Cisco Application Control Engine モジュール Virtualization コンフィギュレーション ガイド

Software Version A2(1.0)
March 2008

Text Part Number: OL-11870-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。米国サイト掲載ドキュメントとの差異が生じる場合があるため、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco Application Control Engine モジュール Virtualization コンフィギュレーション ガイド

CONTENTS

はじめに

このマニュアルでは、Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータ（以下、それぞれスイッチまたはルータと呼ぶ）を対象に、1 つまたは複数のコンテキストでの Cisco Application Control Engine（ACE）モジュールの設定方法について説明します。

複数のコンテキストでは、仮想化の概念を使用して、ACE を複数の仮想デバイスまたは仮想コンテキストに分割します。また、このマニュアルでは、仮想化機能ツールを使用して、ACE のシステム リソースおよびユーザだけでなく、顧客に提供するサービスも緊密かつ効率的に管理する方法を説明します。

ここで説明する内容は、次のとおりです。

対象読者

このマニュアルは、ACE の設定責任者であり、トレーニングを受け、資格を持った次のサービス担当者を対象としています。

- Web マスター
- システム管理者
- システム オペレータ

このマニュアルの使用方法

このマニュアルは、次の章で構成されています。

章	説明
第 1 章「概要」	ACE を複数の仮想デバイスまたは仮想コンテキストに分割するための基本的な概念を説明します。これには、以下に関する情報が含まれます。 • コンテキスト • ドメイン • ロールベース アクセス コントロール（RBAC） • リソース クラス
第 2 章「仮想化の設定」	1 つのまたは複数のコンテキストでの動作、リソースの割り当て、ドメインの作成、ユーザおよびユーザ ロールの作成を行うための、ACE の設定方法を説明します。
第 3 章「仮想化設定および統計の表示」	ACE で設定されているコンテキストのコンフィギュレーションや統計情報を表示する方法を説明します。

関連資料

このマニュアルのほかに、ACE マニュアル セットには以下のものが含まれています。

マニュアル タイトル	説明
『*Release Note for the Cisco Application Control Engine Module*』	ACE の操作上の考慮事項や警告、および CLI コマンドが記載されています。
『*Cisco Application Control Engine Module Hardware Installation Note*』	Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータへの、ACE の搭載方法が掲載されています。
『*Cisco Application Control Engine Module Getting Started Guide*』	ACE で、初期セットアップおよび設定作業を実行する方法を説明しています。
『*Cisco Application Control Engine Module Administration Guide*』	ACE で以下の管理作業を実行する方法を説明しています。 • ACE のセットアップ • リモート アクセスの確立 • ソフトウェア ライセンスの管理 • クラス マップおよびポリシー マップの設定 • ACE ソフトウェアの管理 • SNMP の設定 • 冗長性の設定 • XML インターフェイスの設定 • ACE ソフトウェアのアップグレード
『*Cisco Application Control Engine Module Routing and Bridging Configuration Guide*』	ACE で、以下のルーティングおよびブリッジング機能を設定する方法を説明しています。 • VLAN インターフェイス • ルーティング • ブリッジング • Dynamic Host Configuration Protocol（DHCP）

マニュアル タイトル	説明
『*Cisco Application Control Engine Module Server Load-Balancing Guide*』	ACE で、以下のサーバ ロード バランシング機能を設定する方法を説明しています。 • 実サーバおよびサーバ ファーム • サーバ ファーム内で実サーバへのトラフィックのロード バランシングを行うためのクラスマップおよびポリシー マップ • サーバのヘルス モニタリング（プローブ） • スティッキ性 • ファイアウォールのロード バランシング • TCL スクリプト
『*Cisco Application Control Engine Module Security Configuration Guide*』	以下の ACE セキュリティ機能の設定方法を説明しています。 • セキュリティ アクセス コントロール リスト（ACL） • TACACS+（Terminal Access Controller Access Control System Plus）、RADIUS（DRemote Authentication Dial-In User Service）、または LDAP（Lightweight Directory Access Protocol）サーバを使用したユーザ認証およびアカウンティング • アプリケーション プロトコルおよび HTTP ディープ パケット インスペクション • TCP/IP 標準化およびターミネーション パラメータ • ネットワーク アドレス変換（NAT）
『*Cisco Application Control Engine Module SSL Configuration Guide*』	ACE で、以下の Secure Sockets Layer（SSL）機能を設定する方法を説明しています。 • SSL 証明書およびキー • SSL 開始 • SSL 終了 • エンドツーエンド SSL

マニュアル タイトル	説明
『*Cisco Application Control Engine Module System Message Guide*』	ACE でシステム メッセージ ロギングを設定する方法を説明しています。このマニュアルには、ACE で生成されるシステム ログ（Syslog）メッセージのリストと説明も記載されています。
『*Cisco Application Control Engine Module Command Reference*』	構文、オプション、および関連コマンドなど、モードごとのすべての CLI コマンドのアルファベット順のリストと説明が記載されています。
『*Cisco CSM-to-ACE Conversion Tool User Guide*』	CSM-to-ACE Conversion Tool を使用して、Cisco Content Switching Module（CSM; コンテント スイッチング モジュールまたはスタートアップ コンフィギュレーション ファイルを ACE に移行する方法を説明しています。
『*Cisco CSS-to-ACE Conversion Tool User Guide*』	CSS-to-ACE Conversion Tool を使用して、Cisco Content Services Switches（CSS; コンテント サービス スイッチ）またはスタートアップ コンフィギュレーション ファイルを ACE に移行する方法を説明しています。

記号と表記

このマニュアルでは、次の表記法を使用しています。

表記	説明
太字	コマンド、コマンド オプション、およびキーワードは**太字**で示しています。段落中のコマンドも太字で示されます。
イタリック体	ユーザが値を指定する引数は、*イタリック体*で示しています。初めて記載される新しい用語、文書のタイトル、強調されるテキストもイタリック体で示されます。
{ }	必要な引数およびキーワードを囲んで示します。
[ ]	省略可能な引数およびキーワードを囲んで示します。
{ x | y | z }	必ずどれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
ストリング	引用符を付けない一組の文字。ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングとみなされます。
`screen` フォント	システムが表示する端末セッションおよび情報は、`screen` フォントで示しています。
太字の **`screen`** フォント	コマンドライン中にユーザが入力しなければならない情報は、**太字**の **`screen`** フォントで示しています。
*イタリック体*の *`screen`* フォント	ユーザが値を指定する引数は、*イタリック体* の *`screen`* フォントで示しています。
^	^ 記号は、Ctrl キーを表します。たとえば、画面に表示される ^D というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します。
< >	パスワードのように出力されない文字は、かぎカッコ（< >）で囲んで示しています。

（注）は、次のように表しています。

（注） 「*注釈*」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意は、次のように表しています。

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。

CLI 構文のフォーマットの詳細については、『*Cisco Application Control Engine Module Command Reference*』を参照してください。

マニュアルの入手方法、テクニカル サポート、およびセキュリティ ガイドライン

マニュアルの入手方法、テクニカル サポート、マニュアルに関するフィードバックの提供、セキュリティ ガイドライン、および推奨エイリアスと一般的なシスコのマニュアルに関する情報については、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。ここには、シスコのすべての新規および改訂版の技術マニュアルの一覧も掲載されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。

Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register/

オープン ソース ライセンスの利用に対する謝辞

本ソフトウェア ライセンスでの利用に対して、以下のとおり謝辞を表します。

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

CHAPTER 1

概要

Cisco Application Control Engine（ACE）モジュールは、1 つまたは複数のコンテキストで操作できます。複数のコンテキストでは、仮想化を使用して、ACE を複数の仮想デバイスまたは仮想コンテキストに分割します。各コンテキストには、それぞれ一連のポリシー、インターフェイス、リソース、および管理者が含まれます。この機能では、ACE のシステム リソースおよびユーザだけでなく、顧客に提供するサービスもさらに緊密かつ効率的に管理できるようなツールを提供しています。

ACE にはデフォルトで、Admin コンテキストおよび 5 つのユーザ コンテキストが提供されており、それらを設定すると、複数のコンテキストを使用できます。ユーザ コンテキストを追加する（最大 250 まで）には、シスコ システムズから別売のライセンスを入手する必要があります。ライセンスの詳細については、*Cisco Application Control Engine Module Administration Guide* を参照してください。

この章では、仮想化に関連する基本的概念の概要を説明します。主な内容は次のとおりです。

- コンテキスト
- ドメイン
- ロールベース アクセス コントロール
- リソース クラス

コンテキスト

仮想化された環境は、コンテキストと呼ばれるオブジェクトに分割されます。各コンテキストは、それぞれのポリシー、インターフェイス、ドメイン、サーバファーム、実サーバ、および管理者を持つ、独立した ACE のように動作します。各コンテキストでは管理 VLAN も設定でき、この VLAN には、Telnet または Secure Shell（SSH; セキュア シェル）を使用してアクセスできます。管理ポリシーを定義してインターフェイスに適用する方法については、『*Cisco Application Control Engine Module Administration Guide*』を参照してください。

グローバル管理者（Admin）は、各仮想デバイスまたはコンテキストの基本設定を含む Admin コンテキストから、すべてのコンテキストを設定および管理できます。スーパーバイザ エンジン経由でコンソールまたは Telnet を使用して ACE にログインすると、Admin コンテキストで認証されます。

Admin コンテキストは、他のコンテキストとほぼ同じです。相違点は、Admin コンテキストに（SSH などを使用して）ログインすると、ACE 全体および、その中のすべてのコンテキストおよびオブジェクトへの、システム管理者としての完全なアクセス権が付与されるということです。Admin コンテキストでは、Syslog サーバまたはコンテキスト設定サーバなどのネットワーク全体のリソースにアクセスできます。ACE 設定、コンテキスト、リソース クラスなどのグローバル コマンドはすべて、Admin コンテキストでのみ使用可能です。

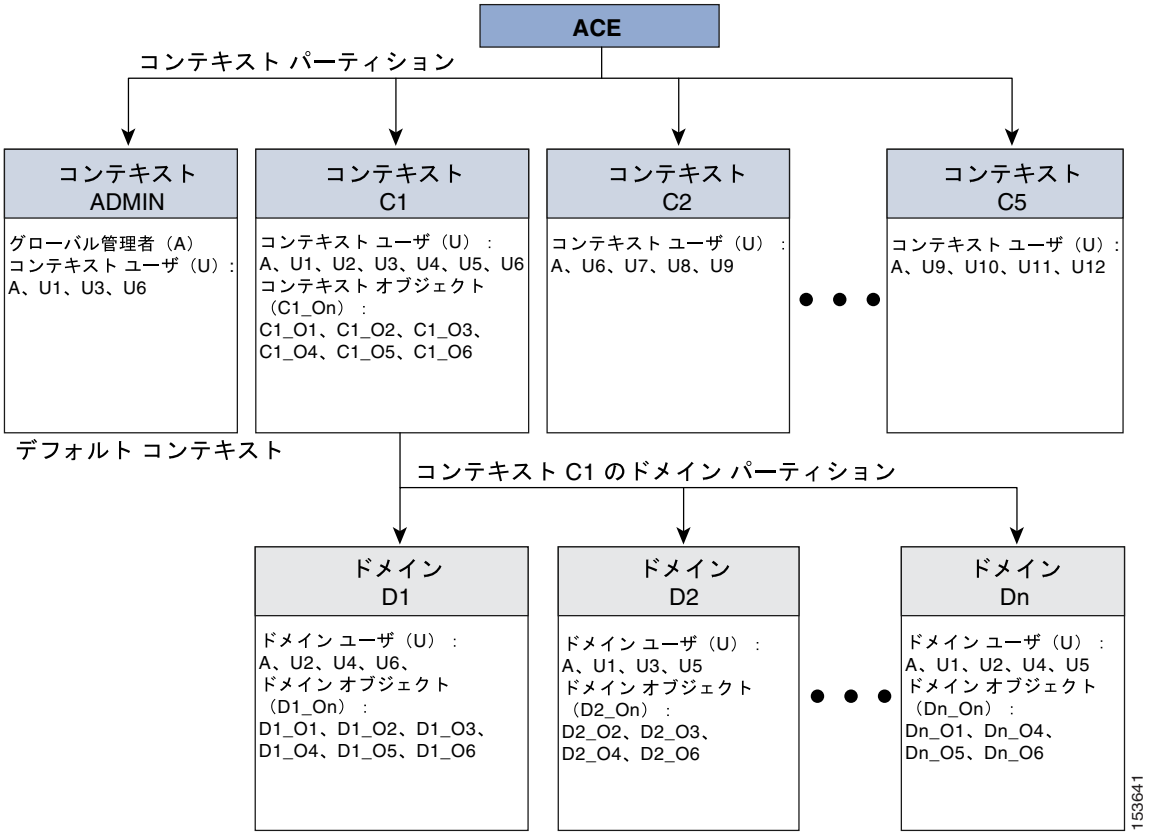
Admin コンテキストを含む各コンテキストには、それぞれのコンフィギュレーション ファイルおよびローカル ユーザ データベースがあります。これらは、フラッシュ ディスク上のローカル ディスク パーティションに格納されていますが、File Transfer Protocol（FTP; ファイル転送プロトコル）サーバ、Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバ、または HTTP（S）サーバからダウンロードすることもできます。各コンテキストの startup-config ファイルは、フラッシュ ディスク上にスタートアップ コンフィギュレーション ファイルとして格納されています。

Admin コンテキストでは、EXEC モードで **changeto** コマンドを、またはコンフィギュレーション モードで **do changeto** コマンドを使用して、コンテキスト間を移動できます。**changeto** コマンドを使用できるのは、Admin コンテキストで認証されたユーザのみです。

コンテキストの設定の詳細については、第 2 章「仮想化の設定」を参照してください。

図 1-1 は、仮想化を使用して、ACE が複数の仮想デバイスとして機能するようパーティションを作成する方法を示しています。

図 1-1　ACE 仮想化チャート



作成した各コンテキストは、仮想デバイスを表します。各コンテキストは、コンテキストへのアクセスを管理するためのドメインに分割できます。表 1-1 で、図 1-1 内に示したコンポーネントについて説明します。

表 1-1　ACE 仮想化要素

要素	説明
コンテキスト（**C*n***）	1 つの ACE に *コンテキスト*と呼ばれるパーティションを作成することで、複数の仮想化デバイスとして動作するよう設定できます。各コンテキストは、それぞれ一連のユーザ、オブジェクト、および割り当てられたリソースを持つ独立したデバイスとして機能します。ACE にはデフォルトで、Admin コンテキストおよび 5 つの設定可能なユーザ コンテキストが設定されています。ユーザ コンテキストを 250 まで作成できるようアップグレードするには、シスコ システムズから別売のライセンスを購入する必要があります。コンテキストの詳細については、「コンテキスト」を参照してください。
ドメイン（**D*n***）	各コンテキストは、*ドメイン*と呼ばれる複数のパーティションに分割でき、これを使用して、コンテキスト内のオブジェクトへのユーザのアクセスを管理できます。ドメインを作成する場合は、選択されたコンテキスト ユーザのグループと選択されたコンテキスト オブジェクトのグループの間の関連付けを作成します。ドメインの詳細については、「ドメイン」を参照してください。
ユーザ（**A**、**U*n***）	ACE にはデフォルトのグローバル システム管理者が設定されており、この管理者は、すべての ACE 機能にアクセスしたり、追加のユーザを作成したりできます。Admin コンテキスト内で作成したユーザはすべて、デフォルトで、ACE のすべてのリソースにアクセスできます。ユーザ定義のコンテキスト内で作成したユーザはすべて、そのコンテキスト内のリソースにのみアクセスできます。各ユーザにはロールを割り当てます。このロールにより、そのユーザが使用可能なコマンドおよびリソースが決定されます。ユーザおよびユーザ ロールの詳細については、第 2 章「仮想化の設定」を参照してください。

表 1-1　ACE 仮想化要素（続き）

要素	説明
オブジェクト（**C*n*_O*n***、**D*n*_O*n***）	以下のオブジェクトは、ユーザが設定可能な項目です。 • アクセス リスト • 定義済みインターフェイス • ポリシー マップ • ヘルス プローブ • 実サーバ • サーバ ファーム • スクリプト • スティッキ グループ 作成したオブジェクトは、作成時のコンテキストに固有のオブジェクトです。コンテキストが複数のドメインに分割されている場合は、各ドメイン内でオブジェクトを割り当てます。

ドメイン

管理しやすいように、コンテキストは *ドメイン*と呼ばれるオブジェクトに分割され、各ドメインは、その全体が 1 つのコンテキスト内に含まれます。ドメインには、ユーザが動作する場所となる名前空間があり、各ユーザは、少なくとも 1 つのドメインに関連付けられています。ユーザに割り当てられたロールにより、そのユーザがドメイン内のオブジェクトに対して実行可能な動作および使用可能なコマンド セットが決定されます。コンテキストを作成すると、ACE により自動的に、そのコンテキストのデフォルト ドメインが作成されます。

グローバル管理者（Admin）またはコンテキスト管理者は、追加のドメインを作成できます。ドメイン名は、関連付けられたコンテキスト内で一意である必要があります。

作成可能なオブジェクト（サーバ ファーム、実サーバ、プローブ、VLAN など）はどれでも、ドメインに追加でき、複数のドメインに同じオブジェクトを追加できます。他のオブジェクトが関連付けられているオブジェクト（実サーバが設定されているサーバ ファームなど）をドメインに追加した場合、関連付けられているオブジェクトは、自動的にはそのドメインの一部になりません。各オブジェクトを個別に追加する必要があります。オブジェクトを作成すると、ACE により自動的にドメインに追加されます。

（注） **show running-config** コマンドで表示できるコンテキスト設定が、ドメインにより制限されることはありません。ただし、ACE 内の設定可能なオブジェクトへのユーザのアクセスは、ドメインによって制限されます。ユーザにロールを割り当てることで、それらの設定可能なオブジェクトに対してユーザが実行できる動作をさらに制限できます。ユーザ ロールの詳細については、「ロールベース アクセス コントロール」を参照してください。

ドメインの設定の詳細については、第 2 章「仮想化の設定」を参照してください。

ロールベース アクセス コントロール

ACE では、各ユーザが使用可能なコマンドおよびリソースを決定するメカニズムであるロールベース アクセス コントロール（RBAC）が提供されています。ロールにより一連の権限が定義され、コンテキスト内のオブジェクトとリソース、およびそれらを実行する動作にアクセスできるようになります。グローバル管理者またはコンテキスト管理者は、ユーザのネットワーク機能およびユーザにアクセスを許可するリソースに基づいて、ユーザにロールを割り当てます。

ACE では以下の定義済みロールが提供されており、これらは、削除することも変更することもできません。

- Admin ― Admin コンテキスト内で作成した場合は、ACE 全体のすべてのコンテキスト、ドメイン、ロール、リソース、およびオブジェクトに対して完全なアクセスと制御が可能となります。ユーザ コンテキスト内でユーザを作成した場合、そのユーザはこのロールにより、そのコンテキスト内のすべてのオブジェクトに対する完全なアクセスと制御が可能となります。コンテキスト管理者は、ポリシー、ロール、ドメイン、サーバ ファーム、実サーバなど、そのコンテキスト内のあらゆるオブジェクトの作成、設定、および変更を実行できます。
- Network Admin ― 以下の機能に対する完全なアクセスと制御が可能です。
  - インターフェイス
  - ルーティング
  - 接続パラメータ
  - ネットワーク アドレス変換（NAT）
  - VIP
  - コピー設定
  - **changeto** コマンド
- Network-Monitor ― すべての **show** コマンドおよび **changeto** コマンドのみにアクセスできます。これは、**username** コマンドで明示的にユーザにロールを割り当てていない場合のデフォルトのロールです。
- Security-Admin ― コンテキスト内の以下のセキュリティ関連機能に対する完全なアクセスと制御が可能です。
  - アクセス コントロール リスト（ACL）
  - アプリケーション インスペクション
  - 接続パラメータ

  - インターフェイス
  - Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）
  - NAT
  - コピー設定
  - **changeto** コマンド
- Server-Appln-Maintenance ― 以下の機能に対する完全なアクセスと制御が可能です。
  - 実サーバ
  - サーバ ファーム
  - ロードバランシング
  - コピー設定
  - **changeto** コマンド
- Server-Maintenance ― 以下の機能に対する実サーバのメンテナンス、監視、デバッグが可能です。
  - 実サーバ ― 変更権限
  - サーバ ファーム ― デバッグ権限
  - VIP ― デバッグ権限
  - プローブ ― デバッグ権限
  - ロードバランシング ― デバッグ権限
  - **changeto** コマンド ― 作成権限
- SLB-Admin ― コンテキスト内の以下の ACE 機能に対する完全なアクセスと制御が可能です。
  - 実サーバ
  - サーバ ファーム
  - VIP
  - プローブ
  - ロードバランシング（レイヤ 3/4 およびレイヤ 7）
  - NAT
  - インターフェイス
  - コピー設定

  - **changeto** コマンド
- SSL-Admin ― すべての Secure Sockets Layer（SSL）機能の管理者です。
  - SSL ― 作成権限
  - Public Key Infrastructure（PKI; 公開鍵インフラストラクチャ）― 作成権限
  - インターフェイス ― 変更権限
  - コピー設定 ― 作成権限
  - **changeto** コマンド ― 作成権限

あらゆるコンテキストの Admin は、これらの定義済みロールの他に新しいロールを定義できます。詳細については、第 2 章「仮想化の設定」を参照してください。

リソース クラス

リソース クラスで、同時接続または帯域幅レートなどの ACE リソースへのコンテキスト アクセスを管理できます。ACE には、Admin コンテキストおよび、作成したあらゆるユーザ コンテキストに適用されるデフォルト リソース クラスが設定されています。デフォルト 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%）までのいずれかの範囲内でコンテキストが動作できるよう設定されています。

デフォルト リソース クラスを複数のコンテキストで使用すると、ACE により先着順で、すべてのコンテキストにすべてのリソースへのフル アクセスが許可されるため、ACE リソースをオーバーサブスクライブするおそれがあります。リソースがその最大限まで使用されると、そのリソースのあらゆるコンテキストからの追加要求は、ACE により拒否されます。

リソースのオーバーサブスクライブを避け、あらゆるコンテキストが確実にリソースにアクセスできるようにするために、ACE では、カスタマイズされたリソース クラスを作成して、1 つ以上のコンテキストに関連付けることができます。関連付けたコンテキストは、リソース クラスの*メンバ*となります。リソース クラスを作成すると、メンバ コンテキストが使用できる各 ACE リソースの量の最小値と最大値を制限できます。最小値と最大値は、全体に対するパーセンテージで定義します。たとえば、リソース クラスを作成して、ACE がサポートする SSL 接続の総数の 25% 以上へのアクセスをメンバ コンテキストに許可することができます。

以下の ACE リソースの割り当ての制限および管理が可能です。

- ACL メモリ
- Syslog メッセージおよび TCP out-of-order（OOO）セグメント用のバッファ
- 同時接続（ACE 経由のトラフィック）
- 管理接続（ACE へのトラフィック）
- プロキシ接続
- リソースの制限をレート（秒単位の数）で設定
- 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）

デフォルトでは、コンテキストの作成時に、ACE によりコンテキストにデフォルト リソース クラスが関連付けられます。デフォルト リソース クラスにより、スティッキ エントリを除くすべてのリソースに対する 0 という最小値および無制限という最大値がリソースに設定されます。スティッキ性が正常に機能するためには、**limit-resource** コマンドを使用して、スティッキ エントリに明示的に最小リソース制限を設定する必要があります。

リソースの設定および制限の詳細については、第 2 章「仮想化の設定」を参照してください。スティッキ性の詳細については、『*Cisco Application Control Engine Module Server Load-Balancing Guide*』を参照してください。

CHAPTER 2

仮想化の設定

この章では、ACE の仮想化を作成し、設定する方法を説明します。グローバル管理者（SuperUser）は、各仮想デバイスまたはコンテキストの基本設定を含む Admin コンテキスト経由で、すべてのコンテキストを設定および管理します。設定する各コンテキストには、それぞれ一連のポリシー、インターフェイス、リソース、および管理者が含まれます。

この章の内容は、次のとおりです。

（注） デフォルトでは、ACE に Admin コンテキストが作成されており、さらに 5 つのユーザ コンテキストを設定できます。ユーザ コンテキストを 6 つ以上、最大 250 まで作成するには、シスコシステムズから別のライセンスを購入する必要があります。ライセンスの詳細については、『*Cisco Application Control Engine Module Administration Guide*』を参照してください。

仮想化設定のクイック スタート

表 2-1 は、仮想化機能の作成と設定に必要な手順の概要を示しています。各手順には、作業の完了に必要なコマンドライン インターフェイス（CLI）コマンドが含まれます。

表 2-1　仮想化設定のクイック スタート

作業とコマンドの例
1. コンソールで、グローバル管理者として ACE にログインします。デフォルトでは、コンソールが Admin と呼ばれる 1 つのコンテキストで起動します。

2. コンフィギュレーション モードを入力します。
`host1/Admin# config`
`Enter configuration commands, one per line. End with CNTL/Z.`
`host1/Admin(config)#`

3. リソース クラスを設定して、ユーザ コンテキストで使用するリソースを制限します。たとえば、コンテキストのリソースを、使用可能なリソース全体の 10% に制限するには、次のコマンドを入力します。
`host1/Admin(config)# resource-class RC1`
`host1/Admin(config-resource)# limit resource all minimum 10 maximum equal-to-min`
`host1/Admin(config-resource)# exit`

4. 新しいコンテキストを作成します。
`host1/Admin(config)# context C1`
`host1/Admin(config-context)#`

5. 作成したコンテキストがそのコンテキスト用に分類されたトラフィックを受け取るように、既存の VLAN をコンテキストに関連付けます。 `host1/Admin(config-context)# allocate-interface vlan 100`
6. ステップ 3 で作成したリソース クラスにコンテキストを関連付けます。 `host1/Admin(config-context)# member RC1`

7. コンテキストを、ステップ 4 で作成した C1 コンテキストに変更して、コンフィギュレーション モードにします。
`host1/Admin(config-context)# do changeto C1`
`host1/C1(config-context)# exit`
`host1/C1(config)#`

表 2-1　仮想化設定のクイック スタート（続き）

作業とコマンドの例

8. コンテキストのドメインを作成します（オプション）。
`host1/C1(config)# **domain D1**`
`host1/C1(config-domain)#`

9. オブジェクト（実サーバ、サーバ ファーム、プローブ、ACL など）を、必要に応じてドメインに割り当てます。 `host1/C1(config-domain)# **add-object rserver SERVER1**`
10. ロールを作成して、ユーザのさまざまなグループのオブジェクトおよびリソース権限を定義します（オプション）。 `host1/C1(config)# **role UR1**`

11. 規則を作成して、ロール権限を定義します。
`host1/C1(config-role)# **rule 1 permit create feature real**`
`host1/C1(config-role)# **rule 2 deny create feature acl**`

12. 必要に応じてユーザを設定し、ロールおよびドメインをユーザに関連付けます。 `host1/C1(config)# **username user1 password 5 MYPASSWORD role UR1 domain D1**`

13. 次のコマンドのいずれかを入力して、仮想化設定を検証します。
`host1/C1# **show running-config context**`
`host1/C1# **show running-config domain**`
`host1/C1# **show running-config resource-class**`
`host1/C1# **show running-config role**`

ACE リソースの管理

1 つまたは複数のリソース クラスを作成および定義し、コンテキストをリソース クラスに関連付けることで、システム リソースを複数のコンテキストに割り当てることができます。ここでは、次の内容について説明します。

- リソース管理のためのリソース クラスの作成
- リソース クラス内でのリソースの割り当て
- リソース クラスのリソース割り当ての変更

リソース管理のためのリソース クラスの作成

リソース クラスを作成して、1 つ以上のコンテキストでシステム リソースを割り当てたり、管理したりできます。ACE は、100 までのリソース クラスをサポートしています。リソース クラスを作成し、設定したあとに、コンテキスト コンフィギュレーション モードで **member** コマンドを使用して、コンテキストにリソース クラスに割り当てます（「コンテキストのリソース クラスへの関連付け」を参照）。リソース クラスを作成するには、コンフィギュレーション モードで **resource-class** コマンドを使用します。コマンドの構文は次のとおりです。

resource-class *name*

name 引数には、引用符もスペースも含まない、64 文字以下の英数字のテキスト文字列を入力します。

以下は入力例です。

```
host1/Admin(config)# resource-class RC1
host1/Admin(config-resource)
```

設定からリソース クラスを削除するには、次のように入力します。

```
host1/Admin(config)# no resource-class RC1
```

ACE からリソース クラスを削除すると、そのリソース クラスのメンバであったコンテキストはすべて、自動的にデフォルト リソース クラスのメンバとなります。デフォルト リソース クラスでは、すべての ACE リソースの最小 0.00% から最大 100.00% までが各コンテキストに割り当てられます。デフォルト リソース クラスは変更できません。

リソース クラス内でのリソースの割り当て

設定での仮想コンテキストの初期リソース割り当てを計画するときは、必要なリソースまたは推定リソースの最小値を割り当ててください。ACE では、使用中のリソースが保護されるため、コンテキストのリソースを削減するには、リソースが未使用である必要があります。リアルタイムでリソース割り当てを削減することも可能ですが、削減する前に使用中のリソースを解放するために、さらに管理オーバーヘッドが必要になる場合があります。したがって、最初にできるだけ多くのリソースを確保しておき、必要に応じて、未使用のリソースを割り当てるのがベスト プラクティスと考えられます。

スケーラビリティと容量管理の問題に対処するために、新しく取り付ける ACE が、モジュールの容量全体の 60 ～ 80% を超えないことを推奨します。全体の 60 ～ 80% を超えないようにするには、確保しておくリソース クラスを、ACE リソース全体の 20 ～ 40% となるように作成し、専用の仮想コンテキストを設定して、これらのリソースが確実に予約されるようにします。その後、時間が経つにつれ、増加するクライアント トラフィックの処理に必要となる容量に合わせて、確保されたリソースを効率的にコンテキストに配分できます。

すべてのリソースまたは各リソースを、リソース クラスのすべてのメンバ コンテキストに割り当てることができます。たとえば、数例として、同時接続、スティッキ テーブル メモリ、管理トラフィックなどにのみ割り当てることができます。リソース クラスのすべてのメンバ（コンテキスト）にシステム リソースを割り当てるには、resource-class コンフィギュレーション モードで **limit-resource** コマンドを使用します。

このコマンドの構文は次のとおりです。

limit-resource {**acl-memory** | **all** | **buffer** {**syslog**} | **conc-connections** | **mgmt-connections** | **proxy-connections** | **rate** {**bandwidth** | **connections** | **inspect-conn** | **mac-miss** | **mgmt-traffic** | **ssl-bandwidth** | **syslog**} | **regexp** | **sticky** | **xlates**} {**minimum** *number*} {**maximum** {**equal-to-min** | **unlimited**}}

引数とキーワードは次のとおりです。

- **acl-memory** ― ACL に割り当てられるメモリ スペースを制限します。
- **all** ― 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のすべてのリソースを指定した値に制限します（管理トラフィックの帯域幅を除く）。管理トラフィックの帯域幅は、管理トラフィックの最小値を明示的に設定しないかぎり、デフォルト値のまま維持されます。

- **buffer** ― Syslog バッファの数を制限します。
- **conc-connections** ― 同時接続の数を制限します。
- **mgmt-connections** ― 管理（ACE への）接続の数を制限します。
- **proxy-connections** ― プロキシ接続の数を制限します。
- **rate** ― 以下の 1 秒あたりの数としてリソースを制限します。
  - **bandwidth** ― 1 つまたは複数のコンテキストについて、ACE の合計スループットを 1 秒あたりのバイト数で制限します。コンテキストあたりの帯域幅の最大レートは、帯域幅のライセンスによって異なります。エントリレベルの ACE ではデフォルトで、5 Gbps の合計最大帯域幅に対して、伝送トラフィック用の帯域幅が 4 Gbps、管理トラフィック用の帯域幅が 1 Gbps に設定されています。オプションの 8 Gbps または 16 Gbps 帯域幅ライセンスを購入すると、ACE をアップグレードできます。8 Gbps ライセンスでは、ACE の合計最大帯域幅が 9 Gbps に、伝送トラフィック用の帯域幅が 8 Gbps に、管理トラフィック用の帯域幅が 1 Gbps になります。

    ACE でリソース クラスの最小帯域幅の値を設定した場合、ACE ではコンテキストが関連付けられているリソース クラスとは関係なく、その設定値を ACE 内の全コンテキストの合計最大帯域幅から差し引きます。コンテキストの合計帯域幅レートは、次の 2 つの要素で構成されています。

    スループット ― ACE 経由で伝送されるトラフィックを制限します。これは算出された値（ユーザによる直接設定は不可）であり、4 Gbps および 8 Gbps ライセンスを使用する場合、**帯域幅**レートから **mgmt-traffic** レートを引いた値と等しくなります。16 Gbps ライセンスでは、この値の計算方法が若干異なります。詳細については、次に示す **show resource-usage** コマンドの出力例を参照してください。

    mgmt-traffic ― 管理（ACE への）トラフィックを、1 秒あたりのバイト数で制限します。このパラメータは、**limit-resource all minimum** コマンドとは独立して機能します。管理トラフィックの最小帯域幅を確保するには、**limit-resource rate mgmt-traffic minimum** コマンドを使用して、明示的に管理トラフィックに最小比率を割り当てる必要があります。管理トラフィックに最小比率の帯域幅を割り当てると、その値が ACE によって、ACE 内の全コンテキストで利用可能な管理トラフィックの最大帯域幅から差し引かれます。デフォルトでは、ACE にインストールされた帯域幅ライセンスの種類に関係なく、管理トラフィックで保証される最小帯域幅レートは 0 に、最大帯域幅レートは 1 Gbps に設定されています。

スループットおよび管理トラフィックに関して ACE で帯域幅を管理する方法については、次に示す **show resource-usage** コマンドの出力例を参照してください。各帯域幅ライセンスについて、3 種類の例を示します。デフォルト値を使用した場合、全リソースの最小割り当て値が 25% の場合、および全リソースの最小割り当て値が 25% で、かつ管理トラフィックの最小割り当て値が 10% の場合です。出力例は、関連フィールドのみを示すために編集されています。すべての値の単位はバイト / 秒です。ビット / 秒に変換するには、各値に 8 を掛けてください。

```
switch/Admin# show resource usage
```

例 2-1　デフォルトの show resource usage コマンドの出力（4 Gbps ライセンスの場合）

	Allocation	
Resource	Min	Max
bandwidth	0	625000000
throughput	0	500000000
mgmt-traffic rate	0	125000000

例 2-2　show resource usage コマンドの出力（4 Gbps ライセンスで、全リソースの最小割り当て値が 25% の場合）（続き）

	Allocation	
Resource	Min	Max
bandwidth	125000000	500000000
throughput	125000000	375000000
mgmt-traffic rate	0	125000000

例 2-3　show resource usage コマンドの出力（4 Gbps ライセンスで、全リソースの最小割り当て値が 25%、管理トラフィックの最小割り当て値が 10% の場合）

```
                                    Allocation
Resource                Min                     Max
bandwidth               137500000               487500000
 throughput             125000000               375000000
 mgmt-traffic rate       12500000               112500000
```

例 2-4　デフォルトの show resource usage コマンドの出力（8 Gbps ライセンスの場合）

```
                                    Allocation
Resource                Min                     Max
bandwidth               0                       1125000000
 throughput             0                       1000000000
 mgmt-traffic rate      0                        125000000
```

例 2-5　show resource usage コマンドの出力（8 Gbps ライセンスで、全リソースの最小割り当て値が 25% の場合）

```
                                    Allocation
Resource                Min                     Max
bandwidth               250000000               875000000
 throughput             250000000               750000000
 mgmt-traffic rate      0                       125000000
```

例 2-6　show resource usage コマンドの出力（8 Gbps ライセンスで、全リソースの最小割り当て値が 25%、管理トラフィックの最小割り当て値が 10% の場合）

```
                                  Allocation
Resource                  Min                     Max
bandwidth                 262500000               862500000
 throughput               250000000               750000000
 mgmt-traffic rate         12500000               112500000
```

例 2-7　デフォルトの show resource usage コマンドの出力（16 Gbps ライセンスの場合）

```
                                  Allocation
Resource                  Min                     Max
bandwidth                 0                       2000000000
 throughput               0                       2000000000
 mgmt-traffic rate        0                        125000000
```

例 2-8　show resource usage コマンドの出力（16 Gbps ライセンスで、全リソースの最小割り当て値が 25% の場合）

```
                                  Allocation
Resource                  Min                     Max
bandwidth                 500000000               1500000000
 throughput               500000000               1500000000
 mgmt-traffic rate        0                        125000000
```

例 2-9　show resource usage コマンドの出力（16 Gbps ライセンスで、全リソースの最小割り当て値が 25%、管理トラフィックの最小割り当て値が 10% の場合）

```
                                   Allocation
Resource                 Min                   Max
bandwidth                500000000             1500000000
 throughput              487500000             1500000000
 mgmt-traffic rate        12500000              112500000
```

  - **connections** ― 1 秒あたりのあらゆる接続の数を制限します。
  - **inspect conn** ― File Transfer Protocol（FTP; ファイル転送プロトコル）および Real-Time Streaming Protocol（RTSP; リアルタイム ストリーミング プロトコル）のみの 1 秒あたり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数を制限します。
  - **mac-miss** ― カプセル化の 1 秒あたりのバイト数が正しくない場合にコントロール プレーンに送られる ACE トラフィックを制限します。
  - **ssl-bandwidth** ― 1 秒あたりの SSL 接続数を制限します。
  - **syslog** ― 1 秒あたりの Syslog メッセージ数を制限します。
- **regexp** ― 正規表現メモリの量を制限します。
- **sticky** ― スティッキ テーブルのエントリ数を制限します。スティッキ ソフトウェアは、設定が**制限されていない**場合はリソースを受け取らないため、スティッキ データベースのエントリにリソースを割り当てるには、スティッキの最小値を設定する必要があります。スティッキにリソースを割り当てるには、スティッキのみにリソースの最小比率を設定する（**limit-resource sticky**）か、または全体的なリソースの最小比率を設定（**limit-resource all**）します。
- **xlates** ― ネットワーク エントリおよびポート アドレス変換エントリの数を制限します。
- **minimum** *number* ― リソースの最小許容値を指定します。0.00 ～ 100.00%（小数点 2 位まで）の整数を入力します。*number* 引数で、リソース クラスのメンバであるすべてのコンテキストのパーセンテージ値が指定されます。**rate** キーワードと併用すると、*number* 引数で 1 秒あたりの値が指定されます。ACE で特定のリソース クラスのリソースに最小値を設定すると、ACE では対象のリソース クラスのメンバであるコンテキストにのみ、所定の最小リソースを割り当てます。全コンテキストに関しては、コンテキストが関

連付けられているリソース クラスには関係なく、ACE によって設定した最小値がリソースの最大値から差し引かれます。リソース クラスに 1 つ以上のコンテキストが関連付けられている場合は、ACE によって、最小値にリソース クラスが含むコンテキストの数を掛けた値が最大値から差し引かれます。たとえば、4 Gbps 帯域幅ライセンスで、リソース クラスに 2 つのコンテキストが関連付けられており、そのクラスの最小帯域幅レートとして 25% を割り当てたとします。**show resource usage** コマンドを実行すると、リソース クラス内の各コンテキストの帯域幅レートおよびスループット レートは、表 2-2 に示す値となります。

表 2-2　show resource usage コマンドの出力（4 Gbps ライセンスで、帯域幅の最小割り当て値が 25% の場合）

	Allocation	
Resource	Min	Max
bandwidth	125000000	375000000
throughput	125000000	250000000
mgmt-traffic rate	0	125000000

ACE のその他の全コンテキストについて、最大値はすべて表 2-2 と同一になりますが、最小値はすべて 0 になります。表 2-2 と、リソース クラスにコンテキストが 1 つだけ含まれる場合の例を示した表 2-1 を比較してみてください。

- **maximum** {**equal-to-min** | **unlimited**} ― リソースの最大値を指定します。最小値と同じか、または無制限に設定できます。

（注） **limit-resource** コマンドを使用して個々のリソースに設定した制限は、**limit-resource all** コマンドを使用してすべてのリソースに設定した制限に優先して使用されます。

1 つのコンテキスト（コンテキスト A とします）の制限を、別のコンテキスト（コンテキスト B とします）の制限を増やす目的で削減すると、設定の変更に時間がかかる場合があります。これは、ACE では、コンテキスト A でのリソースの使用が終了するまで、その制限が削減されないためです。

たとえば、すべてのリソース（最小および最大）の 20% を、リソース クラスのすべてのメンバ コンテキストに割り当てるには、次のように入力します。

```
(config-resource)# limit-resource all minimum 20% maximum equal-to-min
```

すべてのメンバ コンテキストのすべてのリソースで、リソース割り当てを最小値 0% および最大値 100% のデフォルト値に戻すには、次のように入力します。

```
(config-resource)# no limit-resource all
```

表 2-3 は、ACE の管理されたシステム リソースの一覧です。**limit-resource** コマンドを使用して、コンテキストごとに、またはリソース クラスに関連付けられたすべてのコンテキストについて、これらのリソースを制限できます。「リソース クラス内でのリソースの割り当て」を参照してください。

表 2-3　システム リソースの最大値

Resource	最大値
ACL メモリ	78,610,432 バイト
バッファ メモリ（Syslog）	4,000,000 バイト
同時接続（レイヤ 4）	4,000,000 接続
同時接続（SSL）	200,000
管理接続	5000 接続
プロキシ接続（レイヤ 7）	524,286 接続
SSL プロキシ接続	100,000
レート	
帯域幅	4 ギガビット / 秒（Gbps） ACE 最大帯域幅は、シスコシステムズから別売のライセンスを購入して、8 Gbps または 16 Gbps にアップグレードできます。詳細については、『*Cisco Application Control Engine Module Administration Guide*』を参照してください。
接続（全種類）	325,000 接続 / 秒
MAC ミス	2000 パケット / 秒

表 2-3　システム リソースの最大値（続き）

Resource	最大値
管理トラフィック	1 Gbps
SSL トランザクション	1000 TPS（トランザクション / 秒）（個別ライセンスで 15000 TPS にアップグレード可能）詳細については、『*Cisco Application Control Engine Module Administration Guide*』を参照してください。
Syslog	ACE へのトラフィック（コントロール プレーン）の場合は 5000 メッセージ / 秒 ACE 経由のトラフィック（データ プレーン）の場合は 350,000 メッセージ / 秒
正規表現メモリ	1,048,576 バイト
スティッキ エントリ	4,194,304 エントリ
Xlates（ネットワーク エントリおよびポート アドレス変換エントリ）	524,286 個

リソース クラスのリソース割り当ての変更

2 つ以上のコンテキストをメンバとするリソース クラスで、リソース割り当てを変更する場合は（グローバル管理者権限が必要）、適切な CLI コマンドを入力することで、いつでも実行できます（リソース割り当ての詳細については、「リソース クラス内でのリソースの割り当て」を参照してください）。ただし、コンテキスト間でのリソースの移動は、適切なリソースで変更を反映する必要があるため、すぐには実行できません。多くのケースでは、リソース割り当ての変更を行うには、関連するコンテキストの管理者に連絡してリソースの割り当て変更が可能であることを確認する必要があります。

たとえば、クラスで利用可能なリソースのすべてがコンテキスト A で使用されている状況で、リソースの 50% をコンテキスト A に、残りの 50% をコンテキスト B に割り当てるよう変更するとします。CLI でリソースを割り当てるためのコマンドを実行しても、コンテキスト A のリソースのうち 50% の割り当てが解除されないかぎり、コンテキスト B に 50% のリソースは割り当てられません。

次に、この場合の対処法を示します。

- コンテキスト A の管理者に連絡し、リソースの割り当て解除を依頼
- コンテキスト B の管理者に連絡し、コンテキスト A のリソース解放後にリソースの割り当て作業を行うよう依頼

（注） 他のコンテキストからリソースが解放されると、ACE はリソースの不足したコンテキスト（リソース クラスの最小割り当て条件が満たされていないコンテキスト）にそのリソースを割り当てます。

コンテキストの設定

コンテキストにより ACE のユーザ ビューが提供され、ユーザが使用できるリソースが決定されます。ここでは、次の内容について説明します。

コンテキストの作成

コンテキストを作成するには、コンフィギュレーション モードで **context** コマンドを使用します。このコマンドの構文は次のとおりです。

context *name*

name 引数は、コンテキストの一意の ID です。引用符もスペースも含まない、64 文字以下の英数字のテキスト文字列を入力してください。

たとえば、C1 というコンテキストを作成するには、次のように入力します。

```
host1/Admin(config)# context C1
host1/Admin(config-context)#
```

設定からコンテキストを削除するには、次のように入力します。

```
host1/Admin(config)# no context C1
```

コンテキストの説明の設定

context コンフィギュレーション モードで **description** コマンドを使用して、コンテキストの説明を入力できます。このコマンドの構文は次のとおりです。

description *text*

text 引数には、引用符を含まない 240 字までの英数字のテキスト文字列で説明を入力します。

以下は入力例です。

```
host1/Admin(config-context)# description context for accounting users
```

設定からコンテキスト説明を削除するには、次のように入力します。

```
host1/Admin(config-context)# no description
```

コンテキストの VLAN の設定

ACE は、クラス マップおよびポリシー マップを使用して、トラフィックを分類（フィルタリング）し、サービス ポリシーを使用してさまざまなインターフェイス（VLAN）へと誘導します。コンテキストは、VLAN を使用して、その VLAN に分類されたパケットを受信します。ユーザ コンテキストがパケットを受信するための 1 つ以上の既存の VLAN を割り当てるには、Admin コンテキストの context コンフィギュレーション モードで **allocate-interface** コマンドを使用します。このコマンドを複数回入力して、ユーザ コンテキストに複数の VLAN を指定できます。

（注） インターフェイス設定はユーザ　コンテキストから直接行うことができますが、Admin コンテキストで対象のインターフェイスに対して **allocate-interface** コマンドを実行するまでは、インターフェイスはダウン ステートのままになります。インターフェイスの設定および割り当ては、任意の順番で実行できます。

このコマンドの構文は次のとおりです。

allocate-interface vlan *number1*

number 引数には、コンテキストに割り当てる既存の VLAN の数または VLAN の範囲を 2 ～ 4094 の整数で入力します。

（注） Admin コンテキストでインターフェイスを削除した場合に、そのインターフェイスがユーザ コンテキストで使用されていると、対象のインターフェイスはダウン ステートになります。ユーザ コンテキストで **show interface** コマンドを実行すると、該当するインターフェイスがダウン ステートであることと、そのインターフェイスが現在、Admin コンテキストで割り当てられていないのが原因であることが表示されます。

たとえば、コンテキストに VLAN 100 を割り当てるには、次のように入力します。

```
host1/Admin(config-context)# allocate-interface vlan 100
```

VLAN 100 ～ VLAN 200 の範囲の VLAN をコンテキストに割り当てるには、次のように入力します。

```
host1/Admin(config-context)# allocate-interface vlan 100-200
```

コンテキストから VLAN の割り当てを解除するには、次のように入力します。

```
host1/Admin(config-context)# no allocate-interface vlan 100
```

コンテキストから VLAN の範囲の割り当てを解除するには、次のように入力します。

```
host1/Admin(config-context)# no allocate-interface vlan 100-200
```

（注） ユーザ コンテキストで VLAN が使用中の場合は、その割り当てをコンテキストから解除できません。

コンテキストのリソース クラスへの関連付け

リソース クラスは、1 つ以上のコンテキストで使用できるリソースを制限します。リソース クラスを指定しない場合は、コンテキストが自動的にデフォルト リソース クラスのメンバとなります。デフォルト リソース クラスでは、すべての ACE リソースの最小 0.00% から最大 100.00% までが各コンテキストに割り当てられます。コンテキストは、1 つのリソース クラスにのみ関連付けられます。リソース クラスの詳細については、「リソース管理のためのリソース クラスの作成」を参照してください。コンテキストをリソース クラスに関連付けるには、context コンフィギュレーション モードで **member** コマンドを使用します。

このコマンドの構文は次のとおりです。

member *class*

class 引数には、引用符もスペースも含まない、64 文字以下の英数字のテキスト文字列で既存のリソース クラスの名前を入力します。リソース クラスの設定の詳細については、「リソース管理のためのリソース クラスの作成」を参照してください。

たとえば、コンテキストを RC1 リソース クラスに関連付けるには、次のように入力します。

```
host1/Admin(config-context)# member RC1
```

RC1 リソース クラスからコンテキストの関連付けを削除するには、次のように入力します。

```
host1/Admin(config-context)# no member RC1
```

コンテキストのリソース クラスの変更

リソース クラスからコンテキストを削除するには、context コンフィギュレーション モードで **no member** コマンドを使用します（「コンテキストのリソース クラスへの関連付け」を参照）。リソース クラスからコンテキストを削除すると、ACE はそのコンテキストに関連付けられていた全リソースを解放するため、そのクラス内の他のコンテキストで、解放されたリソースを利用できるようになります。

同一のコンテキストを異なるリソース クラスに関連付けるには、context コンフィギュレーション モードで **member** コマンドを使用します（「コンテキストのリソース クラスへの関連付け」を参照）。リソース クラスにコンテキストを追加すると、ACE では、設定範囲内で残っているリソースだけを割り当てます。リソースに余裕がある場合は、対象のコンテキストに対して、さらにリソースを割り当てることができます。リソースに余裕がない場合は、あらかじめリソース クラス内の他のコンテキストに割り当てられたリソースを解放する必要があります。コンテキスト間でのリソース割り当ての修正については、「リソース クラスのリソース割り当ての変更」を参照してください）。

コンテキスト間の移動

EXEC モードで **changeto** コマンドを、またはコンフィギュレーション モードで **do changeto** コマンドを使用して、コンテキスト間を移動できます。**changeto** コマンドを使用するには、Admin コンテキストに定義済みのユーザ ロールのいずれかが存在している必要があります。定義済みユーザ ロールの詳細については、第 1 章「概要」の「ロールベース アクセス コントロール」を参照してください。複数のコンテキストにアクセスできるコンテキスト管理者は、アクセス可能な他のコンテキストに明示的にログインする必要があります。このコマンドの構文は次のとおりです。

changeto *name*

name 引数は、既存のコンテキストの ID を指定します。引用符もスペースも含まない、64 文字以下の英数字のテキスト文字列を入力してください。

以下は入力例です。

```
host1/Admin# changeto C1
host1/C1#
```

ユーザ ロールの作成と設定

ユーザ ロールで、ユーザが持つ権限、ユーザが入力できるコマンド、および特定のコンテキストでユーザが実行できる動作が決定されます。ACE で提供される定義済みロールのリストについては、第 1 章「概要」を参照してください。CLI で定義済みロールを表示するには、EXEC モードで **show role** コマンドを入力します。グローバル管理者またはコンテキスト管理者は、追加のロールを設定できます。作成したロールは、それを作成したコンテキスト中でのみ適用できます。

ロールを設定するには、コンフィギュレーション モードで **role** コマンドを使用します。このコマンドの構文は次のとおりです。

role *name*

name 引数は、ロールに関連付けられた ID です。引用符もスペースも含まない、64 文字以下の英数字のテキスト文字列を入力してください。

新規ユーザにロールを割り当てない場合、割り当てられるデフォルト ロールは Network-Monitor です。Admin コンテキストで作成したユーザの場合、デフォルトのアクセス範囲はデバイス全体です。その他のコンテキストで作成したユーザの場合、デフォルトのアクセス範囲はコンテキスト全体です。ユーザのアクセスを制限する必要がある場合は、**username** コマンドを使用して、ロールとドメインのペアを割り当てる必要があります（「ユーザの設定」を参照）。

以下は入力例です。

```
host1/C1(config)# role TECHNICIAN
host1/C1(config-role)#
```

設定からロールを削除するには、次のように入力します。

```
host1/C1(config)# no role TECHNICIAN
```

ユーザ ロールを作成したあとに、そのロールに規則を設定して、ユーザがアクセスできる機能、およびユーザがその機能を使用するために入力できるコマンドを制限できます。機能ごとの権限をロールに割り当てるには、role コンフィギュレーション モードで **rule** コマンドを使用します。

このコマンドの構文は次のとおりです。

rule *number* {**permit** | **deny**} {**create** | **modify** | **debug** | **monitor**} [**feature** {**AAA** | **access-list** | **config-copy** | **connection** | **dhcp** | **fault-tolerant** | **inspect** | **interface** | **loadbalance** | **nat** | **pki** | **probe** | **real-inservice** | **routing** | **rserver** | **serverfarm** | **ssl** | **sticky** | **syslog** | **vip**}]

キーワード、引数、およびオプションは次のとおりです。

- *number* ― ルールおよび優先順位の ID。1 ～ 16 の一意の整数を入力します。ルール番号により、ACE がルールを適用する順序が決定され、大きい番号のルールが小さい番号のルールのあとに適用されます。
- **permit** ― ロールによる、残りのコマンド キーワードで定義される操作の実行を許可します。
- **deny** ― ロールによる、残りのコマンド キーワードで定義される操作の実行を禁止します。
- **create** ― 新規オブジェクトの作成または既存オブジェクトの削除に使用するコマンドを指定します（**modify**、**debug**、および **monitor** コマンドなど）。
- **modify** ― 既存の設定の変更に使用するコマンドを指定します（**debug** および **monitor** コマンドなど）。
- **debug** ― デバッグの問題に使用するコマンドを指定します（**monitor** コマンドなど）。
- **monitor** ― リソースおよびオブジェクトの監視に使用するコマンドを指定します（**show** コマンド）。
- **feature** ― この規則の設定に使用する、以下の ACE 機能を指定します（オプション）。
  - **AAA** ― 認証、認可、アカウンティングに使用するコマンドを指定します。
  - **access-list** ― アクセス コントロール リスト（ACL）に使用するコマンドを指定します。ACL 設定、ACL のクラス マップ、および ACL のクラス マップを含むポリシー マップが含まれます。
  - **config-copy** ― 実行コンフィギュレーション ファイルのスタートアップ コンフィギュレーション ファイルへのコピー、スタートアップ コンフィギュレーション ファイルの実行コンフィギュレーション ファイルへのコピー、および両コンフィギュレーション ファイルのフラッシュ ディスク（disk0:）またはリモート サーバへのコピーに使用するコマンドを指定します。
  - **connection** ― ネットワーク接続に使用するコマンドを指定します。

- **dhcp** ― Dynamic Host Configuration Protocol に使用するコマンドを使用します。
- **fault-tolerant** ― 冗長性に使用するコマンドを指定します。
- **inspect** ― データセンターのセキュリティで使用されるパケット インスペクションに使用するコマンドを指定します。
- **interface** ― すべてのインターフェイス コマンドを指定します。
- **loadbalance** ― ロード バランシングに使用するコマンドを指定します。ポリシー マップでロードバランシング動作を追加できます。
- **nat** ― データセンターのセキュリティで使用されるポリシー マップで、クラス マップに関連付けられたネットワーク アドレス変換（NAT）に使用するコマンドを指定します。
- **pki** ― SSL Public Key Infrastructure（PKI; 公開鍵インフラストラクチャ）に使用するコマンドを指定します。
- **probe** ― 実サーバのキープアライブに使用するコマンドを指定します。
- **real-inservice** ― 実サーバを稼働状態にするためのコマンドを指定します。
- **routing** ― グローバル、およびインターフェイスごとのルーティングに使用するすべてのコマンドを指定します。
- **rserver** ― 物理サーバに使用するコマンドを指定します。
- **serverfarm** ― サーバ ファームに使用するコマンドを指定します。
- **ssl** ― SSL に使用するコマンドを指定します。
- **sticky** ― サーバの永続性に使用するコマンドを指定します。
- **syslog** ― システム ロギング機能のセットアップ コマンドを指定します。
- **vip** ― 仮想 IP アドレスおよび仮想サーバに使用するコマンドを指定します。

たとえば、ロールに実サーバの作成および設定を許可する規則を設定するには、次のように入力します。

```
host1/C1(config-role)# rule 1 permit create rserver
```

ロールから規則を削除するには、次のように入力します。

```
host1/C1(config-role)# no rule 1 permit create rserver
```

ドメインの作成および設定

ドメインとは、ユーザが動作する名前空間です。コンテキストを作成すると、ACE により、そのコンテキストのデフォルト ドメイン（default-domain）が自動的に作成されます。各コンテキストで 63 個までのドメインを新たに作成できます。コンテキストの設定の詳細については、「コンテキストの設定」を参照してください。ドメインを作成するには、コンフィギュレーション モードで **domain** コマンドを使用します。このコマンドの構文は次のとおりです。

domain *name*

name 引数には、引用符もスペースも含まない、64 文字以下の英数字のテキスト文字列を入力します。

たとえば、D1 というドメインを作成するには、次のように入力します。

```
host1/C1(config)# domain D1
host1/C1(config-domain)#
```

設定からドメインを削除するには、次のように入力します。

```
host1/C1(config)# no domain D1
```

（注） **show running-config** コマンドで表示できるコンテキスト設定が、ドメインにより制限されることはありません。コンテキスト全体の実行コンフィギュレーションは表示可能です。ただし、コンテキストで使用可能なすべてのオブジェクトの限定されたサブセットのみをドメインに追加すると、ドメインによる、コンテキスト内の設定可能なオブジェクトへのアクセスの制限が可能となります。ユーザにロールを割り当てることで、それらの設定可能なオブジェクトに対してユーザが実行できる動作をさらに制限できます。ユーザ ロールの設定の詳細については、「ユーザ ロールの作成と設定」を参照してください。

ドメインを作成したあと、設定可能なオブジェクト（実サーバ、サーバ ファーム、インターフェイスなど）をそのドメインに関連付けることができます。設定可能なオブジェクトをドメインに関連付けるには、domain コンフィギュレーション モードで **add-object** コマンドを使用します。

このコマンドの構文は次のとおりです。

add-object {**access-list** {**ethertype** | **extended**} | **all** | **class-map** | **interface** {**bvi** | **vlan**} | **parameter-map** | **policy-map** | **probe** | **rserver** | **script** | **serverfarm** | **sticky**} *name*

キーワード、引数、およびオプションは次のとおりです。

- **access-list** ― ドメインに関連付ける既存のアクセス コントロール リスト（ACL）を指定します。
- **all** ― コンテキスト内のすべての既存の設定オブジェクトがドメインに追加されることを指定します。
- **class-map** ― ドメインに関連付ける既存のフロー分類用クラス マップを指定します。
- **interface** ― ドメインに関連付ける既存のインターフェイスを指定します。
- **parameter-map** ― ドメインに関連付ける既存のパラメータ マップを指定します。
- **policy-map** ― ドメインに関連付ける既存のポリシー マップを指定します。
- **probe** ― ドメインに関連付ける既存の実サーバ プローブ（キープアライブ）を指定します。
- **rserver** ― ドメインに関連付ける既存の実サーバを指定します。
- **script** ― ACE TCL スクリプト言語で作成した既存のスクリプトを指定します。
- **serverfarm** ― ドメインに関連付ける既存のサーバ ファームを指定します。
- **sticky** ― サーバでの永続性を維持するためにドメインに関連付ける、既存のスティッキ グループを指定します。
- *name* ― 指定したオブジェクトの ID。引用符もスペースも含まない、64 文字以下の英数字のテキスト文字列を入力してください。

たとえば、VLAN 10 というインターフェイスをドメインに関連付けるには、次のように入力します。

```
host1/C1(config-domain)# add-object interface vlan 10
```

ドメインからオブジェクトを削除するには、次のように入力します。

```
host1/C1(config-domain)# no add-object interface vlan 10
```

ユーザの設定

ACE を起動すると、2 種類のデフォルト ユーザ アカウントが作成されます。admin ユーザおよび www ユーザです。admin ユーザはグローバル管理者であり、削除できません。ACE では、XML インターフェイスに www ユーザ アカウントを使用します。

注意　www ユーザ アカウントは*削除しないでください*。削除すると、XML インターフェイスが動作しなくなります。誤って www アカウントを削除した場合は、コンフィギュレーション モードで **username www password 5** *password* **domain default-domain role Admin** コマンドを入力すると、アカウントを再設定し、XML 動作を元に戻すことができます。XML インターフェイスの使用の詳細については、*Cisco Application Control Engine Module Administration Guide* を参照してください。

グローバル管理者（admin）は、各コンテキストで 1 名のユーザをコンテキスト管理者として割り当てます。そのあとでコンテキスト管理者は、担当する 1 つ以上のコンテストにログインし、追加のユーザを作成できます。

新規ユーザにロールを割り当てない場合、割り当てられるデフォルト ロールは Network-Monitor です。Admin コンテキストで作成したユーザの場合、デフォルトのアクセス範囲はデバイス全体です。その他のコンテキストで作成したユーザの場合、デフォルトのアクセス範囲はコンテキスト全体です。ユーザのアクセスを制限する必要がある場合は、ロールとドメインのペアを割り当てる必要があります。

ユーザを作成するには、コンフィギュレーション モードで **user** コマンドを使用します。このコマンドの構文は次のとおりです。

username *name1* [**password** [**0** | **5**] {*password*}] [**expire** *date*] [**role** *name2* {**domain** *name3 name4 . . . namen*}]

キーワード、引数、およびオプションは次のとおりです。

- *name1* ― 作成するユーザの ID。引用符もスペースも含まない、24 文字以下の英数字のテキスト文字列を入力してください。
- **password** ― パスワードがあとに続くことを示すキーワード（オプション）。

- **0** ― クリア テキストのパスワードを指定します（オプション）。
- **5** ― MD5 ハッシュ強化暗号化パスワードを指定します（オプション）。
- *password* ― 入力するオプション番号（0、5、または 7）に応じて、クリア テキスト、暗号化テキスト、または MD5 強化暗号化のパスワードを指定します（オプション）。オプション番号を入力しない場合は、デフォルトでクリア テキストのパスワードを指定します。**password** キーワードを入力した場合は、パスワードを入力する必要があります。パスワードは、引用符を含まない 32 文字までの英数字のテキスト文字列で入力します。
- **expire** *date* ― ユーザ アカウントの有効期限の日付を指定します（オプション）。有効期限の日付は *yyyy-mm-dd* という形式で入力します。
- **role** *name2* ― ユーザに割り当てる既存のロールを指定します（オプション）。
- **domain** *name3 name4 . . . namen* ― ユーザが動作できるドメインを指定します。**default-domain** を含め、10 までの複数のドメイン名を入力できます。

以下は入力例です。

```
host1/C1(config)# username USER1 password MYSECRET expire 2005-12-31
role TECHNICIAN domain D1 default-domain

host1/C1(config)# username USER2 password HERSECRET expire 2005-12-31
role Admin domain default-domain D2
```

設定からユーザを削除するには、次のように入力します。

```
host1/C1(config)# no username USER1
```

仮想化設定の例

次の実行コンフィギュレーションの例は、ユーザ定義のコンテキスト、リソースクラス、ドメイン、およびユーザを 1 つずつ含む基本的な仮想化設定を示します。

```
resource-class RC1
  limit-resource rate syslog minimum 10.00 maximum equal-to-min
  limit-resource acl-memory minimum 10.00 maximum unlimited

access-list ACL1 line 10 extended permit ip any any

rserver host RS1
  ip address 192.168.2.251
  inservice
rserver host RS2
  ip address 192.168.2.252
  inservice
serverfarm host SF1
  rserver RS1
    inservice
  rserver RS2
    inservice

domain D1
  add-object access-list extended ACL1
  add-object rserver RS1
  add-object rserver RS2
  add-object serverfarm SF1

role SLB-Admin

context C1
  allocate-interface vlan 100-200
  description accounting department
  member RC1

username JANE password 5 adropgijaeprgja9erjg2uWgtce1 role SLB-Admin
  domain D1
```

CHAPTER 3

仮想化設定および統計の表示

この章では、Cisco Application Control Engine（ACE）モジュールで設定されたコンテキストのさまざまな設定および統計情報の表示を行う **show** コマンドを説明します。

この章の内容は、次のとおりです。

コンテキスト設定の表示

EXEC モードで **show running-config context** を使用すると、コンテキスト設定を表示できます。このコマンドにより、設定したすべてのユーザ コンテキストおよびその説明、リソース クラス、および割り当てた VLAN が表示されます。このコマンドの構文は次のとおりです。

show running-config context

以下は入力例です。

```
host1/Admin# show running-config context
```

ドメイン設定の表示

EXEC モードで **show running-config domain** を使用すると、ドメイン設定を表示できます。このコマンドにより、設定したすべてのドメインおよびそのオブジェクト（アクセス コントロール リスト [ACL]、クラス マップ、インターフェイスなど）が表示されます。このコマンドの構文は次のとおりです。

show running-config domain

以下は入力例です。

```
host1/Admin# show running-config domain
```

リソース クラス設定の表示

EXEC モードで show **running-config resource-class** コマンドを使用すると、リソース設定を表示できます。このコマンドにより、設定したすべてのリソース クラスおよびそのリソース割り当て文が表示されます。このコマンドの構文は次のとおりです。

show running-config resource-class

以下は入力例です。

```
host1/Admin# show running-config resource-class
```

ロール設定の表示

EXEC モードで **show running-config role** を使用すると、ロール設定を表示できます。このコマンドにより、設定したすべてのロール、その説明および関連付けられた規則が表示されます。このコマンドの構文は次のとおりです。

show running-config role

以下は入力例です。

```
host1/Admin# show running-config role
```

コンテキスト情報の表示

EXEC モードで **show context** コマンドを使用すると、コンテキストの名前、説明、リソース クラス、およびインターフェイスを含むコンテキストのリストを表示できます。このコマンドの構文は次のとおりです。

show context *name*

name 引数には、引用符もスペースも含まない、64 文字以下の英数字のテキスト文字列で既存のコンテキストの一意の ID を入力します。

以下は入力例です。

```
host1/Admin# show context C1
```

表 3-1 は、**show context** コマンドの出力に含まれるフィールドの説明です。

表 3-1　show context コマンド出力のフィールドの説明

フィールド	説明
Name	設定したすべてのコンテキストの ID のリストを表示します。*name* 引数を指定すると、指定したコンテキストの名前のみが表示されます。
Description	以前に設定した、コンテキストの説明テキスト
Resource-class	コンテキストがメンバとして含まれるリソース クラス
VLANs	Admin コンテキストからユーザ コンテキストに割り当てられた VLAN

リソース割り当ての表示

EXEC モードで **show resource allocation** コマンドを使用すると、すべてのリソース クラスおよびクラス メンバについて、各リソースの割り当てを表示できます。このコマンドの構文は次のとおりです。

show resource allocation

このコマンドにより、リソース割り当てが表示されますが、実際に使用中のリソースは表示されません。実際のリソース使用状況の詳細については、「リソース使用状況の表示」を参照してください。

以下は入力例です。

```
host1/Admin# show resource allocation
```

表 3-2 は、**show resource allocation** コマンドの出力に含まれるフィールドの説明です。

表 3-2　show resource allocation コマンド出力のフィールドの説明

フィールド	説明
Parameter	制限できるリソースの名前 各リソース名の詳細については、第 2 章「仮想化の設定」を参照してください。
Min	指定したリソース クラスでパラメータに割り当てられたシステム リソースの合計の最小パーセンテージ。デフォルト リソース クラスの各リソースの最小値は 0.00% です。
Max	指定したリソース クラスでパラメータに割り当てられた総システム リソースの最大パーセンテージ。デフォルト リソース クラスでは、各リソース クラスの Max 値は、デフォルト リソース クラスを使用しているすべてのコンテキストの Max 値の合計と同じです。たとえば、2 つのユーザ コンテキストを設定して、それらをリソース クラスに関連付けていない場合は、ACE により自動的にデフォルト リソース クラスが割り当てられます。Admin コンテキストもデフォルト リソース クラスを使用している場合は、各リソースの Max 値が 300% となります。
Class	リソース クラスの名前

リソース使用状況の表示

EXEC モードで **show resource usage** コマンドを使用すると、Admin コンテキストから作成された各コンテキストのリソース使用状況を表示できます。このコマンドの構文は次のとおりです。

show resource usage [**all** | [[**context** *name* | **summary** | **top** *number*] [**resource** {**acl-memory** | **all** | **conc-connections** | **mgmt-connections** | **probes** | **proxy-connections** | **rate** {**bandwidth** | **connections** | **inspect-conn** | **mac-miss** | **mgmt-traffic** | **ssl-connections** | **syslog**} | **regexp** | **sticky** | **syslogbuffer** | **xlates**}]]] [**counter** [**all** | **current** | **denied** | **peak** [*count_threshold*]]]

キーワード、引数、およびオプションは次のとおりです。

- **all** ― （オプション）各コンテキストのリソース使用状況を個別に表示します。これがデフォルトの設定です。
- **context** *name* ―（オプション）指定したコンテキストのリソース使用状況を表示します。*name* 引数では、大文字と小文字が区別されます。
- **summary** ― （オプション）すべてのコンテキストのリソース使用状況の合計を表示します。たとえば、denied 列には、各コンテキストの制限により拒否された項目が表示されます。
- **top** *number* ― （オプション）1 つのリソースをもっとも多く使用している *n* ユーザを、使用しているリソースの比率の高いものから低いものへと順に並べて表示します。1 つのリソース タイプを指定する必要があります。このオプションは、**resource all** キーワードとは併用できません。
- **resource** ―（オプション）指定した以下のリソースのいずれかに関する統計情報を表示します。
  - **acl-memory** ― ACL メモリ使用状況を表示します。

    （注） コンテキストで使用している ACL メモリ リソースが設定済みの最小割り当て値よりも少ない場合は、ACE によって、そのコンテキストに割り当て可能な実際の最小値が表示されます。

  - **all** ― 指定した 1 つ以上のコンテキストで使用されているすべてのリソースについて、リソース使用状況を表示します。
  - **conc-connections** ― 同時接続の数のリソース使用状況を表示します。

- **mgmt-connections** ― 管理接続の数のリソース使用状況を表示します。
- **probes** ― プローブのリソース使用状況を表示します。
- **proxy-connections** ― プローブ接続のリソース使用状況を表示します。
- **rate** ― 指定した接続または Syslog メッセージの 1 秒あたりのレートを表示します。
- **regexp** ― 正規表現のリソース使用状況を表示します。

（注） コンテキストで使用している正規表現のリソースが設定済みの最小割り当て値よりも少ない場合は、ACE によって、そのコンテキストに割り当て可能な実際の最小値が表示されます。

- **sticky** ― スティッキ エントリのリソース使用状況を表示します。

（注） コンテキストで使用している スティッキ リソースが設定済みの最小割り当て値よりも少ない場合は、ACE によって、そのコンテキストに割り当て可能な実際の最小値が表示されます。

- **syslogbuffer** ― Syslog バッファのリソース使用状況を表示します。Syslog バッファを開放するには、**clear logging** コマンドを使用します。

（注） ACE では、1024 を単位として Syslog バッファを割り当てます。リソース クラスの最小割り当て値が適用される場合、**show resource usage syslogbuffer** コマンドの Current フィールドには、最小割り当て値を下回るような、1024 の最も大きな倍数が表示されます。

- **xlates** ― ネットワーク アドレス変換（NAT）およびポート アドレス変換（PAT）エントリのリソース使用状況を表示します。

- **counter** ― （オプション）以下のキーワードの 1 つをカウンタ名として指定します。

  - **all** ― （オプション）すべての統計を表示します。これがデフォルトの設定です。
  - **current** ―（オプション）アクティブな同時インスタンス、またはリソースの現在のレートを表示します。
  - **denied** ― （オプション）リソースの統計が最後にクリアされたあとの、リソースの使用拒否の数を表示します。
  - **peak** ― （オプション）ピーク時の同時インスタンス、または統計が最後にクリアされたあとのリソースのピーク時のレートを、**clear resource usage** コマンドを使用して表示します。または、デバイスを再起動したときに表示します。

- *count_threshold* ― （オプション）リソースの下に表示される番号。0 ～ 4294967295 までの整数を入力します。デフォルト値は 1 です。リソースの使用状況が、設定した数字を下回っている場合は、リソースが設定されません。カウンタ名に ***all*** を指定すると、現在の使用状況にも *count_threshold* が適用されます。すべてのリソースを表示するには、*count_threshold* を ***0*** に設定します。

以下は入力例です。

```
host1/Admin# show resource usage context C1 resource conc-connections
counter denied 0
```

表 3-3 は、**show resource usage** コマンドの出力に含まれるフィールドの説明です。

表 3-3　show resource usage コマンド出力のフィールドの説明

フィールド	説明
Resource	各コンテキスト内の制限されたリソースの名前 各リソース名の詳細については、第 2 章「仮想化の設定」を参照してください。
Current	アクティブな同時インスタンスまたはリソースの現在のレート
Peak	リソース使用状況の最高値

表 3-3　show resource usage コマンド出力のフィールドの説明（続き）

フィールド	説明
Allocation (Min/Max)	各コンテキストで確実に使用可能なリソースの単位を示す、割り当ての最小値。各コンテキストで使用可能なリソースの単位を示す割り当ての最大値。オーバーサブスクライブ プールからのすべてのリソースが、この単位を共有します。最大値を **equal-to-minimum** に設定している場合は、最大値が自動的に 0 に設定されます。割り当て最大値が 0 の場合、各コンテキストで使用可能なリソース単位は割り当て最小値までとなります。
Denied	オーバーサブスクライブされたり、リソースが使い果たされたりしたために拒否されたリソースの数
Actual Min	リソースクラスの最小値を適用できない場合に、コンテキストに割り当て可能な ACL、正規表現、スティッキ、または Syslog バッファの最小リソース

（注） **show resource usage** コマンドを使用して、同時接続、プロキシ接続、およびその他パラメータの最小割り当て値と最大割り当て値のフルの値を表示すると、ACE 内の IXP プロセッサの両方に対応する、双方向の接続数（入力側と出力側）が表示されます。たとえば、ACE でサポートされる同時接続の最大数が 4,000,000 である場合に、**show resource usage** コマンドで同時接続の最大数が 8,000,000 と表示されるのは、各ネットワーク プロセッサの単一方向の接続数が 4,000,000 であり、ネットワーク プロセッサが 2 つあるために 2 倍されていると考えることができます。

ユーザ ロールの表示

show role コマンドを使用すると、ロール（定義済みおよびユーザ設定の）を表示できます。このコマンドの構文は次のとおりです。

show role [*name*]

name 引数には、引用符もスペースも含まない、64 文字以下の英数字のテキスト文字列でロールの一意の ID を入力します。このパラメータにより、指定した名前付きロールのみが表示されます。すべてのロールを表示するには、名前を含めずにコマンドを入力します。

たとえば、すべてのロールを表示するには、次のように入力します。

```
host1/C1# show role
```

表 3-4 は、**show role** コマンドの出力に含まれるフィールドの説明です。

表 3-4　show role コマンド出力のフィールドの説明

フィールド	説明
Role	ロールの名前（Admin など）
Description	ロールを説明するテキスト（Administrator など）
Number of Rules	ロールに関連付けられた規則の数
Rule	規則のシーケンス番号
Type	規則のタイプ。出力される値は Permit または Deny です。
Permission	規則の許可レベル。出力される値は、高い方から順に Create、Modify、Debug、および Monitor です。
Feature	規則に関連付けられたソフトウェア機能（access-list など）

ドメインの表示

show domain コマンドを使用すると、ACE で設定されているドメインに関する情報を表示できます。このコマンドの構文は次のとおりです。

show domain [*name*]

name 引数には、引用符もスペースも含まない、64 文字以下の英数字のテキスト文字列で既存のドメインの一意の ID を入力します。

以下は入力例です。

```
host1/C1# show domain D1
```

表 3-5 は、**show domain** コマンドの出力に含まれるフィールドの説明です。

表 3-5　show domain コマンド出力のフィールドの説明

フィールド	説明
Name	ドメインの一意の ID
Object Type	ドメインに関連付けられたオブジェクトのリスト（Class-map など）
Object Name	オブジェクトに設定された ID

ユーザ情報の表示

show users コマンドを使用すると、ACE に現在ログインしているユーザの情報を表示できます。このコマンドの構文は次のとおりです。

show users [*name*]

name 引数には、引用符もスペースも含まない、64 文字以下の英数字のテキスト文字列でユーザの一意の ID を入力します。

以下は入力例です。

```
host1/Admin# show users admin
```

表 3-6 は、**show users***name* コマンドの出力に含まれるフィールドの説明です。

表 3-6　show users コマンド出力のフィールドの説明

フィールド	説明
User	ユーザの名前
Context	ユーザに関連付けられたコンテキストの名前
Line	ユーザが ACE への接続に使用するポート（pts/1 など）
Login Time	ユーザが ACE にログインした月、日、および時間（Dec 7 20:11 など）
Location	IP アドレスで表示されたユーザのロケーション
Role	ユーザに割り当てられたロール（Admin など）
Domain(s)	ユーザに関連付けられたドメイン（default-domain など）

EXEC モードで **show user-account** コマンドを使用すると、ユーザ アカウント情報を表示できます。このコマンドの構文は次のとおりです。

show user-account *name*

name 引数には、引用符もスペースも含まない、64 文字以下の英数字のテキスト文字列でユーザの一意の ID を入力します。

以下は入力例です。

```
host1/Admin# show user-account admin
```

表 3-7 は、**show user-account** コマンドの出力に含まれるフィールドの説明です。

表 3-7　show user-account コマンド出力のフィールドの説明

フィールド	説明
User	ユーザの名前
Account Expiry	ユーザ アカウントの有効期限の日付（設定されている場合）
Roles	ユーザに割り当てられたロール（Admin など）
Domain	ユーザに関連付けられたドメイン（default-domain など）
Context	ユーザに関連付けられたコンテキストの名前（Admin など）

ユーザのログアウト

EXEC モードで **clear user** コマンドを使用すると、ユーザを強制的にログアウトさせる（ユーザ セッションをクリアする）ことができます。このコマンドの構文は次のとおりです。

clear user *name*

name 引数には、引用符もスペースも含まない、64 文字以下の英数字のテキスト文字列で既存のユーザの名前を入力します。

たとえば、John という名前のユーザをログアウトさせるには、次のように入力します。

```
host1/Admin# clear user John
```

コンテキストのすべての統計のクリア

EXEC モードで **clear stats all** コマンドを使用すると、コンテキスト内のすべての統計情報をクリアできます。このコマンドの構文は次のとおりです。

clear stats all

たとえば、コンテキスト C1 のすべての統計情報をクリアするには、次のように入力します。

```
host1/Admin# clear statistics all
```

コンテキストのすべての統計のクリア

INDEX