CHAPTER 2

仮想コンテキストの設定

Cisco Application Control Engine Appliance Device Manager（ACE Appliance Device Manager）には、ACE Appliance の作成、設定、管理に関する数多くのオプションがあります。

これらのオプションの詳細については、次の項目を参照してください。

仮想コンテキストの使用

仮想コンテキストでは、ACE Appliance を複数の仮想デバイスやコンテキストに分割するバーチャライゼーション コンセプトを使用しています。各コンテキストにポリシー、インターフェイス、リソース、および管理者の専用セットを与えます。この機能により、より緊密で効率的にリソース、ユーザ、およびお客様に提供するサービスを管理できます。

仮想コンテキストを初めて使用すると、Admin コンテキストだけが表示されます。他の仮想コンテキストの設定可能アトリビュートのほかに、Admin コンテキストでは次のものを設定できます。

- ACE Appliance ライセンス
- リソース クラス
- ポート チャネル、管理、およびギガビット イーサネット インターフェイス
- ハイ アベイラビリティ（ACE Appliance 間の HA または耐障害性）

- ACE Appliance でのアプリケーション アクセラレーションおよび最適化

関連トピック

- 「仮想コンテキストの作成」（P.2-2）
- 「仮想コンテキストの設定」（P.2-4）
- 「仮想コンテキストの削除」（P.2-60）

仮想コンテキストの作成

この手順を使用して仮想コンテキストを作成します。

（注） Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）アクセス用に管理 VLAN を設定していない場合、ACE Appliance Device Manager でコンテキストをポーリングできません。

（注） ACE Appliance がハイ アベイラビリティ ペアでホットスタンバイとして設定されている場合、その設定を変更することはできず、仮想コンテキストの追加や修正を行えません。*ホットスタンバイ メンバー*として設定されている　ACE Appliance では、[All Virtual Contexts] テーブル（[**Config**] > [**Virtual Contexts**]）内にある [HA State] 列に [Standby Hot] と表示されます。詳細については、「ハイ アベイラビリティ ポーリング」（P.9-6）を参照してください。

手順

ステップ 1　[**Config**] > [**Virtual Contexts**] を選択します。[All Virtual Contexts] テーブルが表示されます。

ステップ 2　[**Add**] をクリックします。[New Virtual Context] 画面が表示されます。

ステップ 3　表 2-1 内の情報を使用して仮想コンテキストを設定します。

ヒント 2 ～ 3 の選択肢のあるフィールドではラジオ ボタンを使用します。3 つを超える選択肢のあるフィールドでは、ドロップダウン リストを使用します。

表 2-1　仮想コンテキスト設定アトリビュート

フィールド	説明
[Name]	仮想コンテキストの一意の名前を入力します。有効な値は、スペースを含まない引用符抜きの英数字です（最大 64 文字）。 このフィールドは、既存コンテキストの場合読み取り専用です。
[Resource Class]	この仮想コンテキストが使用するリソース クラスを選択します。

表 2-1　仮想コンテキスト設定アトリビュート （続き）

フィールド	説明
[Allocate-Interface VLANs]	コンテキストが関連トラフィックを受信できるように VLAN または VLAN 範囲の番号を入力します。次のいずれかの方法で VLAN を指定できます。 • 単一 VLAN の場合、2 ～ 4096 の整数を入力します。 • 複数の、非連続の VLAN の場合、`101, 201, 302` というような形のカンマ区切りを使用して入力します。 • VLAN 範囲の場合、フォーマット <*最初の VLAN*>-<*最後の VLAN*> を使用します（たとえば `101-150`）。 **（注）** VLAN は Admin コンテキストで変更できません。
説明	仮想コンテキストの簡単な説明を入力します。
[Shared VLAN Host ID]	ACE により使用される具体的な MAC アドレス バンクを入力します。1 ～ 16 の数値を入力してください。必ず、複数の ACE に対して異なるバンク番号を設定してください。
[Policy Name]	新しい管理 VLAN の場合、管理ポリシー名を入力します。このフィールドは、既存コンテキストの場合読み取り専用です。
[Management VLAN]	コンテキストのリモート管理に使用される VLAN を入力します。
[Management IP]	コンテキストのリモート管理に使用される IP アドレスを入力します。 **（注）** VLAN インターフェイスに管理ポリシー マップが関連付けられている場合、Device Manager はそのインターフェイスを管理インターフェイスと見なします。「VLAN インターフェイス ポリシー マップ使用の設定」（P.8-10）を参照してください。
[Management Netmask]	この IP アドレスに適用するサブネット マスクを選択します。
[Protocols To Allow]	この VLAN で許可されているプロトコルを選択します。 • [HTTP] : Hypertext Transfer Protocol （HTTP）を指定します。 • [HTTPS] : ポート 443 を使用した ACE Appliance Device Manager インターフェイスとの接続に セキュア（SSL）Hypertext Transfer Protocol （HTTP）を指定します。 • [ICMP] : ICMP （通常、ping を意味します）を指定します。 • [KALAP-UDP] : Keepalive Appliance Protocol over UDP を指定します。 • [SNMP] : 簡易ネットワーク管理プロトコル（SNMP）を指定します。 **（注）** SNMP が選択されていない場合、ACE Appliance Device Manager はコンテキストをポーリングできません。 • [SSH] : ACE Appliance との接続に Secure Shell（SSH; セキュア シェル）を指定します。 • [TELNET] : ACE Appliance との接続に Telnet を指定します。 • [XML-HTTPS] : ACE Appliance と Network Management System（NMS; ネットワーク管理システム）間における XML 文書の送受信に使う転送プロトコルに HTTPS を指定します。通信はポート 10443 を使用して実行されます。 プロトコル選択中に Shift キーを押すことで、複数のプロトコルを選択できます。

表 2-1　仮想コンテキスト設定アトリビュート （続き）

フィールド	説明
[Default Gateway IP]	デフォルト ゲートウェイの IP アドレスを入力します。`192.168.65.1, 192.168.64.2` のように、複数の IP アドレスを指定するのにカンマ区切りのリストを使用します。 すでに ACE Appliance で設定された、ネットマスクのある IP アドレスが 0.0.0.0 のデフォルト スタティック ルートがこのフィールドに表示されます。
[SNMP v2c Read-Only Community String]	SNMP が許可プロトコルの 1 つである場合、SNMPv2c コミュニティ ストリングを使用するように入力します。 （注）　SNMP が許可されていないプロトコルの場合、ACE Appliance Device Manager はコンテキストをポーリングできません。

ステップ 4　次のいずれかをクリックします。

- [**Deploy Now**]：この仮想コンテキストを配置します。別の仮想コンテキスト アトリビュートを設定するには、「仮想コンテキストの設定」（P.2-4）を参照してください。
- [**Cancel**]：エントリを保存せずにこの手順を終了して、[All Virtual Contexts] テーブルに戻ります。

関連トピック

- 「仮想コンテキストの使用」（P.2-1）
- 「仮想コンテキストの設定」（P.2-4）

仮想コンテキストの設定

仮想コンテキストの作成後、これを設定できます。仮想コンテキストの設定には、*設定サブセット*にグループ化された、多くのアトリビュートの構成が必要です。表 2-2 は、ACE Appliance Device Manager の設定サブセットを示したもので、関連トピックへのリンクも示しています。

（注）　ACE Appliance がハイ アベイラビリティ ペアでホットスタンバイとして設定されている場合、その設定を変更することはできず、仮想コンテキストの追加や修正を行えません。*ホットスタンバイ メンバー*として設定されている　ACE Appliance では、[All Virtual Contexts] テーブル（[**Config**] > [**Virtual Contexts**]）内にある [HA State] 列に [Standby Hot] と表示されます。詳細については、「ハイ アベイラビリティ ポーリング」（P.9-6）を参照してください。

（注）　実サーバやサーバ ファームなどのオブジェクトをカスタマイズ済みドメインに追加するには、CLI を使用してから、ACE Appliance Device Manager の同期機能を使用してこのオブジェクトを ACE Appliance Device Manager のカスタマイズ済みドメインに追加します。ACE Appliance Device Manager 内でオブジェクトをカスタマイズ済みドメインに直接追加すると、オブジェクトはデフォルト ドメインに追加されます。

同期オプションは、[All Virtual Contexts] テーブルで利用可能です（[**Config**] > [**Virtual Contexts**]）。

ヒント　2 ～ 3 の選択肢のあるフィールドではラジオ ボタンを使用します。3 つを超える選択肢のあるフィールドでは、ドロップダウン リストを使用します。

表 2-2　ACE Appliance および仮想コンテキスト設定オプション

設定サブセット	説明	関連トピック
システム	システム設定オプションにより、次のことが設定可能です。 • VLAN、SNMP アクセス、およびリソース クラスなどのプライマリ アトリビュート • ログされる syslog メッセージのタイプや重大度、syslog ログ ホスト、ログ メッセージ、ログ レート制限を含む、Syslog アトリビュート • SNMP オプション • 仮想コンテキスト上の全 VLAN に対するグローバル ポリシー マップ設定 • ACE Appliance で使用する ACE Appliance ライセンス • ACE Appliance リソース割り当てのリソース クラス • ACE Appliance でのアプリケーション アクセラレーションおよび最適化 **（注）** ACE Appliance ライセンス、リソース クラス、アクセラレーションおよび最適化は、Admin コンテキストだけで設定可能です。	• 「仮想コンテキスト プライマリ アトリビュートの設定」（P.2-8） • 「仮想コンテキスト syslog ロギングの設定」（P.2-9） • 「仮想コンテキストの SNMP 設定」（P.2-16） • 「仮想コンテキスト グローバル トラフィック ポリシーの設定」（P.2-23） • 「ACE Appliance ライセンスの管理」（P.2-24） • 「リソース クラスの管理」（P.2-29） • 「グローバル アプリケーション アクセラレーションおよび最適化の設定」（P.11-10）

表 2-2　ACE Appliance および仮想コンテキスト設定オプション （続き）

設定サブセット	説明	関連トピック
ロード バランシング	ロード バランシング アトリビュートで可能なことは次のとおりです。 • ロード バランシングに対する仮想サーバ、実サーバ、およびサーバ ファームの設定 • プレディクタ方式およびリターン コード チェックの確立 • セッション固定に対するスティッキ グループの実装 • ポリシー マップの関連アクションを組み合わせるためのパラメータ マップの設定 ロード バランシング設定オプションには、次のものがあります。 • 仮想サーバ • 実サーバ • サーバ ファーム • ヘルス モニタリング • スティッキ アトリビュート • パラメータ マップ	• 「ロード バランシングの概要」（P.3-1） • 「仮想サーバの設定」（P.3-2） • 「サーバ ファームの設定」（P.4-11） • 「実サーバに対するヘルス モニタリングの設定」（P.4-26） • 「スティッキ グループの設定」（P.5-6） • 「パラメータ マップの設定」（P.6-1）
SSL	SSL 設定オプションにより、次のことが可能になります。 • SSL 認証およびキーのインポートとエクスポート • SSL パラメータ マップのセットアップおよびグループ パラメータのチェーン • 認証局への登録に関する証明書署名依頼の生成 • ピア証明書の認証 • クライアント認証中に使用する証明書失効リストの設定	• 「SSL の設定」（P.7-1） • 「SSL 証明書の使用」（P.7-6） • 「SSL 鍵の使用」（P.7-9） • 「CSR の生成」（P.7-21） • 「SSL パラメータ マップの設定」（P.7-17） • 「SSL チェーン グループ パラメータの設定」（P.7-19） • 「SSL プロキシ サービスの設定」（P.7-22） • 「SSL 証明書グループの設定」（P.7-24） • 「クライアント認証での CRL の設定」（P.7-25）
セキュリティ	セキュリティ設定オプションにより、アクセス制御リストの作成、Access Control List（ACL; アクセス コントロール リスト）アトリビュートの設定、ACL のリシーケンス、ACL の削除、オブジェクト グループの設定が可能になります。	• 「仮想コンテキスト エキスパート オプション設定」（P.2-55） • 「ACL の作成」（P.2-38） • 「オブジェクト グループの設定」（P.2-47）

表 2-2　ACE Appliance および仮想コンテキスト設定オプション （続き）

設定サブセット	説明	関連トピック
ネットワーク	ネットワーク設定オプションにより、次のことが設定可能です。 • ポート チャネル インターフェイス • ギガビット イーサネット インターフェイス • VLAN インターフェイス • BVI インターフェイス • スタティック ルート • DHCP リレー エージェント （注）　ポート チャネルおよびギガビット イーサネット インターフェイスは、Admin コンテキストだけで設定できます。	• 「仮想コンテキスト BVI インターフェイスの設定」（P.8-15） • 「ギガビット イーサネット インターフェイスの設定」（P.8-3） • 「仮想コンテキスト VLAN インターフェイスの設定」（P.8-6） • 「仮想コンテキスト BVI インターフェイスの設定」（P.8-15） • 「仮想コンテキスト スタティック ルートの設定」（P.8-17） • 「グローバル IP DHCP の設定」（P.8-18）
ハイ アベイラビリティ	ハイアベイラビリティ（HA）アトリビュートにより、フォルトトレラント冗長性に対して 2 つの ACE Appliance を設定できます。 （注）　ハイ アベイラビリティは管理仮想コンテキストだけで設定できます。	• 「ハイ アベイラビリティの設定」（P.9-1） • 「ハイ アベイラビリティ ピアの設定」（P.9-8） • 「ACE ハイ アベイラビリティ グループの設定」（P.9-11）
HA トラッキングおよび障害検出	HA トラッキングおよび障害検出アトリビュートにより、信頼できる耐障害性を確保するのに役立つトラッキング プロセスを設定できます。	• 「ハイ アベイラビリティ トラッキングおよび障害検出の概要」（P.9-16） • 「ハイ アベイラビリティ対応 VLAN インターフェイスのトラッキング」（P.9-17） • 「ハイ アベイラビリティ対応ホストのトラッキング」（P.9-18）
エキスパート	エキスパート オプションにより、次のことが可能になります。 • ACE Appliance を通じて受信または渡されたトラフィックのフィルタリングと処理のトラフィック ポリシー設定 • 最適化アクション リストの設定 • HTTP ヘッダー修正アクション リストの設定	• 「トラフィック ポリシーの設定」（P.10-1） • 「HTTP 最適化アクション リストの設定」（P.11-4） • 「HTTP ヘッダー修正アクション リストの設定」（P.10-84）

仮想コンテキスト システム アトリビュートの設定

表 2-3 は、ACE Appliance Device Manager 仮想コンテキスト システム設定オプションと詳細情報の関連トピックを示したものです。

表 2-3　仮想コンテキスト システム設定オプション

システム設定オプション	関連トピック
仮想コンテキスト プライマリ アトリビュートの指定	「仮想コンテキスト プライマリ アトリビュートの設定」（P.2-8）
syslog オプションの指定	• 「仮想コンテキスト syslog ロギングの設定」（P.2-9） • 「syslog ログ ホストの設定」（P.2-13） • 「syslog ログ メッセージの設定」（P.2-14） • 「syslog ログ レート制限の設定」（P.2-15）
SNMP オプションの設定	• 「仮想コンテキストの SNMP 設定」（P.2-16） • 「SNMPv2c コミュニティの設定」（P.2-17） • 「SNMPv3 ユーザの設定」（P.2-18） • 「SNMP トラップ宛先ホストの設定」（P.2-20） • 「SNMP 通知の設定」（P.2-21）
仮想コンテキスト上の全 VLAN に対するグローバル ポリシー マップの確立	「仮想コンテキスト グローバル トラフィック ポリシーの設定」（P.2-23）
ACE Appliance ライセンスの管理	「ACE Appliance ライセンスの管理」（P.2-24）
仮想コンテキスト全体での ACE Appliance リソースの管理	「リソース クラスの管理」（P.2-29）
ACE Appliance のアプリケーション アクセラレーションおよび最適化の確立	「グローバル アプリケーション アクセラレーションおよび最適化の設定」（P.11-10）

仮想コンテキスト プライマリ アトリビュートの設定

プライマリ アトリビュートは、各仮想コンテキストの名前とリソース クラスを指定します。この情報を提供した後、インターフェイス、モニタリング、ロード バランシングなど他のアトリビュートを設定できます。設定オプションの全リストについては、「仮想コンテキストの設定」（P.2-4）を参照してください。

この手順を使用して仮想コンテキスト プライマリ アトリビュートを設定します。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [System] > [Primary Attributes]** を選択します。[Primary Attributes] 設定画面が表示されます。

ステップ 2　表 2-1 の説明に従って、この仮想コンテキストのプライマリ アトリビュートを入力します。

ステップ 3　**[Deploy Now]** をクリックして、ACE Appliance にこの設定を導入します。

入力を受け入れずにこの手順を終了するには、別の設定オプションを選択します。

関連トピック

- 「仮想コンテキストの使用」（P.2-1）
- 「仮想コンテキスト VLAN インターフェイスの設定」（P.8-6）
- 「仮想コンテキスト BVI インターフェイスの設定」（P.8-15）
- 「仮想コンテキスト syslog ロギングの設定」（P.2-9）
- 「トラフィック ポリシーの設定」（P.10-1）

仮想コンテキスト syslog ロギングの設定

ACE Appliance Device Manager は、syslog ロギングを使用して、メッセージを生成したプロセスとは非同期で指定場所にメッセージを記録するプロセスにログ メッセージを送信します。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [System] > [Syslog]** を選択します。[Syslog] 設定画面が表示されます。

ステップ 2　表示されるフィールドに syslog ロギング アトリビュートを入力します（表 2-5 を参照）。

syslog の重大度レベルを選択する必要のある全フィールドでは表 2-4 内の値を使用します。

表 2-4　syslog ロギング レベル

重大度	説明
0：Emergency	使用不能なシステム
1：Critical	クリティカルな状態
2：Warning	警告状態
3：Alert	即座のアクションが必要
4：Error	エラー状態
5：Notification	通常ではあるものの注目すべき状態
6：Information	情報メッセージだけ
7：Debug	デバッグ中だけ表示

指定する重大度は、そのレベル以上の重大度を持つ syslog メッセージを送信する必要があることを示します。たとえば [Error] を指定した場合、syslog には [Error]、[Critical]、[Alert]、[Emergency] メッセージが表示されます。

（注）　すべての syslog のレベルを [Debug] に設定した場合、**switchover** などのコマンドは正常に処理されません。これらのコマンドは、CLI を介して発行され、[Debug] レベルがイネーブルの場合 ACE Appliance Device Manager は返されたプロンプトを解析できません。代わりに、タイムアウト メッセージが表示されます。

syslog レベルを [Debug] に設定し、タイムアウト メッセージとなるコマンドを発行した場合、**[Refresh]** をクリックして操作の結果を表示します。

（注）　通常操作中にすべての syslog レベルを [Debug] に設定すると、全体のパフォーマンスが低下する可能性があります。

表 2-5　仮想コンテキスト syslog 設定アトリビュート

フィールド	説明	処理
[Enable Syslog]	このオプションは、syslog ロギングがイネーブルかディセーブルかを示します。	チェックボックスをオンにして syslog ロギングをイネーブルにするか、チェックボックスをクリアして syslog ロギングをディセーブルにします。
[Facility]	syslog デーモンは、指定された syslog ファシリティを使用して受信したメッセージの処理方法を決定します。メッセージ内のファシリティ番号に基づいた syslog サーバ ファイルまたは直接メッセージです。 syslog デーモンおよびファシリティ レベルの詳細については、syslog デーモンの文書を参照してください。	ネットワークに最適なファシリティを入力します。 有効な入力は 16（LOCAL0）～ 23（LOCAL7）です。ACE Appliance のデフォルトは 20（LOCAL4）です。
[Buffered Level]	このオプションにより、ローカル バッファへのシステム ロギングが可能になり、重大度に基づいてバッファへ送信されるメッセージが制限されます。	システム ログ メッセージをローカル バッファへ送信する必要なレベルを選択します。 このオプションはデフォルトでディセーブルです。
[Console Level]	このオプションは、コンソールに送信されるシステム ログ メッセージの最大レベルを指定します。	システム ログ メッセージをコンソールへ送信する必要なレベルを選択します。 このオプションはデフォルトでディセーブルです。 （注）　コンソールへのロギングは、システム パフォーマンスを低下させる可能性があります。したがって、テストや問題のデバッグ時にだけコンソールへメッセージを記録することを推奨します。ACE Appliance のパフォーマンスが低下する可能性があるため、ネットワークがビジーの場合にこのオプションを使用しないでください。

表 2-5　仮想コンテキスト syslog 設定アトリビュート （続き）

フィールド	説明	処理
[History Level]	このオプションは、SNMP 管理ステーションへトラップとして送信されるシステム ログ メッセージの最大レベルを指定します。	SNMP ネットワーク管理ステーションへトラップとしてシステム ログ メッセージを送信する必要なレベルを選択します。 このオプションはデフォルトでディセーブルです。 （注）　SNMP の設定の詳細については、「SNMP 通知の設定」（P.2-21）を参照してください。
[Monitor Level]	このオプションは、ACE Appliance でセキュア シェル（SSH）または Telnet を使用してリモート接続へ送信されるシステム ログ メッセージの最大レベルを指定します。	ACE Appliance で SSH または Telnet を使用してリモート接続へシステム ログ メッセージを送信する必要レベルを選択します。 このオプションはデフォルトでディセーブルです。 （注）　このオプションが機能するために、ACE Appliance でリモート アクセスをイネーブル化して、PC から SSH または Telnet プロトコルを使用してリモート接続を確立する必要があります。
[Persistence Level]	このオプションは、フラッシュ メモリに送信されるシステム ログ メッセージの最大レベルを指定します。	システム ログ メッセージをフラッシュ メモリへ送信する必要なレベルを選択します。 このオプションはデフォルトでディセーブルです。 （注）　ACE Appliance において高レートでフラッシュ メモリにロギングするとパフォーマンスに影響があるため、3 などの低めの重大度を使用することをお勧めします。
[Trap Level]	このオプションは、syslog サーバに送信されるシステム ログ メッセージの最大レベルを指定します。	システム ログ メッセージを syslog サーバへ送信する必要なレベルを選択します。 このオプションはデフォルトでディセーブルです。
[Queue Size]	このオプションは、処理を待機中に ACE Appliance 内の他のプロセスから受信する syslog メッセージを格納するためのバッファのサイズを指定します。キューが指定の値を超過した場合、超過したメッセージは廃棄されます。	必要なキュー サイズを入力します。 有効な入力は 0 ～ 8192 メッセージです。 デフォルト値は 100 メッセージです。
[Enable Timestamp]	このオプションは、syslog メッセージにメッセージが生成された日付と時刻が含まれているかどうかを示します。	チェックボックスをオンにして syslog メッセージでタイムスタンプをイネーブルにするか、チェックボックスをクリアして syslog メッセージでタイムスタンプをディセーブルにします。 このオプションはデフォルトでディセーブルです。

表 2-5　仮想コンテキスト syslog 設定アトリビュート （続き）

フィールド	説明	処理
[Enable Standby]	このオプションは、フェールオーバー スタンバイ ACE Appliance でロギングをイネーブルにするかどうかを示します。イネーブルの場合: • この機能により、syslog サーバへのメッセージ トラフィックが 2 倍になります。 • フェールオーバー発生時にはスタンバイ ACE Appliance syslog メッセージは同期したままになります。	チェックボックスをオンにしてフェールオーバー スタンバイ ACE Appliance でロギングをイネーブルにするか、チェックボックスをクリアしてフェールオーバー スタンバイ ACE Appliance でロギングをディセーブルにします。
[Enable Fastpath Logging]	このオプションは、接続のセットアップおよびティアダウン メッセージがログされるかどうかを示します。	チェックボックスをオンにしてセットアップおよびティアダウン メッセージのロギングをイネーブルにするか、チェックボックスをクリアしてセットアップおよびティアダウン メッセージのロギングをディセーブルにします。 このオプションはデフォルトでディセーブルです。
[Device Id Type]	このオプションは、syslog サーバに送信される syslog メッセージが含まれる一意のデバイス ID のタイプを指定します。 デバイス ID は、EMBLEM フォーマット化されたメッセージ、SNMP トラップ、ACE Appliance コンソール、管理セッション、またはバッファで表示されません。	使用されるデバイス ID のタイプを選択します。 • [Any String]：テスト文字列を使用して、ACE Appliance から送信された syslog メッセージを一意に識別することを示します。 • [Context Name]：現在の仮想コンテキスト名を使用して、ACE Appliance から送信される syslog メッセージを一意に識別することを示します。 • [Host Name]：ACE Appliance のホスト名を使用して、ACE Appliance から送信される syslog メッセージを一意に識別することを示します。 • [Interface]：インターフェイスの IP アドレスを使用して、ACE Appliance から送信される syslog メッセージを一意に識別することを示します。 • [Undefined]：使用される ID がないことを示します。
[Device Interface Name]	[Device Id Type] が [Interface] である場合このフィールドが表示されます。 このオプションは、ロギング デバイス インターフェイスを使用して ACE Appliance から送信された syslog メッセージを一意に識別することを指定します。	ID がシステム メッセージに含まれているロギング デバイス インターフェイス名を一意に識別するテキスト文字列を入力します。最大文字列長はスペースなしで 64 文字です。&（アンパサンド）、'（単一引用符）、"（二重引用符）、<（小なり）、>（大なり）、または ?（疑問符）は使用しないでください。
[Logging Device Id]	[Device ID Type] が [Any String] である場合このフィールドが表示されます。 このオプションは、テキスト文字列を使用して ACE Appliance から送信された syslog メッセージを一意に識別することを指定します。	ACE Appliance から送信された syslog メッセージを一意に識別するテキスト文字列を入力します。最大文字列長はスペースなしで 64 文字です。&（アンパサンド）、'（単一引用符）、"（二重引用符）、<（小なり）、>（大なり）、または ?（疑問符）は使用しないでください。

ステップ 3　**[Deploy Now]** をクリックして、ACE Appliance にこの設定を導入します。この仮想コンテキストの他の Syslog アトリビュートを設定するには、次の項目を参照してください。

- 「syslog ログ ホストの設定」（P.2-13）
- 「syslog ログ メッセージの設定」（P.2-14）
- 「syslog ログ レート制限の設定」（P.2-15）

関連トピック

- 「仮想コンテキストの設定」（P.2-4）
- 「syslog ログ ホストの設定」（P.2-13）
- 「syslog ログ メッセージの設定」（P.2-14）
- 「syslog ログ レート制限の設定」（P.2-15）

syslog ログ ホストの設定

基本 syslog 特性を設定した後（「仮想コンテキスト syslog ロギングの設定」（P.2-9）を参照）、ログ ホスト、ログ メッセージ、ログ レート制限を設定できます。これらのアトリビュートのタブは、[Syslog] 設定画面の下に表示されます。

この手順を使用して syslog ログ ホストを設定します。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [System] > [Syslog]** を選択します。[Syslog] 設定画面が表示されます。

ステップ 2　[Log Host] タブを選択します。[Log Host] テーブルが表示されます。

ステップ 3　**[Add]** をクリックして新規ログ ホストを追加するか、既存のログ ホストを選択して **[Edit]** をクリックしてこれを修正します。[Log Host] 設定画面が表示されます。

ステップ 4　[IP Address] フィールドに、syslog サーバとして使用されるホストの IP アドレスを入力します。

ステップ 5　[Protocol] フィールドで、使用するプロトコルとして [TCP] または [UDP] を選択します。

ステップ 6　[Protocol Port] フィールドに、syslog サーバが syslog メッセージをリッスンするポートの数を入力します。有効な入力は 1024 ～ 65535 で、デフォルトは 514 です。

ステップ 7　[Protocol] フィールドで [TCP] を選択する（ステップ 5）と、[Default UDP] チェックボックスが表示されます。syslog サーバとの通信で TCP 転送が失敗した場合に、ACE Appliance で UDP がデフォルトになるように指定するには、[Default UDP] チェックボックスをオンにします。TCP 転送が失敗した場合に ACE Appliance で UDP がデフォルトにならないようにするには、このチェックボックスをクリアします。

ステップ 8　[Format] フィールドで、EMBLEM フォーマット ロギングを使用するかどうかを示します。

- [N/A]：EMBLEM フォーマット ロギングをイネーブルにしないことを示します。
- [Emblem]：EMBLEM フォーマット ロギングが各 syslog サーバでイネーブルであることを示します。Cisco Resource Manager Essentials（RME）ソフトウェアを使用してネットワーク上で syslog メッセージを収集し処理する場合、RME を処理できるように EMBLEM フォーマット ロギングをイネーブルにします。同様に、Cisco Resource Manager Essentials（RME）syslog アナライザでは UDP syslog メッセージだけがサポートされるため、UDP をイネーブルにする必要があります。

ステップ 9　次のいずれかをクリックします。

- **[Deploy Now]**：ACE Appliance にこの設定を導入します。
- **[Cancel]**：エントリを保存せずにこの手順を終了して、[Log Host] テーブルに戻ります。
- **[Next]**：別の syslog ホストを設定します。

関連トピック

- 「仮想コンテキスト syslog ロギングの設定」（P.2-9）
- 「syslog ログ メッセージの設定」（P.2-14）
- 「syslog ログ レート制限の設定」（P.2-15）

syslog ログ メッセージの設定

基本 syslog 特性を設定した後（「仮想コンテキスト syslog ロギングの設定」（P.2-9）を参照）、ログ ホスト、ログ メッセージ、ログ レート制限を設定できます。これらのアトリビュートのタブは、[Syslog] 設定画面の下に表示されます。

この手順を使用して syslog ログ メッセージを設定します。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [System] > [Syslog]** を選択します。[Syslog] 設定画面が表示されます。

ステップ 2　[Log Message] タブを選択します。[Log Message] テーブルが表示されます。

ステップ 3　**[Add]** をクリックして新規エントリをこのテーブルに追加するか、既存エントリを選択して **[Edit]** をクリックしてこれを修正します。[Log Message] 設定画面が表示されます。

ステップ 4　[Message Id] フィールドで、syslog サーバに送信されるか、syslog サーバに送信されない syslog メッセージのシステム ログ メッセージ ID を選択します。

ステップ 5　指定されたメッセージ ID でロギングがイネーブルであることを示すには、[Enable State] チェックボックスをオンにします。指定されたメッセージ ID でロギングがイネーブルでないことを示すには、[Enable State] チェックボックスをクリアします。[Enable State] チェックボックスをオンにした場合、[Log Level] フィールドが表示されます。

ステップ 6　[Log Level] フィールドで、表 2-4 で識別されたレベルを使用して、syslog サーバへ送信される syslog メッセージの必要なレベルを選択します。

ステップ 7　次のいずれかをクリックします。

- **[Deploy Now]**：ACE Appliance にこの設定を導入します。
- **[Cancel]**：エントリを保存せずにこの手順を終了して、[Log Message] テーブルに戻ります。
- **[Next]**：エントリを保存し、この仮想コンテキストの追加 syslog メッセージ エントリを設定します。

関連トピック

- 「仮想コンテキスト syslog ロギングの設定」（P.2-9）
- 「syslog ログ ホストの設定」（P.2-13）

- 「syslog ログ レート制限の設定」（P.2-15）

syslog ログ レート制限の設定

基本 syslog 特性を設定した後（「仮想コンテキスト syslog ロギングの設定」（P.2-9）を参照）、ログ ホスト、ログ メッセージ、ログ レート制限を設定できます。これらのアトリビュートのタブは、[Syslog] 設定画面の下に表示されます。

この手順を使用して、ACE Appliance が syslog 内でメッセージを生成するレートを制限します。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [System] > [Syslog]** を選択します。[Syslog] 設定画面が表示されます。

ステップ 2　[Log Rate Limit] タブを選択します。[Log Rate Limit] テーブルが表示されます。

ステップ 3　**[Add]** をクリックして新規エントリをこのテーブルに追加するか、既存エントリを選択して **[Edit]** をクリックしてこれを修正します。[Log Rate Limit] 設定画面が表示されます。

ステップ 4　[Type] フィールドで、syslog メッセージを制限する方法を指定します。

- **[Level]** を選択して、syslog レベルによって syslog メッセージを制限します。[Level] フィールドで、表 2-4 で識別されたレベルを使用して、syslog サーバへ送信される syslog メッセージのレベルを選択します。
- **[Message]** を選択して、メッセージ識別番号で syslog メッセージを制限します。[Message Id] フィールドで、レポートを抑制するメッセージの syslog メッセージ ID を選択します。

ステップ 5　システム メッセージ ロギングに制限を適用しないことを示すには、[Unlimited] チェックボックスをオンにします。システム メッセージ ロギングに制限を適用することを示すには、[Unlimited] チェックボックスをクリアします。[Unlimited] チェックボックスをクリアすると、[Rate] および [Time Interval] フィールドが表示されます。

ステップ 6　[Unlimited] チェックボックスをクリアする場合は、システム メッセージ ロギングに適用する制限を指定します。

a. [Rate] フィールドで、syslog メッセージ作成を制限する数を入力します。この制限に到達した場合、ACE Appliance が指定レートを超えないように新規 syslog メッセージの作成を制限します。有効な入力は 0 ～ 2147483647 の整数です。

b. [Time Interval (Seconds)] フィールドに、システム メッセージ ログを制限する期間（秒数）を入力します。デフォルトの時間間隔は 1 秒です。たとえば、[Rate] フィールドに 42 を入力して [Time Interval (Seconds)] フィールドに 60 を入力した場合、ACE Appliance では、最大 42 のメッセージを 60 秒間隔で送信するように syslog メッセージの作成が制限されます。有効な入力は 0 ～ 2147483647 秒です。

ステップ 7　次のいずれかをクリックします。

- **[Deploy Now]**：ACE Appliance にこの設定を導入します。
- **[Cancel]**：エントリを保存せずにこの手順を終了して、[Log Rate Limit] テーブルに戻ります。
- **[Next]**：エントリを保存し、別のエントリを [Log Rate Limit] テーブルに追加します。

関連トピック

- 「仮想コンテキストの設定」（P.2-4）

- 「仮想コンテキスト syslog ロギングの設定」（P.2-9）
- 「syslog ログ ホストの設定」（P.2-13）
- 「syslog ログ メッセージの設定」（P.2-14）

仮想コンテキストの SNMP 設定

この手順を使用して、この仮想コンテキストとともに使用するために SNMP を設定します。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [System] > [SNMP]** を選択します。[SNMP] 設定画面が表示されます。

ステップ 2　SNMP アトリビュートを入力します（表 2-6 を参照）。

表 2-6　SNMP アトリビュート

フィールド	説明
[Contact Information]	スペースを含めて最大 240 文字のテキスト文字列として、仮想コンテキスト内の SNMP サーバの連絡情報を入力します。名前の他に、電話番号や電子メール アドレスを含めることができます。スペースを含めるには、エントリの最初と最後に引用符を追加します。
[Location]	スペースを含めて最大 240 文字のテキスト文字列としてシステムの物理的な場所を入力します。スペースを含めるには、エントリの最初と最後に引用符を追加します。
[Trap Source Interface]	SNMP トラップが生成されるインターフェイスを識別する有効な VLAN 番号を入力します。
[IETF Trap]	ACE Appliance が、ifIndex、ifAdminStatus、ifOperStatus で構成されている、IETF 標準 IF-MIB（RFC 2863）変数バインドを持つ linkUp および linkDown トラップを送信することを示すには、チェックボックスをオンにします。 ACE Appliance が IETF 標準 IF-MIB（RFC 2863）変数バインドを持つ linkUp および linkDown トラップを送信しないことを示すには、チェックボックスをクリアします。代わりに、ACE Appliance はデフォルトで Cisco var-binds を送信します。

ステップ 3　**[Deploy Now]** をクリックして、ACE Appliance にこの設定を導入します。他の SNMP アトリビュートを設定するには、次の項目を参照してください。

- 「SNMPv2c コミュニティの設定」（P.2-17）
- 「SNMPv3 ユーザの設定」（P.2-18）
- 「SNMP トラップ宛先ホストの設定」（P.2-20）
- 「SNMP 通知の設定」（P.2-21）

関連事項

「仮想コンテキストの設定」（P.2-4）

SNMPv2c コミュニティの設定

仮想コンテキストの基本 SNMP 情報を設定した後（「仮想コンテキストの SNMP 設定」（P.2-16）を参照）、SNMPv2c コミュニティ、SNMPv3 ユーザ、トラップ宛先ホスト、SNMP 通知などの他の SNMP アトリビュートを設定できます。これらのアトリビュートのタブは、[SNMP] 設定画面の下に表示されます。

（注）　ACE Appliance Device Manager 内のすべての SNMP コミュニティは、読み取り専用コミュニティで、すべてのコミュニティはグループ *network monitors* に属します。

この手順を使用して、仮想コンテキスト用の SNMPv2c コミュニティを設定します。

前提

少なくとも 1 つの SNMP 接点を設定しておきます（「仮想コンテキストの SNMP 設定」（P.2-16）を参照）。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [System] > [SNMP]** を選択します。[SNMP] 設定画面が表示されます。

ステップ 2　[SNMP v2c Configuration] タブを選択します。[SNMP v2c Configuration] テーブルが表示されます。

ステップ 3　**[Add]** をクリックして、SNMP v2c コミュニティを追加します。[SNMP v2c Configuration] 画面が表示されます。

（注）　既存 SNMP v2c コミュニティは修正できません。代わりに、既存 SNMP v2c コミュニティを削除した後で、新規コミュニティを追加します。

ステップ 4　[Read-Only Community] フィールドに、このコンテキストの SNMP v2c コミュニティ名を入力します。有効な入力は、引用符で囲まずスペースを含まない 32 文字以下のテキスト文字列です。

ステップ 5　次のいずれかをクリックします。

- **[Deploy Now]**：ACE Appliance にこの設定を導入します。
- **[Cancel]**：エントリを保存せずにこの手順を終了して、[SNMP v2c Community] テーブルに戻ります。
- **[Next]**：エントリを保存し、この仮想コンテキストの別の SNMP コミュニティを設定します。画面がリフレッシュされて、別のコミュニティ名を入力できます。

関連トピック

- 「仮想コンテキストの設定」（P.2-4）
- 「SNMPv3 ユーザの設定」（P.2-18）
- 「SNMP トラップ宛先ホストの設定」（P.2-20）

- 「SNMP 通知の設定」（P.2-21）

SNMPv3 ユーザの設定

仮想コンテキストの基本 SNMP 情報を設定した後（「仮想コンテキストの SNMP 設定」（P.2-16）を参照）、SNMPv2c コミュニティ、SNMPv3 ユーザ、トラップ宛先ホスト、SNMP 通知などの他の SNMP アトリビュートを設定できます。これらのアトリビュートのタブは、[SNMP] 設定画面の下に表示されます。

この手順を使用して、仮想コンテキスト用の SNMPv3 ユーザを設定します。

前提

少なくとも 1 つの SNMP 接点を設定しておきます（「仮想コンテキストの SNMP 設定」（P.2-16）を参照）。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [System] > [SNMP]** を選択します。[SNMP] 設定画面が表示されます。

ステップ 2　[SNMP v3 Configuration] タブを選択します。[SNMP v3 Configuration] テーブルが表示されます。

ステップ 3　**[Add]** をクリックしてユーザを追加するか、既存エントリを選択して **[Edit]** をクリックしてこれを修正します。[SNMP v3 Configuration] 画面が表示されます。

ステップ 4　SNMPv3 ユーザ アトリビュートを入力します（表 2-7 を参照）。

表 2-7　SNMP v3 ユーザ設定アトリビュート

フィールド	説明
[User Name]	SNMPv3 ユーザ名を入力します。有効な入力は、引用符で囲まずスペースを含まない 24 文字以下のテキスト文字列です。
[Authentication Algorithm]	このユーザに使用する認証アルゴリズムを選択します。 • [N/A]：認証を使用しないことを示します。 • [Message Digest (MD5)]：認証メカニズムとしてメッセージ ダイジェスト 5 を使用することを示します。 • [Secure Hash Algorithm (SHA)]：認証メカニズムとして Secure Hash Algorithm を使用することを示します。
[Authentication Password]	認証アルゴリズムを選択するかどうかを表します。ACE Appliance は、SNMP 認証パスワードで CLI ユーザのパスワードを自動的に更新します。 次のようにして、このユーザの認証パスワードを入力します。 • パスフレーズを平文で指定する場合、テキスト文字列を引用符で囲まず、スペースを使用せずに、8 ～ 64 文字の長さの英数字で入力します。パスワードの長さは偶数でも奇数でも問題ありません。 • ローカライズされたキーの使用がイネーブルにされている場合、テキスト文字列を引用符で囲まず、スペースを使用せずに、8 ～ 130 文字の長さの英数字で入力します。パスワードの長さは偶数でなければなりません。

表 2-7　SNMP v3 ユーザ設定アトリビュート （続き）

フィールド	説明
[Confirm]	認証アルゴリズムを選択するかどうかを表します。 認証パスワードを再入力します。
[Localized]	認証アルゴリズムを選択するかどうかを表します。 パスワードが、セキュリティ暗号化のローカライズされたキー フォーマットかどうかを示します。 • [N/A]：このオプションが設定されていません。 • [False]：パスワードが暗号化用にローカライズされたキー フォーマットになっていないことを示します。 • [True]：パスワードが暗号化用にローカライズされたキー フォーマットになっていることを示します。
[Privacy]	認証アルゴリズムを選択するかどうかを表します。 暗号化アトリビュートがこのユーザ用に設定されているかどうかを示します。 • [N/A]：暗号化アトリビュートが指定されていないことを示します。 • [False]：暗号化パラメータがこのユーザ用に設定されていないことを示します。 • [True]：暗号化パラメータがこのユーザ用に設定されていることを示します。
[AES 128]	[Privacy] を [True] に設定した場合に表示されます。 128 バイト高度暗号化規格（AES）アルゴリズムがプライバシで使用されているかどうかを示します。AES は対称暗号アルゴリズムで、SNMP メッセージ暗号化のプライバシ プロトコルの 1 つです。 • [N/A]：標準が指定されていないことを示します。 • [False]：AES 128 がプライバシに使用されないことを示します。 • [True]：AES 128 がプライバシに使用されることを示します。
[Privacy Password]	[Privacy] を [True] に設定した場合に表示されます。次のようにして、ユーザ暗号化パスワードを入力します。 • パスフレーズを平文で指定する場合、テキスト文字列を引用符で囲まず、スペースを使用せずに、8 ～ 64 文字の長さの英数字で入力します。パスワードの長さは偶数でも奇数でも問題ありません。 • ローカライズされたキーの使用がイネーブルにされている場合、テキスト文字列を引用符で囲まず、スペースを使用せずに、8 ～ 130 文字の長さの英数字で入力します。パスワードの長さは偶数でなければなりません。
[Confirm]	[Privacy] を [True] に設定した場合に表示されます。 プライバシ パスワードを再入力します。

ステップ 5　次のいずれかをクリックします。

- **[Deploy Now]**：ACE Appliance にこの設定を導入します。

- **[Cancel]**：エントリを保存せずにこの手順を終了して、[SNMP v3 Configuration] テーブルに戻ります。
- **[Next]**：エントリを保存し、別のエントリを [SNMP v3 Configuration] テーブルに追加します。画面がリフレッシュされて、別の SNMPv3 ユーザを入力できます。

関連トピック

- 「仮想コンテキストの設定」（P.2-4）
- 「SNMPv2c コミュニティの設定」（P.2-17）
- 「SNMP トラップ宛先ホストの設定」（P.2-20）
- 「SNMP 通知の設定」（P.2-21）

SNMP トラップ宛先ホストの設定

SNMP 通知を受信するには、次のことを設定する必要があります。

- 少なくとも 1 つの SNMP トラップ宛先ホスト。このセクションは、これを実行する方法について説明します。
- 少なくとも 1 タイプの通知。「SNMP 通知の設定」（P.2-21）を参照してください。

仮想コンテキストの基本 SNMP 情報を設定した後（「仮想コンテキストの SNMP 設定」（P.2-16）を参照）、SNMPv2c コミュニティ、SNMPv3 ユーザ、トラップ宛先ホスト、SNMP 通知などの他の SNMP アトリビュートを設定できます。これらのアトリビュートのタブは、[SNMP] 設定画面の下に表示されます。

この手順を使用して、仮想コンテキスト用の SNMP トラップ宛先ホストを設定します。

前提

少なくとも 1 つの SNMP 接点を設定しておきます（「仮想コンテキストの SNMP 設定」（P.2-16）を参照）。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [System] > [SNMP]** を選択します。[SNMP] 設定画面が表示されます。

ステップ 2　[Trap Destination Host] タブを選択します。[Trap Destination Host] テーブルが表示されます。

ステップ 3　**[Add]** をクリックしてホストを追加するか、テーブルで既存エントリを選択して **[Edit]** をクリックしてこれを修正します。[Trap Destination Host] 設定画面が表示されます。

ステップ 4　表 2-8 内の情報を使用して、SNMP トラップ宛先ホストを設定します。

表 2-8　SNMP トラップ宛先ホスト設定アトリビュート

フィールド	説明
[IP Address]	SNMP 通知を受信するサーバの IP アドレスを入力します。192.168.11.1 などのように、ドット付き 10 進表記でアドレスを入力します。
[Port]	SNMP 通知に使用されるポートを入力します。デフォルト ポートは 162 です。

表 2-8　SNMP トラップ宛先ホスト設定アトリビュート （続き）

フィールド	説明
[Version]	トラップを送信するのに使用される SNMP のバージョンを選択します。 • [V1]：SNMPv1 を使用してトラップを送信することを示します。このオプションは、SNMP 通知依頼とともに使用できません。 • [V2c]：SNMPv2c を使用してトラップを送信することを示します。 • [V3]：SNMPv3 を使用してトラップを送信することを示します。このバージョンは、パケット暗号化が可能であるため最も安全なモデルです。
[Community]	通知操作で送信される SNMP コミュニティ ストリングまたはユーザ名を入力します。有効な入力は、引用符で囲まずスペースを含まない 32 文字以下のテキスト文字列です。
[Security Level]	このフィールドは、[V3] が選択されたバージョンの場合に表示されます。 実装されるセキュリティのレベルを選択します。 • [Auth]：メッセージ ダイジェスト 5（MD5）および Secure Hash Algorithm（SHA）がパケット認証に使用されることを示します。 • [Noauth]：AuthNoPriv セキュリティ レベルを使用することを示します。 • [Priv]：データ暗号規格（DES）をパケット暗号化に使用することを示します。

ステップ 5　次のいずれかをクリックします。

- **[Deploy Now]**：ACE Appliance にこの設定を導入します。
- **[Cancel]**：エントリを保存せずにこの手順を終了して、[Trap Destination Host] テーブルに戻ります。
- **[Next]**：エントリを保存し、別のエントリを [Trap Destination Host] テーブルに追加します。画面がリフレッシュされて、別のトラップ宛先ホストを追加できます。

関連トピック

- 「仮想コンテキストの設定」（P.2-4）
- 「SNMPv2c コミュニティの設定」（P.2-17）
- 「SNMPv3 ユーザの設定」（P.2-18）
- 「SNMP 通知の設定」（P.2-21）

SNMP 通知の設定

仮想コンテキストの基本 SNMP 情報を設定した後（「仮想コンテキストの SNMP 設定」（P.2-16）を参照）、SNMPv2c コミュニティ、SNMPv3 ユーザ、トラップ宛先ホスト、SNMP 通知などの他の SNMP アトリビュートを設定できます。これらのアトリビュートのタブは、[SNMP] 設定画面の下に表示されます。

SNMP 通知を受信するには、次のことを設定する必要があります。

- 少なくとも 1 つの SNMP トラップ宛先ホスト。「SNMP トラップ宛先ホストの設定」（P.2-20）を参照してください。
- 少なくとも 1 タイプの通知。このセクションは、これを実行する方法について説明します。

この手順を使用して、仮想コンテキスト用の SNMP 通知設定します。

前提

- 少なくとも 1 つの SNMP 接点を設定しておきます（「仮想コンテキストの SNMP 設定」（P.2-16）を参照）。
- 少なくとも 1 つの SNMP サーバ ホストを設定しておきます（「SNMP トラップ宛先ホストの設定」（P.2-20）を参照）。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [System] > [SNMP]** を選択します。[SNMP] 設定画面が表示されます。

ステップ 2　[SNMP Notification] タブを選択します。[SNMP Notification] テーブルが表示されます。

ステップ 3　**[Add]** をクリックして新しいエントリを追加します。[SNMP Notification] 設定画面が表示されます。

（注）　既存エントリは修正できません。代わりに、既存通知エントリを削除した後で、新規エントリを追加します。

ステップ 4　[Option] フィールドで、SNMP ホストに送信される通知のタイプを選択します。Admin コンテキストだけで使用できるオプションもあります。

- [License]：SNMP ライセンス通知が送信されます。このオプションを使用できるのは、Admin コンテキストだけです。
- [SLB]：サーバのロードバランシング通知が送信されます。
- [SLB Real Server]：実サーバ ステート変更の通知が送信されます。
- [SLB Virtual Server]：仮想サーバ ステート変更の通知が送信されます。
- [SNMP]：SNMP 通知が送信されます。
- [SNMP Authentication]：SNMP 依頼で間違ったコミュニティ ストリングの通知が送信されます。
- [SNMP Cold-Start]：ACE のコールド リスタート（完全な電源の再投入）後に SNMP エージェント再起動通知が送信されます。このオプションを使用できるのは、Admin コンテキストだけです。
- [SNMP Link-Down]：VLAN インターフェイスがダウンしたときに通知が送信されます。
- [SNMP Link-Up]：VLAN インターフェイスがアップしたときに通知が送信されます。
- [Syslog]：エラー メッセージ通知（Cisco Syslog MIB）が送信されます。
- [Virtual Context]：仮想コンテキスト通知が送信されます。

ステップ 5　次のいずれかをクリックします。

- **[Deploy Now]**：ACE Appliance にこの設定を導入します。
- **[Cancel]**：選択を保存せずにこの手順を終了して、[SNMP Notification] テーブルに戻ります。
- **[Next]**：エントリを保存し、別のエントリを [SNMP Notification] テーブルに追加します。画面がリフレッシュされて、別の SNMP 通知オプションを選択できます。

関連トピック

- 「仮想コンテキストの設定」（P.2-4）

- 「SNMPv2c コミュニティの設定」（P.2-17）
- 「SNMPv3 ユーザの設定」（P.2-18）

仮想コンテキスト グローバル トラフィック ポリシーの設定

ACE Appliance Device Manager を使用して、トラフィック ポリシーを特定の VLAN インターフェイスまたは同じ仮想コンテキスト内の全 VLAN インターフェイスに適用できます。

この手順を使用して、選択されたコンテキスト内の全 VLAN インターフェイスにポリシーを適用します。

ポリシーを特定の VLAN に適用するには、「トラフィック ポリシーの設定」（P.10-1）を参照してください。

（注）　既存ポリシーは修正できません。代わりに、既存グローバル ポリシーを削除した後で、新規ポリシーを作成します。

前提

この仮想コンテキスト用にレイヤ 3/ レイヤ 4 または管理ポリシー マップを設定しておく必要があります。詳細については、「仮想コンテキスト ポリシー マップの作成」（P.10-35）を参照してください。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [System] > [Global Policy]** を選択します。[Global Policies] テーブルが表示されます。

ステップ 2　**[Add]** をクリックして新規グローバル ポリシーを追加します。[Global Policies] 設定画面が表示されます。

（注）　既存ポリシーは修正できません。代わりに、既存グローバル ポリシーを削除した後で、新規ポリシーを作成します。

ステップ 3　[Policy Maps] フィールドで、このコンテキスト内の全 VLAN に適用するポリシー マップを選択します。

ステップ 4　[Direction] フィールドで、ポリシーが着信通信に適用されることを確認します。

ステップ 5　次のいずれかをクリックします。

- **[Deploy Now]**：ACE Appliance にこの設定を導入します。
- **[Cancel]**：エントリを保存せずにこの手順を終了して、[Global Policies] テーブルに戻ります。
- **[Next]**：エントリを保存し、このコンテキストの別のグローバル ポリシーを設定します。

関連トピック

- 「仮想コンテキストの使用」（P.2-1）
- 「仮想コンテキスト プライマリ アトリビュートの設定」（P.2-8）
- 「仮想コンテキスト VLAN インターフェイスの設定」（P.8-6）

- 「仮想コンテキスト syslog ロギングの設定」（P.2-9）
- 「トラフィック ポリシーの設定」（P.10-1）

ACE Appliance ライセンスの管理

（注）　この機能は、Admin コンテキストだけで使用できます。

シスコシステムズでは、パフォーマンス スループット、デフォルト コンテキストの数、SSL TPS（1 秒あたりのトランザクション数）、HTTP 圧縮パフォーマンス、アプリケーション アクセラレーションおよび最適化を向上させるように、ACE Appliance 用のライセンスを提供しています。これらのライセンスの詳細については、cisco.com の『*Cisco 4700 Series Application Control Engine Appliance Administration Guide*』を参照してください。

ACE Appliance を使用して、ACE Appliance Device Manager ライセンスの表示、インストール、削除、アップデートを行うことができます。

ACE Appliance ライセンスのインストールまたはアップデートには、次の 2 つのプロセスが必要です。

- リモート ネットワーク サーバから ACE Appliance 上のフラッシュ メモリ内にある disk0: ファイル システムへのライセンスのコピー。
- ACE Appliance でのライセンスのインストールまたはアップデート。

ACE Appliance Device Manager を使用すると、単一のダイアログボックスから両方のプロセスを実行できます。**copy** CLI コマンドを使用して以前にライセンスを ACE 上の disk0: にコピーした場合は、このダイアログボックスを使用して、ACE で新規ライセンスをインストールするか、ライセンスをアップグレードできます。

関連トピック

- 「ACE Appliance ライセンスの表示」（P.2-24）
- 「ACE Appliance ライセンスのインストール」（P.2-25）
- 「ACE Appliance ライセンスのアップデート」（P.2-26）
- 「ACE Appliance ライセンスのアンインストール」（P.2-28）
- 「ライセンス設定および統計情報の表示」（P.2-29）

ACE Appliance ライセンスの表示

（注）　この機能は、Admin コンテキストだけで使用できます。

この手順を使用して、現在 ACE Appliance にインストールされているライセンスを表示します。

手順

ステップ 1　**[Config] > [Virtual Contexts]** を選択します。[All Virtual Context] テーブルが表示されます。

ステップ 2　表示する ACE Appliance ライセンスの Admin コンテキストを選択して、**[System] > [Licenses]** をクリックします。[License] テーブルが表示され、インストールされているすべてのライセンスが一覧表示されます。

関連トピック

- 「ACE Appliance ライセンスの管理」（P.2-24）
- 「ACE Appliance ライセンスのインストール」（P.2-25）
- 「ACE Appliance ライセンスのアップデート」（P.2-26）
- 「ACE Appliance ライセンスのアンインストール」（P.2-28）
- 「ライセンス設定および統計情報の表示」（P.2-29）

ACE Appliance ライセンスのインストール

（注）　この機能は、Admin コンテキストだけで使用できます。

ACE Appliance ライセンスをリモート サーバから ACE Appliance にコピーして新規インストールするか、アップグレードするには、次の手順を使用します。

前提

- ACE Appliance の正しいソフトウェア ライセンス キーを受領しておきます。
- ACE Appliance ライセンスは、ACE Appliance にインポートするためにリモート サーバで使用可能です。または、ソフトウェア ライセンス キーを受領して、**copy disk0:** CLI コマンドを使用してライセンス ファイルを ACE Appliance 上の disk0: ファイル システムにコピーしておきます。

手順

ステップ 1　**[Config] > [Virtual Contexts]** を選択します。[All Virtual Contexts] テーブルが表示されます。

ステップ 2　ライセンスをインポートしてインストールする Admin コンテキストを選択して **[System] > [Licenses]** をクリックします。[License] テーブルが表示され、インストールされているすべてのライセンスが一覧表示されます。

ステップ 3　**[Install License]** をクリックします。[Copy a License File and Install It On The ACE] ダイアログボックスが表示されます。

ステップ 4　現在フラッシュ メモリ内の ACE Appliance disk0: ファイル システムにライセンスが存在する場合は、**[License needs to be copied to disk0:?]** チェックボックスはオフのままにします。ステップ 10 に進みます。

ステップ 5　アップデート ライセンスをフラッシュ メモリ内の disk0: ファイル システムにコピーする必要がある場合は、**[License needs to be copied to disk0:?]** チェックボックスをオンにします。ステップ 6 に進みます。

ステップ 6　[Protocol] フィールドで、リモート サーバから ACE Appliance にライセンス ファイルをインポートするのに使用されるプロトコルを選択します。

- [FTP] を選択すると、[User] および [Password] フィールドが表示されます。ステップ 7 に進みます。

- [SFTP] を選択すると、[User] および [Password] フィールドが表示されます。ステップ 7 に進みます。
- [TFTP] を選択した場合は、ステップ 8 に進みます。

ステップ 7　[FTP] または [SFTP] を選択した場合

a. [User] フィールドに、ネットワーク サーバ上のアカウントのユーザ名を入力します。

b. [Password] フィールドに、ユーザ アカウントのパスワードを入力します。[Confirm] フィールドにパスワードを再入力します。

ステップ 8　[Source File Name] フィールドに、リモート サーバ上にあるライセンス ファイルのホスト IP アドレス、パス、ファイル名を、*host-ip/path/filename* のフォーマットで入力します。ここで、

- *host-ip* は、リモート サーバの IP アドレスを表します。
- *path* は、リモート サーバのライセンス ファイルのディレクトリ パスを表します。
- *filename* は、リモート サーバのライセンス ファイルのファイル名を表します。

たとえば、このエントリは **192.168.11.2/usr/bin/ACE-VIRT-020.lic** に似ています。

ステップ 9　[Destination] フィールドに、インストールやアップデートの準備のために ACE Appliance 上にライセンス ファイルを常駐させる場所を入力します。デフォルトの場所は disk0: です。

ステップ 10　[User-Specified Name for the License file:] フィールドに、**myACE-AP-VIRT-020.lic** のように、このライセンス ファイルに使用する名前を入力します。

ステップ 11　次のいずれかをクリックします。

- **[OK]**：エントリを受け入れて、ファイルをリモート サーバから ACE Appliance へコピーしてからインストールします。
- **[Cancel]**：リモート サーバからファイルをコピーせずにこの手順を終了して、[Licenses] テーブルに戻ります。

関連トピック

- 「ACE Appliance ライセンスの管理」（P.2-24）
- 「ACE Appliance ライセンスの表示」（P.2-24）
- 「ACE Appliance ライセンスのアップデート」（P.2-26）
- 「ACE Appliance ライセンスのアンインストール」（P.2-28）
- 「ライセンス設定および統計情報の表示」（P.2-29）

ACE Appliance ライセンスのアップデート

（注）　この機能は、Admin コンテキストだけで使用できます。

ACE Appliance Device Manager により、デモンストレーション ライセンスを永続ライセンスに変換することと、永続ライセンスをアップグレードして仮想コンテキストの数を増やすことができます。

この手順を使用して、ACE Appliance のアップデート ライセンスをインストールします。

前提

- ACE Appliance の正しいアップデート ソフトウェア ライセンスを受領しておきます。

- ACE Appliance ライセンスは、ACE Appliance にインポートするためにリモート サーバで使用可能です。または、アップデート ソフトウェア ライセンスを受領して、**copy disk0:** CLI コマンドを使用してライセンス ファイルを ACE Appliance 上の disk0: ファイル システムにコピーしておきます。

手順

ステップ 1　**[Config] > [Virtual Contexts]** を選択します。[All Virtual Contexts] テーブルが表示されます。

ステップ 2　アップデートするライセンスの Admin コンテキストを選択して、**[System] > [Licenses]** をクリックします。[License] テーブルが表示され、インストールされているすべてのライセンスが一覧表示されます。

ステップ 3　アップデートするライセンスを選択して、**[Update]** をクリックします。[Update License On The ACE] ダイアログボックスが表示されます。

ステップ 4　（おそらく **copy disk0:** CLI コマンドを使用したために）現在アップデート ライセンスが ACE のフラッシュ メモリ内の disk0: ファイル システムに存在する場合は、次の手順を実行します。

a. **[Update License needs to be copied to disk0:?]** チェックボックスはオフのままにします。

b. [License File Name] フィールドに、disk0: 上のアップデート ライセンス ファイルの名前を入力します。

ステップ 5　アップデート ライセンスをフラッシュ メモリ内の disk0: ファイル システムにコピーする必要がある場合は、**[Update License needs to be copied to disk0:?]** チェックボックスをオンにします。ステップ 6 に進みます。

ステップ 6　[Protocol] フィールドで、リモート サーバから ACE Appliance にライセンス ファイルをインポートするのに使用されるプロトコルを選択します。

- [FTP] を選択すると、[User] および [Password] フィールドが表示されます。ステップ 7 に進みます。
- [SFTP] を選択すると、[User] および [Password] フィールドが表示されます。ステップ 7 に進みます。
- [TFTP] を選択した場合は、ステップ 8 に進みます。

ステップ 7　[FTP] または [SFTP] を選択した場合

a. [User] フィールドに、ネットワーク サーバ上のアカウントのユーザ名を入力します。

b. [Password] フィールドに、ユーザ アカウントのパスワードを入力します。[Confirm] フィールドにパスワードを再入力します。

ステップ 8　[Source File Name] フィールドに、リモート サーバ上にあるライセンス ファイルのホスト IP アドレス、パス、ファイル名を、*host-ip/path/filename* のフォーマットで入力します。ここで、

- *host-ip* は、リモート サーバの IP アドレスを表します。
- *path* は、リモート サーバのライセンス ファイルのディレクトリ パスを表します。
- *filename* は、リモート サーバのライセンス ファイルのファイル名を表します。

たとえば、このエントリは **192.168.11.2/usr/bin/ACE-VIRT-020.lic** に似ています。

ステップ 9　[Destination] フィールドに、インストールやアップデートの準備のために ACE Appliance 上にライセンス ファイルを常駐させる場所を入力します。デフォルトの場所は disk0: です。

ステップ 10　次のいずれかをクリックします。

- **[OK]** : ライセンスをアップデートして、[Licenses] テーブルに戻ります。[Licenses] テーブルにアップデート情報が表示されます。

- **[Cancel]**：ライセンスをアップデートせずにこの手順を終了し、[Licenses] テーブルに戻ります。

関連トピック

- 「ACE Appliance ライセンスの管理」（P.2-24）
- 「ACE Appliance ライセンスの表示」（P.2-24）
- 「ACE Appliance ライセンスのインストール」（P.2-25）
- 「ACE Appliance ライセンスのアンインストール」（P.2-28）
- 「ライセンス設定および統計情報の表示」（P.2-29）

ACE Appliance ライセンスのアンインストール

（注） この機能は、Admin コンテキストだけで使用できます。

注意 ライセンスの削除は、ACE Appliance の帯域やパフォーマンスに影響を与える可能性があります。使用している ACE Appliance でのライセンス削除による影響の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Administration Guide*』を参照してください。

この手順を使用して、ACE Appliance ライセンスを削除します。

手順

ステップ 1　**[Config] > [Virtual Contexts]** を選択します。[All Virtual Contexts] テーブルが表示されます。

ステップ 2　削除するライセンスの Admin コンテキストを選択して、**[System] > [Licenses]** をクリックします。[License] テーブルが表示され、インストールされているすべてのライセンスが一覧表示されます。

ステップ 3　削除するライセンスを選択します。

ステップ 4　**[Uninstall]** をクリックします。ウィンドウが表示され、ライセンス削除プロセスが確認されます。

（注） ライセンスの削除は、コンテキストの数、ACE Appliance の帯域幅、または SSL TPS（1 秒あたりのトランザクション数）に影響する可能性があります。削除を続ける前に、使用している環境でライセンスを削除することの影響を把握しておいてください。

ステップ 5　**[OK]** をクリックして削除を確定するか、**[Cancel]** をクリックして削除プロセスを停止します。

[OK] をクリックした場合、ライセンス削除のステータスがステータス ウィンドウに表示されます。ライセンスが削除される際に、削除されたライセンスがなくなって [Licenses] テーブルがリフレッシュされます。

関連トピック

- 「ACE Appliance ライセンスの管理」（P.2-24）
- 「ACE Appliance ライセンスのインストール」（P.2-25）

- 「ACE Appliance ライセンスのアップデート」（P.2-26）
- 「ACE Appliance ライセンスの表示」（P.2-24）
- 「ライセンス設定および統計情報の表示」（P.2-29）

ライセンス設定および統計情報の表示

（注）　この機能は、Admin コンテキストだけで使用できます。

この手順を使用して、ACE Appliance のライセンスに関する情報を表示します。

手順

ステップ 1　**[Config] > [Virtual Contexts]** を選択します。[All Virtual Contexts] テーブルが表示されます。

ステップ 2　表示するライセンス情報の Admin コンテキストを選択して、**[System] > [Licenses]** を選択します。[License] テーブルが表示され、インストールされているすべてのライセンスが一覧表示されます。

ステップ 3　ライセンスと表示する情報を選択して、**[Status]** をクリックします。[Show License Status] ウィンドウが次の情報とともに表示されます。

- メガビット / 秒またはギガビット / 秒単位での圧縮パフォーマンス
- 1 秒あたりの接続数で表されるアプリケーション アクセラレーションおよび最適化
- 1 秒あたりの SSL トランザクション
- サポートされている仮想コンテキストの数
- ギガビット / 秒単位の ACE Appliance の帯域幅

ステップ 4　情報の確認が終了したら、**[Close]** をクリックします。

関連トピック

- 「ACE Appliance ライセンスのインストール」（P.2-25）
- 「ACE Appliance ライセンスのアップデート」（P.2-26）

リソース クラスの管理

リソース クラスは、たとえば同時接続や帯域幅レートなど、ACE Appliance リソースへの仮想コンテキスト アクセスを管理する方法です。ACE Appliance には、作成時に Admin コンテキストとユーザ コンテキストに適用されるデフォルトのリソース クラスが事前設定されています。デフォルトのリソース クラスは、リソース アクセスなし（0%）から完全なリソース アクセス（100%）まで変更可能な範囲でコンテキストを操作できるように設定されています。複数のコンテキストでデフォルトのリソース クラスを使用する場合、ACE Appliance リソースのオーバーサブスクライブが発生する危険があります。つまり、ACE Appliance が、すべてのコンテキストに対して、ファースト カム ファースト サーブド ベースでの全リソースへの完全アクセスを許可することになります。リソースが最大限度で利用される場合、ACE Appliance がそのリソースに対する任意のコンテキストからの追加要求を拒否します。

リソースのオーバーサブスクライブを回避して、任意のコンテキストによるリソースへのアクセスを保証させるために、1 つ以上のコンテキストに関連付ける、カスタマイズ済みのリソース クラスを作成できます。コンテキストは、アソシエーションの作成時にリソース クラスのメンバーとなります。リソース クラスを作成することにより、メンバー コンテキストが利用する権利のある各 ACE Appliance リソースの最大および最小量の制限を設定できます。全体に対するパーセンテージにより最小および最大値を定義します。たとえば、ACE Appliance がサポートする合計 SSL 接続数の少なくとも 25 % にメンバー コンテキストがアクセスできるように、リソース クラスを作成できます。

次の ACE Appliance リソースの割り当てを制限して管理できます。

- ACL メモリ
- アプリケーション アクセラレーション接続
- syslog メッセージおよび TCP 異常（OOO）セグメントのバッファ
- 同時接続（ACE トラフィック経由）
- 管理接続（ACE トラフィック方向）
- HTTP 圧縮パーセンテージ
- プロキシ接続
- レートとしてのリソース制限の設定（1 秒あたりの数）
- 正規表現（regexp）メモリ
- SSL 接続
- スティッキ エントリ
- スタティックまたはダイナミック ネットワーク アドレス変換（Xlates）

表 2-9 は、リソース クラスに対して設定可能なリソースを識別し、定義するものです。

リソース割り当ての制約

（注） この機能は、Admin コンテキストだけで使用できます。

次のリソースは、Admin コンテキストへの接続を維持するのに重要です。

- [Rate Bandwidth]
- [Rate Management Traffic]
- [Rate SSL Connections]
- [Rate Connections]
- [Management Connections]
- [Concurrent Connections]

注意 これらのリソースをリソース クラスに 100% 割り当てて、リソース クラスを仮想コンテキストに適用する場合、Admin コンテキストへの接続が切断される可能性があります。

IP 接続を維持できるように、Admin コンテキストに対して特別にリソース クラスを作成してこれをコンテキストに適用することをお勧めします。

表 2-9　リソース クラス アトリビュート

リソース	定義
[All]	管理トラフィック帯域幅を除いて、このリソース クラスに割り当てられたすべてのコンテキストに対してすべてのリソースを指定した値に制限します。管理トラフィック帯域幅は、明示的に管理トラフィックの最小値を設定するまでデフォルト値のままになります。
[Acceleration Connections]	アプリケーション アクセラレーション接続のパーセンテージ。
[ACL Memory]	ACL に割り当てられたメモリのパーセンテージ。
[Concurrent Connections]	同時接続のパーセンテージ。 （注）　仮想コンテキストに 100% を割り当てることによってすべての同時接続を消費する場合、Admin コンテキストへの IP 接続が失われる可能性があります。
[HTTP Compression]	HTTP データの圧縮パーセンテージ。
[Management Connections]	管理接続のパーセンテージ。 （注）　仮想コンテキストに 100% を割り当てることによってすべての管理接続を消費する場合、Admin コンテキストへの IP 接続が失われる可能性があります。
[Proxy Connections]	プロキシ接続のパーセンテージ。
[Regular Expressions]	正規表現メモリのパーセンテージ。
[Sticky]	スティッキ テーブル内のエントリのパーセンテージ。 （注）　スティッキ エントリのリソースを割り当てるためにスティッキの最小値を設定する必要があり、設定が無制限の場合スティッキ ソフトウェアはリソースを受け取りません。
[Xlates]	ネットワークおよびポート アドレス変換エントリのパーセンテージ。
[Buffer Syslog]	syslog バッファのパーセンテージ。
[Rate Inspect Connection]	FTP および RTSP のアプリケーション プロトコル インスペクション接続のパーセンテージ。

表 2-9　リソース クラス アトリビュート （続き）

リソース	定義
[Rate Bandwidth]	コンテキスト スループットのパーセンテージ このアトリビュートは、1 つ以上のコンテキストに対してバイト/秒単位で ACE スループットの合計を制限します。 **（注）** 仮想コンテキストに 100% を割り当てることによってすべてのレート帯域幅を消費する場合、Admin コンテキストへの IP 接続が失われる可能性があります。 コンテキスト当たりの最大帯域幅レートは、帯域幅ライセンスによって決定されます。デフォルトで、ACE では 1 ギガビット/秒（Gbps）のアプライアンス スループットがサポートされます。オプションで 2 Gbps 帯域幅ライセンスに ACE をアップグレードできます。ACE 内のリソース クラスに対して最小帯域幅値を設定した場合、ACE は、関連付けられているリソース クラスに関係なく、ACE 内の全コンテキストの合計帯域幅最大値から設定値を減算します。コンテキストの合計帯域幅レートは、次の 2 つのコンポーネントから構成されています。 • [Throughput]：ACE を通過するトラフィックを制限します。これは派生値で（直接は設定できない）、1 Gbps および 2 Gbps ライセンスの bandwidth レートから mgmt-traffic レートを引いた値になります。 • [Management Traffic]：バイト/秒単位で（ACE への）管理トラフィックを制限します。管理トラフィック帯域幅の最小量を保証するためには、[Resource Classes] テーブルを使用して最小パーセンテージを管理トラフィックに明示的に割り当てる必要があります（**[Config] > [Virtual Contexts] > [*admin context*] > [System] > [Resource Class]**）。帯域幅の最小パーセンテージを管理トラフィックに割り当てる際に、ACE は、その値を ACE 内の全コンテキストに対する最大利用可能管理トラフィック帯域幅から減算します。
[Rate Connections]	任意の種類の接続のパーセンテージ。 **（注）** 仮想コンテキストに 100% を割り当てることによってすべてのレート接続を消費する場合、Admin コンテキストへの IP 接続が失われる可能性があります。
[Rate Management Traffic]	管理トラフィック接続のパーセンテージ。 **（注）** 仮想コンテキストに 100% を割り当てることによってすべてのレート管理トラフィックを消費する場合、Admin コンテキストへの IP 接続が失われる可能性があります。
[Rate SSL Connections]	SSL 接続のパーセンテージ。 **（注）** 仮想コンテキストに 100% を割り当てることによってすべてのレート管理トラフィックを消費する場合、Admin コンテキストへの IP 接続が失われる可能性があります。
[Rate Syslog]	1 秒当たりの syslog メッセージのパーセンテージ。
[Rate MAC Miss]	パケット内でのカプセル化が間違っている場合に、コントロール プレーンに送信される ACE Appliance に通じるメッセージのパーセンテージ。

関連トピック

- 「リソース クラスの追加」（P.2-33）
- 「リソース クラスの修正」（P.2-34）

- 「リソース クラスの削除」（P.2-35）
- 「仮想コンテキストにおけるリソース クラスの使用の表示」（P.2-36）

リソース クラスの追加

（注）　この機能は、Admin コンテキストだけで使用できます。

サービスのプロビジョニング、仮想コンテキストの確立、デバイスの管理、仮想コンテキスト リソース消費のモニタリングを行う際に、リソース クラスが使用されます。

リソース クラスの定義は、自動的にコンテキストに適用されません。新規リソース クラスは、リソース クラスが仮想コンテキストに割り当てられる際にだけ適用されます。

注意　これらのリソースをリソース クラスに 100% 割り当ててリソース クラスを仮想コンテキストに適用する場合、Admin コンテキストへの接続が切断される可能性があります。詳細については、「リソース割り当ての制約」（P.2-30）を参照してください。

この手順を使用して、新規リソース クラスを作成します。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*admin context*] > [System] > [Resource Class]** を選択します。[Resource Classes] テーブルが表示されます。

ステップ 2　**[Add]** をクリックして、新規リソース クラスを作成します。[New Resource Class] 設定画面が表示されます。

ステップ 3　[Name] フィールドに、このリソース クラスの一意の名前を入力します。有効な入力は、スペースを含まず引用符なしの最大 64 文字です。

ステップ 4　各リソースで同じ値を使用するには、[All] 行に次の情報を入力します（リソースの説明については、表 2-9 を参照してください）。

a. [Min.] フィールドに、このリソース クラスに割り当てる各リソースの最小パーセンテージを入力します。有効な入力は、0.1 ずつ増加する 10 進数を含む 0 ～ 100 の数字です。

b. [Max.] フィールドで、このリソース クラスに割り当てる各リソースの最大パーセンテージを選択します。

- [Equal to Min]：各リソースに割り当てられた最大パーセンテージが [Min.] フィールド内に指定された最小値と等しいことを示します。
- [Unlimited]：このリソース クラスに割り当て可能な各リソースのパーセンテージに上限がないことを示します。

ステップ 5　リソースに対して別の値を使用するために、各リソースに対して、割り当てリソースの方法を選択します。

- **[Default]** を選択して、ステップ 4 に指定された値を使用します。
- **[Min.]** を選択して、リソースの特定の最小値を入力します。

ステップ 6　[Min.] を選択する場合

a. [Min.] フィールドに、このリソース クラスに割り当てるこのリソースの最小パーセンテージを入力します。たとえば、ACL メモリの場合は、[Min.] フィールドに 10 を入力して、最小で 10% の利用可能 ACL メモリをこのリソース クラスに割り当てることを指定します。

b. [Max.] フィールドで、このリソース クラスに割り当てるリソースの最大パーセンテージを選択します。

- [Equal To Min] : このリソースに割り当てられた最大パーセンテージが [Min.] フィールド内に指定された最小値と等しいことを示します。
- [Unlimited] : このリソース クラスに割り当て可能なリソースのパーセンテージに上限がないことを示します。

ステップ 7　このリソース クラスのリソースの割り当てを終了する場合、次のものをクリックします。

- **[Deploy Now]** をクリックして、ACE Appliance にこの設定を導入します。
- **[Cancel]** をクリックして、エントリを保存せずにこの手順を終了して、[Resource Classes] テーブルに戻ります。

ステップ 8　**[Deploy Now]** をクリックした場合、ACE Appliance Device Manager によって、このリソース クラスを使用してサポート可能な仮想コンテキストの数が [Maximum VC] 列に表示されます。より多くの、あるいはより少ない仮想コンテキストをサポートするには、リソース クラスを選択して、**[Edit]** をクリックし、この手順で説明されているように修正します。

関連トピック

- 「リソース クラスの管理」（P.2-29）
- 「リソース クラスの修正」（P.2-34）
- 「リソース クラスの削除」（P.2-35）
- 「仮想コンテキストにおけるリソース クラスの使用の表示」（P.2-36）

リソース クラスの修正

（注）　この機能は、Admin コンテキストだけで使用できます。

リソース クラスを修正する際に、ACE Appliance Device Manager によって、進行中のリソース クラスに関連付けられた仮想コンテキストに変更が適用されます。変更は、すでにリソース クラスに関連付けられている既存の仮想コンテキストに適用されます。

注意　これらのリソースをリソース クラスに 100% 割り当ててリソース クラスを仮想コンテキストに適用する場合、Admin コンテキストへの接続が切断される可能性があります。詳細については、「リソース割り当ての制約」（P.2-30）を参照してください。

この手順を使用して、既存のリソース クラスを修正します。

（注）　デフォルトのリソース クラスは修正できません。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*admin context*] > [System] > [Resource Class]** を選択します。[Resource Classes] テーブルが表示されます。

ステップ 2　修正するリソース クラスを選択して、**[Edit]** をクリックします。[Edit Resource Class] 設定画面が表示されます。

ステップ 3　必要に応じてフィールドを変更します。設定値の詳細については、「リソース クラスの追加」（P.2-33）を参照してください。リソースの説明については、表 2-9 を参照してください。

ステップ 4　このリソース クラスのリソースの割り当てを終了する場合、次のものをクリックします。

- **[Deploy Now]** をクリックして、ACE Appliance にこの設定を導入します。設定画面が更新され、[Name] フィールドの下にある [Max. Provisionable] フィールドに、このリソース割り当てを使用してサポート可能な仮想コンテキスト数が示されます。リソース割り当てに満足していてエントリを保存する場合、**[Cancel]** をクリックして [Resource Classes] テーブルに戻ります。
- **[Cancel]** をクリックして、エントリを保存せずにこの手順を終了して、[Resource Classes] テーブルに戻ります。

ACE Appliance Device Manager によって、すべての変更が、このリソース クラスを使用する仮想コンテキストに適用されます。

関連トピック

- 「リソース クラスの管理」（P.2-29）
- 「リソース クラスの追加」（P.2-33）
- 「リソース クラスの修正」（P.2-34）
- 「リソース クラスの削除」（P.2-35）
- 「仮想コンテキストにおけるリソース クラスの使用の表示」（P.2-36）

リソース クラスの削除

（注）　この機能は、Admin コンテキストだけで使用できます。

この手順を使用して、リソース クラスを ACE Appliance Device Manager データベースから削除します。

（注）　ACE Appliance Device Manager からリソース クラスを削除する際に、このリソース クラスに関連付けられていた仮想コンテキストはすべて、自動的にデフォルト リソース クラスのメンバーとなります。デフォルトのリソース クラスは、最小 0.00% から最大 100.00% までの全 ACE Appliance リソースを各コンテキストに割り当てます。デフォルトのリソース クラスは修正できません。

仮想コンテキストでのリソース クラスの削除の影響により、削除する前にリソース クラスの現在の構成を確認しておくことをお勧めします。「仮想コンテキストにおけるリソース クラスの使用の表示」（P.2-36）を参照してください。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*admin context*] > [System] > [Resource Class]** を選択します。[Resource Classes] テーブルが表示されます。

ステップ 2　削除するリソース クラスを選択して、**[Delete]** をクリックします。ウィンドウが表示され、削除が確認されます。

ステップ 3　**[OK]** をクリックしてリソース クラスの削除を継続するか、**[Cancel]** をクリックしてリソース クラスを保持します。

更新された情報で [Resource Classes] テーブルがリフレッシュされます。

関連トピック

- 「リソース クラスの管理」（P.2-29）
- 「リソース クラスの追加」（P.2-33）
- 「リソース クラスの修正」（P.2-34）
- 「仮想コンテキストにおけるリソース クラスの使用の表示」（P.2-36）

仮想コンテキストにおけるリソース クラスの使用の表示

（注）　この機能は、Admin コンテキストだけで使用できます。

この手順を使用して、選択されたリソース クラスを使用する全仮想コンテキストの一覧を表示します。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*admin context*] > [System] > [Resource Class]** を選択します。[Resource Class] テーブルでは、2 列目に各リソース クラスを使用している仮想コンテキストの数がリストされます。

ステップ 2　利用状況を表示するリソース クラスを選択して、**[Virtual Contexts]** をクリックします。[Virtual Contexts Using Resource Class] テーブルが表示され、関連コンテキストがリストされます。

ステップ 3　**[Cancel]** をクリックして、[Resource Classes] テーブルに戻ります。

関連トピック

- 「リソース クラスの管理」（P.2-29）
- 「リソース クラスの追加」（P.2-33）
- 「リソース クラスの修正」（P.2-34）
- 「リソース クラスの削除」（P.2-35）
- 「仮想コンテキストにおけるリソース クラスの使用の表示」（P.2-36）

ACL を使用したセキュリティの設定

ACL（アクセス コントロール リスト）は、ネットワーク トラフィック プロファイルを一括して定義する、ACL エントリと呼ばれる一連の文で構成されています。各エントリは、エントリ内に指定されたネットワークの一部に対してネットワーク トラフィック（受信および送信）を許可または拒否します。アクション エレメント（「許可」または「拒否」）の他に、各エントリには、送信元アドレス、宛先アドレス、プロトコル、プロトコル固有パラメータなどの基準に基づくフィルタ エレメントが含まれています。暗黙的な「全拒否」エントリがすべての ACL エントリの終わりに存在するため、接続を許可するすべてのインターフェイスに ACL を設定する必要があります。設定しない場合、ACE はインターフェイス上の全トラフィックを拒否します。

ACL は、各パケットを処理するのではなく、ネットワーク接続セットアップを制御できるようにすることで、すべてのネットワークに対して基本セキュリティを提供します。このような ACL は一般的に *セキュリティ ACL* と呼ばれます。

たとえば、Network Address Translation（NAT; ネットワーク アドレス変換）、Server Load Balancing（SLB; サーバ ロード バランシング）などの他の機能の一部として ACL を設定できます。ACE は、これらの個別の ACL を、*マージド ACL* と呼ばれる 1 つの大きい ACL にマージします。次にマージド ACL が ACL コンパイラによって解析され、ACL 参照メカニズムが生成されます。このマージド ACL への合致が 1 回発生するたびに、複数のアクションを実行できます。すでに [Summary] テーブル内にある ACL へのエントリの追加、エントリの修正、またはエントリの削除を行ったり、新規 ACL をリストに追加したりすることができます。

ACL を使用する場合、回線上のすべての電子メール トラフィックを許可するものの、FTP トラフィックをブロックするようなこともできます。ACL を使用してあるクライアントにネットワークの一部へのアクセスを許可して、別のクライアントが同じ領域にアクセスできないようにすることもできます。

ACL を設定する際に、ACL をインターフェイスに適用して、そのインターフェイスのトラフィックを制御する必要があります。インターフェイスに ACL を適用すると、ACL とそのエントリがそのインターフェイスに割り当てられます。

インターフェイスの各方向（着信または送信）に適用できるのは 1 つの拡張 ACL だけです。同じ ACL を複数のインターフェイスに適用することもできます。EtherType ACL は、着信方向およびレイヤ 2 インターフェイスだけに適用できます。

（注） デフォルトで、明示的に許可しない限りすべてのトラフィックが ACE で拒否されます。ACL 内で明示的に許可されたトラフィックだけが通過できます。その他のすべてのトラフィックは拒否されます。

特定の手順については、次の項目を参照してください。

- 「ACL の作成」（P.2-38）
- 「EtherType ACL アトリビュートの設定」（P.2-44）
- 「拡張 ACL アトリビュートの設定」（P.2-40）
- 「拡張 ACL のリシーケンス」（P.2-44）
- 「コンテキスト別の全 ACL の表示」（P.2-46）
- 「ACL の編集または削除」（P.2-46）

ACL の作成

（注）　デフォルトで、明示的に許可しない限りすべてのトラフィックが ACE で拒否されます。ACL 内で明示的に許可されたトラフィックだけが通過できます。その他のすべてのトラフィックは拒否されます。

ACL の作成、修正、または削除を行うには、次の手順を使用します。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [Security] > [ACLs]** を選択します。[ACL Summary] テーブルが表示され、既存 ACL が一覧表示されます。[ACL Summary] のフィールドについては、表 2-10 で説明します。

表 2-10　[ACL Summary] テーブル

フィールド	説明
[Name]	ACL の一意な識別子を入力します。有効な入力は、引用符なしの最大 64 文字の英数字です。
[Type]	次の ACL タイプを指定します。 • [Extended]：トラフィックの送信元と宛先の両方の IP アドレスと、プロトコルおよび実行するアクションを指定できます。詳細については、「拡張 ACL アトリビュートの設定」を参照してください。 • [Ethertype]：この ACL は、EtherType に基づいて非 IP トラフィックのネットワーク アクセスを制御します。EtherType は、サブプロトコル ID です。詳細については、「EtherType ACL アトリビュートの設定」を参照してください。
[Line Number]	拡張種別 ACL エントリの ACL 行番号。
[Action]	適用するアクション（許可/拒否）。
[Protocol]	この ACL エントリに適用するプロトコル番号またはサービス オブジェクト グループ。
[Source]	ソースの IP アドレス（拡張種別 ACL 用に設定されている場合はポート番号付きソース ネットマスク）、またはこの ACL エントリに適用されるソース ネットワーク オブジェクト グループ（設定されている場合）。
[Destination]	宛先の IP アドレス（拡張種別 ACL 用に設定されている場合はポート番号付き宛先ネットマスク）、またはこの ACL エントリに適用される宛先ネットワーク オブジェクト グループ（設定されている場合）。
[ICMP]	この ACL で ICMP（インターネット制御メッセージ プロトコル）が使用されるかどうかを示します。詳細については、「プロトコル名と番号」を参照してください。
[Interface(s)]	この ACL に関連付けられた VLAN インターフェイス。たとえば、<4,5:4> などです。ここで、< は入力方向を示し、> は出力方向を示します。
[Remark]	この ACL について含めるコメントを入力します。有効な入力は、引用符で囲まない 100 文字以下のテキスト文字列です。テキストまたは特殊文字の最初に先行スペースを入力できます。後続スペースは無視されます。

ステップ 2　[Summary] テーブルから、次のいずれかを実行します。

- ACL インラインの完全な詳細を表示するには、テーブル エントリの左側にあるプラス記号をクリックします。
- ACL を作成するには、**[Add]** アイコンをクリックします。
- ACL を修正するには、任意のテーブル エントリの左側にあるラジオ ボタンを選択してから、**[Edit]** アイコンをクリックします。
- ACL を削除するには、任意のテーブル エントリの左側にあるラジオ ボタンを選択してから、**[Delete]** アイコンをクリックします。

作成を選択した場合は、[New Access List] 画面が表示されます。

修正を選択した場合は、テーブル エントリの左側で選択したラジオ ボタンに基づいて、[Edit ACL] または [Edit ACL entry] 画面が表示されます。

ステップ 3　表 2-11 の説明に従って、必要なフィールドを追加または編集します。

表 2-11　ACL 設定アトリビュート

フィールド	説明
[ACL Properties]	名前、タイプ（Extended、Ethertype）、備考が含まれています。詳細については、「[ACL Summary] テーブル」を参照してください。
[ACL Entries]	
[Entry Attributes]	行番号、アクションとプロトコル/サービス オブジェクト グループのドロップダウン記述子メニューが含まれています。
[Source]	ソースの IP アドレス（拡張種別 ACL 用に設定されている場合はポート番号付きソース ネットマスク）、またはこの ACL エントリに適用されるソース ネットワーク オブジェクト グループ（設定されている場合）。
[Destination]	宛先の IP アドレス（拡張種別 ACL 用に設定されている場合はポート番号付き宛先ネットマスク）、またはこの ACL エントリに適用される宛先ネットワーク オブジェクト グループ（設定されている場合）。
[Add To Table] ボタン	**[Deploy]** をクリックする前に、このボタンを使用して一度に 1 つの ACL エントリを追加することで、複数のエントリを追加するために使用されます。以前は、UI 内の 2 つの異なる場所を移動する 2 つの手順のプロセスで一度に追加できたのは 1 つのエントリだけでした。
[Remove From Table] ボタン	**[Deploy]** をクリックする前に、このボタンを使用して一度に 1 つの ACL エントリを削除することで、複数のエントリを削除するために使用されます。
[Interfaces]	
• [Input/Output Direction] • [Currently Assigned (ACL:Direction)]	ACL を 1 つ以上のインターフェイスに関連付けて、インターフェイスごとに 1 つの入力 ACL と 1 つの出力 ACL だけを許可できるようにします。[Interfaces] セクションの下にある左上部のチェックボックスを使用すると、すべてのインターフェイスを選択して、「access-group input」を適用できます。
[Deploy] ボタン	新たに作成した ACL エントリを、設定した VLAN インターフェイス割り当てとともに導入できます。
[Cancel] ボタン	エントリを保存せずに終了します。

（注）　オブジェクト グループを追加、修正、または削除するには、「オブジェクト グループの設定」（P.2-47）を参照してください。

ステップ 4　次のいずれかをクリックします。

- **[Deploy]**：この設定を ACE Appliance に導入します。
- **[Cancel]**：エントリを保存せずにこの手順を終了して、[ACLs] テーブルに戻ります。

関連トピック

- 「ACL を使用したセキュリティの設定」（P.2-37）
- 「EtherType ACL アトリビュートの設定」（P.2-44）
- 「拡張 ACL アトリビュートの設定」（P.2-40）
- 「拡張 ACL のリシーケンス」（P.2-44）
- 「ACL の編集または削除」（P.2-46）

拡張 ACL アトリビュートの設定

（注）　デフォルトで、明示的に許可しない限りすべてのトラフィックが ACE で拒否されます。ACL 内で明示的に許可されたトラフィックだけが通過できます。その他のすべてのトラフィックは拒否されます。

拡張 ACL により、トラフィックの送信先と宛先の両方の IP アドレスと、プロトコルおよび実行するアクションを指定できます。

TCP、UDP、ICMP 接続の場合、ACE では確立した接続ですべての戻りトラフィックが許可されるため、戻りトラフィックを許可するために ACL を宛先インターフェイスにも適用する必要はありません。

（注）　ACE は、明示的に標準 ACL をサポートしません。標準 ACL を設定するために、宛先アドレスを **[any]** に指定して、拡張 ACL にポートを指定しません。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [Security] > [ACLs]** を選択します。[ACLs] テーブルが表示され、既存 ACL がリストされます。

ステップ 2　**[Add]** をクリックします。[New Access List] 設定画面が表示されます。

ステップ 3　[ACL Properties] ペインに ACL 名を入力して、タイプに [Extended] を選択します。

ステップ 4　表 2-12 内の情報を使用して拡張 ACL エントリを設定します。

表 2-12　拡張 ACL 設定オプション

フィールド	説明
[Entry Attributes]	
[Line Number]	ACL 内でこのエントリの位置を指定する番号を入力します。エントリの位置は、ACL 内のエントリの参照順に影響します。既存の拡張 ACL のシーケンスを変更するには、「拡張 ACL のリシーケンス」（P.2-44）を参照してください。
[Action]	適用するアクション（許可/拒否）。
[Service Object Group]	この ACL に適用するサービス オブジェクト グループを選択します。
[Protocol]	この ACL エントリに適用するプロトコルまたはプロトコル番号を選択します。表 2-13 には、一般的なプロトコル名と番号が一覧表示されています。
[Source]	
[Source Network]	ACE が送信元ネットワークから受信するネットワーク トラフィックを定義します。 • [Any]：すべての送信元からのネットワーク トラフィックを許可することを示すには、[Any] ラジオ ボタンを選択します。 • [IP/Netmask]：アクセスを特定の送信元 IP アドレスに制限するには、このフィールドを使用します。この ACL で使用可能な送信元 IP アドレスを入力します。特定の送信元 IP アドレスを入力して、そのサブネット マスクを選択します。 • [Network Object Group]：この ACL に適用する送信元ネットワーク オブジェクト グループを選択します。
[Source Port Operator]	このフィールドは、[Protocol] フィールドで [TCP] または [UPD] が選択された場合に表示されます。 送信元ポート番号を比較するために使用するオペランドを選択します。 • [Equal To]：送信元ポートは [Source Port Number] フィールドの番号と同じでなければなりません。 • [Greater Than]：送信元ポートは [Source Port Number] フィールドの番号よりも大きくなければなりません。 • [Less Than]：送信元ポートは [Source Port Number] フィールドの番号よりも小さくなければなりません。 • [Not Equal To]：送信元ポートは [Source Port Number] フィールドの番号と等しくなってはいけません。 • [Range]：送信元ポートは、[Lower Source Port Number] フィールドと [Uppser Source Port Number] フィールドに指定されたポートの範囲内でなければなりません。
[Source Port Number]	このフィールドは、[Source Port Operator] フィールドで [Equal To]、[Greater Than]、[Less Than]、または [Not Equal To] が選択された場合に表示されます。 アクセスを許可または拒否するポート名とポート番号を入力します。
[Lower Source Port Number]	このフィールドは、[Source Port Operator] フィールドで [Range] が選択された場合に表示されます。 アクセスを許可または拒否する下限のポート番号を入力します。有効な入力は 0 ～ 65535 の整数です。このフィールド内の数字は、[Upper Source Port Number] フィールドに入力した数字よりも小さい必要があります。

表 2-12　拡張 ACL 設定オプション （続き）

フィールド	説明
[Upper Source Port Number]	このフィールドは、[Source Port Operator] フィールドで [Range] が選択された場合に表示されます。 アクセスを許可または拒否する上限のポート番号を入力します。有効な入力は 0 ～ 65535 の整数です。このフィールド内の数字は、[Lower Source Port Number] フィールドに入力した数字よりも大きい必要があります。
[Destination]	
[Destination Network]	ACE から宛先ネットワークに送信するネットワーク トラフィックを定義します。 • [Any] : すべての宛先へのネットワーク トラフィックを許可することを示すには、[Any] ラジオ ボタンを選択します。 • [IP/Netmask] : アクセスを特定の宛先 IP アドレスに制限するには、このフィールドを使用します。この ACL で使用可能な送信元 IP アドレスを入力します。特定の宛先 IP アドレスを入力して、そのサブネット マスクを選択します。 • [Network Object Group] : この ACL に適用する宛先ネットワーク オブジェクト グループを選択します。
[Destination Port Operator]	このフィールドは、[Protocol] フィールドで [TCP] または [UPD] が選択された場合に表示されます。 宛先ポート番号を比較するために使用するオペランドを選択します。 • [Equal To] : 宛先ポートは [Destination Port Number] フィールドの番号と同じでなければなりません。 • [Greater Than] : 宛先ポートは [Destination Port Number] フィールドの番号よりも大きくなければなりません。 • [Less Than] : 宛先ポートは [Destination Port Number] フィールドの番号よりも小さくなければなりません。 • [Not Equal To] : 宛先ポートは [Destination Port Number] フィールドの番号と等しくなってはいけません。 • [Range] : 宛先ポートは、[Lower Destination Port Number] フィールドと [Upper Destination Port Number] フィールドに指定されたポートの範囲内でなければなりません。
[Destination Port Number]	このフィールドは、[Destination Port Operator] フィールドで [Equal To]、[Greater Than]、[Less Than]、または [Not Equal To] が選択された場合に表示されます。 アクセスを許可または拒否するポート名とポート番号を入力します。
[Lower Destination Port Number]	このフィールドは、[Destination Port Operator] フィールドで [Range] が選択された場合に表示されます。 アクセスを許可または拒否する下限のポート番号を入力します。有効な入力は 0 ～ 65535 の整数です。このフィールド内の数字は、[Upper Destination Port Number] フィールドに入力した数字よりも小さい必要があります。
[Upper Destination Port Number]	このフィールドは、[Destination Port Operator] フィールドで [Range] が選択された場合に表示されます。 アクセスを許可または拒否する上限のポート番号を入力します。有効な入力は 0 ～ 65535 の整数です。このフィールド内の数字は、[Lower Destination Port Number] フィールドに入力した数字よりも大きい必要があります。

表 2-13　プロトコル名と番号

プロトコル名[1]	プロトコル番号	説明
AH	51	認証ヘッダー
EIGRP	88	拡張 IGRP
ESP	50	カプセル化セキュリティ ペイロード
GRE	47	総称ルーティング カプセル化
ICMP	1	インターネット制御メッセージ プロトコル
IGMP	2	インターネット グループ管理プロトコル
IP	0	インターネット プロトコル
IP-In-IP	4	IP-in-IP レイヤ 3 トンネリング プロトコル
OSPF	89	Open Shortest Path First
PIM	103	Protocol Independent Multicast
TCP	6	Transmission Control Protocol
UDP	17	ユーザ データグラム プロトコル

1. 全プロトコルとその番号の完全なリストについては、www.iana.org/numbers.html にある「Internet Assigned Numbers Authority」を参照してください。

ステップ 5　1 つ以上の ACL エントリをテーブルに追加する場合は、**[Add To Table]** をクリックします。拡張 ACL エントリの設定については、ステップ 4 を参照してください。

ステップ 6　必要に応じて任意の VLAN インターフェイスをこの ACL に関連付けて、次のいずれかをクリックします。

- **[Deploy]**：この設定をただちに使用します。
- **[Cancel]**：エントリを保存せずにこの手順を終了して、[ACL Summary] テーブルに戻ります。

関連トピック

- 「ACL を使用したセキュリティの設定」（P.2-37）
- 「ACL の作成」（P.2-38）
- 「EtherType ACL アトリビュートの設定」（P.2-44）
- 「拡張 ACL のリシーケンス」（P.2-44）
- 「ACL の編集または削除」（P.2-46）

拡張 ACL のリシーケンス

この手順を使用して、拡張 ACL のエントリのシーケンスを変更します。EtherType ACL エントリはリシーケンスを行えません。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [Security] > [ACLs]** を選択します。[ACLs] テーブルが表示され、既存 ACL がリストされます。

ステップ 2　番号を付け替える拡張 ACL を選択して、フィルタ フィールドの左側に表示される **[Resequence]** アイコンをクリックします。[ACL Line Number Resequence] ウィンドウが表示されます。

ステップ 3　[Start] フィールドに、ACL 内の最初のエントリに割り当てる番号を入力します。有効な入力は 1 ～ 2147483647 です。

ステップ 4　[Increment] フィールドに、最初のエントリの後に ACL 内の各エントリに追加する番号を入力します。任意の整数を入力できます。有効な入力は 1 ～ 2147483647 です。

ステップ 5　次のいずれかをクリックします。

- **[Resequence]**：エントリを保存し、[ACLs] テーブルに戻ります。
- **[Cancel]**：エントリを保存せずにこの手順を終了して、[ACLs] テーブルに戻ります。

関連トピック

- 「ACL を使用したセキュリティの設定」（P.2-37）
- 「ACL の作成」（P.2-38）
- 「EtherType ACL アトリビュートの設定」（P.2-44）
- 「拡張 ACL アトリビュートの設定」（P.2-40）
- 「ACL の編集または削除」（P.2-46）

EtherType ACL アトリビュートの設定

（注）　デフォルトで、明示的に許可しない限りすべてのトラフィックが ACE で拒否されます。ACL 内で明示的に許可されたトラフィックだけが通過できます。その他のすべてのトラフィックは拒否されます。

EtherType に基づいてトラフィックを制御する ACL を設定できます。EtherType は、サブプロトコル ID です。EtherType ACL は、イーサネット V2 フレームをサポートしています。EtherType ACL は、タイプ フィールドとは逆に長さフィールドを使用しているため、802.3 フォーマット化されたフレームをサポートしません。唯一の例外は、ブリッジ プロトコル データ ユニット（BPDU）で、SNAP カプセル化されており、ACE は特別に BPDU を処理するように設計されています。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [Security] > [ACLs]** を選択します。[ACLs] テーブルが表示され、既存 ACL がリストされます。

ステップ 2　**[Add]** をクリックします。[New Access List] 設定画面が表示されます。

ステップ 3　[ACL Properties] ペインに ACL 名を入力して、[Ethertype] を選択します。

ステップ 4　次のいずれかのラジオ ボタンを選択します。

- ACE が接続をブロックすることを示すには、**[Deny]** をクリックします。
- ACE が接続を許可することを示すには、**[Permit]** をクリックします。

ステップ 5　この ACL の [Protocol] フィールド プルダウン メニューから次のいずれかを選択します。

- [Any]：任意の EtherType を指定します。
- [BPDU]：ブリッジ プロトコル データ ユニットを指定します。ACE ポートはトランク ポートであるため、ACE はトランク ポート（シスコ専用）BPDU を受信します。トランク BPDU にはペイロード内の VLAN 情報があるため、BPDU を許可した場合に ACE が発信 VLAN のあるペイロードを修正します。冗長性を設定する場合、ブリッジング ループを回避するために、EtherType ACL のある両方のインターフェイスで BPDU を許可する必要があります。冗長性の設定に関する詳細については、「ハイ アベイラビリティの設定」（P.9-1）を参照してください。
- [IPv6]：インターネット プロトコル バージョン 6 を指定します。
- [MPLS]：マルチプロトコル ラベル スイッチングを指定します。[MPLS] を選択すると、MPLS ユニキャストおよび MPLS マルチキャスト トラフィックの両方に適用されます。MPLS を許可する場合、ラベル配布プロトコル（LDP）またはタグ配布プロトコル（TDP）セッションのルータ ID として ACE インターフェイス上の IP アドレスを使用するように、ACE に接続された両方の MPLS ルータを設定することにより、LDP および TDP TCP 接続が ACE を通じて確立されるようにします。LDP および TDP により、MPLS ルータは、パケットを転送するために使用されるラベル（アドレス）をネゴシエーションできます。

ステップ 6　必要に応じてステップ 4 とステップ 5を繰り返して、**[Add To Table]** をクリックして 1 つ以上の ACL エントリを追加します。

ステップ 7　必要に応じて任意の VLAN インターフェイスをこの ACL に関連付けて、次のいずれかをクリックします。

- **[Deploy]**：この設定をただちに使用します。
- **[Cancel]**：エントリを保存せずにこの手順を終了して、[ACL Summary] テーブルに戻ります。

関連トピック

- 「ACL を使用したセキュリティの設定」（P.2-37）
- 「ACL の作成」（P.2-38）
- 「拡張 ACL アトリビュートの設定」（P.2-40）
- 「拡張 ACL のリシーケンス」（P.2-44）
- 「ACL の編集または削除」（P.2-46）

コンテキスト別の全 ACL の表示

この手順を使用して、設定されたすべてのアクセス コントロール リストを表示します。

手順

ステップ 1　**[Config] > [Virtual Contexts]** を選択します。[All Virtual Contexts] テーブルが表示されます。

ステップ 2　表示する ACL のある仮想コンテキストを選択し、**[Security] > [ACLs]** を選択します。[ACLs] テーブルが表示され、名前、そのタイプ（Extended か EtherType か）、およびコメントとともに既存 ACL がリストされます。

関連トピック

- 「仮想コンテキスト エキスパート オプション設定」（P.2-55）
- 「ACL の作成」（P.2-38）
- 「EtherType ACL アトリビュートの設定」（P.2-44）
- 「拡張 ACL アトリビュートの設定」（P.2-40）
- 「ACL の編集または削除」（P.2-46）

ACL の編集または削除

ACL またはそのいずれかのサブエントリを削除または編集するには、次の手順を使用します。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [Security] > [ACLs]** を選択します。[ACLs] テーブルが表示され、既存 ACL がリストされます。

ステップ 2　編集または削除する ACL の左側にあるラジオ ボタンを選択します。検索しているサブエントリ ACL が表示されるまで、ACL エントリの左側にあるプラス記号をクリックして必要に応じてエントリを展開します。または、**[Expand All]** アイコンをクリックして、すべての ACL とサブエントリを表示します。

ステップ 3　次のいずれかの手順を実行します。

- ACL またはそのエントリの 1 つを編集する場合は、**[Edit]** をクリックして、ステップ 4 に進みます。

または

- ACL またはそのエントリの 1 つを削除する場合は、**[Delete]** をクリックして、ステップ 5 に進みます。

ステップ 4　必要に応じて表 2-11 に一覧表示されている概要情報を使用してエントリを編集して、完了したら **[Deploy]** をクリックします。

ステップ 5　**[Delete]** をクリックします。削除の確認を求めるウィンドウが表示されます。**[OK]** をクリックした場合、[ACLs] テーブルが ACL を削除せずにリフレッシュされます。

関連トピック

- 「ACL の作成」（P.2-38）
- 「EtherType ACL アトリビュートの設定」（P.2-44）
- 「拡張 ACL アトリビュートの設定」（P.2-40）
- 「拡張 ACL のリシーケンス」（P.2-44）

オブジェクト グループの設定

オブジェクト グループ（object group）は、ホスト（サーバおよびクライアント）、サービス、ネットワークなどのオブジェクトの論理グループです。オブジェクト グループを作成した場合、ネットワークやサービスなどのタイプを選択し、グループに属するオブジェクトを指定します。全体で、4 つのタイプのオブジェクト グループ（ネットワーク、プロトコル、サービス、ICMP）があります。

オブジェクト グループの設定後、これを ACL 内に含めることができ、それによってそのグループ内に全オブジェクトを含めて、全体的な設定サイズを削除します。

この手順を使用して ACL に関連付けることのできるオブジェクト グループを設定します。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [Security] > [Object Groups]** を選択します。[Object Groups] テーブルが表示され、既存のオブジェクト グループがリストされます。

ステップ 2　**[Add]** をクリックして新規オブジェクト グループを作成するか、既存のオブジェクト グループを選択して、**[Edit]** をクリックしてこれを修正します。[Object Groups] 設定画面が表示されます。

ステップ 3　[Name] フィールドで、このオブジェクト グループの一意の名前を入力します。有効な値は、スペースを含まない引用符抜きの英数字です（最大 64 文字）。

ステップ 4　[Description] フィールドに、このオブジェクト グループの概要を入力します。

ステップ 5　[Type] フィールドで、作成しているオブジェクト グループのタイプを選択します。

- [Network]：オブジェクト グループがホストのグループやサブネット IP アドレスに基づいています。
- [Service]：オブジェクト グループが TCP または UDP プロトコルおよびポート、または echo や echo-reply などの ICMP タイプに基づいています。

ステップ 6　次のいずれかをクリックします。

- **[Deploy Now]**：この設定をただちに使用します。このオプションが表示されるのは、仮想コンテキストの場合です。
- **[Cancel]**：エントリを保存せずにこの手順を終了して、[Object Groups] テーブルに戻ります。
- **[Next]**：エントリを導入して、別のエントリを [Object Groups] テーブルに追加します。

[Deploy Now] または **[OK]** をクリックすると、追加の設定オプションが示されたテーブルで画面がリフレッシュされます。

ステップ 7　オブジェクト グループのオブジェクトを設定します。

ネットワークタイプ オブジェクト グループの場合、オプションには次のものが含まれています。

- 「オブジェクト グループの IP アドレス設定」（P.2-48）
- 「オブジェクト グループのサブネット オブジェクト設定」（P.2-49）

サービスタイプ オブジェクト グループの場合、オプションには次のものが含まれています。

- 「オブジェクト グループのプロトコル設定」（P.2-49）
- 「オブジェクト グループの TCP/UDP サービス パラメータ設定」（P.2-50）
- 「オブジェクト グループの ICMP サービス パラメータ設定」（P.2-52）

関連トピック

- 「仮想コンテキスト エキスパート オプション設定」（P.2-55）
- 「ACL の作成」（P.2-38）
- 「拡張 ACL アトリビュートの設定」（P.2-40）
- 「拡張 ACL のリシーケンス」（P.2-44）

オブジェクト グループの IP アドレス設定

この手順を使用して、ネットワークタイプのオブジェクト グループのホスト IP アドレスを指定します。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [Security] > [Object Groups]** を選択します。[Object Groups] テーブルが表示され、既存のオブジェクト グループがリストされます。

ステップ 2　ホスト IP アドレスを設定するオブジェクト グループを選択して、[Host Setting For Object Group] タブを選択します。[Host Setting For Object Group] テーブルが表示されます。

ステップ 3　**[Add]** をクリックして、このテーブルにエントリを追加します。

ステップ 4　[Host IP Address] フィールドに、このグループに含めるホストの IP アドレスを入力します。

ステップ 5　次のいずれかをクリックします。

- **[Deploy Now]**：この設定をただちに使用します。このオプションが表示されるのは、仮想コンテキストの場合です。
- **[Cancel]**：エントリを保存せずにこの手順を終了します。
- **[Next]**：エントリを導入して、別のエントリを [Host Setting] テーブルに追加します。

関連トピック

- 「オブジェクト グループの設定」（P.2-47）
- 「オブジェクト グループのサブネット オブジェクト設定」（P.2-49）
- 「オブジェクト グループのプロトコル設定」（P.2-49）
- 「オブジェクト グループの TCP/UDP サービス パラメータ設定」（P.2-50）
- 「オブジェクト グループの ICMP サービス パラメータ設定」（P.2-52）

オブジェクト グループのサブネット オブジェクト設定

この手順を使用して、ネットワークタイプのオブジェクト グループのサブネット オブジェクトを指定します。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [Security] > [Object Groups]** を選択します。[Object Groups] テーブルが表示され、既存のオブジェクト グループがリストされます。

ステップ 2　サブネット オブジェクトを設定するオブジェクト グループを選択して、[Network Setting For Object Group] タブを選択します。[Network Setting For Object Group] テーブルが表示されます。

ステップ 3　**[Add]** をクリックして、このテーブルにエントリを追加します。

ステップ 4　[IP Address] フィールドに、サブネット オブジェクトを定義する IP アドレスとサブネット マスクを入力します。

ステップ 5　[Netmask] フィールドで、このサブネット オブジェクト用のサブネット マスクを選択します。

ステップ 6　次のいずれかをクリックします。

- **[Deploy Now]**：この設定をただちに使用します。このオプションが表示されるのは、仮想コンテキストの場合です。
- **[Cancel]**：エントリを保存せずにこの手順を終了します。
- **[Next]**：エントリを導入して、別のエントリを [Network Setting] テーブルに追加します。

関連トピック

- 「オブジェクト グループの設定」（P.2-47）
- 「オブジェクト グループの IP アドレス設定」（P.2-48）
- 「オブジェクト グループのプロトコル設定」（P.2-49）
- 「オブジェクト グループの TCP/UDP サービス パラメータ設定」（P.2-50）
- 「オブジェクト グループの ICMP サービス パラメータ設定」（P.2-52）

オブジェクト グループのプロトコル設定

この手順を使用して、サービスタイプ オブジェクト グループのプロトコルを指定します。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [Security] > [Object Groups]** を選択します。[Object Groups] テーブルが表示され、既存のオブジェクト グループがリストされます。

ステップ 2　既存のサービスタイプ オブジェクト グループを選択して、[Protocol Selection] タブを選択します。[Protocol Selection] テーブルが表示されます。

ステップ 3　**[Add]** をクリックして、このテーブルにエントリを追加します。

ステップ 4　[Protocol Number] フィールドで、このオブジェクト グループに追加するプロトコルまたはプロトコル番号を選択します。一般的なプロトコルとその番号については、表 2-13 を参照してください。

ステップ 5　次のいずれかをクリックします。

- **[Deploy Now]**：この設定をただちに使用します。このオプションが表示されるのは、仮想コンテキストの場合です。
- **[Cancel]**：エントリを保存せずにこの手順を終了します。
- **[Next]**：エントリを導入して、別のエントリを [Protocol Selection] テーブルに追加します。

関連トピック

- 「オブジェクト グループの設定」（P.2-47）
- 「オブジェクト グループの IP アドレス設定」（P.2-48）
- 「オブジェクト グループのサブネット オブジェクト設定」（P.2-49）
- 「オブジェクト グループの TCP/UDP サービス パラメータ設定」（P.2-50）
- 「オブジェクト グループの ICMP サービス パラメータ設定」（P.2-52）

オブジェクト グループの TCP/UDP サービス パラメータ設定

この手順を使用して、TCP または UDP サービス オブジェクトをサービスタイプ オブジェクト グループに追加します。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [Security] > [Object Groups]** を選択します。[Object Groups] テーブルが表示され、既存のオブジェクト グループがリストされます。

ステップ 2　既存のサービスタイプ オブジェクト グループを選択して、[TCP/UDP Service Parameter] タブを選択します。[TCP/UDP Service Parameters] テーブルが表示されます。

ステップ 3　**[Add]** をクリックして、このテーブルにエントリを追加します。

ステップ 4　表 2-14 内の情報を使用して、TCP または UDP サービス オブジェクトを設定します。

表 2-14　TCP および UDP サービス パラメータ

フィールド	説明
[Protocol]	このサービス オブジェクトのプロトコルを選択します。 • [TCP] : TCP は、このサービス オブジェクト用のプロトコルです。 • [UDP] : UDP は、このサービス オブジェクト用のプロトコルです。 • [TCP And UDP] : TCP と UDP の両方が、このサービス オブジェクト用のプロトコルです。
[Source Port Operator]	このサービス オブジェクトの送信元ポート番号を比較する際に使用するオペランドを選択します。 • [Equal To] : 送信元ポートは [Source Port] フィールドの番号と同じでなければなりません。 • [Greater Than] : 送信元ポートは [Source Port] フィールドの番号よりも大きくなければなりません。 • [Less Than] : 送信元ポートは [Source Port] フィールドの番号よりも小さくなければなりません。 • [Not Equal To] : 送信元ポートは [Source Port] フィールドの番号と等しくなってはいけません。 • [Range] : 送信元ポートは、[Lower Source Port] フィールドと [Upper Source Port] フィールドに指定されたポートの範囲内でなければなりません。
[Source Port]	このフィールドは、[Source Port Operator] フィールドで [Equal To]、[Greater Than]、[Less Than]、または [Not Equal To] が選択された場合に表示されます。 このサービス オブジェクトの送信元ポート名または番号を入力します。
[Lower Source Port]	このフィールドは、[Source Port Operator] フィールドで [Range] が選択された場合に表示されます。 このサービス オブジェクトのサービス範囲の開始値である番号を入力します。有効な入力は 0 ～ 65535 の整数です。このフィールド内の数字は、[Uppser Source Port] フィールドに入力した数字よりも小さい必要があります。
[Upper Source Port]	このフィールドは、[Source Port Operator] フィールドで [Range] が選択された場合に表示されます。 このサービス オブジェクトのサービス範囲の終了値である番号を入力します。有効な入力は 0 ～ 65535 の整数です。このフィールド内の数字は、[Lower Source Port] フィールドに入力した数字よりも大きい必要があります。
[Destination Port Operator]	宛先ポート番号を比較する際に使用するオペランドを選択します。 • [Equal To] : 宛先ポートは [Destination Port] フィールドの番号と同じでなければなりません。 • [Greater Than] : 宛先ポートは [Destination Port] フィールドの番号よりも大きくなければなりません。 • [Less Than] : 宛先ポートは [Destination Port] フィールドの番号よりも小さくなければなりません。 • [Not Equal To] : 宛先ポートは [Destination Port] フィールドの番号と等しくなってはいけません。 • [Range] : 宛先ポートは、[Lower Destination Port] フィールドと [Upper Destination Port] フィールドに指定されたポートの範囲内でなければなりません。

表 2-14　TCP および UDP サービス パラメータ （続き）

フィールド	説明
[Destination Port]	このフィールドは、[Destination Port Operator] フィールドで [Equal To]、[Greater Than]、[Less Than]、または [Not Equal To] が選択された場合に表示されます。 このサービス オブジェクトの宛先ポート名または番号を入力します。
[Lower Destination Port]	このフィールドは、[Destination Port Operator] フィールドで [*Range*] が選択された場合に表示されます。 このサービス オブジェクトのサービス範囲の開始値である番号を入力します。有効な入力は 0 ～ 65535 の整数です。このフィールド内の数字は、[Upper Destination Port] フィールドに入力した数字よりも小さい必要があります。
[Upper Destination Port]	このフィールドは、[Destination Port Operator] フィールドで [*Range*] が選択された場合に表示されます。 このサービス オブジェクトのサービス範囲の終了値である番号を入力します。有効な入力は 0 ～ 65535 の整数です。このフィールド内の数字は、[Lower Destination Port] フィールドに入力した数字よりも大きい必要があります。

ステップ 5　次のいずれかをクリックします。

- **[Deploy Now]**：この設定をただちに使用します。このオプションが表示されるのは、仮想コンテキストの場合です。
- **[Cancel]**：エントリを保存せずにこの手順を終了します。
- **[Next]**：エントリを導入して、別のエントリを [TCP/UDP Service Parameters] テーブルに追加します。

関連トピック

- 「オブジェクト グループの設定」（P.2-47）
- 「オブジェクト グループの IP アドレス設定」（P.2-48）
- 「オブジェクト グループのサブネット オブジェクト設定」（P.2-49）
- 「オブジェクト グループのプロトコル設定」（P.2-49）
- 「オブジェクト グループの ICMP サービス パラメータ設定」（P.2-52）

オブジェクト グループの ICMP サービス パラメータ設定

この手順を使用して、ICMP サービス パラメータをサービスタイプ オブジェクト グループに追加します。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [Security] > [Object Groups]** を選択します。[Object Groups] テーブルが表示され、既存のオブジェクト グループがリストされます。

ステップ 2　既存のサービスタイプ オブジェクト グループを選択して、[ICMP Service Parameters] タブを選択します。[ICMP Service Parameters] テーブルが表示されます。

ステップ 3　**[Add]** をクリックして、このテーブルにエントリを追加します。

ステップ 4　表 2-15 内の情報を使用して ICMP タイプ オブジェクトを設定します。

表 2-15　ICMP タイプ サービス パラメータ

フィールド	説明
[ICMP Type]	このサービス オブジェクトの ICMP タイプまたは番号を選択します。 表 2-16 に、一般的な ICMP タイプと番号をリストします。
[Message Code Operator]	このサービス オブジェクトのメッセージ コードを比較する際に使用するオペランドを選択します。 • [Equal To]：メッセージ コードは [Message Code] フィールドの番号と同じでなければなりません。 • [Greater Than]：メッセージ コードは [Message Code] フィールドの番号よりも大きくなければなりません。 • [Less Than]：メッセージ コードは [Message Code] フィールドの番号よりも小さくなければなりません。 • [Not Equal To]：メッセージ コードは [Message Code] フィールドの番号と等しくなってはいけません。 • [Range]：メッセージ コードは、[Min. Message Code] フィールドと [Max. Message Code] フィールドで指定された コードの範囲内に 収まっていなければいけません。
[Message Code]	このフィールドは、[Message Code Operator] フィールドで [Equal To]、[Greater Than]、[Less Than]、または [Not Equal To] が選択された場合に表示されます。 このサービス オブジェクトの ICMP メッセージ コードを入力します。
[Min.Message Code]	このフィールドは、[Message Code Operator] フィールドで [Range] が選択された場合に表示されます。 このサービス オブジェクトのサービス範囲の開始値である番号を入力します。有効な入力は 0 ～ 255 の整数です。このフィールド内の番号は、[Max. Message Code] フィールド内に入力された番号よりも 小さくなければいけません。
[Max.Message Code]	このフィールドは、[Message Code Operator] フィールドで [Range] が選択された場合に表示されます。 このサービス オブジェクトのサービス範囲の終了値である番号を入力します。有効な入力は 0 ～ 255 の整数です。このフィールド内の番号は、[Min. Message Code] フィールド内に入力された番号よりも 大きくなければいけません。

表 2-16　ICMP タイプ番号と名前

番号	ICMP タイプ名
0	Echo-Reply
3	Unreachable
4	Source-Quench
5	Redirect
6	Alternate-Address

表 2-16　ICMP タイプ番号と名前 （続き）

番号	ICMP タイプ名
8	Echo
9	Router-Advertisement
10	Router-Solicitation
11	Time-Exceeded
12	Parameter-Problem
13	Timestamp-Request
14	Timestamp-Reply
15	Information-Request
16	Information-Reply
17	Mask-Request
18	Mask-Reply
31	Conversion-Error
32	Mobile-Redirect

ステップ 5　次のいずれかをクリックします。

- **[Deploy Now]**：この設定をただちに使用します。このオプションが表示されるのは、仮想コンテキストの場合です。
- **[Cancel]**：エントリを保存せずにこの手順を終了します。
- **[Next]**：エントリを導入して、別のエントリを [ICMP Service Parameters] テーブルに追加します。

関連トピック

- 「オブジェクト グループの設定」（P.2-47）
- 「オブジェクト グループの IP アドレス設定」（P.2-48）
- 「オブジェクト グループのサブネット オブジェクト設定」（P.2-49）
- 「オブジェクト グループのプロトコル設定」（P.2-49）
- 「オブジェクト グループの TCP/UDP サービス パラメータ設定」（P.2-50）

仮想コンテキスト エキスパート オプション設定

表 2-17 は、ACE Appliance Device Manager 仮想コンテキスト エキスパート設定オプションと詳細情報の関連トピックを示したものです。

表 2-17　仮想コンテキスト エキスパート設定オプション

エキスパート設定オプション	関連トピック
ネットワーク トラフィックのタイプを分類し、その後トラフィックを処理するためのルールとアクションを適用することによるトラフィック ポリシーの確立	• 「トラフィック ポリシーの設定」（P.10-1） • 「仮想コンテキスト クラス マップの作成」（P.10-9） • 「仮想コンテキスト ポリシー マップの作成」（P.10-35）
HTTP 最適化アクション リストの設定	「HTTP 最適化アクション リストの設定」（P.11-4）
HTTP ヘッダー修正アクション リストの設定	「HTTP ヘッダー修正アクション リストの設定」（P.10-84）

仮想コンテキストの管理

仮想コンテキストで次の管理アクションを実行できます。

- 「仮想コンテキスト設定の同期」（P.2-55）
- 「仮想コンテキストの編集」（P.2-59）
- 「仮想コンテキストの削除」（P.2-60）
- 「すべての仮想コンテキストの表示」（P.2-60）

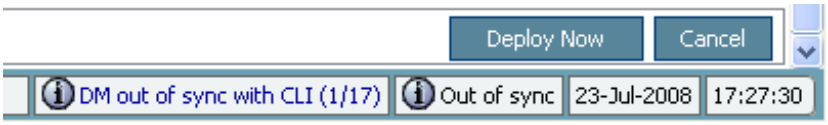
仮想コンテキスト設定の同期

ACE Appliance Device Manager は、ACE Appliance と ACE Appliance Device Manager の別の設定で仮想コンテキストを特定します。これらの設定の不一致は、ユーザが ACE Appliance Device Manager ではなく CLI を使用して直接 ACE Appliance を設定した場合に発生します。

ACE Appliance Device Manager は、2 分おきに自動的に CLI をポーリングします。CLI を使用して ACE Appliance の仮想コンテキストの設定を変更して、デバイス マネージャがこのポーリング期間中にコンテキストでのアウトオブバンド設定変更を検出した場合、設定変更がデバイス マネージャによって適用されます。

ACE Appliance Device Manager の右下にあるステータス バーに、ユーザが CLI と DM GUI 同期ステータスを監視するための 2 つのインジケータが表示されます（図 2-1）。1 つのインジケータには、さまざまな同期ステータスになっているコンテキストの概要カウントとともに ACE Appliance Device Manager GUI と CLI 同期ステータスが表示され、もう 1 つのインジケータには、アクティブ コンテキストの CLI 同期およびポーリング ステータスが表示されます。ステータス バーは 10 秒ごとに自動的にリフレッシュされます。

図 2-1　CLI および DM GUI 同期ステータス バー



たとえば、図 2-1 で示しているように、メッセージ「DM out of sync with CLI (1/17)」は、17 の設定済みコンテキストから 1 つのコンテキストが「Out of sync」CLI 同期ステータス状態になっていることを示します。

（注）　特定コンテキストで同期が進行している間に、([Deploy Now] ボタンをクリックして）ACE Appliance Device Manager からユーザが設定を導入しようとすると、同期が進行中であり、ユーザは後の時点で設定の導入を試行する必要があることを示すエラー メッセージが表示されます。

ACE Appliance Device Manager には、設定の不一致を特定し同期するための次のオプションがあります。

- 「仮想コンテキスト同期ステータスの表示」（P.2-56）
- 「ハイ アベイラビリティおよび仮想コンテキスト設定ステータス」（P.2-57）
- 「個々の仮想コンテキスト設定の手動同期」（P.2-58）
- 「全仮想コンテキスト設定の手動同期」（P.2-58）

仮想コンテキスト同期ステータスの表示

ACE Appliance Device Manager では、ACE Appliance と ACE Appliance Device Manager とで異なる設定を使用して仮想コンテキストを特定します。これらの設定の不一致は、ユーザが ACE Appliance Device Manager ではなく CLI を使用して直接 ACE Appliance を設定した場合に発生します。

[Config] 画面で、CLI および DM GUI 設定ステータスが ACE Appliance Device Manager の次の場所に表示されます。

- [All Virtual Contexts] テーブル（**[Config] > [Virtual Contexts]**）の、[CLI Sync Status] 列
- ACE Appliance Device Manager ブラウザの下部にあるステータス バー（図 2-1 を参照）

次のレポートされた CLI 同期状態が [All Virtual Context] テーブルに表示されます。

- [OK]：選択された仮想コンテキストの設定が CLI で同期されます。
- [Out Of sync]：選択された仮想コンテキストの設定が CLI で同期されません。
- [Sync In progress]：このコンテキストに対する CLI と DM GUI の同期が進行中で、ACE Appliance Device Manager によって自動的に開始されたか、([CLI Sync] または [CLI Sync All] のいずれかのボタンを使用して）手動で開始されました。
- [Sync Failed]：最後の同期試行に失敗しました。[CLI Sync] または [CLI Sync All] のいずれかのボタンを使用して手動同期を実行する必要があります。失敗ステートは、コンテキストで認識されていない CLI コマンドによるものか、ACE Appliance Device Manager の内部エラーによるものです。問題が解決したら、コンテキストを [OK] 同期状態に移行させるために別の手動同期が必要です。

ACE Appliance Device Manager ブラウザの下にあるステータス バー（図 2-1 を参照）に、さまざまな同期ステートのコンテキストの概要カウントとともに DM GUI と CLI との同期ステータスが表示されます。たとえば、メッセージ「DM out of sync with CLI (1/10), DM sync with CLI failed (2/10)」は、設定済みの 10 コンテキストの内、1 つのコンテキストが「Out Of Sync」ステートで、2 つが「Sync Failed」ステートで、残りのコンテキストが「OK」ステートになっていることを示します。ステータス バーは 10 秒ごとに自動的にリフレッシュされます。

（注）　コンテキスト固有ページからステータスバー内の概要カウントをクリックすると、[All Virtual Contexts] テーブルにアクセスできます。全コンテキストの CLI 同期ステータスを表示できます。

[All Virtual Contexts] テーブルの表示中に、ユーザが CLI を使用してコンテキストの設定を変更した場合、[CLI Sync Status] 列内の情報は同期外状態を反映するために自動的に更新されません。**[Refresh]** をクリックするか、**[Auto Refresh]** をクリックして自動リフレッシュ レートを設定して、同期外設定を確認します。

同期外仮想コンテキスト設定の同期に関する詳細については、次の項目を参照してください。

- 「個々の仮想コンテキスト設定の手動同期」（P.2-58）
- 「全仮想コンテキスト設定の手動同期」（P.2-58）

関連トピック

- 「仮想コンテキスト設定の同期」（P.2-55）
- 「ハイ アベイラビリティおよび仮想コンテキスト設定ステータス」（P.2-57）

ハイ アベイラビリティおよび仮想コンテキスト設定ステータス

ハイ アベイラビリティ ペアでは、継続的なコミュニケーションの一部として、設定された 2 つの仮想コンテキストが相互に同期を図ります。ただし、そのコピーは ACE Appliance Device Manager で同期せず、スタンバイ メンバーの設定が ACE Appliance 上の設定と同期しなくなる可能性があります。

ハイ アベイラビリティ ペアのアクティブ メンバーに障害が発生してスタンバイ メンバーがアクティブになった後で、新規にアクティブになったメンバーの ACE Appliance Device Manager で、同期外仮想コンテキスト設定が検出され、仮想コンテキスト設定を同期できるように、[All Virtual Contexts] テーブル内のそのステータスがレポートされます。

（注）　ある仮想コンテキストが Standby Hot ステート、または Standby Warm ステート（「ハイ アベイラビリティ ポーリング」（P.9-6）を参照）のいずれかである場合、この仮想コンテキストは ACE ピアから設定変更を受け取る可能性があります。Device Manager の GUI が変更されることはありません。結果として、ACE Appliance の Device Manager の GUI は、CLI 設定と同期しなくなります。HA トラッキングおよび障害検出（「ハイ アベイラビリティ対応 VLAN インターフェイスのトラッキング」（P.9-17）を参照）を使用してスタンバイ仮想コンテキストで設定を検査する必要がある場合は、設定値を検査する前に、まず [CLI Sync] または [CLI Sync All] のいずれかのボタンを使用して手動同期を実行することをお勧めします。

同期外仮想コンテキスト設定の同期に関する詳細については、次の項目を参照してください。

- 「個々の仮想コンテキスト設定の手動同期」（P.2-58）
- 「全仮想コンテキスト設定の手動同期」（P.2-58）

関連トピック

- 「仮想コンテキスト同期ステータスの表示」（P.2-56）
- 「ハイ アベイラビリティ設定の概要」（P.9-6）

個々の仮想コンテキスト設定の手動同期

選択された仮想コンテキストの設定を手動で同期する場合にこの手順を使用します。この手順では、ACE Appliance Device Manager からこの仮想コンテキストの設定情報を削除して、ACE Appliance からの CLI 設定で置き換えます。自動同期が発生するまで待ちたくない場合は仮想コンテキスト設定を手動で同期して、CLI コンテキスト設定の変更を ACE Appliance Device Manager に即座に適用できます。

手順

ステップ 1　**[Config] > [Virtual Contexts]** を選択します。[All Virtual Contexts] テーブルが表示されます。同期されていない設定のあるコンテキストの場合、[CLI Sync Status] 列に [*Out of sync*] が表示されます。

（注）　[All Virtual Contexts] テーブルの表示中に、ユーザが CLI を使用してコンテキストの設定を変更した場合、[CLI Sync Status] 列内の情報は同期外状態を反映するために自動的に更新されません。**[Refresh]** をクリックするか、**[Auto Refresh]** をクリックして自動リフレッシュ レートを設定して、同期外設定を確認します。

ステップ 2　同期する設定のある仮想コンテキストを選択して、**[CLI Sync]** をクリックします。ウィンドウが表示され、操作の確認を求められます。

ステップ 3　**[OK]** をクリックして ACE Appliance から設定をアップロードするか、**[Cancel]** をクリックして設定をアップロードせずにこの手順を終了します。

[OK] をクリックした場合、画面で進行状況がレポートされて、[CLI Sync Status] 列で更新された設定ステータスで画面がリフレッシュされます。

関連トピック

- 「仮想コンテキスト設定の同期」（P.2-55）
- 「仮想コンテキスト同期ステータスの表示」（P.2-56）
- 「全仮想コンテキスト設定の手動同期」（P.2-58）

全仮想コンテキスト設定の手動同期

この手順を使用して、すべての仮想コンテキスト設定を手動で同期します。この手順は、すべての仮想コンテキスト設定を ACE Appliance Device Manager から削除して、ACE Appliance からの CLI 設定でこれを置き換えます。自動同期が発生するまで待ちたくない場合は仮想コンテキストをすべて手動で同期して、CLI コンテキスト設定の変更を ACE Appliance Device Manager に即座に適用できます。

仮想コンテキストの数によっては、この操作を完了するには数分かかる可能性があります。

（注）　CLI を使用して仮想サーバを設定し、[CLI Sync All] オプション（**[Config] > [Virtual Contexts]**）を使用して手動で設定を同期する場合、ACE Appliance Device Manager に表示される仮想サーバの設定には、その仮想サーバの全設定オプションが表示されない可能性があります。ACE Appliance Device Manager に表示される設定は、クラス マップに設定されているプロトコルや、ポリシー マップに対して定義されているルールなど、項目の数によって異なります。

たとえば、任意のプロトコルと一致するクラス マップを含む CLI 上に仮想サーバを設定した場合、仮想サーバのアプリケーション アクセラレーションおよび最適化設定サブセットは ACE Appliance Device Manager に表示されません。

（注）　この手順は、Admin コンテキストの管理ユーザだけが使用できます。

手順

ステップ 1　**[Config] > [Virtual Contexts]** を選択します。[All Virtual Contexts] テーブルが表示されます。

ステップ 2　**[CLI Sync All]** をクリックします。ウィンドウが表示され、操作の確認を求められます。

ステップ 3　**[OK]** をクリックしてこのオプションを続けるか、**[Cancel]** をクリックしてこの手順を終了します。

[OK] をクリックする場合、現時点でインポートされたコンテキストがリストされた [All Virtual Contexts] テーブルで画面がリフレッシュされ、設定更新の進捗が表示されます。

（注）　コンテキストの数によっては、このプロセスが完了するのに数分かかる場合があります。

ステップ 4　**[Refresh]** をクリックして、インポートされた追加コンテキストを表示します。

関連事項

- 「仮想コンテキスト設定の同期」（P.2-55）
- 「個々の仮想コンテキスト設定の手動同期」（P.2-58）

仮想コンテキストの編集

この手順を使用して、既存仮想コンテキストの設定を修正します。

手順

ステップ 1　**[Config] > [Virtual Contexts]** を選択します。[All Virtual Contexts] テーブルが表示されます。

ステップ 2　仮想コンテキストを選択して、修正する設定アトリビュートを選択します。設定オプションの詳細については、「仮想コンテキストの設定」（P.2-4）を参照してください。

ステップ 3　**[Deploy Now]** をクリックして、ACE Appliance にこの設定を導入します。

エントリを保存せずに手順を終了する場合、**[Cancel]** をクリックするか、メニュー バー内の別の項目または設定する別のアトリビュートを選択します。ウィンドウが表示され、エントリを保存しなかったことが確認されます。

関連事項

- 「仮想コンテキストの使用」（P.2-1）

仮想コンテキストの削除

この手順を使用して、既存仮想コンテキストを削除します。

手順

ステップ 1　**[Config] > [Virtual Contexts]** を選択します。[All Virtual Contexts] テーブルが表示されます。

ステップ 2　削除する仮想コンテキストを選択して、**[Delete]** をクリックします。ウィンドウが表示され、削除が確認されます。

ステップ 3　次のいずれかをクリックします。

- **[OK]**：選択されたコンテキストを削除します。デバイス ツリーがリフレッシュされ、削除されたコンテキストが表示されなくなります。
- **[Cancel]**：この手順を終了し、選択されたコンテキストを残します。

関連事項

- 「仮想コンテキストの使用」（P.2-1）

すべての仮想コンテキストの表示

すべての仮想コンテキストを表示するには、**[Config] > [Virtual Contexts]** を選択します。[All Virtual Contexts] テーブルが表示されます。

（注）　コンテキスト固有ページからステータスバー内の概要カウントをクリックすると、[All Virtual Contexts] テーブルにアクセスできます。すべての利用可能なコンテキストの同期設定詳細を見直すことができます。管理者ではない場合、ユーザ コンテキストの詳細だけが表示されます。

[All Virtual Contexts] テーブルに、各仮想コンテキストの次の情報が表示されます。

- 名前
- リソース クラス
- 管理 IP アドレス
- 仮想コンテキスト同期ステータス（コンテキストの ACE Appliance Device Manager GUI および CLI 設定が同期しているか、同期していないか、同期中か、同期試行に失敗したのか）。詳細については、「仮想コンテキスト同期ステータスの表示」（P.2-56）を参照してください。

- ACE ハイ アベイラビリティ ステート。利用可能な ACE ハイ アベイラビリティ ステートの詳細については、「ハイ アベイラビリティ ポーリング」（P.9-6）を参照してください。

（注）　ACE Appliance Device Manager GUI および CLI 設定同期における ACE ハイ アベイラビリティの意味の詳細については、「ACE Appliance Device Manager とのハイ アベイラビリティ設定の同期」（P.9-7）を参照してください。

- ACE ハイ アベイラビリティ ピアの状態
- ACE ハイ アベイラビリティ ピア名
- ハイ アベイラビリティ ペアの自動同期が設定されているかどうか

（注）　[All Virtual Contexts] テーブルの表示中に、ユーザが CLI を使用してコンテキストの設定を変更した場合、またはハイ アベイラビリティ ステートを変更した場合、テーブル列内の情報は同期外状態を反映するために自動的に更新されません。**[Refresh]** をクリックするか、**[Auto Refresh]** をクリックして自動リフレッシュ レートを設定して、同期外設定を確認します。

（注）　[All Virtual Contexts] テーブルの表示中に、ユーザが別のセッションで新規仮想コンテキストを作成した場合、新規仮想コンテキストは自動的にこのテーブルに表示されません。**[Refresh]** をクリックするか、**[Auto Refresh]** をクリックして自動リフレッシュ レートを設定して、新規作成コンテキストを表示します。

選択されたコンテキストのポーリング ステータスが、右上隅にあるコンテンツ エリアの上部に表示されます（図 1-2 を参照）。表 12-1 で、さまざまなポーリング状態を説明します。

この画面から次のことが可能です。

- 新規仮想コンテキストの追加（「仮想コンテキストの作成」（P.2-2）を参照）
- 既存の仮想コンテキストの編集（「仮想コンテキストの設定」（P.2-4）を参照）
- 既存の仮想コンテキストの削除（「仮想コンテキストの削除」（P.2-60）を参照）
- 1 つまたはすべての仮想コンテキストの ACE Appliance Device Manager および CLI 設定の手動同期（「仮想コンテキスト設定の同期」（P.2-55）を参照）

関連事項

「仮想コンテキストの管理」（P.2-55）