



INDEX

C

close-notify メッセージ、送信 3-14, 4-14, 4-15

CSR パラメータ セット

E メールアドレス 2-13

概要 2-7

国 2-10

作成 2-8

州または行政区分 2-10

詳細レポートおよび要約レポートの表示
6-2

シリアル番号 2-11

組織名 2-12

組織ユニット 2-12

地域 2-11

通常名 2-9

P

PKI 1-3

R

RSA 鍵ペア

概要 1-4

生成 2-6

説明 2-3

S

SSL

ACE の機能の概要 1-10

PKI の概要 1-3

RSA 鍵ペア 1-4

URL リライト、設定 3-31

エンドツーエンド

概要 5-2

開始

概要 4-2

設定 4-6

開始の設定例 4-32

概要 1-1

鍵と証明書の生成 2-6

基本 ACE 設定 1-10

グローバル サイト証明書、準備 2-16

公開鍵インフラストラクチャ (PKI) 1-3

終了

概要 1-11, 3-2

設定 3-5

終了の設定例 3-42

仕様 1-8

証明書 1-4, 2-17

証明書署名要求

グローバル サイト 2-15

生成 2-14

- 設定の前提条件 1-13
 - 設定フロー図
 - SSL 開始 4-4
 - SSL 終了 3-3
 - エンドツーエンド SSL 5-4
 - 統計情報 6-14
 - パラメータ マップ
 - SSL/TLS バージョンの定義 3-15
 - 暗号スイートの追加 3-10
 - 作成 3-8
 - 失効したサーバ証明書または無効なサーバ証明書の無視 3-14, 4-14
 - ハンドシェイク 1-6
 - プロキシ サービス
 - SSL パラメータ マップの関連付け 3-20
 - プロキシ サービス (クライアント)
 - SSL パラメータ マップの関連付け 4-19
 - サーバ認証のイネーブル化 4-19
 - 作成、SSL 開始 4-18
 - プロキシ サービス (サーバ)
 - 鍵ペアの指定 3-20
 - クライアント認証のイネーブル化 3-23
 - 作成、SSL 終了 3-19
 - 証明書チェーン グループの指定 3-22
 - 証明書の指定 3-21
 - SSL 開始のプロキシ サービス (クライアント) 4-18
 - SSL 終了のプロキシ サービス (サーバ) 3-19
 - SSL 証明書のアップグレード 2-22
- T
- 統計情報 6-14
- U
- URL
 - リライト、設定 3-31
- あ
- アクション リスト
 - ポリシー マップと関連付け 3-35
 - 暗号スイート
 - サポート 3-13
 - 指定 3-10, 4-11
- え
- エンドツーエンド SSL 5-2
- か
- 鍵ペア ファイル
 - 証明書および鍵ペア ファイルの表示 6-4
 - 要約レポートおよび詳細レポートの表示 6-10
 - 鍵 (SSL)
 - インポートまたはエクスポート 2-17
 - 概要 1-3
 - 鍵交換 1-3
 - 冗長構成での同期化 2-3

- き
- 機密性 1-3
 - キュー遅延時間、設定 3-16
- く
- クイック スタート
 - SSL 開始 4-6
 - SSL 終了 3-5
 - エンドツーエンド SSL 5-6
 - クライアント認証
 - CRL の使用 3-24
 - イネーブル化 3-23
 - クラス マップ
 - レイヤ 3 およびレイヤ 4、SSL 開始 4-26
 - レイヤ 3 およびレイヤ 4、SSL 終了 3-36
 - レイヤ 7、SSL 開始 4-21
 - クローズ プロトコルの動作、定義 3-14, 4-14, 4-15
- さ
- サーバ認証、認証グループの使用 4-19
- し
- 冗長性
 - 証明書と鍵の同期化 2-3
 - 証明書失効リスト (CRL)
 - 拒否 3-18
 - クライアント認証での使用 3-24
 - ダウンロード 3-25
 - 証明書チェーン グループ
 - 作成 2-25
 - 要約レポートおよび詳細レポートの表示 6-12
 - 証明書ファイル
 - 証明書および鍵ペア ファイルの表示 6-4
 - 要約レポートおよび詳細レポートの表示 6-5
 - 証明書 (SSL)
 - アップグレード 2-22
 - インポートまたはエクスポート 2-17
 - 概要 1-3
 - グローバル サイト証明書 2-15
 - グローバル サイトの準備 2-16
 - 公開鍵の確認 2-23
 - サブジェクト 1-4, 2-2
 - 失効したサーバ証明書または無効なサーバ証明書の無視 3-14, 4-14
 - 冗長構成での同期化 2-3
 - 証明書署名要求、生成 2-14
 - チェーンニング 1-5
 - チェーン 2-25
 - 認証グループの作成 2-27
 - 発行元 1-4, 2-2
 - ルート認証局 1-5
- せ
- セッション ID 再利用キャッシュ タイムアウト、設定 3-17, 4-17
 - セッション キャッシュ情報のクリア 3-18
 - 設定例
 - SSL 開始 4-32

SSL 終了 3-42

ち

チェーン グループ 2-25

と

統計情報

SSL と TLS 6-14

ドメイン

名前検索リスト、設定 3-29

名前、デフォルト設定 3-28

ネーム サーバ、設定 3-29

ロックアップ、イネーブル化 3-27

ドメイン ネーム システム (DNS) クライアント、
設定 3-27

に

認証 1-4

グループ、証明書の設定 2-27

認証局 1-4

認定者名

概要 2-7

設定 2-8

は

バージョン、SSL または TLS を定義 3-15, 4-16

ほ

ポリシー マップ

レイヤ 3 およびレイヤ 4

SSL プロキシ サービスの関連付け
3-39

クラス マップの関連付け 3-38, 4-28

作成 3-37, 4-27

すべての VLAN へのグローバル適用
3-40, 4-30

特定の VLAN への適用 3-41, 4-31

レイヤ 7 ポリシー マップの関連付け
4-28

レイヤ 7

SLB ポリシー アクションの指定
4-24

クラス マップの関連付け 4-23

作成 4-22

め

メッセージ整合性 1-5

メッセージ認証コード (MAC) 1-2, 1-6