](#)
- [AAA サーバーのモニタリングパラメータをグローバルに設定, on page 51](#)
- [LDAP の設定, on page 52](#)
- [RADIUS サーバー モニタリングパラメータの設定, on page 68](#)
- [ワンタイムパスワードサポート, on page 81](#)
- [管理者パスワードの回復, on page 81](#)
- [TACACS+ サーバー モニタリングパラメータの設定, on page 84](#)
- [サーバーグループの設定, on page 97](#)
- [AAA サーバーへの配信, on page 101](#)
- [CHAP 認証, on page 107](#)
- [MSCHAP による認証, on page 107](#)
- [ローカル AAA サービス, on page 109](#)
- [アカウントングサービスの設定, on page 111](#)
- [Cisco Access Control Servers の設定, on page 113](#)

- [デフォルト設定, on page 116](#)

スイッチ管理のセキュリティ

Cisco MDS 9000 ファミリー スイッチの管理セキュリティは、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) を含む、すべての管理アクセス方式にセキュリティを提供します。

このセクションは、次のトピックで構成されています。

CLI セキュリティ オプション

CLI にはコンソール (シリアル接続) 、Telnet、またはセキュア シェル (SSH) を使用してアクセスできます。

- リモート セキュリティ制御
 - RADIUS を利用
[RADIUS サーバー モニタリング パラメータの設定, on page 68](#)を参照してください。
 - TACACS+ を利用
[TACACS+ サーバー モニタリング パラメータの設定, on page 84](#)を参照してください。
- ローカル セキュリティ制御
[ローカル AAA サービス, on page 109](#)を参照してください。

これらのセキュリティ機能は、次のシナリオにも設定できます。

- Small Computer Systems Interface over IP (iSCSI) 認証
『*Cisco MDS 9000 Family NX-OS IP Services Configuration Guide*』および『*Cisco Fabric Manager IP Services Configuration Guide*』を参照してください。
- Fibre Channel Security Protocol (FC-SP) 認証
「[ファブリック認証の概要](#)」を参照してください。

SNMP セキュリティ オプション

SNMP エージェントは、SNMPv1、SNMPv2c、およびSNMPv3のセキュリティ機能をサポートしています。SNMP を使用するすべてのアプリケーション (Cisco MDS 9000 Fabric Manager など) に、標準 SNMP セキュリティ機能が適用されます。

SNMP セキュリティ オプションは Fabric Manager と Device Manager にも適用できます。

SNMP セキュリティ オプションの詳細については、『*Cisco MDS 9000 NX-OS Family System Management Configuration Guide*』を参照してください。

Fabric Manager と Device Manager の詳細については、『*Cisco Fabric Manager Fundamentals Configuration Guide*』を参照してください。

スイッチの AAA 機能

CLI または Fabric Manager あるいは SNMP アプリケーションを使用して、すべての Cisco MDS 9000 ファミリ スイッチに AAA スイッチ機能を設定できます。

このセクションは、次のトピックで構成されています。

認証

認証は、スイッチにアクセスするユーザーまたはデバイスの識別情報を検証するプロセスです。この ID 確認は、スイッチにアクセスしようとするエンティティが提出するユーザー ID およびパスワードの組み合わせに基づいて行われます。Cisco MDS 9000 ファミリ スイッチでは、ローカル認証（ローカルルックアップデータベースを使用）またはリモート認証（1 台または複数の RADIUS サーバーまたは TACACS+ サーバーを使用）を実行できます。



Note Fabric Manager は末尾が空白スペースの AAA パスワードをサポートしません（例「passwordA」）。

認証

すべての Cisco MDS スイッチに次の認可ロールがあります。

- ネットワーク オペレータ（`network-operator`）：設定を表示する権限だけがあります。オペレータは設定内容を変更できません。
- ネットワーク管理者（`network-admin`）：すべてのコマンドを実行し、設定内容を変更する権限があります。管理者は最大 64 の追加ロールを作成し、カスタマイズできます。
- デフォルトロール：GUI を利用する権限があります（Fabric Manager および Device Manager）。このアクセス権は、GUI にアクセスすることを目的として、すべてのユーザーに自動的に与えられます。

これらのロールは変更または削除ができません。追加のロールを作成することで、次のオプションを設定できます。

- ユーザー ロールをローカルに割り当てるか、またはリモート AAA サーバーを使用して、ロールベースの認可を設定します。
- ロール情報を格納するように、リモート AAA サーバーのユーザー プロファイルを設定します。このロール情報は、リモート AAA サーバーを通じてユーザーを認証したときに、自動的にダウンロードされ、使用されます。



Note ユーザーが新しく作成されたロールのうちの 1 つだけに属している場合、このロールが削除されると、ユーザーにはただちにデフォルトの `network-operator` ロールが設定されます。

アカウンティング

アカウンティング機能はスイッチへのアクセスに使用されるすべての管理設定のログを追跡し、管理します。この情報を利用して、トラブルシューティングや監査に使用するレポートを生成できます。アカウンティングログはローカルで保存したり、リモート AAA サーバーに送信したりできます。

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対するユーザーパスワードリストをより簡単に管理できます。
- AAA サーバーはすでに企業全体に配置済みであり、簡単に導入できます。
- 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。
- ファブリック内の各スイッチに対するユーザーロール設定をより簡単に管理できます。

リモート認証に関する注意事項

リモート AAA サーバーを使用する場合は、次の注意事項に従ってください。

- 最低 1 つの AAA サーバーが IP で到達可能になっている必要があります。
- すべての AAA サーバーが到達不能である場合のポリシーとして、適切なローカル AAA ポリシーを必ず設定してください。
- オーバーレイ Ethernet LAN がスイッチに接続している場合、AAA サーバーは容易に到達可能です（『Cisco Fabric Manager IP Services Configuration Guide』および『Cisco MDS 9000 Family NX-OS Configuration Guide』を参照）。この方法を推奨します。
- スwitchに接続された SAN ネットワーク内のゲートウェイスイッチを 1 つまたは複数、AAA サーバーに到達するイーサネット LAN に接続する必要があります。

サーバーグループ

認証、許可、アカウンティングのためのリモート AAA サーバーは、サーバーグループを使用して指定できます。サーバーグループは、同じ AAA プロトコルを実装するリモート AAA サーバーセットです。サーバグループの目的は、リモート AAA サーバが応答できなくなったときにフェールオーバーサーバを提供することです。グループ内の最初のリモートサーバが応答しなかった場合、いずれかのサーバ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

で試行が行われます。サーバグループ内のすべての AAA サーバが応答しなかった場合、そのサーバグループオプション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、複数のサーバグループを指定できます。Cisco MDS 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 MDS 9000 ファミリー スイッチ製品内の AAA 設定は、サービス ベースです。次のサービスごとに、異なる AAA 設定を作成できます。

- Telnet または SSH ログイン (Fabric Manager および Device Manager ログイン)
- コンソール ログイン
- iSCSI 認証 (『Cisco Fabric Manager IP Services Configuration Guide』 および 『Cisco MDS 9000 Family NX-OS IP Services Configuration Guide』 を参照)
- FC-SP 認証 (「[ファブリック認証の概要](#)」を参照)
- アカウンティング

一般に、AAA 設定の任意のサービスに対して指定できるオプションは、サーバー グループ、ローカル、および none の 3 つです。各オプションは指定した順序で試行されます。すべてのオプションが失敗した場合、ローカルが試行されます。



Caution

Cisco MDS NX-OS では、ユーザ名がアルファベットで始まる限り、リモートで作成するか (TACACS+ または RADIUS を使用) ローカルで作成するかに関係なく、英数字または特定の特殊文字 (+ (プラス)、= (等号)、_ (下線)、- (ハイフン)、\ (バックスラッシュ)、および . (ピリオド)) を使って作成したユーザ名がサポートされます。ローカル ユーザー名をすべて数字で作成したり、特殊文字 (上記の特殊文字を除く) を使用して作成したりすることはできません。数字だけのユーザー名やサポートされていない特殊文字によるユーザー名が AAA サーバーに存在し、ログイン時に入力されると、そのユーザーはアクセスを拒否されます。



Note

オプションの 1 つとしてローカルが指定されていない場合でも、認証用に設定されたすべての AAA サーバーに到達不能であるかどうかはデフォルトで試行されます。ユーザーは、このフォールバックを柔軟にディセーブルにすることができます。

RADIUS がタイムアウトする際は、フォールバック設定に応じてローカルログインが試行されます。このローカルログインに成功するには、同一のパスワードを持つそのユーザーのローカルアカウントが存在し、かつ RADIUS のタイムアウトと再試行は 40 秒未満でなければなりません。そのユーザーが認証されるのは、ローカルの認証設定にそのユーザー名とパスワードが存在する場合です。

次の表に、AAA サービス設定オプションごとに CLI（コマンドライン インターフェイス）の関連コマンドを示します。

Table 3: 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（Cisco Fabric Manager および Device Manager ログイン）	aaa authentication login default
コンソール ログイン	aaa authentication login console
Small Computer Systems Interface over IP（iSCSI）認証	aaa authentication iscsi default
FC-SP 認証	aaa authentication dhchap default
アカウントティング	aaa accounting default



Note コンソールで認証方法を何も設定しない場合は、コンソールと Telnet または SSH の両方にデフォルトの認証方法が適用されます。

エラー対応ステータス

ログイン時にリモート AAA サーバーが応答しない場合、そのログインは、ローカルユーザーデータベースにロールオーバーして処理されます。この場合は、**error-enabled** 機能をイネーブにした場合、次のメッセージが画面に表示されます。

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

このメッセージの表示をイネーブにするには、**aaa authentication login error-enable** コマンドを使用します。

このメッセージの表示をディセーブにするには、**no aaa authentication login error-enable** コマンドを使用します。

現在の表示ステータスを表示するには、**show aaa authentication login error-enable** コマンドを使用します（次の例を参照）。

AAA 認証ログイン情報の表示

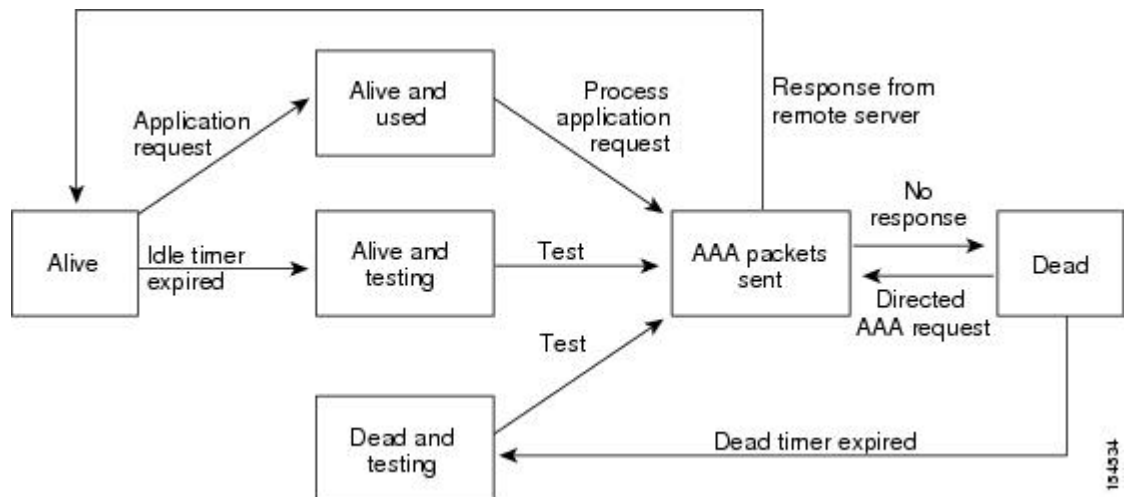
```
switch# show aaa authentication login error-enable enabled
```

AAA サーバーのモニタリング

応答の途絶えた AAA サーバーは AAA 要求の処理に遅延をもたらします。AAA 要求の処理時間を節約するため、MDS スイッチは定期的に AAA サーバーをモニターして AAA サーバーが

応答している（または稼働している）かどうかを確認できます。MDS スイッチは、応答のない AAA サーバーを停止中としてマーク付けします。また、停止中のいずれの AAA サーバーにも AAA 要求を送りません。MDS スイッチは定期的に停止中の AAA サーバーを監視し、応答するようになったら稼働中と認識します。このモニタリングプロセスでは、実際の AAA 要求を送出する前にその AAA サーバーが稼働中であることを確認します。AAA サーバーのステータスが停止中または稼働中に変わると常に SNMP トラップが生成され、MDS スイッチはパフォーマンスに影響が出る前に、管理者に対して障害が発生していることを警告します。AAA サーバーのステータスについては、[Figure 2: AAA サーバーのステータス](#), on page 43 を参照してください。

Figure 2: AAA サーバーのステータス



Note 稼働中のサーバーと停止中のサーバーのモニタリング間隔はそれぞれ別で、ユーザーが設定できます。AAA サーバーのモニタリングはテスト用認証要求を AAA サーバーに送信することで行われます。

テスト パケットで使用されるユーザー名とパスワードは設定が可能です。

[RADIUS サーバー モニタリング パラメータの設定](#), on page 68と[RADIUS サーバーの詳細の表示](#), on page 80の項を参照してください。

認証と許可のプロセス

認証は、スイッチを管理する人物の ID を確認するプロセスです。この ID 確認は、スイッチを管理しようとする人物が入力したユーザー ID およびパスワードの組み合わせに基づいて行われます。Cisco MDS 9000 ファミリー スイッチでは、ローカル認証（ルックアップデータベースを使用）またはリモート認証（1 台または複数の RADIUS サーバーまたは TACACS+ サーバーを使用）を実行できます。

許可は、アクセスコントロールを提供します。これは、ユーザー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プロセスです。ユーザーは、ユーザー ID とパスワード

の組み合わせに基づいて認証および認可され、割り当てられているロールに従ってネットワークにアクセスします。スイッチで TACACS+ プロトコルを使用していれば、ユーザーによる不正なアクセスを防ぐことができるパラメータを設定できます。

AAA の許可は、ユーザー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プロセスです。Cisco NX-OS ソフトウェアでは、AAA サーバからダウンロードされる属性を使用して権限付与が行われます。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。

認証と認可の手順は次のとおりです。

Procedure

-
- ステップ 1** Cisco MDS 9000 ファミリ内の必要なスイッチへのログインには、Telnet、SSH、Fabric Manager/Device Manager、またはコンソールのログイン オプションを使用します。
- ステップ 2** サーバー グループ認証方式を使用するサーバー グループを設定した場合は、グループ内の最初の AAA サーバーに認証要求が送信されます。
- その AAA サーバーが応答に失敗すると次の AAA サーバーに送信され、リモートサーバーが認証要求に応答するまで繰り返されます。
 - サーバー グループ内のすべての AAA サーバーが応答に失敗した場合は、次のサーバー グループのサーバーに送信が行われます。
 - 設定されているすべての方式で応答が得られなかった場合、デフォルトでローカルデータベースが認証に使用されます。次の項で、このフォールバックをディセーブルにする方法について説明します。
- ステップ 3** リモートの AAA サーバーにより認証に成功すると、場合に応じて次の処理が実行されます。
- AAA サーバーのプロトコルが RADIUS の場合は、認証応答に伴って **cisco-av-pair** 属性で指定されたユーザー ロールが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。
 - リモート AAA サーバーからのユーザー ロールの入手に失敗した場合、**show aaa user default-role** コマンドがイネーブルであれば、ユーザーには **network-operator** ロールが割り当てられます。このコマンドがディセーブルの場合には、アクセスが拒否されます。
- ステップ 4** ユーザー名とパスワードがローカルで認証に成功した場合は、ログインが許可され、ローカルデータベースに設定されているロールが割り当てられます。
-

AAA 認証のデフォルトユーザ ロールのイネーブル化

ユーザ ロールを持たないリモートユーザに、デフォルトのユーザ ロールを使用して、リモート認証による Cisco NX-OS デバイスへのログインを許可できます。AAA のデフォルトのユーザ ロール機能をディセーブルにすると、（デバイスの中でローカルに一致したユーザ ロールを持たない）リモートユーザはデバイスにログインできなくなります。

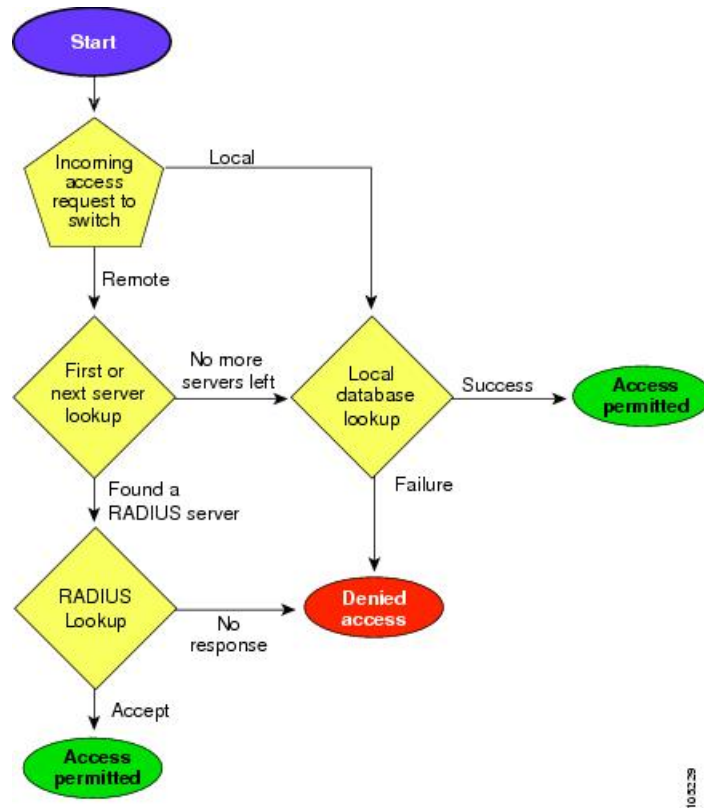
Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	コンフィギュレーションモードに入ります。
ステップ 2	aaa user default-role Example: switch(config)# aaa user default-role	AAA 認証のためのデフォルト ユーザ ロール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。 デフォルト ユーザ ロールの機能をディセーブルにするには、このコマンドの no 形式を使用します。
ステップ 3	exit Example: switch(config)# exit switch#	設定モードを終了します。
ステップ 4	(Optional) show aaa user default-role Example: switch# show aaa user default-role	AAA デフォルトユーザ ロールの設定を表示します。

TACACS+ サーバーでのロールベース認証の設定

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。

図 3: スイッチの認可と認証のフロー



(注) 残りのサーバーグループがないということは、どのサーバーグループのどのサーバーからも応答がないということを意味します。残りのサーバーがないということは、このサーバーグループのどのサーバーからも応答がないということを意味します。

TACACS+ サーバーでロールベースの認証を設定するには、次の手順に従います。

手順

ステップ 1 switch# configure terminal

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# aaa authorization

認証方式の設定を有効にします。

ステップ 3 switch(config)# aaa authorization config-commands

config モード Layer2 および Layer3 のすべてのコマンドの認証を有効にします。

ステップ 4 switch(config)# aaa authorization config-commands default group tac1

指定した TACACS+ サーバー グループの認証を有効にします。

ステップ 5 switch(config)# **aaa authorization commands**

すべての EXEC モード コマンドへの AAA 許可を有効にします。

ステップ 6 switch(config)# **aaa authorization commands default group tac1**

指定した TACACS+ サーバー グループの認証を有効にします。

ステップ 7 switch(config)# **aaa authorization commands default group local**

デフォルトの TACACS+ サーバー グループの認証を有効にします。認証は、ローカルユーザー データベースに基づいています。

ステップ 8 switch(config)# **no aaa authorization command default group tac1**

認証されたユーザーに対し指定した機能の認証を削除します。

- (注)
- 承認の設定は、TACACS+サーバーを使用して実施する認証にのみ提供されます。
 - AAA 許可方式の「none」オプションは廃止されました。4.x イメージからアップグレードし、「none」を許可方式の1つとして設定した場合、ローカルに置き換えられます。機能は変わりません。
 - コマンド許可では、デフォルト ロールを含むユーザーのロールベース許可コントロール (RBAC) がディセーブルになります。

AAA 許可情報の詳細の表示

AAA 認証に関する情報と、リモート認証に割り当てられたデフォルト ユーザー ロールを表示するには、show コマンドを使用できます。(次の例を参照)

```
switch# show aaa authorization all
AAA command authorization:
default authorization for config-commands: local
default authorization for commands: local
cts: group radl
```

リモート認証のデフォルト ユーザー ロールの表示

```
switch# show aaa user default-role
enabled
```

認証のフォールバック メカニズムの設定

リモート認証が設定され、すべての AAA サーバーに到達不能 (認証エラー) である場合は、ローカルデータベースへのフォールバックをイネーブルまたはディセーブルにできます。認証エラーの場合、フォールバックはデフォルトでローカルに設定されています。コンソールログインと ssh/telnet ログインの両方に対して、このフォールバックをディセーブルにすることもできます。このフォールバックを無効にすると、認証のセキュリティが強化されます。

CLI 構文と動作は次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **show run aaa all**

```
aaa authentication login default fallback error local
aaa authentication login console fallback error local
```

デフォルトのフォールバックの動作が表示されます。

ステップ 3 switch(config)# **no aaa authentication login default fallback error local**

```
WARNING!!! Disabling fallback can lock your switch.
```

認証用のローカルデータベースへのフォールバックをディセーブルにします。

Note コンソールへフォールバックをディセーブルにするには、このコマンドの **default** を **console** で置き換えます。



Caution デフォルトとコンソールの両方に対してフォールバックがディセーブルである場合は、リモート認証がイネーブルになり、サーバーに到達不能であるため、スイッチはロックされます。

認可プロファイルの確認

各種コマンドの認可プロファイルを確認できます。イネーブルの場合、すべてのコマンドは、検証用に Access Control Server (ACS) に転送されます。検証が完了すると、検証の詳細が表示されます。

```
switch# terminal verify-only username sikander
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# feature telnet
% Success
switch(config)# feature ssh
% Success
switch(config)# end
% Success
switch# exit
```



Note このコマンドは、コマンドを確認するだけで設定をイネーブルにしません。

認証のテスト

コマンドの認証設定をテストできます。

コマンドの認証をテストするには、`test aaa authorization command-type` コマンドを使用します。

```
switch(config)# test aaa authorization command-type commands user ul command "feature dhcp"
% Success
```

ログインパラメータの設定

Cisco MDS 9000 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イネーブルにする `login block-for` コマンドを入力する必要があります。`login block-for` コマンドをイネーブルにすると、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。

ログインパラメータを設定するには、次の手順を実行します。

Procedure

ステップ 1 コンフィギュレーションモードを開始します。

```
switch# configure terminal
```

ステップ 2 Cisco MDS 9000 デバイスで DoS の検出に役立つログインパラメータを設定します。

```
switch(config)# login block-for 100 attempts 2 within 100
```

Note このコマンドは、その他のログインコマンドの前に発行する必要があります。

ステップ 3 (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。

```
switch(config)# login quiet-mode access-class myacl
```

ステップ 4 特権 EXEC モードに戻ります。

```
switch(config)# exit
```

ステップ 5 ログインパラメータを表示します。

```
switch# show login
```

ステップ 6 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。

```
switch# show login failures
```

ログインパラメータの設定

ログインパラメータなしの確認

ログインパラメータの確認

失敗したログイン試行に関する情報の表示

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
```

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 15 login failures occur in 100 seconds or less, logins will be disabled for
 100 seconds.
Switch presently in Normal-Mode.
Current Watch Window remaining time 49 seconds.
Present login failure count 0.
```

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ることを確認します。

```
switch# show login
```

```
Quiet-Mode access list myacl is applied.
Switch is enabled to watch for login Attacks.
If more than 15 login failures occur in 100 seconds or less, logins will be disabled for
 100 seconds.

Switch presently in Normal-Mode.
Current Watch Window remaining time 49 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   TimeStamp           Line   Source           Appname
admin     Wed Jun 10 04:56:16 2015   pts/0   10.10.10.1       login
admin     Wed Jun 10 04:56:19 2015   pts/0   10.10.10.2       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.***
```

AAA サーバーのモニタリングパラメータをグローバルに設定

AAA サーバー モニタリング パラメータは、すべてのサーバーにグローバルに設定、または特定のサーバーに対して個別に設定できます。この項では、グローバルコンフィギュレーションの設定方法について説明します。グローバルコンフィギュレーションは、個別のモニタリングパラメータが定義されていないすべてのサーバーに適用されます。各サーバーで、特定のサーバーに対して定義された個々のテストパラメータは、グローバル設定よりも常に優先されません。

RADIUS サーバーのグローバル モニタリング パラメータを設定するには、次のコマンドを使用します。

Procedure

ステップ 1 switch# **configure terminal**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **radius-server deadtime 10**

RADIUS サーバーのグローバル デッド タイムを 10 分間に設定します。

許容範囲は 0 ~ 1440 分です。

ステップ 3 switch(config)# **radius-server timeout 20f**

RADIUS サーバーのグローバル タイムアウトを 20 分間に設定します。

許容範囲は 1 ~ 60 分です。

ステップ 4 switch(config)# **radius-server retransmit 2**

RADIUS サーバーのグローバル再送信回数を 2 に設定します。

許容範囲は 0 ~ 5 です。

ステップ 5 switch(config)# **radius-server test username username password password idle-time time**

RADIUS サーバーのテスト パラメータをグローバルに設定します。

ステップ 6 switch(config)# **radius-server test username username password password no**

RADIUS サーバーのグローバルなテスト パラメータを無効にします。

Example



Note TACACS サーバーのグローバルテストパラメータの設定の場合に相当するコマンドを取得するには、上記の手順の `radius` を `tacacs` と置き換えます。

グローバル AAA サーバー モニタリング パラメータは次の動作を確認します。

- 新しい AAA サーバーを設定すると、その AAA サーバーは、グローバルテストパラメータを使用して監視されます（定義されている場合）。
- グローバルテストパラメータが追加または変更されると、テストパラメータが設定されていないすべての AAA サーバーは、新しいグローバルテストパラメータを使用して監視されるようになります。
- サーバーのサーバーテストパラメータを削除した場合、またはアイドル時間を 0（デフォルト値）に設定した場合、そのサーバーは、グローバルテストパラメータを使用して監視されるようになります（定義されている場合）。
- グローバルテストパラメータを削除したり、グローバルアイドル時間を 0 に設定したりしても、サーバーテストパラメータが存在するサーバーは影響を受けません。ただし、これまではグローバルパラメータを使用して監視されていた他のすべてのサーバーのモニタリングが停止します。
- ユーザー指定のサーバーテストパラメータによってサーバーのモニタリングが失敗した場合は、グローバルテストパラメータにフォールバックしません。

LDAP の設定

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ー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 つのアクセスコントロールサーバー (LDAP デーモン) が認証と許可の各サービス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ーまたはネットワークで使用できる他のサービスを使用できます。

LDAP クライアント/サーバープロトコルでは、トランスポート要件を満たすために、TCP (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。



Note 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。

このセクションは、次のトピックで構成されています。

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。



Note 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。

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
- Cisco MDS NX-OS リリース 8.1 (1) 以降から、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 1.0 と 1.2 をサポートします。

- DNSSEC による安全な DNS 探索はサポートされていません。
- ローカルの Cisco NX-OS デバイス上に設定されているユーザー アカウントが、AAA サーバー上のリモートユーザーアカウントと同じ名前の場合、Cisco NX-OS ソフトウェアは、AAA サーバー上に設定されているユーザー ロールではなく、ローカルユーザーアカウントのユーザー ロールをリモートユーザーに適用します。
- Cisco MDS スイッチは、次のすべての条件を満たし、LDAP がリモート認証プロトコルを使用している場合、ローカル ロールをリモートユーザーに割り当てます。
 - LDAP サーバーのリモートユーザー名は、Cisco MDS スイッチのローカルユーザーと同じ名前です。（たとえば、「test」がADサーバーでのユーザー名の場合は、Cisco MDS スイッチでも同じユーザー名が作成されます）
 - LDAP サーバーは、Cisco MDS スイッチで AAA 認証として設定されます。
 - ローカルユーザーとリモートユーザーに割り当てられるロールは異なります。

次の例では、LDAP サーバーのユーザー名が "test" で、AD グループ "testgroup" のメンバーである場合について検討します。Cisco MDS スイッチは、名前が "testgroup" に設定されたロールを使用し、このロールには特定の許可ロールが割り当てられています。このロールは Cisco MDS スイッチで作成され、LDAP を使用してスイッチにログインするリモートユーザー用です。また、Cisco MDS スイッチにはローカルユーザー名 "test" も使用し、ロールとして "network-admin" が割り当てられています。Cisco MDS スイッチは AAA 認証用に設定され、認証プロトコルとして LDAP を使用します。この場合、ユーザーがユーザー名 "test" を使用して Cisco MDS スイッチにログインすると、スイッチは LDAP 認証を使用するユーザーを認証します（AD サーバーで作成された "test" ユーザーのパスワードを使用します）。ただし、ロールは、リモートで認証されたユーザーに割り当てられる「testgroup」ロールではなく、ローカルユーザー「test」に割り当てられる「network-admin」が割り当てられます。

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 のイネーブル化

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。

LDAP をイネーブルにするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

```
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 switch(config)# **feature ldap**

LDAP をイネーブルにします。

ステップ 3 switch(config)# **exit**

```
switch#
```

設定モードを終了します。

ステップ 4 switch# **copy running-config startup-config**

(任意) 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。

リモート LDAP サーバ プロファイルを構成

リモートの LDAP サーバにアクセスするには、Cisco NX-OS デバイス上で最初にプロファイル をサーバ IP アドレスまたはホスト名と一緒に作成します。サーバのプロファイル内の同じパラメーターによって上書きされない限り、グローバル LDAP サーバ パラメーターが使用されます。

構成可能なパラメーターは、SSL トランスポートの使用、サーバ上のターゲットポート番号、要求のタイムアウト期間、ルート識別名 (バインドユーザー) とパスワード、および検索参照です。

最大 64 の LDAP サーバ プロファイルがサポートされます。



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。

LDAP サーバを構成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

```
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 switch(config)# **ldap-server host 10.10.2.2**

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。

ステップ 3 switch(config)# **exit**

switch#

設定モードを終了します。

ステップ 4 switch# **copy running-config startup-config**

(任意) 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。

LDAP サーバに RootDN を設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

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 switch(config)# **ldap-server host 10.10.1.1 rootDN cn=manager,dc=acme,dc=com password Ur2Gd2BH timeout 60**

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。

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 switch(config)# **exit**

switch#

設定モードを終了します。

ステップ 4 switch# **show ldap-server**

(任意) LDAP サーバの設定を表示します。

ステップ 5 switch# **copy running-config startup-config**

(任意) 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。

Cisco MDS NX-OS リリース 6.2(1) 以降では、Cisco MDS 9000 シリーズスイッチがグループベースのユーザーロールをサポートします。LDAP サーバで、LDAP ユーザーが、スイッチで作成されたロール名（カスタマイズされたロール）または組み込みのロール名（ネットワーク管理者または属性管理者）と同じグループに属していることを確認します。

**Note**

- ユーザーはスイッチで使用可能な 1 つのグループだけに属することができます。
- ユーザーは複数のグループに属することができますが、スイッチロールに含めることができるのは 1 つのグループのみです。
- グループ名にスペースを含めることはできません。

LDAP サーバグループを設定するには、次の手順を実行します。

Procedure**ステップ 1** switch# **configure terminal**

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 switch(config)# **aaa group server ldap LDAPServer1**

switch(config-ldap)#

LDAP サーバグループを作成し、そのグループの LDAP サーバグループコンフィギュレーションモードを開始します。

ステップ 3 switch(config-ldap)# **server 10.10.2.2**

LDAP サーバを、LDAP サーバグループのメンバとして設定します。

指定した LDAP サーバーが見つからない場合は、`ldap-server host` コマンドを使用してサーバーを設定し、このコマンドをもう一度実行します。

ステップ 4 `switch(config-ldap)# authentication compare password-attribute TyuL&r`

(任意) 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。

ステップ 5 `switch(config-ldap)# enable user-server-group`

(任意) グループ検証をイネーブルにします。LDAP サーバー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ー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 `switch(config-ldap)# enable Cert-DN-match`

(任意) ユーザープロファイルでユーザー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ーがログインできるようにします。

ステップ 7 `switch(config)# exit`

`switch#`

設定モードを終了します。

ステップ 8 `switch# show ldap-server groups`

(任意) LDAP サーバー グループの設定を表示します。

ステップ 9 `switch# show run ldap`

(任意) LDAP の設定を表示します。

ステップ 10 `switch# copy running-config startup-config`

(任意) 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 LDAP タイムアウト間隔の設定

Cisco NX-OS LDAP クライアントが、タイムアウト エラーを宣言する前に LDAP サーバの応答を待機する最大時間を設定できます。LDAP サーバグループに他の LDAP サーバが存在する場合、タイムアウト後に次のサーバが試行されます。他に LDAP サーバがない場合、リクエストは機能不全になります。デフォルトでは、Cisco NX-OS LDAP クライアントは、各 LDAP サーバが応答するために 5 秒のグローバルタイムアウト期間を使用します。グローバルタイムアウト値は、各 LDAP サーバプロファイルで上書きできます。

グローバルな LDAP タイムアウト間隔を設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

```
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 switch(config)# **ldap-server timeout 10**

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 switch(config)# **exit**

```
switch#
```

設定モードを終了します。

ステップ 4 switch# **show ldap-server**

(任意) LDAP サーバーの設定を表示します。

ステップ 5 switch# **copy running-config startup-config**

(任意) 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 サーバーの接続タイムアウトの構成

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。

LDAP サーバーに接続タイムアウト期間を設定するには、次の手順を実行します。

手順

ステップ 1 switch# **configure terminal**

```
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 switch(config)# **ldap-server host 10.10.2.2 timeout 3**

サーバのタイムアウト間隔を指定します。有効な範囲は 1 ~ 60 秒です。

ステップ 3 switch(config)# **exit**

```
switch#
```

設定モードを終了します。

ステップ 4 switch# **show ldap-server**

(任意) LDAP サーバーの設定を表示します。

ステップ 5 switch# **copy running-config startup-config**

(任意) 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 LDAP サーバー ポートの設定

クライアントが TCP 接続を開始するグローバル LDAP サーバー宛て先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。

グローバルな LDAP サーバー ポートを設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

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 switch(config)# **ldap-server port 789**

サーバーへの LDAP メッセージに使用するグローバル 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。

ステップ 3 switch(config)# **exit**

switch#

設定モードを終了します。

ステップ 4 switch# **show ldap-server**

(任意) LDAP サーバーの設定を表示します。

ステップ 5 switch# **copy running-config startup-config**

(任意) 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 サーバーの宛て先ポートを構成

特定の LDAP サーバに指定した宛て先ポートは、すべての LDAP サーバで使用されるグローバルな宛て先ポートを上書きします。

接続先 TCP ポートを設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

```
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 switch(config)# **ldap-server host 10.10.2.2 port 200**

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。

ステップ 3 switch(config)# **exit**

```
switch#
```

設定モードを終了します。

ステップ 4 switch# **show ldap-server**

(任意) LDAP サーバーの設定を表示します。

ステップ 5 switch# **copy running-config startup-config**

(任意) 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 サーバの SSL トランスポートの構成

LDAP クライアントとサーバ間のトランスポートとして Secure Sockets Layer (SSL) を使用すると、ユーザーパスワードなどの転送データの完全性と機密性が保証されます。Cisco NX-OS LDAP クライアントは、バインドまたは検索要求を送信する前に SSL 接続を交渉することをサポートしています。リモート LDAP サーバへのトランスポートとして SSL を使用するには、Cisco NX-OS デバイスの LDAP サーバプロファイルで SSL オプションを有効にします。Cisco NX-OS デバイスでこの機能を有効にする前に、リモート LDAP サーバもこの機能をサポートしていることを確認してください。

TLS (SSL 経由) を介したリモート LDAP サーバへの接続は、RFC4513 に準拠しています。これには、セキュアトランスポート交渉中にサーバによって提示される ID が、サーバプロファイル名とスイッチ上の証明書の両方と正確に一致する必要があります。一致は、証明書の「情報カテゴリの別名」の IP アドレスまたはホスト名による可能性があります。この方式が

推奨されます。一致がない場合は、証明書「サブジェクト」の共通名 (CN) がチェックされますが、この方法は RFC4513 によって非推奨になっています。サーバ証明書は、Cisco NX-OS デバイスに個別にインストールされます。詳しい情報を表示するために [認証局およびデジタル証明書の設定](#) 章を参照します。



- (注) Cisco MDS NX-OS リリース 8.2 (1) 以降、接続先 TCP ポートが 636 として構成されている場合は、LDAP クライアントは自動的に SSL または TLS ネゴシエーションを開始されます。他の宛て先ポートを使用する場合は、**enable-ssl** オプションを使用して SSL トランスポートを手動で有効にする必要があります。

SSL トランスポートをリモート LDAP サーバに構成するには、次の手順を実行します。

手順

ステップ 1 switch# **configure terminal**

```
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 switch(config)# **ldap-server host 10.10.2.2 enable-ssl**

リモート LDAP サーバへのバインドおよび検索要求の SSL トランスポートを有効にします。

ステップ 3 switch(config)# **exit**

```
switch#
```

設定モードを終了します。

ステップ 4 switch# **copy running-config startup-config**

(任意) 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 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。

LDAP 検索マップを設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

```
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 switch(config)# ldap search-map map1

```
switch(config-ldap-search-map)#
```

LDAP 検索マップを設定します。

ステップ 3 例 1

```
switch(config-ldap-search-map) # userprofile attribute-name description search-filter  
"(&(objectClass=inetOrgPerson)(cn=$userid))" base-DN dc=acme,dc=com
```

例 2

```
switch(config-ldap-search-map) # userprofile attribute-name "memberOf" search-filter  
"(&(objectClass=inetOrgPerson)(cn=$userid))" base-DN dc=acme,dc=com
```

(任意) ユーザープロファイル、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 サーバーに送信するために使用されます。

Note LDAP 検索フィルタ文字列は最大 128 文字に制限されています。

ユーザーがメンバーとして所属しているグループを指定します。

ステップ 4 switch(config-ldap-search-map)# exit

```
switch(config)#
```

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 switch(config)# show ldap-search-map

(任意) 設定された LDAP 検索マップを表示します。

ステップ 6 switch# copy running-config startup-config

(任意) 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 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。



Note 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。

LDAP のデッド タイム間隔を設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

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 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 1 ～ 60 分です。

ステップ 3 switch(config)# **exit**

switch#

設定モードを終了します。

ステップ 4 switch# **show ldap-server**

(任意) LDAP サーバーの設定を表示します。

ステップ 5 switch# **copy running-config startup-config**

(任意) 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。

LDAP サーバに AAA 許可を設定するには、次の手順を実行します。

Before you begin

LDAP サーバで SSH 公開鍵と秘密鍵が構成されていることを確認してください。

Procedure

ステップ 1 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。

switch# **configure terminal**

ステップ 2 SSH 公開キーと SSH 証明書を構成します。

SSH 公開キー

- a. LDAP サーバのデフォルトの AAA 許可方式を構成します。

```
switch(config)# aaa authorization ssh-publickey default {group group-list | local}
```

この **ssh-publickey** キーワードは、SSH 公開キーを使用して LDAP またはローカル承認を構成します。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。

group-list 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。**local** 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。

- b. 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：

```
switch(config)# ldap-server host {ipv4-address | ipv6-address | hostname} rootDN root-name
[password password [port tcp-port [timeout seconds] | timeout seconds]]
```

- c. LDAP 検索マップを構成します：

```
switch(config)# ldap search-map map-name
```

- d. 一致する公開キーを指定します：

```
switch(config-ldap-search-map)# user-pubkey-match attribute-name attribute-name search-filter
search-filter base-dn
```

- e. 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 を構成します。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。

```
switch(config-ldap-search-map)# userprofile attribute-name "memberOf" search-filter
"&(objectClass=inetOrgPerson)(cn=$userid)" base-DN dc=acme,dc=com
```

- f. 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：

```
switch(config-ldap-search-map)# aaa group server ldap group-name
```

- g. LDAP サーバを、LDAP サーバグループのメンバとして構成します。

```
switch(config-ldap)# server {ipv4-address | ipv6-address | host-name}
```

[SSH 証明書 (SSH Certificate)]

- a. LDAP サーバのデフォルトの AAA 許可方式を構成します：

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

ssh-certificate 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。

group-list 引数は、スペースで区切られた LDAP サーバグループ名のリストです。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。**local** 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。

- b. 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：

```
switch(config)# ldap-server host {ipv4-address | ipv6-address | hostname} rootDN root-name
[password password [port tcp-port [timeout seconds] | timeout seconds]]
```

- c. LDAP 検索マップを構成します：

```
switch(config)# ldap search-map map-name
```

- d. 証明書照合を指定します：

```
switch(config-ldap-search-map)# user-certdn-match attribute-name attribute-name search-filter
search-filter base-dn
```

- e. 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 を構成します。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。

```
switch(config-ldap-search-map)# userprofile attribute-name “memberOf” search-filter
“(objectClass=inetOrgPerson)(cn=$userid)” base-DN dc=acme,dc=com
```

- f. LDAP サーバグループを作成し、そのグループの LDAP サーバグループ構成モードを開始します：

```
switch(config-ldap-search-map)# aaa group server ldap group-name
```

- g. LDAP サーバを、LDAP サーバグループのメンバとして構成します。

```
switch(config-ldap)# server {ipv4-address | ipv6-address | host-name}
```

What to do next

SSH 証明書の場合、次の機能を構成します。

1. ホスト名または、IP ドメイン名の構成します。「[ホスト名および IP ドメイン名の設定, on page 144](#)」を参照してください。
2. トラスト ポイント認証局関連付けを作成します。「[トラスト ポイント認証局関連付けを作成, on page 146](#)」を参照してください。
3. トラスト ポイント認証局の認証します。「[トラスト ポイントの認証局, on page 147](#)」を参照してください。

LDAP のディセーブル化

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。

LDAP をディセーブルにするには、次の手順を実行します。

Procedure

ステップ 1 switch# configure terminal


```
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 switch(config)# no feature ldap

LDAP をディセーブルにします。

ステップ 3 switch(config)# exit

```
switch#
```

設定モードを終了します。

ステップ 4 switch# copy running-config startup-config

(任意) 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

このコマンドの出力フィールドの詳細については、『Cisco MDS 9000 Family Command Reference, Release 5.0(1a)』を参照してください。

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 description search-filter
(&(objectClass=inetOrgPerson)(cn=$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
```

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。

Table 4: LDAP パラメータのデフォルト設定

パラメータ	デフォルト
LDAP	ディセーブル
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
デッド間隔時間	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

RADIUS サーバー モニタリング パラメータの設定

Cisco MDS 9000 ファミリー スイッチは、RADIUS プロトコルを使用してリモート AAA サーバーと通信できます。複数の RADIUS サーバーおよびサーバー グループを設定し、タイムアウトおよび再試行回数を設定できます。

RADIUS はネットワークへの不正なアクセスを防ぐ分散型クライアント/サーバー プロトコルです。Cisco の実装では、RADIUS クライアントは Cisco MDS 9000 ファミリー スイッチで実行され、ユーザー認証およびネットワーク サービス アクセス情報がすべて含まれる RADIUS 中央サーバーに認証要求が送信されます。

ここでは、RADIUS の動作の定義、ネットワーク環境の特定、および設定可能な内容について説明します。

このセクションは、次のトピックで構成されています。

RADIUS サーバーのデフォルト設定

Fabric Manager を利用すると、スイッチとの通信を設定するなどの RADIUS サーバーにも利用できるデフォルト設定をセットアップできます。デフォルト設定には次の内容が含まれます。

- 暗号の種類
- タイムアウトの値
- 送信試行回数

- ユーザーによるログイン時の RADIUS サーバー指定の許可

RADIUS サーバーの IPv4 アドレスの設定

最大 64 台の RADIUS サーバーを追加できます。RADIUS のキーは永続性ストレージに必ず暗号化して保存されます。実行コンフィギュレーションにも、暗号化されたキーが表示されません。

ホスト RADIUS サーバーの IPv4 アドレスおよびその他のオプションを指定する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **radius-server host 10.10.0.0 key HostKey**

選択した RADIUS サーバーの事前共有キーを指定します。このキーは **radius-server key** コマンドを使用して割り当てたキーを上書きします。この例では、ホストは 10.10.0.0 で、キーは HostKey です。

ステップ 3 switch(config)# **radius-server host 10.10.0.0 auth-port 2003**

RADIUS 認証メッセージを送信する宛先 UDP ポート番号を指定します。この例では、ホストは 10.10.0.0 で、認証ポートは 2003 です。デフォルトの認証ポートは 1812 で、有効な範囲は 0 ~ 65366 です。

ステップ 4 switch(config)# **radius-server host 10.10.0.0 acct-port 2004**

RADIUS アカウンティングメッセージを送信する宛先 UDP ポート番号を指定します。デフォルトのアカウンティングポートは 1813 で、有効な範囲は 0 ~ 65366 です。

ステップ 5 switch(config)# **radius-server host 10.10.0.0 accounting**

アカウンティングの目的のみに使用されるこのサーバーを指定します。

Note **authentication** と **accounting** オプションのどちらも指定しないと、サーバーは認証およびアカウンティングの両方の目的に使用されます。

ステップ 6 switch(config)# **radius-server host 10.10.0.0 key 0 abcd**

指定したサーバーのクリアテキストキーを指定します。キーの長さは 64 文字に制限されています。

ステップ 7 switch(config)# **radius-server host 10.10.0.0 key 4 da3Asda2ioyuoIUH**

指定したサーバーの暗号化キーを指定します。キーの長さは 64 文字に制限されています。

RADIUS サーバーの IPv6 アドレスの設定

ホスト RADIUS サーバーの IPv6 アドレスおよびその他のオプションを指定する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **radius-server host 2001:0DB8:800:200C::417A Key HostKey**

選択した RADIUS サーバーの事前共有キーを指定します。このキーは **radius-server key** コマンドを使用して割り当てたキーを上書きします。この例では、ホストは 2001:0DB8:800:200C::417A で、キーは HostKey です。

ステップ 3 switch(config)# **radius-server host 2001:0DB8:800:200C::417A auth-port 2003**

RADIUS 認証メッセージを送信する宛先 UDP ポート番号を指定します。この例では、ホストは 2001:0DB8:800:200C::417A で、認証ポートは 2003 です。デフォルトの認証ポートは 1812 で、有効な範囲は 0 ~ 65366 です。

ステップ 4 switch(config)# **radius-server host 2001:0DB8:800:200C::417A acct-port 2004**

RADIUS アカウンティングメッセージを送信する宛先 UDP ポート番号を指定します。デフォルトのアカウンティングポートは 1813 で、有効な範囲は 0 ~ 65366 です。

ステップ 5 switch(config)# **radius-server host 2001:0DB8:800:200C::417A accounting**

アカウンティングの目的のみに使用されるこのサーバーを指定します。

Note authentication と accounting オプションのどちらも指定しないと、サーバーは認証およびアカウンティングの両方の目的に使用されます。

ステップ 6 switch(config)# **radius-server host 2001:0DB8:800:200C::417A key 0 abcd**

指定したサーバーのクリアテキストキーを指定します。キーの長さは 64 文字に制限されています。

ステップ 7 switch(config)# **radius-server host 2001:0DB8:800:200C::417A key 4 da3Asda2ioyuoIUH**

指定したサーバーの暗号化キーを指定します。キーの長さは 64 文字に制限されています。

RADIUS サーバーの DNS 名の設定

ホスト RADIUS サーバーの DNS 名およびその他のオプションを指定する手順は、次のとおりです。

手順

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **radius-server host radius2 key HostKey**

選択した RADIUS サーバーの事前共有キーを指定します。このキーは **radius-server key** コマンドを使用して割り当てたキーを上書きします。この例では、ホストは radius2 で、キーは HostKey です。

ステップ 3 switch(config)# **radius-server host radius2 auth-port 2003**

RADIUS 認証メッセージを送信する宛先 UDP ポート番号を指定します。この例では、ホストは radius2 で、認証ポートは 2003 です。デフォルトの認証ポートは 1812 で、有効な範囲は 0 ~ 65366 です。

ステップ 4 switch(config)# **radius-server host radius2 acct-port 2004**

RADIUS アカウンティングメッセージを送信する宛先 UDP ポート番号を指定します。デフォルトのアカウンティングポートは 1813 で、有効な範囲は 0 ~ 65366 です。

ステップ 5 switch(config)# **radius-server host radius2 accounting**

アカウンティングの目的のみに使用されるこのサーバーを指定します。

(注) **authentication** と **accounting** オプションのどちらも指定しないと、サーバーは認証およびアカウンティングの両方の目的に使用されます。

ステップ 6 switch(config)# **radius-server host radius2 key 0 abcd**

指定したサーバーのクリアテキスト キーを指定します。キーの長さは 64 文字に制限されています。

ステップ 7 switch(config)# **radius-server host radius2 key 4 da3Asda2ioyuoiuH**

指定したサーバーの暗号化キーを指定します。キーの長さは 64 文字に制限されています。

RADIUS サーバーにおける暗号の種類と事前共有キーのデフォルト値の概要

スイッチを RADIUS サーバーに対して認証するには、RADIUS 事前共有キーを設定する必要があります。キーの長さは 64 文字に制限され、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)。グローバル鍵は、スイッチにあるすべての RADIUS サーバー コンフィギュレーションで使用できるよう設定できます。

グローバル キーの割り当てを上書きするには、**radius-server host** コマンドで個々の RADIUS サーバーの設定時に **key** オプションを明示的に使用する必要があります。

RADIUS サーバーにおける暗号の種類と事前共有キーのデフォルト値の設定

RADIUS 事前共有キーを設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **radius-server key AnyWord**

RADIUS クライアントおよびサーバー間の通信を認証する事前共有キー (AnyWord) を設定します。デフォルトはクリアテキストです。

ステップ 3 switch(config)# **radius-server key 0 AnyWord**

RADIUS クライアントとサーバー間の通信を認証する、クリアテキスト (0 で指定) で記述された事前共有キー (AnyWord) を設定します。

ステップ 4 switch(config)# **radius-server key 7 abc4DFeeweo00o**

RADIUS クライアントとサーバー間の通信を認証する、暗号化テキスト (7 で指定) で指定された事前共有キー (暗号化テキストで指定) を設定します。

RADIUS サーバーのタイムアウト間隔の設定

すべての RADIUS サーバーに対して送信間のグローバル タイムアウト値を設定できます。



Note タイムアウト値が個々のサーバーに設定されている場合は、グローバル設定された値よりもそれらの値が優先されます。

RADIUS サーバーへの再送信間のタイムアウト値を指定するには、次の手順を実行してください。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **radius-server timeout 30**

スイッチがタイムアウト障害を宣言する前に、すべての RADIUS+ サーバーからの応答を待機する、スイッチのグローバルタイムアウト期間（秒）を設定します。指定できる範囲は 1 ～ 1440 秒です。

ステップ 3 switch(config)# no radius-server timeout 30

送信時間をデフォルト値（1 秒）に戻します。

RADIUS サーバーのタイムアウト間隔および再送信のデフォルト値の設定

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。RADIUS サーバーに対してタイムアウトの値を設定することもできます。

RADIUS サーバーがユーザーを認証する試行回数を指定するには、次の手順を実行します。

Procedure

ステップ 1 switch# configure terminal

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# radius-server retransmit 3

ローカル認証に戻る前に、スイッチが RADIUS サーバーへの接続を試行する回数（3）を設定します。

ステップ 3 switch(config)# no radius-server retransmit

デフォルトの試行回数（1）に戻します。

RADIUS サーバー モニタリング パラメータの設定

RADIUS サーバーをモニターするためのパラメータを設定できます。サーバーを定期的にテストするためにこのオプションを設定できるほか、1 回だけのテストを行うこともできます。

このセクションは、次のトピックで構成されています。

テストアイドルタイマーの設定

テストアイドルタイマーには、MDS スイッチがテストパケットを送るまで RADIUS サーバーが要求を受信しないでいる時間間隔を指定します。



Note デフォルトのアイドルタイマー値は0分です。アイドルタイムインターバルが0分の場合、RADIUS サーバの定期的なモニタリングは実行されません。

アイドルタイマーを設定するには、次の手順を実行します。

Procedure

ステップ1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ2 switch(config)# **radius-server host 10.1.1.1 test idle-time 20**

テスト用のアイドル間隔の値を分で設定します。有効な範囲は1～1440分です。

ステップ3 switch(config)# **no radius-server host 10.1.1.1 test idle-time 20**

デフォルト値（0分）に戻します。

テストユーザー名の設定

定期的な RADIUS サーバーのステータステストに使用するユーザー名とパスワードを設定できます。RADIUS サーバーを監視するテストメッセージを発行するために、テストユーザー名とパスワードを設定する必要はありません。デフォルトのテストユーザー名（test）とデフォルトのパスワード（test）を利用できます。



Note セキュリティ上の理由から、テストユーザー名を RADIUS データベースに存在する既存のユーザー名と同一にしないことを推奨します。

定期的な RADIUS サーバーのステータステストに使用するオプションのユーザー名とパスワードを設定するには、次の手順を実行します。

Procedure

ステップ1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ2 switch(config)# **radius-server host 10.1.1.1 test username testuser**

テストユーザー（testuser）にデフォルトのパスワード（test）を設定します。デフォルトのユーザー名は test です。

ステップ 3 switch(config)# **no radius-server host 10.1.1.1 test username testuser**

テスト ユーザー名 (testuser) を削除します。

ステップ 4 switch(config)# **radius-server host 10.1.1.1 test username testuser password Ur2Gd2BH**

テスト ユーザー (testuser) を設定し、強力なパスワードを割り当てます。

デッド タイマーの設定

デッドタイマーには、MDS スイッチが、RADIUS サーバーをデッド状態であると宣言した後、そのサーバーがアライブ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。



Note デフォルトのデッドタイマー値は0分です。デッドタイマーの間隔が0分の場合、RADIUS サーバーがサーバー グループの一部でグループのデッドタイム インターバルが0分を超えていないかぎり、RADIUS サーバー モニタリングは実行されません。(サーバー グループ, on page 40を参照してください)。



Note デッド RADIUS サーバーに RADIUS テスト メッセージが送信される前に、同サーバーのデッドタイマーの期限が切れた場合、同サーバーがまだ応答していないとしても再度アライブ状態としてマークされます。このシナリオを回避するには、デッドタイマーの時間よりも短いアイドル時間でテスト ユーザーを設定します。

デッドタイマーを設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **radius-server deadtime 30**

デッドタイマー間隔値を分で設定します。有効な範囲は1 ~ 1440 分です。

ステップ 3 switch(config)# **no radius-server deadtime 30**

デフォルト値 (0 分) に戻します。

RADIUS サーバーの概要

最大 64 台の RADIUS サーバーを追加できます。RADIUS のキーは永続性ストレージに必ず暗号化して保存されます。実行コンフィギュレーションにも、暗号化されたキーが表示されません。新しい RADIUS サーバーを設定する際は、デフォルト設定を利用することも、パラメータのいずれかを修正してデフォルトの RADIUS サーバー設定を上書きすることもできます。

テスト アイドル タイマーの設定

テストアイドルタイマーには、MDS スイッチがテストパケットを送るまで RADIUS サーバーが要求を受信しないでいる時間間隔を指定します。



Note デフォルトのアイドルタイマー値は 0 分です。アイドルタイムインターバルが 0 分の場合、RADIUS サーバの定期的なモニタリングは実行されません。

テストアイドルタイマーを設定するには、[RADIUS サーバー モニタリング パラメータの設定, on page 68](#)を参照してください。

テスト ユーザー名の設定

定期的な RADIUS サーバーのステータステストに使用するユーザー名とパスワードを設定できます。RADIUS サーバーを監視するテストメッセージを発行するために、テストユーザー名とパスワードを設定する必要はありません。デフォルトのテストユーザー名 (test) とデフォルトのパスワード (test) を利用できます。



Note セキュリティ上の理由から、テストユーザー名を RADIUS データベースに存在する既存のユーザー名と同一にしないことを推奨します。

定期的な RADIUS サーバーのステータステストに使用するオプションのユーザー名とパスワードの設定については、[RADIUS サーバー モニタリング パラメータの設定, on page 68](#)を参照してください。

RADIUS サーバーの検証の概要

Cisco SAN-OS リリース 3.0(1) では、RADIUS サーバーを定期的に検証できます。スイッチは、設定されたユーザー名とパスワードを使用してテスト用認証をサーバーに送信します。このテスト認証にサーバーが応答しない場合、サーバーは応答能力がないものと見なされます。



Note セキュリティ上の理由から、RADIUS サーバーで設定されたユーザー名をテストユーザー名として使用しないことを推奨します。

サーバーを定期的にテストするためにこのオプションを設定できるほか、1 回だけのテストを行うこともできます。

モニタリング用 RADIUS テストメッセージの送信

RADIUS サーバーをモニターするテストメッセージを手動で送信できます。

RADIUS サーバーにテストメッセージを送信するには、次の手順を実行します。

Procedure

ステップ 1 switch# test aaa server radius 10.10.1.1 test test

デフォルトのユーザー名 (test) とパスワード (test) を使用して RADIUS サーバーにテストメッセージを送信します。

ステップ 2 switch# test aaa server radius 10.10.1.1 testuser Ur2Gd2BH

設定されたテストユーザー名 (testuser) とパスワード (Ur2Gd2BH) を使用して RADIUS サーバーにテストメッセージを送信します。

Note 設定済みのユーザー名およびパスワードはオプションです ([テストユーザー名の設定, on page 91](#)の項を参照)。

ログイン時にユーザによる RADIUS サーバの指定を許可

デフォルトでは、MDS スイッチは認証要求を RADIUS サーバー グループの最初のサーバーに転送します。誘導要求オプションをイネーブルにすると、どの RADIUS サーバーに認証要求を送信するかをユーザーが指定できるようにスイッチを設定できます。このオプションをイネーブルにすると、ユーザーは `username@hostname` としてログインできます。hostname は設定した RADIUS サーバーの名前です。



Note ユーザー指定のログインは Telnet セッションに限りサポートされます。

MDS スイッチにログインしているユーザーが認証用の RADIUS サーバーを選択できるようにする手順は、次のとおりです。

Procedure

ステップ 1 switch# configure terminal

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **radius-server directed-request**

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。

ステップ 3 switch(config)# **no radius-server directed-request**

サーバー グループの最初のサーバーに認証要求を送信するように戻します（デフォルト）。

Example

RADIUS への誘導要求設定を表示するには、**show tacacs-server directed-request** コマンドを使用できます。

```
switch# show radius-server directed-request
disabled
```

ベンダー固有属性の概要

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 サーバーと RADIUS サーバー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 で、サポートするオプションはベンダー タイプ 1、名前は **cisco-avpair** です。値は次の形式のストリングです。

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

protocol は、特定の認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 =（等号記号）、省略可能な属性の場合は *（アスタリスク）です。

Cisco MDS 9000 ファミリー スイッチに対するユーザー認証に RADIUS サーバーを使用した場合、RADIUS プロトコルは、認証結果とともに認可情報などのユーザー属性を戻すように 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

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** プロトコル：ユーザー プロファイル情報を提供するために Access-Accept パケットで使用されます。
- **Accounting** プロトコル：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。

次の属性が Cisco NX-OS ソフトウェアでサポートされています。

- **roles** : この属性は、ユーザーが属すすべてのロールをリストします。値フィールドは、グループ名のスペース区切りリストを含む文字列です。たとえば、**vsan-admin** と **storage-admin** に属している場合、値フィールドは“**vsan-admin storage-admin**”になります。このサブ属性は Access-Accept フレームの VSA 部分に格納され、RADIUS サーバーから送信されます。この属性は shell プロトコル値とだけ併用できます。次に、ロール属性を使用する 2 つの例を示します。

```
shell:roles="network-admin vsan-admin"
```

```
shell:roles*“network-admin vsan-admin”
```

VSA が **shell:roles*“network-admin vsan-admin”** として指定されている場合は、この VSA がオプション属性としてフラグ設定されます。その他のシスコデバイスはこの属性を無視します。

- **accountinginfo** : この属性は、標準の RADIUS アカウンティングプロトコルに含まれる属性を補足する追加的なアカウンティング情報を表します。この属性が送信されるのは、Account-Request フレームの VSA 部分に保管され、スイッチ上の RADIUS クライアントから送信される場合だけです。この属性を併用できるのは、アカウンティングプロトコル関連の PDU だけです。

AAA サーバーでの SNMPv3 の指定

ベンダー/カスタム属性 **cisco-av-pair** は、次のフォーマットを使用してユーザーのロールマッピングを指定する場合に使用できます。

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



Note Telnet または SSH により Fabric Manager または Device Manager を利用して Cisco MDS スイッチに正常にログインした場合、スイッチに AAA サーバーベースの認証が設定されていると、1 日の有効期限で一時的な SNMP ユーザー エントリが自動的に作成されます。スイッチは、使用している Telnet または SSH ログイン名を SNMPv3 ユーザー名として SNMPv3 プロトコル データ ユニット (PDU) を認証します。管理ステーションは Telnet または SSH ログイン名を、SNMPv3 の **auth** および **priv** パスフレーズとして一時的に使用できます。この一時的な SNMP ログインが許可されるのは、1 つ以上のアクティブな MDS シェルセッションが存在する場合だけです。指定時刻にアクティブなセッションが存在しない場合は、ログインが削除され、SNMPv3 の操作を実行できません。

cisco-av-pair 属性でロールオプションが設定されていない場合、デフォルトのユーザーロールは **network-operator** になります。

また、VSA フォーマットには、オプションで SNMPv3 認証と機密保全プロトコルの属性を次のように指定できます。

```
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。これらのオプションが ACS サーバー

の **cisco-av-pair** 属性で指定されていない場合は、MD5 および DES がデフォルトで使用されます。

Cisco MDS NX-OS リリース 8.5 (1) から、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。これらのオプションが ACS サーバーの **cisco-av-pair** 属性で指定されていない場合は、MD5 および AES-128 がデフォルトで使用されます。

RADIUS サーバーの詳細の表示

設定された RADIUS パラメータを表示するには、**show radius-server** コマンドを次の例のように使用します。

設定された RADIUS 情報の表示

```
switch# show radius-server
Global RADIUS shared secret:*****
retransmission count:5
timeout value:10
following RADIUS servers are configured:
  myradius.cisco.users.com:
    available for authentication on port:1812
    available for accounting on port:1813
  172.22.91.37:
    available for authentication on port:1812
    available for accounting on port:1813
    RADIUS shared secret:*****
  10.10.0.0:
    available for authentication on port:1812
    available for accounting on port:1813
    RADIUS shared secret:*****
```

設定済みの RADIUS サーバー グループ順序の表示

```
switch# show radius-server groups
total number of groups:4
following RADIUS server groups are configured:
  group radius:
    server: all configured radius servers
  group Group1:
    server: Server3 on auth-port 1812, acct-port 1813
    server: Server5 on auth-port 1812, acct-port 1813
  group Group5:
```

RADIUS サーバー統計情報の表示

show radius-server statistics コマンドを使用して、RADIUS サーバーの統計情報を表示できます。

clear radius-server statistics 10.1.3.2 コマンドを使用して、RADIUS サーバーの統計情報をクリアできます。

RADIUS サーバー統計情報の表示

```
switch# show radius-server statistics 10.1.3.2
Server is not monitored
Authentication Statistics
  failed transactions: 0
  successful transactions: 0
  requests sent: 0
  requests timed out: 0
  responses with no matching requests: 0
  responses not processed: 0
  responses containing errors: 0
Accounting Statistics
  failed transactions: 0
  successful transactions: 0
  requests sent: 0
  requests timed out: 0
  responses with no matching requests: 0
  responses not processed: 0
  responses containing errors:
```

clear radius-server statistics 10.1.3.2 コマンドを使用して、RADIUS サーバーの統計情報をクリアできます。

ワンタイムパスワードサポート

ワンタイムパスワードサポート (OTP) は、1回のログインセッションまたはトランザクションに有効なパスワードです。OTPは、通常の (スタティック) パスワードに関連する多数の欠点を回避します。OTPによって対処される最も重大な欠点は、リプレイ攻撃のリスクにさらされないことです。すでにサービスへのログインまたは操作の実行に使用された OTP を侵入者が記録しようとしても、OTP は有効ではなくなっているため、悪用されません。

ワンタイムパスワードは RADIUS や TACACS プロトコルデーモンに対してのみ適用できます。RADIUS プロトコルデーモンの場合、スイッチ側からの設定はありません。TACACS プロトコルの場合、次のコマンドで使用できる ascii 認証モードを有効にする必要があります。

```
aaa authentication login ascii-authentication
```

管理者パスワードの回復

次の 2 通りの方法のいずれかで管理者パスワードを回復できます。

- network-admin 権限を持つユーザー名による CLI の使用
- スイッチの電源再投入

ここでは、次の項目について説明します。

network-admin 権限での CLI の使用

network-admin 権限を持つユーザー名でスイッチにログインしているか、ログインできる場合に、管理者パスワードを回復するには、次の手順を実行します。

Procedure

- ステップ 1** ユーザー名に network-admin 権限があることを確認するには、**show user-accounts** コマンドを使用します。

Example:

```
switch# show user-account

user:admin
this user account has no expiry date
roles:network-admin
user:dbgusr
this user account has no expiry date
roles:network-admin network-operator
```

- ステップ 2** ユーザー名に network-admin 権限がある場合は、**username** コマンドを発行して新しい管理者パスワードを割り当てます。

Example:

```
switch# configure terminal
switch(config)# username admin password <new password>
switch(config)# exit
switch#
```

- ステップ 3** ソフトウェア設定を保存します。

Example:

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

スイッチの電源の再投入

network-admin 特権を持つスイッチ上でセッションを開始できない場合は、スイッチの電源を再投入して管理者パスワードを回復する必要があります。



Caution この手順を実行すると、スイッチ上のすべてのトラフィックが中断されます。スイッチとの接続はすべて 2 ~ 3 分間切断されます。



Note 管理者パスワードは、Telnet または SSH セッションからは回復できません。ローカル コンソール接続を使用できる必要があります。コンソール接続のセットアップの詳細については、[Cisco MDS 9000 Series Fundamentals Configuration Guide](#)を参照してください。

スイッチの電源を再投入して、管理者パスワードを回復するには、次の手順を実行します。

Procedure

- ステップ 1** スタンバイのスーパーバイザ モジュールをシャーシから取り外します。
- ステップ 2** スwitchの電源を再投入します。
- ステップ 3** スwitchが Cisco NX-OS ソフトウェアのブート シーケンスを開始したときに **Ctrl-]** キー シーケンスを押して、switch(boot)# プロンプト モードを開始します。

Ctrl-]

```
switch(boot)#
```

- ステップ 4** コンフィギュレーション モードに切り替えます。

```
switch(boot)# configure terminal
```

- ステップ 5** admin-password コマンドを発行して、管理者パスワードをリセットします。これは、コンソールを使用してログインのリモート認証を無効にします（有効な場合）。これはパスワードを回復した後、新しいパスワードで管理者がコンソールからログインできるようにするために行います。Telnet/SSH の認証は、これにより影響を受けません。

```
switch(boot-config)# admin-password <new password>  
WARNING! Remote Authentication for login through console will be disabled#
```

強力なパスワードの詳細については、[パスワード強度の確認, on page 15](#)の項を参照してください。

- ステップ 6** EXEC モードに切り替えます。

```
switch(boot-config)# admin-password <new password>
```

- ステップ 7** load コマンドを発行して、Cisco NX-OS ソフトウェアをロードします。

```
switch(boot)# load bootflash:m9700-sf4ek9-mz.8.4.1.bin
```

Caution コンフィギュレーションを保存するために使用するイメージより古いシステムイメージをブートし、**install all** コマンドを使用せずにシステムをブートする場合、スイッチはバイナリ コンフィギュレーションを消去し、ASCII コンフィギュレーションを使用します。この場合は、**init system** コマンドを使用してパスワードを回復する必要があります。

- ステップ 8** 新しい管理者パスワードを使用してスイッチにログインします。

```
switch login: admin  
Password: <newpassword>
```

- ステップ 9** Fabric Manager の SNMP パスワードとしても使用できるようにするために、新しいパスワードをリセットします。

```
switch# configure terminal
switch(config)# username admin password<new password>
switch(config)# exit
switch#
```

- ステップ 10** ソフトウェア設定を保存します。

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

- ステップ 11** 以前に取り外したスーパーバイザ モジュールをシャーシのスロット 6 に挿入します。

TACACS+ サーバー モニタリング パラメータの設定

Cisco MDS スイッチは Terminal Access Controller Access Control System Plus (TACACS+) プロトコルを使用して、リモート AAA サーバーと通信します。複数の TACACS+ サーバーを設定し、タイムアウト値を指定できます。

このセクションは、次のトピックで構成されています。

TACACS+ について

TACACS+ は、TCP (TCP ポート 49) を使用してトランスポート要件を満たすクライアント/サーバー プロトコルです。すべての Cisco MDS 9000 ファミリー スイッチは、TACACS+ プロトコルを使用して中央から認証できます。TACACS+ には、RADIUS 認証と比較して次のような利点があります。

- 独立したモジュラ式 AAA ファシリティを提供します。認証を行わずに、認可を実行できます。
- 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、接続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+ サーバーのデフォルト設定

Fabric Manager を利用すると、スイッチとの通信を設定する際の TACACS+ サーバーにも利用できるデフォルト設定をセットアップできます。デフォルト設定には次の内容が含まれます。

- 暗号の種類
- 事前共有キー
- タイムアウトの値
- 送信試行回数
- ユーザーによるログイン時の TACACS+ サーバー指定の許可

TACACS+サーバーにおける暗号の種類と事前共有キーのデフォルト値の概要

スイッチを TACACS+ サーバーに対して認証するには、TACACS+ 事前共有キーを設定する必要があります。キーの長さは 64 文字に制限され、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）。グローバル鍵を設定して、スイッチにあるすべての TACACS+ サーバー コンフィギュレーションで使用するようにできます。

グローバルキーの割り当てを上書きするには、個々の TACACS+ サーバーの設定時に **key** オプションを使用する必要があります。

TACACS+ のイネーブル化

デフォルトでは、Cisco MDS 9000 ファミリの全スイッチで TACACS+ 機能がディセーブルに設定されています。ファブリック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、TACACS+ 機能を明示的にイネーブルにする必要があります。この機能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。

Cisco MDS スwitchの TACACS+ をイネーブルにする手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **feature tacacs+**

このスイッチの TACACS+ をイネーブルにします。

ステップ 3 switch(config)# **no feature tacacs+**

(オプション) このスイッチの TACACS+ をディセーブル (デフォルト) にします。

TACACS+ サーバーの IPv4 アドレスの設定

設定されたサーバーに秘密キーが設定されていない場合、グローバルキーが設定されていないと、警告メッセージが発行されます。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 ([TACACS+ サーバーのタイムアウト間隔および再送信のデフォルト値の設定](#), on page 89の項を参照)。



Note グローバル秘密キーにはドル記号 (\$)、パーセント記号 (%) を使用できます。

TACACS+ サーバーの IPv4 アドレスおよびその他のオプションを設定する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **tacacs-server host 171.71.58.91**

指定の IPv4 アドレスによって識別される TACACS+ サーバーを設定します。

ステップ 3 switch(config)# **no tacacs-server host 171.71.58.91**

(オプション) IPv4 アドレスによって識別される特定の TACACS+ サーバーを削除します。デフォルトでは、サーバーは設定されません。

ステップ 4 switch(config)# **tacacs-server host 171.71.58.91 port 2**

すべての TACACS+ 要求に対し TCP ポートを設定します。

ステップ 5 switch(config)# **no tacacs-server host 171.71.58.91 port 2**

(オプション) サーバー アクセス用にポート 49 を使用する、工場出荷時のデフォルトに戻ります。

ステップ 6 switch(config)# **tacacs-server host 171.71.58.91 key MyKey**

指定されたドメイン名で指定された TACACS+ サーバーを設定し、秘密キーを割り当てます。

ステップ 7 switch(config)# **tacacs-server host 171.71.58.91 timeout 25**

スイッチがタイムアウト障害を宣言する前に、指定したサーバーからの応答を待機する、スイッチのタイムアウト期間を設定します。

TACACS+ サーバーの IPv6 アドレスの設定

TACACS+ サーバーの IPv6 アドレスおよびその他のオプションを設定する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **tacacs-server host 2001:0DB8:800:200C::417A**

```
warning: no key is configured for the host
```

指定の IPv6 アドレスによって識別される TACACS+ サーバーを設定します。

ステップ 3 switch(config)# **no tacacs-server host 2001:0DB8:800:200C::417A**

(オプション) IPv6 アドレスによって識別される特定の TACACS+ サーバーを削除します。デフォルトでは、サーバーは設定されません。

ステップ 4 switch(config)# **tacacs-server host 2001:0DB8:800:200C::417A port 2**

すべての TACACS+ 要求に対し TCP ポートを設定します。

ステップ 5 switch(config)# **no tacacs-server host 2001:0DB8:800:200C::417A port 2**

(オプション) サーバー アクセス用にポート 49 を使用する、工場出荷時のデフォルトに戻ります。

ステップ 6 switch(config)# **tacacs-server host 2001:0DB8:800:200C::417A key MyKey**

指定されたドメイン名で指定された TACACS+ サーバーを設定し、秘密キーを割り当てます。

ステップ 7 switch(config)# **tacacs-server host 2001:0DB8:800:200C::417A timeout 25**

スイッチがタイムアウト障害を宣言する前に、指定したサーバーからの応答を待機する、スイッチのタイムアウト期間を設定します。

TACACS+ サーバーの DNS 名の設定

TACACS+ サーバーの DNS 名およびその他のオプションを設定する手順は、次のとおりです。

手順

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **tacacs-server host host1.cisco.com**

```
warning: no key is configured for the host
```

指定の DNS 名によって識別される TACACS+ サーバーを設定します。

ステップ 3 switch(config)# **no tacacs-server host host1.cisco.com**

(オプション) 指定の DNS 名によって識別される TACACS+ サーバーを削除します。デフォルトでは、サーバーは設定されません。

ステップ 4 switch(config)# **tacacs-server host host1.cisco.com port 2**

すべての TACACS+ 要求に対し TCP ポートを設定します。

ステップ 5 switch(config)# no tacacs-server host host1.cisco.com port 2

(オプション) サーバー アクセス用にポート 49 を使用する、工場出荷時のデフォルトに戻ります。

ステップ 6 switch(config)# tacacs-server host host1.cisco.com key MyKey

指定されたドメイン名で指定された TACACS+ サーバーを設定し、秘密キーを割り当てます。

ステップ 7 switch(config)# tacacs-server host host1.cisco.com timeout 25

スイッチがタイムアウト障害を宣言する前に、指定したサーバーからの応答を待機する、スイッチのタイムアウト期間を設定します。

グローバル秘密キーの設定

すべての TACACS+ サーバーで秘密キーに対するグローバル値を設定できます。

**Note**

- 秘密キーが個々のサーバーに設定されている場合は、グローバル設定されたキーよりもそれらのキーが優先されます。
- グローバル秘密キーにはドル記号 (\$)、パーセント記号 (%) を使用できます。

TACACS+ サーバーの秘密キーを設定するには、次の手順を実行します。

Procedure**ステップ 1** switch# configure terminal

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# tacacs-server key 7 3sdaA3daKUngd

TACACS+ サーバーにアクセスするには、グローバル秘密キー (暗号化形式) を割り当てます。この例では、使用されている暗号化された形式を表示するのに **7** を指定します。このグローバルキーと各サーバーキーが設定されていない場合、クリアテキストメッセージが TACACS+ サーバーに送信されます。

ステップ 3 switch(config)# no tacacs-server key oldPword

(オプション) 設定されたグローバル秘密キーを TACACS+ サーバーにアクセスするために削除し、すべての設定済みのサーバーへのアクセスを許可する工場出荷時のデフォルトに戻します。

TACACS+サーバーのタイムアウト間隔および再送信のデフォルト値の設定

デフォルトでは、スイッチは TACACS+ サーバーを 1 回だけ試行します。この回数は設定可能です。最大試行回数は、各サーバーで 5 回です。TACACS+ サーバーに対してタイムアウトの値を設定することもできます。

タイムアウト値の設定

すべての TACACS+ サーバーに対して送信間のグローバル タイムアウト値を設定できます。



Note タイムアウト値が個々のサーバーに設定されている場合は、グローバル設定された値よりもそれらの値が優先されます。

TACACS+ サーバーのグローバル タイムアウト値を設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **tacacs-server timeout 30**

スイッチがタイムアウト障害を宣言する前に、すべての TACACS+ サーバーからの応答を待機する、スイッチのグローバル タイムアウト期間（秒）を設定します。指定できる範囲は 1 ~ 1440 秒です。

ステップ 3 switch(config)# **no tacacs-server timeout 30**

（オプション）設定済みのタイムアウト期間を削除し、工場出荷時のデフォルトである 5 秒に戻します。

TACACS+ サーバーの概要

デフォルトでは、Cisco MDS 9000 ファミリの全スイッチで TACACS+ 機能がディセーブルに設定されています。TACACS+ サーバーの設定を行うと、Fabric Manager または Device Manager によって自動的に TACACS+ の機能がイネーブルになります。

設定されたサーバーに秘密キーが設定されていない場合、グローバルキーが設定されていないと、警告メッセージが発行されます。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。



Note Cisco MDS SAN-OS リリース 2.1(2) よりも前のバージョンでは、キーでドル記号 (\$) を使用できますが、二重引用符で囲む必要があります (例、"k\$")。パーセント記号 (%) は使用できません。Cisco MDS SAN-OS リリース 2.1(2) 以降では、二重引用符なしでドル記号 (\$) を使用でき、パーセント記号 (%) はグローバル秘密キーで使用できます。

すべての TACACS+ サーバーで秘密キーに対するグローバル値を設定できます。



Note 秘密キーが個々のサーバーに設定されている場合は、グローバル設定されたキーよりもそれらのキーが優先されます。

TACACS+ サーバー モニタリング パラメータの設定

TACACS+ サーバーをモニターするためのパラメータを設定できます。

このセクションは、次のトピックで構成されています。

TACACS+ テストアイドルタイマーの設定

テストアイドルタイマーには、MDS スイッチがテスト パケットを送るまで TACACS+ サーバーが要求を受信しないでいる時間間隔を指定します。



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。

アイドル タイマーを設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# configure terminal

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# tacacs-server host 10.1.1.1 test idle-time 20

テスト用のアイドル間隔の値を分で設定します。有効な範囲は 1 ~ 1440 分です。

ステップ 3 switch(config)# no tacacs-server host 10.1.1.1 test idle-time 20

(オプション) デフォルト値 (0 分) に戻します。

テストユーザー名の設定

定期的な TACACS+ サーバーのステータステストに使用するユーザー名とパスワードを設定できます。TACACS+ サーバーを監視するためのユーザー名とパスワードを設定する必要はありません。デフォルトのテストユーザー名 (`test`) とデフォルトのパスワード (`test`) を利用できます。

定期的な TACACS+ サーバーのステータステストに使用するオプションのユーザー名とパスワードを設定するには、次の手順を実行します。

Procedure

ステップ 1 `switch# configure terminal`

コンフィギュレーションモードに入ります。

ステップ 2 `switch(config)# tacacs-server host 10.1.1.1 test username testuser`

テストユーザー (`testuser`) にデフォルトのパスワード (`test`) を設定します。デフォルトのユーザー名は `test` です。

ステップ 3 `switch(config)# no tacacs-server host 10.1.1.1 test username testuser`

(オプション) テストユーザー (`testuser`) を削除します。

ステップ 4 `switch(config)# tacacs-server host 10.1.1.1 test username testuser password Ur2Gd2BH`

テストユーザー (`testuser`) を設定し、強力なパスワードを割り当てます。

デッドタイマーの設定

デッドタイマーには、MDS スイッチが、TACACS+ サーバーをデッド状態であると宣言した後、そのサーバーがアライブ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。



Note

- デフォルトのデッドタイマー値は 0 分です。TACACS+ サーバー モニタリングは、TACACS+ サーバーがデッドタイム インターバルが 0 分よりも長い、より大きなグループの一部でない限り、デッドタイマーの間隔が 0 分であれば実行されません。(RADIUS サーバー モニタリング パラメータの設定, on page 68 を参照)。
- デッド TACACS+ サーバーに TACACS+ テストメッセージが送信される前に、同サーバーのデッドタイマーの期限が切れた場合、同サーバーがまだ応答していないとしても再度アライブ状態としてマークされます。このシナリオを回避するには、デッドタイマーの時間よりも短いアイドル時間でテストユーザーを設定します。

デッドタイマーを設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **tacacs-server deadtime 30**

デッドタイム インターバル値を分で設定します。有効な範囲は 1 ～ 1440 分です。

ステップ 3 switch(config)# **no tacacs-server deadtime 30**

(オプション) デフォルト値 (0 分) に戻します。

Note デッドタイム インターバルが 0 分の場合、TACACS+ サーバーがサーバー グループの一部でグループのデッドタイム インターバルが 0 分を超えていないかぎり、TACACS+ サーバーモニタリングは実行されません。(RADIUS サーバーモニタリングパラメータの設定, on page 68の項を参照)。

モニタリング用 TACACS+ テストメッセージの送信

TACACS+ サーバーをモニターするテストメッセージを手動で送信できます。

TACACS+ サーバーにテストメッセージを送信するには、次の手順を実行します。

手順

ステップ 1 switch# **test aaa server tacacs+ 10.10.1.1 test**

デフォルトのユーザー名 (test) とパスワード (test) を使用して TACACS+ サーバーにテストメッセージを送信します。

ステップ 2 switch# **test aaa server tacacs+ 10.10.1.1 testuser Ur2Gd2BH**

設定されたテストユーザー名とパスワードを使用して TACACS+ サーバーにテストメッセージを送信します。設定済みのユーザー名およびパスワードはオプションです(テストユーザー名の設定 (91 ページ) の項を参照)。

TACACS+ サーバーからのパスワードエージング通知

パスワードエージング通知は、ユーザーが TACACS+ アカウント経由で Cisco MDS 9000 スイッチに認証すると開始されます。パスワードの期限切れが近い、または期限が切れたときは、ユーザーに通知されます。パスワードの期限が切れると、ユーザーはパスワードを変更するように求められます。



Note Cisco MDS SAN-OS Release 3.2(1) では、TACACS+ だけがパスワードエージング通知をサポートしています。この機能をイネーブルにして RADIUS サーバーを使用しようとする、RADIUS は SYSLOG メッセージを生成し、認証はローカル データベースにフォールバックします。

パスワードエージング通知により、次の操作が容易になります。

- パスワードの変更：空のパスワードを入力することによってパスワードを変更できます。
- パスワードエージング通知：パスワードエージングを通知します。通知は、AAA サーバーが構成され、MSCHAP および MSCHAPv2 がディセーブルになっている場合にだけ発生します。
- 期限切れ後のパスワードの変更：古いパスワードの期限が切れたら、パスワードの変更を開始します。AAA サーバーから開始します。



Note MSCHAP および MSCHAPv2 認証をディセーブルにしていない場合、パスワードエージング通知は失敗します。

AAA サーバーのパスワードエージング オプションをイネーブルにするには、次のコマンドを入力します。

```
aaa authentication login ascii-authentication
```

パスワードエージング通知を AAA サーバーで有効または無効になっているかどうかを確認するには、次のコマンドを入力します。

```
show aaa authentication login ascii-authentication
```

TACACS+ サーバーの検証の概要

Cisco SAN-OS リリース 3.0(1) では、TACACS+ サーバーを定期的に検証できます。スイッチは、設定されたテスト用ユーザー名とテスト用パスワードを使用してテスト用認証をサーバーに送信します。このテスト認証にサーバーが応答しない場合、サーバーは応答能力がないものと見なされます。



Note セキュリティ上の理由から、TACACS+ サーバーにはテスト用ユーザーを設定しないことを推奨します。

サーバーを定期的にテストするためにこのオプションを設定できるほか、1 回だけのテストを行うこともできます。

TACACS+ サーバーの定期的な検証

Fabric Manager を利用して TACACS+ サーバーを定期的にテストするようにスイッチを設定する手順は [TACACS+ サーバー モニタリング パラメータの設定, on page 84](#) の項を参照してください。

ユーザーによるログイン時の TACACS+ サーバー指定の概要

デフォルトでは、MDS スイッチは認証要求を TACACS+ サーバー グループの最初のサーバーに転送します。どの TACACS+ サーバーに認証要求を送信するかをユーザーが指定できるようにスイッチを設定できます。この機能をイネーブルにすると、ユーザーは `username@hostname` としてログインできます。 `hostname` は設定した TACACS+ サーバーの名前です。



Note ユーザー指定のログインは Telnet セッションに限りサポートされます

ユーザーによるログイン時の TACACS+ サーバ指定の許可

MDS スイッチにログインしているユーザーが認証用の TACACS+ サーバーを選択できるようにする手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **tacacs-server directed-request**

ログイン時に、ユーザーが認証要求の送信先となる TACACS+ サーバーを指定できるようにします。

ステップ 3 switch(config)# **no tacacs-server directed-request**

サーバー グループの最初のサーバーに認証要求を送信するように戻します (デフォルト)。

Example

TACACS+ への誘導要求設定を表示するには、**show tacacs-server directed-request** コマンドを使用できます。

```
switch# show tacacs-server directed-request
disabled
```

Cisco Secure ACS 5.x GUI でのロールの定義

ポリシー要素の GUI で次を入力します。

Table 5: ロールの定義

属性	要件	値
shell:roles	任意	network-admin

ロールのカスタム属性の定義

Cisco MDS 9000 ファミリ スイッチでは、ユーザーが所属するロールの設定には、サービス シェルの TACACS+ カスタム属性を使用します。TACACS+ 属性は **name=value** 形式で指定します。このカスタム属性の属性名は **cisco-av-pair** です。この属性を使用してロールを指定する例を次に示します。

```
cisco-av-pair=shell:roles="network-admin vsan-admin"
```

オプションのカスタム属性を設定して、同じ AAA サーバーを使用する MDS 以外のシスコ製スイッチとの競合を回避することもできます。

```
cisco-av-pair*shell:roles="network-admin vsan-admin"
```

追加カスタム属性 **shell:roles** もサポートされています。

```
shell:roles="network-admin vsan-admin"
OR
shell:roles*"network-admin vsan-admin"
```



Note TACACS+ カスタム属性は、Access Control Server (ACS) でさまざまなサービス (シェルなど) 用に定義できます。Cisco MDS 9000 ファミリ スイッチでは、サービス シェルの TACACS+ カスタム属性を使用して、ロールを定義する必要があります。

サポートされている TACACS+ サーバー パラメータ

Cisco NX-OS ソフトウェアでは現在、下記の TACACS+ サーバーに対して次のパラメータをサポートしています。

- TACACS+

```
cisco-av-pair=shell:roles="network-admin"
```

- Cisco ACS TACACS+

```
shell:roles="network-admin"
shell:roles*"network-admin"
cisco-av-pair*shell:roles="network-admin"
cisco-av-pair*shell:roles*"network-admin"
cisco-av-pair=shell:roles*"network-admin"
```

- Open TACACS+

```
cisco-av-pair*shell:roles="network-admin"
cisco-av-pair=shell:roles*"network-admin"
```

TACACS+ サーバーの詳細の表示

次の例で示すように、Cisco MDS 9000 ファミリ内のすべてのスイッチの TACACS+ サーバーの設定に関する情報を表示するには、**show aaa** および **show tacacs-server** コマンドを使用します。

TACACS+ サーバー情報の表示

```
switch# show tacacs-server

Global TACACS+ shared secret:*****
timeout value:30
total number of servers:3
following TACACS+ servers are configured:
  171.71.58.91:
    available on port:2
  cisco.com:
    available on port:49
  171.71.22.95:
    available on port:49
    TACACS+ shared secret:*****
```

AAA 認証情報の表示

```
switch# show aaa authentication

default: group TacServer local none
console: local
iscsi: local
dhchap: local
```

AAA 認証ログイン情報の表示

```
switch# show aaa authentication login error-enable

enabled
```

設定した TACACS+ サーバー グループの表示

```
switch# show tacacs-server groups

total number of groups:2
following TACACS+ server groups are configured:
  group TacServer:
    server 171.71.58.91 on port 2
  group TacacsServer1:
```

```
server ServerA on port 49
server ServerB on port 49:
```

すべての AAA サーバー グループの表示

```
switch# show aaa groups
```

```
radius
TacServer
```

TACACS+ サーバーの統計情報の表示

```
switch# show tacacs-server statistics 10.1.2.3
```

```
Server is not monitored
Authentication Statistics
  failed transactions: 0
  successful transactions: 0
  requests sent: 0
  requests timed out: 0
  responses with no matching requests: 0
  responses not processed: 0
  responses containing errors: 0
Authorization Statistics
  failed transactions: 0
  successful transactions: 0
  requests sent: 0
  requests timed out: 0
  responses with no matching requests: 0
  responses not processed: 0
  responses containing errors: 0
Accounting Statistics
  failed transactions: 0
  successful transactions: 0
  requests sent: 0
  requests timed out: 0
  responses with no matching requests: 0
  responses not processed: 0
  responses containing errors: 0
```

TACACS+ サーバ統計情報のクリア

`clear tacacs-server statistics 10.1.2.3` コマンドを使用してすべての TACACS+ サーバーの統計情報をクリアできます。

サーバー グループの設定

サーバー グループを使用して、1 台または複数台のリモート AAA サーバーによるユーザー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同じプロトコル (RADIUS または TACACS+) 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ーが試行されます。

AAA サーバー モニタリング機能は AAA サーバーを停止中としてマーク付けできます。スイッチが停止中の AAA サーバーに要求を送信するまでの経過時間を分で設定できます ([AAA サーバーのモニタリング](#), on page 42 の項を参照)。

このセクションは、次のトピックで構成されています。

RADIUS サーバー グループの設定概要

これらのサーバー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。AAA ポリシーは CLI ユーザー、または Fabric Manager ユーザーや Device Manager ユーザーに設定できます。

RADIUS サーバー グループを設定するには、次の手順を実行します。

Procedure

-
- ステップ 1** `switch# configure terminal`
コンフィギュレーションモードに入ります。
- ステップ 2** `switch(config)# aaa group server radius RadServer`
`switch(config-radius)#`
RadServer という名前の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。
- ステップ 3** `switch(config)# no aaa group server radius RadServer`
(オプション) 認証リストから RadServer という名前のサーバーグループを削除します。
- ステップ 4** `switch(config-radius)# server 10.71.58.91`
IPv4 アドレス 10.71.58.91 の RADIUS サーバーをサーバーグループ RadServer 内で最初に実行されるように設定します。
Tip 指定した RADIUS サーバーが見つからなかった場合は、`radius-server host` コマンドを使用してサーバーを設定し、このコマンドをもう一度実行します。
- ステップ 5** `switch(config-radius)# server 2001:0DB8:800:200C::417A`
IPv6 アドレス 2001:0DB8:800:200C::417A の RADIUS サーバーをサーバーグループ RadServer 内で最初に実行されるように設定します。
- ステップ 6** `switch(config-radius)# no server 2001:0DB8:800:200C::417A`
(オプション) IPv6 アドレス 2001:0DB8:800:200C::417A の RADIUS サーバーをサーバーグループ RadServer から削除します。
- ステップ 7** `switch(config-radius)# exit`
コンフィギュレーションモードに戻ります。
- ステップ 8** `switch(config)# aaa group server radius RadiusServer`
`switch(config-radius)#`

RadiusServer という名前のサーバー 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。

ステップ 9 switch(config-radius)# **server ServerA**

ServerA を RadiusServer1 と呼ばれるサーバー グループ内で最初に試行されるように設定します。

Tip 指定した RADIUS サーバーが見つからなかった場合は、**radius-server host** コマンドを使用してサーバーを設定し、このコマンドをもう一度実行します。

ステップ 10 switch(config-radius)# **server ServerB**

ServerB をサーバー グループ RadiusServer1 内で 2 番目に試行されるように設定します。

ステップ 11 switch(config-radius)# **deadtime 30**

モニタリングのデッドタイムを 30 分に設定します。指定できる範囲は 0 ～ 1440 です。

Note 個別の RADIUS サーバーのデッドタイムインターバルが 0 よりも大きい場合は、サーバー グループに設定された値よりもその値が優先されます。

ステップ 12 switch(config-radius)# **no deadtime 30**

(オプション) デフォルト値 (0 分) に戻します。

Note RADIUS サーバー グループおよび RADIUS サーバーの個別の TACACS+ サーバーの両方のデッドタイム間隔が 0 に設定されている場合、スイッチは定期モニタリングによって応答がないと判明した場合に RADIUS サーバーをデッドとしてマークしません。さらにスイッチは、その RADIUS サーバーに対するデッドサーバー モニタリングを実行しません。(RADIUS サーバー モニタリング パラメータの設定, on page 73 の項を参照)。

Example

設定されたサーバー グループ順序を確認するには、**show radius-server groups** コマンドを使用します。

```
switch# show radius-server groups
total number of groups:2
following RADIUS server groups are configured:
  group RadServer:
    server 10.71.58.91 on port 2
  group RadiusServer1:
    server ServerA on port 49
    server ServerB on port 49:
```

TACACS+ サーバー グループの設定概要

TACACS+ サーバー グループを設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **aaa group server tacacs+ TacacsServer1**

switch(config-tacacs+)#

TacacsServer1 という名前のサーバー グループを作成し、そのグループのサブモードを開始します。

ステップ 3 switch(config)# **no aaa group server tacacs+ TacacsServer1**

(オプション) 認証リストから TacacsServer1 という名前のサーバー グループを削除します。

ステップ 4 switch(config-tacacs+)# **server ServerA**

ServerA を TacacsServer1 と呼ばれるサーバー グループ内で最初に試行されるように設定します。

Tip 指定した TACACS+ サーバーが見つからなかった場合は、**tacacs-server host** コマンドを使用してサーバーを設定し、このコマンドをもう一度実行します。

ステップ 5 switch(config-tacacs+)# **server ServerB**

ServerB をサーバー グループ TacacsServer1 内で 2 番目に試行されるように設定します。

ステップ 6 switch(config-tacacs+)# **no server ServerB**

(オプション) サーバーの TacacsServer1 リスト内の ServerB を削除します。

ステップ 7 switch(config-tacacs+)# **deadtime 30**

モニタリングのデッドタイムを 30 分に設定します。指定できる範囲は 0 ~ 1440 です。

Note 個別の TACACS+ サーバーのデッド時間間隔が 0 よりも大きい場合は、サーバー グループに設定された値よりもその値が優先されます。

ステップ 8 switch(config-tacacs+)# **no deadtime 30**

(オプション) デフォルト値 (0 分) に戻します。

Note TACACS+ サーバー グループおよび TACACS+ サーバーの個別の TACACS+ サーバーの両方のデッドタイム間隔が 0 に設定されている場合、スイッチは定期モニタリングによって応答がないと判明した場合に TACACS+ サーバーをデッドとしてマークしません。さらにスイッチは、その TACACS+ サーバーに対するデッドサーバー モニタリングを実行しません。(TACACS+ サーバー モニタリング パラメータの設定, [on page 84](#)の項を参照)。

無応答サーバーのバイパス（回避）の概要

Cisco SAN-OS リリース 3.0(1) では、サーバー グループ内の無応答 AAA サーバーをバイパスできます。スイッチが無応答のサーバーを検出すると、ユーザーを認証する際にそのサーバーをバイパスします。この機能を利用すると、障害を起こしたサーバーが引き起こすログインの遅延を最小限にとどめることができます。無応答サーバーに要求を送信し、認証要求がタイムアウトするまで待つのではなく、スイッチはサーバー グループ内の次のサーバーに認証要求を送信します。サーバー グループに応答できる他のサーバーが存在しない場合は、スイッチは無応答サーバーに対して認証を試み続けます。

AAA サーバーへの配信

MDS スイッチの RADIUS および TACACS+ の AAA 設定は、Cisco Fabric Services (CFS) を使用して配信できます。配信はデフォルトで無効になっています（『Cisco MDS 9000 Family NX-OS System Management Configuration Guide』および『Cisco Fabric Manager System Management Configuration Guide』を参照）。

配信をイネーブルにすると、最初のサーバーまたはグローバル設定により、暗黙のセッションが開始されます。それ以降に入力されたすべてのサーバー コンフィギュレーション コマンドは、一時的なデータベースに保管され、データベースをコミットしたときに、ファブリック内のすべてのスイッチ（送信元スイッチを含む）に適用されます。サーバー キーおよびグローバル キーを除く、さまざまなサーバーおよびグローバル パラメータが配信されます。サーバー キーおよびグローバル キーはスイッチに対する固有の秘密キーです。他のスイッチと共有しないでください。



Note サーバー グループ設定は配信されません。

この項では、次のトピックについて取り上げます。



Note AAA サーバー設定配布を行う MDS スイッチは、Cisco MDS SAN-OS Release 2.0(1b) 以降または Cisco NX-OS Release 4.1(1) を実行する必要があります。

AAA RADIUS サーバーへの配信のイネーブル化

アクティビティに参加できるのは、配信がイネーブルであるスイッチだけです。

RADIUS サーバーでの配信をイネーブルにする手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **radius distribute**

このスイッチの RADIUS 設定の配信をイネーブルにします。

ステップ 3 switch(config)# **no radius distribute**

(オプション) このスイッチの RADIUS 設定の配信をディセーブル (デフォルト) にします。

AAA TACACS+ サーバーへの配信のイネーブル化

TACACS+ サーバーでの配信をイネーブルにする手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **tacacs+ distribute**

このスイッチの TACACS+ 設定の配信をイネーブルにします。

ステップ 3 switch(config)# **no tacacs+ distribute**

(オプション) このスイッチの TACACS+ 設定の配信をディセーブル (デフォルト) にします。

スイッチでの配信セッションの開始

配信セッションは RADIUS/TACACS+ サーバーの設定またはグローバル設定を開始した瞬間に始まります。たとえば、次の作業を実行すると、暗黙のセッションが開始されます。

- RADIUS サーバーのグローバル タイムアウトの指定
- TACACS+ サーバーのグローバル タイムアウトの指定



Note AAA サーバーに関連する最初のコンフィギュレーションコマンドを発行すると、作成されたすべてのサーバーおよびグローバル設定（配信セッションを開始する設定を含む）が一時バッファに格納されます。実行コンフィギュレーションには格納されません。

セッションステータスの表示

暗黙の配信セッションが開始すると、Fabric Manager から [Switches] > [Security] > [AAA] を開いて [RADIUS] または [TACACS+] を選択することで、セッションの状況を確認できます。

show radius コマンドを使用して CFS タブに **distribution status** を表示します。

```
switch# show radius distribution status

distribution : enabled
session ongoing: yes
session owner: admin
session db: exists
merge protocol status: merge activation done
last operation: enable
last operation status: success
```

暗黙的な配信セッションが開始されると、**show tacacs+ distribution status** コマンドを使用してセッションステータスを確認できます。

```
switch# show tacacs+ distribution status

distribution : enabled
session ongoing: yes
session owner: admin
session db: exists
merge protocol status: merge activation done
last operation: enable
last operation status: success
```

配信する保留中の設定の表示

一時バッファに保存された RADIUS または TACACS+ のグローバル設定またはサーバー設定を、**show radius pending** コマンドを使用して表示する手順は次のとおりです。

```
switch(config)# show radius pending-diff

+radius-server host testhost1 authentication accounting
+radius-server host testhost2 authentication accounting
```

一時バッファに保存された TACACS+ のグローバル設定またはサーバー設定を表示するには、**show tacacs+ pending** コマンドを使用します。

```
switch(config)# show tacacs+ pending-diff

+tacacs-server host testhost3
+tacacs-server host testhost4
```

RADIUS 情報の配布のコミット

一時バッファに格納された RADIUS または TACACS+ グローバル設定またはサーバー設定を、ファブリック内のすべてのスイッチ（送信元スイッチを含む）の実行コンフィギュレーションに適用できます。

RADIUS の設定変更をコミットするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **radius commit**

実行コンフィギュレーションへの RADIUS の設定変更をコミットします。

TACACS+ 情報の配信のコミット

TACACS+ の設定変更をコミットするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **tacacs+ commit**

実行コンフィギュレーションへの TACACS+ の設定変更をコミットします。

RADIUS の配布セッションの廃棄

進行中のセッションの配信を廃棄すると、一時バッファ内の設定が廃棄されます。廃棄された配信は適用されません。

RADIUS セッションの進行中の配信を廃棄する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# radius abort

実行コンフィギュレーションへの RADIUS の設定変更を破棄します。

TACACS+ の配布セッションの廃棄

TACACS+ セッションの進行中の配信を廃棄する手順は、次のとおりです。

Procedure

ステップ 1 switch# configure terminal

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# tacacs+ abort

実行コンフィギュレーションへの TACACS+ の設定変更を破棄します。

セッションのクリア

継続的な CFS 配信セッション（ある場合）をクリアし、RADIUS 機能のファブリックを最大限に引き出すには、ファブリック内のすべてのスイッチから **clear radius session** コマンドを入力します。

```
switch# clear radius session
```

継続的な CFS 配信セッション（ある場合）をクリアし、TACACS+ 機能のファブリックを最大限に引き出すには、ファブリック内のすべてのスイッチから **clear tacacs+ session** コマンドを入力します。

```
switch# clear tacacs+ session
```

RADIUS および TACACS+ 設定のマージに関する注意事項

RADIUS および TACACS+ のサーバー設定およびグローバル設定は 2 つのファブリックがマージするときにマージされます。マージされた設定は CFS 配信がイネーブルであるスイッチに適用されます。

ファブリックのマージの際は次の条件に注意してください。

- サーバー グループはマージされません。
- サーバー キーおよびグローバル キーはマージ中に変更されません。

- マージされた設定には、CFS がイネーブルであるすべてのスイッチで見つかったすべてのサーバーが含まれます。
- マージされた設定におけるタイムアウトと再送信のパラメータは、個々のサーバー設定とグローバル設定に指定されている値の最大値になります。



Note テスト パラメータは、CFS を通じて、TACACS+ デーモンのためだけに配信されます。ファブリックに NX-OS リリース 5.0 スイッチだけが含まれる場合、テスト パラメータは配信されます。5.0 バージョンを実行しているスイッチと NX-OS 4.x リリースを実行しているスイッチがファブリックに含まれる場合、テスト パラメータは配信されません。



Caution 設定されたサーバー ポートの 2 つのスイッチの間で矛盾が存在する場合は、マージに失敗します。

show radius distribution status コマンドを使用して、次の例のように RADIUS ファブリックのマージのステータスを参照できます。

RADIUS ファブリックのマージのステータスの表示

```
switch# show radius distribution status

distribution : enabled
session ongoing: no
session db: does not exist
merge protocol status: merge response received
merge error: conflict: server dmttest2 has auth-port 1812 on this switch and 1999
on remote
last operation: enable
last operation status: success
```

TACACS+ ファブリックのマージのステータスの表示

show tacacs+ distribution status コマンドを使用して、次の例のように TACACS+ ファブリックのマージのステータスを参照できます。

```
switch# show tacacs+ distribution status

distribution : enabled
session ongoing: no
session db: does not exist
merge protocol status: merge activation done
last operation: enable
last operation status: success
```


CHAP 認証

CHAP (チャレンジハンドシェイク認証プロトコル) は、業界標準の Message Digest 5 (MD5) ハッシングスキームを使用して応答を暗号化するチャレンジレスポンス認証プロトコルです。CHAP は、さまざまなネットワーク アクセス サーバーおよびクライアントのベンダーによって使用されています。ルーティングおよびリモートアクセスを実行しているサーバーは、CHAP を必要とするリモート アクセス クライアントが認証されるように、CHAP をサポートしています。このリリースでは、認証方式として CHAP がサポートされています。

CHAP 認証の有効化

CHAP 認証を有効にするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **aaa authentication login chap enable**

CHAP ログイン認証をイネーブルにします。

ステップ 3 switch# **no aaa authentication login chap enable**

(オプション) CHAP ログイン認証をディセーブルにします。

Example

CHAP 認証の設定を表示するには、**show aaa authentication login chap** コマンドを使用できます。

```
switch# show aaa authentication login chap
chap is disabled
```

MSCHAP による認証

マイクロソフトチャレンジハンドシェイク認証プロトコル (MSCHAP) は、マイクロソフト版の CHAP です。

Cisco MDS 9000 ファミリー スイッチのユーザー ログインでは、異なるバージョンの MSCHAP を使用してリモート認証を実行できます。MSCHAP は RADIUS サーバーまたは TACACS+ サーバーでの認証に使用され、MSCHAPv2 は RADIUS サーバーでの認証に使用されます。

MSCHAP のイネーブル化の概要

デフォルトでは、スイッチ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 をイネーブルにする場合は、MSCHAP の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。[ベンダー固有属性の概要, on page 78](#)を参照してください。次の表に MSCHAP に必要な RADIUS ベンダー固有属性を示します。

Table 6: MSCHAP 用の RADIUS ベンダー固有属性

ベンダー ID 番号	ベンダータイプ番号	ベンダー固有属性	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	MS-CHAP ユーザーがチャレンジへの応答として提供したレスポンス値が格納されます。Access-Request パケットでしか使用されません。

MSCHAP 認証のイネーブル化

MSCHAP 認証をイネーブルにするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **aaa authentication login mschap enable**

MSCHAP ログイン認証をイネーブルにします。

ステップ 3 switch# **no aaa authentication login mschap enable**

(オプション) MSCHAP ログイン認証をディセーブルにします。

MSCHAPv2 認証のイネーブル化

MSCHAPv2 認証をイネーブルにするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **aaa authentication login mschapv2 enable**

MSCHAPv2 ログイン認証をイネーブルにします。

ステップ 3 switch# **no aaa authentication login mschapv2 enable**

(オプション) MSCHAPv2 ログイン認証をディセーブルにします。

Example



Note

- パスワードエージング、MSCHAPv2、およびMSCHAP 認証は、これらの認証のいずれかがディセーブルでないと失敗する可能性があります。
- TACACS+ サーバーで MSCHAPv2 認証をイネーブルにするコマンドを実行すると、警告メッセージが表示され、設定が失敗します。

MSCHAP 認証の設定を表示するには、**show aaa authentication login mschap** コマンドを使用できます。

```
switch# show aaa authentication login mschap  
  
mschap is disabled
```

MSCHAPv2 認証の設定を表示するには、**show aaa authentication login mschapv2** コマンドを使用できます。

```
switch# show aaa authentication login mschapv2  
  
mschapv2 is enabled
```

ローカル AAA サービス

システムによりユーザー名およびパスワードはローカルで保持され、パスワード情報は暗号化形式で格納されます。ユーザーの認証は、ローカルに保存されているユーザー情報に基づいて実行されます。

ローカルユーザーとそのロールを設定するには、**username** コマンドを使用します。

ローカル アカウンティング ログを表示するには、次の例のように **show accounting log** コマンドを使用します。

アカウンティング ログ情報の表示

```
switch# show accounting log

Thu Dec 10 06:19:21 2009:type=update:id=console0:user=root:cmd=enabled telnet
Thu Dec 10 06:19:21 2009:type=update:id=console0:user=root:cmd=configure terminal ;
feature telnet
(SUCCESS)
Thu Dec 10 06:19:35 2009:type=start:id=171.69.16.56@pts/1:user=admin:cmd=
Thu Dec 10 06:20:16 2009:type=stop:id=171.69.16.56@pts/1:user=admin:cmd=shell te
rminated gracefully
Thu Dec 10 06:20:20 2009:type=stop:id=console0:user=root:cmd=shell terminated gr
acefully
Thu Dec 10 06:29:37 2009:type=start:id=72.163.177.168@pts/1:user=admin:cmd=
Thu Dec 10 06:29:42 2009:type=update:id=72.163.177.168@pts/1:user=admin:cmd=pwd
(SUCCESS)
Thu Dec 10 06:32:49 2009:type=start:id=72.163.190.8@pts/2:user=admin:cmd=
```

AAA 認証のディセーブル化

none オプションを利用するとパスワード確認をオフにできます。このオプションを設定すると、ユーザーは有効なパスワードを提示しなくてもログインできます。ただし、ユーザーは少なくとも Cisco MDS 9000 Family スイッチ上のローカルユーザーである必要があります。



Caution このオプションは注意して使用してください。このオプションを設定すると、あらゆるユーザーがいつでもスイッチにアクセスできるようになります。

このオプションの設定手順については、『*Cisco MDS 9000 Family NX-OS Configuration Guide*』を参照してください。

パスワード確認をディセーブルにするには、**aaa authentication login** コマンドで **none** オプションを使用します。

username コマンドを入力して作成したユーザーは、Cisco MDS 9000 ファミリー スイッチのローカルに存在します。

AAA 認証の表示

show aaa authentication コマンドでは、設定された認証方式が次の例のように表示されます。

認証情報の表示

```
switch# show aaa authentication

No AAA Authentication
default: group TacServer local none
console: local none
```

```
iscsi: local
dhchap: local
```

アカウントング サービスの設定

アカウントングは、スイッチの管理セッションごとに保管されるログ情報を意味しています。この情報はトラブルシューティングと監査を目的としたレポートの生成に利用できます。アカウントングは、(RADIUS を使用して) ローカルまたはリモートで実装できます。アカウントング ログのデフォルトの最大サイズは 250,000 バイトです。これは変更できません。



Tip Cisco MDS 9000 ファミリー スイッチは、interim-update RADIUS アカウントング要求パケットを使用して、アカウントング ログ情報を RADIUS サーバーに送信します。RADIUS サーバーは、これらのパケットで送信された情報を記録するように、適切に設定されている必要があります。一部のサーバーは、通常、AAA クライアントの設定内に `log update/watchdog packets` フラグを持ちます。適切な RADIUS アカウントングを確実に実行するには、このフラグをオンにします。



Note コンフィギュレーション モードで実行された設定操作は、自動的にアカウントング ログに記録されます。重要なシステム イベント (設定保存やシステム スイッチオーバーなど) もアカウントング ログに記録されます。

アカウントング設定の表示

設定したアカウント情報を表示するには `show accounting` コマンドを使用します。次の例を参照してください。表示されるローカルアカウントング ログのサイズを指定するには、`show accounting log` コマンドを使用します。デフォルトでは、アカウントング ログの約 250 KB が表示されます。

設定されたアカウントングパラメータの2つの例の表示

```
switch# show accounting config
```

```
show aaa accounting
default: local
```

```
switch# show aaa accounting
```

```
default: group rad1
```

60,000 バイトのアカウントング ログの表示

```
switch# show accounting log 60000
```

```
Fri Jan 16 15:28:21 1981:stop:snmp_348506901_64.104.131.208:admin:
```

```

Fri Jan 16 21:17:04 1981:start:/dev/pts/0_348527824:admin:
Fri Jan 16 21:35:45 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
Fri Jan 16 21:35:51 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
Fri Jan 16 21:35:51 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group5
Fri Jan 16 21:35:55 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group5
Fri Jan 16 21:35:55 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group3
Fri Jan 16 21:58:17 1981:start:snmp_348530297_171.71.150.105:admin:
...

```

ログ ファイル全体の表示

```
switch# show accounting log
```

```

Fri Jan 16 15:28:21 1981:stop:snmp_348506901_64.104.131.208:admin:
Fri Jan 16 21:17:04 1981:start:/dev/pts/0_348527824:admin:
Fri Jan 16 21:35:45 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
Fri Jan 16 21:35:51 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
Fri Jan 16 21:35:51 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group5
Fri Jan 16 21:35:55 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group5
Fri Jan 16 21:35:55 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group3
Fri Jan 16 21:58:17 1981:start:snmp_348530297_171.71.150.105:admin:
Fri Jan 16 21:58:17 1981:stop:snmp_348530297_171.71.150.105:admin:
Fri Jan 16 21:58:18 1981:start:snmp_348530298_171.71.150.105:admin:
Fri Jan 16 21:58:18 1981:stop:snmp_348530298_171.71.150.105:admin:
...
Fri Jan 16 23:37:02 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group3
Fri Jan 16 23:37:26 1981:update:/dev/pts/0_348527824:admin:updated TACACS+ parameters
for group:TacacsServer1
Fri Jan 16 23:45:19 1981:update:/dev/pts/0_348527824:admin:updated TACACS+ parameters
for group:TacacsServer1
Fri Jan 16 23:45:19 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
...
Fri Jan 16 23:53:51 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
server:Server3
Fri Jan 16 23:54:00 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
server:Server5
Fri Jan 16 23:54:22 1981:update:/dev/pts/0_348527824:admin:updated TACACS+ parameters
for server:ServerA
Fri Jan 16 23:54:25 1981:update:/dev/pts/0_348527824:admin:updated TACACS+ parameters
for server:ServerB
Fri Jan 16 23:55:03 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
...
Sat Jan 17 00:01:41 1981:start:snmp_348537701_171.71.58.100:admin:
Sat Jan 17 00:01:41 1981:stop:snmp_348537701_171.71.58.100:admin:
Sat Jan 17 00:01:42 1981:start:snmp_348537702_171.71.58.100:admin:
Sat Jan 17 00:01:42 1981:stop:snmp_348537702_171.71.58.100:admin:
...

```

アカウントログのクリア

現在のログの内容を消去するには、**clear accounting log** コマンドを使用します。

```
switch# clear accounting log
```

Cisco Access Control Servers の設定

Cisco Access Control Server (ACS) は TACACS+ と RADIUS のプロトコルを利用して、セキュアな環境を作り出す AAA サービスを提供します。AAA サーバーを使用する際のユーザー管理は、通常 Cisco ACS を使用して行われます。Figure 4: RADIUS を使用する場合の **network-admin** ロールの設定, on page 113、Figure 5: RADIUS を使用する場合の SNMPv3 属性を持つ複数ロールの設定, on page 114、Figure 6: TACACS+ を使用する場合の SNMPv3 属性を持つ **network-admin** ロールの設定, on page 115、Figure 7: TACACS+ を使用する場合の SNMPv3 属性を持つ複数ロールの設定, on page 116 に、RADIUS または TACACS+ のいずれかを使用した際の **network-admin** ロールと複数のロールの ACS サーバーのユーザー セットアップ構成を示します。

Figure 4: RADIUS を使用する場合の **network-admin** ロールの設定

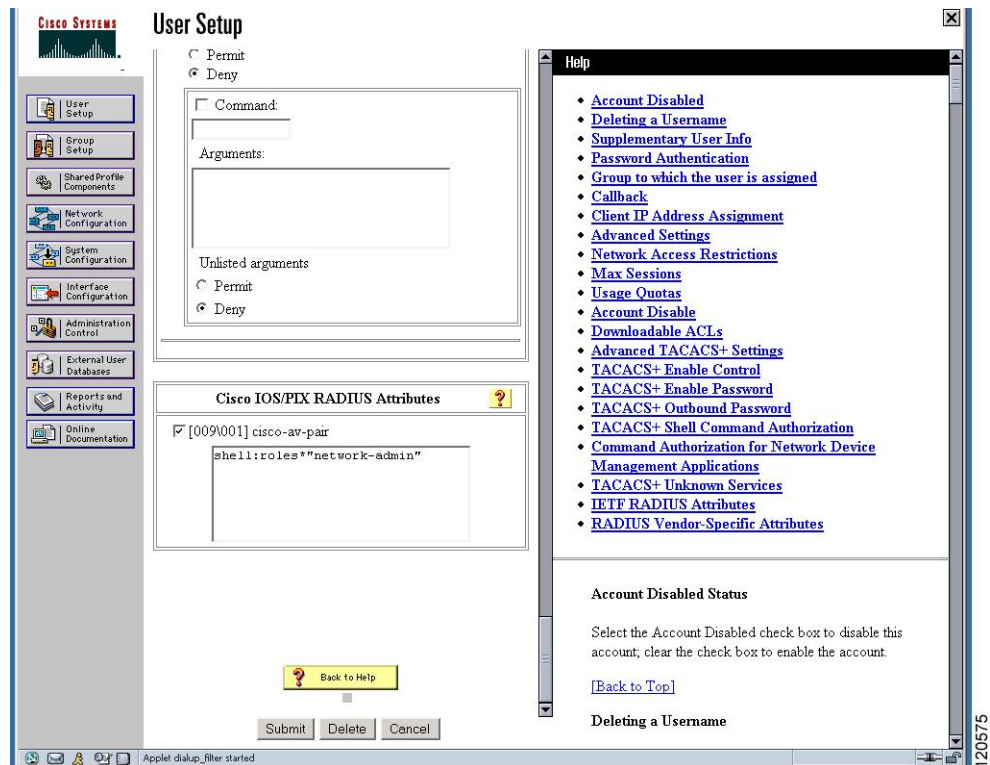


Figure 5: RADIUS を使用する場合の SNMPv3 属性を持つ複数ロールの設定

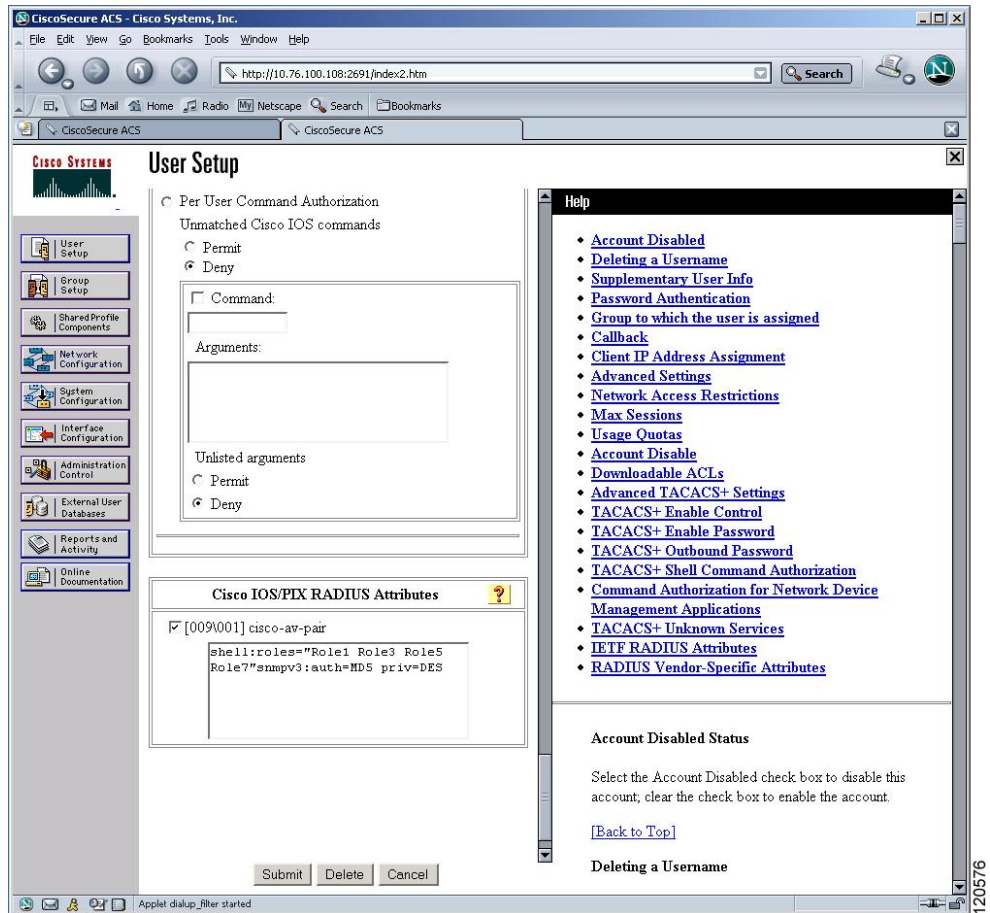


Figure 6: TACACS+ を使用する場合の SNMPv3 属性を持つ network-admin ロールの設定

User Setup

TACACS+ Settings

PPP IP

In access control list

Out access control list

Route

Routing Enabled

Custom attributes

Note: PPP LCP will be automatically enabled if this service is enabled

Shell (exec)

Access control list

Auto command

Callback line

Callback rotary

Idle time

No callback verify Enabled

No escape Enabled

No hangup Enabled

Privilege level

Timeout

Custom attributes

```
cisco-sv-pair=shell:roles=Role1
Role3 snmpv3:auth=MDS |priv=DES
```

Submit Delete Cancel

Help

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Downloadable ACLs
- Advanced TACACS+ Settings
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IETF RADIUS Attributes
- RADIUS Vendor-Specific Attributes

Account Disabled Status

Select the Account Disabled check box to disable this account; clear the check box to enable the account.

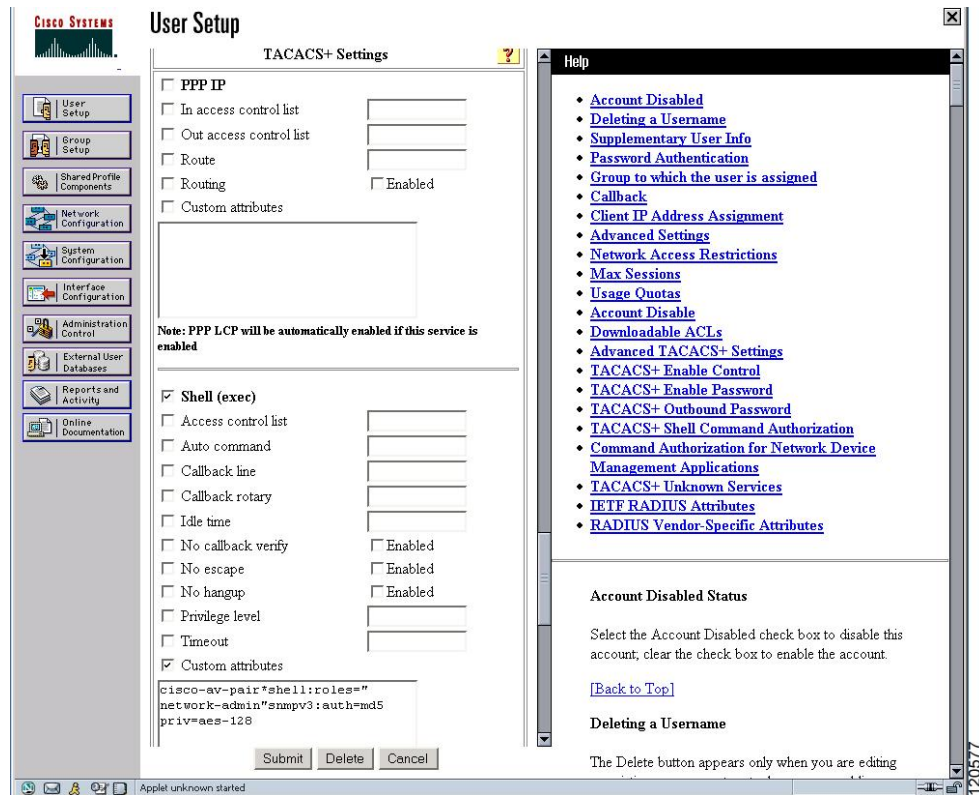
[\[Back to Top\]](#)

Deleting a Username

The Delete button appears only when you are editing an

120578

Figure 7: TACACS+ を使用する場合の SNMPv3 属性を持つ複数ロールの設定



デフォルト設定

次の表に、任意のスイッチにおけるすべてのスイッチセキュリティ機能のデフォルト設定を示します。

Table 7: スイッチセキュリティのデフォルト設定

パラメータ	デフォルト
Cisco MDS スイッチでのロール	ネットワーク オペレータ (network-operator)
AAA 設定サービス	ローカル
認証ポート	1812
アカウンティング ポート	1813
事前共有キーの送受信	クリア テキスト
RADIUS サーバーのタイムアウト	1 秒
RADIUS サーバー再試行	1 回

パラメータ	デフォルト
許可	ディセーブル
デフォルトの AAA ユーザー ロール	enabled
RADIUS サーバーへの誘導要求	ディセーブル
TACACS+	ディセーブル
TACACS+ サーバー	未設定
TACACS+ サーバーのタイムアウト	5 秒
TACACS+ サーバーへの誘導要求	ディセーブル
AAA サーバーへの配信	ディセーブル
アカウントिंग ログ サイズ	250 KB



第 6 章

IPv4 および IPv6 のアクセスコントロールリストの設定

Cisco MDS 9000 シリーズ スイッチ製品は、イーサネットとファイバチャネルインターフェイスの間で IP バージョン 4 (IPv4) トラフィックをルーティングできます。IP スタティックルーティング機能が VSAN 間のトラフィックをルーティングします。これを行うためには、各 VSAN が異なる IPv4 サブネットワークに属していなければなりません。各 Cisco MDS 9000 シリーズスイッチは、ネットワーク管理システム (NMS) に対して次のサービスを提供します。

- スーパーバイザ モジュールの前面パネルにある帯域外イーサネット インターフェイス (mgmt0) での IP 転送
- IP over Fibre Channel (IPFC) 機能を使用したインバンドファイバチャネルインターフェイス上の IP 転送 : IPFC は、IP フレームをカプセル化手法を利用してファイバチャネル上で転送するための方法を定義しています。IP フレームはファイバチャネルフレームにカプセル化されるため、オーバーレイイーサネットネットワークを使用しなくても、ファイバチャネルネットワーク上で NMS 情報を伝達できます。
- IP ルーティング (デフォルトルーティングおよびスタティックルーティング) : 外部ルータを必要としない設定の場合は、スタティックルーティングを使用してデフォルトルートを設定できます。

スイッチは仮想ルータ冗長プロトコル (VRRP) 機能の RFC 2338 標準に準拠します。VRRP は、冗長な代替パスをゲートウェイスイッチに提供する、再起動可能なアプリケーションです。

IPv4 アクセスコントロールリスト (IPv4-ACL および IPv6-ACL) は、すべての Cisco MDS 9000 シリーズスイッチに基本的なネットワークセキュリティを提供します。IPv4-ACL および IPv6-ACL は、設定された IP フィルタに基づいて IP 関連トラフィックを規制します。フィルタには IP パケットと一致させる規則が含まれています。パケットが一致すると、規則に基づいてパケットの許可または拒否が判別されます。

Cisco MDS 9000 シリーズの各スイッチには合計最大 128 の IPv4-ACL または 128 の IPv6-ACL を設定でき、各 IPv4-ACL または IPv6-ACL に最大 256 のフィルタを設定できます。

この章は、次の項で構成されています。

- IPv4 および IPv6 のアクセス コントロール リストの概要, on page 120
- IPv4-ACL および IPv6-ACL 設定に関する考慮事項, on page 121
- フィルタの内容について, on page 121
- IPv4-ACL または IPv6-ACL の作成, on page 125
- IPv4-ACL の作成, on page 125
- IPv6-ACL の作成 (126 ページ)
- IPv4-ACL の定義 (127 ページ)
- IPv6-ACL の定義 (127 ページ)
- IPv4-ACL のオペラントとポートのオプション (128 ページ)
- IPv6-ACL のオペラントとポートのオプション (128 ページ)
- 既存の IPv4-ACL への IP フィルタの追加, on page 129
- 既存の IPv6-ACL への IP フィルタの追加, on page 129
- 既存の IPv4-ACL からの IP フィルタの削除, on page 130
- 既存の IPv6-ACL からの IP フィルタの削除, on page 130
- IPv4-ACL または IPv6-ACL の設定の確認 (131 ページ)
- IP-ACL ログ ダンプの読み取り, on page 132
- インターフェイスへの IP-ACL の適用, on page 133
- インターフェイスへの IPv6-ACL の適用, on page 135
- mgmt0 への IP-ACL の適用, on page 135
- Open IP Ports on Cisco MDS 9000 Series Platforms, on page 137
- IP-ACL カウンタのクリーンアップ, on page 138

IPv4 および IPv6 のアクセス コントロール リストの概要

Cisco MDS 9000 ファミリー スイッチ製品は、イーサネットとファイバチャネルインターフェイスの間でIPバージョン4 (IPv4) トラフィックをルーティングできます。IP スタティックルーティング機能が VSAN 間のトラフィックをルーティングします。これを行うためには、各 VSAN が異なる IPv4 サブネットワークに属していなければなりません。各 Cisco MDS 9000 ファミリー スイッチは、ネットワーク管理システム (NMS) に対して次のサービスを提供します。

- スーパーバイザ モジュールの前面パネルにある帯域外イーサネット インターフェイス (mgmt0) での IP 転送
- IP over Fibre Channel (IPFC) 機能を使用したインバンドファイバチャネルインターフェイス上の IP 転送 : IPFC は、IP フレームをカプセル化手法を利用してファイバチャネル上で転送するための方法を定義しています。IP フレームはファイバチャネルフレームにカプセル化されるため、オーバーレイ イーサネット ネットワークを使用しなくても、ファイバチャネル ネットワーク上で NMS 情報を伝達できます。
- IP ルーティング (デフォルトルーティングおよびスタティックルーティング) : 外部ルータを必要としない設定の場合は、スタティック ルーティングを使用してデフォルト ルートを設定できます。

IPv4 アクセス コントロール リスト (IPv4-ACL および IPv6-ACL) は、すべての Cisco MDS 9000 ファミリスイッチに基本的なネットワークセキュリティを提供します。IPv4-ACL および IPv6-ACL は、設定された IP フィルタに基づいて IP 関連トラフィックを規制します。フィルタには IP パケットと一致させる規則が含まれています。パケットが一致すると、規則に基づいてパケットの許可または拒否が判別されます。

Cisco MDS 9000 ファミリの各スイッチには合計最大 128 の IPv4-ACL または 128 の IPv6-ACL を設定でき、各 IPv4-ACL または IPv6-ACL に最大 256 のフィルタを設定できます。

IPv4-ACL および IPv6-ACL 設定に関する考慮事項

Cisco MDS 9000 ファミリのスイッチまたはディレクタに IPv4-ACL または IPv6-ACL を設定する場合は、次の注意事項に従ってください。

- IPv4-ACL または IPv6-ACL は、VSAN インターフェイス、管理インターフェイス、IPS モジュールおよび MPS-14/2 モジュール上のギガビットイーサネット、およびイーサネットポートチャネルインターフェイスに適用できます。



Caution

ギガビットイーサネットインターフェイスに IPv4-ACL または IPv6-ACL がすでに設定されている場合は、このインターフェイスをイーサネットポートチャネルグループに追加できません。IPv4-ACL または IPv6-ACL は、ポートチャネルグループ内の 1 つのメンバーだけに適用しないでください。IPv4-ACL または IPv6-ACL はチャネルグループ全体に適用します。

- 条件の順序は正確に設定してください。IPv4-ACL または IPv6-ACL フィルタは IP フローに順番に適用されるので、最初の一致によって動作が決定されます。以降の一致は考慮されません。最も重要な条件を最初に設定してください。いずれの条件とも一致しなかった場合、パケットは廃棄されます。
- IP ACL を適用する IP ストレージのギガビットイーサネットポートでは、暗黙的な deny は有効にならないため、明示的な deny を設定してください。

フィルタの内容について

IP フィルタには、プロトコル、アドレス、ポート、ICMP タイプ、およびサービスタイプ (TS) に基づく IP パケットの一致規則が含まれます。

このセクションは、次のトピックで構成されています。

プロトコル情報

各フィルタには、プロトコル情報が必要です。この情報により、IP プロトコルの名前または番号を識別します。IP プロトコルは、次のいずれかの方法で指定できます。

- 0 ~ 255 の整数を指定します。この番号は IP プロトコルを表します。
- プロトコルの名前を指定しますが、インターネットプロトコル (IP)、伝送制御プロトコル (TCP)、ユーザーデータグラムプロトコル (UDP)、および Internet Control Message Protocol (ICMP) には限定されません。



Note ギガビットイーサネットインターフェイスに IPv4-ACL または IPv6-ACL を設定する場合は、TCP または ICMP オプションだけを使用してください。

アドレス情報

各フィルタには、アドレス情報が必要です。アドレス情報により、次の詳細を識別します。

- 送信元：パケット送信元のネットワークまたはホストのアドレス
- 送信元ワイルドカード：送信元に適用されるワイルドカードビット
- 宛先：パケットの送信先となるネットワークまたはホストの番号
- 宛先ワイルドカード：宛先に適用されるワイルドカードビット

送信元/送信元ワイルドカードおよび宛先/宛先ワイルドカードは、次のいずれかの方法で指定します。

- 4 つに区切られたドット付き 10 進表記の 32 ビット数を使用します (10.1.1.2/0.0.0.0 はホスト 10.1.1.2 と同じ)。
 - 各ワイルドカードビットをゼロに設定する場合には、パケットの IPv4 アドレス内の対応するビット位置と送信元の対応するビット位置で、ビット値が正確に一致している必要があります。
 - 各ワイルドカードビットを 1 に設定する場合は、パケットの IPv4 または IPv6 アドレス内の対応する位置のビット値が 0 および 1 のいずれであっても、現在のアクセスリストエントリと一致すると見なされます。無視するビット位置に 1 を入れます。たとえば、0.0.255.255 の場合、送信元の最初の 16 ビットだけが完全に一致する必要があります。複数のワイルドカードビットを 1 に設定する場合、これらのビットが送信元ワイルドカード内で連続している必要はありません。たとえば、送信元ワイルドカード 0.255.0.64 は有効です。
- 送信元/送信元ワイルドカードまたは宛先/宛先ワイルドカード (0.0.0.0/255.255.255.255) の短縮形として、**any** オプションを使用します。

ポート情報

ポート情報はオプションです。送信元ポートと宛先ポートを比較するためには、**eq**（等号）オプション、**gt**（より大きい）オプション、**lt**（より小さい）オプション、または**range**（ポート範囲）オプションを使用します。ポート情報は次のいずれかの方法で指定できます。

- ポート番号を指定します。ポート番号の範囲は0～65535です。次の表に、関連TCPポートおよびUDPポートについて、Cisco NX-OS ソフトウェアが認識するポート番号を示します。
- TCP または UDP ポートの名前を次のように指定します。
 - TCP ポート名は、TCP をフィルタリングする場合にかぎって使用できます。
 - UDP ポート名は、UDP をフィルタリングする場合にかぎって使用できます。

Table 8: TCP および UDP のポート番号

プロトコル	ポート	番号
UDP	dns	53
	dhcps	67
	tftp	69
	rpcbind	111
	ntp	123
	radius アカウンティング	1646 または 1813
	radius 認証	1645 または 1812
	snmp	161
	snmp-trap	162
	syslog	514
	nfs	2049

プロトコル	ポート	番号
TCP ¹	ftp	20
	ftp-data	21
	ssh	22
	Telnet	23
	smtp	25
	tasacs-ds	65
	www	80
	sftp	115
	http	143
	セキュアではない LDAP	389
	https	443
	セキュア LDAP	636
	wbem-http	5988
	wbem-https	5989

¹ コネクションが確立済みの場合は、established オプションを使用して適合するものを探してください。TCP データグラムが ACK、FIN、PSH、RST または URG のコントロールビットセットを持つ場合は、適合と見なされます。

ICMP 情報

オプションとして IP パケットは次の ICMP 条件に基づいて選別できます。

- icmp-type : ICMP メッセージタイプは 0 から 255 の番号から 1 つ選びます。
- icmp-code : ICMP メッセージコードは 0 から 255 の番号から 1 つ選びます。

次の表に各 ICMP タイプの値を示します。

Table 9: ICMP タイプの値

ICMP タイプ ²	コード
echo	8
echo-reply	0
destination unreachable	3

ICMP タイプ ²	コード
traceroute	30
time exceeded	11

² ICMP リダイレクト パケットは必ず拒否されます。

ToS 情報

オプションとして IP パケットは次の ToS 条件に基づいて選別できます。

- ToS レベル：レベルは 0 から 15 の番号で指定します。
- ToS 名：max-reliability、max-throughput、min-delay、min-monetary-cost、および normal から選択できます。

IPv4-ACL または IPv6-ACL の作成

スイッチに入ったトラフィックは、スイッチ内でフィルタが現れる順番に従って IPv4-ACL または IPv6-ACL のフィルタと比較されます。新しいフィルタは IPv4-ACL または IPv6-ACL の末尾に追加されます。スイッチは合致するまで照合を続けます。フィルタの最後に達して合致するものがなかった場合、そのトラフィックは拒否されます。そのため、フィルタの最上部にはヒットする確率の高いフィルタを置く必要があります。許可されないトラフィックに対して、*implied deny* が用意されています。1つの拒否エントリしか持たないシングルエントリの IPv4-ACL または IPv6-ACL には、すべてのトラフィックを拒否する効果があります。

IPv4-ACL または IPv6-ACL を設定する手順は次のとおりです。

Procedure

ステップ 1 IPv4-ACL または IPv6-ACL の作成には、フィルタ名と 1 つ以上のアクセス条件を指定します。フィルタには、条件に合致する発信元と宛先のアドレスが必要です。適切な粒度を設定するために、オプションのキーワードを使用できます。

Note フィルタのエントリは順番に実行されます。エントリは、リストの最後にだけ追加できます。正しい順番でエントリを追加するように注意してください。

ステップ 2 指定したインターフェイスにアクセス フィルタを適用します。

IPv4-ACL の作成

IPv4-ACL を作成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **ip access-list List1 permit ip any any**

List1 と呼ばれる IPv4-ACL を設定し、任意の送信元アドレスから任意の宛先アドレスへの IP トラフィックを許可します。

ステップ 3 switch(config)# **no ip access-list List1 permit ip any any**

(オプション) List1 と呼ばれる IPv4-ACL を削除します。

ステップ 4 switch(config)# **ip access-list List1 deny tcp any any**

送信元アドレスから宛先アドレスへの TCP トラフィックを拒否するように List1 を更新します。

IPv6-ACL の作成

IPv6-ACL を作成するには、次の手順を実行します。

手順

ステップ 1 switch# **configure terminal**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **ipv6 access-list List1**

```
switch(config-ipv6-acl)#
```

List1 という IPv6-ACL を設定し、IPv6-ACL コンフィギュレーションサブモードを開始します。

ステップ 3 switch(config)# **no ipv6 access-list List1**

(オプション) List1 と呼ばれる IPv6-ACL とそのエントリをすべて削除します。

ステップ 4 switch(config-ipv6-acl)# **permit ipv6 any any**

送信元アドレスから宛先アドレスへの IPv6 トラフィックを許可するエントリを追加します。

ステップ 5 switch(config-ipv6-acl)# **no permit ipv6 any any**

(オプション) IPv6-ACL からエントリを削除します。

ステップ 6 `switch(config-ipv6-acl)# deny tcp any any`

送信元アドレスから宛先アドレスへの TCP トラフィックを拒否するエントリを追加します。

IPv4-ACL の定義

管理アクセスを規制する IPv4-ACL を定義する手順は次のとおりです。

手順

ステップ 1 `switch# configure terminal`

コンフィギュレーション モードに入ります。

ステップ 2 `switch(config)# ip access-list restrict_mgmt permit ip 10.67.16.0 0.0.0.255 any`

10.67.16.0/24 サブネットのすべてのアドレスを許可する、`restrict_mgmt` という名前のエントリを IPv4-ACL に定義します。

ステップ 3 `switch(config)# ip access-list restrict_mgmt permit icmp any any eq 8`

デバイスが MDS (icmp type 8) に ping を実行できるようにする、`restrict_mgmt` という名前のエントリを IPv4-ACL に追加します。

ステップ 4 `switch(config)# ip access-list restrict_mgmt deny ip any any`

明示的に `restrict_mgmt` という名前のアクセス リストへの他のすべてのアクセスをブロックします。

IPv6-ACL の定義

管理アクセスを規制する IPv6-ACL を定義する手順は次のとおりです。

手順

ステップ 1 `switch# configure terminal`

コンフィギュレーション モードに入ります。

ステップ 2 `switch(config)# ip access-list RestrictMgmt`

`switch(config-ipv6-acl)#`

RestrictMgmt という IPv6-ACL を設定し、IPv6-ACL コンフィギュレーションサブモードを開始します。

ステップ 3 switch(config)# **permit ipv6 2001:0DB8:800:200C::/64 any**

2001:0DB8:800:200C::/64 プレフィックスのすべてのアドレスを許可するエントリを定義します。

ステップ 4 switch(config)# **permit icmp any any eq 8**

デバイスが MDS (ICMP type 8) に ping を実行できるようにするエントリを追加します。

ステップ 5 switch(config)# **deny ipv6 any any**

明示的に他のすべての IPv6 アクセスをブロックします。

IPv4-ACL のオペランドとポートのオプション

IPv4-ACL 用のオペランドとポートオプションを使用するには、次の手順を実行してください。

手順

ステップ 1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **ip access-list List2 deny tcp 1.2.3.0 0.0.0.255 eq port 5 any**

1.2.3.0 から送信元ポート 5 を経由する宛先への TCP トラフィックを拒否します。

IPv6-ACL のオペランドとポートのオプション

IPv6-ACL 用のオペランドとポートオプションを使用するには、次の手順を実行してください。

手順

ステップ 1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **ip access-list List2 deny tcp 2001:0DB8:800:200C::/64 eq port 5 any**

2001:0DB8:800:200C::/64 からソース ポート 5 を経由し、任意の宛先までの TCP トラフィックを拒否します。

既存の IPv4-ACL への IP フィルタの追加

IPv4-ACL または IPv6-ACL の作成後に、続く IP フィルタを IPv4-ACL または IPv6-ACL の最後に追加できます。IPv4-ACL または IPv6-ACL の中間にはフィルタを挿入できません。設定された各エントリは、自動的に IPv4-ACL または IPv6-ACL の最後に追加されます。

既存の IPv4-ACL にエントリを追加するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **ip access-list List1 permit tcp 10.1.1.2 0.0.0.0 172.16.1.1 0.0.0.0 eq port telnet**

Telnet トラフィック用の TCP を許可します。

ステップ 3 switch(config)# **ip access-list List1 permit tcp 10.1.1.2 0.0.0.0 172.16.1.1 0.0.0.0 eq port http**

HTTP トラフィック用の TCP を許可します。

ステップ 4 switch(config)# **ip access-list List1 permit udp 10.1.1.2 0.0.0.0 172.16.1.1 0.0.0.0**

すべてのトラフィック用の UDP を許可します。

既存の IPv6-ACL への IP フィルタの追加

既存の IPv6-ACL にエントリを追加するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

switch(config)#

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **ipv6 access-list List2**

switch(config-ipv6-acl)#

IPv6-ACL を設定し、IPv6-ACL コンフィギュレーション サブモードを開始します。

ステップ 3 switch(config-ipv6-acl)# **permit ip 2001:0DB8:800:200C::/64 2001:0DB8:800:2010::/64 eq 23**
Telnet トラフィック用の TCP を許可します。

ステップ 4 switch(config-ipv6-acl)# **permit tcp 2001:0DB8:800:200C::/64 2001:0DB8:800:2010::/64 eq 143**
HTTP トラフィック用の TCP を許可します。

ステップ 5 switch(config-ipv6-acl)# **permit udp 2001:0DB8:800:200C::/64 2001:0DB8:800:2010::/64**
すべてのトラフィック用の UDP を許可します。

既存の IPv4-ACL からの IP フィルタの削除

設定されたエントリを IPv4-ACL から削除するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **no ip access-list List2 deny tcp 1.2.3.0 0.0.0.255 eq port 5 any**

IPv4-ACL (List2) からこのエントリを削除します。

ステップ 3 switch(config)# **no ip access-list x3 deny ip any any**

IPv4-ACL (x3) からこのエントリを削除します。

ステップ 4 switch(config)# **no ip access-list x3 permit ip any any**

IPv4-ACL (x3) からこのエントリを削除します。

既存の IPv6-ACL からの IP フィルタの削除

設定したエントリを IPv6-ACL から削除するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

switch(config)#

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **ipv6 access-list List3**

```
switch(config-ipv6-acl)#
```

IPv6-ACL を設定し、IPv6-ACL コンフィギュレーション サブモードを開始します。

ステップ 3 switch(config-ipv6-acl)# **no deny tcp 2001:0DB8:800:2010::/64 eq port 5 any**

IPv6-ACL から TCP エントリが削除されます。

ステップ 4 switch(config-ipv6-acl)# **no deny ip any any**

IPv6-ACL から IP エントリが削除されます。

IPv4-ACL または IPv6-ACL の設定の確認

設定された IPv4-ACL の内容を表示するには、**show ip access-list** コマンドを使用します。IPv4-ACL は 1 つ以上のフィルタを設定できます。（次の例を参照してください。）

IPv4 ACL 用に設定されたフィルタの表示

```
switch# show ip access-list abc

ip access-list abc permit tcp any any (0 matches)
ip access-list abc permit udp any any (0 matches)
ip access-list abc permit icmp any any (0 matches)
ip access-list abc permit ip 10.1.1.0 0.0.0.255 (2 matches)
ip access-list abc permit ip 10.3.70.0 0.0.0.255 (7 matches)
```

設定した IPv6-ACL の表示

設定されたアクセス フィルタの内容を表示するには、**show ipv6 access-list** コマンドを使用します。各アクセスフィルタには、複数の条件を設定できます。（次の例を参照してください。）

```
switch# show ipv6 access-list

switch# show ipv6 access-list
IPv6 access list copp-system-acl-bgp6
    10 permit tcp any gt 1024 any eq bgp
    20 permit tcp any eq bgp any gt 1024
IPv6 access list copp-system-acl-icmp6
    10 permit icmp any any echo-request
    20 permit icmp any any echo-reply
IPv6 access list copp-system-acl-icmp6-msgs
    10 permit icmp any any router-advertisement
    20 permit icmp any any router-solicitation
    30 permit icmp any any nd-na
    40 permit icmp any any nd-ns
    50 permit icmp any any mld-query
    60 permit icmp any any mld-report
    70 permit icmp any any mld-reduction
```

```
IPv6 access list copp-system-acl-ntp6
  10 permit udp any any eq ntp
  20 permit udp any eq ntp any
IPv6 access list copp-system-acl-ospf6
  10 permit 89 any any
IPv6 access list copp-system-acl-pim6
  10 permit 103 any ff02::d/128
  20 permit udp any any eq pim-auto-rp
IPv6 access list copp-system-acl-radius6
```

指定した IPv6-ACL の概要の表示

```
switch# show ipv6 access-list abc
```

IP-ACL ログ ダンプの読み取り

このフィルタに合致するパケットに関する情報をログに記録するには、IPフィルタ作成の際に **LogEnabled** チェックボックスを使用します。ログ出力には ACL の番号、許可または拒否のステータス、およびポート情報が表示されます。

廃棄されたエントリに合致するパケットに関する情報をログに記録するには、フィルタ条件の最後に **log-deny** オプションを使用します。ログ出力には ACL の番号、許可または拒否のステータス、およびポート情報が表示されます。



Note ログ先でこれらのメッセージをキャプチャするには、カーネルおよび **ipacl** ファシリティに重大度 7 を設定し、ログ先のログファイル、モニターに重大度 7 を設定する必要があります。

```
switch# configure terminal
switch(config)# logging level kernel 7
switch(config)# logging level ipacl 7
switch(config)# logging logfile message 7
```

入力 ACL に対しては、ログは無加工の MAC 情報を表示します。キーワード「**MAC=**」は、MAC アドレス情報を持つイーサネットの MAC フレームの表示を意味しません。ログにダンプされるレイヤ 2 の MAC レイヤ情報を意味します。出力 ACL に対しては、無加工のレイヤ 2 情報はログに記録されません。

入力 ACL ログ ダンプの例を次に示します。

```
Jul 17 20:38:44 excal-2
%KERN-7-SYSTEM_MSG:
%IPACL-7-DENY:IN=vsan1 OUT=
MAC=10:00:00:05:30:00:47:df:10:00:00:05:30:00:8a:1f:aa:aa:03:00:00:00:08:00
:45:00:00:54:00:00:40:00:40:01:0e:86:0b:0b:0b:0c:0b:0b:02:08:00:ff:9c:01:15:05:00:6f:09:17:3f:80:02
:01:00:08:09:0a:0b:0c:0d:0e:0f:10:11:12:13:14:15:16:17:18:19:1a:1b
:1c:1d:1e:1f:20:21:22:23:24:25:26:27:28:29:2a:2b SRC=11.11.11.12 DST=11.11.11.2 LEN=84
TOS=0x00
PREC=0x00 TTL=64 ID=0 DF PROTO=ICMP TYPE=8 CODE=0 ID=277 SEQ=1280
```

出力 ACL ログ ダンプの例を次に示します。

```

Jul 17 20:38:44 excal-2
%KERN-7-SYSTEM_MSG:
%IPACL-7-DENY:IN= OUT=vsan1 SRC=11.11.11.2 DST=11.11.11.12 LEN=84 TOS=0x00 PREC=0x00
TTL=255 ID=38095 PROTO=ICMP TYPE=0 CODE=0 ID=277 SEQ=1280

```

インターフェイスへの IP-ACL の適用

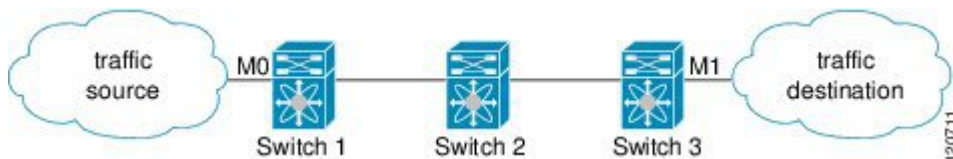
IP-ACLは適用しなくても定義できます。しかし、IP-ACLはスイッチのインターフェイスに適用されるまで効果は出ません。IP-ACLは、VLAN インターフェイス、管理インターフェイス、IPS モジュールおよび MPS-14/2 モジュール上のギガビット イーサネット、およびイーサネット ポートチャンネル インターフェイスに適用できます。



Tip トラフィックの送信元に一番近いインターフェイスに IP-ACL を適用してください。

送信元から宛先へ流れるトラフィックを遮断しようとする場合は、スイッチ 3 の M1 に対するアウトバンドフィルタの代わりに、スイッチ 1 の M0 にインバウンド IPv4-ACL を適用できます (Figure 8: インバウンドインターフェイス上のトラフィックの拒否, on page 133 を参照)。

Figure 8: インバウンドインターフェイス上のトラフィックの拒否



access-group オプションによりインターフェイスへのアクセスを規制できます。各インターフェイスは、1つの方向につき1つの IP-ACL にしか関連付けできません。入力方向には、出力方向とは異なる IP-ACL を持たせることができます。IP-ACL はインターフェイスに適用されたときにアクティブになります。



Tip IP-ACL 中の条件は、インターフェイスに適用する前にすべて作成しておいてください。



Caution IP-ACL を作成前にインターフェイスに適用すると、IP-ACL が空白であるため、そのインターフェイスのすべてのパケットが排除されます。

スイッチにおいては、用語としてのイン、アウト、送信元、宛先は次の意味になります。

- **イン**：インターフェイスに到達してスイッチ内を通過するトラフィック。送信元はそのトラフィックが発信された場所で、宛先は送信される先（ルータの反対側で）を意味します。



Tip 入力トラフィック用インターフェイスに適用された IP-ACL はローカルおよびリモート両方のトラフィックに作用します。

- アウト：スイッチを通過済みで、インターフェイスから離れたトラフィック。送信元はこれが送信された場所であり、宛先は送信先を意味します。



Tip 出力トラフィック用インターフェイスに適用された IP-ACL はローカルトラフィックにだけ作用します。

インターフェイスに IPv4-ACL を適用する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **interface mgmt0**

switch(config-if)#

管理インターフェイスを設定します (mgmt0)。

ステップ 3 switch(config-if)# **ip access-group restrict_mgmt**

入力および出力の両方のトラフィック (デフォルト) の restrict_mgmt と呼ばれる IPv4-ACL を適用します。

ステップ 4 switch(config-if)# **no ip access-group NotRequired**

NotRequired と呼ばれる IPv4-ACL を削除します。

ステップ 5 switch(config-if)# **ip access-group restrict_mgmt in**

入力トラフィックの restrict_mgmt という IPv4-ACL を適用します (まだ存在しない場合)。

ステップ 6 switch(config-if)# **no ip access-group restrict_mgmt in**

入力トラフィックの restrict_mgmt と呼ばれる IPv4-ACL を削除します。

ステップ 7 switch(config-if)# **ip access-group SampleName2 out**

ローカル出力トラフィックの SampleName2 という IPv4-ACL を適用します (まだ存在しない場合)。

ステップ 8 switch(config-if)# **no ip access-group SampleName2 out**

出力トラフィックの SampleName2 と呼ばれる IPv4-ACL を削除します。

インターフェイスへの IPv6-ACL の適用

インターフェイスに IPv6-ACL を適用する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **interface mgmt0**

switch(config-if)#

管理インターフェイスを設定します (mgmt0)。

ステップ 3 switch(config-if)# **ipv6 traffic-filter RestrictMgmt in**

入力トラフィックに RestrictMgmt という IPv6-ACL を適用します (まだ存在しない場合)。

ステップ 4 switch(config-if)# **no ipv6 traffic-filter RestrictMgmt in**

入力トラフィックの RestrictMgmt と呼ばれる IPv6-ACL を削除します。

ステップ 5 switch(config-if)# **ipv6 traffic-filter SampleName2 out**

出力トラフィックの SampleName2 という IPv6-ACL を適用します (まだ存在しない場合)。

ステップ 6 switch(config-if)# **no ipv6 traffic-filter SampleName2 out**

出力トラフィックの SampleName2 と呼ばれる IPv6-ACL を削除します。

mgmt0 への IP-ACL の適用

mgmt0 と呼ばれるシステムのデフォルト ACL は、mgmt0 インターフェイス上に存在します。この ACL はユーザーに表示されないため、mgmt0 は、ユーザーが使用できない予約された ACL 名です。mgmt0 ACL はほとんどのポートをブロックし、許可されたセキュリティ ポリシーに準拠した必須のポートへのアクセスだけを可能にします。



Note mgmt0 インターフェイスに ACL を適用すると、mgmt0 インターフェイスのシステム デフォルト ACL が自動的に置き換えられます。mgmt0 インターフェイスでユーザー定義 ACL を削除すると、mgmt0 がシステム デフォルト ACL に自動的に再適用されます。必要なポートのみを開き、不要なポートを拒否するように ACL を設定することをお勧めします。

インターフェイスの IP-ACL 設定の確認

show interface コマンドを使用して、インターフェイスの IPv4-ACL 設定を表示します。

```
switch# show interface mgmt 0
mgmt0 is up
  Internet address(es):
    10.126.95.180/24
    2001:420:54ff:a4::222:5dd/119
    fe80::eaed:f3ff:fee5:d28f/64
  Hardware is GigabitEthernet
  Address is e8ed.f3e5.d28f
  MTU 1500 bytes, BW 1000 Mbps full Duplex
  5144246 packets input, 1008534481 bytes
    2471254 multicast frames, 0 compressed
  0 input errors, 0 frame
  0 overrun, 0 fifo
  1765722 packets output, 1571361034 bytes
  0 underruns, 0 output errors
  0 collisions, 0 fifo
  0 carrier errors
```

show interface コマンドを使用して、インターフェイスの IPv6-ACL 設定を表示します。

```
switch# show interface gigabitethernet 2/1

GigabitEthernet2/1 is up
Hardware is GigabitEthernet, address is 000e.38c6.28b0
Internet address is 10.1.1.10/24
MTU 1500 bytes
Port mode is IPS
Speed is 1 Gbps
Beacon is turned off
Auto-Negotiation is turned on
ip access-group RestrictMgmt
5 minutes input rate 1208 bits/sec, 151 bytes/sec, 2 frames/sec
5 minutes output rate 80 bits/sec, 10 bytes/sec, 0 frames/sec
6232 packets input, 400990 bytes
0 multicast frames, 0 compressed
0 input errors, 0 frame, 0 overrun 0 fifo
503 packets output, 27054 bytes, 0 underruns
0 output errors, 0 collisions, 0 fifo
0 carrier errors
```

Open IP Ports on Cisco MDS 9000 Series Platforms

Cisco MDS 9000 Series platforms with default configurations have IP ports that are open on the external management interface. The table below lists the open ports and their corresponding services:

Table 10: Open IP Ports on Cisco MDS 9000 Series Platforms

Port number	IP Protocol (UDP/TCP)	Platform	Feature/Service Name	Random Port?
None	UDP	All	—	—
600 - 1024	TCP	All	NFS	Yes
2002	TCP	All	Remote Packet Capture	No
7546	TCP	All	CFS over IPv4	No
9333	TCP	All	Cluster	No
32768 - 32769	TCP	Cisco MDS 8-Gb Fabric Switch for HP c-Class Blade System Cisco MDS 9148 Cisco MDS 9222i Cisco MDS 9506 Cisco MDS 9509 Cisco MDS 9513	License Manager	Yes
44583 - 59121	TCP	Cisco MDS 9148S Cisco MDS 9250i Cisco MDS 9706 Cisco MDS 9710	License Manager	Yes

NFS—A port in this range is used by the NFS service on the switch. This is only for intraswitch use. It is not essential to provide external access to or from these ports. This feature cannot be disabled. To block access to this service, configure an IP access list to deny access to the range of ports. Refer to the [IPv4 および IPv6 のアクセスコントロール リストの概要](#) section for more details.

Remote Packet Capture—This port is used by the Fibre Channel Analyzer service on the switch for communicating with an Ethereal protocol analyzer client on a host using the Remote Capture Protocol (RPCAP). This service is used for troubleshooting and is optional for normal switch operation. This feature cannot be disabled. To block access to this service, configure an IP access list to deny access to the range of ports. Refer to the [IPv4 および IPv6 のアクセスコントロール リストの概要](#) section for more details.

CFS over IPv4—This port is used by the CFS over IPv4 service to distribute switch configuration information to peer switches in the fabric. CFS is an important service for a switch to communicate with

peers, but several transport options are possible. The correct transport depends on the fabric implementation. This port may be closed by disabling the CFS over IPv4 service. Refer to the [Enabling CFS Over IP](#) section of the *Cisco MDS 9000 Family CLI Configuration Guide* for details.

Cluster—This port is used by the cluster service to communicate with peer switches in a cluster. Features such as IOA and SME rely on this service. If such features are not in use, the cluster service is not essential to a switch operation. This port can be closed by disabling the cluster service. Refer to the [Enabling and Disabling Clustering](#) section of the *Cisco MDS 9000 Family Storage Media Encryption Configuration Guide* for details.

License Manager—These ports are used by the License Manager service. This only for intraswitch use. It is not essential to provide external access to or from these ports. This feature cannot be disabled. To block access to this service, configure an IP access list to deny access to the range of ports. Refer to the [IPv4 および IPv6 のアクセスコントロール リストの概要](#) section for more details.

IP-ACL カウンタのクリーンアップ

指定した IPv4 ACL フィルタ エントリのカウンタをクリアするには、**clear** コマンドを使用します。



Note このコマンドを使用して個別のフィルタのカウンタをクリアすることはできません。

```
switch# show ip access-list abc

ip access-list abc permit tcp any any (0 matches)
ip access-list abc permit udp any any (0 matches)
ip access-list abc permit icmp any any (0 matches)
ip access-list abc permit ip 10.1.1.0 0.0.0.255 (2 matches)
ip access-list abc permit ip 10.3.70.0 0.0.0.255 (7 matches)

switch# clear ip access-list counters abc
switch# show ip access-list abc

ip access-list abc permit tcp any any (0 matches)
ip access-list abc permit udp any any (0 matches)
ip access-list abc permit icmp any any (0 matches)
ip access-list abc permit ip 10.1.1.0 0.0.0.255 (0 matches)
ip access-list abc permit ip 10.3.70.0 0.0.0.255 (0 matches)
```

clear ipv6 access-list コマンドを使用してすべての IPv6-ACL のカウンタをクリアします。

```
switch# clear ipv6 access-list
```

指定した IPv6 ACL のカウンタをクリアするには、**clear ipv6 access-list name** コマンドを使用します。

```
switch# clear ipv6 access-list List1
```



Note このコマンドを使用して個別のフィルタのカウンタをクリアすることはできません。



第 7 章

認証局およびデジタル証明書の設定

この章は、次の項で構成されています。

- [認証局およびデジタル証明書について, on page 139](#)
- [認証局およびデジタル証明書の設定, on page 144](#)
- [設定例, on page 156](#)
- [上限, on page 195](#)
- [デフォルト設定, on page 195](#)

認証局およびデジタル証明書について

公開キーインフラストラクチャ (PKI) サポートは、ネットワーク上での安全な通信を確保するために、Cisco MDS 9000 ファミリ スイッチに、デジタル証明書を取得および使用する手段を提供します。PKI サポートにより、IPsec/IKE および SSH の管理機能およびスケラビリティが提供されます。

認証局およびデジタル証明書の目的

認証局 (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、各デバイスまたはユーザーに、秘密キーと公開キーの両方を含むキーペアが設定されます。秘密キーは秘密裡に保管し、これを知っているのは所有するデバイスまたはユーザです。一方、公開キーは誰もが知っているものです。両方のキーは、相互に補完的に動作します。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。証明書自体は、受信者が身元を証明し、デジタル証明書を作成するうえで確実に信頼できるサードパーティである、CA により署名されます。

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。このプロセスは通常、アウトオブバンド、またはインストール時に実行さ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。IPSec の基本コンポーネントであるインターネット キー交換 (IKE) は、デジタル シグニチャをスケールで使用して、セキュリティ アソシエーションを設定する前にピア デバイスを認証できます。

信頼モデル、トラストポイント、アイデンティティ 証明機関

PKI サポートで使用されるトラスト モデルは、設定可能な複数の信頼できる証明機関 (CA) による階層構造です。各加入エンティティには、セキュリティ プロトコル エクスチェンジによって取得したピアの証明書を確認できるように、信頼できる CA のリストが設定されます。ただし、その証明書がローカルの信頼できる CA の 1 つから発行されていることが条件になります。これを実行するために、CA が自己署名したルート証明書 (または下位 CA の証明書チェーン) がローカルに保管されます。これをローカルに安全に取得して保存するプロセスは、[CA 認証 (CA authentication)] と呼ばれます。これは、CA を信頼する上で必須の手順です。

ローカルに設定された信頼できる CA の情報を [トラストポイント (trust point)]、CA そのものを [トラストポイント CA (trust point CA)] と呼びます。この情報は、CA 証明書 (または下位 CA の証明書チェーン) と、証明書失効チェック情報によって構成されます。

[アイデンティティ (identity)] はデバイスの名前です。[アイデンティティ証明書 (identity certificate)] (公開鍵またはデジタル証明書とも呼ばれる) は、トラストポイントによって署名されたデバイスの公開鍵証明書です。[アイデンティティ CA (identity CA)] は、アイデンティティ証明書を発行できるトラストポイントです。

一連のアプリケーション (たとえば、IPsec/IKE) の ID 証明書を取得するためにトラストポイントを使用して MDS スイッチを [登録 (enrollment)] するプロセスは、登録と呼ばれます。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。

RSA キー ペアおよびアイデンティティ証明書

1 つ以上の RSA キー ペアを生成し、各 RSA キー ペアに、アイデンティティ証明書を取得するために MDS スイッチを登録するトラストポイント CA を関連付けることができます。MDS スイッチは、各 CA について 1 つのアイデンティティ、つまり 1 つのキー ペアと 1 つのアイデンティティ証明書だけを必要とします。

Cisco MDS NX-OS では、RSA キー ペアの生成時に、キーのサイズ (または絶対値) を設定できます。他のデバイスでキー ペアを生成し、MDS スイッチにインポートすることもできます。RSA キー ペアごとにラベルを構成できます。RSA キー ペアの最大値とデフォルトの詳細につ

いては、[Table 11: CA およびデジタル証明書の最大限度](#) および [Table 12: CA およびデジタル証明書のパラメータのデフォルト値](#) を参照してください。

次に、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連についての要約を示します。

- トラストポイントは、MDS スイッチが任意のアプリケーション (IKE または SSH など) に関して、ピアの証明書を確認するために信頼する特定の CA になります。
- MDS スイッチには多数のトラストポイントを設定でき、スイッチ上のすべてのアプリケーションは、いずれかのトラストポイント CA から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。
- MDS スイッチは、アイデンティティ証明書を取得するためのトラストポイントに相当する CA に登録されます。スイッチを複数のトラストポイントに登録して、各トラストポイントから個別のアイデンティティ証明書を取得できます。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、証明書の拡張情報として証明書に保管されます。
- トラストポイントへの登録時に、認証される 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生成して、トラストポイントに関連付ける必要があります。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間のアソシエーションは、証明書、キー ペア、またはトラストポイントを削除して明示的に廃棄されるまで有効です。
- アイデンティティ証明書のサブジェクト名は、MDS スイッチの FQDN です。
- スイッチに 1 つ以上の RSA キー ペアを生成して、各キー ペアを 1 つ以上のトラストポイントに関連付けることができます。ただし、トラストポイントに関連付けることができるキー ペアは 1 つだけです。つまり、各 CA から取得できるアイデンティティ証明書は 1 つだけです。
- 複数のアイデンティティ証明書を (それぞれ異なる CA から) 取得した場合、アプリケーションがピアとのセキュリティプロトコルエクステンジに使用する証明書は、アプリケーションによって異なります。
- 1 つのアプリケーションに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。
- 1 つの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取得したり、1 つの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。CA 証明書は、付与されたアイデンティティ (の名前) を一度だけ使用し、同じサブジェクト名で複数の証明書は発行しません。1 つの CA から複数のアイデンティティ証明書を取得する必要がある場合には、同じ CA に対して別のトラストポイントを定義し、別のキー ペアを関連付けて、認証を受けます。ただし、その CA が同じサブジェクト名で複数の証明書を発行できることが条件になります。

複数の信頼された証明機関

複数の信頼された（証明機関）CA のサポートにより、スイッチはさまざまな CA ドメインに登録されているデバイスの識別子を検証できます。複数の信頼できる CA を設定する場合、ピアに証明書を発行した特定の CA に対して、スイッチに登録する必要はありません。代わりに、ピアも信頼する複数の信頼できる CA をスイッチに設定します。スイッチは、ピアの証明書がローカルスイッチのアイデンティティ証明書を定義した CA 以外の CA から発行されていても、設定された信頼できる CA を使用して、ピアの証明書を確認できます。これは、IPsec トンネルを確立するときに IKE で使用できます。

複数のアイデンティティ証明機関

複数のアイデンティティ認証局（CA）をサポートすることにより、スイッチを複数のトラストポイントに登録できます。その結果、異なる CA から1つずつ、複数のアイデンティティ証明書を取得できます。これにより、各ピアで許容される適切な CA から発行された証明書を使用して、多数のピアとの IPsec および他のアプリケーションにスイッチを加入させることができます。

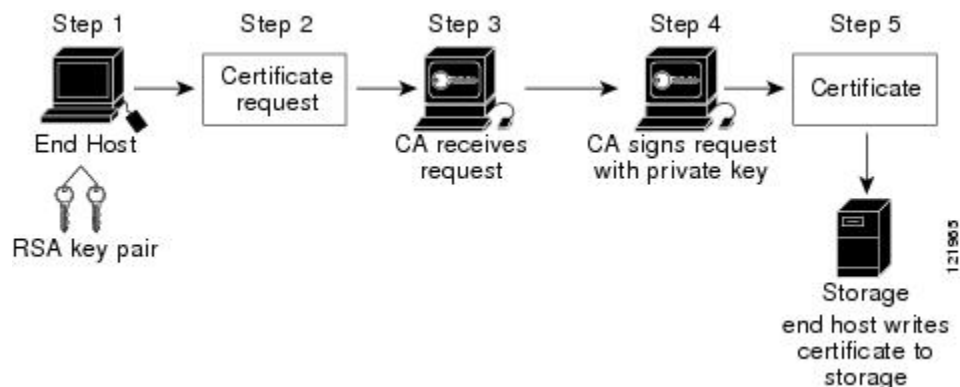
複数の RSA キーペアのサポート機能により、スイッチ上で、登録した各 CA ごとに異なるキーペアを保持できます。したがって、キーの長さなど、他の CA から指定された要件と対立することなく、各 CA のポリシー要件と一致させることができます。トラストポイントへの登録時に、関連付けたキーペアを使用して証明書署名要求を作成できます。

PKI 登録

Public Key Infrastructure (PKI) 登録は、IPsec/IKE または SSH などのアプリケーションに使用する、スイッチのアイデンティティ証明書を取得するプロセスです。このプロセスは、証明書を要求する MDS スイッチと証明機関の間で実行されます。

下の図のおよび次の手順によって、証明書の登録プロセスを説明します。

Figure 9: 証明書の登録プロセス



このプロセスには次の手順が含まれます。

1. RSA 秘密キーと公開キーのキーペアを生成します。

2. 証明書サイン要求 (CSR) を標準形式で生成し、CA に転送します。
3. CA の CSR を承認して、CA の秘密キーで署名された識別子証明書を生成し、それを MDS スイッチ管理者に転送します。要求を承認する場合、CA 上で CA 管理者による手動操作が必要になることがあります。
4. CA からの識別子証明書を MDS スイッチにインストールします。
5. 証明書を MDS スイッチの不揮発性ストレージ領域に保存します。

RSA キーペアと証明書署名要求は、スイッチまたは適切なユーティリティを使用して別のデバイスで生成できます。キーペアが別のデバイスで生成された場合、それらは識別子証明書と同様に MDS スイッチにインストールする必要があります。MDS スイッチは、証明書署名要求に使用できるすべてのフィールドをサポートしているわけではありません。他のデバイスの証明書署名要求生成ツールでは、MDS スイッチからの登録よりも多くのフィールドを指定できる場合があります。

カットアンドペーストによる手動登録

Cisco MDS NX-OS は、手動でのカットアンドペースト方式による証明書の検索および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では、スイッチと CA 間で、証明書要求と生成された証明書をカットアンドペーストする必要があります。手順は、次のとおりです。

1. 登録証明書署名要求を作成します。この要求は、base64 符号化テキスト形式で表示されます。
2. 符号化された証明書要求テキストを、Eメールまたは Web 形式にカットアンドペーストして、CA に送信します。
3. Eメールメッセージまたは Web ブラウザでのダウンロードにより、CA から発行された証明書 (base64 符号化テキスト形式) を受信します。
4. 証明書インポート機能の **certificate import** コマンドを使用して、発行された証明書をスイッチにカットアンドペーストします。

ピア証明書の検証

MDS スイッチの PKI サポートを使用して、ピアの証明書を確認できます。スイッチは、IPsec/IKE および SSH など、アプリケーションのセキュリティ エクスチェンジの実行時に、ピアから提示された証明書を確認します。アプリケーションは、提示されたピア証明書の有効性を確認します。ピア証明書の確認プロセスでは、次の手順が実行されます。

- 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。

失効チェックの場合、スイッチは証明書失効リスト（CRL）方式を使用することができます。トラストポイントではCRL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します。

CRLのダウンロード、キャッシュ、およびチェックのサポート

証明書失効リスト（CRL）は、失効された証明書の情報を提供するためにCAによって保持され、レポジトリで公開されます。ダウンロード用のURLが公開され、すべての発行済み証明書にも指定されています。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する必要があります。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 MDS NX-OS では、トラストポイント用のCRLを事前にダウンロードして、スイッチ証明書ストアにキャッシュされるように手動で設定できます。ピア証明書の確認では、CRLがローカルでキャッシュされ、失効チェックにCRLが使用されるように設定されている場合にかぎり、発行元CAのCRLが参照されます。それ以外の場合、他の失効チェック方式が設定されていなければ、失効チェックは実行されず、証明書は失効していないと見なされます。このモードのCRLチェックは、CRLオプションと呼ばれています。

証明書および関連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）フォーマットでインポートされています。キーペアが外部で生成された場合は、別の手順でインポートする必要があります。

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PKCS12標準フォーマットでファイルにエクスポートできます。この情報を、以降で同じスイッチ（システムクラッシュ後など）または交換したスイッチにインポートできます。PKCS12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。

認証局およびデジタル証明書の設定

ここでは、Cisco MDS スイッチ装置でCAおよびデジタル証明書を相互運用するために必要な作業について説明します。

ホスト名およびIPドメイン名の設定

スイッチのホスト名およびIPドメイン名が未設定の場合には、これらを設定する必要があります。アイデンティティ証明書の情報カテゴリとして、スイッチのFQDNが使用されるからです。また、キーペアの生成時にキーラベルを指定しない場合、デフォルトのキーラベルとしてスイッチのFQDNが使用されます。たとえば、SwitchA.example.comという名前の証明書は、

SwitchA というスイッチのホスト名と、example.com というスイッチの IP ドメイン名で構成されています。



Caution 証明書の生成後に IP ホスト名または IP ドメイン名を変更すると、証明書が無効になることがあります。

スイッチの IP ホスト名および IP ドメイン名を設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

switch(config)#

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **switchname SwitchA**

スイッチの IP ホスト名を「SwitchA」として構成します。

ステップ 3 SwitchA(config)# **ip domain-name example.com**

スイッチの IP ドメイン名を「example.com」として構成します。

RSA キーペアの生成

RSA キーペアは、IKE/IPsec および SSH などのアプリケーションによるセキュリティプロトコル エクステンジの実行中に、署名およびセキュリティ ペイロードの暗号化/復号化に使用されます。RSA キーペアは、スイッチの証明書を取得する前に必要になります。

RSA サーバー キーペアを生成する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

switch(config)#

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **crypto key generate rsa**

デフォルトのラベルとしてスイッチの FQDN を使用し、デフォルトのモジュラスとして 512 を使用する RSA キーペアを生成します。デフォルトでは、キーペアはエクスポートできません。

Note キーの絶対値を指定するときは、ローカルサイト（MDS スイッチ）および CA（登録先）のセキュリティポリシー（または要件）を考慮する必要があります。

サポートされる最大の RSA キー ペアの詳細については、[上限, on page 195](#) を参照してください。

ステップ 3 switch(config)# crypto key generate rsa label SwitchA modulus 768

ラベル SwitchA、モジュラス 768 の RSA キー ペアを生成します。有効なモジュラスの値は 512、768、1024、2048、および 4096 です。デフォルトでは、キー ペアはエクスポートできません。

。

ステップ 4 switch(config)# crypto key generate rsa exportable

デフォルトのラベルとしてスイッチの FQDN を使用し、デフォルトのモジュラスとして 512 を使用する RSA キー ペアを生成します。キーはエクスポート可能です。

Caution キー ペアのエクスポート設定は、キー ペアの生成後は変更できません。

Note RKCS#12 形式でエクスポートできるのは、エクスポート可能なキー ペアだけです。

トラストポイント認証局関連付けを作成

Cisco MDS 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。

トラストポイント CA アソシエーションを作成する手順は、次のとおりです。

Procedure

ステップ 1 switch(config)# crypto ca trustpoint admin-ca

switch(config-trustpoint)#

「admin-ca」というスイッチが信頼するトラストポイント CA を宣言し、このトラストポイントのトラストポイント構成サブモードを開始します。

Note スイッチに設定できるトラストポイントの最大数は 16 です。

ステップ 2 switch(config)# no crypto ca trustpoint admin-ca

(オプション) トラストポイント CA を削除します。

ステップ 3 switch(config-trustpoint)# enroll terminal

カットアンドペーストによる手動での証明書登録を指定します（デフォルト）。

Note 手動でのカット&ペーストの証明書の登録は登録でサポートされている唯一の方法です。

ステップ 4 switch(config-trustpoint)# **rsa**keypair SwitchA

登録の目的でこのトラストポイントに関連付ける RSA キーペアのラベルを指定します。RSA キーペアの生成, on page 145の項で作成した名前です。各 CA に1つの RSA キーペアだけを指定できます。

ステップ 5 switch(config-trustpoint)# **no** rsakeypair SwitchA

(オプション) トラストポイントから RSA キーペアの関連付けを解除します。

ステップ 6 switch(config-trustpoint)# **end**

switch#

トラストポイント コンフィギュレーション サブモードを終了します。

ステップ 7 switch# **copy running-config startup-config**

実行中の設定を起動構成にコピーして、構成がリブート後も保持されるようにします。

トラストポイントの認証局

信頼できる認証局 (CA) の設定プロセスは、MDS スイッチに対して CA が認証された場合にかぎり、完了します。スイッチは、CA を認証する必要があります。CA を認証するには、CA の公開キーが含まれている CA の自己署名付きの証明書を PEM 形式で取得します。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 認証される CA が自己署名した CA ではない場合 (つまり、別の CA の下位 CA で、その別の CA もまた、最終的に自己署名した別の CA の下位 CA であるような場合) には、CA 認証の手順で、認証チェーンに含まれるすべての 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。これは、認証される CA の [CA 認証チェーン (CA certificate chain)] と呼ばれます。CA 証明書チェーン内の証明書の最大数は 10 です。

電子メールまたは Web サイトからの証明書のカットアンドペーストにより CA の証明書を認証するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

switch(config)#

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# crypto ca authenticate admin-ca

```

xEzARBgNVBAStCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJvYYSBD
QTAEFw0wNTA1MMDMyMjQ2MzdaFw0wNzA1MMDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
AQkBFhFhbWFuZGt1QGNpc2NvLmNvbTElMAkGA1UEBhMCSU4xEjAQBgNVBAGTCUth
cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDaXNjbzETMBEG
A1UECzMkbnV0c3RvcnFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHZluNccNM87ypyzwuoSNZXOMpeRXXI
OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAsOBvzCBvDALBgNVHQ8E
BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyRyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJvYYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xccc3N1LTA4XEN1cnRFbnJv
bGxcQXBhcm5hJTlWQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB
BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaNgLh0AFcT0rEyuyt/WYGPzksF9Ea
NBG7E0oN66zex0EOEfG1Vs6mXpl//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

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。

Note 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。

Note 証明書の確認および PKCS#12 形式のエクスポートでは CA チェーンが必要になるので、下位 CA の認証の場合には、最終的に自己署名された CA までの CA 証明書の完全なチェーンが必要になります。

証明書取消確認方法の設定

クライアント (IKE ピアまたは SSH ユーザーなど) とのセキュリティ交換の際に、Cisco MDS スイッチは、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。

送信された証明書が失効しているかどうかを調べるには、複数の方法があります。認証局 (CA) からダウンロードした証明書執行リスト (CRL) を確認するようにスイッチを設定できます ([CRL の設定](#), on page 154の項を参照)。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。ただし、CRL のダウンロード後に証明書が失効された場合、失効ステータスを認識できません。失効証明書をチェックする最も確実な方法は、ローカル CRL チェックを使用することです。



Note 証明書の失効チェックを設定する前に、CA を認証する必要があります。

証明書失効確認方式を設定するには、次の手順を実行します。

Procedure

ステップ 1 switch(config)# **crypto ca trustpoint admin-ca**

```
switch(config-trustpoint)#
```

スイッチ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サブモードを開始します。

ステップ 2 switch(config-trustpoint)# **revocation-check crl**

このトラストポイントと同じCAによって発行されたピア証明書の検証の際に適用される失効チェック方式としてCRLを指定します（デフォルト）。

ステップ 3 switch(config-trustpoint)# **revocation-check none**

失効証明書をチェックしません。

ステップ 4 (Optional) switch(config-trustpoint)# **no revocation-check**

デフォルトの方式に戻ります。

証明書署名要求の生成

スイッチの各RSAキーペアについて、トラストポイントCAからアイデンティティ証明書を取得するには、要求を生成する必要があります。さらに、表示された要求を、CA宛てのEメールメッセージまたはWebサイトフォームにカットアンドペーストします。

CAから署名入り証明書要求を生成する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 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: abc123
The subject name in the certificate will be: SwitchA.example.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: 192.168.31.162
The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
```

```
MIIBqzCCARQCAQAwHDEaMBGGA1UEAxMRVnYXNjby5jb20wgZ8wDQYJ
KoZlHvcNAQEeBBQAdgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVA5MqNiGJ2kt8r141KY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxBLdKTTysnjuCXGvjbb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhhVpj+rargZvHtGJ91XTq4WoVksCzXv8S
VqyH0vEvAgMBAAAGTzAVBqkqkhiG9w0BCQcxCBMGBmJ2MTIzMDYGCsQGSib3DQeJ
DjEpMCcwJQYDVR0RAQH/BBswGYIRVnYXNjby5jb22HBKwWH6IwDQYJ
KoZlHvcNAQEeBBQAdgYEAKT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99G1FWgt
PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6U188nTOjglXMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=
-----END CERTIFICATE REQUEST-----
```

認証した CA に対する証明書要求を作成します。

Note チャレンジパスワードは、設定には保存されません。このパスワードは、証明書を失効する必要がある場合に要求されるので、パスワードを覚えておく必要があります。

アイデンティティ証明書のインストール

CA からのアイデンティティ証明書は、base64 符号化テキスト形式で、E メールまたは Web ブラウザで受信します。CLI インポート機能を使用して符号化テキストをカットアンドペーストすることにより、CA のアイデンティティ証明書をインストールする必要があります。

電子メールまたは Web ブラウザで CA から受信したアイデンティティ証明書をインストールするには、次の手順を実行します。

Procedure

ステップ 1 switch# configure terminal

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# crypto ca import admin-ca certificate

```
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIEADCCA6qgAwIBAgIKCj0OoQAAAAAAdANBgkqhkiG9w0BAQUFADCBkDEgMB4G
CSqGSIb3DQEJARYRYWlhbmrRZUBjaXNjby5jb20xZzA5BGNVBAZTAklOMRIwEAYD
VQIQEw1LYXJuYXRha2ExEjAQBGNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ2l2
Y28xExZARBgNVBAsTCm5ldHN0b3JhZ2UxZjAQBGNVBAmtCUFwYXJuYSDQTAeFw0w
NTEeMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZlZ2FzLzE2
Y2l2Y28uY29tMIGfMA0GCSqGSIb3DQEBQUAA4GNADCBiQKBgQC/GNVACdjQu41C
dQlWkKjKjSICdpLfk5eJSmNcQujGpzcukSZPFxjF2UoiyeCYE8y1ncWyw5E08rJ47
glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYA8rDfz8jMcnIM4W1aY/q2q4Gb
x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABO4ICEZCCAg8wJQYDVR0RAQH/BBsw
GYIRVnYXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR
bhWmlVyo9jngMIHMBgNVHSEgcQwgcGAFCCo8kaDG6wjTEVNjskYUBoLFmxxoYGW
pIGTMIGQMSAwHgYJKoZlHvcNAQkBFhFhbWFWuzGt1QGnpc2NvLmNvbTELMakGA1UE
BhMCSU4xZjAQBGNVBAgTCUthcm5hdGFryTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w
DAYDVQQKEwVDAjNjZjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0MjE0
cm5hIENBghAFYnkYjRlQZlE9JEiWMrR16MGsGA1UdHwRkMGiWlQAsocQgKgh0dHA6
Ly9cZ2UuMDgvd2VydEVucm9sb3Bc9BcGFybmElMjBDQs5jcmwwMKAuoCyGKmZpbGU6
Ly9cXHNzZS0wOFxDZlJ0RW5yb2xsXEFwYXJuYSDYUyMENBmNybDcBicYIKwYBBQUH
AQEefjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0N1cnRfbnJvbGwvc3Nl
```

```
LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xccc3N1LTA4
XEN1cnRfbnJvbGxccc3N1LTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF
AANBADBGBGsb7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw
E36cIZu4WsExREqxbTk8ycx7V5o=
-----END CERTIFICATE-----
```

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。証明書がルート CA によって発行されていない場合、これには複数の「BEGIN CERTIFICATE」行があり、ルート CA 証明書で終わります。CA から提供された証明書チェーン全体を貼り付け、テキストが「END CERTIFICATE」行で終了していることを確認します。

Note スイッチ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。

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

トラストポイント設定は、標準の Cisco NX-OS コンフィギュレーションであるため、スタートアップ コンフィギュレーションに明示的にコピーした場合にかぎり、システム リブート後も存続します。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場合も、削除を反映させるために、実行コンフィギュレーションを保存してください。

特定の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保存されていれば、トラストポイントに関連する証明書および CRL は、インポートした時点で（スタートアップ コンフィギュレーションに明示的にコピーしなくても）自動的に存続します。

また、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、外部サーバーに保存しておくことを推奨します（[PKCS12 フォーマットのアイデンティティ情報をエクスポート](#), on page 152を参照）。



Note スタートアップまたは実行中の構成を外部サーバーにコピーすると、証明書およびキーペアも保存されます。

1. switch# copy running-config startup-config

現在の構成をスタートアップ構成に保存します。

認証局および証明書の構成のモニタリングとメンテナンス

このセクションの作業は、オプションです。

違うデバイスにキーペアと証明書署名要求を生成

RSA キーペアと CSR は、別のデバイスで生成される場合があります。たとえば、`openssl` を使用してホストでこれらを生成するには、次の手順に従います。

1. `host$ openssl req -newkey rsa:2048 -keyout SwitchA.example.com-rsa-pem.privatekey -out SwitchA.example.com-pkcs10.csr`

```
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to SwitchA.example.com-rsa-pem.privatekey'
Enter PEM pass phrase:abc123
Verifying - Enter PEM pass phrase:abc123
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:BE
State or Province Name (full name) []:Brussels
Locality Name (eg, city) []:Brussels
Organization Name (eg, company) []:Example
Organizational Unit Name (eg, section) []:SAN
Common Name (eg, fully qualified host name) []:SwitchA.example.com
Email Address []:cert-admin@example.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:abc123
```

スイッチの FQDN を使用して、2048 ビットのキー モジュールと CSR を持つ RSA キーペアを生成します。

2. `host$ cat SwitchA.example.com-pkcs10.csr`

```
-----BEGIN CERTIFICATE REQUEST-----
...
-----END CERTIFICATE REQUEST-----
```

CA に送信するために生成された base-64 フォーマットの証明書署名要求を表示します。

PKCS12 フォーマットのアイデンティティ情報をエクスポート

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 PKCS12 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。後で、スイッチをシステムクラッシュから回復する場合、またはスーパーバイザ モジュールを交換する場合に、証明書および RSA キーペアをインポートできます。



Note エクスポートおよびインポートの URL の指定では、`bootflash:filename` 形式のローカル構文だけがサポートされます。

証明書およびキーペアを PKCS12 フォーマットファイルにエクスポートする手順は、次のとおりです：

Procedure

ステップ 1 switch# **configure terminal**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **crypto ca export admin-ca pkcs12 bootflash:adminid.p12 abc123**

トラストポイント **admin-ca** のアイデンティティ証明書および関連付けられたキーペアと CA 証明書をファイル **bootflash:adminid.p12** に、パスワード「**abc123**」によって保護された PKCS12 フォーマットでエクスポートします。

ステップ 3 switch(config)# **exit**

```
switch#
```

EXEC モードに戻ります。

ステップ 4 switch# **copy bootflash:adminid.p12 tftp:adminid.p12**

PKCS12 フォーマットのファイルを TFTP サーバにコピーします。

PKCS12 形式でのアイデンティティ情報のインポート

証明書および/またはキーペアを PKCS12 フォーマットファイルからインポートする手順は、次のとおりです：

Procedure

ステップ 1 switch# **copy tftp:adminid.p12 bootflash:adminid.p12**

PKCS12 フォーマットのファイルを TFTP サーバからコピーします。

ステップ 2 switch# **configure terminal**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 3 switch(config)# **crypto ca import admin-ca pkcs12 bootflash:adminid.p12 abc123**

トラストポイント `admin-ca` のアイデンティティ証明書および関連付けられたキーペアと CA 証明書をファイル `bootflash:adminid.p12` から、パスワード「`abc123`」によって保護された PKCS12 フォーマットでインポートします。

CRL の設定

ファイルからトラストポイントに CRL をインポートする手順は、次のとおりです。

Procedure

ステップ 1 `switch# copy tftp:adminca.crl bootflash:adminca.crl`

CRL をダウンロードします。

ステップ 2 `switch# configure terminal`

`switch(config)#`

コンフィギュレーションモードに入ります。

ステップ 3 `switch(config)# crypto ca crl request admin-ca bootflash:adminca.crl`

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。

認証局構成から認定を削除

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認証局 (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あと、トラストポイントから RSA キーペアの関連付けを解除できます。期限切れまたは失効した証明書、キーペアが信用できない (または信用できない可能性がある) 証明書、または信頼できなくなった CA を除去するには、証明書を削除する必要があります。

トラストポイントから CA 証明書 (または下位 CA のチェーン全体) を削除する手順は、次のとおりです。

Procedure

ステップ 1 `switch# configure terminal`

`switch(config)#`

コンフィギュレーションモードに入ります。

ステップ 2 `switch(config)# crypto ca trustpoint myCA`

トラストポイント コンフィギュレーション サブモードを開始します。

ステップ 3 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 switch(config-trustpoint)# **delete certificate**

アイデンティティ証明書を削除します。

ステップ 5 switch(config-trustpoint)# **delete certificate force**

アイデンティティ証明書を削除します。

Note 削除するアイデンティティ証明書が、デバイスの最後または唯一のアイデンティティ証明書である場合には、**force** オプションを使用して削除する必要があります。これは、管理者が最後または唯一のアイデンティティ証明書を誤って削除し、アプリケーション（IKE および SSH など）で使用する証明書が存在しない状態になるのを防止するためです。

ステップ 6 switch(config-trustpoint)# **end**

switch#

EXEC モードに戻ります。

ステップ 7 switch# **copy running-config startup-config**

実行中の設定を起動設定にコピーして、設定がリブート後も保持されるようにします。

スイッチからの RSA キーペアの削除

特定の状況では、スイッチの RSA キーペアの削除が必要になることがあります。たとえば、何らかの原因で RSA キーペアの信用性が失われ、もはや使用しない場合には、そのキーペアを削除すべきです。

スイッチから RSA キーペアを削除する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

switch(config)#

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **crypto key zeroize rsa MyKey**

ラベルが MyKey である RSA キーペアを削除します。

ステップ 3 switch(config)# **end**

switch#

EXEC モードに戻ります。

ステップ 4 switch# copy running-config startup-config

実行中の設定を起動設定にコピーして、設定がリブート後も保持されるようにします。

Example

Note スイッチから RSA キーペアを削除した後、CA でそのスイッチの証明書を失効するように、CA 管理者に依頼してください。その証明書を要求した場合には、作成したチャレンジパスワードを提供する必要があります。「[証明書署名要求の生成, on page 149](#)」を参照してください。

キーペアと証明機関情報の表示

キーペアと証明機関 (CA) 情報を表示するには、次のコマンドを使用します：

コマンド	目的
switch# show crypto key mypubkey rsa	スイッチの RSA 公開キーに関する情報が表示されます。
switch# show crypto ca certificates	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。
switch# show crypto ca crl	CA の CRL についての情報を表示します。
switch# show crypto ca trustpoints	CA トラストポイントについての情報を表示します。

設定例

ここでは、Microsoft Windows Certificate サーバを使用して、Cisco MDS 9000 ファミリスイッチ上に証明書および CRL を設定するための作業例を示します。

MDS スイッチでの証明書の設定

MDS スイッチで証明書を設定する手順は、次のとおりです。

Procedure

ステップ 1 スイッチの FQDN を設定します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# switchname SwitchA
SwitchA(config)#
```

ステップ 2 スイッチの DNS ドメイン名を設定します。

```
SwitchA(config)# ip domain-name example.com
SwitchA(config)#
```

ステップ 3 トラストポイントを作成します。

```
SwitchA(config)# crypto ca trustpoint myCA
SwitchA(config-trustpoint)# exit
SwitchA(config)# show crypto ca trustpoints

trustpoint: myCA; key:
revokation methods: crl
SwitchA(config)#
```

ステップ 4 スイッチの RSA キーペアを作成します。

```
SwitchA(config)# crypto key generate rsa label myKey exportable modulus 1024
SwitchA(config)# show crypto key mypubkey rsa

key label: myKey
key size: 1024
exportable: yes
SwitchA(config)#
```

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。

```
SwitchA(config)# crypto ca trustpoint myCA
SwitchA(config-trustpoint)# rsaakeypair myKey
SwitchA(config-trustpoint)# exit
SwitchA(config)# show crypto ca trustpoints

trustpoint: myCA; key: myKey
revokation methods: crl
SwitchA(config)#
```

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 ([認証局の CA 証明書をダウンロード](#), on page 160を参照)。

ステップ 7 トラストポイントに登録する CA を認証します。

```
SwitchA(config)# crypto ca authenticate myCA

input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRI1jK0ZeJANBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAk1o
MRIwEAYDVQQIEw1LYXJuYXRha2ExEjAQBGNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE
ChMFQ21lZy28xEzARBGNVBAStCm5ldHN0b3JhZ2UxEjAQBGNVBAMTCUFWYXJuYSBD
QTAEFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
AQkBFhFhbWFuZGt1QGhpc2NvLmNvbTELMARGA1UEBhMCSU4xEjAQBGNVBAgTCUth
cm5hdGFrYTESMBAGA1UEBxMjQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDaXNjbzETMBEG
A1UECXMkbnV0c3RvcnFnZTESMBAGA1UEAxMjQXBhcm5hIENBMFwDQYJKoZIhvcN
```

```
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMperXXI
OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxyYKvysCAwEAAoBvzCBvDALBgNVHQ8E
BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyJyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xccc3NlLTA4XENlcnRFbnJv
bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB
BQUAA0EAAHv6UQ+8nE399Tww+KaGr0g0NIJaNgLh0AFcT0rEyuyt/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]:y
SwitchA(config)#
SwitchA(config)# show crypto ca certificates
```

```
Trustpoint: myCA
CA certificate 0:
subject= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/L=Bangalore/O=Yourcompany/O
U=netstorage/CN=Aparna CA
issuer= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/L=Bangalore/O=Yourcompany/OU
=netstorage/CN=Aparna CA
serial=0560D289ACB419944F4912258CAD197A
notBefore=May 3 22:46:37 2005 GMT
notAfter=May 3 22:55:17 2007 GMT
MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
purposes: sslserver sslclient ike
```

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。

```
SwitchA(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:abc123
The subject name in the certificate will be: SwitchA.example.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-----
MIIBqzCCARQCAQAwHDEaMBGGA1UEAxMRVnVnYXNjby5jb20wgZ8wDQYJ
KoZlHvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8rl4lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhhVpjj+rargZvHtGJ91XTq4WoVksCzXv8S
VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCsGSIb3DQEJ
DjEPMcCwJQYDVR0RAQH/BBswGYIRVmVnYXNjby5jb22HBKwWH6IwDQYJ
KoZlHvcNAQEBBQADgYEAkt60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99G1FWgt
PftrNcWUE/pw6HayfQ12T3ecgNwel2d15133YBF2bktExiI6U188nTOjg1XMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=
-----END CERTIFICATE REQUEST-----

SwitchA(config)#
```

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 (アイデンティティ証明書の要求, [on page 168](#) を参照)。

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。

```
SwitchA(config)# crypto ca import myCA certificate

input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIEADCCA6qqAwIBAgIKCj0OoQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G
CSqGSIB3DQEJARYRYWlhbmrRZUBjaXNjby5jb20xZCZAJBgNVBAYTAklOMRIWEAYD
VQQIEWllYXJuYXRha2ExEjAQBGNVBAcTCUJhbmhhdG9yZTEOMAwGA1UEChMFQ2l2
Y28xEzARBGNVBAStCm5ldHN0b3JhZ2UxEjAQBGNVBAMTCUFwYXJuYzY2bDQTAeFw0w
NTEeMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZlZ2FzLzE2
Y21zY28uY29tMIGfMA0GCSqGSIB3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C
dQ1WkJKjSICdpLfK5eJSmNCQujGpzcKsZPFxf2UoIyeCYE8ylnCwyw5E08rJ47
glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb
x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw
GYIRVmVnYXMTMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR
bhWmLVyo9jngMIHMBGNVHSMGcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW
pIGTMIGQMSAwHgYJKoZIHvCNAQkBFhFhbWfuZGt1QGnNpc2NvLmNvbTELMaKGA1UE
BhMCSU4xEjAQBGNVBAgTCUthcm5hdGFryTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w
DAYDVQQKEwVDaXNjby5jb2EjTMBEGA1UECzMkbnV0c3RvcnFnZTESMBAGA1UEAxMJQXBh
cm5hIENBghAFYnkjRlQZLE9JEiWMrRl6MGsGA1UdHwRkMGiWlQAsocCqGKGh0dHA6
Ly9zc2U2MDgvQ2VydEVucm9sbC9BcGFybmElMjBDQS5jcmwwMKAuoCYGKmZpbGU6
Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYzY2bDQTAeFw0wNTEeMTIwMzAy
NDBaMBwxGjAYBgNVBAMTEVZlZ2FzLzE2Y21zY28uY29tMIGfMA0GCSqGSIB3DQE
BAQUAA4GNADCBiQKBgQAAANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw
E36cIZu4WsExREqxbTk8yxc7V5o=
-----END CERTIFICATE-----
SwitchA(config)# exit
SwitchA#
```

ステップ 11 証明書の設定を確認します。

```
SwitchA# show crypto ca certificates

Trustpoint: myCA
certificate:
subject= /CN=SwitchA.example.com
issuer= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/L=Bangalore/O=Cisco/OU
=netstorage/CN=Aparna CA
serial=0A338EA1000000000074
notBefore=Nov 12 03:02:40 2005 GMT
notAfter=Nov 12 03:12:40 2006 GMT
MD5 Fingerprint=3D:33:62:3D:B4:D0:87:A0:70:DE:A3:87:B3:4E:24:BF
purposes: sslserver sslclient ike

CA certificate 0:
subject= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/L=Bangalore/O=Yourcompany/O
U=netstorage/CN=Aparna CA
issuer= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/L=Bangalore/O=Yourcompany/OU
=netstorage/CN=Aparna CA
serial=0560D289ACB419944F4912258CAD197A
notBefore=May 3 22:46:37 2005 GMT
notAfter=May 3 22:55:17 2007 GMT
MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
purposes: sslserver sslclient ike
```

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。

```
SwitchA# copy running-config startup-config
```

認証局の CA 証明書をダウンロード

Microsoft Certificate Service の Web インターフェイスから認証局 (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 Web インターフェイスの [Retrieve the CA certificate or certificate revocation task] オプション ボタンを選択し、[Next] ボタンをクリックします。

Microsoft Certificate Services -- Aparna CA

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other software. 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 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] オプション ボタンをクリックし、[Download CA certificate] リンクをクリックします。

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...

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

Choose file to download:

CA Certificate:

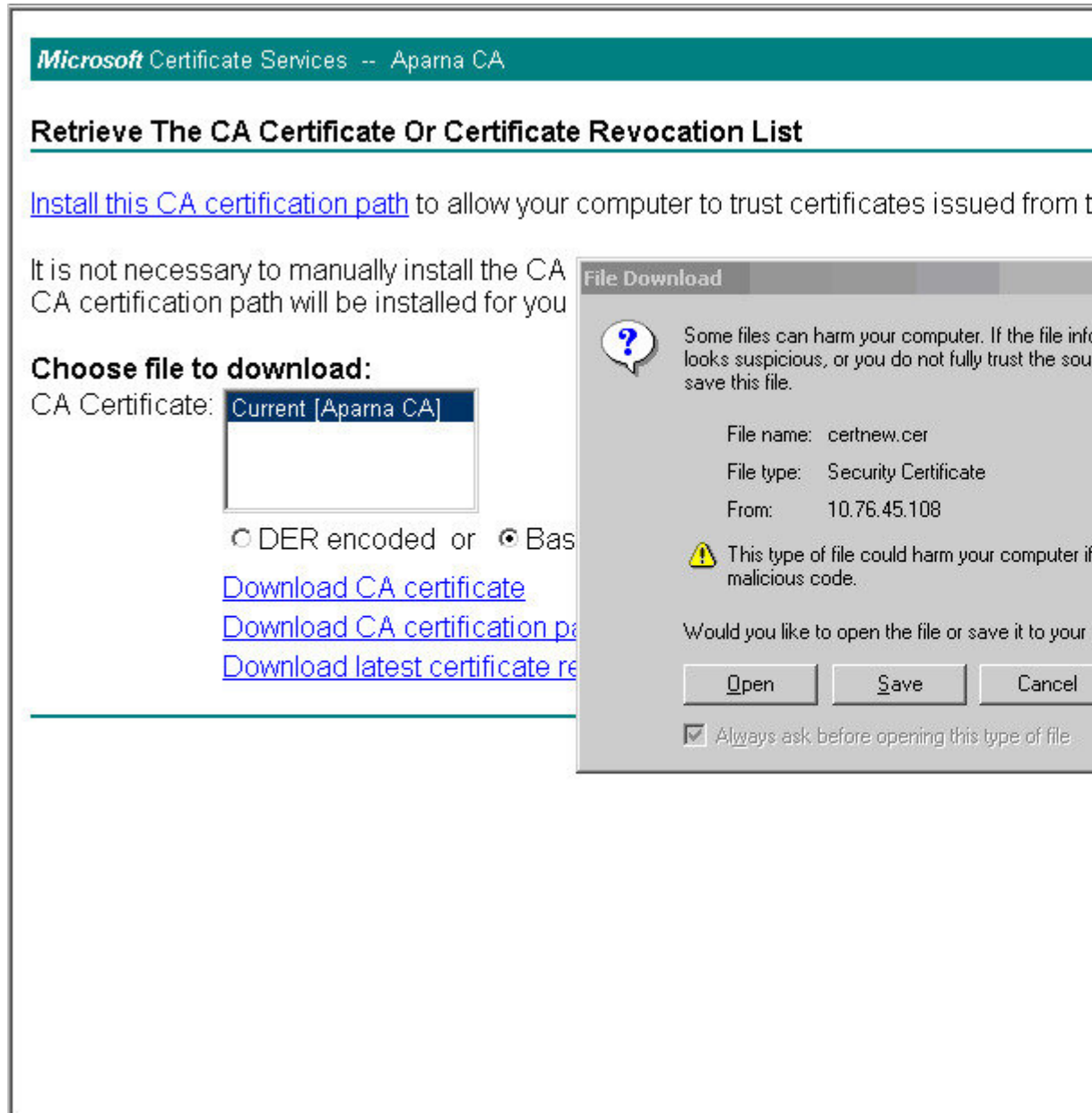
DER encoded or Base 64 encoded

[Download CA certificate](#)

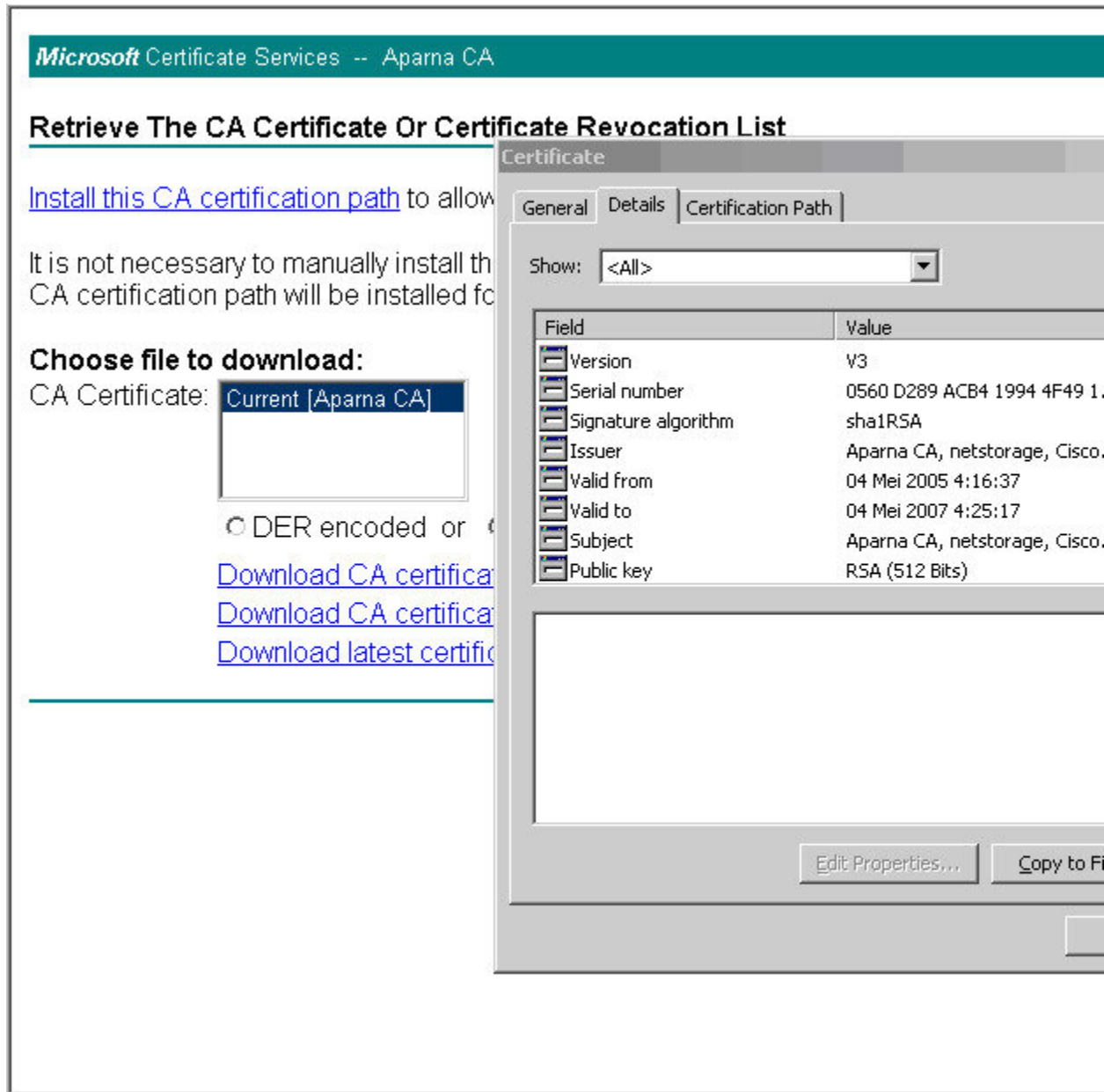
[Download CA certification path](#)

[Download latest certificate revocation list](#)

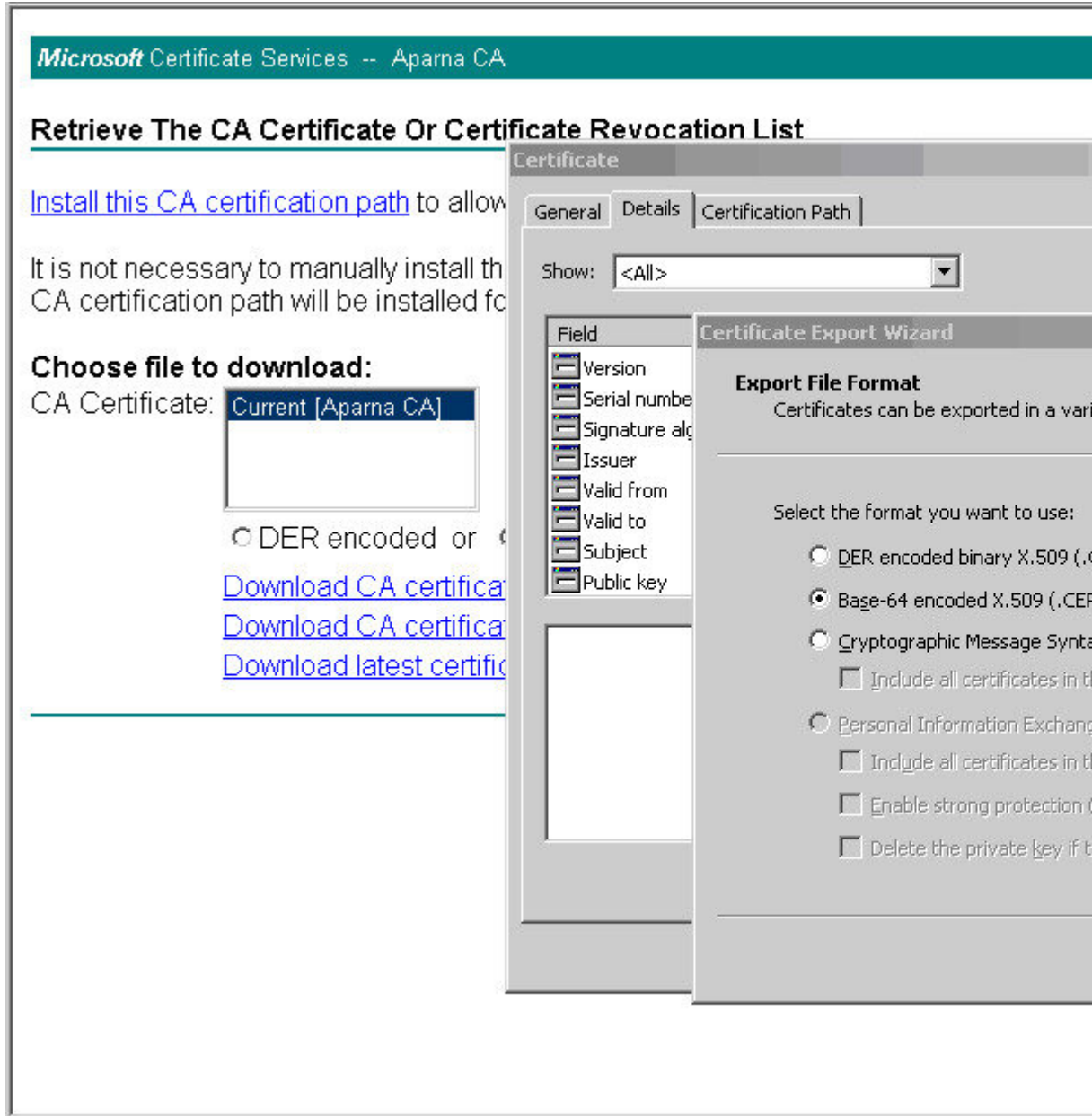
ステップ 3 [File Download] ダイアログボックスで、[Open] ボタンをクリックします。



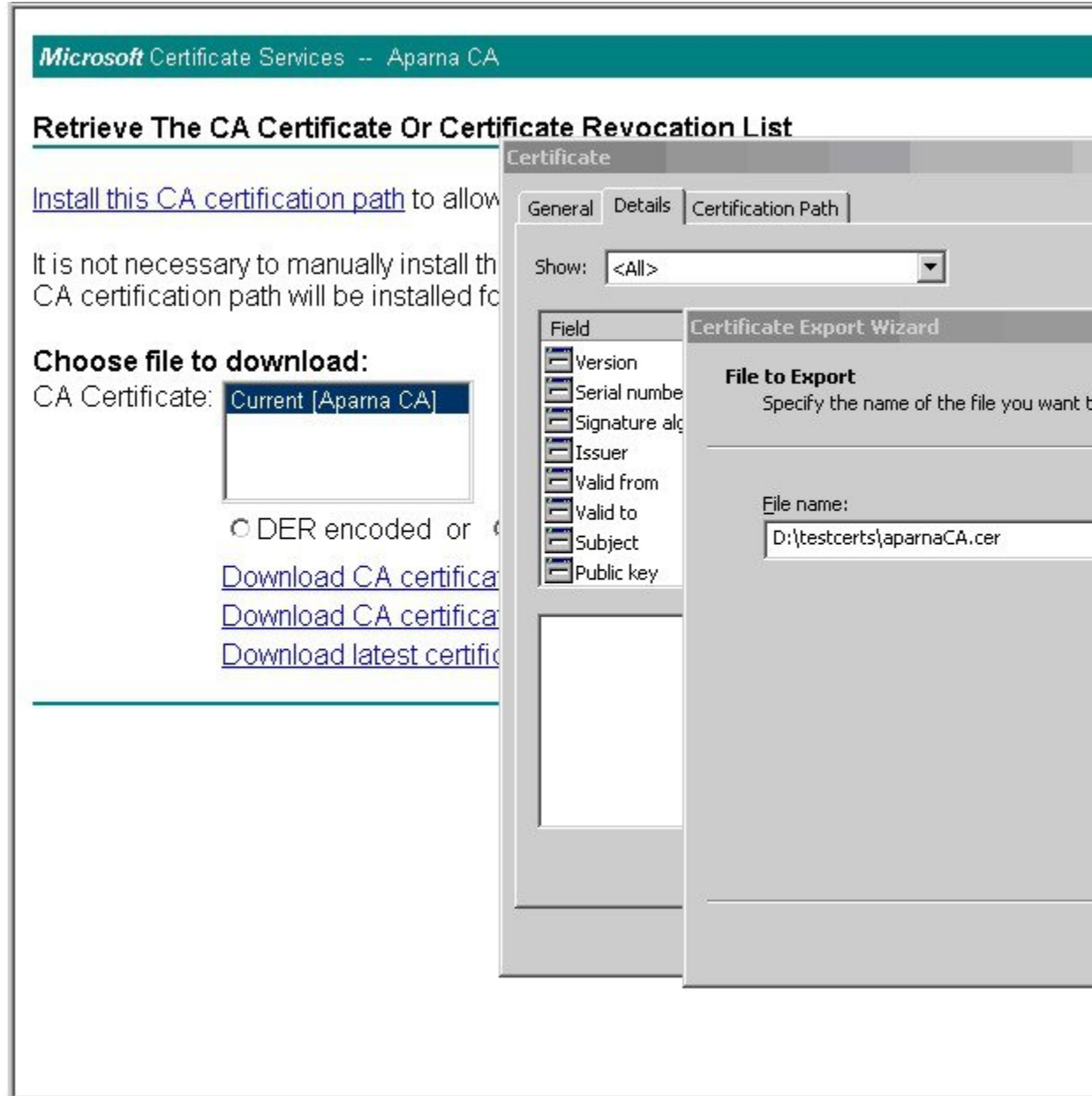
ステップ 4 [Certificate] ダイアログボックスで [Copy to File] ボタンをクリックし、[OK] をクリックします。



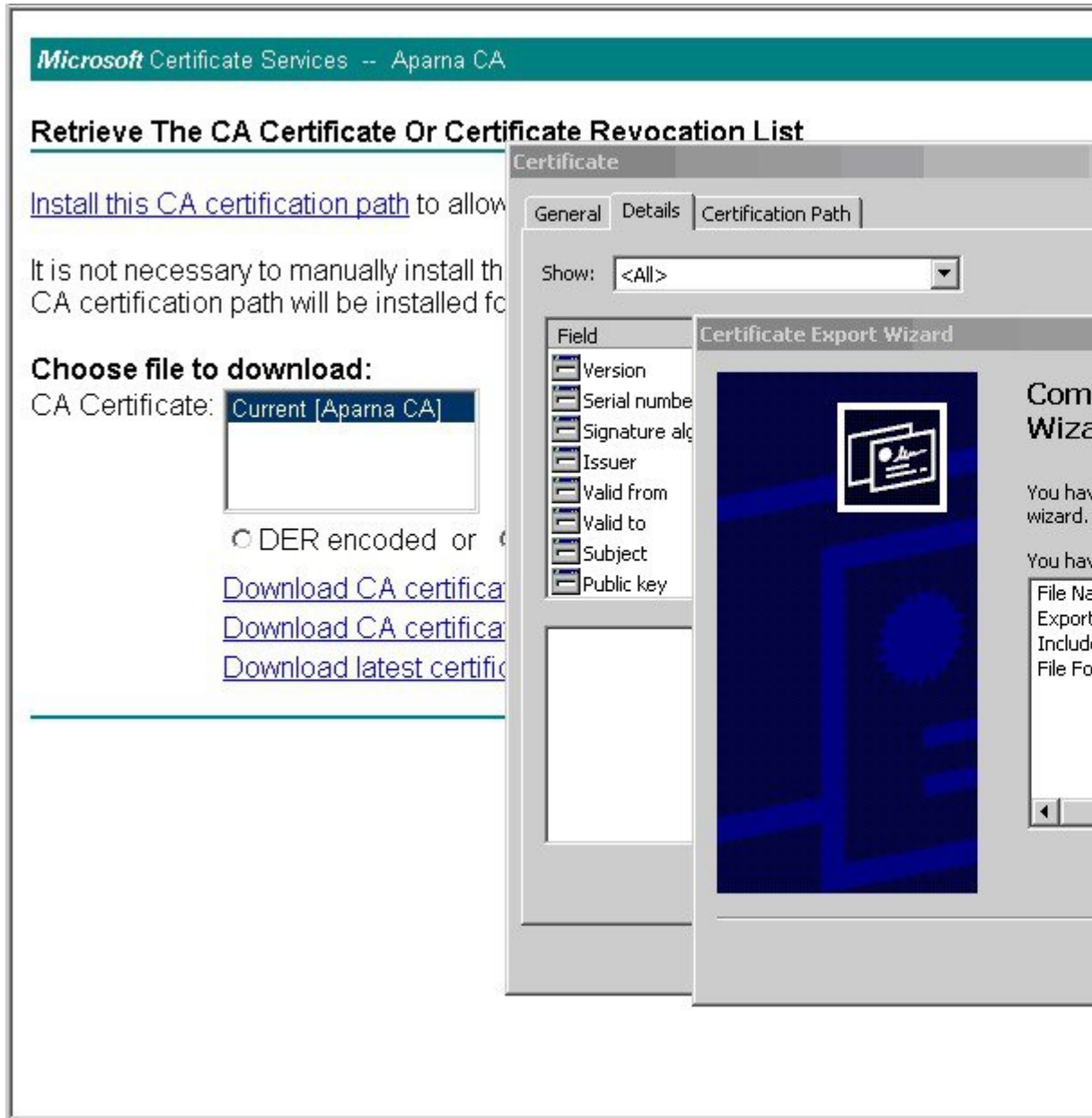
ステップ 5 [Certificate Export Wizard] ダイアログボックスで [Base-64 encoded X.509 (CER)] を選択し、[Next] をクリックします。



ステップ 6 [Certificate Export Wizard] ダイアログボックスの [File name:] テキスト ボックスに宛先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の [Finish] ボタンをクリックします。



- ステップ 8 Microsoft Windows の **type** コマンドを使用して、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-----
MIIC4jCCAoYgAwIBAgIQBWDSiaY0GZRPSRI1jK0ZeJANBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjb3Y5LjB20xCzAJBgNUBAYTAkLO
MRIwEAYDUQqIEwLLYXJuYXRRha2ExEjAQBgNUBACITCUJhbmdhbG9yZTEOMAwGA1UE
ChMFQ21zY28xEzARBgNUBAsTCm5ldHN0b3JhZ2UxEjAQBgNUBAMTCUFWYXJuYSBD
QTAEFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIQMSAwHgYJKoZIhvcNAQ
kBFhFhbWZGt1QGNpc2NuLmNvbTEELMAkGA1UEBhMCSU4xEjAQBgNUBAGTCUth
cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDUQqKEwUdAaXNjbzETMBEG
A1UECzMkbnU0c3RvcnFnZTESMBAGA1UEAxMjQXBhcm5hIENBMFwwDQYJKoZIhvcNAQ
AQBEBBQADSwwSAJBAMW/7b3+DXJPANBsIHHZluNccNM87yppyzwuoSNZXOMpeRXXI
OzyBAGiXT2ASFuUOwQ1iDM8r0/41jF8RxyYKuysCAwEAaA0BuzCBuDALBgNUHQ8E
BAMCAcYwDwYDUR0TAQH/BAUwAwEB/zAdBgNUHQ4EFgQUJyJyRombrCNMRU20yRhQ
GgsWbHEwawYDUR0fBGQwYjAuoCygKoYoahR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYSUyMENBLmNybDAwOC6gLIYqZmlsZTovL1xc3N1LLTA4XEN1cnRfbnJu
bGxcQXBhcm5hJTl1wQ0EuY3JsMBAGCSsGAQQBgjcUAQQDAgEAMAGCSqGSIb3DQEB
BQUAA0EAAHv6UQ+8nE399Tww+KaGr0g0NIJaNgLh0AFcT0rEyuyt/WYGPzksF9Ea
NBG7E0oN66zex0EOEfG1Us6mXp1//w==
-----END CERTIFICATE-----

D:\testcerts>

```

アイデンティティ証明書の要求

PKCS#10 CRS を使用して Microsoft Certificate サーバーにアイデンティティ証明書を要求する手順は、次のとおりです。

Procedure

- ステップ 1** Microsoft Certificate Services Web インターフェイス上の [Request a certificate] ラジオ ボタンを選択し、[Next] を選択します。

The screenshot shows the Microsoft Certificate Services Web interface for the 'Aparna CA'. The page has a teal header with the text 'Microsoft Certificate Services -- Aparna CA'. Below the header, the word 'Welcome' is displayed in bold. The main content area contains a paragraph explaining the site's purpose: 'You use this web site to request a certificate for your web browser, e-mail client, or other... will be able to securely identify yourself to other people over the web, sign your e-mail... depending upon the type of certificate you request.' Below this paragraph, there is a section titled 'Select a task:' followed by three radio button options: 'Retrieve the CA certificate or certificate revocation list', 'Request a certificate' (which is selected), and 'Check on a pending certificate'.

ステップ2 [Advanced Request] ラジオ ボタンを選択し、[Next] をクリックします。

The screenshot shows a web browser window with the title "Microsoft Certificate Services -- Apama CA". The main heading is "Choose Request Type". Below the heading, the text reads "Please select the type of request you would like to make:". There are two radio button options: "User certificate request:" and "Advanced request". The "Advanced request" option is selected. A dropdown menu is open under "User certificate request:", showing "Web Browser Certificate" (highlighted) and "E-Mail Protection Certificate".

- ステップ 3** [Submit a certificate request using a base64 encoded PKCS#10 file or a renewal request using a base64 encoded PKCS#7 file] オプション ボタンを選択し、[Next] ボタンをクリックします。

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 options. 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** Saved Request テキスト ボックスに base64 PKCS 10 証明書要求をペーストし、[次 (Next)] をクリックします。

MDS スイッチのコンソールから、証明書要求がコピーされます (証明書署名要求の生成, on page 149 および MDS スイッチでの証明書の設定, on page 156 を参照)。

Microsoft Certificate Services -- Aparna CA

Submit A Saved Request

Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generated by the client (or a request from a self-signed server) into the request field to submit the request to the certification authority (CA).

Saved Request:

Base64 Encoded Certificate Request (PKCS #10 or #7):

```
VqyHOvEvAgMBAAGgTzAVBgkqhkiG9wOBCQcxCBMG
DjEpMCcwJQYDVRORAQH/BBswGYIRVmVnYXMtMS5j
KoZlhvcNAQEEBQADgYEAKT6OKER6Qo8nj0sDXZVH
PftrNcWUE/pw6HayfQ12T3ecgNwe12d15133YBF2:
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

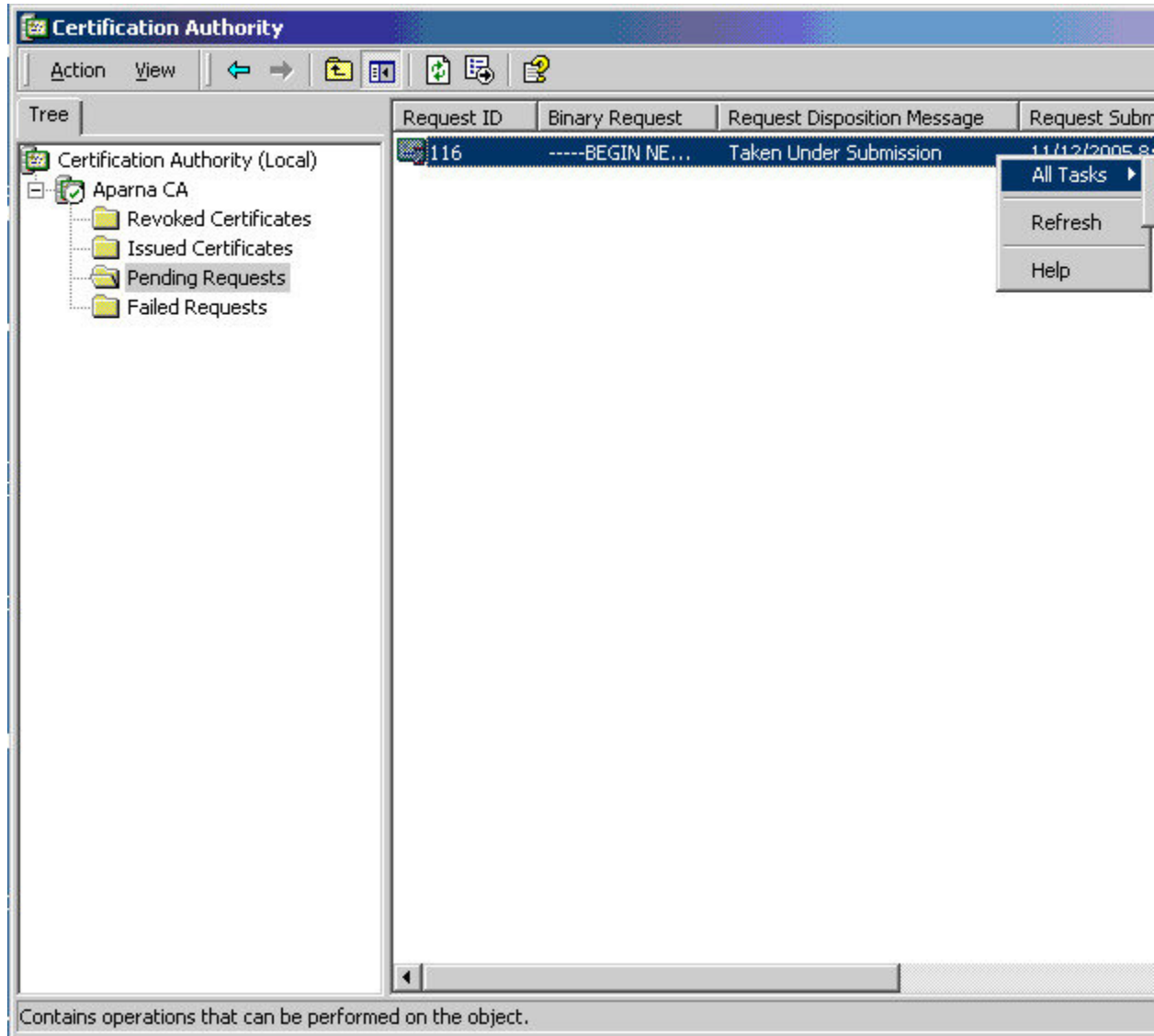
Certificate Pending

Your certificate request has been received. However, you must wait for an administrator to approve your request.

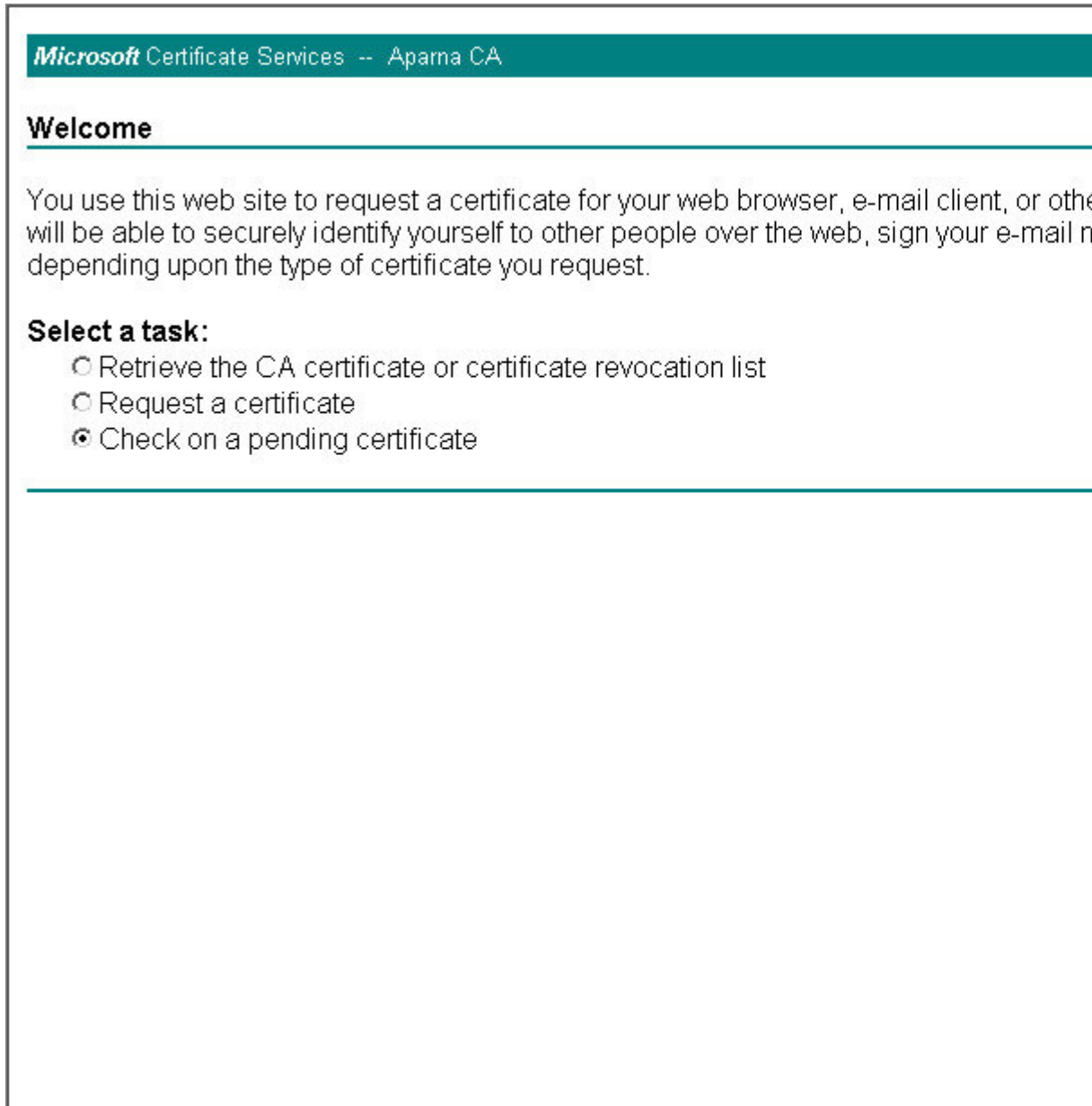
Please return to this web site in a day or two to retrieve your certificate.

Note: You must return with **this** web browser within 10 days to retrieve your certificate.

ステップ 6 CA 管理者により証明書要求が承認されます。



- ステップ 7** Microsoft Certificate Services Web インターフェイス上の [Check on a pending certificate] オプション ボタンを選択し、[Next] ボタンをクリックします。



ステップ 8 確認する証明書要求を選択し、[Next] をクリックします。

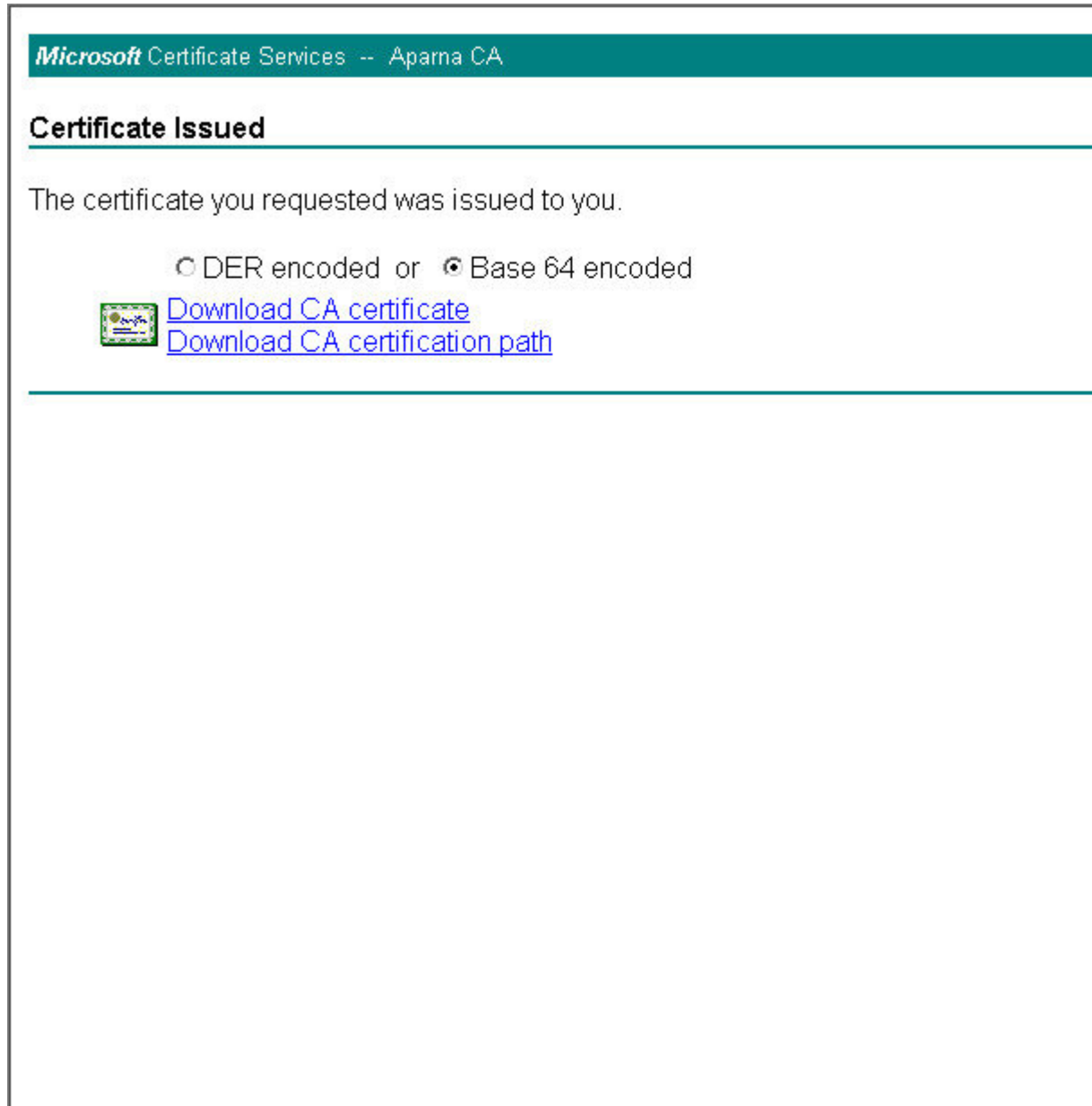
Microsoft Certificate Services -- Apama CA

Check On A Pending Certificate Request

Please select the certificate request you want to check:

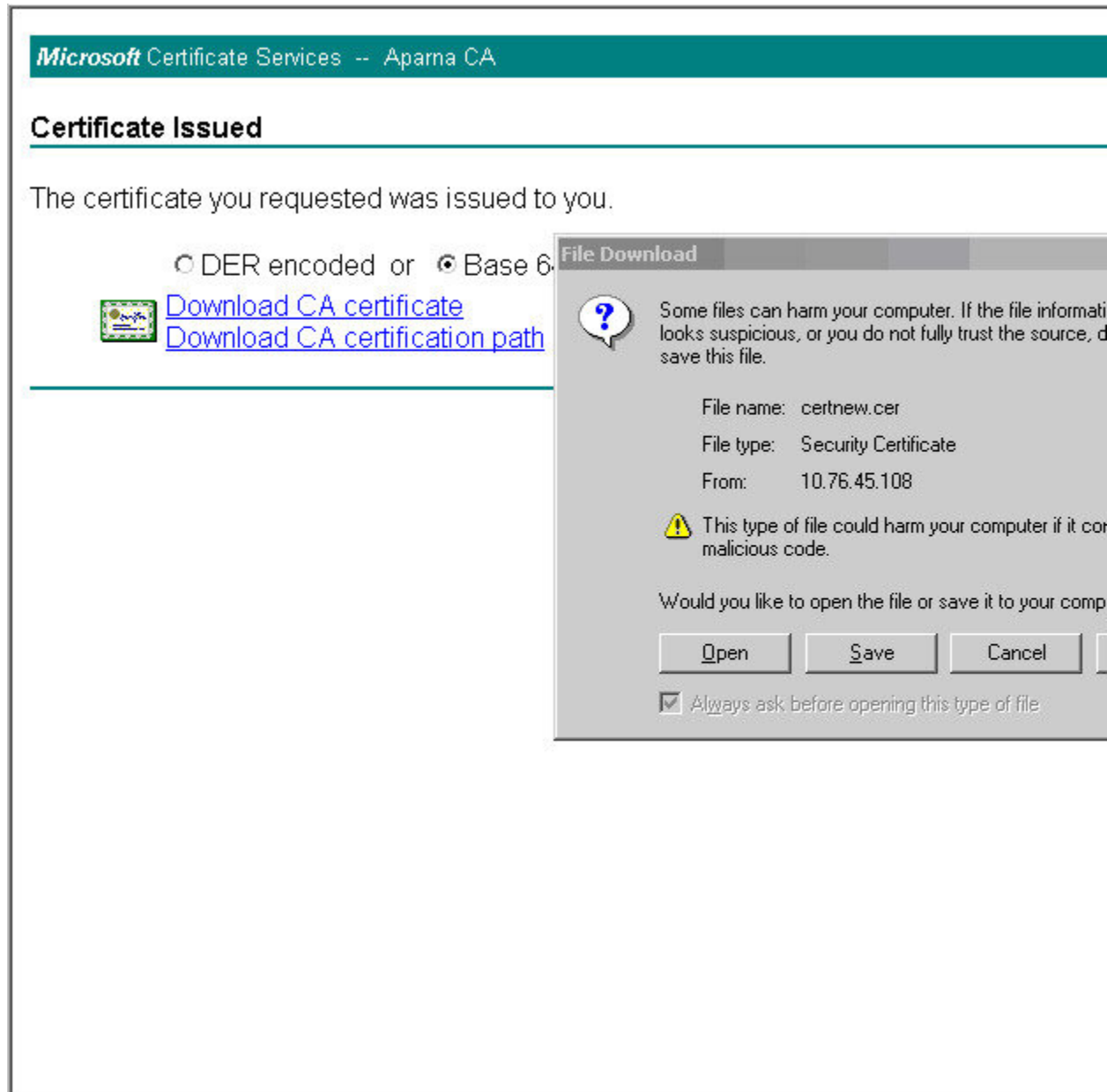
Saved-Request Certificate (12 Nopember 2005 20:30:22)

ステップ 9 [Base 64 encoded] を選択し、[Download CA certificate] リンクをクリックします。



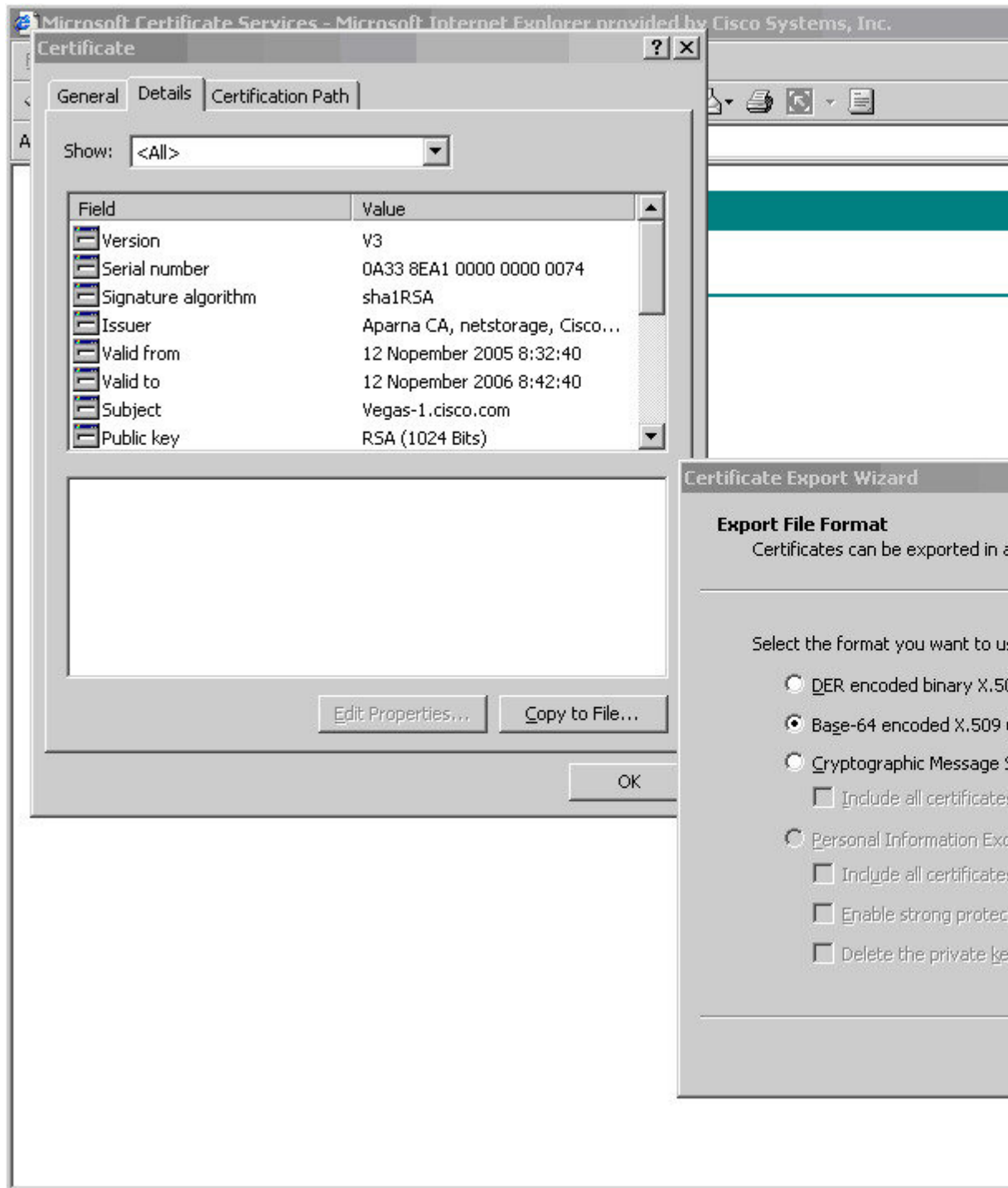
The screenshot displays a web page from Microsoft Certificate Services for the 'Aparna CA'. The page title is 'Certificate Issued'. Below the title, it states 'The certificate you requested was issued to you.' There are two radio buttons for encoding: 'DER encoded' (unselected) and 'Base 64 encoded' (selected). Below these options are two blue underlined links: 'Download CA certificate' and 'Download CA certification path'. A small icon of a certificate is visible to the left of the first link.

ステップ 10 [File Download] ダイアログボックスで、[Open] をクリックします。

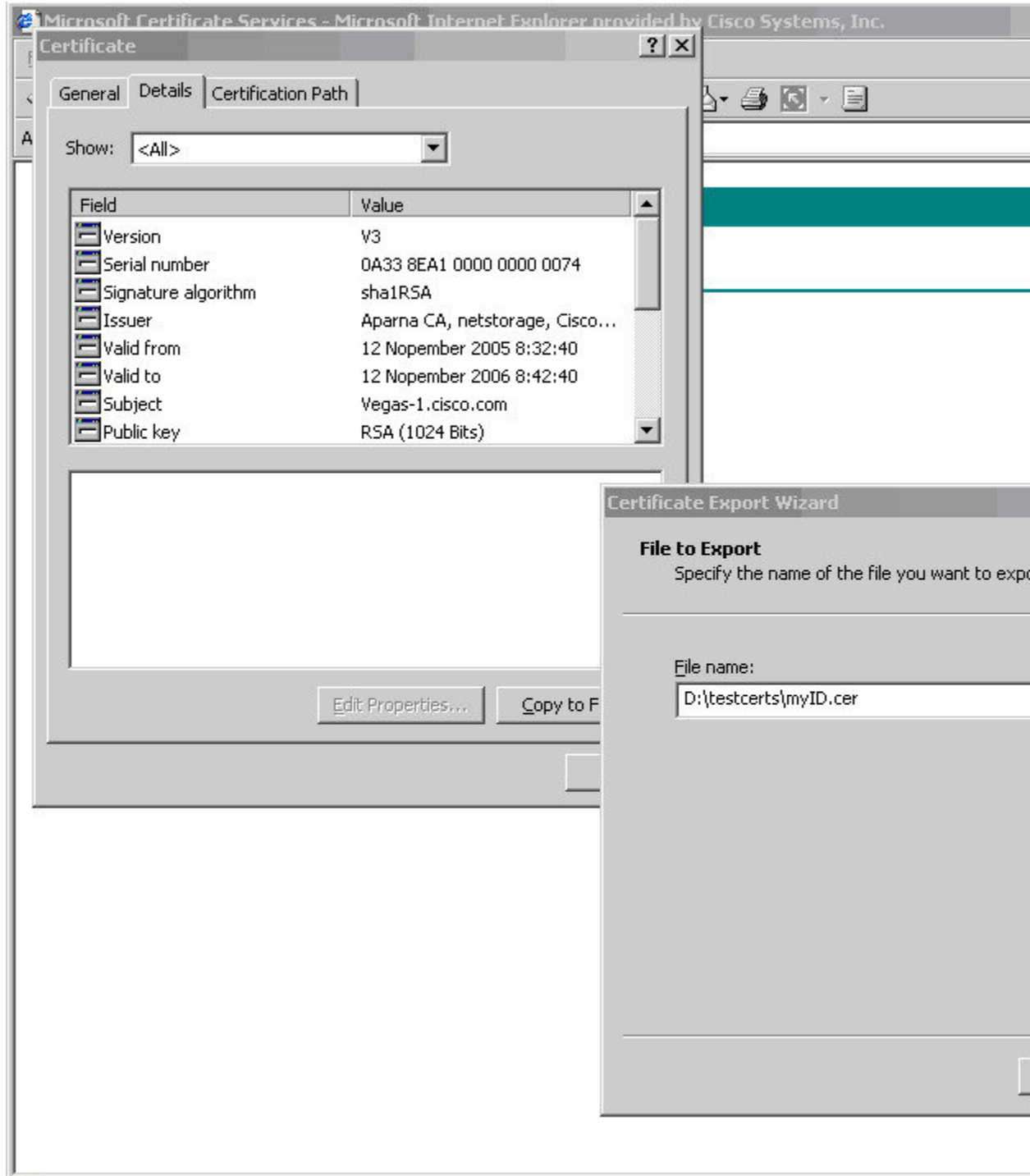


ステップ 11 [Certificate] ダイアログボックスで [Details] タブをクリックし、[Copy to File] ボタンをクリックします。[Certificate Export Wizard] ダイアログボックスで [Base-64 encoded X.509 (.CER)] オプション

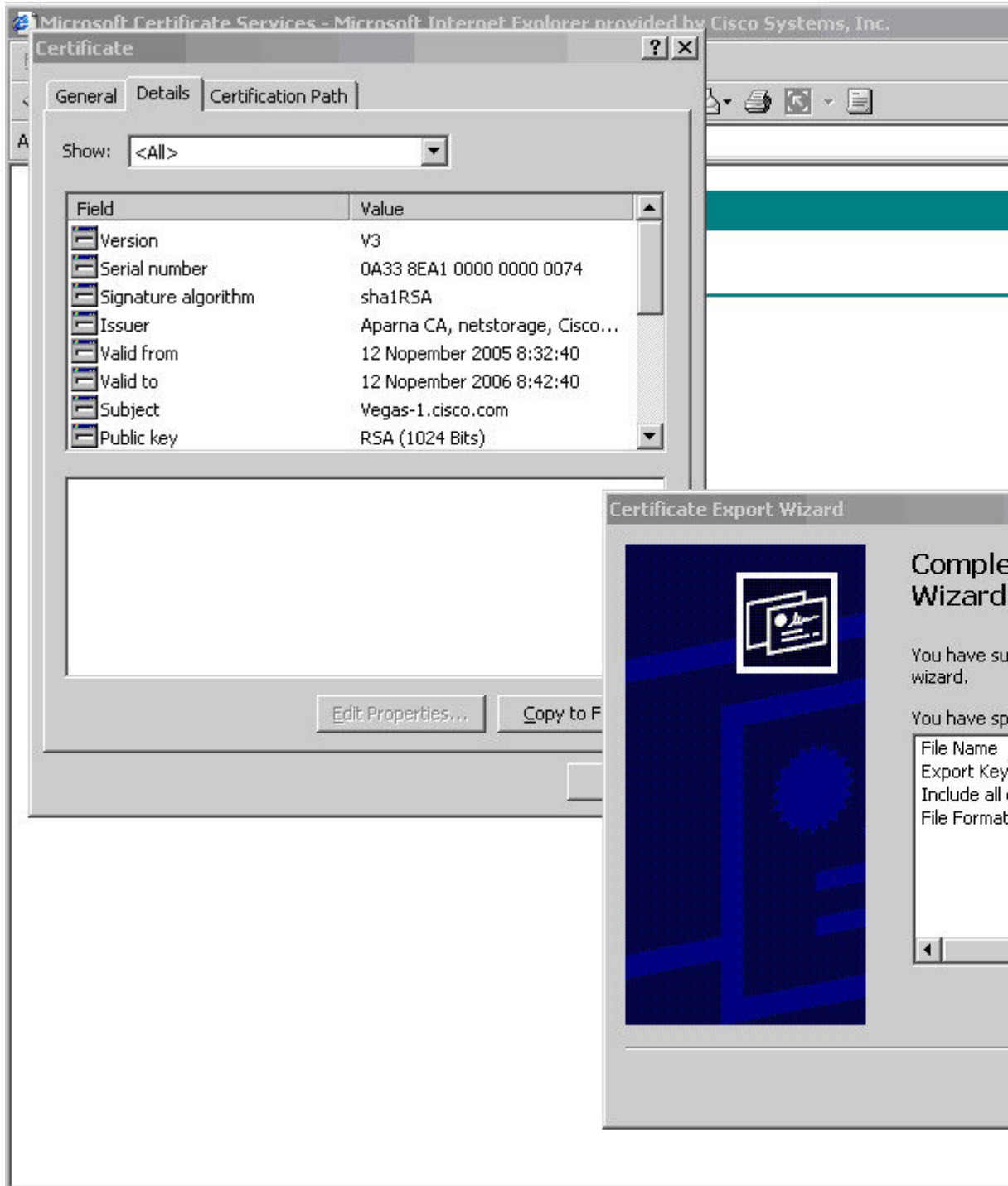
シヨン ボタンを選択し、[Next] ボタンをクリックします。



ステップ 12 [Certificate Export Wizard] ダイアログボックスの [File name:] テキストボックスに宛先ファイル名を入力し、[Next] をクリックします。



ステップ 13 [Finish] をクリックします。



ステップ 14 Microsoft Windows の **type** コマンドを使用して、base-64 符号化形式のアイデンティティ証明書を表示します。

```
C:\WINNT\system32\cmd.exe

D:\testcerts>type myID.cer
-----BEGIN CERTIFICATE-----
MIIEADCCA6ggAwIBAgIKCj00oQAAAAAADANBgkqhkiG9w0BAQUFADCBIkDEgMB4G
CSqGSIb3DQEJARYRYW1hbWRRZUBjaXNjb5jb20xCzAIBgNUBAYTAkLOMRIwEAyD
UQQIEwLLYXJuYXRha2ExEjAQBgNUBAc1CUJhbmdhbG9yZTEOMAAGA1UEChMFQ2lz
Y28xZARARBgNUBAsTCA5IldHN0b3JhZ2UxEjAQBgNUBAMTCUFWYXJuYSBDQTAeFw0w
NTExMTIwMzA0NDBaFw0wNTExMTIwMzEyNDBaMBwXGjAYBgNUBAMTEUZlZ2FzLTUu
Y2lzY28uY29tMIgfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNUAcDjQu41C
dQ1WkjkjSICdpLfK5eJSmNCQujGpzcuksZPFxjF2UoieCYE8y1ncWyw5E08rJ47
gLxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xwYAu8rDfz8jMCnIM4W1aY/q2q4Gb
x7RifdU06uFqFZEgs17/E1ash9LxLwIDAQABo4ICEzCCAq8wJQYDUR0RAQH/BBsw
GYIRUmUnYXMcMS5jaXNjb5jb22HBKwWH6IwHQYDUR0OBBYEFKCLi+2sspwEfgR
bhWm1Uyo9jngMIHMBgNUHSMEGcQwgcGAFCCo8kaDG6wJTEUNjskYUBoLPmxxoYGW
pIGTMIQMSAwHgYJKoZIHvcNAQkBFhFhbWFuZGt1QGNpc2NoLmNoIElMAkGA1UE
BHMCSU4xEjAQBgNUBAgICUthcm5hdGFyYTESMBAAGA1UEBxMjQmZ2FzL3JlMQ4w
DAYDUQQKEwUDaXNjbzETMBEGA1UECzMKbmU0c3RvcnFnZTESMBAAGA1UEAxMjQX
cm5hIENBghAFYnkjrLQZlE9JEiWMrR16MGsGA1UdHwRkMG1wLqAsCqGKgh0dHA6
Ly9zc2UtdG9vQ2UydEUucm9sbC9BcGFybmlMjBDQS5jcmwwMKAuoCyGKmZpbGU6
Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNydCBigYIKwYBBQUH
AQEefjB8MDsGCCsGAQUFBzAChio9odHRwOi8vc3NlLTA4L0NlcnRFbnJvbGwvc3Nl
LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZT0vL1xc3NlLTA4
XENlcnRFbnJvbGwvc3NlLTA4X0FwYXJuYSUyMENBLmNydANBgkqhkiG9w0BAQUF
AANBA DbGBGsbG9NLh9xe0TWBNbm24U69ZSuDDc0cUZUUTgrpn1qUpPyejtsyf1w
E36cIZu4WsExREqxbTk8ycx7U5o=
-----END CERTIFICATE-----

D:\testcerts>
```

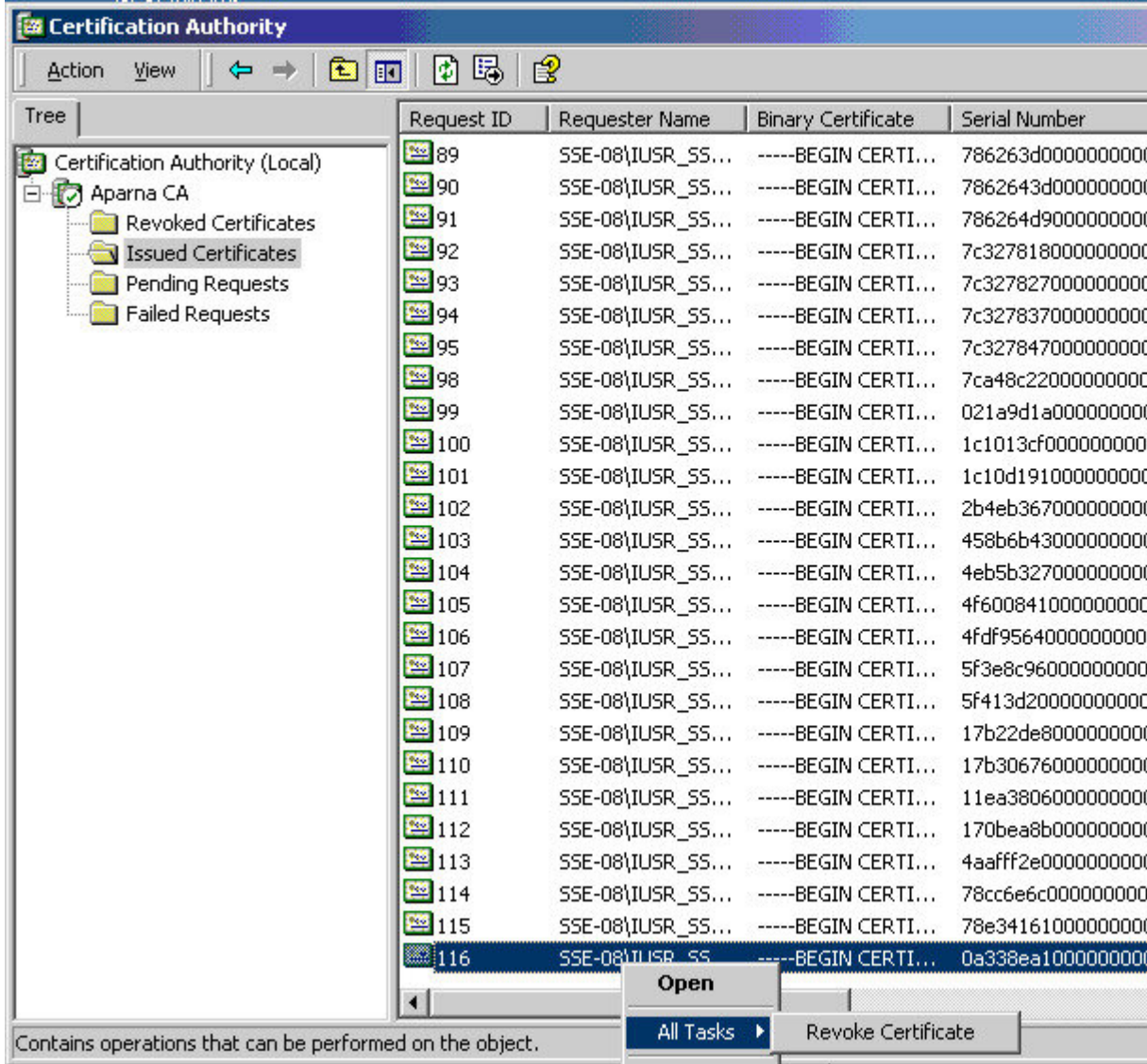
証明書の取り消し

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。

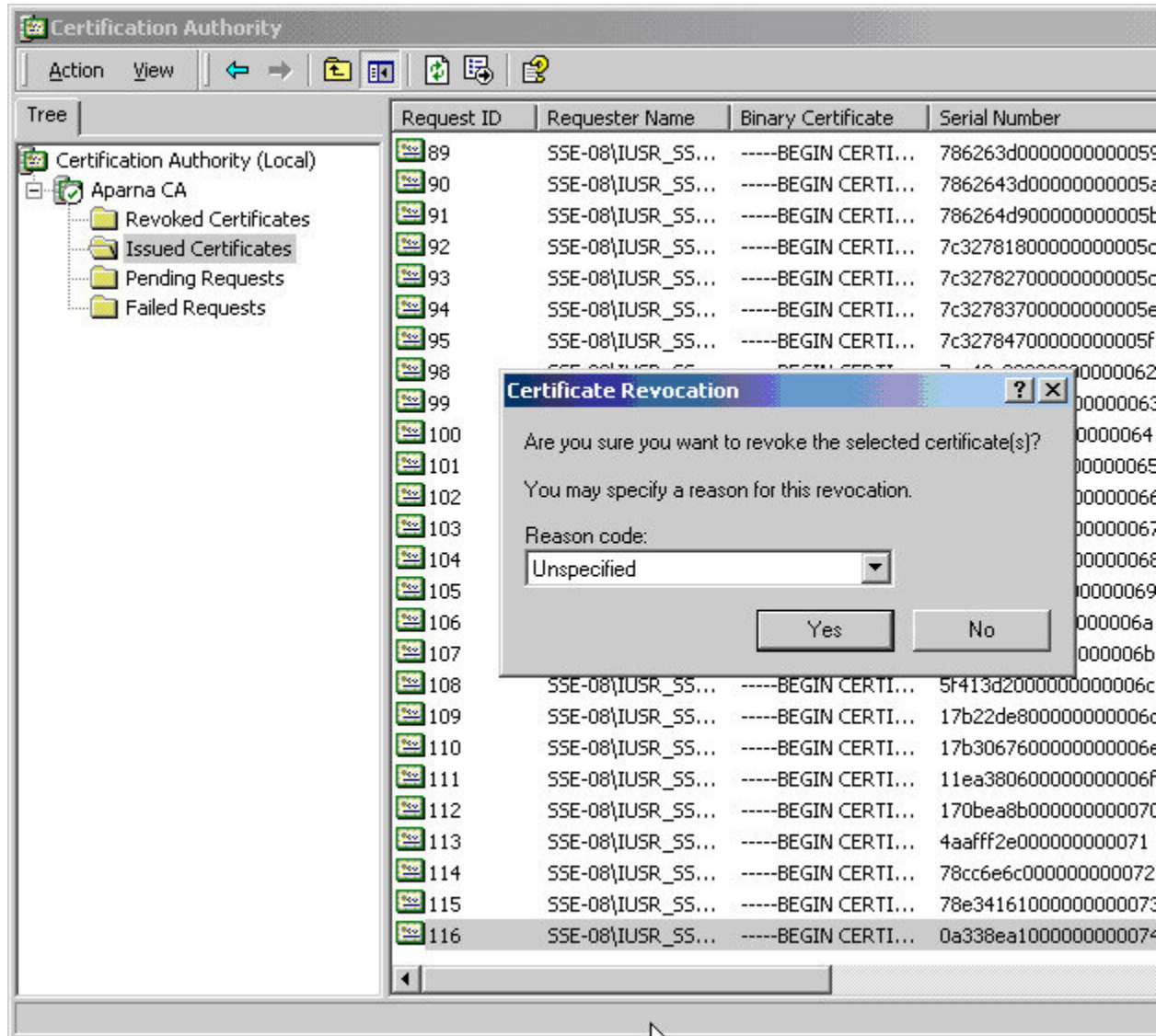
Procedure

ステップ 1 Certification Authority ツリーで、**Issued Certificates** フォルダをクリックします。リストから、失効させる証明書を右クリックします。

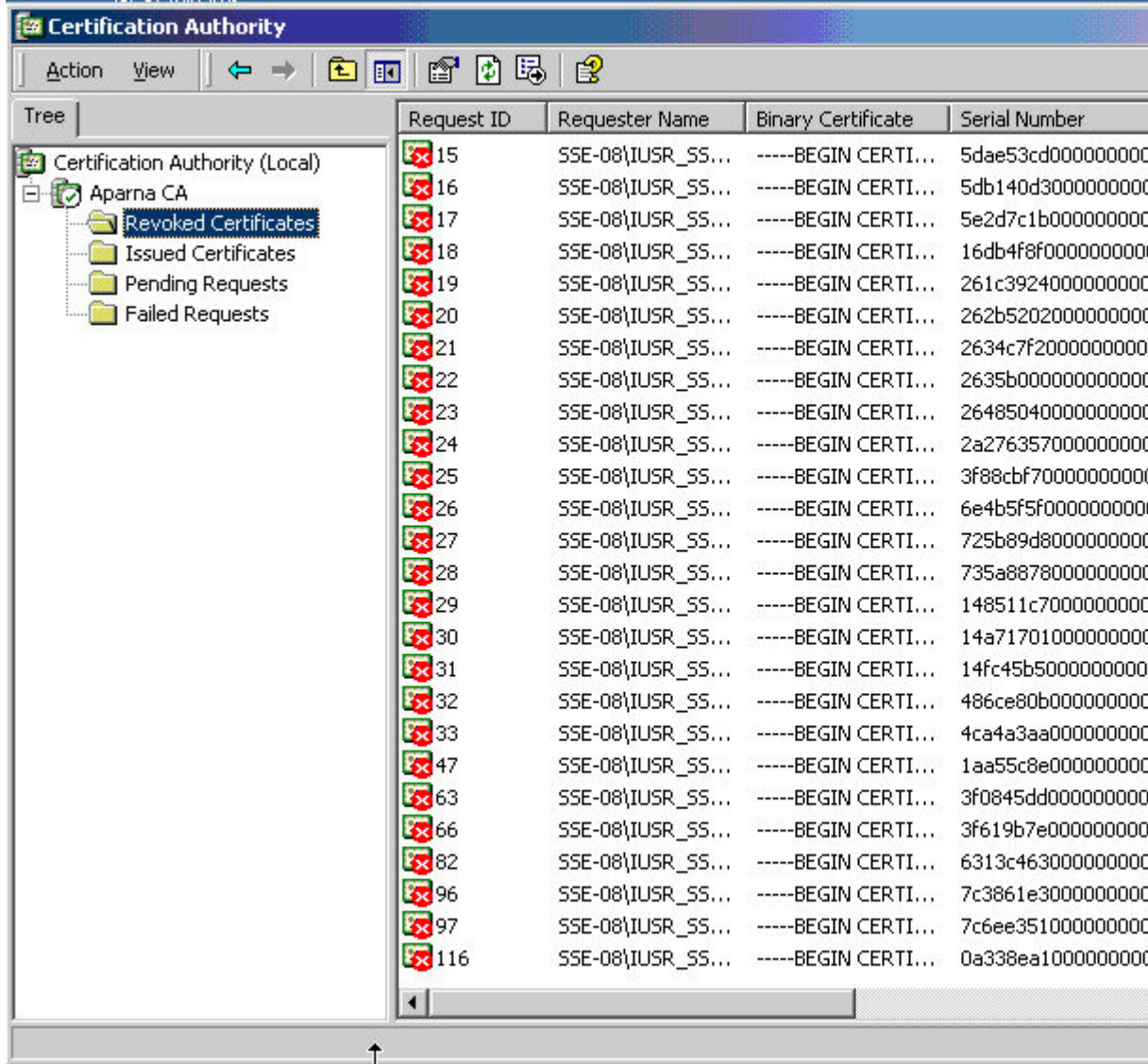
ステップ2 [All Tasks] > [Revoke Certificate] を選択します。



ステップ3 [Reason code] ドロップダウン リストから失効の理由を選択し、[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。

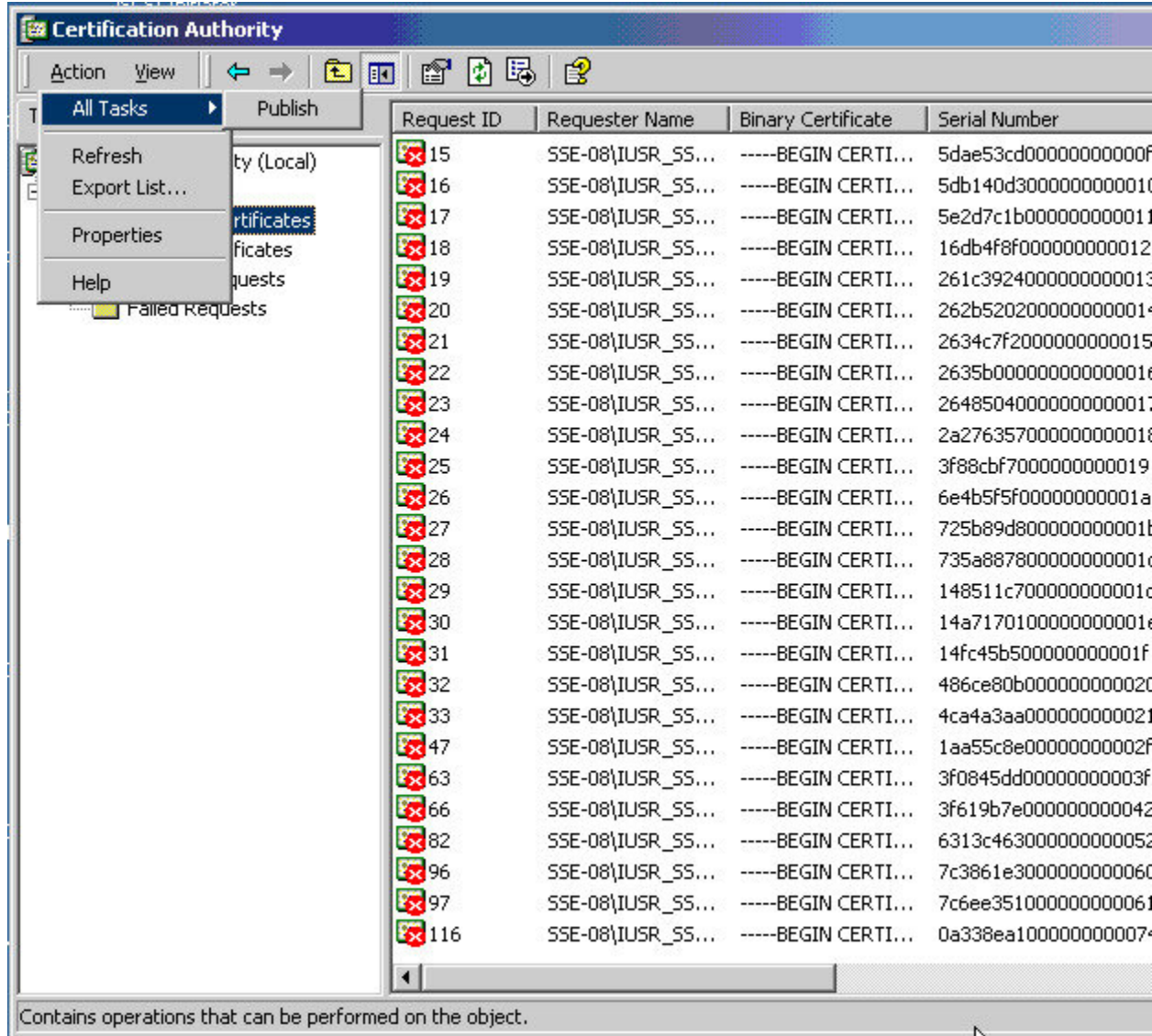


CRL の作成と公開

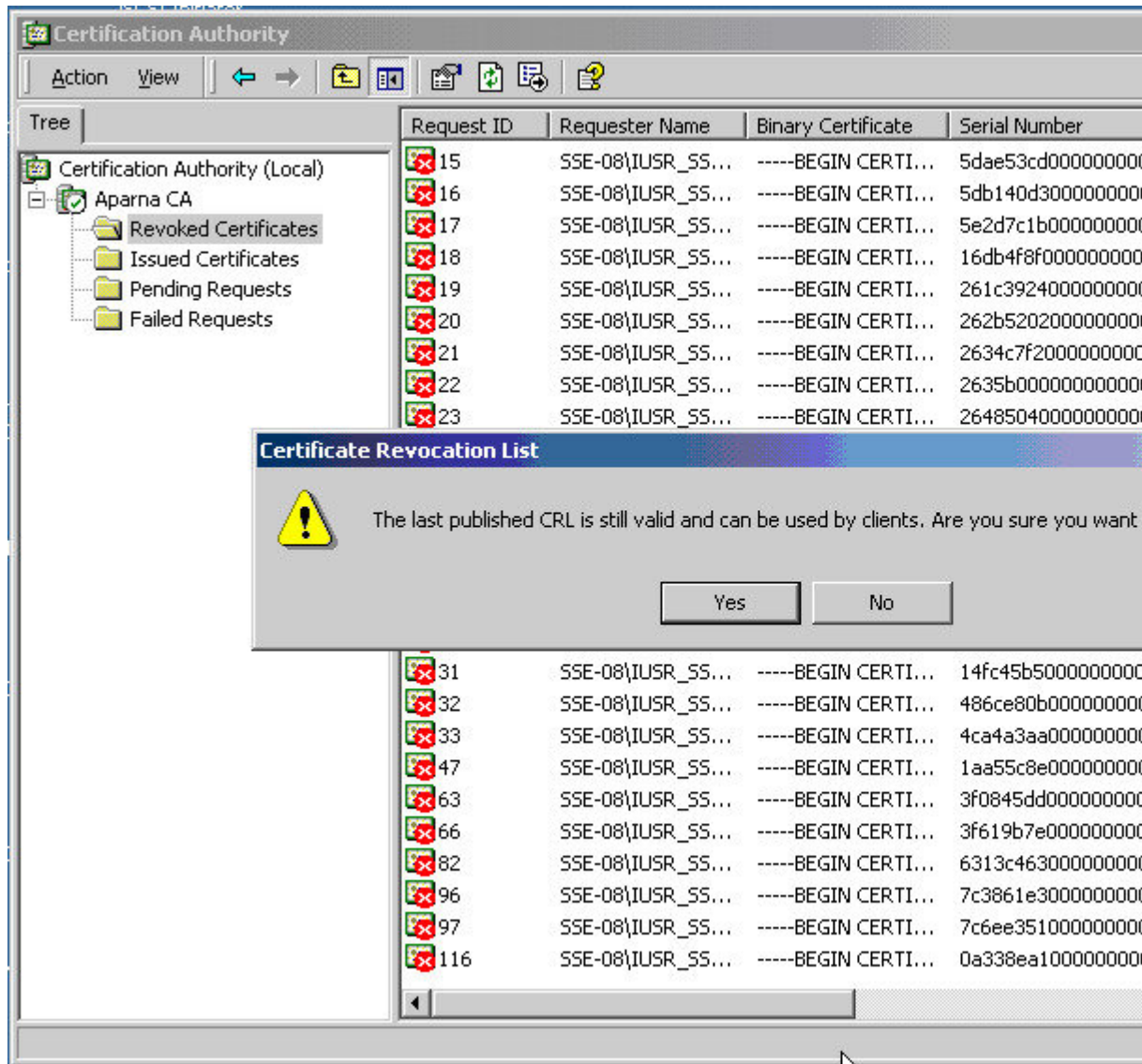
Microsoft CA 管理者プログラムを使用して CRL を作成および公開する手順は、次のとおりです。

Procedure

ステップ1 [Certification Authority] 画面で、[Action] > [All Tasks] > [Publish] を選択します。



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、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 Web インターフェイス上の [Request the CA certificate or certificate revocation list] オプション ボタンを選択し、[Next] ボタンをクリックします。

Microsoft Certificate Services -- Apama CA

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other software. You will be able to securely identify yourself to other people over the web, sign your e-mail messages, and perform other tasks 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] リンクをクリックします。

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 t

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

Choose file to download:

CA Certificate:

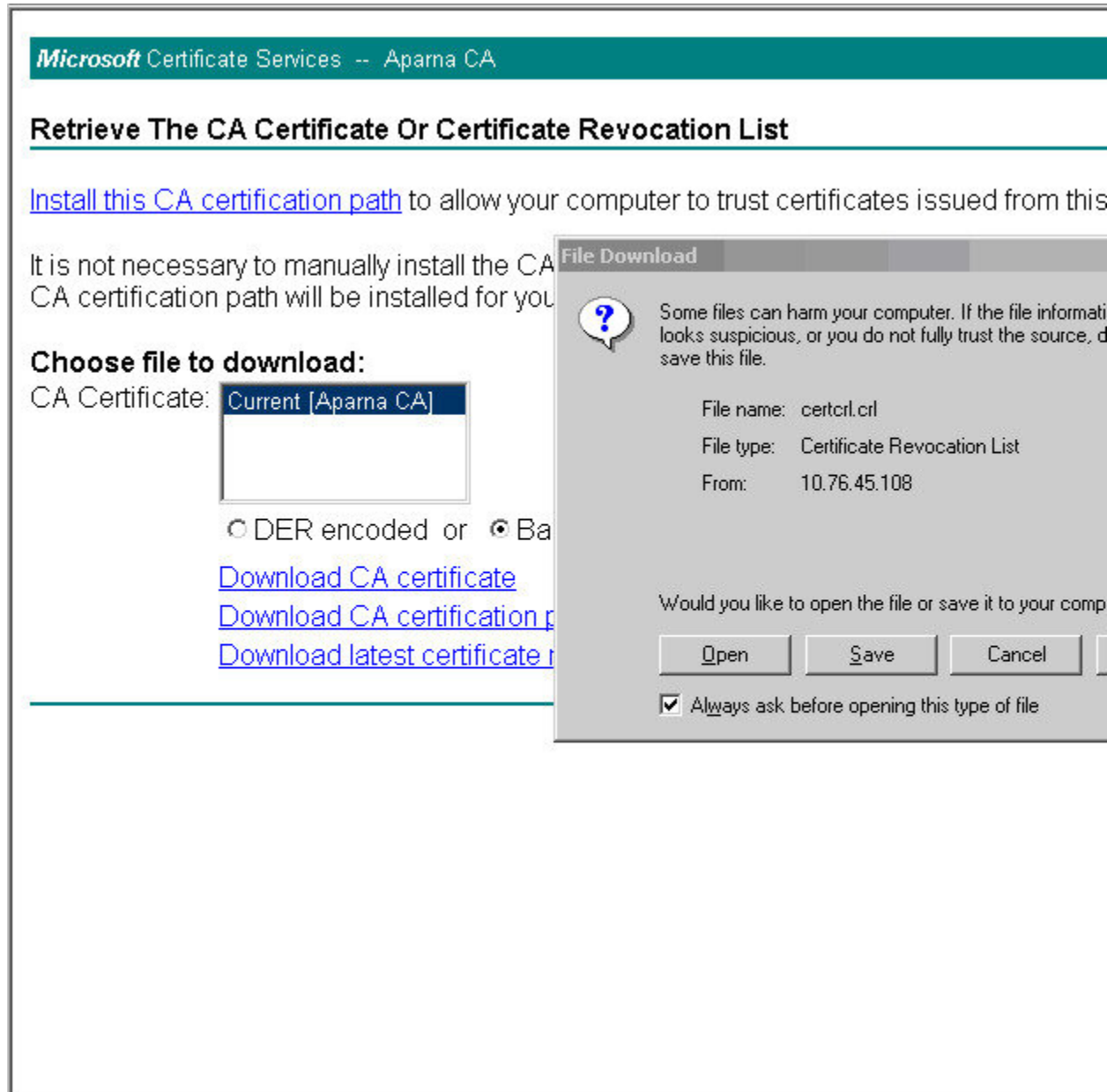
DER encoded or Base 64 encoded

[Download CA certificate](#)

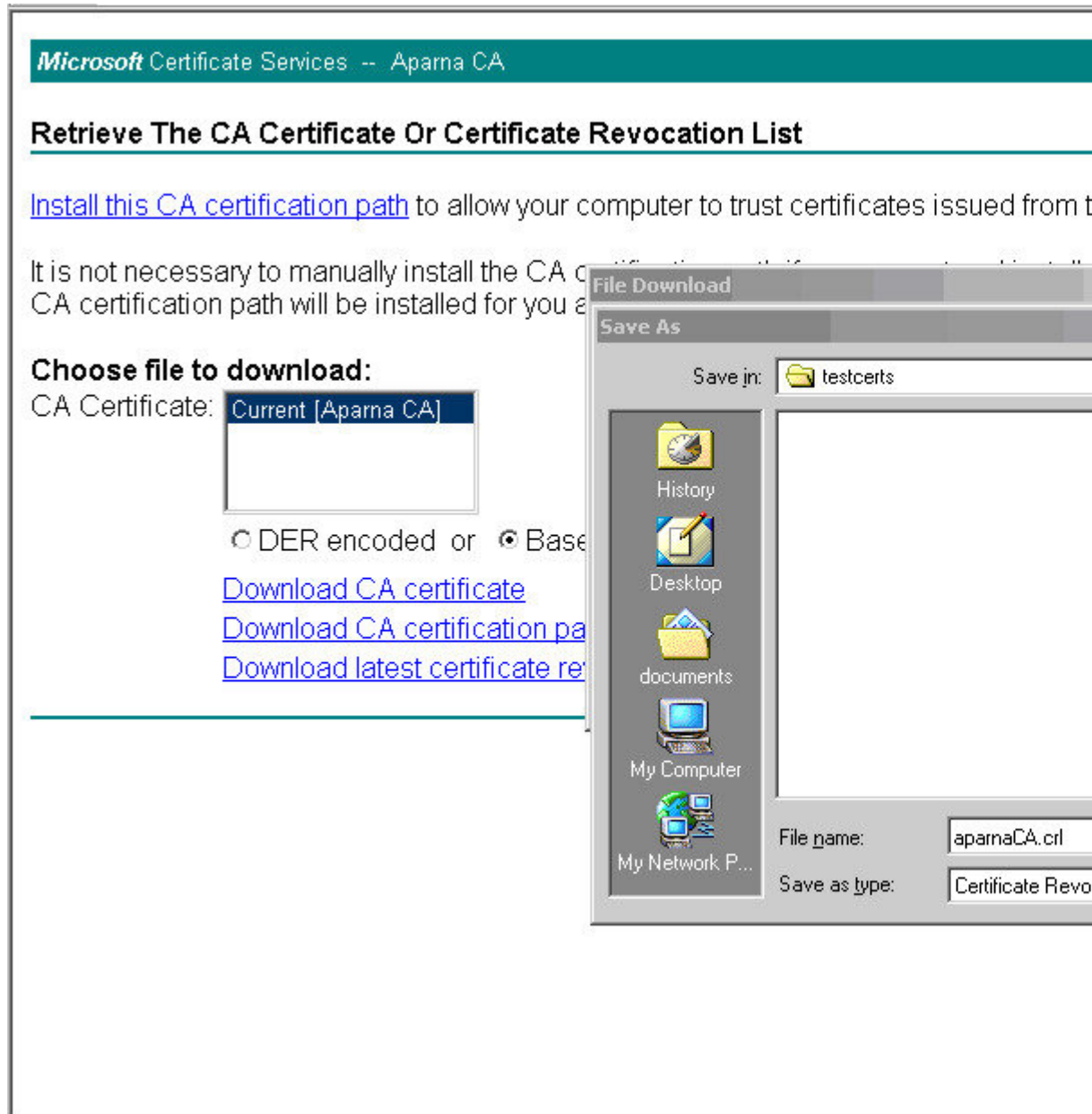
[Download CA certification path](#)

[Download latest certificate revocation list](#)

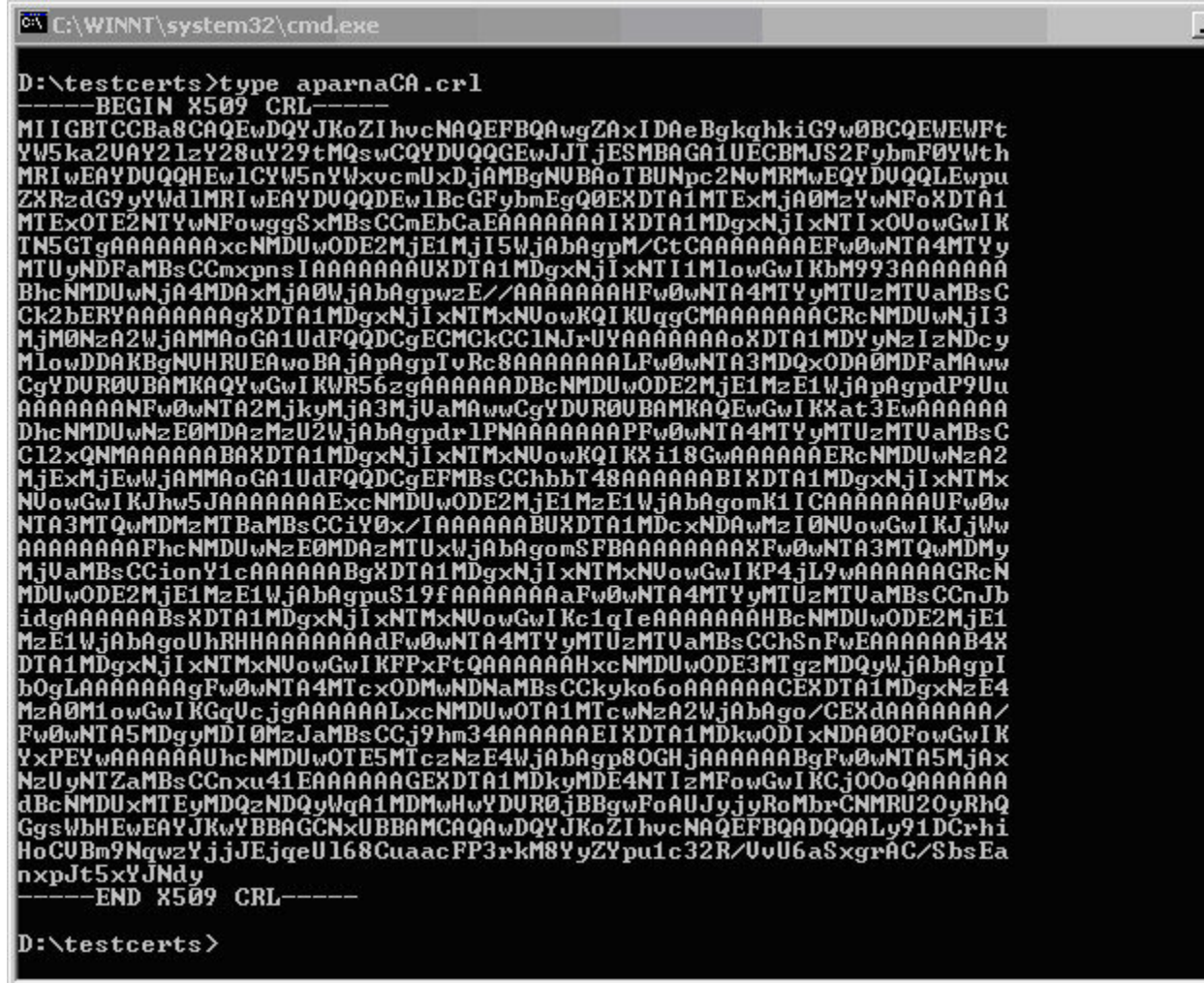
ステップ3 [File Download] ダイアログボックスで、[Save] をクリックします。



ステップ 4 [Save As] ダイアログボックスに宛先ファイル名を入力し、[Save] をクリックします。



ステップ 5 Microsoft Windows の **type** コマンドを使用して、CRL を表示します。



CRL のインポート

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。

Procedure

ステップ 1 CRL ファイルを MDS スイッチのブートフラッシュにコピーします。

```
SwitchA# copy tftp:aparnaCA.crl bootflash:aparnaCA.crl
```

ステップ 2 CRL を設定します。

```
SwitchA# config terminal
SwitchA(config)# crypto ca crl request myCA bootflash:aparnaCA.crl
```

```
SwitchA(config)#
```

ステップ3 CRL の内容を表示します。

```
SwitchA(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: 611B09A1000000000002
    Revocation Date: Aug 16 21:52:19 2005 GMT
  Serial Number: 4CDE464E000000000003
    Revocation Date: Aug 16 21:52:29 2005 GMT
  Serial Number: 4CFC2B42000000000004
    Revocation Date: Aug 16 21:52:41 2005 GMT
  Serial Number: 6C699EC2000000000005
    Revocation Date: Aug 16 21:52:52 2005 GMT
  Serial Number: 6CCF7DDC000000000006
    Revocation Date: Jun 8 00:12:04 2005 GMT
  Serial Number: 70CC4FFF000000000007
    Revocation Date: Aug 16 21:53:15 2005 GMT
  Serial Number: 4D9B1116000000000008
    Revocation Date: Aug 16 21:53:15 2005 GMT
  Serial Number: 52A80230000000000009
    Revocation Date: Jun 27 23:47:06 2005 GMT
    CRL entry extensions:
      X509v3 CRL Reason Code:
        CA Compromise
  Serial Number: 5349AD4600000000000A
    Revocation Date: Jun 27 23:47:22 2005 GMT
    CRL entry extensions:
      X509v3 CRL Reason Code:
        CA Compromise
  Serial Number: 53BD173C00000000000B
    Revocation Date: Jul 4 18:04:01 2005 GMT
    CRL entry extensions:
      X509v3 CRL Reason Code:
        Certificate Hold
  Serial Number: 591E7ACE00000000000C
    Revocation Date: Aug 16 21:53:15 2005 GMT
  Serial Number: 5D3FD52E00000000000D
    Revocation Date: Jun 29 22:07:25 2005 GMT
    CRL entry extensions:
      X509v3 CRL Reason Code:
        Key Compromise
  Serial Number: 5DAB771300000000000E
    Revocation Date: Jul 14 00:33:56 2005 GMT
  Serial Number: 5DAE53CD00000000000F
    Revocation Date: Aug 16 21:53:15 2005 GMT
  Serial Number: 5DB140D3000000000010
    Revocation Date: Aug 16 21:53:15 2005 GMT
```



```
Serial Number: 5E2D7C1B000000000011
  Revocation Date: Jul  6 21:12:10 2005 GMT
  CRL entry extensions:
    X509v3 CRL Reason Code:
      Cessation Of Operation
Serial Number: 16DB4F8F000000000012
  Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 261C3924000000000013
  Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 262B5202000000000014
  Revocation Date: Jul 14 00:33:10 2005 GMT
Serial Number: 2634C7F2000000000015
  Revocation Date: Jul 14 00:32:45 2005 GMT
Serial Number: 2635B000000000000016
  Revocation Date: Jul 14 00:31:51 2005 GMT
Serial Number: 26485040000000000017
  Revocation Date: Jul 14 00:32:25 2005 GMT
Serial Number: 2A276357000000000018
  Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 3F88CBF7000000000019
  Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 6E4B5F5F00000000001A
  Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 725B89D800000000001B
  Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 735A887800000000001C
  Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 148511C700000000001D
  Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 14A7170100000000001E
  Revocation Date: Aug 16 21:53:15 2005 GMT
Serial Number: 14FC45B500000000001F
  Revocation Date: Aug 17 18:30:42 2005 GMT
Serial Number: 486CE80B000000000020
  Revocation Date: Aug 17 18:30:43 2005 GMT
Serial Number: 4CA4A3AA000000000021
  Revocation Date: Aug 17 18:30:43 2005 GMT
Serial Number: 1AA55C8E00000000002F
  Revocation Date: Sep  5 17:07:06 2005 GMT
Serial Number: 3F0845DD00000000003F
  Revocation Date: Sep  8 20:24:32 2005 GMT
Serial Number: 3F619B7E000000000042
  Revocation Date: Sep  8 21:40:48 2005 GMT
Serial Number: 6313C463000000000052
  Revocation Date: Sep 19 17:37:18 2005 GMT
Serial Number: 7C3861E3000000000060
  Revocation Date: Sep 20 17:52:56 2005 GMT
Serial Number: 7C6EE351000000000061
  Revocation Date: Sep 20 18:52:30 2005 GMT
Serial Number: 0A338EA1000000000074      <-- 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
```

上限

次の表に、CA およびデジタル証明書のパラメータの最大限度を示します。

Table 11: CA およびデジタル証明書の最大限度

機能	最大制限
スイッチ上で宣言するトラスト ポイント	16
スイッチ上で生成する RSA キー ペア	16
RSA キー ペア サイズ	4096 ビット
スイッチ上に設定するアイデンティティ証明書	16
CA 証明書チェーンに含まれる証明書	10
特定の CA に対して認証されるトラスト ポイント	10

デフォルト設定

次の表に、CA およびデジタル証明書のパラメータのデフォルト設定を示します。

Table 12: CA およびデジタル証明書の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	Switch FQDN
RSA キー ペアのモジュール	1024
RSA キー ペアのエクスポートの可否	Yes
トラスト ポイントの失効チェック方式	CRL



CHAPTER 8

SSH サービスおよび Telnet の構成

この章では、Cisco MDS デバイス上でセキュア シェル プロトコル (SSH) サービスおよび Telnet を設定する手順について説明します。

この章は、次の項で構成されています。

- [SSH サービスに関する情報, on page 197](#)
- [Telnet サーバ, on page 199](#)
- [SSH の設定, on page 199](#)
- [SSH のデフォルト設定, on page 211](#)

SSH サービスに関する情報

セキュア シェル (SSH) は、Cisco NX-OS CLI に対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。SSH キーは、次の SSH オプションに使用できます。

- Rivest, Shamir, Adelman (RSA) を使用する SSH2
- DSA を使用する SSH2

Cisco MDS NX-OS リリース 8.2(1) 以降、SHA2 フィンガープリントハッシュはすべての Cisco MDS デバイスでデフォルトでサポートされています。

RSA キーによるセキュア SSH 接続は、Cisco MDS 9000 シリーズのすべてのスイッチでデフォルトで使用できます。DSA キーによるセキュア SSH 接続が必要な場合は、デフォルトの SSH 接続をディセーブルにし、DSA キーを生成して、SSH 接続をイネーブルにする必要があります ([SSH サーバー キー ペアの生成, on page 201](#) を参照)。

サーバー キーを生成するには、`ssh key` コマンドを使用します。



Caution SSH でスイッチにログインし、**aaa authentication login default none** コマンドを発行した場合、ログインするために1つ以上のキーストロークを入力する必要があります。少なくとも1つのキーストロークを入力せずに **Enter** キーを押すと、ログインは拒否されます。

SSH サービスの設定の詳細については、次を参照してください。 [SSH サービスおよび Telnet の構成, on page 197](#)

SSH サーバー

SSH サーバを使用すると、SSH クライアントは Cisco MDS デバイスとの間で暗号化された安全な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 MDS 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。

SSH がサポートするユーザ認証メカニズムには、Remote Authentication Dial-In User Service (RADIUS)、TACACS+、LDAP、およびローカルに格納されたユーザ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 クライアントは、SSH プロトコルで稼働しデバイス認証および暗号化を提供するアプリケーションです。Cisco MDS デバイスは、SSH クライアントを使用して、別の Cisco MDS デバイスまたは SSH サーバの稼働する他のデバイスとの間で暗号化された安全な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 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。

SSH サーバキー

SSH では、Cisco MDS 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 サーバキーは、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 サービスは、SSH バージョン 2 で使用する次の 2 種類のキーペアを受け入れます。

- **dsa** オプションでは、SSH バージョン 2 プロトコル用の DSA キーペアを作成します。
- **rsa** オプションでは、SSH バージョン 2 プロトコル用の RSA キーペアを作成します。

デフォルトでは、Cisco NX-OS ソフトウェアは 1024 ビットの RSA キーを作成します。

SSH は、次の公開キー形式をサポートします。

- OpenSSH
- IETF SSH (SECSH)
- Privacy-Enhanced Mail (PEM) の公開キー証明書



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 MDS 9000 ファミリー スイッチ製品の SSH 認証はホスト認証に X.509 デジタル証明書のサポートを提供します。X.509 デジタル証明書は出处と完全性を保証する 1 つのデータ項目です。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。

証明書インフラストラクチャは Secure Socket Layer (SSL) をサポートする最初の証明書を使用し、セキュリティインフラストラクチャにより照会または通知の形で返信を受け取ります。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。

スイッチは、X.509 証明書を使用する SSH 認証、または公開キー証明書を使用する SSH 認証のいずれかに設定できますが、両方に設定することはできません。いずれかに設定されている場合は、その認証が失敗すると、パスワードの入力を求められます。

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。

デフォルトでは、Telnet サーバは Cisco NX-OS デバイス上でディセーブルになっています。

SSH の設定

ここでは、SSH の設定方法について説明します。

SSH 名の構成

ユーザーのプライマリ SSH 接続の名前を構成するには、次の手順に従います。

始める前に

機能 SSH を有効にします。

手順

	コマンドまたはアクション	目的
ステップ 1	<pre>switch#ssh name ssh-nameuser-nameip-address</pre> <p>例 :</p> <pre>switch# ssh name myhost user 192.168.1.1</pre>	プライマリ SSH 接続の SSH 名を構成します。
ステップ 2	<pre>switch# no ssh name</pre> <p>例 :</p> <pre>switch# no ssh name myhost user 192.168.1.1</pre>	(オプション)SSH 接続の名前を削除します。
ステップ 3	<pre>switch# show ssh names</pre> <p>例 :</p> <pre>switch# show ssh names</pre>	(オプション)SSH 接続の名前を表示します。

SSH 接続の構成

ユーザーの SSH 接続を構成するには、次の手順に従います。

始める前に

- 機能 SSH を有効にします。
- SSH 名を構成します。SSH 名の設定については、[SSH 名の構成 \(199 ページ\)](#) 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	<pre>switch#ssh connectdummy</pre> <p>例 :</p> <pre>switch# ssh connect myhost</pre>	SSH 名の SSH 接続を構成します。
ステップ 2	<pre>switch# no ssh connect</pre> <p>例 :</p> <pre>switch# no ssh connect myhost</pre>	(オプション) SSH 接続を削除します。

	コマンドまたはアクション	目的
ステップ 3	<pre>switch# show ssh names</pre> <p>例 :</p> <pre>switch# show ssh names</pre>	(オプション)SSH接続の名前を表示します。

SSH サーバー キー ペアの生成

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。SSH サービスを確立する前に、SSH サーバキーペアおよび適切なバージョンが存在することを確認します。使用中の SSH クライアントバージョンに従って、SSH サーバー キー ペアを生成します。各キー ペアに指定するビット数は、768 ~ 2048 です。

Cisco MDS NX-OS リリース 8.2(1) 以降、FIPS モードの最小 RSA キー サイズは 2048 ビットである必要があります。

RSA キー ペアの最大値とデフォルトの詳細については、[Table 11: CA およびデジタル証明書の最大限度](#) および [Table 12: CA およびデジタル証明書のパラメータのデフォルト値](#) を参照してください。

SSH サービスは、SSH バージョン 2 で使用する 2 種類のキー ペアを受け入れます。

- **dsa** オプションでは、SSH バージョン 2 プロトコル用の DSA キー ペアを作成します。
- **rsa** オプションでは、SSH バージョン 2 プロトコル用の RSA キー ペアを作成します。



Caution SSH キーをすべて削除した場合、新しい SSH セッションを開始できません。

SSH サーバー キー ペアを生成する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **ssh key dsa 1024**

Example:

```
generating dsa key.....
generated dsa key
```

DSA サーバー キー ペアを生成します。

ステップ 3 switch(config)# **ssh key rsa 1024**

Example:

Procedure

- ステップ 1** switch# **copy tftp://10.10.1.1/secsh_file.pub bootflash:secsh_file.pub**
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。
- ステップ 2** switch# **configure terminal**
コンフィギュレーション モードに入ります。
- ステップ 3** switch(config)# **username admin sshkey file bootflash:secsh_file.pub**
ユーザー アカウント (admin) の SSH キーを指定します。
- ステップ 4** switch(config)# **no username admin sshkey file bootflash:secsh_file.pub**
(オプション) ユーザー アカウント (admin) の SSH キーを削除します。
-

PEM の公開キー証明書による SSH キーの指定

指定したユーザーの PEM フォーマット化された公開キー証明書形式の SSH キーを指定または削除するには、次の手順を実行します。

手順

- ステップ 1** switch# **copy tftp://10.10.1.1/cert.pem bootflash:cert.pem**
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。
- ステップ 2** switch# **configure terminal**
switch(config)#
コンフィギュレーション モードに入ります。
- ステップ 3** switch(config)# **username admin sshkey file bootflash:cert.pem**
ユーザー アカウント (usam) の SSH キーを指定します。
- ステップ 4** switch(config)# **no username admin sshkey file bootflash:cert.pem**
(オプション) ユーザー アカウント (usam) の SSH キーを削除します。
-

ログイン グレイス タイムの SSH コネクションの構成

リモート デバイスから Cisco MDS デバイスへの SSH 接続のログイン 猶予時間を設定できます。これにより、クライアントが自身を認証するための 猶予時間が構成されます。SSH セッションへのログイン時間が指定された 猶予時間を超えると、セッションが切断され、再度ログインする必要があります。



Note リモート デバイスの SSH サーバをイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <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	feature ssh Example: <pre>switch# feature ssh switch(config)#</pre>	SSH を有効にします。
ステップ 3	ssh login-gracetime number Example: <pre>switch(config)# ssh login-gracetime 120</pre>	<p>リモート デバイスから Cisco MDS デバイスへの SSH 接続のログイン 猶予時間を秒単位で構成します。SSH がセッションを切断する前に、SSH サーバへの認証が成功するまでの時間を指定します。デフォルトログイン 猶予時間は 120 秒です。範囲は 10 ~ 600 です。</p> <p>Note このコマンドの no 形式は、設定されたログイン 猶予時間を削除し、デフォルト値の 120 秒にリセットします。</p>
ステップ 4	(Optional) exit Example: <pre>switch(config)# exit</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 5	(Optional) show running-config security Example: <pre>switch(config)# show running-config security</pre>	構成された SSH ログインの 猶予時間を表示します。

	Command or Action	Purpose
ステップ 6	(Optional) show running-config security all Example: switch(config)# show running-config security all	構成されたまたはデフォルト SSH ログインの猶予時間を表示します。
ステップ 7	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	(任意) 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。

生成したキー ペアの上書き

必要なバージョンの SSH キー ペア オプションがすでに生成されている場合は、前回生成されたキー ペアをスイッチに上書きさせることができます。

前回生成されたキー ペアを上書きする手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **ssh key dsa force**

Example:

```
switch(config)# ssh key dsa 512 force
deleting old dsa key.....
generating dsa key.....
generated dsa key
```

サーバー キー ペアの設定を試みます。必要なサーバー キー ペアがすでに設定されている場合は、**force** オプションを使用して、そのサーバー キー ペアを上書きします。古い DSA キーを削除し、新しく指定されたビットを使用してサーバー キー ペアを設定します。

SSH ログイン試行の最大回数の設定

SSH ログイン試行の最大回数を設定できます。許可される試行の最大回数を超えると、セッションが切断されます。



- (注) ログイン試行の合計回数には、公開キー認証、証明書ベースの認証、およびパスワードベースの認証を使用した試行が含まれます。イネーブルにされている場合は、公開キー認証が優先されます。証明書ベースとパスワードベースの認証だけがイネーブルにされている場合は、証明書ベースの認証が優先されます。これらすべての方法で、ログイン試行の設定された数を超えると、認証失敗回数を超過したことを示すメッセージが表示されます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal	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	ssh login-attempts number 例： switch(config)# ssh login-attempts 5	ユーザが SSH セッションへのログインを試行できる最大回数を設定します。ログイン試行のデフォルトの最大回数は3です。値の範囲は1～10です。 (注) このコマンドの no 形式を使用すると、以前のログイン試行の値が削除され、ログイン試行の最大回数がデフォルト値の3に設定されます。 SSH ログイン試行の値を2以上に設定することをお勧めします。
ステップ 3	(任意) show running-config security all 例： switch(config)# show running-config security all	SSH ログイン試行の設定された最大回数を表示します。
ステップ 4	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行設定を、スタートアップ設定にコピーします。

SSH ホストのクリア

clear ssh hosts コマンドは、信頼できる SSH ホストの既存のリストをクリアし、SCP/SFTP を特定のホストの **copy** コマンドとともに使用することを再許可します。

SCP/SFTP を **copy** コマンドとともに使用する場合は、信頼できる SSH ホストのリストが作成され、スイッチ内に保存されます（次の例を参照）。

SCP/SFTP を使用したファイルのコピー

```
switch# copy scp://abcd@10.10.1.1/users/abcd/abc

bootflash:abc The authenticity of host '10.10.1.1 (10.10.1.1)'
can't be established.
RSA1 key fingerprint is 01:29:62:16:33:ff:f7:dc:cc:af:aa:20:f8:20:a2:db.
Are you sure you want to continue connecting (yes/no)? yes
Added the host to the list of known hosts
(/var/home/admin/.ssh/known_hosts). [SSH key information about the host is
stored on the switch]
abcd@10.10.1.1's password:
switch#
```

SCP/SFTP を使用したファイルのコピー（SSH キーの変更によるエラーの発生）

copy コマンドとともに SCP/SFTP を使用する前にホストの SSH キーが変更された場合は、エラーが表示されます（次の例を参照）。

```
switch# copy scp://apn@10.10.1.1/isan-104

bootflash:isan-ram-1.0.4
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@  WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!  @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA1 host key has just been changed.
The fingerprint for the RSA1 key sent by the remote host is
36:96:ca:d7:29:99:79:74:aa:4d:97:49:81:fb:23:2f.
Please contact your system administrator.
Add correct host key in /mnt/pss/.ssh/known_hosts to get rid of this
message.
Offending key in /mnt/pss/.ssh/known_hosts:2
RSA1 host key for 10.10.1.1 has changed and you have requested strict
checking.
```

SSH または Telnet サービスのイネーブル化

デフォルトでは、SSH サービスは、RSA キーによってイネーブルになっています。

SSH または Telnet サービスをイネーブルまたはディセーブルにするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **feature ssh**

SSH サービスの使用を有効にします。

ステップ 3 switch(config)# **no feature ssh**

(オプション) SSH サービスの使用をディセーブル (デフォルト) にします。

ステップ 4 switch(config)# **feature telnet**

Telnet サービスの使用をイネーブルにします。

ステップ 5 switch(config)# **no feature telnet**

(オプション) Telnet サービスの使用をディセーブル (デフォルト) にします。

SSH プロトコル ステータスの表示

SSH プロトコルのステータスの表示

SSH プロトコルのステータス (イネーブルまたはディセーブル) 、およびそのスイッチでイネーブルになっているバージョンを表示するには、**show ssh server** コマンドを使用します (次の例を参照) 。

```
switch# show ssh server

ssh is enabled
version 1 enabled
version 2 enabled
```

サーバー キーペアの詳細の表示

指定されたキーまたはすべてのキーのサーバー キーペアの詳細を表示するには、**show ssh key** コマンドを使用します (次の例を参照) 。



Note SHA-2 値は安全だと考えられるため、Cisco MDS NX-OS リリース 8.2(1) 以降、**show ssh key [rsa | dsa]** コマンドの出力に表示されるフィンガープリント値は SHA-2 値になります

```
switch# show ssh key

rsa Keys generated:Thu Feb 16 14:12:21 2017
```

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQDQ7si46R6sYsWNBFRV+v662vbY6wmr9QMBU4N+BK8F
Iez+7U+2VRdyz1Mykbb1HF/2zth3ZWuTkrTX+8cMnVdcw1frvWY3g7CLmq5Wkxkq5PiSHsG9pnKM0ubw
Unqc4HYrjEiwJKAR2OBAylfH1ajf7wYGQbOiTQMeMyo2nQK8yQ==
```

```
bitcount:1024
fingerprint:
SHA256:D4F+T17R3fVunGz9A4GKGLWMQ0r4YRbzf5GfNwylneg
*****
dsa keys generated:Tue Feb 28 07:47:04 2017
```

```
ssh-dss AAAAB3NzaC1kc3MAAACBAJan5V/6YiKQZG2SCChmn9Mu5EbUQoTuCDyTCIYM35ofzh+dEALU
11XZrkG17V2Hfbgp57dcTyalgjeNOzWU32oOvbA8osJ3BWPiePkZv+/t0feOz4LUhBz85ccmQeLJQ86R
UeJ6pAFsq+yk4XB/15qMv9SN/QY0/95gCIDt8Uq7AAAAFQDZUMiLvTZwIwajLdu8OtLfBlvmuWAAAIAE
7rIwqUlrDTqmvzRdrmayYM2cGfwL4x+8gGpGe2kZoedFzv4vmmW2npD0E8qTWS4nD0k7cioTjdgLXQoZ
yaQIPiEtD+qS8NHuCrTrguVuDDCEOMTlhwNwL0iChm08YgJIR3ho+V/nm5ko4kp7jA5e0h/9P/Rr4hCO
aZBNxPcSewAAAIbhcNhaVDYvEri7JCH8DbiZr30z2P3PpIQ8YwPbcOE7CBXkp++HjMFUKd9HJlIwd4bA
81tTkTfSxkPBc9ocHOv1vusVufj423HFjcbIODixY76gJzqlt3aNs54MdfiYxyJLh6yp6LzZffDn4t2HF
x7tZSb4UJQKHdNR05d63Pybdbg==
```

```
bitcount:1024
fingerprint:
SHA256:kbHB73ZEhZaqJp/J68f1nfN9pJaQUkdHt0iKJc0c+Ao
```



Note SSH でスイッチにログインし、**aaa authentication login default none CLI** コマンドを発行した場合、ログインするために 1 つ以上のキーストロークを入力する必要があります。少なくとも 1 つのキーストロークを入力せずに **Enter** キーを押すと、ログインは拒否されます。

パスワードのないファイルコピーおよび SSH

セキュアシェル (SSH) 公開キー認証は、パスワードのないログインを行うために使用できません。SCP および SFTP は SSH をバックグラウンドで使用するため、これらのコピープロトコルを使用することにより、公開キー認証によるパスワードのないコピーが可能になります。この NX-OS バージョンは、SCP および SFTP クライアント機能だけをサポートしています。

SSH による認証に使用できる RSA および DSA ID を作成できます。この ID は、公開キーと秘密キーという 2 つの部分から構成されています。公開キーおよび秘密キーはスイッチによって生成されますが、外部で生成してスイッチにインポートすることもできます。インポートするためには、キーが OPENSSH 形式であることが必要です。

SSH サーバーをホストしているホストマシン上でキーを使用するには、そのマシンに公開キーファイルを送り、サーバーの SSH ディレクトリ (たとえば、\$HOME/.ssh) にあるファイル `authorized_keys` に内容を追加します。秘密キーをインポートおよびエクスポートする場合、キーは暗号化によって保護されます。同一のパスワードを入力するように求められます。パスワードを入力すると、秘密キーは暗号化によって保護されます。パスワードフィールドを空白のままにしておくと、キーは暗号化されません。

キーを別のスイッチにコピーする必要がある場合は、スイッチからホストマシンにキーをエクスポートし、そのマシンから他のスイッチに同じキーをインポートします。

- キー ファイルは、リブート後も維持されます。

キー ペアをインポートおよびエクスポートするために、次の CLI が提供されます。スイッチで SSH ユーザー キー ペアを生成する CLI コマンドは次のように定義されます。

Procedure

ステップ 1 switch# configure terminal

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# username admin keypair generate rsa

Example:

```
generating rsa key(1024 bits).....
generated rsa key
```

アカウント (admin) の公開および秘密 RSA キーを生成します。その後、指定されたユーザーのホームディレクトリにキー ファイルを保存します。そのサーバー キー ペアを上書きするには force オプションを使用します。

Note この例は RSA キーの場合です。DSA キーの場合、rsa を dsa に置き換えます。

ステップ 3 switch(config)# no username admin keypair generate rsa

(オプション) アカウント (admin) の公開および秘密 RSA キーを削除します。

ステップ 4 switch# show username admin keypair

Example:

```
*****
rsa Keys generated: Thu Jul 9 11:10:29 2009
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcvnrMbx2BmD
0P8boZElTfJFx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvq
srU9TByjYDPQkR/+Y6cKubyFWVxSBG/NHztQc3+QC1zdkIxGNJ
bEHyFoaajzNEO8LLOVFIMCZ2Td7gxUGRZc+fbqS33GZsCAX6v0=
bitcount:262144
fingerprint:
8d:44:ee:6c:ca:0b:44:95:36:d0:7d:f2:b5:78:74:7d
*****
could not retrieve dsa key information
*****
```

アカウント (admin) の公開キーを示します。

ステップ 5 switch(config)# username admin keypair export bootflash:key_rsa rsa

Example:

```
Enter Passphrase:
switch(config)# dir
 951 Jul 09 11:13:59 2009 key_rsa
 221 Jul 09 11:14:00 2009 key_rsa.pub
```

ユーザー (admin) のホームディレクトリからブートフラッシュメモリにキー ペアをエクスポートします。

キーペア（公開キーと秘密キー）が指定の場所にエクスポートされます。ユーザーは秘密キーを暗号化するパスフレーズを入力するように求められます。秘密キーは `uri` で指定したファイル名としてエクスポートされ、公開キーは「.pub」拡張子が後に付く同じファイル名でエクスポートされます。

ユーザーは任意のスイッチにこのキーペアをコピーして、さらに SCP サーバーのホームディレクトリに公開ファイルをコピーできるようになります。

ステップ 6 `switch(config)# username admin keypair import bootflash:key_rsa rsa`

Example:

```
Enter Passphrase:
switch(config)# show username admin keypair
*****
rsa Keys generated: Thu Jul 9 11:10:29 2009
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcvnrmBx2BmD
0P8boZE1TFJFx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvq
srU9TBypYDPQkR/+Y6cKubyFWVxSBG/NHztQc3+QC1zdkIxGNJ
bEHyFoajzNEO8LLOVFIMCZ2Td7gxUGRZc+fbqS33GZsCAX6v0=
bitcount:262144
fingerprint:
8d:44:ee:6c:ca:0b:44:95:36:d0:7d:f2:b5:78:74:7d
*****
could not retrieve dsa key information
*****
```

スイッチのホームディレクトリにキーペアをインポートします。

ここで示す `uri` は秘密キーの `uri` であり、公開キーは「.pub」拡張子が付いて同じ場所に存在する必要があります。ユーザーはパスフレーズの入力が求められ、キーの暗号化に使用されたのと同じパスフレーズを入力する必要があります。

サーバーにパスワードレスコピーをする必要があるスイッチに秘密キーがコピーされ、そのサーバーのホームディレクトリの `authorized_keys` ファイルにコピーされた公開キーがある場合、ユーザーはスイッチからサーバーへのパスワードレスファイルコピーおよび `ssh` を実行できます。

Note サーバーの `authorized_keys` ファイルに公開キーをコピーするのに、ユーザーは前述の `show` コマンドからキーをコピーすることもできます。

ステップ 7 `server# cat key_rsa.pub >> $HOME/.ssh/authorized_keys`

SCP サーバーの `authorized_keys` ファイルに `key_rsa.pub` に保存されている公開キーを追加します。標準 `ssh` と `scp` コマンドを使用して、スイッチからこのサーバーへのパスワードレス `ssh` および `scp` が有効になりました。

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 13: 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
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
SSH ログインの最大試行回数	3
SCP サーバ	ディセーブル
SFTP サーバ	ディセーブル



第 9 章

IPS セキュリティ構成の指定

この章では、Cisco MDS 9000 シリーズ スイッチの IP セキュリティ (IPsec) プロトコル サポートについて説明します。IP Security (IPSec) プロトコルは、加入ピア間にデータ機密保持、データの整合性、およびデータ認証を提供するオープン規格のフレームワークです。IPSec は、Internet Engineering Task Force (IETF) により開発されました。IPSec は、ホスト ペア間、セキュリティ ゲートウェイ ペア間、またはセキュリティ ゲートウェイ とホスト間の 1 つまたは複数のデータフローの保護など、IP レイヤにセキュリティ サービスを提供します。IPSec 実装全体は、RFC 2401 の最新バージョンに準じています。Cisco NX-OS の IPSec は、RFC 2402 ~ RFC 2410 を実装しています。



(注) IPSec という用語は、IPSec データ サービスのプロトコル全体および IKE セキュリティ プロトコルを示す場合や、データ サービスだけを指す場合に使用されることがあります。

この章は、次の項で構成されています。

- [IPsec についての情報, on page 214](#)
- [IKE の概要, on page 216](#)
- [IPSec の互換性, on page 216](#)
- [IPSec および IKE に関する用語, on page 217](#)
- [サポート対象の IPSec トランスフォームおよびアルゴリズム, on page 219](#)
- [サポート対象の IKE トランスフォームおよびアルゴリズム, on page 219](#)
- [IPSec デジタル証明書のサポート, on page 220](#)
- [IPsec および IKE の手動設定, on page 223](#)
- [オプションの IKE パラメータの設定, on page 229](#)
- [クリプト IPv4-ACL, on page 233](#)
- [IPsec のメンテナンス, on page 247](#)
- [グローバル ライフタイム値, on page 248](#)
- [IKE 設定の表示, on page 249](#)
- [IPsec 設定の表示, on page 250](#)
- [FCIP の設定例, on page 254](#)
- [iSCSI の設定例, on page 259](#)

- デフォルト設定, on page 260

IPsecについての情報

IPsec はインターネット キー交換 (IKE) プロトコルを使用して、プロトコルおよびアルゴリズムのネゴシエーションを処理し、IPsec で使用される暗号キーおよび認証キーを生成します。IKE は他のプロトコルとともに使用できますが、その初期実装時は IPsec プロトコルで使われます。IKE は、IPsec ピアを認証し、IPsec セキュリティ アソシエーションをネゴシエーションし、IPsec キーを確立します。IKE は RFC 2408、2409、2410、2412 を使用し、さらに draft-ietf-ipsec-ikev2-16.txt ドラフトを実装しています。

IPsec は、インターネットなどの保護されていないネットワークを使用して機密情報を送信する場合に、セキュリティを提供します。IPsec はネットワーク層で機能し、参加する IPsec デバイス (ピア) 間の IP パケットを保護し、認証します。



Note HP c-Class BladeSystem 対応 Cisco Fabric Switch および IBM BladeCenter 対応 Cisco Fabric Switch は、IPsec をサポートしていません。

IPsec は、インターネットなどの保護されていないネットワークを使用して機密情報を送信する場合に、セキュリティを提供します。IPsec はネットワーク層で機能し、参加する IPsec デバイス (ピア) 間の IP パケットを保護し、認証します。

IPsec は、次のネットワーク セキュリティ サービスを提供します。一般に、関与する 2 つの IPsec デバイス間でどのサービスが使用されるかは、ローカルセキュリティ ポリシーによって決まります。

- データ機密性：ネットワークにパケットを伝送する前に IPsec 送信側がパケットを暗号化できます。
- データ整合性：IPsec 受信者は、IPsec 送信者から送信されたパケットを認証し、伝送中にデータが変更されていないかを確認できます。
- データ送信元認証：IPsec 受信者は、送信された IPsec パケットの送信元を認証できます。このサービスは、データ整合性サービスに依存します。
- リプレイ防止：IPsec 受信側でリプレイ パケットを検出し、拒否できます。



Note [データ認証 (*data authentication*)] は、データ整合性およびデータ発信元認証を意味します。この章では、特に明記されていないかぎり、データ認証にはリプレイ防止サービスも含まれます。

IPsec を使用すれば、データを、観察、変更、またはスプーフィングされることを心配することなく、パブリック ネットワークを介して転送できます。これにより、インターネット、エク

ストラネット、リモートユーザーアクセス、バーチャルプライベートネットワーク (VPN) などのアプリケーションを含みます。

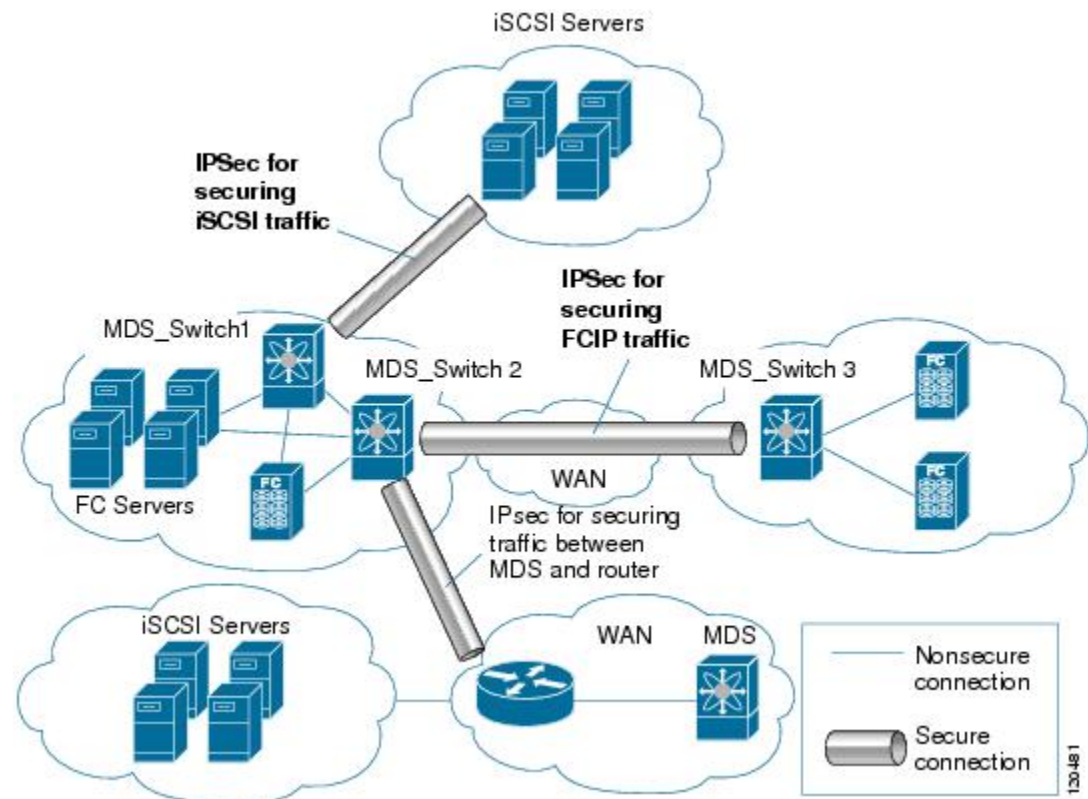
Cisco NX-OS ソフトウェアに実装された IPsec は、カプセル化セキュリティペイロード (ESP) プロトコルをサポートしています。このプロトコルはデータをカプセル化して保護し、データプライバシーサービス、オプションのデータ認証、およびオプションのリプレイ防止サービスを提供します。

**Note**

- カプセル化セキュリティペイロード (ESP) プロトコルは、既存の TCP/IP パケットに挿入されたヘッダーで、サイズは実際の暗号化およびネゴシエートされた認証アルゴリズムによって異なります。フラグメンテーションを防止するために、暗号化パケットは、インターフェイスの最大伝送単位 (MTU) と一致します。TCP のパス MTU の暗号化計算には、ESP ヘッダーの追加分、およびトンネルモードの外部 IP ヘッダーが考慮されます。MDS スイッチは、IPsec 暗号化によるパケット増加を 100 バイトまで許容します。
- IPsec 暗号化は、2500 を超える MTU を備えた FCIP トンネルではサポートされていません。FCIP と IPsec を一緒に使用する場合、2500 以下の MTU を設定することをお勧めします。
- IPsec および IKE を使用する場合、IPS モジュールの各 IPStorage ポートは、独自の IP サブネットで構成する必要があります。同じ IP サブネットの IP アドレスまたはネットワークマスクで複数の IPStorage インターフェイスが構成される場合、IKE パケットは正しい IPS ポートに送信されず、IPsec リンクは起動しません。

Figure 10: MPS-14/2 モジュールを使用する FCIP および iSCSI のシナリオ, on page 216 に、各種 IPsec のシナリオを示します。

Figure 10: MPS-14/2 モジュールを使用する FCIP および iSCSI のシナリオ



IKE の概要

IKE は、IPSec セキュリティ アソシエーション (SA) を自動的にネゴシエートし、IPSec 機能を使用してすべてのスイッチのキーを生成します。IKE の具体的な利点は次のとおりです。

- IPSec SA をリフレッシュできます。
- IPSec でアンチ リプレイ サービスが使用可能です。
- 管理可能でスケーラブルな IPSec 設定をサポートします。
- ピアのダイナミック認証が可能です。

IPSec の互換性

IPSec 機能は、次の Cisco MDS 9000 シリーズ ハードウェアと互換性があります。

- Cisco MDS 9220i ファブリック スイッチ
- Cisco MDS 9250i マルチサービス ファブリック スイッチ

- Cisco MDS 9700 シリーズ スイッチの Cisco MDS 24/10 ポート SAN 拡張モジュール。
- IPSec 機能は、管理インターフェイス上ではサポートされません。

IPSec 機能は、次のファブリック設定と互換性があります。

- Cisco MDS SAN-OS Release 2.0(1b) 以降または Cisco NX-OS 4.1(1) を実装している、2 台の接続された Cisco MDS 9200 スイッチまたは Cisco MDS 9500 ディレクタ。
- Cisco MDS SAN-OS Release 2.0(1b) 以降または Cisco NX-OS 4.1(1) を実装し、任意の IPSec 互換デバイスに接続された Cisco MDS 9200 スイッチまたは Cisco MDS 9500 ディレクタ。
- Cisco NX-OS 上に実装された IPSec 機能では、次の機能はサポートされません。
 - 認証ヘッダー (AH)
 - トランスポート モード
 - SA のバンドル
 - SA の手動設定
 - クリプト マップにおけるホスト単位の SA オプション
 - SA アイドル タイムアウト
 - ダイナミック クリプト マップ

**Note**

このマニュアルでは、クリプトマップという用語は、スタティッククリプトマップだけを意味します。

IPSec および IKE に関する用語

ここでは、この章で使用する用語について説明します。

- セキュリティ アソシエーション (SA) : IP パケットの暗号化および暗号解除に必要なエントリに関する、2つの参加ピア間の合意。ピア間に双方向通信を確立するには、ピアごとに各方向（着信および発信）に対応する2つのSAが必要です。双方向のSAレコードのセットは、SA データベース (SAD) に保管されます。IPSec は IKE を使用して SA をネゴシエートし、起動します。各 SA レコードには、次の情報が含まれます。
 - セキュリティパラメータインデックス (SPI) : 宛先IPアドレスおよびセキュリティプロトコルと組み合わせて、特定のSAを一意に識別する番号。IKEを使用してSAを確立する場合、各SAのSPIは疑似乱数によって生成された番号です。
 - ピア : IPSecに参加するスイッチなどのデバイス。IPSecをサポートするCisco MDS スイッチまたはその他のシスコ製ルータなどがあります。

- **トランスフォーム**：データ認証およびデータ機密保持を提供するために実行される処理のリスト。Hash Message Authentication Code (HMAC) -MD5 認証アルゴリズムを使用する ESP プロトコルなどがあります。
- **セッションキー**：セキュリティ サービスを提供するためにトランスフォームによって使用されるキー。
- **ライフタイム**：SA を作成した時点から、ライフタイム カウンタ（秒およびバイト単位）がカウントされます。制限時間が経過すると、SA は動作不能になり、必要に応じて、自動的に再ネゴシエート（キーが再設定）されます。
- **動作モード**：IPSec では通常、2 つの動作モード（トンネル モードおよびトランスペアレント モード）を使用できます。Cisco NX-OS に実装された IPSec は、トンネル モードだけをサポートします。IPSec トンネルモードは、ヘッダーを含めた IP パケットを暗号化して、認証します。ゲートウェイは、ホストおよびサブネットの代わりにトラフィックを暗号化します。Cisco NX-OS に実装された IPSec では、トランスペアレント モードはサポートされません。



Note トンネル モードという用語は、FCIP リンクで接続された 2 台のスイッチなど、2 つのピア間のセキュアな通信パスを示すためのトンネルとは異なります。

- **リプレイ防止**：受信側がリプレイ攻撃から自身を保護するために、古いパケットまたは重複パケットを拒否できるセキュリティ サービス。IPSec は、データ認証とシーケンス番号を組み合わせて使用することにより、このオプション サービスを提供します。
- **データ認証**：データ認証は整合性だけ、または整合性と認証の両方を意味することがあります（データ発信元認証はデータ整合性に依存します）。
 - **データ整合性**：データが変更されていないことを確認します。
 - **データ発信元認証**：要求を受けた送信側からデータが実際に送信されたことを確認します。
- **データ機密保護**：保護されたデータを傍受できないようにするセキュリティ サービス。
- **データ フロー**：送信元アドレス/マスクまたはプレフィックス、宛先アドレス/マスクまたはプレフィックス長、IP ネクスト プロトコル フィールド、および送信元/宛先ポートの組み合わせで識別されるトラフィック グループ（プロトコルおよびポート フィールドにいずれかの値を設定できます）。これらの値の特定の組み合わせと一致するトラフィックは、1 つのデータ フローに論理的にグループ化されます。データ フローは、2 台のホスト間の単一の TCP 接続、あるいは 2 つのサブネット間のトラフィックを示します。IPSec 保護はデータ フローに適用されます。
- **Perfect Forward Secrecy (PFS)**：取得された共有シークレット値に対応する暗号特性。PFS を使用すると、1 つのキーが損なわれても、これ以降のキーは前のキーの取得元から取得されないため、前および以降のキーには影響しません。
- **Security Policy Database (SPD)**：トラフィックに適用される順序付きポリシー リスト。ポリシーにより、パケットに IPSec 処理が必要かどうか、クリアテキストでの送信を許可するかどうか、または廃棄するかどうかを判別されます。
 - IPSec SPD は、クリプト マップのユーザー設定から取得されます。

- IKE SPD はユーザーが設定します。

サポート対象の IPSec トランスフォームおよびアルゴリズム

IPSec に実装されたコンポーネントテクノロジーには、次のトランスフォームが含まれます。

- **Advanced Encrypted Standard (AES)** : 暗号化アルゴリズム。AES は Cipher Block Chaining (CBC) またはカウンタモードを使用して、128 ビットまたは 256 ビットを実装します。
- **データ暗号規格 (DES)** : パケットデータを暗号化するために使用され、必須の 56 ビット DES-CBC を実装します。CBC には、暗号化を開始するための初期ベクトル (IV) が必要です。IV は IPSec パケットに明示的に指定されます。
- **Triple DES (3DES)** : 信頼できないネットワーク上で重要な情報を送信できるようにする、168 ビット暗号キーを使用した強力な DES 形式です。



Note

強力な暗号化を使用する Cisco NX-OS イメージは、米国政府の輸出規制の対象で、配信が制限されています。米国以外の国でインストールされるイメージには、輸出許可が必要です。米国政府の規制により、お客様の注文が拒否されたり、納入が遅れたりすることがあります。詳細については、営業担当者または販売業者、あるいは export@cisco.com までお問い合わせください。

- **Message Digest 5 (MD5)** : HMAC バリエーションを使用するハッシュアルゴリズム。HMAC はデータの認証に使用されるキー付きハッシュバリエーションです。
- **Secure Hash Algorithm (SHA-1、SHA-2)** はハッシュメッセージ認証コード (HMAC) バリエーションを使用するハッシュアルゴリズムです。Cisco MDS NX-OS リリース 7.3(0)D1(1) 以降の Cisco MDS 9250i マルチサービス ファブリック スイッチで、IPsec は SHA-2 をサポートします。
- **AES-XCBC-MAC** : AES アルゴリズムを使用する Message Authentication Code (MAC) 。

サポート対象の IKE トランスフォームおよびアルゴリズム

IKE に実装されたコンポーネントテクノロジーには、次のトランスフォームが含まれます。

- **Diffie-Hellman (DH)** : 保護されていない通信チャネルを介して 2 つのパーティが共有シークレットを確立できるようにする、公開キー暗号化プロトコル。Diffie-Hellman は、IKE 内でセッションキーを確立するために使用されます。グループ 1 (768 ビット)、グループ 2 (1024 ビット)、およびグループ 5 (1536 ビット) がサポートされます。

- **Advanced Encrypted Standard (AES)** : 暗号化アルゴリズム。AES は、CBC を使用する 128 ビット、またはカウンタ モードを実装します。
- **データ暗号規格 (DES)** : パケットデータを暗号化するために使用され、必須の 56 ビット DES-CBC を実装します。CBC には、暗号化を開始するための初期ベクトル (IV) が必要です。IV は IPSec パケットに明示的に指定されます。
- **Triple DES (3DES)** : 信頼できないネットワーク上で重要な情報を送信できるようにする、168 ビット暗号キーを使用した強力な DES 形式です。



Note 強力な暗号化を使用する Cisco NX-OS イメージは、米国政府の輸出規制の対象で、配信が制限されています。米国以外の国でインストールされるイメージには、輸出許可が必要です。米国政府の規制により、お客様の注文が拒否されたり、納入が遅れたりすることがあります。詳細については、営業担当者または販売業者、あるいは export@cisco.com までお問い合わせください。

- **Message Digest 5 (MD5)** : HMAC バリエーションを使用するハッシュ アルゴリズム。HMAC はデータの認証に使用されるキー付きハッシュ バリエーションです。
- **Secure Hash Algorithm (SHA-1、SHA-2)** はハッシュ メッセージ認証コード (HMAC) バリエーションを使用するハッシュ アルゴリズムです。IKEv2 は Cisco MDS NX-OS リリース 7.3(0)D1(1) 以降、Cisco MDS 9250i マルチサービス ファブリック スイッチで SHA-2 をサポートします。



Note IKEv1 は SHA-2 をサポートしません。

- **スイッチの認証アルゴリズム** : IP アドレスに基づく事前共有キーを使用します。

IPSec デジタル証明書のサポート

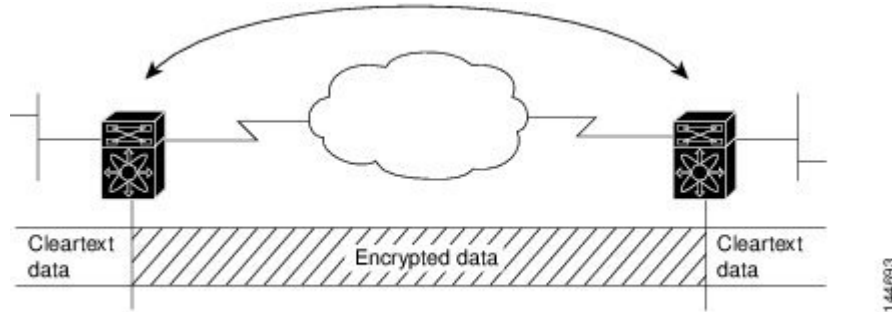
ここでは、認証局 (CA) およびデジタル証明書を使用した認証の利点について説明します。

CA およびデジタル証明書を使用しない IPSec の実装

CA およびデジタル証明書を使用しない場合、2 台の Cisco MDS スイッチ間で IPSec サービス (暗号化など) をイネーブルにするには、各スイッチに他方のスイッチのキー (RSA 公開キーまたは共有キーなど) が必要になります。IPSec サービスを使用するファブリック内の各スイッチに、RSA 公開キーまたは事前共有キーのどちらかを手動で指定する必要があります。また、ファブリックに新しいデバイスを追加する場合、安全な通信をサポートするには、ファブリック内の他方のスイッチを手動で設定する必要があります。各 (Figure 11: CA およびデジタル証明書を使用しない 2 台の IPSec スイッチ, on page 221 を参照) スイッチは他方のスイッチのキーを使用して、他方のスイッチのアイデンティティを認証します。この認証は、2 台のスイッチ間で IPSec トラフィックが交換される場合に、必ず実行されます。

複数の Cisco MDS スイッチをメッシュ トポロジで配置し、すべてのスイッチ間で IPSec トラフィックを交換させる場合には、最初に、すべてのスイッチ間に共有キーまたは RSA 公開キーを設定する必要があります。

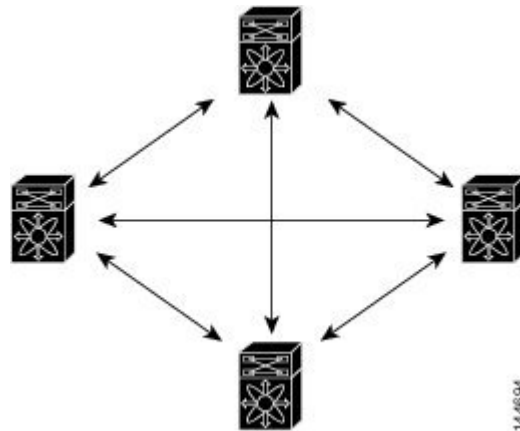
Figure 11: CA およびデジタル証明書を使用しない 2 台の IPSec スイッチ



IPSec ネットワークに新しいスイッチを追加するごとに、新しいスイッチと既存の各スイッチ間にキーを設定する必要があります (Figure 12: CA およびデジタル証明書を使用しない 4 台の IPSec スイッチ, on page 221 の場合、このネットワークに 1 台の暗号化スイッチを追加するには、新たに 4 つのスイッチ間キーの設定が必要になります)。

したがって、IPSec サービスを必要とするデバイスが増えるほど、キー管理は複雑になります。このアプローチでは、より大型で複雑な暗号化ネットワークには拡張できません。

Figure 12: CA およびデジタル証明書を使用しない 4 台の IPSec スイッチ



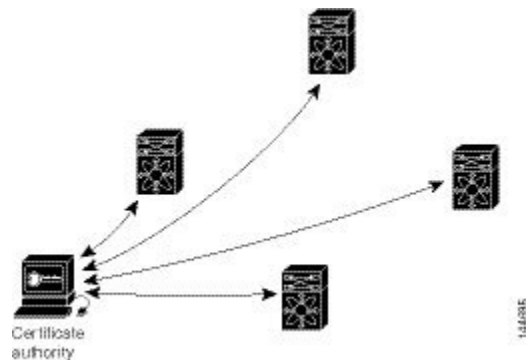
CA およびデジタル証明書を使用した IPSec の実装

CA およびデジタル証明書を使用する場合には、すべての暗号化スイッチ間にキーを設定する必要はありません。代わりに、加入させる各スイッチを CA に個別に登録し、各スイッチの証明書を要求します。この設定が完了していれば、各加入スイッチは、他のすべての加入スイッチを動的に認証できます。2 台のデバイスが通信する場合、証明書を交換し、データをデジタル署名して、お互いを認証します。ネットワークに新しいデバイスを追加する場合には、そのデバイスを CA に登録するだけでよく、他のデバイスの設定を変更する必要はありません。

せん。新しいデバイスが IPSec 接続を試みると、証明書が自動的に交換され、そのデバイスが認証されます。

Figure 13: CA によるデバイスのダイナミックな認証, on page 222 に、デバイスをダイナミックに認証するプロセスを示します。

Figure 13: CA によるデバイスのダイナミックな認証



ネットワークに新しい IPSec スイッチを追加する場合、新しいスイッチが CA に証明書を要求するように設定するだけでよく、既存の他のすべての IPSec スイッチとの間に複数のキー設定を行う必要はありません。

IPSec デバイスによる CA 証明書の使用方法

2 台の IPSec スイッチが IPSec で保護されたトラフィックを交換するには、最初に相互に認証しあう必要があります。認証されていない場合、IPSec 保護が適用されません。この認証を行うには、IKE を使用します。

IKE では、2 つの方法を使用してスイッチを認証できます。CA を使用しない場合には事前共有キーを使用し、CA を使用する場合には RSA キー ペアを使用します。どちらの方法も、2 台のスイッチ間にキーが事前設定されている必要があります。

CA を使用しない場合、スイッチは RSA 暗号化事前共有キーを使用して、リモートスイッチに対して自身を認証します。

CA を使用する場合、スイッチはリモートスイッチに証明書を送信し、何らかの公開キー暗号法を実行することによって、リモートスイッチに対して自身を認証します。各スイッチは、CA により発行されて検証された、スイッチ固有の証明書を送信する必要があります。このプロセスが有効なのは、各スイッチの証明書にスイッチの公開キーがカプセル化され、各証明書が CA によって認証されることにより、すべての加入スイッチが CA を認証局として認識するからです。この機構は、RSA シグニチャを使用する IKE と呼ばれます。

スイッチは、証明書が期限切れになるまで、複数の IPSec ピアに対して、複数の IPSec セッション用に自身の証明書を継続的に送信できます。証明書が期限切れになった場合、スイッチ管理者は CA から新しい証明書を取得する必要があります。

また、CA は、IPSec に参加しなくなったデバイスの証明書を失効できます。失効された証明書は、他の IPSec デバイスから有効とは見なされません。失効された証明書は、証明書失効リス

ト (CRL) にリストされ、各ピアは相手側ピアの証明書を受け入れる前に、このリストを確認できます。

IKE の証明書サポートでは、次の考慮事項に留意してください。

- IKE 用の証明書をインストールする前に、スイッチの FQDN (ホスト名およびドメイン名) が設定されている必要があります。
- IKE が使用するののは、IKE 用または汎用として設定された証明書だけです。
- スイッチに設定された最初の IKE 用または汎用証明書が、IKE のデフォルトの証明書として使用されます。
- ピアが別の証明書を指定しないかぎり、すべての IKE ピアに対してデフォルトの証明書が使用されます。
- ピアが、そのピアが信頼する CA によって署名された証明書を要求した場合、IKE は、要求された証明書がスイッチに存在すれば、デフォルトの証明書でなくても、その証明書を使用します。
- デフォルトの証明書が削除された場合、次の IKE 用または汎用証明書が存在すれば、IKE はそれをデフォルトの証明書として使用します。
- IKE では、証明書チェーンはサポートされません。
- IKE は、CA チェーン全体ではなく、アイデンティティ証明書だけを送信します。ピア上で証明書が確認されるには、ピア上に同じ CA チェーンが存在する必要があります。

IPsec および IKE の手動設定

ここでは、IPSec および IKE を手動で設定する方法について説明します。

IPSec は、加入ピア間に安全なデータフローを提供します。2つのピア間では、異なる SA セットを使用する各トンネルで異なるデータフローを保護することにより、複数の IPSec データフローをサポートできます。

IKE 設定の完了後、IPSec を設定します。

各加入 IPSec ピアに IPSec を設定する手順は、次のとおりです。

Procedure

-
- ステップ 1** トラフィック用の安全なトンネルを確立する必要があるピアを識別します。
 - ステップ 2** 必要なプロトコルとアルゴリズムにより、トランスフォーム セットを設定します。
 - ステップ 3** クリプトマップを作成し、適切なアクセスコントロールリスト (IPv4-ACL)、トランスフォーム セット、ピア、およびライフタイム値を適用します。
 - ステップ 4** クリプトマップを、必要なインターフェイスに適用します。
-

IKE Prerequisites

Before using IPsec and IKE on IPStorage or Gigabit Ethernet interfaces, ensure these local interfaces are configured in separate IP subnets. If not, IKE packets may not be sent to the right peer and thus the IPsec tunnel will not come up.

You cannot disable IKE if IPsec is enabled. If you disable the IKE feature, the IKE configuration is cleared from the running configuration.

For more information, see the [Interface Subnet Requirements](#) section in the *Cisco MDS 9000 Series IP Services Configuration Guide, Release 8.x*.

IPsec Prerequisites

To use the IPsec feature, you need to perform the following tasks:

- Obtain the ENTERPRISE_PKG license (see the [Cisco MDS 9000 Series NX-OS Licensing Guide](#)).
From Cisco MDS NX-OS Release 9.2(2), the IPsec feature is included in the default feature set and does not require an ENTERPRISE_PKG license on the Cisco MDS 9220i Fabric Switch.
- Configure IKE as described in the [IKE のイネーブル化](#), on page 224 section.

IKE のイネーブル化

IKE をイネーブルにするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **feature crypto ike**

IKE 機能をイネーブルにします。

ステップ 3 switch(config)# **no feature crypto ike**

(オプション) IKE 機能をディセーブル (デフォルト) にします。

Note IKE 機能をディセーブルにする前に、IPsec をディセーブルにする必要があります。

IKE ドメインの設定

ローカルスイッチのスーパーバイザモジュールにトラフィックを到達させるには、IPSec ドメインに IKE 設定を適用する必要があります。Fabric Manager では、IKE の設定時に IPSec ドメインが自動的に設定されます。

IPsec ドメインを設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **crypto ike domain ipsec**

```
switch(config-ike-ipsec)#
```

IPsec ドメインに対する IKE の設定を許可します。

IKE トンネルの概要

IKE トンネルは、2つのエンドポイント間の安全な IKE セッションです。IKE は、IPSec SA ネゴシエーションで使用される IKE メッセージを保護するために、このトンネルを作成します。

Cisco NX-OS の実装では、2つのバージョンの IKE が使用されています。

- IKE バージョン 1 (IKEv1) は、RFC 2407、2408、2409、および 2412 を使用して実装されます。
- IKE バージョン 2 (IKEv2) は、より効率的な簡易バージョンで、IKEv1 とは相互運用できません。IKEv2 は、draft-ietf-ipsec-ikev2-16.txt ドラフトを使用して実装されます。

IKE ポリシー ネゴシエーションの概要

IKE ネゴシエーションを保護するには、各 IKE ネゴシエーションを共通（共有）IKE ポリシーで開始します。IKE ポリシーを使い、IKE ネゴシエーション中に使用するセキュリティパラメータの組み合わせを定義します。デフォルトでは、IKE ポリシーは設定されません。各ピアに IKE ポリシーを作成する必要があります。このポリシーにより、以降の IKE ネゴシエーションを保護するために使用するセキュリティパラメータを指定し、ピアの認証方法を指示します。最低1つのポリシーがリモートピアのポリシーと一致するように、各ピアに優先順位を付けた複数のポリシーを設定できます。

ポリシーは、暗号化アルゴリズム（DES、3DES、AES）、ハッシュアルゴリズム（SHA、MD5）、および DH グループ（1、2、5）に基づいて設定できます。各ポリシーに、パラメータ値の異なる組み合わせを設定できます。設定したポリシーには、固有のプライオリティ番号

を指定します。この番号の範囲は、1（最上位のプライオリティ）～255（最下位のプライオリティ）です。スイッチに、複数のポリシーを設定できます。リモートピアに接続する必要がある場合、ローカルスイッチの少なくとも1つのポリシーが、リモートピアに設定されているパラメータ値と一致する必要があります。同じパラメータ設定のポリシーが複数ある場合には、最も小さい番号のポリシーが選択されます。

次の表に、許可されるトランスフォームの組み合わせのリストを示します。

Table 14: IKE トランスフォーム設定パラメータ

パラメータ	許容値	キーワード	デフォルト値
暗号化アルゴリズム	56 ビット DES-CBC 168 ビット DES 128 ビット AES	des 3des aes	3des
ハッシュアルゴリズム	SHA-1 (HMAC バリエント) 、SHA-2 (HMAC バリエント) MD5 (HMAC バリエント)	sha sha256 sha512 md5	sha
認証方式	事前共有キー	設定なし	事前共有キー
DH グループ識別名	768 ビット DH 1024 ビット DH 1536 ビット DH	1 2 5	1

次の表に、Microsoft Windows および Linux プラットフォームでサポートおよび検証されている、IPSec および IKE 暗号化認証アルゴリズムの設定を示します。

プラットフォーム	IKE	IPSec
Microsoft iSCSI 発信側 (Microsoft Windows 2000 プラットフォームの Microsoft IPSec 実装)	3DES、SHA-1、SHA-2 または MD5、DH グループ 2	3DES、SHA-1、SHA-2
Cisco iSCSI 発信側 (Linux プラットフォームの Free Swan IPSec 実装)	3DES、MD5、DH グループ 1	3DES、MD5



Note ハッシュアルゴリズムを設定すると、対応する HMAC バージョンが認証アルゴリズムとして使用されます。

IKE ネゴシエーションが開始されると、IKE は、両ピア上で同一の IKE ポリシーを検索します。ネゴシエーションを開始したピアがすべてのポリシーをリモートピアに送信し、リモート

ピアの方では一致するポリシーを探そうとします。リモートピアは、相手側ピアから受信したすべてのポリシーと自身の最優先ポリシーを比較することにより、一致しているポリシーを検索します。一致するポリシーが見つかるまで、リモートピアは優先順位が高い順に各ポリシーをチェックします。

2つのピアの暗号化、ハッシュアルゴリズム、認証アルゴリズム、およびDHグループ値が同じであれば、一致していると判断されます。一致しているポリシーが見つかったら、IKE はセキュリティ ネゴシエーションを完了し、IPSec SA が作成されます。

一致しているポリシーが見つからない場合、IKE はネゴシエーションを拒否し、IPSec データフローは確立されません。

IKE ポリシーの設定

IKE ポリシー ネゴシエーション パラメータを設定するには、次の手順を実行します。

Procedure

-
- ステップ 1** `switch# configure terminal`
`switch(config)#`
コンフィギュレーション モードに入ります。
- ステップ 2** `switch(config)# crypto ike domain ipsec`
`switch(config-ike-ipsec)#`
IPsec ドメインをこのスイッチで設定できます。
- ステップ 3** `switch(config-ike-ipsec)# identity address`
IKE プロトコルが IP アドレスを使用するようにアイデンティティ モードを設定します (デフォルト)。
- ステップ 4** `switch(config-ike-ipsec)# identity hostname`
IKE プロトコルが完全修飾ドメイン名 (FQDN) を使用するようにアイデンティティ モードを設定します。
- Note** FQDN は認証に RSA シグニチャを使用する必要があります。
- ステップ 5** `switch(config-ike-ipsec)# no identity`
(オプション) デフォルトのアイデンティティ モード (**address**) に戻ります。
- ステップ 6** `switch(config-ike-ipsec)# key switch1 address 10.10.1.1`
ピアの IP アドレスに事前共有キーを関連付けます。
- ステップ 7** `switch(config-ike-ipsec)# no key switch1 address 10.10.1.1`
(オプション) 事前共有キーとピアの IP アドレスの関連付けを削除します。

- ステップ 8** `switch(config-ike-ipsec)# key switch1 hostname switch1.cisco.com`
ピアの FQDN と事前共有キーを関連付けます。
Note FQDNを使用するには、ピアのスイッチ名とドメイン名を設定する必要があります。
- ステップ 9** `switch(config-ike-ipsec)# no key switch1 hostname switch1.cisco.com`
(オプション) 事前共有キーとピアの IP アドレスの関連付けを削除します。
- ステップ 10** `switch(config-ike-ipsec)# policy 1`
`switch(config-ike-ipsec-policy)#`
設定するポリシーを指定します。
- ステップ 11** `switch(config-ike-ipsec)# no policy 1`
(オプション) 指定されたポリシーを削除します。
- ステップ 12** `switch(config-ike-ipsec-policy)# encryption des`
暗号化ポリシーを設定します。
- ステップ 13** `switch(config-ike-ipsec-policy)# no encryption des`
(オプション) デフォルトは 3DES 暗号化です。
- ステップ 14** `switch(config-ike-ipsec-policy)# group 5`
DH グループを設定します。
- ステップ 15** `switch(config-ike-ipsec-policy)# no group 5`
(オプション) デフォルトは DH グループ 1 です。
- ステップ 16** `switch(config-ike-ipsec-policy)# hash md5`
ハッシュ アルゴリズムを設定します。
- ステップ 17** `switch(config-ike-ipsec-policy)# no hash md5`
(オプション) デフォルトは SHA です。
- ステップ 18** `switch(config-ike-ipsec-policy)# authentication pre-share`
認証方式を事前共有キーを使用するように設定します (デフォルト)。
- ステップ 19** `switch(config-ike-ipsec-policy)# authentication rsa-sig`
認証方式を RSA シグニチャを使用するように設定します。
Note 認証のために RSA シグニチャを使用するには、FQDN を使用してアイデンティティ認証モードを設定する必要があります (手順 3 を参照)。
- ステップ 20** `switch(config-ike-ipsec-policy)# no authentication`

デフォルト値 (**pre-share**) に戻します。

Example



Note

- IKE 証明書は FQDN タイプのサブジェクト名を使用するので、認証方式が `rsa-sig` の場合には、IKE 用のアイデンティティ ホスト名が設定されていることを確認してください。
- Cisco MDS NX-OS リリース 5.2(x) にダウングレードする前に、事前共有キーを解除します。ダウングレードを完了したら、`key key-name hostname host` または `key key-name address ip-address` コマンドを使用して、事前共有キーを再設定します。

オプションの IKE パラメータの設定

IKE 機能には、オプションで次のパラメータを設定できます。

- 各ポリシーのライフタイム アソシエーション：ライフタイムの範囲は 600 ~ 86,400 秒です。デフォルトは、86,400 秒 (1 日) です。各ポリシーのライフタイム アソシエーションは、IKE ポリシーの設定時に設定します。IKE ポリシーの設定, on page 227 を参照してください。
- 各ピアのキープアライブ タイム (IKEv2 を使用する場合)：キープアライブの範囲は 120 ~ 86,400 秒です。デフォルトは、3,600 秒 (1 時間) です。
- 各ピアの発信側バージョン：IKEv1 または IKEv2 (デフォルト)。発信側バージョンの選択は、リモート デバイスがネゴシエーションを開始する場合、相互運用性に影響しません。このオプションは、ピア デバイスが IKEv1 をサポートしていて、指定したデバイスを IKE の発信側として動作させる場合に設定します。FCIP トンネルの発信側バージョンを設定する場合には、次の事項に注意してください。
 - FCIP トンネルの両側のスイッチが MDS SAN-OS Release 3.0(1) 以降または Cisco NX-OS 4.1(1) を実行している場合、IKEv1 だけを使用するには、FCIP トンネルの両側に発信側バージョン IKEv1 を設定する必要があります。FCIP トンネルの一方の側が IKEv1 を使用し、他方の側が IKEv2 を使用している場合には、FCIP トンネルは IKEv2 を使用します。
 - FCIP トンネルの片側のスイッチが MDS SAN-OS Release 3.0(1) 以降または Cisco NX-OS 4.1(1b) を実行し、FCIP トンネルの他方の側のスイッチが MDS SAN-OS Release 2.x を実行している場合、どちらか (または両方) の側に IKEv1 を設定すると、FCIP トンネルは IKEv1 を使用します。



Note 2.x MDS スイッチと 3.x MDS スイッチ間の IPsec 構築では、IKEv1 だけがサポートされません。



Caution 通常的环境ではスイッチが IKE 発信側として動作しない場合でも、発信側バージョンの設定が必要になることがあります。このオプションを常に使用することにより、障害時にトラフィック フローをより速く回復できます。



Tip キープアライブ タイムが適用されるのは、IKEv2 ピアだけで、すべてのピアではありません。



Note ホストの IPsec 実装により IPsec キー再設定を開始する場合には、Cisco MDS スイッチの IPsec のライフタイム値を、必ず、ホストのライフタイム値よりも大きい値に設定してください。

このセクションは、次のトピックで構成されています。

ポリシーのライフタイム アソシエーションの設定

各ポリシーのライフタイム アソシエーションを設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

switch(config)#

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **crypto ike domain ipsec**

switch(config-ike-ipsec)#

IPsec ドメインをこのスイッチで設定できます。

ステップ 3 switch(config-ike-ipsec)# **policy 1**

switch(config-ike-ipsec-policy)#

設定するポリシーを指定します。

ステップ 4 switch(config-ike-ipsec-policy) **lifetime seconds 6000**

6,000 秒のライフタイムを設定します。

ステップ 5 switch(config-ike-ipsec-policy)# **no lifetime seconds 6000**

(オプション) 設定したライフタイム値を削除し、デフォルトの 86,400 秒に設定します。

ピアのキープアライブタイムの設定

各ピアのキープアライブタイムを設定する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **crypto ike domain ipsec**

```
switch(config-ike-ipsec)#
```

IPsec ドメインをこのスイッチで設定できます。

ステップ 3 switch(config-ike-ipsec)# **keepalive 60000**

すべてのピアのキープアライブタイムを 60,000 秒に設定します。

ステップ 4 switch(config-ike-ipsec)# **no keepalive 60000**

(オプション) 設定したキープアライブタイムを削除し、デフォルトの 3,600 秒に設定します。

発信側バージョンの設定

IPv4 を使用して発信側バージョンを設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **crypto ike domain ipsec**

```
switch(config-ike-ipsec)#
```

IPsec ドメインをこのスイッチで設定できます。

ステップ 3 switch(config-ike-ipsec)# **initiator version 1 address 10.10.10.1**

デバイス 10.10.10.0 で IKE を開始するときに、IKEv1 を使用するようにスイッチを設定します

Note IKE は、IPv4 アドレスをサポートし、IPv6 アドレスはサポートしません。

ステップ 4 switch(config-ike-ipsec)# **no initiator version 1 address 10.10.10.1**

(オプション) 指定したデバイスのデフォルトは IKEv2 です。

ステップ 5 switch(config-ike-ipsec)# **no initiator version 1**

すべてのデバイスについてデフォルトの IKEv2 に設定します。

IKE トンネルまたはドメインのクリア

IKE 設定に IKE トンネル ID を指定していない場合は、EXEC モードで **clear crypto ike domain ipsec sa** コマンドを発行することにより、既存のすべての IKE ドメイン接続をクリアできます。

```
switch# clear crypto ike domain ipsec sa
```



Caution IKEv2 トンネル内のすべての SA を削除すると、その IKE トンネルは自動的に削除されません。

IKE 設定に SA を指定している場合、EXEC モードで **clear crypto ike domain ipsec sa IKE_tunnel-ID** コマンドを発行して、指定した IKE トンネル ID 接続をクリアできます。

```
switch# clear crypto ike domain ipsec sa 51
```



Caution IKEv2 トンネルを削除すると、その IKE トンネルの下の関連付けられた IPsec トンネルが自動的に削除されます。

SA のリフレッシュ

IKEv2 設定変更が行われた後に SA をリフレッシュするには、**crypto ike domain ipsec rekey IPv4-ACL-index** コマンドを使用します。

クリプト IPv4-ACL

IP アクセス コントロール リスト (IPv4-ACL) は、すべての Cisco MDS 9000 ファミリ スイッチに基本的なネットワークセキュリティを提供します。IPv4 IP-ACL は、設定された IP フィルタに基づいて IP 関連トラフィックを制限します。IPv4-ACL の作成と定義の詳細については、「[IPv4 および IPv6 のアクセス コントロール リストの概要](#)」を参照してください。

クリプト マップのコンテキストでは、IPv4-ACL は標準の IPv4-ACL と異なります。標準の IPv4-ACL は、インターフェイス上で転送またはブロックするトラフィックを判別します。たとえば、IPv4-ACL を作成して、サブネット A とサブネット Y 間のすべての IP トラフィックを保護したり、ホスト A とホスト B 間の Telnet トラフィックを保護できます。

ここでは、次の内容について説明します。

クリプト IPv4-ACL の概要

クリプト IPv4-ACL は、暗号による保護が必要な IP トラフィックと、必要ではないトラフィックとを定義するために使用します。

IPSec のクリプト マップ エントリに関連付けるクリプト IPv4-ACL には、4 つの主要な機能があります。

- IPSec で保護する発信トラフィックを選択する (permit に一致したものが保護の対象)。
- IPSec SA のネゴシエーションの開始時に、新しい SA で保護するデータ フロー (1 つの permit エントリで指定) を示す。
- 着信トラフィックを処理して、IPSec で保護すべきであったトラフィックをフィルタリングして廃棄する。
- IPSec ピアからの IKE ネゴシエーションの処理時に、要求されたデータ フローのために、IPSec SA の要求を受け入れるかどうかを判別する。

**Tip**

一部のトラフィックに1つのタイプのIPSec保護（暗号化だけ、など）を適用し、他のトラフィックに異なるタイプのIPSec保護（認証と暗号化の両方など）を適用する場合には、2つのIPv4-ACLを作成してください。異なるIPSecポリシーを指定するには、異なるクリプトマップで両方のIPv4-ACLを使用します。

**Note**

IPSec は、IPv6-ACL をサポートしていません。

クリプト IPv4-ACL の注意事項

IPSec 機能に関する IPv4-ACL を設定する場合には、次の注意事項に従ってください。

- Cisco NX-OS ソフトウェアで使用できるのは、名前ベースの IPv4-ACL だけです。

- IPv4-ACL をクリプト マップに適用するときは、次のオプションを適用します。
 - 許可 (permit) : トラフィックに IPSec 機能を適用します。
 - 拒否 (deny) : クリア テキストを許可します (デフォルト)。



Note IKE トラフィック (UDP ポート 500) は、必ずクリア テキストで送信されます。

- IPSec 機能が考慮するのは、送信元/宛先 IPv4 アドレスとサブネットマスク、プロトコル、および 1 つのポート番号だけです。IPSec では、IPv6 はサポートされません。



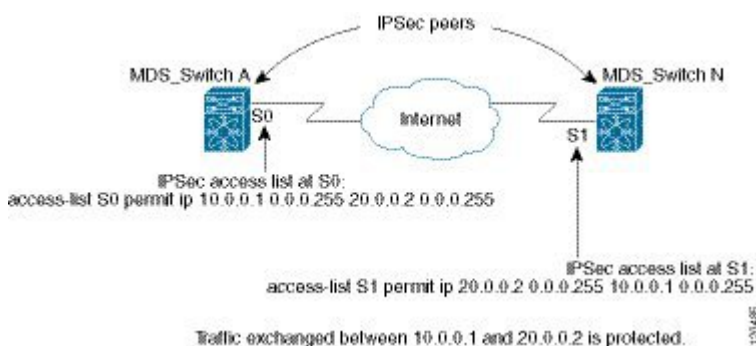
Note IPSec 機能はポート番号範囲をサポートしていないので、指定されている場合には上位ポート番号フィールドは無視されます。

- permit オプションを指定すると、対応するクリプトマップエントリで指定されたポリシーを使用して、指定条件に一致するすべての IP トラフィックが暗号によって保護されます。
- deny オプションを指定すると、トラフィックは暗号によって保護されません。最初の deny ステートメントにより、トラフィックはクリア テキストで送信されます。
- 定義するクリプト IPv4-ACL がインターフェイスに適用されるのは、対応するクリプトマップエントリを定義して、インターフェイスにクリプトマップセットを適用したあとです。
- 同じクリプトマップセットのエントリごとに、異なる IPv4-ACL を使用する必要があります。
- インバウンドおよびアウトバウンドトラフィックは、同じアウトバウンド IPv4-ACL に対して評価されます。したがって、IPv4-ACL の条件は、スイッチからの発信トラフィックに対して順方向に、スイッチへの着信トラフィックに対して逆方向に適用されます。
- クリプトマップエントリに割り当てられた各 IPv4-ACL フィルタは、1 つのセキュリティポリシー エントリと同等です。IPSec 機能は、各 MPS-14/2 モジュールおよび Cisco MDS 9216i スイッチに対して、最大 120 のセキュリティポリシー エントリをサポートします。
- スイッチ A の S0 インターフェイスから発信されたデータがスイッチ インターフェイス S1 にルーティングされるときに、スイッチ インターフェイス S0 (IPv4 アドレス 10.0.0.1) とスイッチ インターフェイス S1 (IPv4 アドレス 20.0.0.2) 間のトラフィックに IPSec 保護 (Figure 14: クリプト IPv4-ACL の IPSec 処理, on page 235 を参照) が適用されます。10.0.0.1 から 20.0.0.2 へのトラフィックの場合、スイッチ A の IPv4-ACL エントリは次のように評価されます。
 - 送信元 = IPv4 アドレス 10.0.0.1
 - 宛先 = IPv4 アドレス 20.0.0.2

20.0.0.2 から 10.0.0.1 へのトラフィックの場合、スイッチ A の IPv4-ACL エントリは次のように評価されます。

- 送信元 = IPv4 アドレス 20.0.0.2
- 宛先 = IPv4 アドレス 10.0.0.1

Figure 14: クリプト IPv4-ACL の IPsec 処理



- IPsec に使用する指定のクリプト IPv4-ACL に複数のステートメントを設定した場合には、一致した最初の permit ステートメントにより、IPsec SA の有効範囲が判別されます。その後、トラフィックがクリプト IPv4-ACL の別の permit ステートメントと一致した場合には、新しい、別の IPsec SA がネゴシエートされ、新たに一致した IPv4-ACL ステートメントと一致するトラフィックが保護されます。
- クリプトマップエントリに IPsec がフラグ設定されている場合、クリプト IPv4-ACL 内の permit エントリと一致する保護されていないインバウンドトラフィックは、IPsec によって保護されていると見なされ、廃棄されます。
- すべての IP-ACL を表示するには、**show ip access-lists** コマンドを使用できます。トラフィックをフィルタリングするために使用される IP-ACL は、暗号化にも使用されます。
- IPsec を Microsoft iSCSI 発信側と効率的に相互運用するには、IPv4-ACL に TCP プロトコルとローカル iSCSI TCP ポート番号（デフォルトは 3260）を指定します。この設定により、ギガビットイーサネットインターフェイスのシャットダウン、VRRP スイッチオーバー、ポート障害などにより処理が中断されても、暗号化 iSCSI セッションを迅速に回復できます。
- IPv4-ACL エントリの次の例では、MDS スイッチの IPv4 アドレスが 10.10.10.50 で、暗号化 iSCSI セッションが実行中のリモート Microsoft ホストが 10.10.10.16 であることを示しています。

```
switch(config)# ip access-list aclmsiscsi2 permit tcp 10.10.10.50 0.0.0.0 range port
3260 3260 10.10.10.16 0.0.0.0
```

ミラーイメージクリプト IPv4-ACL

ローカルピアで定義されたクリプトマップエントリがある場合は、このエントリで指定されたすべてのクリプト IPv4-ACL に対して、リモートピアでミラーイメージクリプト IPv4-ACL を定義します。この設定により、ローカルで適用された IPSec トラフィックをリモートピアで正しく処理できるようになります。



Tip また、クリプトマップエントリ自体が共通のトランスフォームをサポートし、ピアとして他のシステムを参照する必要があります。

Figure 15: ミラーイメージ設定の IPSec 処理, on page 236 に、ミラーイメージ IPv4-ACL を使用した場合と、使用しない場合のサンプルシナリオを示します。

Figure 15: ミラーイメージ設定の IPSec 処理

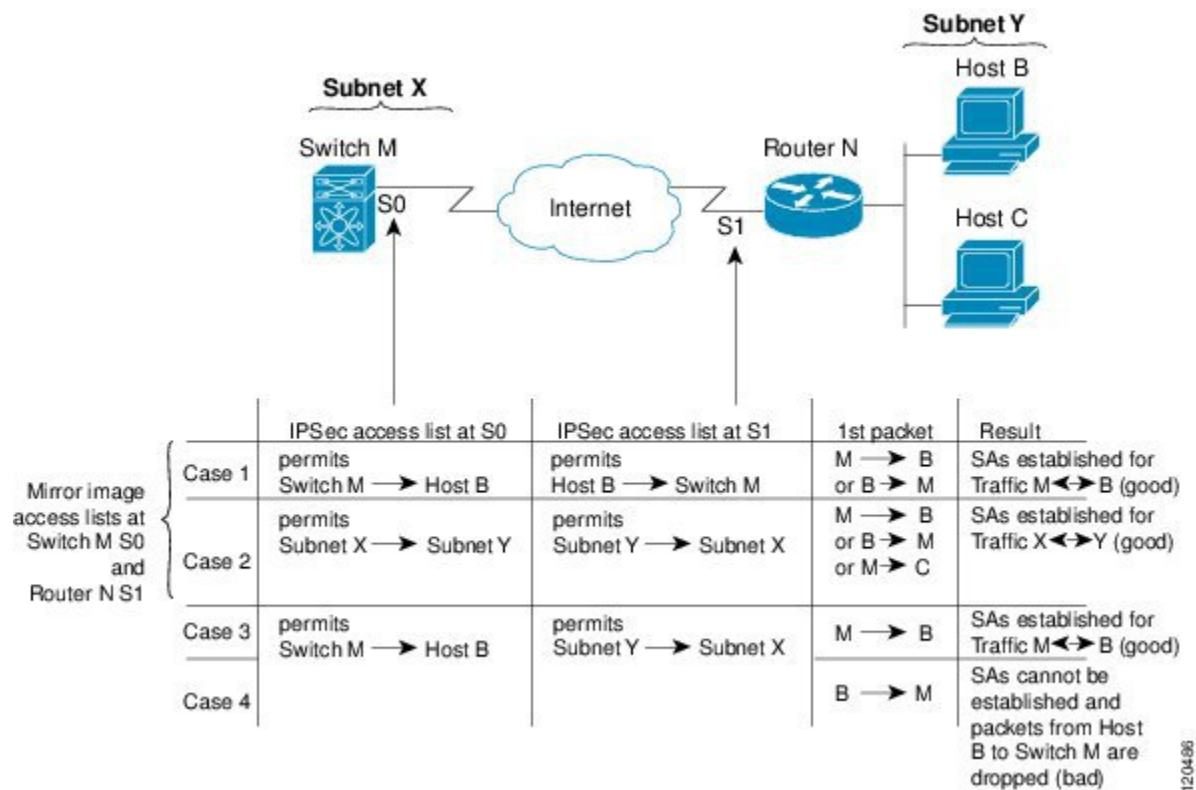


Figure 15: ミラーイメージ設定の IPSec 処理, on page 236 に示すように、2つのピアのクリプト IPv4-ACL が相互のミラーイメージである場合、想定どおりに IPSec SA を確立できます。ただし、IPv4-ACL が相互のミラーイメージでない場合にも、IPSec SA を確立できることがあります。たとえば、Figure 15: ミラーイメージ設定の IPSec 処理, on page 236 のケース 3 および 4 のように、一方のピアの IPv4-ACL エントリが他方のピアの IPv4-ACL エントリのサブセットになっている場合です。IPSec SA の確立は、IPSec にとって非常に重要です。SA が存在しないと IPSec は機能せず、クリプト IPv4-ACL の条件と一致するパケットは、IPSec セキュリティで保護されて転送される代わりに、すべて廃棄されます。

ケース 4 では、SA を確立できません。開始元パケットが終了すると、クリプト IPv4-ACL に従って必ず SA が要求されるためです。ケース 4 では、ルータ N はサブネット X とサブネット Y 間のすべてのトラフィックを保護するように要求します。ただし、このトラフィックはスイッチ M のクリプト IPv4-ACL で許可される特定のフローのスーパーセットであるため、要求は許可されません。スイッチ M の要求はルータ N のクリプト IPv4-ACL で許可される特定のフローのサブセットであるため、ケース 3 は機能します。

ピア IPSec デバイスにクリプト IPv4-ACL をミラー イメージとして設定しないと、設定が複雑化するので、ミラー イメージクリプト IPv4-ACL を使用することを強く推奨します。

クリプト IPv4-ACL の any キーワード



Tip IPSec で使用するミラー イメージクリプト IPv4-ACL は、**any** オプションを使用しないで設定することを推奨します。

IPSec インターフェイスを経由してマルチキャスト トラフィックを転送すると、**permit** ステートメントの **any** キーワードは廃棄されます。これは、マルチキャスト トラフィックの転送が失敗する原因になります。

permit any ステートメントを使用すると、すべてのアウトバウンドトラフィックが保護され（保護されたすべてのトラフィックが、対応するクリプト マップ エントリで指定されたピアに送信され）、すべてのインバウンドトラフィックの保護が必要になります。ルーティング プロトコル、NTP、エコー、エコー応答用のパケットを含む、IPSec で保護されないすべてのインバウンドパケットは、自動的に廃棄されます。

保護するパケットを確実に定義する必要があります。**permit** ステートメント内で **any** オプションを使用する必要がある場合は、保護しないすべてのトラフィックを除外する一連の **deny** ステートメントを、**permit** ステートメントの前に付加する必要があります（付加しない場合、これらのトラフィックが **permit** ステートメントの対象になります）。

クリプト IPv4-ACL の作成

IPv4-ACL を作成するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **ip access-list List1 permit ip 10.1.1.100 0.0.0.255 11.1.1.100 0.0.0.255**

指定のネットワークから、または指定のネットワークへの、すべての IP トラフィックを許可します。

Example



Note `show ip access-list` コマンドではクリプト マップ エントリは表示されません。関連エントリを表示するには、`show crypto map` コマンドを使用します。

IPSec のトランスフォーム セットの概要

トランスフォーム セットは、特定のセキュリティ プロトコルとアルゴリズムの組み合わせを表します。IPSec SA のネゴシエーション中に、ピアは特定のトランスフォーム セットを使用して特定のデータ フローを保護することに合意します。

複数のトランスフォーム セットを指定し、これらのトランスフォーム セットの 1 つまたは複数 をクリプト マップ エントリに指定できます。クリプト マップ エントリで定義されたトランスフォーム セットは、このクリプト マップ エントリのアクセス リストで指定されたデータ フローを保護するために、IPSec SA ネゴシエーションで使用されます。

IKE との IPSec セキュリティ アソシエーションのネゴシエーション中に、ピアは両方のピア上で同じトランスフォーム セットを検索します。同一のトランスフォーム セットが検出された場合には、そのトランスフォーム セットが選択され、両方のピアの IPSec SA の一部として、保護するトラフィックに適用されます。



Tip トランスフォーム セット定義を変更した場合には、トランスフォーム セットを参照するクリプト マップ エントリだけに変更が適用されます。変更は既存の SA には適用されませんが、新規 SA を確立するために以降のネゴシエーションで使用されます。新規設定を即座に有効にする場合には、SA データベースのすべてまたは一部を消去します。



Note IPSec をイネーブルにすると、Cisco NX-OS ソフトウェアにより、AES-128 暗号化および SHA-1 認証アルゴリズムを使用したデフォルトのトランスフォーム セット (`ipsec_default_transform_set`) が自動的に作成されます。

次の表に、IPsec で許可されるトランスフォームの組み合わせのリストを示します。

Table 15: IPSec トランスフォーム設定パラメータ

パラメータ	許容値	キーワード
暗号化アルゴリズム	56 ビット DES-CBC 168 ビット DES 128 ビット AES-CBC 128 ビット AES-CTR ³ 256 ビット AES-CBC 256 ビット AES-CTR 1	esp-des esp-3des esp-aes 128 esp-aes 128 ctr esp-aes 256 esp-aes 256 ctr
ハッシュ/認証アルゴリズム1 (オプション)	SHA-1 (HMAC バリエント) SHA-2 (HMAC バリエント) MD5 (HMAC バリエント) AES-XCBC-MAC	esp-sha1-hmac esp-sha256-hmac ⁴ esp-sha512-hmac ⁵ esp-md5-hmac esp-aes-xcbc-mac ⁶

³ AES カウンタ (CTR) モードを設定する場合には、認証アルゴリズムも設定する必要があります。

⁴ **esp-sha256-hmac** 認証アルゴリズムは、IKEv2 でのみサポートされています。

⁵ **esp-sha512-hmac** 認証アルゴリズムは、IKEv2 でのみサポートされています。

⁶ Cisco MDS NX-OS リリース 5.2(2)以降、**esp-aes-xcbc-mac** 認証アルゴリズムはサポートされていません。

次の表に、Microsoft Windows および Linux プラットフォームでサポートおよび検証されている、IPSec および IKE 暗号化認証アルゴリズムの設定を示します。

プラットフォーム	IKE	IPSec
Microsoft iSCSI 発信側 (Microsoft Windows 2000 プラットフォームの Microsoft IPSec 実装)	3DES、SHA-1、SHA-2 または MD5、DH グループ 2	3DES、SHA-1、SHA-2
Cisco iSCSI 発信側 (Linux プラットフォームの Free Swan IPSec 実装)	3DES、MD5、DH グループ 1	3DES、MD5

トランスフォームセットの設定

トランスフォームセットを設定する手順は、次のとおりです。

Procedure

ステップ 1 switch# configure terminal

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# crypto transform-set domain ipsec test esp-3des esp-md5-hmac

3DES 暗号化アルゴリズムと MD5 認証アルゴリズムを指定する、test というトランスフォーム セットを設定します。許可されるトランスフォームの組み合わせを確認するには、IPsec トランスフォーム設定パラメータの表を参照してください。

ステップ 3 switch(config)# no crypto transform-set domain ipsec test esp-3des esp-md5-hmac

(オプション) 適用されたトランスフォーム セットを削除します。

ステップ 4 switch(config)# crypto transform-set domain ipsec test esp-3des

3DES 暗号化アルゴリズムを指定する、test というトランスフォーム セットを設定します。この例では、デフォルトの認証は実行されません。

ステップ 5 switch(config)# no crypto transform-set domain ipsec test esp-3des

(オプション) 適用されたトランスフォーム セットを削除します。

クリプト マップ エントリの概要

クリプト IPv4-ACL とトランスフォーム セットの作成が完了すると、次のように、IPSec SA のさまざまな部分を組み合わせたクリプト マップ エントリを作成できます。

- IPSec で保護するトラフィック (クリプト IPv4-ACL 単位)。クリプト マップ セットには、それぞれ異なる IPv4-ACL を使用する複数のエントリを設定できます。
- SA セットで保護するフローの詳細度。
- IPSec で保護されるトラフィックの宛先 (リモート IPSec ピアの名前)。
- IPSec トラフィックが使用するローカル アドレス (インターフェイスに適用)。
- 現在のトラフィックに適用する IPSec セキュリティ (1 つまたは複数のトランスフォーム セットから選択)。
- IPSec SA を定義するその他のパラメータ。

同じクリプト マップ名 (マップ シーケンス番号が異なる) を持つクリプト マップ エントリは、クリプト マップ セットにグループ化されます。

クリプト マップ セットをインターフェイスに適用すると、次のイベントが発生します。

- そのインターフェイス用の Security Policy Database (SPD) が作成されます。
- インターフェイスを経由するすべての IP トラフィックが、SPD に対して評価されます。

クリプト マップ エントリにより保護を必要とするアウトバウンド IP トラフィックが確認されると、クリプト マップ エントリ内のパラメータに従って、SA とリモート ピアのネゴシエーションが行われます。

SA のネゴシエーションでは、クリプト マップ エントリから取得したポリシーが使用されます。ローカルスイッチがネゴシエーションを開始した場合、ローカルスイッチはクリプト マップ エントリに指定されたポリシーを使用して、指定された IPSec ピアに送信するオファーを作成します。IPSec ピアがネゴシエーションを開始した場合、ローカルスイッチはクリプト マップ エントリのポリシーを調べて、ピアの要求（オファー）を受け入れるか、または拒否するかを判断します。

2つの IPSec ピア間で IPSec を成立させるには、両方のピアのクリプト マップ エントリに互換性のあるコンフィギュレーション ステートメントが含まれている必要があります。

ピア間の SA の確立

2つのピアが SA を確立する場合、各ピアのクリプト マップ エントリの1つまたは複数と、相手ピアのクリプト マップ エントリの1つに互換性がなければなりません。

2つのクリプト マップ エントリで互換性が成立するには、少なくとも次の基準を満たす必要があります。

- クリプト マップ エントリに、互換性のあるクリプト IPv4-ACL（ミラーイメージ IPv4-ACL など）が含まれていること。応答側のピア エントリがローカルで暗号化されている場合、IPv4-ACL がこのピアのクリプト IPv4-ACL で許可されている必要があります。
- クリプト マップ エントリが互いに相手ピアを識別しているか、または自動ピアが設定されていること。
- 特定のインターフェイスに複数のクリプト マップ エントリを作成するときは、各マップ エントリの seq-num を使用して、マップ エントリにランクを設定します。seq-num の値が小さいほど、プライオリティは高くなります。クリプト マップ セットがあるインターフェイスでは、トラフィックは、最初にプライオリティの高いマップ エントリに対して評価されます。
- IKE ネゴシエーションを実行して SA を確立するには、クリプト マップ エントリに最低1つの共通トランスフォームセットが含まれている必要があります。IPSec SA のネゴシエーション中に、両ピアは特定のトランスフォームセットを使用して特定のデータフローを保護することに合意します。

パケットが特定の IPv4-ACL 内の permit エントリと一致すると、対応するクリプト マップ エントリにタグが付けられ、接続が確立されます。

クリプト マップ 設定の注意事項

クリプト マップ エントリを設定する場合には、次の注意事項に従ってください。

- ポリシーが適用される順序は、各クリプト マップ のシーケンス番号によって決まります。シーケンス番号が小さいほど、プライオリティは高くなります。
- 各クリプト マップ エントリに使用できる IPv4-ACL は1つだけです（IPv4-ACL 自体には複数の permit エントリまたは deny エントリを設定できます）。

- トンネルエンドポイントが宛先アドレスと同じである場合は、`auto-peer` オプションを使用して、ピアを動的に設定できます。
- IPsec を Microsoft iSCSI 発信側と効率的に相互運用するには、IPv4-ACL に TCP プロトコルとローカル iSCSI TCP ポート番号（デフォルトは 3260）を指定します。この設定により、ギガビットイーサネットインターフェイスのシャットダウン、VRRP スイッチオーバー、ポート障害などにより処理が中断されても、暗号化 iSCSI セッションを迅速に回復できます。

クリプト マップ エントリの作成



Note クリプトマップエントリで指定されたピアの IP アドレスがリモートの Cisco MDS スイッチの VRRP IP アドレスである場合、IP アドレスが **secondary** オプションを使用して作成されることを確認します（詳細については、『Cisco MDS 9000 Family NX-OS IP Services Configuration Guide』を参照してください）。

必須のクリプト マップ エントリを作成する手順は、次のとおりです。

Procedure

- ステップ 1** `switch# configure terminal`
`switch(config)#`
 コンフィギュレーションモードに入ります。
- ステップ 2** `switch(config)# crypto map domain ipsec SampleMap 31`
`ips-hacl(config-crypto-map-ip)#`
 シーケンス番号が 31 の SampleMap というエントリに対し、クリプトマップ設定モードを開始します。
- ステップ 3** `switch(config)# no crypto map domain ipsec SampleMap 31`
 (オプション) 指定されたクリプトマップエントリを削除します。
- ステップ 4** `switch(config)# no crypto map domain ipsec SampleMap`
 (オプション) SampleMap と呼ばれるクリプトマップセット全体を削除します。
- ステップ 5** `switch(config-crypto-map-ip)# match address SampleAcl`
 このクリプトマップエントリのコンテキストで、IPsec によって保護するトラフィックと保護しないトラフィックを決定する ACL を指定します。
- ステップ 6** `switch(config-crypto-map-ip)# no match address SampleAcl`
 (オプション) 一致したアドレスを削除します。

- ステップ 7** switch(config-crypto-map-ip)# **set peer 10.1.1.1**
特定のピアの IPv4 アドレスを設定します。
- Note** IKE は、IPv4 アドレスのみをサポートし、IPv6 アドレスはサポートしません。
- ステップ 8** switch(config-crypto-map-ip)# **no set peer 10.1.1.1**
(オプション) 設定されたピアを削除します。
- ステップ 9** switch(config-crypto-map-ip)# **set transform-set SampleTransform1 SampleTransmfor2**
指定した暗号マップ エントリに対し許可するトランスフォーム セットを指定します。複数のトランスフォームセットをプライオリティ順 (最高のプライオリティのものが最初) に列挙します。
- ステップ 10** switch(config-(crypto-map-ip))# **no set transform-set**
(オプション) すべてのトランスフォームセットのアソシエーションを削除します (トランスフォームセットの名前の指定に関係なく)。

SA ライフタイム ネゴシエーションの概要

SA 固有のライフタイム値を設定することにより、グローバル ライフタイム値 (サイズおよびタイム) を書き換えることができます。

SA ライフタイム ネゴシエーション値を指定する場合、指定したクリプトマップにライフタイム値を設定することもできます。この場合、設定されたライフタイム値によってグローバルな設定値が上書きされます。クリプトマップ固有のライフタイムを指定しない場合には、グローバル値 (またはグローバルなデフォルト値) が使用されます。

グローバル ライフタイム値の詳細については、[グローバル ライフタイム値, on page 248](#)を参照してください。

SA ライフタイムの設定

指定したクリプト マップ エントリの SA ライフタイムを設定する手順は、次のとおりです。

Procedure

- ステップ 1** switch# **configure terminal**
switch(config)#
コンフィギュレーション モードに入ります。
- ステップ 2** switch(config)# **crypto map domain ipsec SampleMap 31**
switch(config-crypto-map-ip)#

シーケンス番号が 31 の SampleMap というエントリに対し、クリプトマップ設定サブモードを開始します。

ステップ 3 switch(config-crypto-map-ip)# set security-association lifetime seconds 8640

クリプトマップのエントリに対するグローバルなライフタイムとは異なる IPsec SA ライフタイムを使用して、このクリプトマップのエントリに対する SA ライフタイムを指定します。

ステップ 4 switch(config-crypto-map-ip)# no set security-association lifetime seconds 8640

(オプション) エントリ固有の設定を削除し、グローバル設定に戻します。

ステップ 5 switch(config-crypto-map-ip)# set security-association lifetime gigabytes 4000

指定したトラフィック量 (GB 単位) が SA を使用して FCIP リンクを通過した後、この SA のトラフィック量ライフタイムがタイムアウトするように設定します。ライフタイムの範囲は 1 ~ 4095 GB です。

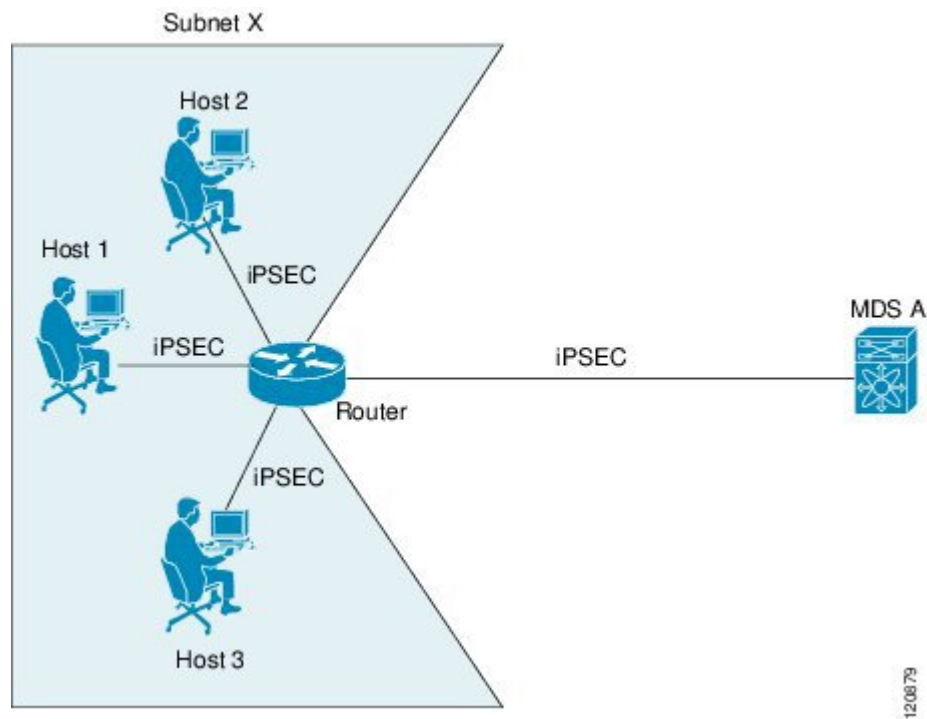
AutoPeer オプションの概要

クリプトマップ内でピアアドレスを **auto-peer** として設定した場合は、トラフィックの宛先エンドポイントが SA のピアアドレスとして使用されます。同じクリプトマップを使用して、クリプトマップの IPv4-ACL エントリで指定されたサブネット内の各エンドポイントに、固有の SA を設定できます。auto-peer を使用すると、トラフィック エンドポイントが IPsec に対応している場合に、設定が簡素化されます。auto-peer は、同じサブネット内の複数の iSCSI ホストで個別の設定が必要ない場合、特に役立ちます。

Figure 16: auto-peer オプションを使用した iSCSI のエンドツーエンド IPsec, on page 245 に、auto-peer オプションによって設定が簡素化される例を示します。auto-peer オプションを使用すると、サブネット X からの全ホストについて、1 つのクリプトマップ エントリだけを使用してスイッチとの SA を確立できます。各ホストは独自の SA を確立しますが、クリプトマップ エントリは共有されます。auto-peer オプションを使用しない場合、各ホストに 1 つのクリプトマップ エントリが必要になります。

詳細については、[iSCSI の設定例, on page 259](#)を参照してください。

Figure 16: auto-peer オプションを使用した iSCSI のエンドツーエンド IPsec



120879

AutoPeer オプションの設定

auto-peer オプションを設定するには、次の手順を実行します。

Procedure

ステップ 1 `switch# configure terminal`

`switch(config)#`

コンフィギュレーションモードに入ります。

ステップ 2 `switch(config)# crypto map domain ipsec SampleMap 31`

`ips-hacl(config-crypto-map-ip)#`

シーケンス番号が 31 の SampleMap というエントリに対し、クリプトマップ設定モードを開始します。

ステップ 3 `switch(config-crypto-map-ip)# set peer auto-peer`

ソフトウェアに (SA セットアップの間に) 宛先ピアの IP アドレスを動的に選択するように指示します。

ステップ 4 `switch(config-crypto-map-ip)# no set peer auto-peer`

(オプション) `auto-peer` 設定を削除します。

PFS の概要

SA ライフタイム ネゴシエーション値を指定する場合、オプションでクリプトマップの完全転送秘密 (PFS) 値を設定できます。

PFS 機能は、デフォルトではディセーブルです。PFS グループを設定する場合は、DH グループ 1、2、5、または 14 のうちの 1 つを設定できます。DH グループを指定しない場合、グループ 1 がデフォルトで使用されます。

PFS の設定

PFS 値を設定する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **crypto map domain ipsec SampleMap 31**

```
ips-hacl(config-crypto-map-ip)#
```

シーケンス番号が 31 の SampleMap というエントリに対し、クリプトマップ設定モードを開始します。

ステップ 3 switch(config-crypto-map-ip)# **set pfs group 2**

IPsec がこのクリプトマップエントリの新しい SA を要求した場合、PFS を要求するように、または IPsec ピアから受信する要求に PFS が含まれることを要求するように指定します。

ステップ 4 switch(config-crypto-map-ip)# **no set pfs**

(オプション) 設定済みの DH グループを削除し、工場出荷時のデフォルトである PFS のディセーブル化に戻します。

クリプトマップセットインターフェイスの適用の概要

IPSec トラフィックフローが通過する各インターフェイスにクリプトマップセットを適用する必要があります。インターフェイスにクリプトマップセットを適用すると、スイッチはそのインターフェイスのすべてのトラフィックを指定されたクリプトマップセットに対して評

値し、指定されたポリシーを接続中または SA ネゴシエーション中に使用して、トラフィックが暗号によって保護されるようにします。

1つのインターフェイスに適用できるクリプトマップセットは1つだけです。複数のインターフェイスに同じクリプトマップを適用できます。ただし、各インターフェイスに複数のクリプトマップセットを適用できません。

クリプト マップセットの適用

クリプト マップセットをインターフェイスに適用する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **interface gigabitethernet 4/1**

```
switch(config-if)#
```

IPsec 暗号マップが適用される、必要なギガビットイーサネットインターフェイス（および必要な場合はサブインターフェイス）を選択します。

ステップ 3 switch(config-if)# **crypto map domain ipsec cm10**

暗号マップセットを選択したインターフェイスに適用します。

ステップ 4 switch(config-if)# **no crypto map domain ipsec**

（オプション）現在このインターフェイスに適用されている暗号マップを削除します。

IPsec のメンテナンス

設定の変更は、後続の SA のネゴシエーション時まで適用されません。新しい設定をすぐに適用するには、変更した設定を使用して SA が再確立されるように、既存の SA をクリアする必要があります。スイッチが IPsec トラフィックをアクティブに処理している場合には、SA データベースのうち、設定変更が影響する部分だけを消去してください（つまり、指定のクリプトマップセットによって確立された SA だけを消去します）。SA データベース全体を消去するのは、大規模な変更を行った場合、またはルータが他の IPsec トラフィックをほとんど処理していない場合だけにしてください。



Tip `show crypto sa domain interface gigabitethernet slot/port` コマンドの出力から SA インデックスを得ることができます。

SA データベースの一部を消去するには、次のコマンドを使用します。

```
switch# clear crypto sa domain ipsec interface gigabitethernet 2/1 inbound sa-index 1
```



Note IPsec のセキュリティ アソシエーションをクリアした後、少なくとも 10 秒待ってから `system switchover` コマンドを実行してください。

グローバル ライフタイム値

クリプト マップ エントリにライフタイムが設定されていない場合、新しい IPsec SA のネゴシエーション時にグローバル ライフタイム値が使用されます。

タイムまたはトラフィック ボリュームの2つのライフタイムを設定できます。どちらか一方のライフタイムに到達すると、SA は期限切れになります。デフォルトのライフタイムは 3,600 秒（1 時間）および 450 GB です。

グローバル ライフタイムを変更した場合、新しいライフタイム値は既存の SA には適用されず、以降に確立される SA のネゴシエーションに使用されます。新しいライフタイム値をすぐに使用する場合は、SA データベースのすべてまたは一部を消去します。

特定のクリプト マップ エントリにライフタイム値が設定されていない場合、スイッチは新規 SA を要求するときに、ピアへの要求内でグローバル ライフタイム値を指定します。この値は、新規 SA のライフタイム値として使用されます。ピアからのネゴシエーション要求を受信すると、スイッチは使用中の IKE バージョンによって決まる値を使用します。

- IKEv1 を使用して IPsec SA を設定する場合、SA ライフタイム値は、2つの候補のうち小さい方の値になります。トンネルの両端で、同じ値がプログラムされます。
- IKEv2 を使用して IPsec SA を設定する場合、各端の SA に独自のライフタイム値が設定されるので、両端の SA は個別に期限切れになります。

SA（および対応するキー）は、指定時間（秒単位）または指定トラフィック量（バイト単位）のどちらか一方が先に経過した時点で、期限切れになります。

既存の SA のライフタイムしきい値に到達する前に、新しい SA がネゴシエートされます。これは、既存の SA が期限切れになる前にネゴシエーションを完了するためです。

新しい SA は、次のいずれかのしきい値に先に到達した時点でネゴシエートされます。

- ライフタイムが期限切れになる 30 秒前
- ライフタイムの残りのバイト数が約 10% になったとき

ライフタイムが期限切れになった時点でトラフィックが送受信されていない場合、新しい SA はネゴシエートされません。新しい SA がネゴシエートされるのは、IPSec が別の保護対象パケットを確認した場合だけです。

SA ライフタイムを設定する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **crypto global domain ipsec security-association lifetime seconds 86400**

指定した秒数が経過した後、IPsec SA のグローバルライフタイムがタイムアウトするように設定します。グローバル ライフタイムの範囲は 120 ~ 86400 秒です。

ステップ 3 switch(config)# **no crypto global domain ipsec security-association lifetime seconds 86400**

(オプション) 出荷時デフォルトの 3,600 秒に戻します。

ステップ 4 switch(config)# **crypto global domain ipsec security-association lifetime gigabytes 4000**

指定したトラフィック量 (GB 単位) が SA を使用して FCIP リンクを通過した後、IPsec SA のグローバルトラフィック量ライフタイムがタイムアウトするように設定します。グローバル ライフタイムの範囲は 1~4095 GB です。

ステップ 5 switch(config)# **crypto global domain ipsec security-association lifetime kilobytes 2560**

グローバルトラフィック量のライフタイムを設定します (KB 単位)。グローバルライフタイムの範囲は 2560 ~ 2147483647 KB です。

ステップ 6 switch(config)# **crypto global domain ipsec security-association lifetime megabytes 5000**

グローバルトラフィック量のライフタイムを設定します (MB 単位)。グローバル ライフタイムの範囲は 3 ~ 4193280 MB です。

ステップ 7 switch(config)# **no crypto global domain ipsec security-association lifetime megabytes**

現在設定されている値に関係なく、工場出荷時のデフォルトの 450 GB に戻します。

IKE 設定の表示

show コマンドのセットを使用して、IKE 情報を確認できます。次の例を参照してください。

各 IKE ポリシー用に設定されたパラメータの表示

```
switch# show crypto ike domain ipsec

keepalive 60000
```

イニシエータ設定の表示

```
switch# show crypto ike domain ipsec initiator

initiator version 1 address 1.1.1.1
initiator version 1 address 1.1.1.2
```

キーの設定の表示

```
switch# show crypto ike domain ipsec key

key abcdefgh address 1.1.1.1
key bcdefghi address 1.1.2.1
```

IKE 用の現在確立されたポリシーの表示

```
switch# show crypto ike domain ipsec policy 1

Priority 1, auth pre-shared, lifetime 6000 secs, encryption 3des, hash md5, DH group 5
Priority 3, auth pre-shared, lifetime 86300 secs, encryption aes, hash sha1, DH group 1
Priority 5, auth pre-shared-key, lifetime 86400 secs, encryption 3des, hash sha256, DH
group 1
```

IKE 用の現在確立された SA の表示

```
switch# show crypto ike domain ipsec sa
```

Tunn	Local Addr	Remote Addr	Encr	Hash	Auth Method	Lifetime
1*	172.22.31.165[500]	172.22.31.166[500]	3des	sha1	preshared key	86400
2	172.22.91.174[500]	172.22.91.173[500]	3des	sha1	preshared key	86400

NOTE: tunnel id ended with * indicates an IKEv1 tunnel

IPsec 設定の表示

show コマンドのセットを使用して、IPsec 情報を確認できます。次の例を参照してください。

指定された ACL の情報の表示

```
switch# show ip access-list acl10

ip access-list acl10 permit ip 10.10.10.0 0.0.0.255 10.10.10.0 0.0.0.255 (0 matches)
```

上記の例では、表示出力一致に、この条件を満たすインターフェイス（暗号マップではない）だけが表示されます。

トランスフォームセットの設定の表示

```
switch# show crypto transform-set domain ipsec

Transform set: 1/1 {esp-3des esp-sha256-hmac}
    will negotiate {tunnel}
Transform set: ipsec_default_transform_set {esp-aes 128 esp-sha1-hmac}
    will negotiate {tunnel}
```

設定されたすべての暗号マップの表示

```
switch# show crypto map domain ipsec

Crypto Map "cm10" 1 ipsec
  Peer = Auto Peer
  IP ACL = acl10
    permit ip 10.10.10.0 255.255.255.0 10.10.10.0 255.255.255.0
  Transform-sets: 3des-md5, des-md5,
  Security Association Lifetime: 4500 megabytes/3600 seconds
  PFS (Y/N): N
  Interface using crypto map set cm10:
    GigabitEthernet4/1
Crypto Map "cm100" 1 ipsec
  Peer = Auto Peer
  IP ACL = acl100
    permit ip 10.10.100.0 255.255.255.0 10.10.100.0 255.255.255.0
  Transform-sets: 3des-md5, des-md5,
  Security Association Lifetime: 4500 megabytes/3600 seconds
  PFS (Y/N): N
  Interface using crypto map set cm100:
    GigabitEthernet4/2
```

特定のインターフェイス用の暗号マップ情報の表示

```
switch# show crypto map domain ipsec interface gigabitethernet 4/1

Crypto Map "cm10" 1 ipsec
  Peer = Auto Peer
  IP ACL = acl10
    permit ip 10.10.10.0 255.255.255.0 10.10.10.0 255.255.255.0
  Transform-sets: 3des-md5, des-md5,
  Security Association Lifetime: 4500 megabytes/3600 seconds
  PFS (Y/N): N
  Interface using crypto map set cm10:
    GigabitEthernet4/1
```

指定した暗号マップ情報の表示

```
switch# show crypto map domain ipsec tag cm100

Crypto Map "cm100" 1 ipsec
  Peer = Auto Peer
  IP ACL = acl100
    permit ip 10.10.100.0 255.255.255.0 10.10.100.0 255.255.255.0
  Transform-sets: 3des-md5, des-md5,
  Security Association Lifetime: 4500 megabytes/3600 seconds
  PFS (Y/N): N
  Interface using crypto map set cm100:
    GigabitEthernet4/2
```

指定したインターフェイス用の SA アソシエーションの表示

```
switch# show crypto sad domain ipsec interface gigabitethernet 4/1

interface: GigabitEthernet4/1
  Crypto map tag: cm10, local addr. 10.10.10.1
  protected network:
  local ident (addr/mask): (10.10.10.0/255.255.255.0)
  remote ident (addr/mask): (10.10.10.4/255.255.255.255)
  current_peer: 10.10.10.4
    local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.4
    mode: tunnel, crypto algo: esp-3des, auth algo: esp-md5-hmac
    current outbound spi: 0x30e000f (51249167), index: 0
    lifetimes in seconds:: 3600
    lifetimes in bytes:: 423624704
  current inbound spi: 0x30e0000 (51249152), index: 0
  lifetimes in seconds:: 3600
  lifetimes in bytes:: 423624704
```

すべての SA アソシエーションの表示

```
switch# show crypto sad domain ipsec

interface: GigabitEthernet4/1
  Crypto map tag: cm10, local addr. 10.10.10.1
  protected network:
  local ident (addr/mask): (10.10.10.0/255.255.255.0)
  remote ident (addr/mask): (10.10.10.4/255.255.255.255)
  current_peer: 10.10.10.4
    local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.4
    mode: tunnel, crypto algo: esp-3des, auth algo: esp-md5-hmac
    current outbound spi: 0x30e000f (51249167), index: 0
    lifetimes in seconds:: 3600
    lifetimes in bytes:: 423624704
  current inbound spi: 0x30e0000 (51249152), index: 0
  lifetimes in seconds:: 3600
  lifetimes in bytes:: 423624704
```

ポリシー データベースに関する情報の表示

```
switch# show crypto spd domain ipsec

Policy Database for interface: GigabitEthernet4/1, direction: Both
# 0:      deny  udp any port eq 500 any
# 1:      deny  udp any any port eq 500
# 2:      permit ip 10.10.10.0 255.255.255.0 10.10.10.0 255.255.255.0
# 63:     deny  ip any any
Policy Database for interface: GigabitEthernet4/2, direction: Both
# 0:      deny  udp any port eq 500 any <-----UDP default entry
# 1:      deny  udp any any port eq 500 <----- UDP default entry
# 3:      permit ip 10.10.100.0 255.255.255.0 10.10.100.0 255.255.255.0
# 63:     deny  ip any any <----- Clear text default
entry
```

特定のインターフェイス用の SPD 情報の表示

```
switch# show crypto spd domain ipsec interface gigabitethernet 4/2

Policy Database for interface: GigabitEthernet3/1, direction: Both
# 0:      deny  udp any port eq 500 any
# 1:      deny  udp any any port eq 500
```

```
# 2:      permit ip 10.10.10.0 255.255.255.0 10.10.10.0 255.255.255.0
# 127:    deny ip any any
```

特定のインターフェースの詳細な iSCSI セッション情報の表示

```
switch# show iscsi session detail

Initiator iqn.1987-05.com.cisco:01.9f39f09c7468 (ips-host16.cisco.com)
  Initiator ip addr (s): 10.10.10.5
  Session #1 (index 24)
    Discovery session, ISID 00023d000001, Status active
  Session #2 (index 25)
    Target ibml
    VSAN 1, ISID 00023d000001, TSIH 0, Status active, no reservation
    Type Normal, ExpCmdSN 42, MaxCmdSN 57, Barrier 0
    MaxBurstSize 0, MaxConn 1, DataPDUInOrder Yes
    DataSeqInOrder Yes, InitialR2T Yes, ImmediateData No
    Registered LUN 0, Mapped LUN 0
    Stats:
      PDU: Command: 41, Response: 41
      Bytes: TX: 21388, RX: 0
    Number of connection: 1
    Connection #1
      iSCSI session is protected by IPsec -----The iSCSI session protection status

      Local IP address: 10.10.10.4, Peer IP address: 10.10.10.5
      CID 0, State: Full-Feature
      StatSN 43, ExpStatSN 0
      MaxRecvDSLength 131072, our_MaxRecvDSLength 262144
      CSG 3, NSG 3, min_pdu_size 48 (w/ data 48)
      AuthMethod none, HeaderDigest None (len 0), DataDigest None (len 0)
      Version Min: 0, Max: 0
      FC target: Up, Reorder PDU: No, Marker send: No (int 0)
      Received MaxRecvDSLen key: Yes
```

特定のインターフェース用の FCIP 情報の表示

```
switch# show interface fcip 1
fcip1 is trunking
  Hardware is GigabitEthernet
  Port WWN is 20:50:00:0d:ec:08:6c:c0
  Peer port WWN is 20:10:00:05:30:00:a7:9e
  Admin port mode is auto, trunk mode is on
  Port mode is TE
  Port vsan is 1
  Speed is 1 Gbps
  Trunk vsans (admin allowed and active) (1)
  Trunk vsans (up) (1)
  Trunk vsans (isolated) ()
  Trunk vsans (initializing) ()
  Using Profile id 1 (interface GigabitEthernet2/1)
  Peer Information
    Peer Internet address is 10.10.11.1 and port is 3225
  FCIP tunnel is protected by IPsec -----The FCIP tunnel protection status
  Write acceleration mode is off
  Tape acceleration mode is off
  Tape Accelerator flow control buffer size is 256 KBytes
  IP Compression is disabled
  Special Frame is disabled
  Maximum number of TCP connections is 2
  Time Stamp is disabled
  QOS control code point is 0
  QOS data code point is 0
```

```

B-port mode disabled
TCP Connection Information
  2 Active TCP connections
    Control connection: Local 10.10.11.2:3225, Remote 10.10.11.1:65520
    Data connection: Local 10.10.11.2:3225, Remote 10.10.11.1:65522
  2 Attempts for active connections, 0 close of connections
TCP Parameters
  Path MTU 1400 bytes
  Current retransmission timeout is 200 ms
  Round trip time: Smoothed 2 ms, Variance: 1
  Advertized window: Current: 124 KB, Maximum: 124 KB, Scale: 6
  Peer receive window: Current: 123 KB, Maximum: 123 KB, Scale: 6
  Congestion window: Current: 53 KB, Slow start threshold: 48 KB
  Current Send Buffer Size: 124 KB, Requested Send Buffer Size: 0 KB
  CWM Burst Size: 50 KB
  5 minutes input rate 128138888 bits/sec, 16017361 bytes/sec, 7937 frames/sec
  5 minutes output rate 179275536 bits/sec, 22409442 bytes/sec, 46481 frames/sec
  10457037 frames input, 21095415496 bytes
    308 Class F frames input, 32920 bytes
    10456729 Class 2/3 frames input, 21095382576 bytes
    9907495 Reass frames
    0 Error frames timestamp error 0
  63792101 frames output, 30250403864 bytes
    472 Class F frames output, 46816 bytes
    63791629 Class 2/3 frames output, 30250357048 bytes
    0 Error frames

```

スイッチのグローバル IPsec 統計情報の表示

```

switch# show crypto global domain ipsec

IPSec global statistics:
  Number of crypto map sets: 3
  IKE transaction stats: 0 num, 256 max
  Inbound SA stats: 0 num
  Outbound SA stats: 0 num

```

指定したインターフェースの IPsec 統計情報の表示

```

switch# show crypto global domain ipsec interface gigabitethernet 3/1

IPSec interface statistics:
  IKE transaction stats: 0 num
  Inbound SA stats: 0 num, 512 max
  Outbound SA stats: 0 num, 512 max

```

グローバル SA ライフタイム値の表示

```

switch# show crypto global domain ipsec security-association lifetime

Security Association Lifetime: 450 gigabytes/3600 seconds

```

FCIP の設定例

Figure 17: FCIP のシナリオの IP セキュリティの使用, on page 255 では 1 つの FCIP リンク (トンネル 2) の IPsec の実装に注目しています。トンネル 2 は MDS A と MDS C 間で暗号化データを伝送します。

Figure 17: FCIP のシナリオの IP セキュリティの使用

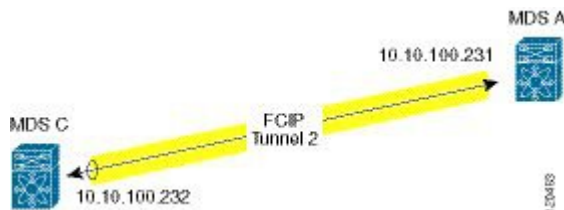


Figure 17: FCIP のシナリオの IP セキュリティの使用, on page 255 に示す FCIP シナリオで IPsec を設定するには、次の手順を実行します。

Procedure

ステップ 1 スイッチ MDS A で IKE および IPsec をイネーブルにします。

```
sw10.1.1.100# configure terminal
sw10.1.1.100(config)# feature crypto ike
sw10.1.1.100(config)# feature crypto ipsec
```

ステップ 2 スイッチ MDS A に IKE を設定します。

```
sw10.1.1.100(config)# crypto ike domain ipsec
sw10.1.1.100(config-ike-ipsec)# key ctct address 10.10.100.232
sw10.1.1.100(config-ike-ipsec)# policy 1
sw10.1.1.100(config-ike-ipsec-policy)# encryption 3des
sw10.1.1.100(config-ike-ipsec-policy)# hash md5
sw10.1.1.100(config-ike-ipsec-policy)# end
sw10.1.1.100#
```

ステップ 3 スイッチ MDS A に ACL を設定します。

```
sw10.1.1.100# configure terminal
sw10.1.1.100(config)# ip access-list acl1 permit tcp 10.10.100.231 0.0.0.0 10.10.100.232
0.
0.0.0
```

ステップ 4 スイッチ MDS A にトランスフォームセットを設定します。

```
sw10.1.1.100(config)# crypto transform-set domain ipsec tfs-02 esp-aes 128
esp-sha1-hmac
```

ステップ 5 スイッチ MDS A に暗号マップを設定します。

```
sw10.1.1.100(config)# crypto map domain ipsec cmap-01 1
sw10.1.1.100(config-crypto-map-ip)# match address acl1
sw10.1.1.100(config-crypto-map-ip)# set peer 10.10.100.232
sw10.1.1.100(config-crypto-map-ip)# set transform-set tfs-02
sw10.1.1.100(config-crypto-map-ip)# set security-association lifetime seconds 3600
sw10.1.1.100(config-crypto-map-ip)# set security-association lifetime gigabytes 3000
sw10.1.1.100(config-crypto-map-ip)# set pfs group5
sw10.1.1.100(config-crypto-map-ip)# end
sw10.1.1.100#
```

ステップ 6 スイッチ MDS A の暗号マップセットにインターフェイスをバインドします。

```
sw10.1.1.100# configure terminal
sw10.1.1.100(config)# int gigabitethernet 7/1
```

```
sw10.1.1.100(config-if)# ip addr 10.10.100.231 255.255.255.0
sw10.1.1.100(config-if)# crypto map domain ipsec cmap-01
sw10.1.1.100(config-if)# no shut
sw10.1.1.100(config-if)# exit
sw10.1.1.100(config)#
```

ステップ7 スイッチ MDS A に FCIP を設定します。

```
sw10.1.1.100(config)# feature fcip
sw10.1.1.100(config)# fcip profile 2
sw10.1.1.100(config-profile)# ip address 10.10.100.231
sw10.1.1.100(config-profile)# int fcip 2
sw10.1.1.100(config-if)# peer-info ipaddr 10.10.100.232
sw10.1.1.100(config-if)# use-profile 2
sw10.1.1.100(config-if)# no shut
sw10.1.1.100(config-if)# end
sw10.1.1.100#
```

ステップ8 スイッチ MDS A の設定を確認します。

```
sw10.1.1.100# show crypto global domain ipsec security-association lifetime
Security Association Lifetime: 4500 megabytes/3600 seconds

sw10.1.1.100# show crypto map domain ipsec
Crypto Map "cmap-01" 1 ipsec
  Peer = 10.10.100.232
  IP ACL = acl1
    permit ip 10.10.100.231 255.255.255.255 10.10.100.232 255.255.255.255
  Transform-sets: tfs-02,
  Security Association Lifetime: 3000 gigabytes/3600 seconds
  PFS (Y/N): Y
  PFS Group: group5
Interface using crypto map set cmap-01:
  GigabitEthernet7/1

sw10.1.1.100# show crypto transform-set domain ipsec
Transform set: tfs-02 {esp-aes 128 esp-shal-hmac}
  will negotiate {tunnel}

sw10.1.1.100# show crypto spd domain ipsec
Policy Database for interface: GigabitEthernet7/1, direction: Both
# 0:      deny  udp any port eq 500 any
# 1:      deny  udp any any port eq 500
# 2:      permit ip 10.10.100.231 255.255.255.255 10.10.100.232 255.255.255.255
# 63:     deny  ip any any

sw10.1.1.100# show crypto ike domain ipsec
keepalive 3600

sw10.1.1.100# show crypto ike domain ipsec key
key ctct address 10.10.100.232

sw10.1.1.100# show crypto ike domain ipsec policy
Priority 1, auth pre-shared, lifetime 86300 secs, encryption 3des, hash md5, DH group 1
```

ステップ9 スイッチ MDS C で IKE および IPsec をイネーブルにします。

```
sw11.1.1.100# configure terminal
sw11.1.1.100(config)# feature crypto ike
sw11.1.1.100(config)# feature crypto ipsec
```

ステップ10 スイッチ MDS C に IKE を設定します。

```
sw11.1.1.100(config)# crypto ike domain ipsec
sw11.1.1.100(config-ike-ipsec)# key ctct address 10.10.100.231
sw11.1.1.100(config-ike-ipsec)# policy 1
sw11.1.1.100(config-ike-ipsec-policy)# encryption 3des
sw11.1.1.100(config-ike-ipsec-policy)# hash md5
sw11.1.1.100(config-ike-ipsec-policy)# exit
sw11.1.1.100(config-ike-ipsec)# end
sw11.1.1.100#
```

ステップ 11 スイッチ MDS C に ACL を設定します。

```
sw11.1.1.100# configure terminal
sw11.1.1.100(config)# ip access-list acl1 permit ip 10.10.100.232 0.0.0.0 10.10.100.231
0.0.0.0
```

ステップ 12 スイッチ MDS C にトランスフォームセットを設定します。

```
sw11.1.1.100(config)# crypto transform-set domain ipsec tfs-02 esp-aes 128
esp-sha1-hmac
```

ステップ 13 スイッチ MDS C に暗号マップを設定します。

```
sw11.1.1.100(config)# crypto map domain ipsec cmap-01 1
sw11.1.1.100(config-crypto-map-ip)# match address acl1
sw11.1.1.100(config-crypto-map-ip)# set peer 10.10.100.231
sw11.1.1.100(config-crypto-map-ip)# set transform-set tfs-02
sw11.1.1.100(config-crypto-map-ip)# set security-association lifetime seconds 3600
sw11.1.1.100(config-crypto-map-ip)# set security-association lifetime gigabytes 3000
sw11.1.1.100(config-crypto-map-ip)# set pfs group5
sw11.1.1.100(config-crypto-map-ip)# exit
sw11.1.1.100(config)#
```

ステップ 14 スイッチ MDS C のクリプトマップセットにインターフェイスをバインドします。

```
sw11.1.1.100(config)# int gigabitethernet 1/2
sw11.1.1.100(config-if)# ip addr 10.10.100.232 255.255.255.0
sw11.1.1.100(config-if)# crypto map domain ipsec cmap-01
sw11.1.1.100(config-if)# no shut
sw11.1.1.100(config-if)# exit
sw11.1.1.100(config)#
```

ステップ 15 スイッチ MDS C の FCIP を設定します。

```
sw11.1.1.100(config)# feature fcip
sw11.1.1.100(config)# fcip profile 2
sw11.1.1.100(config-profile)# ip address 10.10.100.232
sw11.1.1.100(config-profile)# int fcip 2
sw11.1.1.100(config-if)# peer-info ipaddr 10.10.100.231
sw11.1.1.100(config-if)# use-profile 2
sw11.1.1.100(config-if)# no shut
sw11.1.1.100(config-if)# exit
sw11.1.1.100(config)# exit
```

ステップ 16 スイッチ MDS C の設定を確認します。

```
sw11.1.1.100# show crypto global domain ipsec security-association lifetime
Security Association Lifetime: 4500 megabytes/3600 seconds

sw11.1.1.100# show crypto map domain ipsec
Crypto Map "cmap-01" 1 ipsec
  Peer = 10.10.100.231
  IP ACL = acl1
    permit ip 10.10.100.232 255.255.255.255 10.10.100.231 255.255.255.255
```

```

    Transform-sets: tfs-02,
    Security Association Lifetime: 3000 gigabytes/3600 seconds
    PFS (Y/N): Y
    PFS Group: group5
Interface using crypto map set cmap-01:
    GigabitEthernet1/2

sw11.1.1.100# show crypto spd domain ipsec
Policy Database for interface: GigabitEthernet1/2, direction: Both
# 0:    deny  udp any port eq 500 any
# 1:    deny  udp any any port eq 500
# 2:    permit ip 10.10.100.232 255.255.255.255 10.10.100.231 255.255.255.255
# 63:   deny  ip any any

sw11.1.1.100# show crypto sad domain ipsec
interface: GigabitEthernet1/2
Crypto map tag: cmap-01, local addr. 10.10.100.232
protected network:
local ident (addr/mask): (10.10.100.232/255.255.255.255)
remote ident (addr/mask): (10.10.100.231/255.255.255.255)
current_peer: 10.10.100.231
  local crypto endpt.: 10.10.100.232, remote crypto endpt.: 10.10.100.231
  mode: tunnel, crypto algo: esp-3des, auth algo: esp-md5-hmac
  current outbound spi: 0x38f96001 (955867137), index: 29
  lifetimes in seconds:: 3600
  lifetimes in bytes:: 3221225472000
  current inbound spi: 0x900b011 (151040017), index: 16
  lifetimes in seconds:: 3600
  lifetimes in bytes:: 3221225472000

sw11.1.1.100# show crypto transform-set domain ipsec
Transform set: tfs-02 {esp-aes 128 esp-sha1-hmac}
  will negotiate {tunnel}

sw11.1.1.100# show crypto ike domain ipsec
keepalive 3600

sw11.1.1.100# show crypto ike domain ipsec key
key ctct address 10.10.100.231

sw11.1.1.100# show crypto ike domain ipsec policy
Priority 1, auth pre-shared, lifetime 86300 secs, encryption 3des, hash md5, DH
group 1

sw11.1.1.100# show crypto ike domain ipsec sa
Tunn    Local Addr          Remote Addr          Encr    Hash    Auth Method    Lifetime
-----
1*      10.10.100.232[500]  10.10.100.231[500]  3des   md5     preshared key   86300
-----
NOTE: tunnel id ended with * indicates an IKEv1 tunnel

```

ステップ 17 スイッチ MDS A の設定を確認します。

```

sw10.1.1.100# show crypto sad domain ipsec
interface: GigabitEthernet7/1
Crypto map tag: cmap-01, local addr. 10.10.100.231
protected network:
local ident (addr/mask): (10.10.100.231/255.255.255.255)
remote ident (addr/mask): (10.10.100.232/255.255.255.255)
current_peer: 10.10.100.232
  local crypto endpt.: 10.10.100.231, remote crypto endpt.: 10.10.100.232
  mode: tunnel, crypto algo: esp-3des, auth algo: esp-md5-hmac
  current outbound spi: 0x900b01e (151040030), index: 10
  lifetimes in seconds:: 3600

```



```

lifetimes in bytes:: 3221225472000
current inbound spi: 0x38fe700e (956198926), index: 13
lifetimes in seconds:: 3600
lifetimes in bytes:: 3221225472000

```

```

sw10.1.1.100# show crypto ike domain ipsec sa
Tunn Local Addr          Remote Addr          Encr Hash Auth Method Lifetime
-----
  1 10.10.100.231[500] 10.10.100.232[500] 3des md5  preshared key   86300

```

これで、スイッチ MDS A および MDS C の両方に IPsec を設定しました。

iSCSI の設定例

Figure 18: iSCSI のエンドツーエンド Ipsec, on page 259 では、サブネット 12.12.1/24 のホストと MDS A の間の iSCSI セッションに注目しています。auto-peer オプションを使用して、サブネット 12.12.1.0/24 からのホストが、MDS スイッチのギガビットイーサネットポート 7/1 へ接続しようとしたときに、ホストと MDS の間に SA が作成されます。auto-peer を使用して、1 つの暗号マップだけが、同じサブネット内のすべてのホストの SA を作成するために必要です。auto-peer がないと、ホストごとに 1 つの暗号マップが必要です。

Figure 18: iSCSI のエンドツーエンド Ipsec

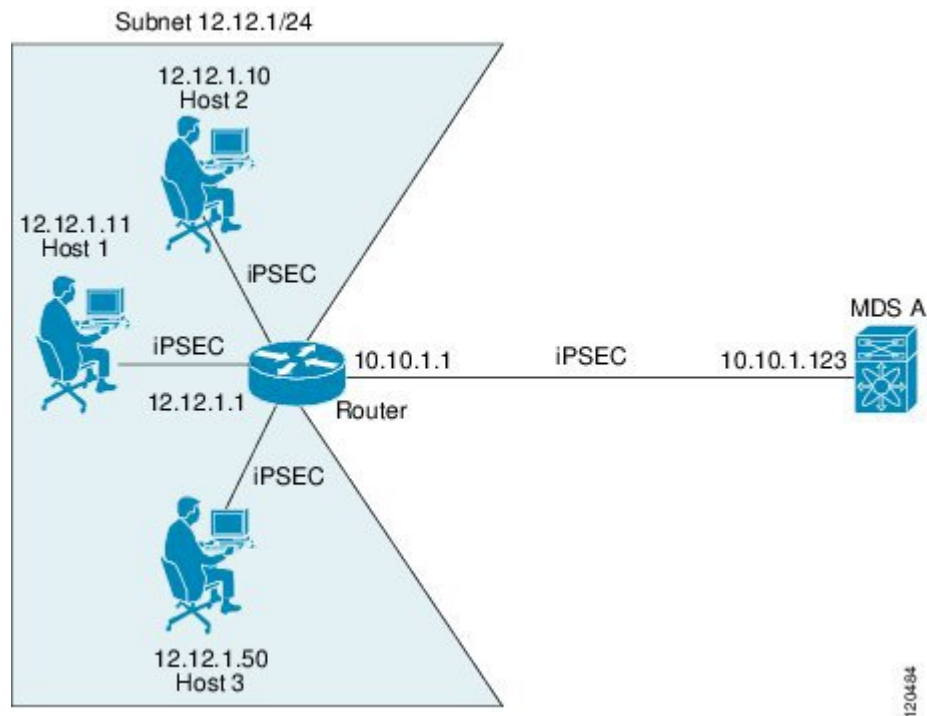


Figure 18: iSCSI のエンドツーエンド Ipsec, on page 259 に示す iSCSI シナリオで IPsec を設定するには、次の手順を実行します。

Procedure

ステップ 1 スイッチ MDS A に ACL を設定します。

```
sw10.1.1.100# configure terminal
sw10.1.1.100(config)# ip access-list acl1 permit tcp 10.10.1.0 0.0.0.255 range port 3260
3260 12.12.1.0 0.0.0.255
```

ステップ 2 スイッチ MDS A にトランスフォームセットを設定します。

```
sw10.1.1.100(config)# crypto transform-set domain ipsec tfs-01 esp-3des esp-md5-hmac
```

ステップ 3 スイッチ MDS A に暗号マップを設定します。

```
sw10.1.1.100(config)# crypto map domain ipsec cmap-01 1
sw10.1.1.100(config-crypto-map-ip)# match address acl1
sw10.1.1.100(config-crypto-map-ip)# set peer auto-peer
sw10.1.1.100(config-crypto-map-ip)# set transform-set tfs-01
sw10.1.1.100(config-crypto-map-ip)# end
sw10.1.1.100#
```

ステップ 4 スイッチ MDS A の暗号マップセットにインターフェイスをバインドします。

```
sw10.1.1.100# configure terminal
sw10.1.1.100(config)# int gigabitethernet 7/1
sw10.1.1.100(config-if)# ip address 10.10.1.123 255.255.255.0
sw10.1.1.100(config-if)# crypto map domain ipsec cmap-01
sw10.1.1.100(config-if)# no shut
sw10.1.1.100(config-if)# end
sw10.1.1.100#
```

Cisco MDS IPsec および iSCSI 機能を使用して、MDS A に IPsec を設定しました。

デフォルト設定

次の表に、IKE パラメータのデフォルト設定を示します。

Table 16: IKE パラメータのデフォルト値

パラメータ	デフォルト
IKE	ディセーブル
IKE バージョン	IKE version 2
IKE 暗号化アルゴリズム	3DES
IKE ハッシュ アルゴリズム	SHA
IKE 認証方式	設定不可 (事前共有事前共有キーを使用)
IKE DH グループ識別名	グループ 1

パラメータ	デフォルト
IKE ライフタイム アソシエーション	86400 秒 (24 時間)。
各ピアの IKE キープアライブ タイム (v2)	3600 秒 (1 時間)。

次の表は、IPsec パラメータのデフォルト設定をまとめたものです。

Table 17: IPsec パラメータのデフォルト値

パラメータ	デフォルト
IPsec	ディセーブル
トラフィックへの IPsec の適用	拒否 (deny) : クリアテキストを許可
IPsec PFS	ディセーブル
IPsec グローバル ライフタイム (トラフィック量)	450 GB
IPsec グローバル ライフタイム (タイム)	3,600 秒 (1 時間)



第 10 章

FC-SP および DHCHAP の設定

\

この章は、次の項で構成されています。

- [ファブリック認証の概要, on page 263](#)
- [DHCHAP, on page 264](#)
- [設定例, on page 275](#)
- [デフォルト設定, on page 276](#)

ファブリック認証の概要

Fibre Channel Security Protocol (FC-SP) 機能は、スイッチ間およびホストとスイッチ間で認証を実行して、企業全体のファブリックに関するセキュリティ問題を解決します。Diffie-Hellman (DH) Challenge Handshake Authentication Protocol (DHCHAP) は、Cisco MDS 9000 ファミリースイッチとその他のデバイス間で認証を行う FC-SP プロトコルです。DHCHAP は、CHAP プロトコルと Diffie-Hellman 交換を組み合わせで構成されています。



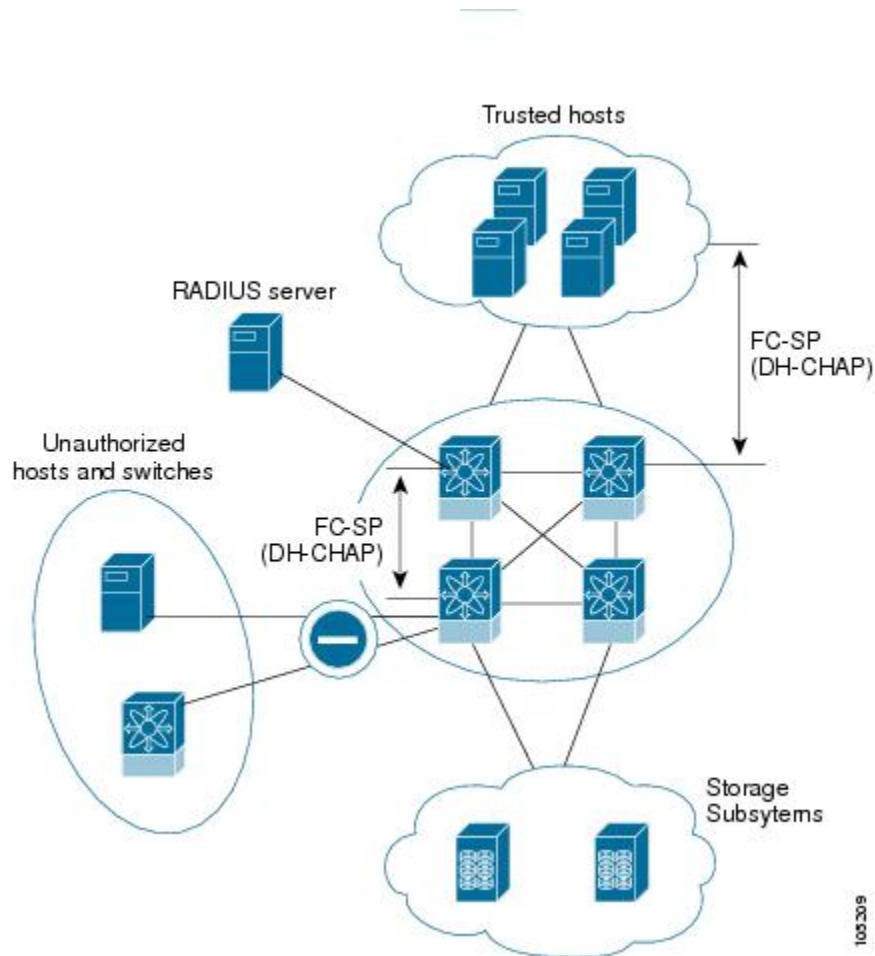
Note Cisco NX-OS リリース 6.2(1) は Cisco MDS 9710 のみでファイバチャネルセキュリティプロトコル (FC-SP) 機能をサポートしていません。Cisco MDS 9710 での FC-SP のサポートは、Cisco NX-OS リリース 6.2(9) 以降です。

VFC ポートを介して認証するには、FC-SP が通信にポート VSAN を使用する必要があります。したがって、認証メッセージを送受信するには、両方のピアでポート VSAN が同じで、かつアクティブになっている必要があります。

Cisco MDS 9000 ファミリースイッチはすべて、スイッチ間またはスイッチとホスト間の認証をファブリック全体で実行できます。これらのスイッチおよびホスト認証は、各ファブリックでローカルまたはリモートで実行できます。ストレージアイランドを企業全体のファブリックに統合して、移行すると、新しいセキュリティ問題が発生します。ストレージアイランドを保護する方法が、企業全体のファブリックで必ずしも保証されなくなります。

たとえば、スイッチが地理的に分散しているキャンパス環境では、他のユーザーが故意に、またはユーザー自身が偶然に、互換性のないスイッチに故意に相互接続することにより、スイッチ間リンク（ISL）分離やリンク切断が発生することがあります。Cisco MDS 9000 ファミリースイッチでは、物理セキュリティに対するこのようなニーズに対応しています（[Figure 19: スイッチおよびホストの認証](#), on page 264 を参照）。

Figure 19: スイッチおよびホストの認証



Note ホスト スイッチ認証には、適切なファームウェアおよびドライバを備えたファイバチャネル（FC）Host Bus Adapter（HBA）が必要です。

DHCHAP

DHCHAPは、スイッチに接続しているデバイスを認証する認証プロトコルです。ファイバチャネル認証を使用すると、信頼できるデバイスだけをファブリックに追加できるので、不正なデバイスのスイッチへのアクセスを防止できます。



Note この章では、FC-SP および DHCHAP という用語を共通の意味で使用しています。

DHCHAP は、必須のパスワードに基づくキー交換による認証プロトコルであり、スイッチ間およびホストスイッチ間の認証をサポートします。DHCHAP はハッシュ アルゴリズムおよび DH グループをネゴシエートしてから、認証を実行します。また、MD5 および SHA-1 アルゴリズムベース認証をサポートします。

DHCHAP 機能の設定には、ENTERPRISE_PKG ライセンスが必要です（『Cisco MDS 9000 Family NX-OS Licensing Guide』を参照）。

ローカルパスワードデータベースを使用して DHCHAP 認証を設定する手順は、次のとおりです。

Procedure

- ステップ 1 DHCHAP をイネーブルにします。
- ステップ 2 DHCHAP 認証モードを識別して設定します。
- ステップ 3 ハッシュ アルゴリズムおよび DH グループを設定します。
- ステップ 4 ローカルスイッチおよびファブリックの他のスイッチの DHCHAP パスワードを設定します。
- ステップ 5 再認証の DHCHAP タイムアウト値を設定します。
- ステップ 6 DHCHAP の設定を確認します。

Example

このセクションは、次のトピックで構成されています。

既存の Cisco MDS 機能との DHCHAP の互換性

ここでは、DHCHAP 機能および既存の Cisco MDS 機能の設定の影響について説明します。

- ポートチャネルインターフェイス：ポートチャネルに属しているポートに対して DHCHAP がイネーブルの場合、DHCHAP 認証はポートチャネル レベルでなく、物理インターフェイス レベルで実行されます。
- FCIP インターフェイス：DHCHAP プロトコルは、物理インターフェイスの場合と同様に、FCIP インターフェイスと連携します。
- ポートセキュリティまたはファブリック バインディング：ファブリック バインディング ポリシーは、DHCHAP によって認証される ID に基づいて実行されます。
- VSAN：DHCHAP 認証は、VSAN 単位では実行されません。
- ハイ アベイラビリティ：DHCHAP 認証は既存の HA 機能とトランスペアレントに連携します。

DHCHAP イネーブル化の概要

デフォルトでは、Cisco MDS 9000 ファミリの全スイッチで DHCHAP 機能はディセーブルに設定されています。

ファブリック認証用のコンフィギュレーションコマンドおよび確認コマンドにアクセスするには、DHCHAP 機能をイネーブルにする必要があります。この機能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。

DHCHAP のイネーブル化

Cisco MDS スwitchの DHCHAP をイネーブルにする手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **feature fcsp**

このスイッチ上で DHCHAP をイネーブルにします。

ステップ 3 switch(config)# **no feature fcsp**

このスイッチ上で DHCHAP をディセーブル（デフォルト）にします。

DHCHAP 認証モードの概要

各インターフェイスの DHCHAP 認証ステータスは、DHCHAP ポートモードの設定によって変化します。

スイッチ内で DHCHAP 機能がイネーブルの場合には、各ファイバチャネルインターフェイスまたは FCIP インターフェイスを次の 4 つの DHCHAP ポートモードのいずれかに設定できます。

- **On** : 接続元デバイスが DHCHAP 認証をサポートしている場合、スイッチ初期化中に認証シーケンスが実行されます。接続元デバイスが DHCHAP 認証をサポートしていない場合には、リンクが分離状態になります。
- **auto-Active** : 接続元デバイスが DHCHAP 認証をサポートしている場合、スイッチ初期化中に認証シーケンスが実行されます。接続元デバイスが DHCHAP 認証をサポートしていない場合には、ソフトウェアにより、初期化シーケンスの残りが実行されます。
- **auto-Passive** (デフォルト) : スイッチは DHCHAP 認証を開始しませんが、接続元デバイスが DHCHAP 認証を開始すれば、DHCHAP 認証に参加します。

- **Off** : スイッチはDHCHAP 認証をサポートしません。このようなポートに認証メッセージが送信された場合、開始元スイッチにエラーメッセージが戻されます。



Note DHCHAP ポートモードを off モード以外のモードに変更すると、再認証が実行されます。VE リンクの DHCHAP ポートモードの変更には、両端のポートフラップが必要です。

次の表で、さまざまなモードに設定した2台のシスコスイッチ間での認証動作について説明します。

Table 18: 2台の MDS スイッチ間の DHCHAP 認証ステータス

スイッチ N の DHCHAP モード	スイッチ 1 の DHCHAP モード			
	on	auto-active	auto-passive	off
on	FC-SP 認証が実行されます。	FC-SP 認証が実行されます。	FC-SP 認証が実行されます。	リンクがダウンになります。
auto-active			FC-SP 認証は実行されません。	
auto-passive				
off	リンクがダウンになります。	FC-SP 認証は実行されません。		

DHCHAP モードの設定

特定のインターフェイスに DHCHAP モードを設定する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **interface fc2/1-3**

switch(config-if)#

インターフェイスの範囲を選択し、インターフェイス コンフィギュレーションサブモードを開始します。

ステップ 3 switch(config-if)# **fcsp on**

選択したインターフェイスの DHCHAP モードを on ステートに設定します。

ステップ 4 switch(config-if)# no fcsp on

(オプション) これら3つのインターフェイスを出荷時デフォルトの auto-passive に戻します。

ステップ 5 switch(config-if)# fcsp auto-active 0

選択したインターフェイスの DHCHAP 認証モードを auto-active に変更します。0 は、ポートが再認証を実行しないことを表します。

ステップ 6 switch(config-if)# fcsp auto-active 120

DHCHAP 認証モードを選択したインターフェイスの auto-active に変更し、最初の認証後に再認証を2時間 (120 分) ごとにイネーブルにします。

ステップ 7 switch(config-if)# fcsp auto-active

選択したインターフェイスの DHCHAP 認証モードを auto-active に変更します。再認証はディセーブルになります (デフォルト)。

DHCHAP ハッシュ アルゴリズムの概要

Cisco MDS スイッチは、DHCHAP 認証用のデフォルトハッシュ アルゴリズム プライオリティ リスト (MD5 のあとに SHA-1) をサポートしています。



Tip ハッシュ アルゴリズムの設定を変更する場合は、ファブリック上の全スイッチに対して設定をグローバルに変更してください。



Caution fcsp dhchap 用の AAA 認証を有効にすると、AAA 認証に RADIUS または TACACS+ を使用する場合は、MD5 ハッシュ アルゴリズムを設定する必要があります。これは、RADIUS および TACACS+ のアプリケーションが他のハッシュ アルゴリズムをサポートしていないためです。

DHCHAP ハッシュ アルゴリズムの設定

ハッシュ アルゴリズムを設定する手順は、次のとおりです。

Procedure

ステップ 1 switch# configure terminal

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# fcsp dhchap hash sha1

SHA-1 ハッシュ アルゴリズムだけを使用するように設定します。

ステップ 3 switch(config)# **fcsp dhchap hash MD5**

MD5 ハッシュ アルゴリズムだけを使用するように設定します。

ステップ 4 switch(config)# **fcsp dhchap hash md5 sha1**

DHCHAP 認証に対して、MD5 ハッシュ アルゴリズムを使用してから SHA-1 を使用するデフォルトのプライオリティ リストを定義します。

ステップ 5 switch(config)# **no fcsp dhchap hash sha1**

デフォルトのハッシュ アルゴリズム プライオリティ リスト（最初に MD5、次に SHA-1）に戻します。

DHCHAP グループ設定の概要

FC-SP では、複数の DHCHAP グループがサポートされています。使用できるグループは、デフォルトリストから変更される可能性があります。リストは、優先順位の最も高いものから低いものへの順序で FC-SP ピアとネゴシエートするときに使用されるように設定されています。どちらの側も、受信したグループのリストとローカルグループのリストを比較し、優先度の最も高いグループが使用されます。各グループは設定コマンドで一度しか指定できません。

グループに関する詳細については、『*Cisco MDS 9000 Series NX-OS Command Reference Guide*』の **fcsp dhchap dhgroup** コマンドを参照してください。



Tip DH グループの設定を変更する場合は、ファブリック内のすべてのスイッチの設定をグローバルに変更してください。

DHCHAP グループの設定

DH グループ設定を変更する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **fcsp dhchap dhgroup 2 3 4**

DH グループ リストを使用するように指定します。リストは降順の優先度の順に指定されます。指定されないグループは DHCHAP により使用から除外されます。

ステップ 3 switch(config)# no fensp dhchap dhgroup 2 3 4

(オプション) DHCHAP のデフォルトの順番に戻ります。

DHCHAP パスワードの概要

DHCHAP 認証を実行する方向ごとに、接続デバイス間の共有シークレットパスワードが必要です。このパスワードを使用するには、DHCHAPに参加するファブリック上のすべてのスイッチで、次の3つの方法のいずれかを使用してパスワードを管理します。

- 方法1：ファブリック上のすべてのスイッチに同じパスワードを使用します。これは最も簡単な方法です。新しいスイッチを追加する場合、このファブリック内では同じパスワードを使用してそのスイッチを認証します。したがって、ファブリック内のいずれかのスイッチに外部から不正アクセスを試みる場合、これは最も脆弱な方法です。
- 方法2：ファブリック上のスイッチごとに異なるパスワードを使用して、このパスワードリストを維持します。新しいスイッチを追加する場合は、新規パスワードリストを作成して、この新規リストを使用してすべてのスイッチを更新します。いずれかのスイッチにアクセスすると、このファブリック上のすべてのスイッチに関するパスワードリストが生成されます。
- 方法3：ファブリック上のスイッチごとに異なるパスワードを使用します。新しいスイッチを追加する場合は、ファブリック内の各スイッチに対応する複数の新規パスワードを生成して、各スイッチに設定する必要があります。いずれかのスイッチが被害にあっても、他のスイッチのパスワードは引き続き保護されます。この方法では、ユーザー側で大量のパスワードメンテナンス作業が必要になります。



Note パスワードはすべて 64 文字以内の英数字に制限されます。パスワードは変更できますが、削除はできません。



Tip スイッチが 6 台以上のファブリックでは、RADIUS または TACACS+ の使用をお勧めします。ローカルパスワードデータベースを使用する必要がある場合には、方法 3 を使用し、Cisco MDS 9000 ファミリー Fabric Manager を使用して、パスワードデータベースを管理します。

ローカルスイッチの DHCHAP パスワードの設定

ローカルスイッチに DHCHAP パスワードを設定する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **fensp dhchap password 0 mypassword**

ローカル スイッチのクリアテキスト パスワードを設定します。

ステップ 3 switch(config)# **fensp dhchap password 0 mypassword 30:11:bb:cc:dd:33:11:22**

指定 WWN のデバイスで使用する、ローカル スイッチのクリア テキスト パスワードを設定します。

ステップ 4 switch(config)# **no fensp dhchap password 0 mypassword 30:11:bb:cc:dd:33:11:22**

(オプション) 指定 WWN のデバイスで使用する、ローカル スイッチのクリア テキスト パスワードを削除します。

ステップ 5 switch(config)# **fensp dhchap password 7 sfsfdf**

ローカル スイッチに対して暗号化フォーマットで入力されるパスワードを設定します。

ステップ 6 switch(config)# **fensp dhchap password 7 sfsfdf 29:11:bb:cc:dd:33:11:22**

指定 WWN のデバイスで使用する、ローカル スイッチに対して暗号化フォーマットで入力されるパスワードを設定します。

ステップ 7 switch(config)# **no fensp dhchap password 7 sfsfdf 29:11:bb:cc:dd:33:11:22**

(オプション) 指定 WWN のデバイスで使用する、ローカル スイッチに対して暗号化フォーマットで入力されるパスワードを削除します。

ステップ 8 switch(config)# **fensp dhchap password mypassword1**

接続するデバイスで使用する、ローカルスイッチのクリアテキストパスワードを設定します。

リモート デバイスのパスワード設定の概要

ファブリック内の他のデバイスのパスワードを、ローカル認証データベースに設定できます。他のデバイスは、スイッチ WWN やデバイス WWN といったデバイス名で表されます。パスワードは 64 文字に制限され、クリア テキスト (0) または暗号化テキスト (7) で指定できます。



Note スイッチ WWN は、物理スイッチを識別します。この WWN はスイッチの認証に使用されます。また、VSAN ノード WWN とは異なります。

リモート デバイスの DHCHAP パスワードの設定

ファブリック内の別のスイッチのリモート DHCHAP パスワードをローカルで設定する手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **fcsp dhchap devicename 00:11:22:33:44:aa:bb:cc password NewPassword**

スイッチ WWN デバイス名で表される、ファブリック上の他のスイッチのパスワードを設定します。

ステップ 3 switch(config)# **no fcsp dhchap devicename 00:11:22:33:44:aa:bb:cc password NewPassword**

(オプション) ローカル認証データベースから、このスイッチのパスワードエントリを削除します。

ステップ 4 switch(config)# **fcsp dhchap devicename 00:11:55:66:00:aa:bb:cc password 0 NewPassword**

スイッチ WWN デバイス名で表される、ファブリック上の他のスイッチのクリアテキストパスワードを設定します。

ステップ 5 switch(config)# **fcsp dhchap devicename 00:11:22:33:55:aa:bb:cc password 7 asdfkjh**

スイッチ WWN デバイス名で表される、ファブリック内の他のスイッチの暗号化形式で入力されるパスワードを設定します。

DHCHAP タイムアウト値の概要

DHCHAP プロトコルの交換中に、MDS スイッチが待機中の DHCHAP メッセージを指定インターバル内に受信しなかった場合、認証は失敗したと見なされます。この（認証が失敗したと見なされるまでの）時間は、20 ~ 1000 秒の範囲で設定できます。デフォルトは 30 秒です。

タイムアウト値を変更する場合には、次の要因について考慮してください。

- 既存の RADIUS および TACACS+ タイムアウト値。
- ファブリック内のすべてのスイッチに同じ値を設定する必要もあります。

DHCHAP タイムアウト値の設定

DHCHAP タイムアウト値を構成する手順は、次のとおりです。

Procedure

- ステップ 1** switch# **configure terminal**
コンフィギュレーション モードに入ります。
- ステップ 2** switch(config)# **fcsp timeout 60**
再認証タイムアウトを 60 秒に設定します。
- ステップ 3** switch(config)# **no fcsp timeout 60**
(オプション) 出荷時デフォルトの 30 秒に戻します。
-

DHCHAP AAA 認証の設定

認証オプションは個別に設定できます。認証を設定しない場合、デフォルトでローカル認証が使用されます。

AAA 認証を設定するには、次の手順を実行します。

Procedure

- ステップ 1** switch# **configure terminal**
コンフィギュレーション モードに入ります。
- ステップ 2** switch(config)# **aaa authentication dhchap default group TacacsServer1**
認証に TACACS+ サーバー グループ (この例では、TacacsServer1) を使用する DHCHAP をイネーブルにします。
- ステップ 3** switch(config)# **aaa authentication dhchap default local**
ローカル認証用の DHCHAP をイネーブルにします。
- ステップ 4** switch(config)# **aaa authentication dhchap default group RadiusServer1**
認証に RADIUS サーバー グループ (この例では、RadiusServer1) を使用する DHCHAP をイネーブルにします。
-

プロトコル セキュリティ情報の表示

ローカルデータベースの設定を表示するには、**show fcsp** コマンドを使用します (次の例を参照)。

FC インターフェイスの DHCHAP 設定の表示

```
switch# show fcsp interface fc1/9

fc1/9:
  fcsp authentication mode:SEC_MODE_ON
  Status: Successfully authenticated
```

FC インターフェイスの DHCHAP 統計情報の表示

```
switch# show fcsp interface fc1/9 statistics

fc1/9:
  fcsp authentication mode:SEC_MODE_ON
  Status: Successfully authenticated
  Statistics:
  FC-SP Authentication Succeeded:5
  FC-SP Authentication Failed:0
  FC-SP Authentication Bypassed:0
```

指定されたインターフェイスを介して接続されたデバイスの FC-SP WWN の表示

```
switch# show fcsp interface fc 2/1 wwn

fc2/1:
  fcsp authentication mode:SEC_MODE_ON
  Status: Successfully authenticated
  Other device's WWN:20:00:00:e0:8b:0a:5d:e7
```

ハッシュ アルゴリズムとローカル スイッチ用に設定された DHCHAP グループの表示

```
switch# show fcsp dhchap

Supported Hash algorithms (in order of preference):
DHCHAP_HASH_MD5
DHCHAP_HASH_SHA_1
Supported Diffie Hellman group ids (in order of preference):
DHCHAP_GROUP_NULL
DHCHAP_GROUP_1536
DHCHAP_GROUP_1024
DHCHAP_GROUP_1280
DHCHAP_GROUP_2048
```

DHCHAP ローカルパスワード データベースの表示

```
switch# show fcsp dhchap database

DHCHAP Local Password:
  Non-device specific password:*****
  Password for device with WWN:29:11:bb:cc:dd:33:11:22 is *****
  Password for device with WWN:30:11:bb:cc:dd:33:11:22 is *****
Other Devices' Passwords:
  Password for device with WWN:00:11:22:33:44:aa:bb:cc is *****
```

デバイス WWN の ASCII 表記の表示

```
switch# show fcsp asciiwwn 30:11:bb:cc:dd:33:11:22

Ascii representation of WWN to be used with AAA servers:Ox_3011bbccdd331122
```

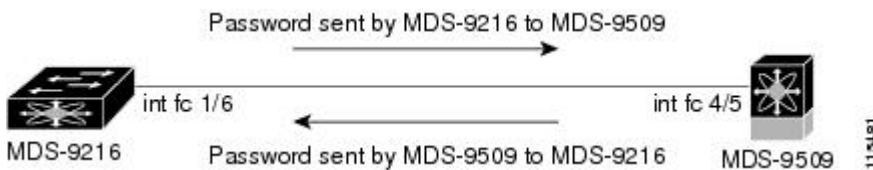



Tip RADIUS サーバーおよび TACACS+ サーバーにスイッチ情報を設定する場合、デバイス WWN の ASCII 表記（太字で表記）を使用してください。

設定例

ここでは、[Figure 20: DHCHAP 認証の例, on page 275](#) に示した例を設定する手順を示します。

Figure 20: DHCHAP 認証の例



[Figure 20: DHCHAP 認証の例, on page 275](#) に示す認証設定を設定するには、次の手順を実行します。

Procedure

ステップ 1 ファブリック内の MDS9216 スイッチのデバイス名を取得します。ファブリック内の MDS9216 スイッチは、スイッチ WWN によって識別されます。

```
MDS-9216# show wwn switch
Switch WWN is 20:00:00:05:30:00:54:de
```

ステップ 2 このスイッチで DHCHAP を明示的にイネーブルにします。

```
MDS-9216(config)# feature fcsp
```

Note DHCHAP 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 このスイッチのクリア テキスト パスワードを設定します。このパスワードは、接続先デバイスで使用されます。

```
MDS-9216(config)# fcsp dhchap password rtp9216
```

ステップ 4 スイッチ WWN デバイス名で表される、ファブリック上の他のスイッチのパスワードを設定します。

```
MDS-9216(config)# fcsp dhchap devicename 20:00:00:05:30:00:38:5e password rtp9509
```

ステップ 5 目的のファイバチャネルインターフェイスの DHCHAP モードをイネーブルにします。

```
MDS-9216(config)# interface fc 1/16
MDS-9216(config-if)# fcsp on
```

Note DHCHAP ポート モードを off モード以外のモードに変更すると、再認証が実行されます。

ステップ6 DHCHAP ローカルパスワードデータベースを表示して、このスイッチに設定されたプロトコルセキュリティ情報を確認します。

```
MDS-9216# show fcsp dhchap database
DHCHAP Local Password:
    Non-device specific password:*****
Other Devices' Passwords:
    Password for device with WWN:20:00:00:05:30:00:38:5e is *****
```

ステップ7 ファイバチャネルインターフェイスの DHCHAP 設定を表示します。

```
MDS-9216# show fcsp interface fc 1/6
fc1/6
    fcsp authentication mode:SEC_MODE_ON
    Status:Successfully authenticated
```

ステップ8 接続先の MDS 9509 スイッチでこれらの手順を繰り返します。

```
MDS-9509# show wwn switch
Switch WWN is 20:00:00:05:30:00:38:5e

MDS-9509(config)# feature fcsp
MDS-9509(config)# fcsp dhchap password rtp9509
MDS-9509(config)# fcsp dhchap devicename 20:00:00:05:30:00:54:de password rtp9216
MDS-9509(config)# interface fc 4/5
MDS-9509(config-if)# fcsp on
MDS-9509# show fcsp dhchap database

DHCHAP Local Password:
    Non-device specific password:*****
Other Devices' Passwords:
    Password for device with WWN:20:00:00:05:30:00:54:de is *****

MDS-9509# show fcsp interface fc 4/5

Fc4/5
    fcsp authentication mode:SEC_MODE_ON
    Status:Successfully authenticated
```

これで、[Figure 20: DHCHAP 認証の例, on page 275](#) に示す設定例の DHCHAP 認証のイネーブル化と設定の作業が完了します。

デフォルト設定

次の表に、任意のスイッチにおけるすべてのファブリックセキュリティ機能のデフォルト設定を示します。

Table 19: デフォルトのファブリックセキュリティ設定値

パラメータ	デフォルト
DHCHAP 機能	ディセーブル
DHCHAP ハッシュ アルゴリズム	最初に MD5、次に SHA-1 のプライオリティリストで DHCHAP 認証を実行

パラメータ	デフォルト
DHCHAP 認証モード	auto-passive
DHCHAP グループのデフォルトの交換プライオリティ	0、4、1、2、3 の順
DHCHAP タイムアウト値	30 秒



第 11 章

ポートセキュリティの設定

Cisco MDS 9000 シリーズのスイッチにはすべて、侵入の試みを拒否し、管理者に侵入を報告するポートセキュリティ機能があります。



(注) ポートセキュリティは、fc ポートセキュリティとしてファイバチャネルポートと Fibre Channel over Ethernet (FCoE) ポートの両方をサポートします。

この章は、次の項で構成されています。

- [ポートセキュリティの概要, on page 279](#)
- [ポートセキュリティの設定, on page 282](#)
- [ポートセキュリティのイネーブル化, on page 284](#)
- [ポートセキュリティのアクティブ化, on page 284](#)
- [ポートセキュリティのアクティブ化, on page 284](#)
- [自動学習, on page 287](#)
- [ポートセキュリティの手動設定, on page 291](#)
- [ポートセキュリティ設定の配信, on page 293](#)
- [データベース マージの注意事項, on page 297](#)
- [データベースの相互作用, on page 298](#)
- [デフォルト設定, on page 304](#)

ポートセキュリティの概要

Cisco MDS 9000 ファミリのスイッチにはすべて、侵入の試みを拒否し、管理者に侵入を報告するポートセキュリティ機能があります。

通常、SAN 内のすべてのファイバチャネルデバイスを任意の SAN スイッチポートに接続して、ゾーンメンバーシップに基づいて SAN サービスにアクセスできます。ポートセキュリティ機能は、次の方法で、Cisco MDS 9000 ファミリのスイッチポートへの不正アクセスを防止します。

- 不正なファイバチャネルデバイス（Nx ポート）およびスイッチ（xE ポート）からのログイン要求は拒否されます。
- 侵入に関するすべての試みは、システムメッセージを通してSAN管理者に報告されます。
- 設定配信はCFSインフラストラクチャを使用し、CFS対応スイッチに制限されています。配信はデフォルトでディセーブルになっています。
- ポートセキュリティポリシーの設定には、ENTERPRISE_PKG ライセンスが必要です（『Cisco MDS 9000 Family NX-OS Licensing Guide』を参照）。

このセクションは、次のトピックで構成されています。

ポートセキュリティの実行

ポートセキュリティを実行するには、デバイスおよびスイッチポートインターフェイス（これらを通じて各デバイスまたはスイッチが接続される）を設定し、設定をアクティブにします。

- デバイスごとに Nx ポート接続を指定するには、Port World Wide Name (pWWN) または Node World Wide Name (nWWN) を使用します。
- スイッチごとに xE ポート接続を指定するには、Switch World Wide Name (sWWN) を使用します。

Nx および xE ポートをそれぞれ設定して、単一ポートまたはポート範囲に限定することができます。

ポートセキュリティポリシーはポートがアクティブになるたび、およびポートを起動しようとした場合に実行されます。

ポートセキュリティ機能は2つのデータベースを使用して、設定の変更を受け入れ、実装します。

- コンフィギュレーションデータベース：すべての設定の変更がコンフィギュレーションデータベースに保存されます。
- アクティブデータベース：ファブリックが現在実行しているデータベース。ポートセキュリティ機能を実行するには、スイッチに接続されているすべてのデバイスがポートセキュリティアクティブデータベースに格納されている必要があります。ソフトウェアはこのアクティブデータベースを使用して、認証を行います。

自動学習の概要

指定期間内にポートセキュリティ設定を自動的に学習するように、スイッチを設定できます。この機能を使用すると、任意の Cisco MDS 9000 ファミリースイッチで、接続先のデバイスおよびスイッチについて自動的に学習できます。ポートセキュリティ機能を初めてアクティブにするときに、この機能を使用してください。ポートごとに手動で設定する面倒な作業が軽減されます。自動学習は、VSAN 単位で設定する必要があります。この機能をイネーブルにすると、

ポートアクセスを設定していない場合でも、スイッチに接続可能なデバイスおよびスイッチが自動学習されます。

自動学習をイネーブルにすると、学習は、すでにスイッチにログインしているデバイスまたはインターフェイス、およびログインする必要がある新しいデバイスまたはインターフェイスで実行されます。ポートでの学習済みエントリは、自動学習がまだイネーブルな場合、そのポートをシャットダウンした後でクリーンアップされます。

学習は、既存の設定済みのポートセキュリティポリシーを上書きしません。たとえば、インターフェイスが特定の pWWN を許可するように設定されている場合、自動学習によって、そのインターフェイスに他の pWWN を許可する新しいエントリが追加されることはありません。他のすべての pWWN は、自動学習モードであってもブロックされます。

シャットダウン状態のポートについては、学習エントリは作成されません。

ポートセキュリティ機能をアクティブにすると、自動学習も自動的にイネーブルになります。



Note ポートセキュリティ機能をアクティブにすると、自動学習機能はデフォルトで有効になります。自動学習がディセーブルであるか、または非アクティブであり、再度アクティブ化されるまで、ポートセキュリティを再度アクティブ化することはできません。

ポートセキュリティのアクティブ化

デフォルトでは、すべての Cisco MDS 9000 ファミリ スイッチで、ポートセキュリティ機能は非アクティブです。

ポートセキュリティ機能をアクティブにすると、次の処理が適用されます。

- 自動学習も自動的にイネーブルになります。つまり、
 - ここから、自動学習はすでにスイッチにログインしたデバイスまたはインターフェイス、および今後ログインする新しいデバイスに対して発生します。
 - 自動学習をディセーブルにするまで、データベースをアクティブにできません。
- すでにログインしているすべてのデバイスは学習され、アクティブデータベースに追加されます。
- 設定済みデータベースのすべてのエントリがアクティブデータベースにコピーされます。

データベースをアクティブにすると、以降のデバイスのログインは、自動学習されたエントリを除き、アクティブ化されたポートによってバインドされた WWN ペアの対象になります。自動学習されたエントリがアクティブになる前に、自動学習をディセーブルにする必要があります。

ポートセキュリティ機能をアクティブにすると、自動学習も自動的にイネーブルになります。ポートセキュリティ機能をアクティブにし、自動学習をディセーブルにすることもできます。



Tip ポートがログインを拒否されて停止している場合、その後でログインを許可するようにデータベースを設定しても、ポートは自動的に起動しません。そのポートをオンラインに戻すには、`no shutdown CLI` コマンドを明示的に発行する必要があります。

ポートセキュリティの設定

ポートセキュリティを設定する手順は、使用する機能によって異なります。CFS 配信を使用している場合、自動学習の動作が異なります。

このセクションは、次のトピックで構成されています。

自動学習と CFS 配信を使用するポートセキュリティの設定

自動学習およびCFS配信を使用してポートセキュリティを設定する手順は、次のとおりです。

Procedure

- ステップ 1** ポートセキュリティをイネーブルにします。 [ポートセキュリティのイネーブル化, on page 284](#) を参照してください。
- ステップ 2** CFS 配信をイネーブルにします。 [配信のイネーブル化, on page 293](#) を参照してください。
- ステップ 3** 各 VSAN で、ポートセキュリティをアクティブにします。デフォルトで自動学習が有効になります。 [ポートセキュリティのアクティブ化, on page 284](#) を参照してください。
- ステップ 4** CFS コミットを発行して、ファブリック内のすべてのスイッチにこの設定をコピーします。 [変更のコミット, on page 295](#) を参照してください。この時点で、すべてのスイッチがアクティブになり、自動学習が有効になります。
- ステップ 5** すべてのスイッチとすべてのホストが自動的に学習されるまで待ちます。
- ステップ 6** 各 VSAN で、自動学習をディセーブルにします。 [自動学習のディセーブル化, on page 288](#) を参照してください。
- ステップ 7** CFS コミットを発行して、ファブリック内のすべてのスイッチにこの設定をコピーします。 [変更のコミット, on page 295](#) を参照してください。この時点で、すべてのスイッチから自動学習されたエントリが、すべてのスイッチに配信されるスタティックなアクティブデータベースに組み込まれます。
- ステップ 8** 各 VSAN のコンフィギュレーションデータベースにアクティブデータベースをコピーします。 [ポートセキュリティ データベースのコピー, on page 299](#) を参照してください。
- ステップ 9** CFS コミットを発行して、ファブリック内のすべてのスイッチにこの設定をコピーします。 [変更のコミット, on page 295](#) を参照してください。これで、ファブリック内のすべてのスイッチのコンフィギュレーションデータベースが同一になります。
- ステップ 10** ファブリック オプションを使用して、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。これにより、ポートセキュリティ コンフィギュレーション

データベースが、ファブリック内のすべてのスイッチのスタートアップコンフィギュレーションに保存されます。

自動学習を使用し、CFS 配信を使用しないポートセキュリティの設定

自動学習を使用し、CFS 配信を使用しないポートセキュリティを設定する手順は、次のとおりです。

Procedure

- ステップ 1** ポートセキュリティをイネーブルにします。ポートセキュリティのイネーブル化, on page 284 を参照してください。
- ステップ 2** 各 VSAN で、ポートセキュリティをアクティブにします。デフォルトで自動学習が有効になります。ポートセキュリティのアクティブ化, on page 284 を参照してください。
- ステップ 3** すべてのスイッチとすべてのホストが自動的に学習されるまで待ちます。
- ステップ 4** 各 VSAN で、自動学習をディセーブルにします。自動学習のディセーブル化, on page 288 を参照してください。
- ステップ 5** 各 VSAN のコンフィギュレーションデータベースにアクティブデータベースをコピーします。ポートセキュリティデータベースのコピー, on page 299 を参照してください。
- ステップ 6** 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。これにより、ポートセキュリティ コンフィギュレーションデータベースがスタートアップ コンフィギュレーションに保存されます。
- ステップ 7** ファブリック内のすべてのスイッチに対して、ステップ 1～6 を繰り返します。

手動データベース設定によるポートセキュリティの設定

ポートセキュリティを設定し、ポートセキュリティ データベースを手動設定する手順は、次のとおりです。

Procedure

- ステップ 1** ポートセキュリティをイネーブルにします。ポートセキュリティのイネーブル化, on page 284 を参照してください。
- ステップ 2** 各 VSAN のコンフィギュレーションデータベースにすべてのポートセキュリティ エントリを手動で設定します。ポートセキュリティの手動設定, on page 291 を参照してください。
- ステップ 3** 各 VSAN で、ポートセキュリティをアクティブにします。デフォルトで自動学習が有効になります。ポートセキュリティのアクティブ化, on page 284 を参照してください。

- ステップ 4** 各 VSAN で、自動学習をディセーブルにします。自動学習のディセーブル化, on page 288を参照してください。
- ステップ 5** 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。これにより、ポートセキュリティコンフィギュレーションデータベースがスタートアップコンフィギュレーションに保存されます。
- ステップ 6** ファブリック内のすべてのスイッチに対して、ステップ 1～5 を繰り返します。

ポートセキュリティのイネーブル化

デフォルトでは、すべての Cisco MDS 9000 ファミリ スイッチで、ポートセキュリティ機能はディセーブルです。

ポートセキュリティをイネーブルにするには、次の手順を実行します。

Procedure

- ステップ 1** `switch# configure terminal`
コンフィギュレーションモードに入ります。
- ステップ 2** `switch(config)# feature port-security`
スイッチ上でポートセキュリティをイネーブルにします。
- ステップ 3** `switch(config)# no feature port-security`
(オプション) スイッチ上でポートセキュリティをディセーブル (デフォルト) にします。

ポートセキュリティのアクティブ化

このセクションは、次のトピックで構成されています。

ポートセキュリティのアクティブ化

ポートセキュリティ機能をアクティブ化するには、次の手順を実行します。

Procedure

- ステップ 1** `switch# configure terminal`

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# port-security activate vsan 1

指定された VSAN のポートセキュリティ データベースをアクティブにし、自動的に自動学習をイネーブルにします。

ステップ 3 switch(config)# port-security activate vsan 1 no-auto-learn

指定された VSAN のポートセキュリティデータベースをアクティブにし、自動学習をディセーブルにします。

ステップ 4 switch(config)# no port-security activate vsan 1

(オプション) 指定された VSAN のポートセキュリティデータベースを無効にし、自動的に自動学習をディセーブルにします。

Example



Note 必要に応じて、自動学習をディセーブルに設定できます ([自動学習のディセーブル化](#), on [page 288](#)を参照)。

データベースのアクティブ化の拒否

次の場合は、データベースをアクティブ化しようとしても、拒否されます。

- 存在しないエントリや矛盾するエントリがコンフィギュレーション データベースにあるが、アクティブ データベースにはない場合。
- アクティベーションの前に、自動学習機能がイネーブルに設定されていた場合。この状態のデータベースを再アクティブ化するには、自動学習をディセーブルにします。
- 各ポート チャネル メンバーに正確なセキュリティが設定されていない場合。
- 設定済みデータベースが空であり、アクティブ データベースが空でない場合。

上記のような矛盾が1つ以上発生したためにデータベースアクティベーションが拒否された場合は、ポートセキュリティアクティベーションを強制して継続することができます。

ポートセキュリティの強制的なアクティブ化

ポートセキュリティアクティベーション要求が拒否された場合は、アクティベーションを強制できます。



Note **force** オプションを使用してアクティブ化すると、アクティブデータベースに違反している既存のデバイスをログアウトさせることができます。

存在しないエントリや競合するエントリを表示するには、EXECモードで **port-security database diff active vsan** コマンドを使用します。

ポートセキュリティデータベースを強制的にアクティブにするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **port-security activate vsan 1 force**

競合にもかかわらず、VSAN1 ポートセキュリティデータベースを強制的にアクティブ化します。

データベースの再アクティブ化

ポートセキュリティデータベースを再アクティブ化するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **no port-security auto-learn vsan 1**

自動学習をディセーブルにし、スイッチにアクセスする新規デバイスをスイッチが学習しないように設定します。この時点までに学習されたデバイスに基づいて、データベースの内容を処理します。

ステップ 3 switch(config)# **exit**

```
switch# port-security database copy vsan 1
```

アクティブデータベースから設定済みデータベースにコピーします。

ステップ 4 switch# **configure terminal**

```
switch(config)# port-security activate vsan 1
```

指定された VSAN のポートセキュリティ データベースをアクティブにし、自動的に自動学習をイネーブルにします。

Example



Tip 自動学習がイネーブルで、データベースをアクティブ化できない場合、自動学習機能をディセーブルにするまで **force** オプションなしで作業を進めることはできません。

自動学習

ここでは、次の内容について説明します。

自動学習のイネーブル化の概要

自動学習設定の状態は、ポートセキュリティ機能の状態によって異なります。

- ポートセキュリティ機能がアクティブでない場合、自動学習はデフォルトでディセーブルです。
- ポートセキュリティ機能がアクティブである場合、自動学習はデフォルトでイネーブルです（このオプションを明示的にディセーブルにしていない場合）。



Tip VSAN 上で自動学習がイネーブルの場合、**force** オプションを使用して、この VSAN のデータベースだけをアクティブにできます。

自動学習のイネーブル化

自動学習をイネーブルにするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **port-security auto-learn vsan 1**

自動学習をイネーブルにして、VSAN1へのアクセスが許可されたすべてのデバイスについて、スイッチが学習できるようにします。これらのデバイスは、ポートセキュリティアクティブデータベースに記録されます。

自動学習のディセーブル化

自動学習をディセーブルにするには、次の手順を実行します。

Procedure

ステップ1 switch# **configure terminal**

```
switch(config)#
```

コンフィギュレーションモードに入ります。

ステップ2 switch(config)# **no port-security auto-learn vsan 1**

自動学習をディセーブルにし、スイッチにアクセスする新規デバイスをスイッチが学習しないように設定します。この時点までに学習されたデバイスに基づいて、データベースの内容を処理します。

自動学習デバイスの許可

次の表に、デバイス要求に対して接続が許可される条件をまとめます。

Table 20: 許可される自動学習デバイス要求

条件	デバイス (pWWN、nWWN、sWWN)	接続先	許可
1	1つまたは複数のスイッチポートに設定されている場合	設定済みスイッチポート	許可
2		他のすべてのスイッチポート	拒否
3	設定されていない場合	設定されていないスイッチポート	自動学習がイネーブルの場合は許可
4			拒否 (自動学習がディセーブルの場合)
5	設定されている場合、または設定されていない場合	任意のデバイスを接続許可するスイッチポート	許可

条件	デバイス (pWWN、nWWN、sWWN)	接続先	許可
6	任意のスイッチポートにログインするように設定されている場合	スイッチ上の任意のポート	許可
7	設定されていない場合	その他のデバイスが設定されたポート	Denied

許可の例

ポートセキュリティ機能がアクティブで、アクティブ データベースに次の条件が指定されていることが前提です。

- pWWN (P1) には、インターフェイス fc1/1 (F1) からアクセスできる。
- pWWN (P2) には、インターフェイス fc1/1 (F1) からアクセスできる。
- nWWN (N1) には、インターフェイス fc1/2 (F2) からアクセスできる。
- インターフェイス fc1/3 (F3) からは、任意の WWN にアクセスできる。
- nWWN (N3) には、任意のインターフェイスからアクセスできる。
- pWWN (P3) には、インターフェイス fc1/4 (F4) からアクセスできる。
- sWWN (S1) には、インターフェイス fc1/10 ~ 13 (F10 ~ F13) からアクセスできる。
- pWWN (P10) には、インターフェイス fc1/11 (F11) からアクセスできる。

次の表に、このアクティブ データベースに対するポートセキュリティ許可の結果を要約します。リスト内の条件は、許可される自動学習デバイス要求の表に記載されている条件です。

Table 21: 各シナリオの許可結果

デバイス接続要求	許可	条件	理由
P1、N2、F1	許可	1	競合しません。
P2、N2、F1	許可	1	競合しません。
P3、N2、F1	拒否	2	F1 が P1/P2 にバインドされています。
P1、N3、F1	許可	6	N3 に関するワイルドカード一致です。
P1、N1、F3	許可	5	F3 に関するワイルドカード一致です。

デバイス接続要求	許可	条件	理由
P1、N4、F5	拒否	2	P1 が F1 にバインドされています。
P5、N1、F5	拒否	2	N1 は F2 でだけ許可されます。
P3、N3、F4	許可	1	競合しません。
S1、F10	許可	1	競合しません。
S2、F11	拒否	7	P10 が F11 にバインドされています。
P4、N4、F5 (自動学習が有効)	許可	3	競合しません。
P4、N4、F5 (自動学習が無効)	拒否	4	一致しません。
S3、F5 (自動学習が有効)	許可	3	競合しません。
S3、F5 (自動学習が無効)	拒否	4	一致しません。
P1、N1、F6 (自動学習が有効)	拒否	2	P1 が F1 にバインドされています。
P5、N5、F1 (自動学習が有効)	拒否	7	P1 と P2 だけが F1 にバインドされています。
S3、F4 (自動学習が有効)	拒否	7	P3 と F4 がペアになります。
S1、F3 (自動学習が有効)	許可	5	競合しません。
P5、N3、F3	許可	6	F3 および N3 に関するワイルドカード (*) が一致しています。
P7、N3、F9	許可	6	N3 に関するワイルドカード (*) が一致しています。

ポートセキュリティの手動設定

Cisco MDS 9000 ファミリの任意のスイッチにポートセキュリティを設定する手順は、次のとおりです。

Procedure

-
- ステップ 1** 保護する必要があるポートの WWN を識別します。
 - ステップ 2** 許可された nWWN または pWWN に対して fWWN を保護します。
 - ステップ 3** ポートセキュリティ データベースをアクティブにします。
 - ステップ 4** 設定を確認します。
-

Example

このセクションは、次のトピックで構成されています。

WWN の識別の概要

ポートセキュリティを手動で設定する場合は、次の注意事項に従ってください。

- インターフェイスまたは fWWN でスイッチ ポートを識別します。
- pWWN または nWWN でデバイスを識別します。
- Nx ポートが SAN スイッチ ポート Fx にログインできる場合、その Nx ポートは指定された Fx ポートを通じた場合に限りログインできます。
- Nx ポートの nWWN が Fx ポート WWN にバインドされている場合、Nx ポートのすべての pWWN は暗黙的に Fx ポートとペアになります。
- TE ポート チェックは、トランク ポートの許可 VSAN リスト内の VSAN ごとに実行されます。
- 同じポートチャネル内のすべてのポートチャネル xE ポートに、同じ WWN セットを設定する必要があります。
- E ポートのセキュリティは、E ポートのポート VSAN に実装されます。この場合、sWWN を使用して許可チェックを保護します。
- アクティブ化されたコンフィギュレーション データベースは、アクティブ データベースに影響を与えることなく変更できます。
- 実行コンフィギュレーションを保存することにより、コンフィギュレーション データベースおよびアクティブ データベース内のアクティブ化されたエントリを保存します。アクティブ データベース内の学習済みエントリは保存されません。

許可済みのポートペアの追加

許可済みのポートペアをポートセキュリティに追加するには、次の手順を実行します。

Procedure

-
- ステップ 1** switch# **configure terminal**
switch(config)#
コンフィギュレーションモードに入ります。
- ステップ 2** switch(config)# **port-security database vsan 1**
switch(config-port-security)#
指定された VSAN に対してポートセキュリティデータベースモードを開始します。
- ステップ 3** switch(config)# **no port-security database vsan 1**
switch(config)#
(オプション) 指定された VSAN からポートセキュリティコンフィギュレーションデータベースを削除します。
- ステップ 4** switch(config-port-security)# **swwn 20:01:33:11:00:2a:4a:66 interface port-channel 5**
PortChannel 5 を介した場合だけログインするように、指定された sWWN を設定します。
- ステップ 5** switch(config-port-security)# **any-wwn interface fc1/1 - fc1/8**
指定されたインターフェイスを介してログインするようにすべての WWN を設定します。
- ステップ 6** switch(config-port-security)# **pwwn 20:11:00:33:11:00:2a:4a fwwn 20:81:00:44:22:00:4a:9e**
指定された fWWN を介した場合だけログインするように、指定された pWWN を設定します。
- ステップ 7** switch(config-port-security)# **no pwwn 20:11:00:33:11:00:2a:4a fwwn 20:81:00:44:22:00:4a:9e**
(オプション) 前の手順で設定した指定の pWWN を削除します。
- ステップ 8** switch(config-port-security)# **nwwn 26:33:22:00:55:05:3d:4c fwwn 20:81:00:44:22:00:4a:9e**
指定された fWWN を介した場合だけログインするように、指定された nWWN を設定します。
- ステップ 9** switch(config-port-security)# **pwwn 20:11:33:11:00:2a:4a:66**
ファブリック内の任意のポートを介してログインするように、指定された pWWN を設定します。
- ステップ 10** switch(config-port-security)# **pwwn 20:11:33:11:00:2a:4a:66 swwn 20:00:00:0c:85:90:3e:80**
指定されたスイッチ内の任意のインターフェイスを介してログインするように、指定された pWWN を設定します。

ステップ 11 switch(config-port-security)# **pwwn 20:11:33:11:00:2a:4a:66 swwn 20:00:00:0c:85:90:3e:80 interface fc3/1**

指定されたスイッチの指定されたインターフェイスを介してログインするように、指定された pWWN を設定します

ステップ 12 switch(config-port-security)# **any-wwn interface fc3/1**

任意のスイッチの指定されたインターフェイスを介してログインするようにすべての WWN を設定します。

ステップ 13 switch(config-port-security)# **no any-wwn interface fc2/1**

(オプション) 前の手順で設定したワイルドカードを削除します。

Example

バインドする必要がある WWN ペアを識別したら、これらのペアをポートセキュリティ データベースに追加します。



Tip リモートスイッチのバインドは、ローカルスイッチで指定できます。リモートインターフェイスを指定する場合、fWWN または sWWN インターフェイスの組み合わせを使用できます。

ポートセキュリティ設定の配信

ポートセキュリティ機能は Cisco Fabric Services (CFS) インフラストラクチャを使用して効率的なデータベース管理を実現し、VSAN 内のファブリック全体に 1 つの設定を提供します。また、ファブリック全体でポートセキュリティ ポリシーを実行します。

このセクションは、次のトピックで構成されています。

配信のイネーブル化

ポートセキュリティ配信をイネーブルにするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

switch(config)#

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **port-security distribute**

配信をイネーブルにします。

ステップ 3 switch(config)# **no port-security distribute**

(オプション) 配信をディセーブルにします。

Example

たとえば、ポートセキュリティをアクティブにし、自動学習をディセーブルにし、保留状態のデータベースに変更をコミットすると、**port-security activate vsan vsan-id no-auto-learn** コマンドを発行した場合と同じ結果になります。

配信モードで実行されたすべての設定は保留中の（一時的な）データベースに保存されます。設定を変更する場合、設定に対して保留中のデータベースの変更をコミットまたは廃棄する必要があります。その間、ファブリックはロックされた状態になります。保留中のデータベースへの変更は、変更をコミットするまで設定に反映されません。



Note CFS 配信がイネーブルの場合、ポートのアクティベーションまたは非アクティベーションおよび自動学習のイネーブル化またはディセーブル化は、CFS コミットを発行するまで有効になりません。常に CFS コミットとこれらの処理のいずれかを使用して、正しい設定を確認してください。[アクティブ化および自動学習の設定の配信, on page 296](#)を参照してください。



Tip この場合、各処理の最後にコミットを実行することを推奨します。つまり、ポートセキュリティのアクティブ化のあと、および自動学習のイネーブル化のあとです。

ファブリックのロック

既存の設定を変更するときの最初のアクションが実行されると、保留中のデータベースが作成され、VSAN内の機能がロックされます。ファブリックがロックされると、次のような状況になります。

- 他のユーザーがこの機能の設定に変更を加えることができなくなります。
- コンフィギュレーションデータベースのコピーが保留中のデータベースになります。

CFS のロック情報を表示するには、**show cfs lock** コマンドを使用します。詳細については、『Cisco MDS 9000 Family Command Reference』を参照してください。

変更のコミット

設定に加えられた変更をコミットする場合、保留中のデータベースの設定が他のスイッチに配信されます。コミットが正常に行われると、設定の変更がファブリック全体に適用され、ロックが解除されます。

指定された VSAN のポートセキュリティ設定の変更をコミットするには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **port-security commit vsan 3**

指定された VSAN のポートセキュリティの変更をコミットします。

変更の廃棄

保留中のデータベースに加えられた変更を廃棄（終了）する場合、構成は影響を受けないまま、ロックがリリースされます。

CFS のロック情報を表示するには、`show cfs lock` コマンドを使用します。詳細については、『Cisco MDS 9000 Family Command Reference』を参照してください。

指定された VSAN のポートセキュリティ設定の変更を破棄するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **port-security abort vsan 5**

指定された VSAN のポートセキュリティの変更を廃棄し、保留中のコンフィギュレーションデータベースをクリアします。

アクティブ化および自動学習の設定の配信

配信モードのアクティベーション設定および自動学習設定は、保留中のデータベースの変更をコミットするときに実行する処理として記憶されます。

学習済みエントリは一時的なもので、ログインを許可するか否かを決定するロールを持ちません。そのため、学習済みエントリは配信に参加しません。学習をディセーブルにし、保留中のデータベースの変更をコミットする場合、学習済みエントリはアクティブデータベース内のスタティックエントリになり、ファブリック内のすべてのスイッチに配信されます。コミット後は、すべてのスイッチのアクティブデータベースは同一です。

変更をコミットする場合、保留中のデータベースに複数のアクティブ化および自動学習の設定が含まれていると、アクティブ化と自動学習の変更が統合され、処理が変更されることがあります（次の表を参照）。

Table 22: 配信モードでのアクティブ化および自動学習の設定シナリオ

シナリオ	アクション	配信がオフの場合	配信がオンの場合
コンフィギュレーションデータベースに A および B が存在し、アクティベーションが行われておらず、デバイス C および D がログインされています。	1. ポートセキュリティデータベースをアクティブにし、自動学習をイネーブルにします。	コンフィギュレーションデータベース = {A、B} アクティブデータベース = {A、B、C ² 、D*}	コンフィギュレーションデータベース = {A、B} アクティブデータベース = {ヌル} 保留中のデータベース = {A、B+アクティベーション (イネーブル) }
	1. 新規のエントリ E がコンフィギュレーションデータベースに追加されました。	コンフィギュレーションデータベース = {A、B、E} アクティブデータベース = {A、B、C*、D*}	コンフィギュレーションデータベース = {A、B} アクティブデータベース = {ヌル} 保留中のデータベース = {A、B、E+アクティベーション (イネーブル) }
	1. コミットを行います。	N/A	コンフィギュレーションデータベース = {A、B、E} アクティブデータベース = {A、B、E、C*、D*} 保留中のデータベース = 空の状態

シナリオ	アクション	配信がオフの場合	配信がオンの場合
コンフィギュレーションデータベースに A および B が存在し、アクティベーションが行われておらず、デバイス C および D がログインされています。	1. ポートセキュリティデータベースをアクティブにし、自動学習をイネーブルにします。	コンフィギュレーションデータベース = {A、B} アクティブ データベース = {A、B、C*、D*}	コンフィギュレーションデータベース = {A、B} アクティブ データベース = {ヌル} 保留中のデータベース = {A、B+アクティベーション (イネーブル) }
	1. 学習をディセーブルにします。	コンフィギュレーションデータベース = {A、B} アクティブ データベース = {A、B、C、D}	コンフィギュレーションデータベース = {A、B} アクティブ データベース = {ヌル} 保留中のデータベース = {A、B+アクティベーション (イネーブル) + 学習 (ディセーブル) }
	1. コミットを行います。	N/A	コンフィギュレーションデータベース = {A、B} アクティブ データベース = {A、B}、デバイス C および D がログアウトされます。これは、自動学習をディセーブルにした場合のアクティベーションと同じです。 保留中のデータベース = 空の状態

⁷ * (アスタリスク) : 自動学習済みエントリ * (アスタリスク) は学習済みエントリであることを示します。



Tip 各処理の最後にコミットを実行することを推奨します。つまり、ポートセキュリティのアクティブ化の後、および自動学習のイネーブル化の後です。

データベース マージの注意事項

データベースのマージとは、コンフィギュレーションデータベースとアクティブ データベース内のスタティック (学習されていない) エントリの統合を指します。

2つのファブリック間のデータベースをマージする場合は、次のことに気をつけて行ってください。

- アクティベーションステータスと自動学習ステータスが両方のファブリックで同じであることを確認します。
- 両方のデータベースの各 VSAN のコンフィギュレーションの合計数が、2K を超えていないことを確認してください。

**Caution**

この2つの条件に従わない場合は、マージに失敗します。次の配信がデータベースとファブリック内のアクティベーション ステートを強制的に同期化します。

データベースの相互作用

次の表に、アクティブ データベースとコンフィギュレーション データベースの差異および相互作用を示します。

Table 23: アクティブおよびコンフィギュレーション ポートセキュリティ データベース

アクティブ データベース	コンフィギュレーション データベース
読み取り専用。	読み取りと書き込み。
設定を保存すると、アクティブなエントリだけが保存されます。学習済みエントリは保存されません。	設定を保存すると、コンフィギュレーション データベース内のすべてのエントリが保存されます。
アクティブ化すると、VSAN にログイン済みのすべてのデバイスも学習され、アクティブ データベースに追加されます。	アクティブ化されたコンフィギュレーション データベースは、アクティブ データベースに影響を与えることなく変更できます。
アクティブ データベースを設定済みデータベースで上書きするには、ポートセキュリティ データベースをアクティブ化します。強制的にアクティブにすると、アクティブ データベースの設定済みエントリに違反が生じることがあります。	コンフィギュレーション データベースをアクティブ データベースで上書きできます。

**Note**

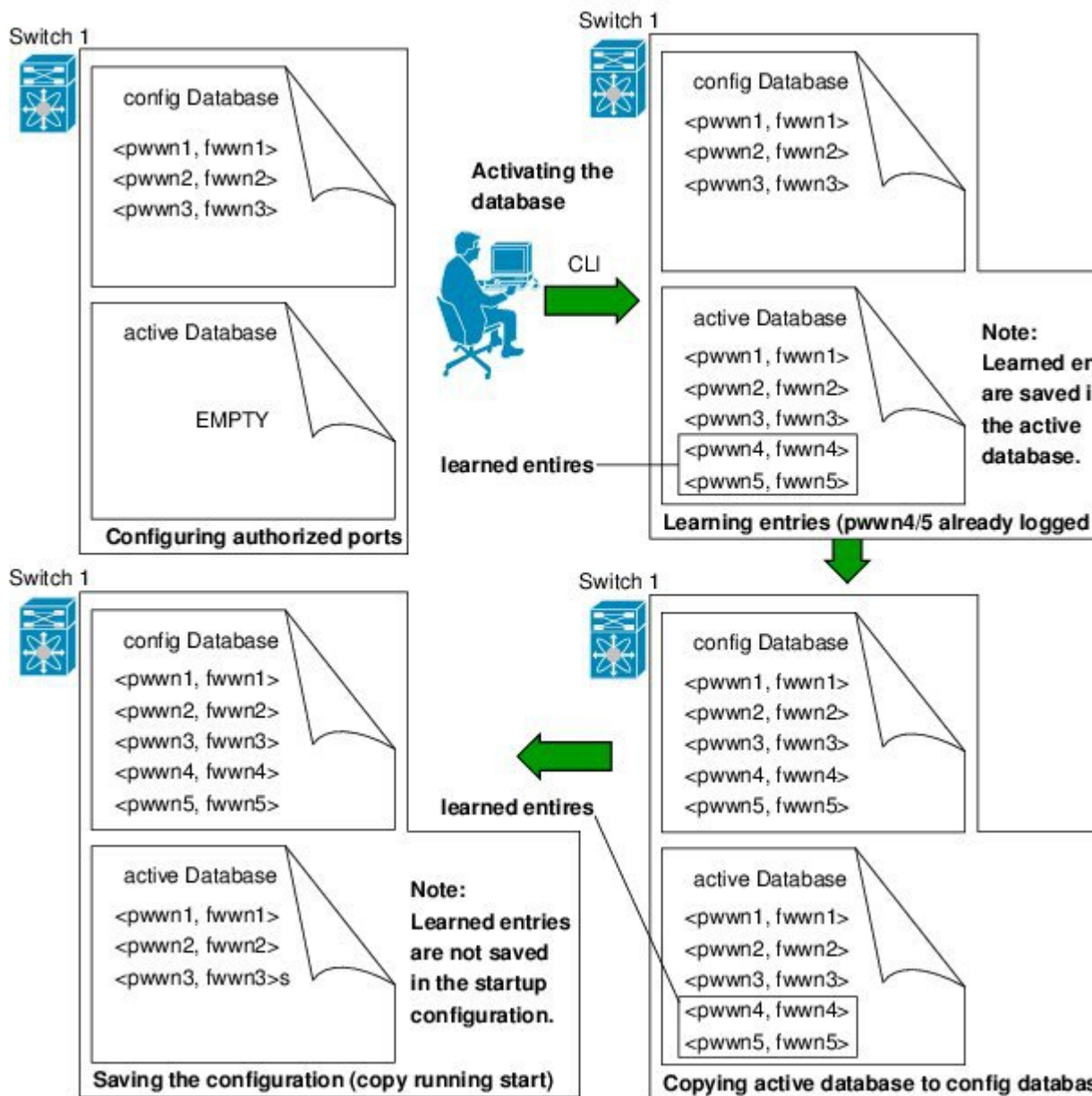
port-security database copy vsan コマンドを使用すると、コンフィギュレーション データベースをアクティブ データベースで上書きできます。アクティブ データベースとコンフィギュレーション データベースとの相違を表示するには、EXEC モードで **port-security database diff active vsan** コマンドを使用します。

このセクションは、次のトピックで構成されています。

データベースのシナリオ

[Figure 21: ポートセキュリティ データベースのシナリオ, on page 299](#) の各シナリオは、ポートセキュリティ設定に基づくアクティブ データベースとコンフィギュレーション データベースのステータスを示しています。

Figure 21: ポートセキュリティ データベースのシナリオ



ポートセキュリティ データベースのコピー

アクティブデータベースから設定済みデータベースにコピーするには、**port-security database copy vsan** コマンドを使用します。アクティブデータベースが空の場合、このコマンドは受け付けられません。

```
switch# port-security database copy vsan 1
```

アクティブ データベースとコンフィギュレーション データベースとの相違を表示するには、**port-security database diff active vsan** コマンドを使用します。このコマンドは、競合を解決する場合に使用できます。

```
switch# port-security database diff active vsan 1
```

コンフィギュレーション データベースとアクティブ データベースとの違いに関する情報を取得するには、**port-security database diff config vsan** コマンドを使用します。

```
switch# port-security database diff config vsan 1
```



Tip 自動学習をディセーブルにしてから、**port-security database copy vsan** コマンドを発行することを推奨します。これにより、コンフィギュレーション データベースとアクティブ データベースを確実に同期化できます。配信がイネーブルの場合、このコマンドによってコンフィギュレーション データベースの一時的なコピーが作成され、結果としてファブリックがロックされます。ファブリックをロックする場合、すべてのスイッチのコンフィギュレーション データベースに変更をコミットする必要があります。

ポートセキュリティ データベースの削除



Tip 配信がイネーブルの場合、削除によってデータベースのコピーが作成されます。実際にデータベースを削除するには、明示的に **port-security commit** コマンドを入力する必要があります。

指定された VSAN の設定済みデータベースを削除するには、コンフィギュレーション モードで **no port-security database vsan** コマンドを使用します

```
switch(config)# no port-security database vsan 1
```

ポートセキュリティ データベースのクリア

指定された VSAN のポートセキュリティ データベースから既存の統計情報をすべてクリアするには、**clear port-security statistics vsan** コマンドを使用します。

```
switch# clear port-security statistics vsan 1
```

VSAN 内の指定したインターフェイスについて、すべての学習済みエントリをアクティブ データベースからクリアするには、**clear port-security database auto-learn interface** コマンドを使用します。

```
switch# clear port-security database auto-learn interface fc1/1 vsan 1
```

VSAN全体に関するアクティブデータベース内の学習済みエントリをすべてクリアするには、**clear port-security database auto-learn vsan** コマンドを使用します。

```
switch# clear port-security database auto-learn vsan 1
```



Note **clear port-security database auto-learn** と **clear port-security statistics** コマンドはローカルスイッチにのみ関連するもので、ロックは取得しません。また、学習済みエントリはスイッチにだけローカルで、配信に参加しません。

VSAN内で、任意のスイッチからVSANの保留中のセッションをクリアするには、**port-security clear vsan** コマンドを使用します。

```
switch# clear port-security session vsan 5
```

ポートセキュリティ設定の表示

show port-security database コマンドを使用すると、設定されたポートセキュリティ情報が表示されます（次の例を参照）。

ポートセキュリティコンフィギュレーションデータベースの内容の表示

```
switch# show port-security database
```

```
-----
VSAN      Logging-in Entity                               Logging-in Point                               (Interface)
-----
1         21:00:00:e0:8b:06:d9:1d (pwwn)                20:0d:00:05:30:00:95:de (fc1/13)
1         50:06:04:82:bc:01:c3:84 (pwwn)                20:0c:00:05:30:00:95:de (fc1/12)
2         20:00:00:05:30:00:95:df (swwn)                20:0c:00:05:30:00:95:de (port-channel 128)
3         20:00:00:05:30:00:95:de (swwn)                20:01:00:05:30:00:95:de (fc1/1)
[Total 4 entries]
```

show port-security コマンドで fWWN や VSAN、またはインターフェイスや VSAN を指定すると、アクティブなポートセキュリティの出力を表示することもできます（「VSAN 1 のポートセキュリティコンフィギュレーションデータベースの表示」を参照）。

VSAN 1 のポートセキュリティコンフィギュレーションデータベースの表示

```
switch# show port-security database vsan 1
```

```
-----
Vsan      Logging-in Entity                               Logging-in Point                               (Interface)
-----
```

```

1          *          20:85:00:44:22:00:4a:9e (fc3/5)
1      20:11:00:33:11:00:2a:4a (pwwn)  20:81:00:44:22:00:4a:9e (fc3/1)
[Total 2 entries]

```

アクティブ化されたデータベースの表示

```
switch# show port-security database active
```

```

-----
VSAN      Logging-in Entity          Logging-in Point      (Interface)          Learnt
-----
1         21:00:00:e0:8b:06:d9:1d (pwwn)  20:0d:00:05:30:00:95:de (fc1/13)          Yes
1         50:06:04:82:bc:01:c3:84 (pwwn)  20:0c:00:05:30:00:95:de (fc1/12)          Yes
2         20:00:00:05:30:00:95:df (swwn)  20:0c:00:05:30:00:95:de (port-channel 128) Yes
3         20:00:00:05:30:00:95:de (swwn)  20:01:00:05:30:00:95:de (fc1/1)          Yes
[Total 4 entries]

```

一時的なコンフィギュレーションデータベースの内容の表示

```
switch# show port-security pending vsan 1
```

```
Session Context for VSAN 1
```

```

-----
Activation Status: Active
Auto Learn Status: On
Force activate: No
Config db modified: Yes
Activation done: Yes
Session owner: admin(2)
Session database:

```

```

-----
VSAN Logging-in Entity Logging-in Point (Interface)
-----
1 20:11:00:33:22:00:2a:4a (pwwn) 20:41:00:05:30:00:4a:1e (fc2/1)
[Total 1 entries]

```

一時的なコンフィギュレーションデータベースとコンフィギュレーションデータベースの相違の表示

```
switch# show port-security pending-diff vsan 1
```

```

Session Diff for VSAN: 1
-----
Database will be activated
Learning will be turned ON
Database Diff:
+pwwn 20:11:00:33:22:00:2a:4a fwwn 20:41:00:05:30:00:4a:1e

```

各ポートのアクセス情報は個別に表示されます。fwwn または interface オプションを指定すると、（その時点で）アクティブデータベース内で指定された fwwn またはインターフェイスとペアになっているすべてのデバイスが表示されます（次の例を参照）。

VSAN 1 内のワイルドカード fwwn ポートセキュリティの表示

```
switch# show port-security database fwwn 20:85:00:44:22:00:4a:9e vsan 1

Any port can login thru' this fwwn
```

VSAN 1 内の設定済み fwwn ポートセキュリティの表示

```
switch# show port-security database fwwn 20:01:00:05:30:00:95:de vsan 1

20:00:00:0c:88:00:4a:e2(swwn)
```

VSAN 2 内のインターフェイス ポート情報の表示

```
switch# show port-security database interface fc 1/1 vsan 2

20:00:00:0c:88:00:4a:e2(swwn)
```

ポートセキュリティの統計情報は、常時更新され、いつでも入手できます（「ポートセキュリティ統計の表示」を参照）。

ポートセキュリティ統計の表示

```
switch# show port-security statistics

Statistics For VSAN: 1
-----
Number of pWWN permit: 2
Number of nWWN permit: 2
Number of sWWN permit: 2
Number of pWWN deny : 0
Number of nWWN deny : 0
Number of sWWN deny : 0
Total Logins permitted : 4
Total Logins denied : 0
Statistics For VSAN: 2
-----
Number of pWWN permit: 0
Number of nWWN permit: 0
Number of sWWN permit: 2
Number of pWWN deny : 0
Number of nWWN deny : 0
Number of sWWN deny : 0
...
```

アクティブなデータベースおよび自動学習設定のステータスを確認するには、**show port-security status** コマンドを使用します（「ポートセキュリティのステータスの表示」を参照）。

ポートセキュリティのステータスの表示

```
switch# show port-security status

Fabric Distribution Enabled
VSAN 1 :No Active database, learning is disabled, Session Lock Taken
```

```
VSAN 2 :No Active database, learning is disabled, Session Lock Taken
...
```

show port-security コマンドは、デフォルトでこれまでの 100 の違反を表示します（「ポートセキュリティ データベース違反の表示」を参照）。

ポートセキュリティ データベースでの違反の表示

```
switch# show port-security violations
```

```
-----
VSAN      Interface      Logging-in Entity      Last-Time      [Repeat count]
-----
1         fc1/13          21:00:00:e0:8b:06:d9:1d(pwn)  Jul  9 08:32:20 2003      [20]
          20:00:00:e0:8b:06:d9:1d(nwn)
1         fc1/12          50:06:04:82:bc:01:c3:84(pwn)  Jul  9 08:32:20 2003      [1]
          50:06:04:82:bc:01:c3:84(nwn)
2         port-channel 1  20:00:00:05:30:00:95:de(swn)  Jul  9 08:32:40 2003      [1]
[Total 2 entries]
```

show port-security コマンドを **last number** オプションを指定して発行すると、先頭に表示される指定した数のエントリだけが表示されます。

デフォルト設定

次の表に、任意のスイッチにおけるすべてのポートセキュリティ機能のデフォルト設定を示します。

Table 24: セキュリティのデフォルト設定値

パラメータ	デフォルト
自動学習	ポートセキュリティがイネーブルの場合は、イネーブル。
ポートセキュリティ	ディセーブル
Distribution	ディセーブル Note 配信をイネーブルにすると、スイッチ上のすべての VSAN の配信がイネーブルになります。



第 12 章

Fibre Channel Common Transport 管理セキュリティの設定

この章では、Cisco MDS 9000 シリーズ スイッチの Fibre Channel Common Transport (FC-CT) 管理セキュリティ機能について説明します。

この章は、次の項で構成されています。

- [Fibre Channel Common Transport の概要](#) , on page 305
- [設定のガイドライン](#) , on page 306
- [Fibre Channel Common Transport クエリーの設定](#) , on page 306
- [Fibre Channel Common Transport 管理セキュリティの確認](#) , on page 307
- [デフォルト設定](#) , on page 307

Fibre Channel Common Transport の概要

FC-CT 管理セキュリティ機能により、ストレージ管理者またはネットワーク管理者だけが、スイッチに対してクエリーを送信し、情報にアクセスできるようにネットワークを設定できます。このような情報には、ファブリック内のログインデバイス、ファブリック内のスイッチなどのデバイス、デバイスの接続方法、各スイッチのポートの数、各ポートの接続先、設定済みゾーンの情報、ゾーンまたはゾーンセットの追加と削除の権限、ファブリックに接続するすべてのホストのホストバスアダプタ (HBA) の詳細などがあります。



Note Cisco MDS NX-OS Release 6.2(9) では、FC 管理機能はデフォルトで無効です。FC 管理機能を有効にするには、`fc-management enable` コマンドを使用します。

FC-CT 管理クエリーを送信し、管理サーバーへの要求を変更できる pWWN を設定できます。いずれかのモジュール (ゾーン サーバー、ゾーン分割されていないファイバ チャネル ネーム サーバー (FCNS) 、またはファブリック コンフィギュレーション サーバー (FCS) など) が FC-CT 管理クエリーを受信すると、FC 管理データベースに対する読み取り操作が実行されます。FC 管理データベースでデバイスが検出されると、付与されている権限に基づいて応答が

送信されます。デバイスが FC 管理データベースにない場合は、各モジュールが拒否を送信します。FC 管理が無効な場合、各モジュールが各管理クエリーを処理します。

設定のガイドライン

FC 管理セキュリティ機能には、次の設定に関する注意事項があります。

- Cisco MDS スイッチで FC 管理セキュリティ機能が有効な場合、管理クエリーを送信するデバイスのポート ワールドワイド ネーム (pWWN) が FC 管理データベースに追加されていないと、サーバーへのすべての管理クエリーが拒否されます。
- FC 管理を有効にすると、N_Port Virtualization (NPV) スイッチから N_Port Identifier Virtualization (NPIV) スイッチへの FC-CT 管理サーバー クエリーが拒否されます。FC 管理セキュリティ機能を有効にした後で、NPV スイッチのスイッチ ワールドワイド ネーム (sWWN) を NPIV スイッチの FC 管理データベースに追加することが推奨されます。

Fibre Channel Common Transport クエリーの設定

FC-CT 管理セキュリティを設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **fc-management enable**

```
switch(config)#
```

FC-CT 管理セキュリティを有効にします。

ステップ 3 switch(config)# **fc-management database vsan 1**

FC-CT 管理セキュリティ データベースを設定します。

ステップ 4 switch(config-fc-mgmt)# **pwwn 1:1:1:1:1:1 feature all operation both**

pWWN を FC 管理データベースに追加します。また、pwwn コマンドを設定するときには次に示すオプションのキーワードも使用できます。

- **fcs** : ファブリック コンフィギュレーション サーバーに対する FC-CT クエリーを有効または無効にします。
- **fdmi** : FDMI に対する FC-CT クエリーを有効または無効にします。
- **unzoned-ns** : ゾーン分割されていないネーム サーバーに対する FC-CT クエリーを有効または無効にします。
- **zone** : ゾーン サーバーに対する FC-CT クエリーを有効または無効にします。

ステップ 5 switch# show fc-managment database

設定された FC-CT 管理情報を表示します。

Fibre Channel Common Transport 管理セキュリティの確認

show fc-management database コマンドは、設定されている FC-CT 管理セキュリティ機能の情報を表示します（次の例を参照）。

Fibre Channel Common Transport クエリーの表示

```
switch# show fc-management database
```

```
-----
VSAN PWWN FC-CT Permissions per FC services
-----
1 01:01:01:01:01:01:01:01 Zone (RW), Unzoned-NS (RW), FCS (RW), FDMI (RW)
1 02:02:02:02:02:02:02:02 Zone (R), Unzoned-NS (R), FCS (R), FDMI (R)
1 03:03:03:03:03:03:03:03 Zone (W), Unzoned-NS (W), FCS (W), FDMI (W)
-----
Total 3 entries
switch#
```

FC 管理セキュリティ機能が有効であるかどうかを確認するには、**show fc-management status** コマンドを使用します。

```
switch# show fc-management status
```

```
Mgmt Security Disabled
```

デフォルト設定

次の表に、Cisco MDS 9000 ファミリ スイッチの FC 管理セキュリティ機能のデフォルト設定を示します。

Table 25: デフォルトの FC 管理設定

パラメータ	デフォルト
FC-management	ディセーブル



第 13 章

ファブリック バインディングの設定

この章では、Cisco MDS 9000 シリーズのスイッチに組み込まれているファブリック バインディング機能について説明します。内容は次のとおりです。

- [ファブリック バインディングの概要, on page 309](#)
- [ファブリック バインディングの設定, on page 311](#)
- [デフォルト設定, on page 320](#)

ファブリック バインディングの概要

ファブリック バインディング機能を使用すると、ファブリック バインディング設定で指定されたスイッチ間でだけ、ISLをイネーブルにできます。ファブリック バインディングは、VSAN 単位で設定します。

この機能を使用すると、不正なスイッチがファブリックに参加したり、現在のファブリック処理が中断されることがなくなります。Exchange Fabric Membership Data (EFMD) プロトコルが使用されて、許可スイッチリストがファブリック内のすべてのスイッチで同一になります。

ここでは、次の内容について説明します。

ライセンス要件

ファブリック バインディングを使用するには、スイッチ上に MAINFRAME_PKG ライセンスまたは ENTERPRISE_PKG ライセンスのいずれかをインストールする必要があります。

ライセンス機能のサポートとインストールの詳細については、『*Cisco MDS 9000 Family NX-OS Licensing Guide*』を参照してください。

ポート セキュリティとファブリック バインディングの比較

ポートセキュリティとファブリック バインディングは、相互補完するように設定可能な、2つの独立した機能です。次の表で、2つの機能を比較します。

Table 26: ファブリック バインディングとポートセキュリティの比較

ファブリック バインディング	ポート セキュリティ
スイッチ レベルでファブリックをバインドします。	インターフェイス レベルでデバイスをバインドします。
ファブリック バインディングデータベースに格納された設定済み sWWN にだけ、ファブリックへの参加を許可します。	設定済みの一連のファイバチャネルデバイスを SAN ポートに論理的に接続できます。WWN またはインターフェイス番号で識別されるスイッチ ポートは、同様に WWN で識別されるファイバチャネルデバイス (ホストまたは別のスイッチ) に接続されます。これらの 2 つのデバイスをバインドすると、これらの 2 つのポートがグループ (リスト) にロックされます。
VSAN 単位でアクティブ化する必要があります。	VSAN 単位でアクティブ化する必要があります。
ピア スイッチが接続されている物理ポートに関係なく、ファブリックに接続可能な特定のユーザー定義のスイッチを許可します。	別のデバイスを接続できる特定のユーザー定義の物理ポートを許可します。
ログインしているスイッチについて学習しません。	学習モードがイネーブルの場合、ログインしているスイッチまたはデバイスについて学習します。
CFS によって配信できず、ファブリック内の各スイッチで手動で設定する必要があります。	CFS によって配信できます。
一連の sWWN および永続的ドメイン ID を使用します。	pWWN/nWWN または fWWN/sWWN を使用します。

ポート レベルの xE ポート検査は、次のとおりです。

- スイッチ ログインは、指定された VSAN にポートセキュリティ バインディングとファブリック バインディングの両方を使用します。
- バインディング検査は、ポート VSAN で次のように実行されます。
 - ポート VSAN での E ポートセキュリティ バインディング検査
 - 許可された各 VSAN での TE ポートセキュリティ バインディング検査

ポートセキュリティはファブリック バインディングを補完する関係にあります。これらの機能は互いに独立していて、個別にイネーブルまたはディセーブルにできます。

ファブリック バインディングの実行

ファブリック バインディングを実行するには、Switch World Wide Name (sWWN) を設定して、スイッチごとにxEポート接続を指定します。ファブリック バインディングポリシーは、ポートがアクティブになるたび、およびポートを起動しようとした場合に実行されます。FICON VSAN でファブリック バインディング機能を実行するには、すべての sWWN をスイッチに接続し、永続的ドメイン ID をファブリック バインディング アクティブ データベースに格納する必要があります。ファイバチャネル VSAN では、sWWN だけが必要であり、ドメイン ID はオプションです。



Note ファブリック バインディングを使用するファイバチャネル VSAN の全スイッチで、Cisco MDS SAN-OS Release 3.0(1) および NX-OS Release 4.1(1b) 以降を実行している必要があります。

ファブリック バインディングの設定

ファブリック内の各スイッチにファブリック バインディングを設定する手順は、次のとおりです。

Procedure

- ステップ 1** ファブリック設定機能をイネーブルにします。
- ステップ 2** ファブリックにアクセス可能なデバイスにsWWNのリスト、および対応するドメイン ID を設定します。
- ステップ 3** ファブリック バインディング データベースをアクティブにします。
- ステップ 4** ファブリック バインディング アクティブ データベースを、ファブリック バインディング コンフィギュレーション データベースにコピーします。
- ステップ 5** ファブリック バインディング設定を保存します。
- ステップ 6** ファブリック バインディング設定を確認します。

ファブリック バインディングのイネーブル化

ファブリック バインディングに参加するファブリック内のスイッチごとに、ファブリック バインディング機能をイネーブルにする必要があります。デフォルトでは、この機能は Cisco MDS 9000 ファミリのすべてのスイッチでディセーブルになっています。ファブリック バインディング機能に関する設定および確認コマンドを使用できるのは、スイッチ上でファブリック バインディングがイネーブルな場合だけです。この設定をディセーブルにした場合、関連するすべての設定は自動的に廃棄されます。

参加させるスイッチのファブリック バインディングをイネーブルにする手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーションモードに入ります。

ステップ 2 switch(config)# **feature fabric-binding**

現在のスイッチ上でファブリック バインディングをイネーブルにします。

ステップ 3 switch(config)# **no feature fabric-binding**

(オプション) 現在のスイッチ上でファブリック バインディングをディセーブル (デフォルト) にします。

Example

ファブリック バインディングがイネーブルになっているスイッチのファブリック バインディング機能のステータスを表示するには、**show fabric-binding status** コマンドを発行します。

```
switch# show fabric-binding status
```

```
VSAN 1:Activated database  
VSAN 4:No Active database
```

FICON VSAN のスイッチ WWN リストの設定

ユーザー指定のファブリック バインディングリストには、ファブリック内の sWWN のリストが含まれています。リストにない sWWN、または許可リストで指定されているドメイン ID と異なるドメイン ID を使用する sWWN がファブリックへの参加を試みると、スイッチとファブリック間の ISL が VSAN 内で自動的に隔離され、スイッチはファブリックへの参加を拒否されます。

永続的ドメイン ID は sWWN とともに指定できます。FICON VSAN では、ドメイン ID 許可が必要です。FICON VSAN では、ドメインがスタティックに設定されているため、エンドデバイスによって、ファブリック内のすべてのスイッチにおけるドメイン ID の変更が拒否されます。ファイバチャネル VSAN の場合には、ドメイン ID 許可は不要です。

FICON VSAN 用の sWWN およびドメイン ID のリストを設定する手順は、次のとおりです。

Procedure

- ステップ 1** switch# **configure terminal**
switch(config)#
コンフィギュレーション モードに入ります。
- ステップ 2** switch(config)# **fabric-binding database vsan 5**
switch(config-fabric-binding)#
指定された VSAN のファブリック バインディング サブモードを開始します。
- ステップ 3** switch(config)# **no fabric-binding database vsan 5**
(オプション) 指定された VSAN のファブリック バインディング データベースを削除します。
- ステップ 4** switch(config-fabric-binding)# **swwn 21:00:05:30:23:11:11:11 domain 102**
設定したデータベース リストにスイッチの sWWN およびドメイン ID を追加します。
- ステップ 5** switch(config-fabric-binding)# **swwn 21:00:05:30:23:1a:11:03 domain 101**
設定したデータベース リストに別のスイッチの sWWN およびドメイン ID を追加します。
- ステップ 6** switch(config-fabric-binding)# **no swwn 21:00:15:30:23:1a:11:03 domain 101**
(オプション) 設定されたデータベース リストから、スイッチの sWWN およびドメイン ID を削除します。
- ステップ 7** switch(config-fabric-binding)# **exit**
switch(config)#
ファブリック バインディング サブモードを終了します。
-

ファイバチャネル VSAN のスイッチ WWN リストの設定

ファイバチャネル VSAN 用の sWWN および任意のドメイン ID のリストを設定する手順は、次のとおりです。

Procedure

- ステップ 1** switch# **configure terminal**
switch(config)#
コンフィギュレーション モードに入ります。
- ステップ 2** switch(config)# **fabric-binding database vsan 10**

```
switch(config-fabric-binding)#
```

指定された VSAN のファブリック バインディング サブモードを開始します。

ステップ 3 switch(config)# **no fabric-binding database vsan 10**

(オプション) 指定された VSAN のファブリック バインディング データベースを削除します。

ステップ 4 switch(config-fabric-binding)# **swwn 21:00:05:30:23:11:11:11**

設定したデータベース リストに全ドメインのスイッチの sWWN を追加します。

ステップ 5 switch(config-fabric-binding)# **no swwn 21:00:05:30:23:11:11:11**

(オプション) 設定したデータベース リストから全ドメインのスイッチの sWWN を削除します。

ステップ 6 switch(config-fabric-binding)# **swwn 21:00:05:30:23:1a:11:03 domain 101**

設定されたデータベース リストに、特定のドメイン ID 用の別のスイッチの sWWN を追加します。

ステップ 7 switch(config-fabric-binding)# **no swwn 21:00:15:30:23:1a:11:03 domain 101**

(オプション) 設定されたデータベース リストから、スイッチの sWWN およびドメイン ID を削除します。

ステップ 8 switch(config-fabric-binding)# **exit**

```
switch(config)#
```

ファブリック バインディング サブモードを終了します。

ファブリック バインディングのアクティブ化

ファブリック バインディング機能によって、コンフィギュレーション データベース (config-database) およびアクティブ データベースが保持されます。コンフィギュレーション データベースは、実行された設定を収集する読み書きデータベースです。これらの設定を実行するには、データベースをアクティブにする必要があります。データベースがアクティブになると、アクティブ データベースにコンフィギュレーション データベースの内容が上書きされます。アクティブ データベースは、ログインを試みる各スイッチをチェックする読み取り専用データベースです。

デフォルトでは、ファブリック バインディング機能は非アクティブです。設定したデータベース内の既存のエントリがファブリックの現在の状態と矛盾していると、スイッチ上のファブリック バインディング データベースをアクティブにできません。たとえば、ログイン済みのスイッチの1つが、コンフィギュレーション データベースによってログインを拒否されている場合などです。これらの状態を強制的に上書きできます。



Note アクティベーションのあと、現在アクティブなデータベースに違反するログイン済みのスイッチは、ログアウトされ、ファブリック バインディング制限によってログインが拒否されたすべてのスイッチは再初期化されます。

ファブリック バインディング機能をアクティブにする手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **fabric-binding activate vsan 10**

指定された VSAN のファブリック バインディング データベースをアクティブにします。

ステップ 3 switch(config)# **no fabric-binding activate vsan 10**

(オプション) 指定された VSAN のファブリック バインディング データベースを非アクティブにします。

ファブリック バインディングの強制的なアクティベーション

上記のような競合が1つまたは複数発生したためにデータベースのアクティブ化が拒否された場合は、**force** オプションを使用してアクティブ化を継続できます。

ファブリック バインディング データベースを強制的にアクティブにする手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

```
switch(config)#
```

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **fabric-binding activate vsan 3 force**

指定した VSAN のファブリック バインディング データベースを強制的に（設定が許可されていない場合でも）アクティブにします。

ステップ 3 switch(config)# **no fabric-binding activate vsan 3 force**

(オプション) 元の設定状態、または (状態が設定されていない場合は) 出荷時の設定に戻します。

ファブリック バインディング設定の保存

ファブリック バインディング設定を保存すると、コンフィギュレーション データベースが実行コンフィギュレーションに保存されます。



Caution FICON がイネーブルである VSAN では、ファブリック バインディングをディセーブルにできません。

- アクティブ データベースからコンフィギュレーション データベースにコピーするには、**fabric-binding database copy vsan** コマンドを使用します。設定されたデータベースが空の場合、このコマンドは受け付けられません。

```
switch# fabric-binding database copy vsan 1
```

- アクティブ データベースとコンフィギュレーション データベースとの相違を表示するには、**fabric-binding database diff active vsan** コマンドを使用します。このコマンドは、競合を解決する場合に使用できます。

```
switch# fabric-binding database diff active vsan 1
```

- コンフィギュレーション データベースとアクティブ データベースとの違いに関する情報を取得するには、**fabric-binding database diff config vsan** コマンドを使用します。

```
switch# fabric-binding database diff config vsan 1
```

- 再起動後にファブリック バインディング設定データベースを使用できるよう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保存するには、**copy running-config startup-config** コマンドを使用します。

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

ファブリック バインディング統計情報のクリア

指定された VSAN のファブリック バインディング データベースから既存の統計情報をすべてクリアするには、**clear fabric-binding statistics** コマンドを使用します。

```
switch# clear fabric-binding statistics vsan 1
```

ファブリック バインディング データベースの削除

指定された VSAN の設定済みデータベースを削除するには、コンフィギュレーション モードで **no fabric-binding** コマンドを使用します。

```
switch(config)# no fabric-binding database vsan 10
```

ファブリック バインディング設定の確認

show コマンドを使用して、このスイッチに設定されているすべてのファブリック バインディング情報を表示します（次の例を参照）。

設定したファブリック バインディング データベース情報の表示

```
switch# show fabric-binding database
```

```
-----
Vsan   Logging-in Switch WWN      Domain-id
-----
1      21:00:05:30:23:11:11:11   0x66(102)
1      21:00:05:30:23:1a:11:03   0x19(25)
1      20:00:00:05:30:00:2a:1e   0xea(234) [Local]
4      21:00:05:30:23:11:11:11   Any
4      21:00:05:30:23:1a:11:03   Any
4      20:00:00:05:30:00:2a:1e   0xea(234) [Local]
61     21:00:05:30:23:1a:11:03   0x19(25)
61     21:00:05:30:23:11:11:11   0x66(102)
61     20:00:00:05:30:00:2a:1e   0xea(234) [Local]
[Total 7 entries]
```

アクティブ ファブリック バインディング情報の表示

```
switch# show fabric-binding database active
```

```
-----
Vsan   Logging-in Switch WWN      Domain-id
-----
1      21:00:05:30:23:11:11:11   0x66(102)
1      21:00:05:30:23:1a:11:03   0x19(25)
1      20:00:00:05:30:00:2a:1e   0xea(234) [Local]
61     21:00:05:30:23:1a:11:03   0x19(25)
61     21:00:05:30:23:11:11:11   0x66(102)
61     20:00:00:05:30:00:2a:1e   0xef(239) [Local]
```

設定した VSAN 固有のファブリック バインディング情報の表示

```
switch# show fabric-binding database vsan 4
```

```
-----
Vsan   Logging-in Switch WWN      Domain-id
-----
4      21:00:05:30:23:11:11:11   Any
4      21:00:05:30:23:1a:11:03   Any
4      20:00:00:05:30:00:2a:1e   0xea(234) [Local]
[Total 2 entries]
```

アクティブな VSAN 固有のファブリック バインディング情報の表示

```
switch# show fabric-binding database active vsan 61
```

```
-----
Vsan   Logging-in Switch WWN      Domain-id
-----
61     21:00:05:30:23:1a:11:03    0x19(25)
61     21:00:05:30:23:11:11:11    0x66(102)
61     20:00:00:05:30:00:2a:1e    0xef(239) [Local]
[Total 3 entries]
```

ファブリック バインディング統計情報の表示

```
switch# show fabric-binding statistics
```

```
Statistics For VSAN: 1
-----
Number of sWWN permit: 0
Number of sWWN deny  : 0
Total Logins permitted : 0
Total Logins denied   : 0
Statistics For VSAN: 4
-----
Number of sWWN permit: 0
Number of sWWN deny  : 0
Total Logins permitted : 0
Total Logins denied   : 0
Statistics For VSAN: 61
-----
Number of sWWN permit: 0
Number of sWWN deny  : 0
Total Logins permitted : 0
Total Logins denied   : 0
Statistics For VSAN: 345
-----
Number of sWWN permit: 0
Number of sWWN deny  : 0
Total Logins permitted : 0
Total Logins denied   : 0
Statistics For VSAN: 346
-----
Number of sWWN permit: 0
Number of sWWN deny  : 0
Total Logins permitted : 0
Total Logins denied   : 0
Statistics For VSAN: 347
-----
Number of sWWN permit: 0
Number of sWWN deny  : 0
Total Logins permitted : 0
Total Logins denied   : 0
Statistics For VSAN: 348
-----
Number of sWWN permit: 0
Number of sWWN deny  : 0
Total Logins permitted : 0
Total Logins denied   : 0
Statistics For VSAN: 789
-----
Number of sWWN permit: 0
Number of sWWN deny  : 0
Total Logins permitted : 0
Total Logins denied   : 0
```

```

Statistics For VSAN: 790
-----
Number of sWWN permit: 0
Number of sWWN deny  : 0
Total Logins permitted : 0
Total Logins denied   : 0
    
```

VSAN ごとのファブリック バインディング状態の表示

```
switch# show fabric-binding status
```

```

VSAN 1 :Activated database
VSAN 4 :No Active database
VSAN 61 :Activated database
VSAN 345 :No Active database
VSAN 346 :No Active database
VSAN 347 :No Active database
VSAN 348 :No Active database
VSAN 789 :No Active database
VSAN 790 :No Active database
    
```

ファブリック バインディング違反の表示

```
switch# show fabric-binding violations
```

```

-----
VSAN Switch WWN [domain]      Last-Time                [Repeat count] Reason
-----
2    20:00:00:05:30:00:4a:1e [0xeb] Nov 25 05:46:14 2003  [2]  Domain mismatch
3    20:00:00:05:30:00:4a:1e [*] Nov 25 05:44:58 2003  [2]  sWWN not found
4    20:00:00:05:30:00:4a:1e [*] Nov 25 05:46:25 2003  [1]  Database mismatch
    
```



(注) VSAN3 では、sWWN 自身がリストにありません。VSAN2 では、sWWN がリストで見つかりましたが、ドメイン ID が一致しませんでした。

EFMD 統計情報の表示

```
switch# show fabric-binding efmd statistics
```

```

EFMD Protocol Statistics for VSAN 1
-----
Merge Requests -> Transmitted : 0 , Received : 0
Merge Accepts  -> Transmitted : 0 , Received : 0
Merge Rejects  -> Transmitted : 0 , Received : 0
Merge Busy     -> Transmitted : 0 , Received : 0
Merge Errors   -> Transmitted : 0 , Received : 0
EFMD Protocol Statistics for VSAN 4
-----
Merge Requests -> Transmitted : 0 , Received : 0
Merge Accepts  -> Transmitted : 0 , Received : 0
Merge Rejects  -> Transmitted : 0 , Received : 0
Merge Busy     -> Transmitted : 0 , Received : 0
Merge Errors   -> Transmitted : 0 , Received : 0
EFMD Protocol Statistics for VSAN 61
-----
Merge Requests -> Transmitted : 0 , Received : 0
Merge Accepts  -> Transmitted : 0 , Received : 0
Merge Rejects  -> Transmitted : 0 , Received : 0
    
```

```
Merge Busy      -> Transmitted : 0 , Received : 0
Merge Errors    -> Transmitted : 0 , Received : 0
```

指定した VSAN の EFMD 統計情報の表示

```
switch# show fabric-binding efmd statistics vsan 4
```

```
EFMD Protocol Statistics for VSAN 4
-----
Merge Requests -> Transmitted : 0 , Received : 0
Merge Accepts  -> Transmitted : 0 , Received : 0
Merge Rejects  -> Transmitted : 0 , Received : 0
Merge Busy     -> Transmitted : 0 , Received : 0
Merge Errors   -> Transmitted : 0 , Received : 0
```

デフォルト設定

次の表に、ファブリック バインディング機能のデフォルト設定を示します。

Table 27: ファブリック バインディングのデフォルト設定

パラメータ	デフォルト
ファブリック バインディング	ディセーブル



第 14 章

Cisco TrustSec ファイバチャネルリンク暗号化の設定

この章では、Cisco TrustSec ファイバチャネル (FC) リンクの暗号化機能の概要を示し、スイッチ間にリンクレベルの暗号化を設定する方法について説明します。

この章は、次の項目を取り上げます。

- [Cisco TrustSec FC リンク暗号化に関する用語, on page 321](#)
- [AES 暗号化のサポート, on page 322](#)
- [Cisco TrustSec FC リンク暗号化の概要, on page 322](#)
- [Cisco TrustSec FC リンク暗号化情報の表示, on page 328](#)
- [Cisco TrustSec FC リンク暗号化のベストプラクティス, on page 329](#)

Cisco TrustSec FC リンク暗号化に関する用語

この章では、次に示す Cisco TrustSec FC リンク暗号化関連の用語を使用します。

- **ガロアカウンタモード (GCM)** : 機密保持とデータ発信元認証を行う操作のブロック暗号モード。
- **ガロアメッセージ認証コード (GMAC)** : データ発信元認証だけを行う操作のブロック暗号モード。GCM の認証限定バリエーションです。
- **セキュリティアソシエーション (SA)** : セキュリティ認定証を処理し、それらの認定証をスイッチ間にどのように伝播するかを制御する接続。SA には、salt やキーなどのパラメータが含まれます。
- **キー** : フレームの暗号化および復号化に使用する 128 ビットの 16 進数字列。デフォルト値は 0 です。
- **Salt** : 暗号化および復号化の際に使用する 32 ビットの 16 進数字列。適切な通信を行うには、接続の両側に同じ salt を設定する必要があります。デフォルト値は 0 です。
- **セキュリティパラメータインデックス (SPI) 番号** : ハードウェアに設定される SA を識別する 32 ビットの数字。有効な範囲は 256 ~ 65536 です。

AES 暗号化のサポート

Advanced Encryption Standard (AES) は、ハイレベルなセキュリティを実現する対称暗号アルゴリズムであり、さまざまなキー サイズを受け入れることができます。

Cisco TrustSec FC リンク暗号化機能は、セキュリティ暗号用に 128 ビットの AES をサポートし、インターフェイスに AES-GCM または AES-GMAC のいずれかをイネーブルにします。AES-GCM モードではフレームの暗号化と認証が可能であり、AES-GMAC では2つのピア間で送受信されるフレームの認証だけが可能です。

Cisco TrustSec FC リンク暗号化の概要

Cisco TrustSec FC リンク暗号化は、Fibre Channel-Security Protocol (FC-SP) の拡張機能であり、既存の FC-SP アーキテクチャを使用してトランザクションの整合性と機密保持を実現します。セキュリティを保ち、望ましくないトラフィック傍受を防止するため、ピア認証機能に暗号化が追加されました。ピア認証は、Diffie-Hellman (DH) Challenge Handshake Authentication Protocol (DHCHAP) プロトコルを使用した FC-SP 標準に従って実装されます。



Note Cisco TrustSec FC リンク暗号化は現在、Cisco MDS スイッチ間に限りサポートされています。この機能は、カプセル化セキュリティペイロード (ESP) プロトコルをサポートしていないソフトウェア バージョンにダウングレードするとサポートされなくなります。

このセクションは、次のトピックで構成されています。

Supported Modules

For more information about supported modules, see the Cisco TrustSec FC Link Encryption section of the [Cisco MDS 9000 NX-OS and SAN-OS Software Release Notes](#).

Cisco TrustSec FC リンク暗号化のイネーブル化

Cisco MDS 9000 ファミリのすべてのスイッチの FC-SP 機能と Cisco TrustSec FC リンク暗号化機能は、デフォルトでディセーブルになります。

ファブリック認証および暗号化用のコンフィギュレーションコマンドおよび確認コマンドにアクセスするには、FC-SP 機能をイネーブルにする必要があります。この機能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。

Cisco MDS スイッチの FC-SP をイネーブルにする手順は、次のとおりです。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **feature fcsp**

FC-SP 機能をイネーブルにします。

ステップ 3 switch(config)# **no feature fcsp**

(オプション) このスイッチの FC-SP 機能をディセーブル (デフォルト) にします。

Example

Cisco TrustSec FC リンク暗号化機能を設定するには、ENTERPRISE_PKG ライセンスが必要です。詳細については、『Cisco MDS 9000 Family NX-OS Licensing Guide』を参照してください。

セキュリティ アソシエーションの設定

スイッチ間で暗号化を実行するには、セキュリティ アソシエーション (SA) を設定する必要があります。暗号化を実行するには、管理者があらかじめ手動で SA を設定する必要があります。SA には、キーや salt など、暗号化に必要なパラメータが含まれます。スイッチには、最大 2000 の SA を設定できます。

2 台のスイッチ間の SA を設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

コンフィギュレーション モードに入ります。

ステップ 2 switch(config)# **fcsp esp sa spi_number**

SA を設定するための SA サブモードを開始します。spi_number の範囲は 256 ~ 65536 です。

ステップ 3 switch(config)# **no fcsp esp sa spi_number**

(オプション) スイッチ間の SA を削除します。⁸

⁸ 指定した SA が現在ポートにプログラムされている場合、このコマンドは SA が使用中であることを伝えるエラーを返します。

Example

どのポートが SA を使用しているかを調べるには、`show running-config fcsp` コマンドを使用します。実行中のシステム情報の表示, [on page 329](#)を参照してください。



Note Cisco TrustSec FC リンク暗号化は現在、on モードと off モードの DHCHAP だけでサポートされています。

セキュリティ アソシエーションパラメータの設定

キーや salt などの SA パラメータを設定する手順は、次のとおりです。

Procedure

ステップ 1 `switch# configure terminal`

コンフィギュレーションモードに入ります。

ステップ 2 `switch(config)# fcsp esp sa spi_number`

SA を設定するための SA サブモードを開始します。spi_number の範囲は 256 ~ 65536 です。

ステップ 3 `switch(config-sa)# key key`

SA のキーを設定します。key の最大サイズは 34 です。

ステップ 4 `switch(config-sa)# no key key`

(オプション) SA からキーを削除します。

ステップ 5 `switch(config-sa)# salt salt`

SA の salt を設定します。有効な範囲は 0x0 ~ 0xffffffff です。

ステップ 6 `switch(config-sa)# no salt salt`

(オプション) SA の salt が削除されます。

ESP の設定

このセクションは、次のトピックで構成されています。

入力および出力ポートでの ESP の設定

SA が作成されると、ポートにカプセル化セキュリティ プロトコル (ESP) を設定する必要があります。同等のネットワーク間でパケットを暗号化および復号化する出力および入力ポートを指定する必要があります。出力 SA はどのキーまたはパラメータがスイッチから出るパケットの暗号化に使用されるかを指定します。入力 SA はどのキーまたはパラメータが特定のポートに入るパケットの復号化に使用されるかを指定します。



Note ESP を設定する際は、E と自動ポート モードのみがサポートされます。

この項では、次のトピックについて取り上げます。

入力ポートでの ESP の設定

入力のハードウェアに SA を設定するには、次の手順を実行します。

Procedure

ステップ 1 `switch# configure terminal`

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)# interface fc x/y`

スロット x のポート y に FC インターフェイスを設定します。

Note ポート チャネルを選択すると、ポート チャネルのすべてのメンバの設定が適用されます。

ステップ 3 `switch(config-if)# fcsp esp manual`

ESP コンフィギュレーション サブモードを開始します。

ステップ 4 `switch(config-if-esp)# ingress-sa spi_number`

入力のハードウェアに SA を設定します。

ステップ 5 `switch (config-if-esp)# no ingress-sa spi_number`

(オプション) 入力のハードウェアから SA を削除します。⁹

出力ポートでの ESP の設定

出力のハードウェアに SA を設定するには、次の手順を実行します。

⁹ SA が入力ポートで設定されていない場合、このコマンドを実行すると、エラー メッセージが返されます。

Procedure

ステップ 1 switch# **configure terminal**

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)# **interface fc x/y**

スロット x のポート y に FC インターフェイスを設定します。

Note ポート チャネルを選択すると、ポート チャネルのすべてのメンバの設定が適用されます。

ステップ 3 switch(config-if)# **fcsp esp manual**

ESP コンフィギュレーション サブモードを開始します。

ステップ 4 switch(config-if-esp)# **egress-sa spi_number**

出力のハードウェアに SA を設定します。

ステップ 5 switch(config-if)# **no fcsp esp manual**

(オプション) 入力と出力のハードウェアから SA を削除します。[10](#)

Example



Note インターフェイスの入力および出力ハードウェアに SA を適用するには、インターフェイスが `admin shut` モードである必要があります。

ESP モードの設定

GCM としてポートがメッセージ認証と暗号化を有効にする、または GMAC としてポートがメッセージ認証を有効にするように、ESP を設定します。

デフォルトの ESP モードは AES-GCM です。

この項では、次のトピックについて取り上げます。

AES-GCM の設定

AES-GCM モードを設定するには、次の手順を実行します。

¹⁰ SA が出力ポートで設定されていない場合、このコマンドを実行すると、エラー メッセージが返されます。

Procedure

ステップ 1 switch# **configure terminal**

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)# **interface fc x/y**

スロット x のポート y に FC インターフェイスを設定します。

Note ポートチャネルを選択すると、ポートチャネルのすべてのメンバの設定が適用されます。

ステップ 3 switch(config-if)# **fcsp esp manual**

各ポートの ESP を設定するために ESP コンフィギュレーション サブモードを開始します。

ステップ 4 switch(config-if-esp)# **mode gcm**

インターフェイスの GCM モードを設定します。

AES-GMAC の設定

AES-GMAC モードを設定するには、次の手順を実行します。

Procedure

ステップ 1 switch# **configure terminal**

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)# **interface fc x/y**

スロット x のポート y に FC インターフェイスを設定します。

Note ポートチャネルを選択すると、ポートチャネルのすべてのメンバの設定が適用されます。

ステップ 3 switch(config-if)# **fcsp esp manual**

各ポートの ESP を設定するために ESP コンフィギュレーション サブモードを開始します。

ステップ 4 switch(config-if-esp)# **mode gmac**

インターフェイスの GMAC モードを設定します。

ステップ 5 switch(config-if-esp)# **no mode gmac**

(オプション) GMAC モードをインターフェイスから削除し、デフォルトの AES-GCM モードを適用します。

Example



Note

- ESP モードが設定されるのは、入力または出力ハードウェアに SA が設定されている場合だけです。SA が設定されていない場合は、ESP がオフになり、カプセル化は行われません。
- ポートを設定した後で ESP モードを変更した場合は、変更がシームレスでないため、常にポートのフラップが必要です。ただし、設定は拒否されません。
- FC-SP ポートモードが有効で、ESP 対応のスイッチまたはブレードで使用可能な ISL だけが表示されます。
- 選択した ISL がイネーブルであれば、既存の ESP 設定を変更できます。

Cisco TrustSec FC リンク暗号化情報の表示

Fabric Manager または Device Manager では、show コマンドを使用して Cisco TrustSec FC リンク暗号化機能の情報を表示できます。

この項では、次のトピックについて取り上げます。

FC-SP のインターフェイス情報の表示

show fcsp interface コマンドを使用して、特定のインターフェイスのすべての FC-SP 関連情報を表示します。

```
switch# show fcsp interface fc7/41

fc7/41:
fcsp authentication mode:SEC_MODE_OFF
ESP is enabled
configured mode is: GCM
programmed ingress SA: 300, 303
programmed egress SA: 300
Status:FC-SP protocol in progress
```

実行中のシステム情報の表示

FC-SPに関連するすべての実行時の情報を表示するには、**show running-config fcsp** コマンドを使用します。ESPおよび設定されたインターフェイスに関するすべての詳細が表示されます。どのポートがSAを使用しているか調べるには、次のコマンドを使用します。

```
switch# show running-config fcsp

version 4.1(2)
feature fcsp
fcsp esp sa 300
key 0x000000000000000000000000000000123456
salt 0x123456
fcsp esp sa 301
key 0x000000000000000000000000000000123456
salt 0x1234567
fcsp esp sa 302
key 0x000000000000000000000000000000123456
salt 0x123456

interface fc8/48
fcsp off
fcsp esp manual
ingress-sa 300
ingress-sa 301
egress-sa 300
```

FC-SP インターフェイス統計情報の表示

インターフェイスに対しDHCHAPとESPに関連するすべての統計情報を表示するには、**show fcsp interface statistics** コマンドを使用します。示されているESP統計情報はポートASICでサポートされているESPにより異なります。

```
switch# show fcsp interface fc3/31 statistics

fc7/41:
fcsp authentication mode:SEC_MODE_ON
ESP is enabled
configured mode is: GMAC
programmed ingress SA: 256, 257
programmed egress SA: 256
Status:Successfully authenticated
Authenticated using local password database
Statistics:
FC-SP Authentication Succeeded:17
FC-SP Authentication Failed:3
FC-SP Authentication Bypassed:0
FC-SP ESP SPI Mismatched frames:0
FC-SP ESP Auth failed frames:0
```

Cisco TrustSec FC リンク暗号化のベストプラクティス

ベストプラクティスとは、Cisco TrustSec FC リンク暗号化を適切に動作させるための推奨手順です。

この項では、次のトピックについて取り上げます。

一般的なベスト プラクティス

ここでは、Cisco TrustSec FC リンク暗号化に関する一般的なベスト プラクティスを示します。

- Cisco TrustSec FC リンク暗号化が MDS スイッチ間だけでイネーブルであることを確認します。この機能は、E ポートまたは ISL だけでサポートされており、MDS 以外のスイッチを使用している場合はエラーが発生します。
- 接続にかかわるピアの設定が同一であることを確認します。設定に相違があると、「port re-init limit exceeded」というエラー メッセージが表示されます。
- スイッチ インターフェイスの入力および出力ハードウェアに SA を適用する前に、インターフェイスが admin shut モードであることを確認します。

キーの変更に関するベスト プラクティス

入力および出力ポートに SA を適用した後は、キーの設定を定期的に変更してください。トラフィックの中断を避けるには、キーを順番に変更する必要があります。

例として、2つのスイッチ、Switch1 と Switch2 の間に作成されたセキュリティアソシエーションについて考えます。SA は、次の例に示すように、入力および出力ポートに設定されます。

```
switch# configure terminal
switch(config)# interface fc1/1
switch(config-if)# fcsp esp manual
switch(config-if)# ingress-sa 256
switch(config-if)# egress-sa 256
```

これらのスイッチのキーを変更するには、次の手順を実行します。

Procedure

ステップ 1 Switch1 と Switch2 に新しい SA を追加します。

```
switch# configure terminal
switch(config)# fcsp esp sa 257
switch(config-sa)# key 0xAC9EF8BC8DB2DBD2008D184F794E0C38
switch(config-sa)# salt 0x1234
```

ステップ 2 Switch1 に入力 SA を設定します。

```
switch# configure terminal
switch(config)# interface fc1/1
switch(config-if)# fcsp esp manual
switch(config-if)# ingress-sa 257
```

ステップ 3 Switch2 に入出力 SA を設定します。

```
switch# configure terminal
switch(config)# interface fc1/1
switch(config-if)# fcsp esp manual
switch(config-if)# ingress-sa 257
switch(config-if)# egress-sa 257
```

ステップ 4 Switch1 に出力 SA を設定します。


```
switch# configure terminal
switch(config)# interface fcl/1
switch(config-if)# fcsp esp manual
switch(config-if)# egress-sa 257
```

ステップ 5 両方のスイッチから以前に設定された入力 SA を削除します。

```
switch# configure terminal
switch(config)# interface fcl/1
switch(config-if)# fcsp esp manual
switch(config-if)# no ingress-sa 256
```



第 15 章

セキュアブートの構成

- [Cisco Secure Boot に関する情報 \(333 ページ\)](#)
- [偽造防止対策について \(334 ページ\)](#)

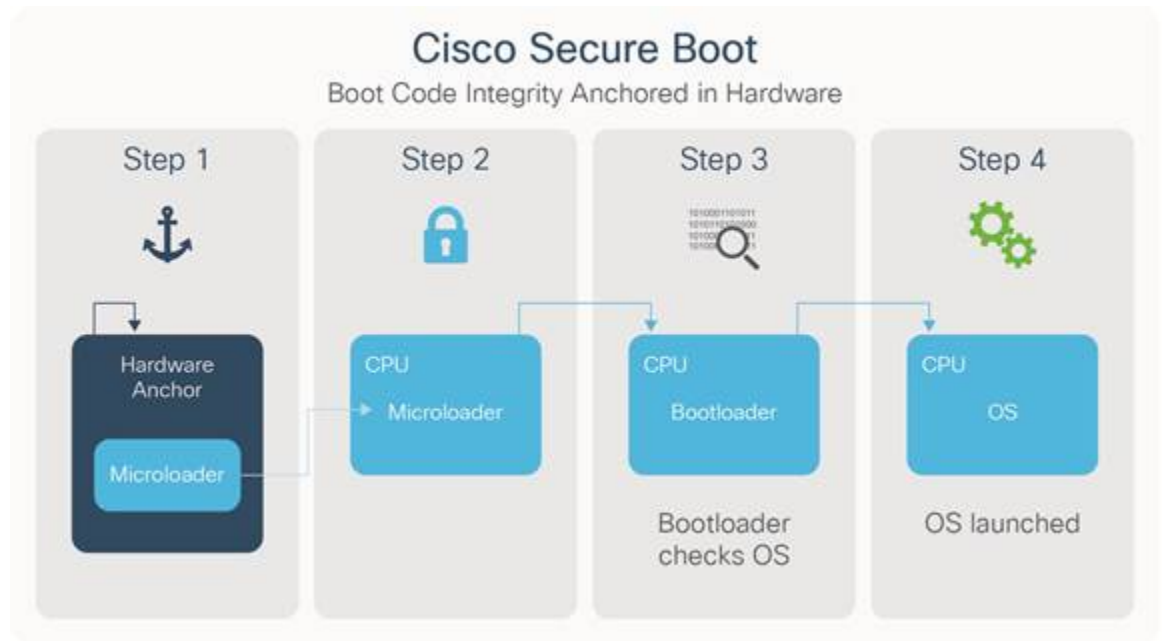
Cisco Secure Boot に関する情報

Cisco Secure Boot サポートは、Cisco MDS NX-OS 8.1(1) 以降のリリースの Cisco MDS 9700 48ポート 32 Gbps ファイバチャネルスイッチング モジュール、Cisco MDS 9132T ファイバチャネルスイッチ、Cisco MDS 9396T ファイバチャネルスイッチ、および Cisco MDS 9148T ファイバチャネルスイッチに導入されました。

シスコのセキュアブートは、シスコ製ハードウェアプラットフォーム上で実行される最初のコードが真正であり、改ざんされていないことを確認します。シスコセキュアブートはマイクロローダーをミュート不可ハードウェアにアンカーリングし、信頼の起点を確立して、シスコのネットワークデバイスが、改ざんされたネットワークソフトウェアを実行するのを防止します。ハードウェアのブートコードを保護し、イメージハッシュを表示し、デバイスのセキュアユニークデバイス ID (SUDI) 証明書を提供します。起動プロセス中にセキュアキーの認証に失敗すると、ラインカードモジュールは起動が機能不全になり、BIOS の改ざんを防ぎます。セキュアブートはデフォルトで有効になっています。

ソフトウェア認証に関して、シスコはハードウェアによるセキュアブートプロセスを実装することによって差別化され、優れた堅牢性を備えたセキュリティを実現します。ハッカーがデバイスを物理的に所有している場合でも、ハードウェアの変更は難しく、コストがかかり、隠蔽も容易ではないため、堅牢です。

シスコのセキュアブート ワークフロー



1. 本物ハードウェアアンカーリングされたセキュアブートの場合により、CPU上で実行される最初の命令は、変更できないハードウェア内に保存されます。
2. デバイスが起動すると、マイクロローダーは、次の一連の指示がシスコからのものかどうかを、その一連の指示にあるシスコのデジタル署名を検証することによって確認します。
3. ブートローダは、オペレーティングシステムがシスコによってデジタル署名されているかどうかを確認することにより、オペレーティングシステムがシスコからのものであることを検証します。
4. すべてのチェックに合格すると、オペレーティングシステムが起動します。デジタル署名チェックが何らかの失敗をした場合、シスコデバイスはそのソフトウェアを起動させず、悪意のあるコードがデバイスに実行されないように確認します。

偽造防止対策について

Cisco MDS NX-OS リリース 8.1 (1) から、偽造防止対策が Cisco MDS 9700 48 ポート 32 Gbps ファイバチャネルスイッチング モジュール、Cisco MDS 9132T ファイバチャネルスイッチ、Cisco MDS 9396T ファイバチャネルスイッチ、および Cisco に導入されました。MDS 9148T ファイバチャネルスイッチ。

偽造防止対策により、Cisco NX-OS ソフトウェアイメージを備えたシスコハードウェアプラットフォームが本物であり、変更されていないことが保証されます。これにより、ハードウェアレベルの信頼のルートと、システムを構築するための不変のデバイス ID が確立されます。

Cisco MDS スイッチは、ACT2 対応の ASIC で構築されています。これにより、対応する SUDI X.509v3 証明書がハードウェアに埋め込まれます。SUDI 証明書、関連付けられたキーペア、その証明書チェーン全体が改ざん防止 Cisco トラストアンカーチップに保存されます。キーペアは特定のチップにバインドされ、秘密キーはエクスポートされません。この機能により、アイデンティティ情報のクローニングやスプーフィングを不可能にします。

SUDI はトラストアンカーモジュール (TAm) に恒久的にプログラムされていて、クローズで、セキュリティ保護され、そして監査されたシスコの製造プロセスにおいてシスコによって記録されます。このプログラミングは強力なサプライチェーンセキュリティを提供します。これは、ルータやスイッチなどの組み込みシステムにとって重要です。

ACT2 認証が失敗すると、エラーメッセージが表示されます：

```
ACT2_AUTH_FAIL: ACT2 test has failed on module 9 with error : ACT2 authentication failure
```

ACT2 認証失敗について支援が必要な場合は、Cisco Technical Assistance Center (TAC) にお問い合わせください。



索引

記号

- * (アスタリスク) [289](#)
 - ポートセキュリティ ワイルドカード* (アスタリスク) [289](#)
 - ポートセキュリティ ワイルドカード [289](#)

数字

- 3DES 暗号化 [219](#)
 - IKE [219](#)
 - IPSec [219](#)

A

- AAA [40, 42-43, 101-102, 105, 109, 111, 113, 116, 273](#)
 - CFS での配信 (手順) [105](#)
 - DHCHAP 認証 [273](#)
 - アカウントサービスの設定 [111, 113](#)
 - エラー対応ステータスの表示 [42](#)
 - 許可プロセス [43](#)
 - サーバーへの配信のイネーブル化 [101-102](#)
 - デフォルト設定 [116](#)
 - 認証プロセス [43](#)
 - 配信セッション TACACS+ の開始 [102](#)
 - 配信セッションの開始 [102](#)
 - リモート サービス [40](#)
 - ローカル サービス AAA [109](#)
 - 認証の設定 [109](#)
- AAA サーバ [40, 42](#)
 - グループ [40](#)
 - モニタリング [42](#)
 - リモート認証 [40](#)
- AAA 認証 [45](#)
 - デフォルト ユーザ ロールのイネーブル化 [45](#)
- Advanced Encrypted Standard 暗号化。「AES 暗号化」を参照してください [219](#)
- AES を使用する Message Authentication Code。
 - 「AES-XCBC-MAC」を参照してください [219](#)
- AES-XCBC-MAC [219](#)
 - IPSec [219](#)

- AES の暗号化 [219](#)
 - IKE [219](#)
 - IPSec [219](#)

C

- CA [139-140, 142-144, 146-147, 151, 154-156, 160, 195](#)
 - identity [140](#)
 - カットアンドペーストによる登録 [143](#)
 - 最大限度 [195](#)
 - 証明書のダウンロード例 [160](#)
 - 設定 [144, 155](#)
 - 設定の表示 [156](#)
 - 設定例 [156](#)
 - 説明 [139, 144](#)
 - デジタル証明書の削除 [154](#)
 - デフォルト設定 [195](#)
 - トラスト ポイントの作成 [146](#)
 - 認証 [147](#)
 - ピア証明書 [143](#)
 - 複数のトラスト ポイント [142](#)
 - 保守 [151](#)
 - 目的 [139](#)
 - モニタリング [151](#)
- Certificate Revocation List。CRL を参照してください [144](#)
- Cisco Access Control Server。「Cisco ACS」を参照 [113](#)
- cisco-av-pair [79](#)
 - SNMPv3 用の指定 [79](#)
- Cisco ACS [113](#)
 - RADIUS での設定 [113](#)
 - TACACS+ の設定 [113](#)
- CRL [144, 148, 154, 185, 187](#)
 - 失効チェック方式の設定 [148](#)
 - 生成の例 [185](#)
 - 設定 [154](#)
 - 説明 [144](#)
 - ダウンロードの例 [187](#)

D

Data Encryption Standard 暗号化。「DES 暗号化」を参照してください [219](#)

DES 暗号化 [219](#)

IKE [219](#)

IPSec [219](#)

DH [219](#)

IKE [219](#)

DHCHAP [263–266, 268–273, 275–276](#)

AAA 認証 DHCHAP [273](#)

AAA 認証の設定 [273](#)

FC-SP[DHCHAP も参照 [263](#)

zzz] [263](#)

グループ設定 [269](#)

セキュリティ情報の表示 [273](#)

設定 [264, 273](#)

設定例 [275](#)

説明 [264](#)

タイムアウト値 [272](#)

デフォルト設定 [276](#)

認証モード [266](#)

ハッシュ アルゴリズム [268](#)

他の SAN-OS 機能との互換性 [265](#)

イネーブル化 [266](#)

ライセンス [264](#)

リモート デバイスのパスワード [271](#)

ローカル スイッチのパスワード [270](#)

Diffie-Hellman Challenge Handshake Authentication Protocol.

「DHCHAP」を参照 [263](#)

Diffie-Hellman プロトコル。「DH」を参照してください [219](#)

DSA キーペア [201](#)

DSA キーペアの生成 [201](#)

生成 [201](#)

E

EFMD [309](#)

ファブリック バインディング [309](#)

Exchange Fabric Membership Data。「EFMD」を参照 [309](#)

E ポート [309](#)

ファブリック バインディングの確認 [309](#)

F

FC-SP [263, 266](#)

DHCHAP[FC-SP も参照 [263](#)

zzz] [263](#)

認証 [263](#)

イネーブル化 [266](#)

FCIP [254, 265](#)

DHCHAP との互換性 [265](#)

FCIP (続き)

IPsec の設定例 [254](#)

Federal Information Processing Standards. See FIPS [9](#)

Fibre Channel Security Protocol。「FC-SP」を参照 [263](#)

FICON [312](#)

ファブリック バインディングの要件 [312](#)

ファブリック バインディング用の sWWN [312](#)

FIPS [9–10](#)

設定時の注意事項 [9](#)

セルフテスト [10](#)

I

ICMP パケット [124](#)

type value [124](#)

ID [78](#)

シスコのベンダー ID [78](#)

IKE [195, 216–217, 219, 224, 232, 249, 260](#)

SA のリフレッシュ [232](#)

暗号化トランスフォーム [219](#)

設定の表示 [249](#)

説明 [216](#)

デジタル証明書のデフォルト設定 [195](#)

デフォルト設定 [195](#)

デフォルト設定 [260](#)

認証アルゴリズム [219](#)

イネーブル化 [224](#)

用語 [217](#)

IKE イニシエータ [231, 249](#)

設定の表示 [249](#)

バージョンの設定 [231](#)

IKE ドメイン [225, 232](#)

クリア [232](#)

設定 [225](#)

IKE トンネル [225, 232](#)

クリア [232](#)

説明 [225](#)

IKE ビア [231, 249](#)

キーブアライブ設定の表示 [249](#)

キーブアライブ タイムの設定 [231](#)

IKE ポリシー [225, 227, 230, 249](#)

現在のポリシーの表示 [249](#)

negotiation [225](#)

ネゴシエーション パラメータの設定 [227](#)

ライフタイム アソシエーションの設定 [230](#)

Internet Key Exchange (インターネットキーエクスチェンジ)。

「IKE」を参照してください [214](#)

IP セキュリティ。「IPsec」を参照してください [214](#)

IPSec [214, 216–217, 219–220, 222, 233, 237–238, 247–248, 250, 254, 259–260](#)

FCIP の設定例 [254](#)

IPSec (続き)

- iSCSI の設定例 [259](#)
- RFC 実装 [214](#)
- 暗号化トランスフォーム [219](#)
- クリプト IPv4-ACL [233, 237](#)
- グローバル ライフタイム値 [248](#)
- サポートされていない機能 [216](#)
- 設定の表示 [250](#)
- 説明 [214](#)
- デジタル証明書のサポート [220, 222](#)
- デフォルト設定 [260](#)
- トランスフォームセット [238](#)
- 認証アルゴリズム [219](#)
- ハードウェアの互換性 [216](#)
- ファブリック設定の要件 [216](#)
- 保守 [247](#)
- 用語 [217](#)

IPsec [224](#)

- licensing requirements [224](#)
- prerequisites [224](#)

IPv4-ACL [121, 129–133, 135–136, 138, 233, 237, 240](#)

- crypto [233, 237](#)
- 暗号マップ エントリ [240](#)
- インターフェイスの設定の確認 [136](#)
- インターフェイスへの適用 [133, 135](#)
- エントリの削除 [130](#)
- エントリの追加 [129](#)
- カウンタのクリア [138](#)
- 設定時の注意事項 [121](#)
- 設定の表示 [131](#)
- ダンプ ログの読み取り [132](#)

IPv6-ACL [120](#)IP ドメイン名 [144](#)

- デジタル証明書の設定 [144](#)

IP フィルタ [120–121](#)

- IP トラフィックの制限 [120](#)
- を提供 [121](#)

iSCSI [259](#)

- IPsec の設定例 [259](#)

M

MD5 認証 [219](#)

- IKE [219](#)
- IPsec [219](#)

Message Digest 5。「MD5 認証」を参照してください [219](#)

Microsoft Challenge Handshake Authentication Protocol。

- 「MSCHAP」を参照 [107](#)

MSCHAP [108](#)

- 説明 [108](#)

O

Open UDP and TCP Ports on Cisco MDS 9000 Series Platforms [137](#)

P

PKI [142](#)

- 登録のサポート [142](#)

R

RADIUS [68–73, 76–77, 80, 98, 101–102, 104–105, 113, 116](#)

- CFS 結合の注意事項 [105](#)
- Cisco ACS の設定 [113](#)
- サーバー グループの設定 [98](#)
- サーバー タイムアウトの指定 [72](#)
- サーバーの指定 [69–70](#)
- サーバー モニタリング パラメータの設定 [73](#)
- 事前共有キーの設定 [71](#)
- 設定されたパラメータの表示 [80](#)
- 設定の配布のイネーブル化 [101–102](#)
- 設定配信セッションの消去 [105](#)
- 設定配信の変更の廃棄 [104–105](#)
- 説明 [68](#)
- タイムアウトの指定 [73](#)
- テスト アイドル タイマーの設定 [76](#)
- テスト ユーザー名の設定 [76](#)
- デフォルト設定 [116](#)
- 配信セッションの開始 [102](#)
- ホスト キーの割り当て [69](#)
- モニタリング用テスト メッセージの送信 [77](#)

RSA キー ペア [140, 144–145, 152, 155–156, 201](#)

- インポート [144, 152](#)
- エクスポート [144, 152](#)
- 削除 [155](#)
- 生成 [145, 201](#)
- 設定の表示 [156](#)
- 説明 [140](#)

S

SA [232, 241, 243, 248–250](#)

- IKE 用の表示 [249](#)
- IPsec ピア間の確立 [241](#)
- グローバル ライフタイム値 [248](#)
- グローバル ライフタイム値の表示 [250](#)
- 更新 [232](#)
- ライフタイム ネゴシエーション [243](#)
- ライフタイムの設定 [243](#)

SHA-1 [219](#)

- IKE [219](#)

SNMP 32-33, 38

- CLI オペレーションのマッピング 33
- セキュリティ機能 38
- ロールの作成 32

SNMPv3 79

- cisco-av-pair の指定 79

SSH 5, 41, 197, 199, 201-202, 205, 207-208

- キーの指定 202
- サーバー キーペアの上書き 205
- サーバー キーペアの生成 5, 201
- ステータスの表示 208
- 説明 5, 197
- デジタル証明書認証 199
- デフォルトのサービス 197
- protocol status 208
- ホストのクリア 207
- イネーブル化 207
- ログイン 41

SSH キー ペア 205

- 上書き 205

SSH クライアント 198

- NX-OS デバイスでのサポート 198

SSH サーバ 198

- NX-OS デバイスでのサポート 198
- キーペアのサポート 198

SSH ログイン試行 204

- 設定 204

sWWN 312-313

- ファブリック バインディングの設定 312-313

T

TACACS+ 84-86, 88-90, 92-94, 96, 99, 101-102, 104-105, 113, 116

- CFS 結合の注意事項 105
- Cisco ACS の設定 113
- グローバル キー 85
- グローバル秘密キーの設定 88
- 検証 93
- サーバー アドレスの設定 85-86
- サーバー グループの設定 99
- サーバー モニタリング パラメータの設定 90
- 事前共有キーの設定 85
- 情報の表示 96
- 設定の配布のイネーブル化 101-102
- 設定配信セッションの消去 105
- 設定配信の変更の廃棄 104-105
- 説明 84
- タイムアウト値の設定 89
- デフォルト設定 116
- デフォルトのサーバー タイムアウトの設定 89
- モニタリング用テスト メッセージの送信 92

TACACS+ (続き)

- イネーブル化 85
- ログイン時にサーバーを指定 94

TCP ポート 123

- IPv4-ACL 123

Telnet 41, 207

- イネーブル化 207
- ログイン 41

Telnet サーバ 199

- NX-OS デバイスでのサポート 199

TE ポート 309

- ファブリック バインディングの確認 309

Triple DES。「3DES 暗号化」を参照してください 219

TrustSec FC Link Encryption 322

- Supported Modules 322

TrustSec FC リンク暗号化 321-324, 326, 328-329

- ESP の設定 324
- ESP モード 326
- Information 328
- セキュリティ アソシエーション 323
- セキュリティ アソシエーションのパラメータ 324
- ベスト プラクティス 329
- イネーブル化 322
- 用語 321

U

UDP ポート 123

- IPv4-ACL 123

V

VSA 78

- 属性の通信 78
- プロトコル オプション 78

VSANs 24, 120, 265

- DHCHAP との互換性 265
- IP ルーティング 120
- ポリシー 24

VSAN ポリシー 24-25, 34

- VSAN のライセンス 24
- ポリシーの設定 24
- デフォルト ロール 34
- 変更 25

W

WWN 291

- ポート セキュリティ 291

あ

- アカウントティング **111, 113**
 - サービスの設定 **111, 113**
- アクセスコントロールリスト。「IPv4-ACL」を参照してください
さい **120**
- 暗号化パスワード **16**
 - ユーザアカウント **16**
- 暗号マップ エントリ **243, 248**
 - SA ライフタイムの設定 **243**
 - グローバル ライフタイム値 **248**
 - グローバル ライフタイム値の設定 **248**

え

- 永続的ドメイン ID **312**
 - FICON VSAN **312**

か

- 管理者パスワード **81**
 - リカバリ手順 **81**

き

- 共通ユーザー **33**
 - SNMP への CLI のマッピング **33**
- 共通ロール **32**
 - 設定 **32**

く

- クリプト IPv4-ACL **233, 236–237, 242**
 - any キーワード **237**
 - クリプト マップ エントリの作成 **242**
 - 作成 **237**
 - 設定時の注意事項 **233**
 - ミラー イメージ **236**
- クリプト マップ **240–246**
 - autopeer オプションの設定 **245**
 - IPv4-ACL のエントリ **240**
 - PFS **246**
 - PFS の設定 **246**
 - SA ライフタイム ネゴシエーション **243**
 - エントリの作成 **242**
 - 自動ピア オプション **244**
 - 設定時の注意事項 **241**
 - ピア間の SA **241**
- クリプト マップ セット **246**
 - インターフェイスへの適用 **246**

- グローバル キー **71**
 - RADIUS への割り当て **71**

さ

- サーバグループ **98–99**
 - 設定 **98–99**

し

- シスコのベンダー ID **78**
 - 説明 **78**
- 事前共有キー **71, 85**
 - RADIUS **71**
 - TACACS+ **85**

す

- スイッチ セキュリティ **34, 116**
 - デフォルト設定 **34, 116**

せ

- セキュリティ **38, 40**
 - アカウントティング **40**
 - スイッチでの管理 **38**
- セキュリティ アソシエーション。「SA」を参照してください
217
- セキュリティ制御 **68, 84, 109**
 - remote **84**
 - リモート AAA サーバー **68**
 - ローカル (local) **109**

て

- デジタル証明書 **139, 143–144, 149–156, 168, 182, 195, 199, 220, 222**
 - CAからの削除 **154**
 - IPSec **220, 222**
 - SSH のサポート **199**
 - アイデンティティ証明書のインストール **150**
 - アイデンティティ証明書の作成要求 **149**
 - アイデンティティ証明書の要求例 **168**
 - インポート **144, 152–153**
 - エクスポート **144, 152–153**
 - 最大限度 **195**
 - 失効の例 **182**
 - 設定 **144, 155**
 - 設定例 **156**
 - 説明 **139, 144**
 - peers **143**
 - 保守 **151**

デジタル証明書 (続き)

目的 [139](#)

モニタリング [151](#)

デジタル署名アルゴリズム (Digital Signature Algorithm)。「DSA キー ペア」を参照 [201](#)

と

トラスト ポイント [140, 142, 146, 151](#)

作成 [146](#)

説明 [140](#)

multiple [142](#)

リポート後の設定の保存 [151](#)

トランスフォーム セット [238–239, 242](#)

IPsec 用の設定 [239](#)

クリプト マップ エントリの作成 [242](#)

説明 [238](#)

に

認証 [39–40, 263](#)

ガイドライン [40](#)

ファブリック セキュリティ [263](#)

ユーザー ID [39](#)

remote [39–40](#)

ローカル (local) [39](#)

ね

ネットワーク オペレータ [39](#)

権限 [39](#)

ネットワーク管理者 [39](#)

権限 [39](#)

追加のロール [39](#)

は

ハイ アベイラビリティ [265](#)

DHCHAP との互換性 [265](#)

パスワード [15–16, 81, 270–271](#)

DHCHAP [270–271](#)

暗号化 [16](#)

強力な特性 [15](#)

リカバリ (手順) [81](#)

ふ

ファイバチャネル [313](#)

ファブリック バインディング用の sWWN [313](#)

ファブリック セキュリティ [263, 276](#)

デフォルト設定 [276](#)

認証 [263](#)

ファブリック バインディング [265, 309, 311, 314–317, 320](#)

DHCHAP との互換性 [265](#)

EFMD [309](#)

Ex ポートの確認 [309](#)

アクティブ化 [314](#)

強制 [311](#)

強制的なアクティベーション [315](#)

設定 [311, 317](#)

設定の確認 [317](#)

設定の保存 [316](#)

説明 [309, 311](#)

データベースの削除 [317](#)

デフォルト設定 [320](#)

統計情報のクリア [316](#)

ポート セキュリティの比較 [309](#)

ライセンス要件 [309](#)

プロファイル [19, 23](#)

設定 [19](#)

変更 [23](#)

へ

ベンダー固有属性「VSA」を参照 [78](#)

ほ

ポート セキュリティ [211, 265, 279–285, 291–293, 296–301, 304, 307, 309](#)

CFS 配信の設定 [293, 296](#)

DHCHAP との互換性 [265](#)

WWN の識別 [291](#)

アクティブ化 [281, 284](#)

アクティブ化の拒否 [285](#)

アクティベーションの強制 [285](#)

許可済みのペアの追加 [292](#)

実行メカニズム [280](#)

自動学習 [280](#)

手動設定時の注意事項ポート セキュリティ データベース [283](#)

手動設定に関する注意事項 [283](#)

設定時の注意事項 [282](#)

設定の表示 [301, 307](#)

設定の表示ポート セキュリティ [301, 307](#)

設定の表示 [301, 307](#)

ディセーブル化 [284](#)

データ シナリオポート セキュリティ データベース [298](#)

シナリオ [298](#)

ポートセキュリティ (続き)

- データベース結合の注意事項ポートセキュリティ データベース **297**
- 結合の注意事項 **297**
- データベースのクリーンアップポートセキュリティ データベース **300**
- クリーンアップ **300**
- データベースのコピーポートセキュリティ データベース **299**
- コピー **299**
- データベースの削除ポートセキュリティデータベース **300**
- 削除 **300**
- データベースの相互作用ポートセキュリティ データベース **298**
- 連携動作 **298**
- デフォルト設定 **211, 304**
- 非アクティブ化 **284**
- ファブリック バインディングとの比較 **309**
- 不正アクセスの防止ポートセキュリティ **279**
- 不正アクセスの防止 **279**
- イネーブル化 **284**
- ライセンス要件 **279**
- ポートセキュリティ データベース **286, 301, 307**
- 違反の表示 **301**
- 再アクティブ化 **286**
- 設定の表示 **301, 307**
- ポートセキュリティの自動学習 **280, 282, 287–288, 296**
- CFS を使用する場合の設定に関する注意事項 **282**
- 設定の配信 **296**
- 説明 **280**
- ディセーブル化 **288**
- デバイス許可 **288**
- イネーブル化 **287**
- ポートチャンネル **265**
- DHCHAP との互換性 **265**
- ホストキー **69**
- 割り当て **69**
- ホスト名 **144**
- デジタル証明書の設定 **144**

ゆ

- ユーザ **13, 16–17**
- アカウント情報の表示 **17**
- 削除 **16**
- 設定 **16**

ユーザ (続き)

- 説明 **13**
- 他のユーザーのログアウト **17**
- ユーザー ID **39**
- 認証 **39**
- ユーザアカウント **13, 15, 17, 19**
- 情報の表示 **17**
- 設定 **13**
- パスワードの特性 **15**
- プロファイルの設定 **19**
- ロールの設定 **19**
- ユーザ プロファイル **39**
- ロール情報 **39**

る

- ルール **21**
- 設定 **21**

ろ

- ロール **19, 21, 23, 26, 28, 30, 32, 34, 39**
- 共通ロールの参照 **32**
- zzz] **32**
- 情報の表示 **28**
- 設定 **19**
- 設定の配布 **26, 30**
- デフォルト権限 **39**
- デフォルト設定 **34**
- プロファイルの変更 **23**
- ユーザ プロファイル **39**
- ロールの設定 **21**
- ロール データベース **26–28, 30**
- Fabric Manager での表示 **30**
- 結合の注意事項 **28**
- 情報の表示 **28**
- 説明 **26**
- データベース変更の破棄 **27**
- 配信のイネーブル化 **27**
- 配信のディセーブル化 **27**
- 配布セッションのクリア **28**
- ファブリックのロック **26**
- ファブリックへの変更のコミット **27**
- ログイン **41**
- SSH **41**
- Telnet **41**

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。

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。